令和５年度産業サイバーセキュリティ強靭化事業

(サイバー・フィジカル・セキュリティ対策フレームワークの利活用に関する調査)

調査報告書

令和 6 年 3 月 29 日

株式会社日立製作所

目次

エクゼクティブサマリー 2

1　本事業の概要 4

1.1　目的 4

1.2　事業内容 4

1.3　実施スケジュール 4

1.4　実施体制 10

1.5　本調査報告書の構成 11

2　CPSF に関する動向等についての調査 12

2.1 本事業項目の目的 12

2.2 本事業項目の実施内容 12

2.3 本事業項目の実施結果 12

3　CPSF 等に基づく国際規格(TS 等を含む)の推進 28

3.1　本事業項目の目的 28

3.2　本事業項目の実施内容 28

3.3　本事業項目の実施結果 28

4　ガイドライン等の普及・啓発の推進 35

4.1 本事業項目の目的 35

4.2 本事業の実施内容 35

4.3 本事業項目の実施結果 35

エクゼクティブサマリー

- AI や IoT、ビッグデータ等、サイバー空間とフィジカル空間を高度に融合させるシステムによって、経済発展と社会的課題の解決を両立する人間中心の社会である「Society 5.0」の実現を目指す我が国にとって、サイバー空間とフィジカル空間を高度に融合させたシステムの社会実装を進めることが必要である一方で、つながることによるネットワーク化の進展は、悪意のある者による新たな攻撃の機会にもなっていくおそれがあり、このような脅威はあらゆる産業活動に及ぶようになってきている。

- 特に、中小の規模を含む各企業でのサイバーセキュリティ対策に加え、関連企業、取引先等のいわゆる「サプライチェーン全体」としてサイバーセキュリティ確保に向けて取り組むと同時に、サイバー攻撃は国境を越えて行われるという特性上、サイバーセキュリティ対策も国内だけの取組では十分ではなく、米欧各国等との連携を強化し、我が国の取組を積極的に国際標準に提案する等、国際ハーモナイゼーションを確保していくことを常に視野に入れた取組を推進していく必要がある。

- 本事業では、産業サイバーセキュリティ研究会等の議論や各国政府の取組及びその他国内外のセキュリティ等に関する文献等の調査を踏まえ、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の検討及び「サイバー・フィジカル・セキュリティ対策フレームワーク」(以下「CPSF」という。)等に基づく国際規格の推進を目的として実施した。

- 事業項目(1)「CPSF に関する動向等についての調査」では、令和 4 年度に実施した第 8 回第 3 層 TF での「協調的なデータ利活用に向けたデータマネジメント・フレームワーク(以下「DMF」という。)の利用イメージ(あるべき姿)」や「ルール策定社との連携の流れ(案)」について示したとおり、令和 5 年度では工場サブワーキンググループ(SWG)と連携した上で、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】」に対する DMF エッセンスの取り込み及びスマート工場を題材にしたユースケースを作成した。また、昨今、国内外で要請が高まっている機微技術に関するデータ保護のさらなる強化を目的として、米国及び欧州における機微技術保有企業や大学に対するサイバーセキュリティ確保の方法についての調査を実施し、整理を行った。

- IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等として、欧州では、この数年、規制によるものを中心にセキュリティ確保に向けたルール策定の取組が進められており、米国では、民間事業者における自発的な取組の促進を中心とした検討が進められている。日本においても、米国と同様に民間事業者における自発的な取組の促進によるセキュリティ確保を目的とした検討が進められている。中国では国家安全保障の観点からネットワーク製品に係るルール策定がなされている。IoT 機器・システムのセキュリティ確保を目的とした制度等の検討は、ここ 1～2 年で大きな変化があった。他方、一部では相互認証等の取組が進むものの、各国・各地域で個別のルールが策定されているのが現状であり、将来的に断片化した規制への対応がグローバルにビジネスを推進する事業者にとって負担としてのしかかってくることも想定される。

- サイバー空間におけるつながりの信頼性を確保するための対策要件等に関する動向等として、欧州では、European Economic Area(EEA)域内のデータ保護とデータ共有の促進を目的としたルールに係る検討が進められており、米国では、連邦法レベルや州法レベルにおいて個人データ保護に関する検討が進められている。日本では、Data Free Flow with Trust(DFFT)のコンセプトのもと、信頼性のあるデータの自由かつ安全な流通に向けて各検討が進められている。特に、日本以外のアジア諸国では、越境データ流通を規制するデータローカライゼーションの動きが顕在化している。欧州ではデータ戦略の策定に端を発する産業データ共有に向けたルール形成や各種データスペースの構築が推進され、域内デジタル経済の確立に向けた検討が具体的に進んでいる。

- 事業項目(2)「CPSF 等に基づく国際規格(TS 等を含む。) の推進」においては、CPSF をベースにした国際標準化を推進することを目的として、推進に必要な諸外国の政府、政府関連機関、業界団体又は標準化団体等によるルール形成の取組状況等の調査や、ISO/IEC 及びそれに関連する会議等における必要な働きかけの実施、CPSF 等に基づく国際規格(案)の作成等を実施した。具体的には、国際規格策定に向けた検討のロードマップを策定し、適宜必要な文献調査等を実施しつつ、サイバーセキュリティに関する国際規格の策定や維持管理を担う ISO/IEC JTC 1/SC27/WG 4(セキュリティコントロールとサービス) の国内エキスパートと連携して本件に係る国際規格策定プロジェクトの提案及び PWI (予備業務項目)、NWIP (新規作業項目提案)としてのプロジェクト推進、その他必要に応じて国内外の関係者との意見交換を行った。

- 事業項目(3)「研究会、各 WG、分野横断 SWG 及び TF の運営」においては、WG、分野横断 SWG 及び 2 つの新たな検討会(「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」、「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環に向けての検討会」)について、構成員への委嘱作業、会議等の日程調整、開催案内(出欠確認)、資料準備等といった事務的な業務を実施した。また、WG2 において、資料の作成及び貴省担当者への報告を行った。

- 事業項目(4)「ガイドライン等の普及・啓発の推進」においては、CPSF に基づくガイドライン及びユースケースを含む政府機関が公開するガイドライン等の認知・利用拡大を推進していく上での現状と課題等を整理しつつ、それに係る貴省、IPA 及び民間団体等との役割分担の明確化を図ることを目的として下記に示す調査を実施し、整理を行った。

- 中小企業における情報セキュリティ対策状況の実態を把握するため、机上調査を行った上で、中小企業を取り巻く主体として、サイバーセキュリティ関連府省庁、IT 事業者、業界団体等及び中小企業自体に対してもヒアリングを実施し、セキュリティガイドラインの普及状況や業界団体や地域コミュニティ等によるセキュリティ対策の普及活動の現状や課題等について調査を実施し、整理を行った。

- 独立行政法人情報処理推進機構(IPA)について、米国国立標準技術研究所(NIST)も参考に、デジタル戦略等における基準・標準機関として位置づけ、これまでの情報処理推進に加え、国全体のデジタル社会形成の観点から、データ戦略に係る基準・標準の整備等を推進されていることを背景に、標準策定機関が有する機能や整備されている基準・標準の体系等について、米 NIST をベンチマークとしつつ調査を実施し、整理を行った。

- サイバーセキュリティを対象とした海外の官民連携センターの設置状況及びその内容についての情報収集を通じて、官民連携センターが持つ機能や特徴、機能を果たすための具体的な取組及びその取組の結果、民間企業に対するサポートの内容を理解することを目的として調査を実施し、整理を行った。

- 海外における IT ベンダーに対する規制に対する調査を通じて、IT ベンダーに対する具体的な要求や過失が発生した場合の行政機関による働きかけの手段の有無(及びその内容)等を理解することを目的として調査を実施し、整理を行った。

- IT ベンダーとユーザー間で実際に起きた紛争の判例を整理・分析することを通じて、システム開発や運用における両者の責任分界や、その明確化がおろそかになることによる弊害及び予め両者で契約等の中で講じておくべき対策を理解することを目的として調査を実施し、整理を行った。

1 本事業の概要

1.1 目的

我が国では、AI や IoT、ビッグデータ等、サイバー空間とフィジカル空間を高度に融合させるシステムによって、経済発展と社会的課題の解決を両立する人間中心の社会である「Society 5.0」の実現を目指している。「Society 5.0」を実現するためには、サイバー空間とフィジカル空間を高度に融合させたシステムの社会実装を進めることが必要である一方、「つながる」ことによるネットワーク化の進展は、悪意のある者にとっての新たな攻撃の機会にもなっていくおそれがある。

サイバー攻撃の起点が急激に拡大し、攻撃の手法も高度化しているため、サイバー攻撃の脅威は、あらゆる産業活動に及ぶようになっている。このような状況下では、各企業でのサイバーセキュリティ対策に加えて、関連企業、取引先等、サプライチェーン全体としてサイバーセキュリティ確保に向けて取り組む必要がある。また、サイバー攻撃は国境を越えて行われるものであり、サイバーセキュリティ対策も国内だけの取組では十分ではなく、米欧各国等との連携を強化し、我が国の取組を積極的に国際標準に提案する等、国際ハーモナイゼーションを確保していくことを常に視野に入れた取組を進めていく必要がある。

本事業では、産業サイバーセキュリティ研究会等の議論や各国政府の取組及びその他国内外のセキュリティ等に関する文献等の調査を踏まえ、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の検討及び CPSF 等に基づく国際規格の推進を目的として実施するものである。

1.2 事業内容

本事業ではこの目的を達成するため、大きく分けて 4 つの事業項目を実施した。本事業において実施した事業内容を図表 1-1 に示す。

図表 1-1 本事業の事業項目と具体的な実施内容

No	事業項目	仕様書の内容	具体的な実施内容
1	CPSF に関する動向等についての調査	【事業内容】 本事業では、CPSFに関し、サイバー空間におけるつながりの信頼性を確保するために求められる外国政府の取組やその他国内外のデータのセキュリティ対策及びそれらの信頼性の確認手法等を調査する。想定する調査項目例を以下に示すが、具体的な調査項目については、商務情報政策局サイバーセキュリティ課の担当者(以下「担当者」という。) と協議の上で決定する。 なお、タスクフォースでの議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。 ＜想定する調査項目の例＞ ●ステークホルダー間でのデータの流通や利活用に向けた国内外の政策動向 ●既に国内外で策定されているデータ等のセキュリティ確保を目的とした制度やガイドライン等の概要(国・地域、適用分野、策定者、対象者、遵守義務、普及状況等) ●データ等の差異や区分(カテゴリー)に応じて異なるセキュリティ水準及びセキュリティ対策が求められている場合には、当該セキュリティ水準及びセキュリティ対策の内容	工場 SWG 事務局や構成員と連携しつつ、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】」に対するデータマネジメント・フレームワーク(DMF)エッセンスの取り込み及びスマート工場を題材にしたユースケースを作成し、第３層 TF の委員にも確認していただいた上で、貴省 HP での公表について支援した。 昨今国内外で要請が高まっている機微技術に関するデータの保護のさら

No	事業項目	仕様書の内容	具体的な実施内容
		●データ等の信頼性を確認するための技術的又は制度的枠組み ●データ等の信頼性を確認する等を目的として策定されているガイドライン等の普及に関する現状と課題 ＜調査報告書における論点の例＞ ●データの区分(カテゴリー)に関する考え方 ●上記の区分に沿ったセキュリティ対策例 ●上記の区分に沿ったデータの信頼性の確認方法 【実施方法】 ・公開情報(外国政府・国際標準化団体の報告資料、国内外の専門誌等を含む。)、国内外のニュース記事、商用データベース等の調査により実施する。調査結果の妥当性確認等を目的として、必要に応じて有識者(国外の有識者を含む各３名程度)に対して面談によるヒアリングを実施することが望ましい。ただし、国外の有識者に対しては電話又はテレビ会議によるヒアリングでもよい。 ・日本に加えて、少なくとも米国、欧州を調査対象の国・地域に含め、３つ以上の国・地域の調査を行う。また、外国語の調査結果や報告資料は日本語に翻訳する。	なる強化を目的として、海外における機微技術保有企業や大学に対するサイバーセキュリティ確保の方法についての調査を行い、本調査報告処理に取りまとめた。
2	CPSF 等に基づく国際規格(TS 等を含む)の推進	【事業内容】 本事業では、日本企業の競争力強化に寄与する国際的なルールを形成していくことを目的とし、ルール形成を構成する一要素になりうるCPSF等をベースにした国際標準化を推進する。具体的には、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理、リスク評価、セキュリティ対策に関する、諸外国の政府又は政府関連機関、業界団体のルール形成の取組状況や、標準化機関における標準化の動向等を調査しつつ、サイバーセキュリティに関する国際的なフレームワークについて、CPSF等の考え方をベースにしたものが採用されるよう必要な働きかけ・検討を行う。 想定する調査項目例を以下に示すが、具体的な調査項目については、担当者と協議の上で決定する。 なお、有識者等との議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。 ＜想定する調査項目の例＞ ●CPSF等に基づく国際規格(TS)策定に向けた具体的なロードマップの提示 ●上記ロードマップに基づく、国内外の関係機関・関係者の巻込みやそのために必要な資料の作成等の実施 ●CPSF等に基づく国際規格策定に向けたドラフト文書の作成、及び国内外の関係機関・関係者との意見交換を踏まえたドラフト文書の更新 ●米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的と	国際規格策定に向けたロードマップを策定し、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理に関する国際的なルール形成の状況を調査しつつ、サイバーセキュリティに関する国際的なフレームワークについて、CPSFの考え方をベースにしたものが採用されるよう、特に前回投票時に賛成だったが積極貢献を表明しなかった国及び棄権票を投じた国のエキスパートに対して、個別の働きかけを実施した。 CPSF等に基づく規格策定に係る具体的なプロジェクトであるISO/IEC WD 5689は、NWIP投票にて可決され、WDの段階に移り、WD第1版をベースに規格(案)を作成

No	事業項目	仕様書の内容	具体的な実施内容
		したリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関係する国際規格、ガイドライン、フレームワーク、政策文書等の調査 上記調査は、文献(国内外の公的機関や標準化機関の公表資料、国内外の専門誌等)、インターネット、意見交換等により実施する。意見交換の対象の国内外の公的機関・有識者・組織や意見交換の内容は実施者が提案することし、担当者と協議の上、決定する。また、必要に応じて国際会議に参加し、日本のCPSFに基づくセキュリティ対策の考え方について諸外国の公的機関と意見交換等を行い、CPSF等に基づく国際標準化を推進すること。加えて、当該意見交換等については、関連するISO/IECの日本のエキスパート等と協力し、可能な限り効果的な方法で行うこと。なお、意見交換を英語で行った場合には、議事概要は日本語に翻訳すること。 【実施方法】 ・公開情報(外国政府・国際標準化団体の報告資料、国内外の専門誌等を含む。)、国内外のニュース記事、商用データベース等の調査により実施する。調査結果の妥当性確認等を目的として、必要に応じてセキュリティの国際標準に精通した有識者(国外の有識者１名以上を含む、３名以上)に対して面談によるヒアリングを実施することが望ましい。ただし、国外の有識者に対しては電話又はテレビ会議によるヒアリングでもよい。また、必要に応じて国際会議に参加することが望ましい。 ・日本に加えて、少なくとも米国、欧州を調査対象の国・地域に含め、3つ以上の国・地域の調査を行う。また、外国語の調査結果や報告資料は日本語に翻訳する。 ・CPSF等に基づく国際規格策定に向けた活動は、ISO/IECの日本のエキスパート等と協力しながら進める。	した。 米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的としたリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関係する国際規格、ガイドライン、フレームワーク、政策文書等の調査を実施し、本調査報告書に取りまとめた。
3	研究会、各WG、分野横断ＳWG 及び TF の運営	【事業内容】 研究会、各WG、分野横断サブワーキンググループ(SWG)及びタスクフォース(TF)の運営本事業では、上記(1)の調査及び検討に関連して、専門的な視点からの検討、分析及び助言を得るために、以下①から⑥までに示す研究会、各WG、分野横断SWG及びTF等(以下①から⑥までをまとめて「研究会等」という。)を以下の要領にて運営を行い、令和5年度中に合計15回程度開催する。 研究会等の構成及び構成員については、別紙を参照すること。 なお、これまでの開催実績を基に別紙を作成しているため、令和5年度においては肩書きや構成員の変更が生じる可能性があることや、新たに研究会等を設置する可能性があることに留意すること。 ①　産業サイバーセキュリティ研究会 大所高所から政策や産業界の取組を議論する。研究会の構成員(10名程度)は、産学を代表する有識者とし、担当者が指定す	WG、分野横断SWG及び2つの新たな検討会(「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」、「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環に向けての検討会」)について、構成員への委嘱作業、会議等の日程調整、開催案内(出欠確認)、資料準備等といった事務的な業務を実施した。 また、WG2において、

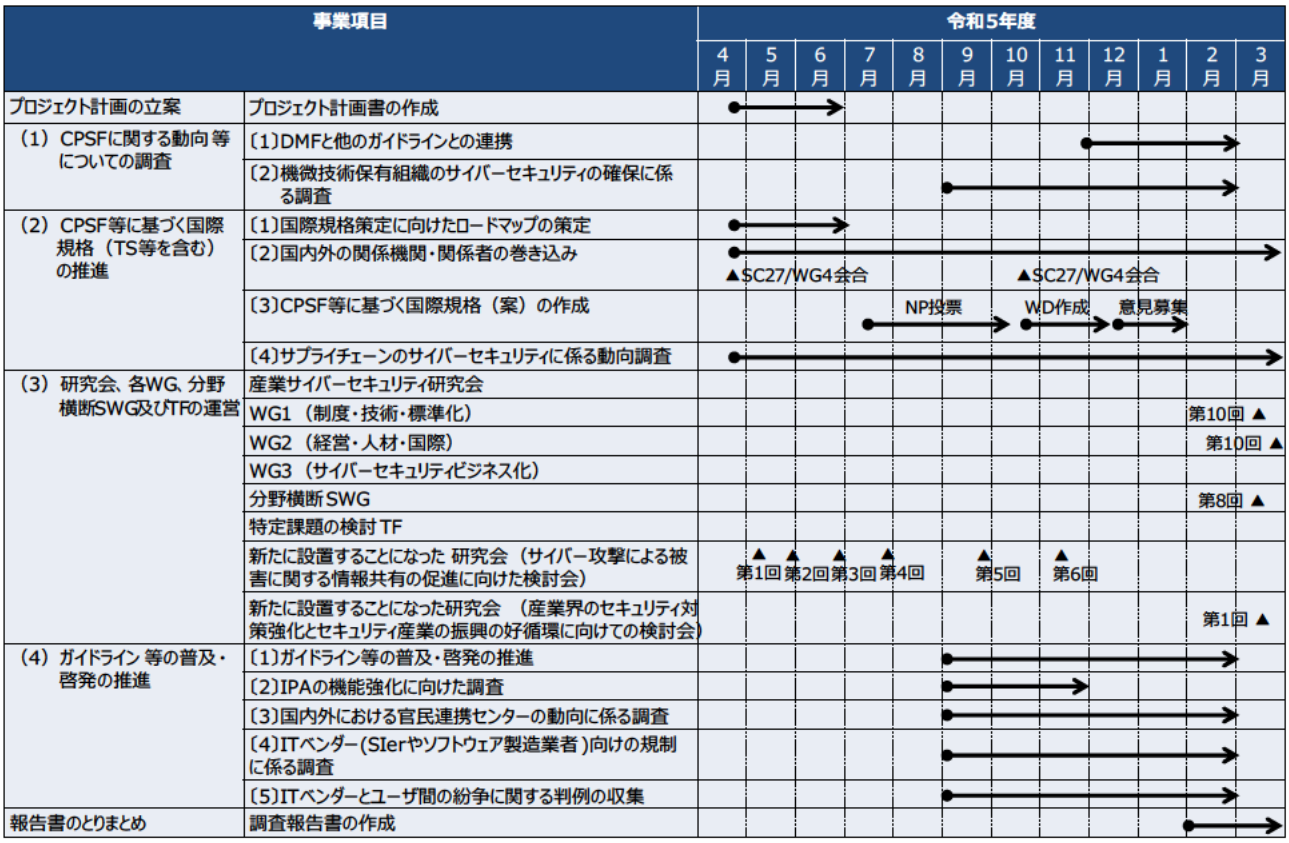
Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		る。 ② WG1(制度・技術・標準化)・分野横断SWG 制度、技術、標準化の関連政策を一体的に政策展開する戦略を議論する。ＷＧの構成員(15～20名程度)は、産学の有識者とし、担当者が指定する。 ③ WG2(経営・人材・国際) サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を議論する。WGの構成員(10～15名程度)は、産学の有識者とし、担当者が指定する。 ④ ＷＧ3(サイバーセキュリティビジネス化) セキュリティサービス品質向上と国際プレイヤー創出に係る政策を議論する。ＷＧの構成員(10～15名程度)は、産学の有識者とし、担当者が指定する。 ⑤ 特定課題の検討TF TFにおいて、(1)の調査結果に基づいて、サイバー空間におけるつながりの信頼性を議論する。TFの構成員(15名程度)は、産学の有識者とし、担当者が指定する。 ⑥ その他、担当者との相談により、新たに設置することになった研究会 新たな研究会を設置することになった場合、研究会の構成員等の詳細は、担当者と協議の上、決定する。 【実施方法】 ・研究会等の開催に当たっては、構成員との日程調整、開催案内(出欠確認)、会場確保(基本的に経済産業省又は経済産業省近郊で開催する。経済産業省以外の会場は、委託先において確保する。Web開催の場合は、経済産業省が指定するオンライン会議システムにより会議を主催する。)、資料準備(印刷等含む。)、会議の議事録の作成(研究会等の開催後に速やかに作成し、経済産業省に対して提出する。)等といった事務的な業務を全て行う。加えて、令和４年度に開催した研究会等に関する事務的な業務を事後的に実施する必要がある場合、担当者と協議の上、決定する。なお、実施に係る経費については事業費に計上する。 ・(3)⑤のTF、⑥の研究会については、(1)(2)の調査に基づく議論を行う場合には資料の作成及び報告を行う。 ・研究会等の資料のうち、国際ハーモナイゼーション及び我が国の取組の海外発信の観点に基づき、担当者との協議に基づいて必要と判断した資料について英訳を行う。	資料の作成及び貴省担当者への報告を行った。
4	ガイドライン等の普及・啓発の推進	【事業内容】 CPSFに基づくガイドライン等の普及・啓発の推進について、様々な産業界での普及・拡大を進めることを目的とし、普及・啓発活動を推進する。具体的には、様々な産業界におけるCPSFやこれに連な	CPSFに基づくガイドライン及びユースケースを含む政府機関が公開するガイドライン等の認知・利用拡

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		るガイドラインやユースケース等の認知・普及の拡大に向けた課題の調査や対策の検討を実施する。具体的な調査項目や実施内容については、担当者と協議の上で決定することとし、(3)に示す研究会等での議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。 　加えて、CPSFに基づき整備が進んでいるガイドラインやユースケース等の認知・拡大を推進していく上での現状と課題等を整理し、調査報告書にまとめる。調査報告書の具体的な内容については担当者と協議の上で決定する。 【実施方法】 ・CPSF等に基づくガイドライン等の普及・啓発の推進に当たっては、様々な産業界の団体や企業等に対するニーズに関するヒアリングやアンケート等、いかなる方策が効果的かを立案しつつ、担当者と具体的な実施方針等について協議を行った上で実施する。	大を推進していく上での現状と課題等を整理及びそれに係る貴省、IPA及び民間団体等との役割分担の明確化を図ることを目的として調査を実施した。 　中小企業における情報セキュリティ対策状況の実態を把握するため、机上調査を行った上で、中小企業を取り巻く主体として、サイバーセキュリティ関連府省庁、IT事業者、業界団体等及び中小企業自体に対してもヒアリングを実施し、セキュリティガイドラインの普及状況や業界団体や地域コミュニティ等によるセキュリティ対策の普及活動の現状や課題等について調査を行った。 　独立行政法人情報処理推進機構(IPA)について、米国国立標準技術研究所(NIST)も参考に、デジタル戦略等における基準・標準機関として位置づけ、これまでの情報処理推進に加え、国全体のデジタル社会形成の観点から、データ戦略に係る基準・標準の整備等を推進されていることを背景に、標準策定機関が有する機能や整備されている基準・標準の体系等について、米NISTをベンチマークとしつつ調査を実施した。 　サイバーセキュリティを対象とした海外の官民連携

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
			センターの設置状況及びその内容についての情報収集を通じて、官民連携センターが持つ機能や特徴、機能を果たすための具体的な取組及びその取組の結果、民間企業に対するサポートの内容を理解することを目的として調査を実施した。 　海外におけるITベンダーに対する規制の整理を通じて、ITベンダーに対する具体的な要求や過失が発生した場合の行政機関による働きかけの手段の有無(及びその内容)等を理解することを目的として調査を実施した。 　ITベンダーとユーザー間で実際に起きた紛争の判例を整理・分析することを通じて、システム開発や運用における両者の責任分界や、その明確化がおろそかになることによる弊害及び予め両者で契約等の中で講じておくべき対策を理解することを目的として調査を実施した。

1.3　実施スケジュール

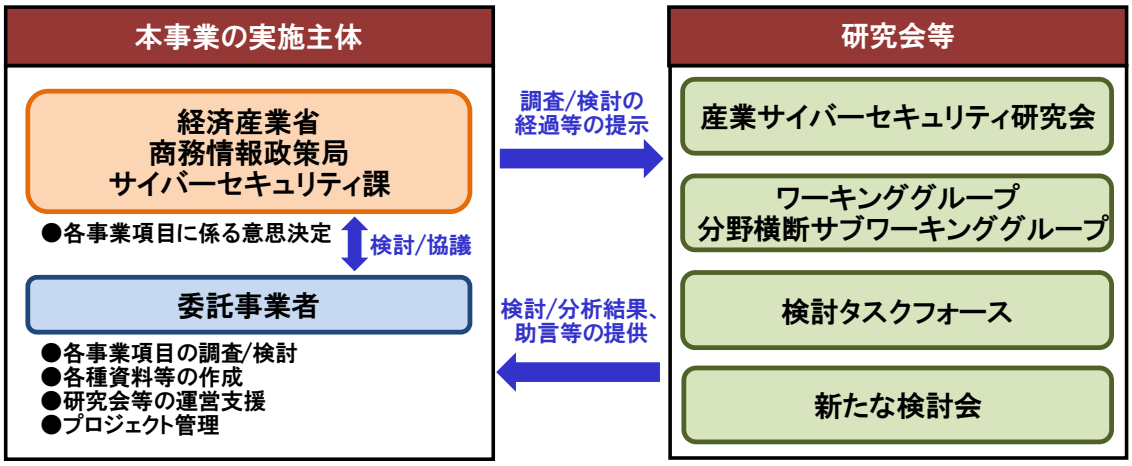
本事業の実施スケジュールを図表 1-2 に示す。「CPSF に関する動向等についての調査」、「CPSF 等に基づく国際規格(TS 等を含む)の推進」、「ガイドライン等の普及・啓発の推進」及び「研究会、各 WG、分野横断 SWG 及び TF の運営」について、産業サイバーセキュリティ研究会、WG、ならびに新たに設置した検討会における議論や助言を踏まえて内容の検討を推進した。



図表 1-2 本事業の実施スケジュール

1.4　実施体制

本事業は、プロジェクトオーナーである貴省商務情報政策局サイバーセキュリティ課と委託事業者が、事業項目(1)、事業項目(2)及び事業項目(4)について検討・協議を実施するとともに、その内容に関して産業サイバーセキュリティ研究会の研究会等における検討や助言等を踏まえながら推進した。本事業の実施体制を図表 1-3 に示す。



図表 1-3 本事業の実施体制

1.5 本調査報告書の構成

本調査報告書では、４つ提示されている事業項目のうち、「研究会、各 WG、分野横断 SWG 及び TF の運営」を除いた、「CPSF に関する動向等についての調査」、「CPSF 等に基づく国際規格(TS 等を含む)の推進」、「ガイドライン等の普及・啓発の推進」について、それぞれ目的、実施内容、実施結果を報告する。

- 第 2 部では、「CPSF に関する動向等についての調査」の目的、実施内容及び実施結果を報告する。
- 第 3 部では、「CPSF 等に基づく国際規格(TS 等を含む)の推進」の目的、実施内容及び実施結果を報告する。
- 第 4 部では、「ガイドライン等の普及・啓発の推進」の目的、実施内容及び実施結果を報告する。

2　CPSF に関する動向等についての調査

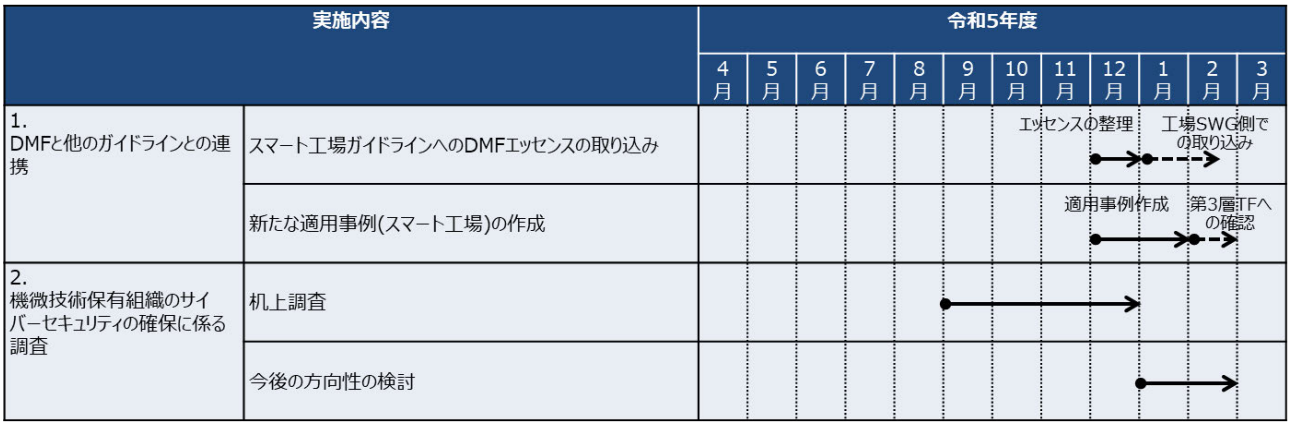
2.1 本事業項目の目的

本事業項目では、CPSF に関し、サイバー空間におけるつながりの信頼性を確保するために求められる外国政府の取組やその他国内外のデータに係るセキュリティ対策及びそれらの信頼性の確認手法等を調査することを目的とした。

2.2 本事業項目の実施内容

上記目的を達成するため、貴省担当者との協議の上、以下の 1～2 を実施内容として整理し、第 3 層 TF の枠組みの中で DMF と他のガイドラインとの連携の推進と外国政府等の取組調査の中で機微技術保有組織のサイバーセキュリティの確保に係る調査を行った。

＜本事業項目の実施内容＞
1. DMF と他のガイドラインとの連携
2. 機微技術保有組織のサイバーセキュリティの確保に係る調査



図表 2-1 本事業項目の実施スケジュール

2.3 本事業項目の実施結果

2.3.1 DMF と他のガイドラインとの連携

令和 4 年 2 月に実施された第 8 回第 3 層 TF[1] では、「DMF の利用イメージ(あるべき姿)」や「ルール策定者との連携の流れ(案)」が提示され、工場 SWG におけるスマート工場分野が連携先の 1 つとして示された。当該会合で合意された方針に基づき、工場 SWG 事務局や構成員と連携を図りながら、DMF に係るユースケースの作成等を推進した。

工場 SWG では、工場システムのセキュリティ対策を実施する上で参考となるような考え方やステップを示す「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」[2] を昨年度に公表するとともに、今年度は「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】」[3](以下、「工場ガイドライン」という。) の公表に向けた検討を進めていたところ、貴省担当者及び工場 SWG 構成員と協議を行い、以下 2 点を DMF に係る具体的な活動とすることについて当事者間で合意した。

① スマート工場ガイドラインへの DMF エッセンスの取り込み

② 新たな適用事例(スマート工場)の作成

以下、①、②のそれぞれについて、実施内容や経過を示す。

① スマート工場ガイドラインへの DMF エッセンスの取り込み

DMF の分析観点を考慮し、現在策定されているスマート工場ガイドラインへの以下の項目に関する追記を検討した。検討の際には、入力、出力及び処理のそれぞれにおいて、リスク(源)と実施が望ましい対策を整理した。

・ データの取扱いに際して想定されるリスク

<信頼できる入力へのリスク>

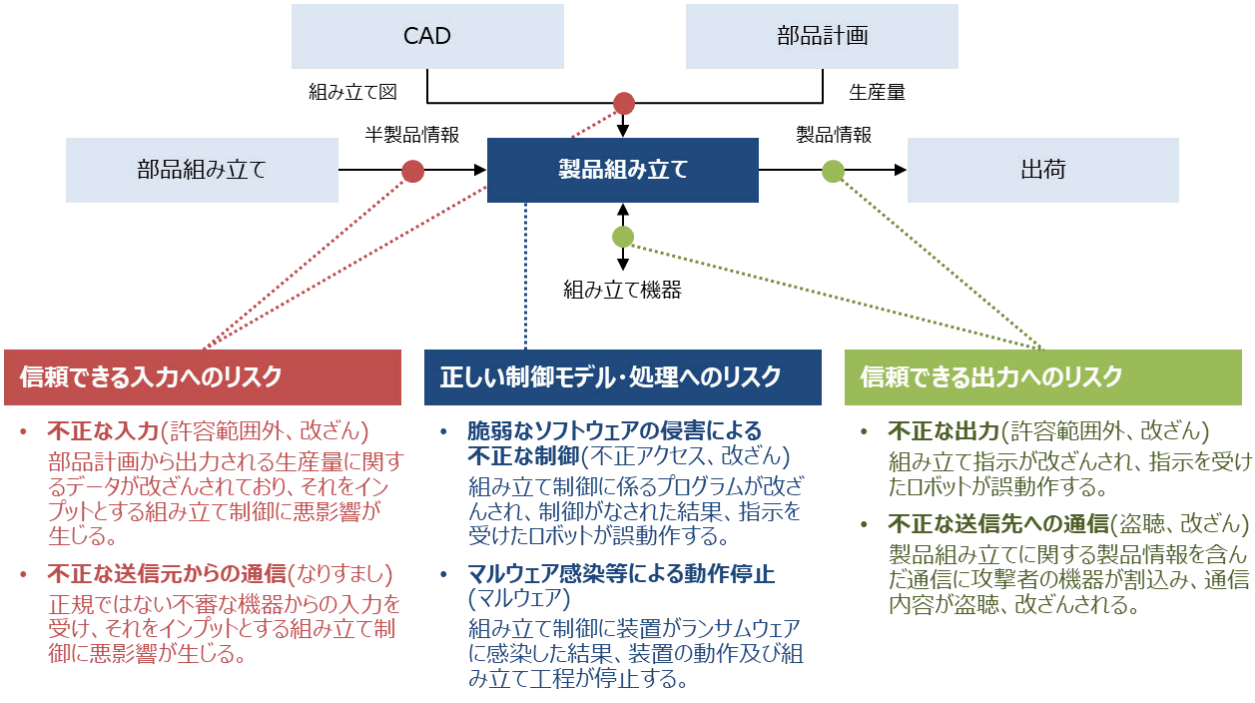
・ 不正な入力(許容範囲外、改ざん):部品計画から出力される生産量に関するデータが改ざんされており、それをインプットとする組立て制御に悪影響が生じる。
・ 不正な送信元からの通信(なりすまし):正規ではない不審な機器からの入力を受け、それをインプットとする組立て制御に悪影響が生じる。

<正しい制御モデル・処理へのリスク>

・ 脆弱なソフトウェアの侵害による不正な制御(不正アクセス、改ざん):組立て制御に係るプログラムが改ざんされ、制御がなされた結果、指示を受けたロボットが誤動作する。
・ マルウェア感染等による動作停止(マルウェア):組立て制御に装置がランサムウェアに感染した結果、装置の動作及び組立工程が停止する。

<信頼できる出力へのリスク>

・ 不正な出力(許容範囲外、改ざん):組立て指示が改ざんされ、指示を受けたロボットが誤動作する。
・ 不正な送信先への通信(盗聴、改ざん):製品組立てに関する製品情報を含んだ通信に攻撃者の機器が割り込み、通信内容が盗聴、改ざんされる。



図表 2-2 想定されるリスク

・　実装・対策要件

講じるべき対策内容(例)とその分類は以下のとおり。講じるべき対策内容(例)を具体化する際には、IEC62443[4]及び NIST SP 800-82 Rev.3[5]を参考とした。

また、対策の実装にあたっては、以下に示すセキュリティ観点の情報に加え、「ポステルの原則」(入力の多様性には寛容に、出力は厳密にするという設計原則)等で示されるようなユーザビリティに関連した事項にも配慮しつつ対応を具体化していくことが望ましい。

図表 2-3 講じるべき対策内容

分類		講じるべき対策内容(例)
入力の信頼確保に資する対策	入力値の検証	● 文字セット、長さ、数値範囲、許容値を含む、システム入力の構文等を確認することで、入力が指定されたフォーマット及びコンテンツ規定と一致することを検証する。 ● 入力の妥当性確認の際に生じたエラーを定期的にレビューして解決する。
		● 通信内容に対する許可されていない変更(改ざん)を検出し、報告及び防御する。
	送信元の検証	● 機器間のネットワーク接続を確立する前に、通信相手を一意に識別し認証する。認証のルールは、機器の種類等考慮して規定され、自組織が管理しない機器も含まれ得る。 ※ 制御システムで利用されるプロトコルには認証等のセキュリティ機能が備えられていないものもあることから、当該プロトコルは制御ネットワーク内でのみ許可し、IT ネットワークへの進入は許可しない等の配慮を行うことが望ましい。 ● システムのセキュリティ分類や事業要件に基づき、認証強度を決定する。 ● 信頼できないネットワーク経由のすべてのアクセスを監視し、制御する。
正しい制御モデル・処理に資する対策	ソフトウェアに実装するセキュリティ機能	● 以下のセキュリティ機能をソフトウェアに実装する。 - 工場固有の特性・要件(システムのパフォーマンス等)を考慮した方法により、アクセス元を一意に識別し認証する。 - 権限付与においては最小権限の原則を採用し、割り当てられた仕事を遂行するのに必要なユーザ(又はその代わりとなるプロセス)だけに権限を与える。
		● 多層防御を前提として、端末やサーバ等のエンドポイント及びネットワーク上の任意のポイントで悪意のコードや不正なソフトウェアの影響を、検出し、管理者へ報告する機能を実装する。 ● 不正な挙動やマルウェア等が検出されたエンドポイントを素早くネットワークから隔離し、システム全体に対する影響を軽減させるために必要な機能を実装する。

分類		講じるべき対策内容(例)
	セキュア開発プロセス	● システムやソフトウェアのライフサイクルを考慮し、例えば以下のものを含むセキュリティ対策を講じる。 ✓ ソフトウェア開発のためのセキュリティ要件を定義する。 ✓ セキュアコーディングの原則を遵守してソースコードを作成する。 ✓ ソフトウェア開発のための安全な環境を実装し維持する。 ✓ テスト及び計画的な保守の際、セキュリティ機能の動作を検証し、異常が検出された場合にレポートする。
	サイバーレジリエンス	● 緊急時・システム障害時・災害時に業務を維持・復旧するために緊急時対応計画を作成する。
		● 重要な業務関連データ及びシステムデータ(ログ等)のバックアップを取得するため、通常の操業に影響を与えないようインフラを整備する。バックアップを行う機能は自動化されていることが望ましい。
		● 障害や異常が発生した後、既知のセキュアな状態に回復及び再構成する機能をシステムに実装する。
出力の信頼確保に資する対策	出力値の検証	● 業務処理を行うソフトウェアから出力された情報を検証し、情報が期待される内容と一致していることを確認する。当該確認プロセスでは、無関係なコンテンツ(例：SQL インジェクションを含む特定の攻撃)を検知し、そのようなコンテンツが出力されないようにし、異常な動作が検出されたことを監視ツールにアラートする。
	送信先の検証	● [送信元の検証]と同様

② 新たな適用事例(スマート工場)の作成

これまで作成してきたユースケースと同様の方法で、スマート工場を題材に DMF の適用事例を作成した。更新した適用事例を既に公開されている DMF に追加し、Version1.1 として経産省の HP 上で公開[6]した。

新たに作成したユースケースは、日本国内の ATM・金融端末の生産工場において、板金加工工程に係る作業を可視化し業務効率化に役立てることを目的とする工場の製造部門によるデータ取得、加工プロセスを対象とした。

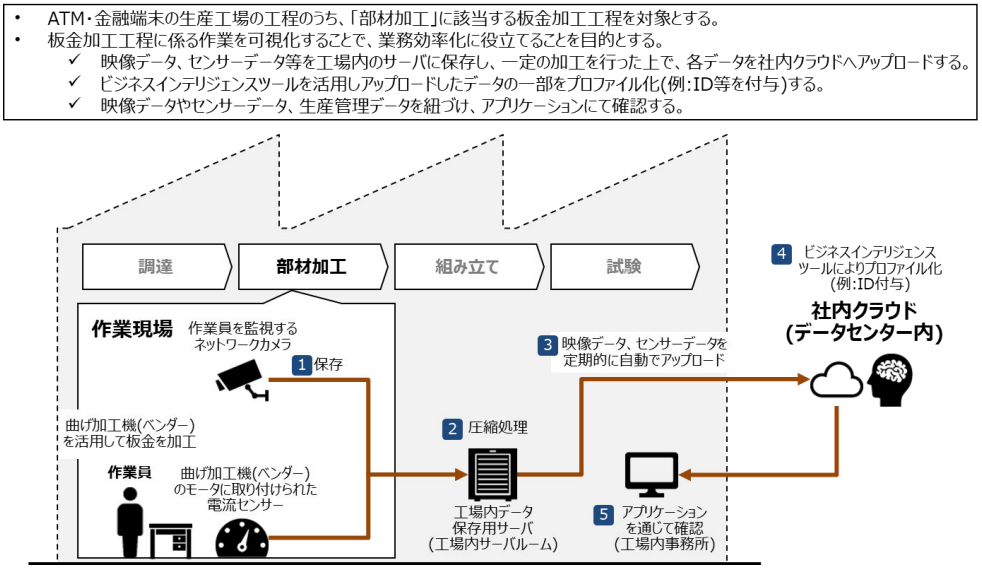
ATM・金融端末の生産工場における調達、部材加工、組み立て、試験の 4 つのステップのうち、部材加工作業をデータ取得の対象とする。

・ 作業員は曲げ加工機(ベンダー)を活用して板金を加工する。作業現場では、例えば以下のデータを取得、加工する。
  - ➢ 作業現場において作業員を監視するネットワークカメラにて取得した映像データ
  - ➢ 曲げ加工機(ベンダー)のモータに取り付けられた電流センサーにて取得したセンサーデータ

・ 以下に示すプロセスにてデータを取得、加工する。
  ① 以下に示すプロセスで各データを保存用サーバに保存する。
  - ➢ 作業員を監視するネットワークカメラにて映像データを取得し、工場内に設置されたデータ保存用サーバに保存する。
  - ➢ 曲げ加工機(ベンダー)のモータに取り付けられた電流センサーにてセンサーデータを取得

し、同じデータ保存用サーバに保存する。
② データ保存用サーバにて映像データ等を圧縮処理する。
③ 圧縮処理した映像データ及びセンサーデータを社内クラウドへ定期的に自動でアップロードする。
④ 社内クラウド上でビジネスインテリジェンスツールを活用しプロファイル化(例:ID 付与)を行う。

・ ID によって紐づけられた映像データやセンサーデータ、生産管理データを社内クラウドのアプリケーションを通じて確認する。ただし、現時点で現場改善を目的としたデータの利活用を想定しており、社外への公開は想定していない。
・ 本ユースケースでは、新規でシステム構築を行うとともに、工場内の制御システムとは接続しないことを想定する。



図表 2-4 ユースケースの概要

上記ユースケースは、工場 SWG の委員と連携を行った上で作成した。作成する際に工場 SWG の委員から頂戴した意見は随時反映した。

<工場 SWG の委員から頂戴した主なご意見>

・ DMF では、保護すべき個々のデータに着目した上で AIC が評価基準となるが、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」ではゾーン全体のセキュリティに着目した上で、業務への影響度が評価基準となる。
・ DMF とスマート工場のガイドライン間の差を埋めるためには、その違いを埋めるための別のモデルが必要となる。

上記ユースケースを作成した後に、1/29 から 2/9 の期間で第 3 層 TF 委員に内容を確認いただいた。頂戴したご意見を踏まえて、適宜修正を加えた上で、2/19 から 2/16 の期間で第 3 層 TF 委員に再度ご確認いただいた。

<第 3 層 TF の委員から頂戴した主なご意見>

・ 「プロファイル化された映像データ」の定義を明確にした方がよい。
・ 特定された脅威分類について、「適法な手段によるデータ取得」ではなく「違法な手段によるデータ取得」とした方が理解しやすい。

③ まとめ

・ 昨年度実施した第 8 回第 3 層 TF において示された「DMF の利用イメージ(あるべき姿)」や「ルール策定社との連携の流れ(案)」にあるとおり、今年度の検討では工場 SWG と連携した上で、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上

でのポイント】」に対する DMF エッセンスの取り込みやスマート工場を題材にしたユースケースを作成することができた。

- 一方で、工場 SWG と連携したことによって、他のセキュリティアセスメントとの違い(例:ゾーンの設定に関する考え方)が浮き彫りになるとともに、その違いを埋めるためのモデルの必要性を認識した。
- 今後は、信頼ある企業間データ流通・利活用の促進を目的として、上記の課題を考慮しつつ、さらに他の分野との連携や他団体(例:地方公共団体)等への適用を行うことが重要と考えられる。

2.3.2 機微技術保有組織のサイバーセキュリティの確保に係る調査

本項では、昨今国内外で要請が高まっている機微技術情報に関するデータの保護のさらなる強化を目的として、海外における機微技術情報保有企業や大学に対するサイバーセキュリティ確保の方法についての調査を行った。

- 調査内容

本調査は、表 2-5 に示す調査項目のそれぞれについて、米国及び EU(EU 単位で推進されるものに加え、一部加盟国単位のものも含む)及び英国における取組を対象として行った。

その際、大学や各種研究所等の研究機関を対象としたものと営利を目的とした企業を対象としたものは別個の体系をなしていると考えられることから、内容としてはそれらを分ける形で調査を推進した。

図表 2-5 主な調査項目

No	分類	調査項目	整理の観点等
1-1	大学を対象にした取組	リスクに対する考え方	● 「研究インテグリティ」(研究の国際化やオープン化に伴う新たなリスクに対して新たに確保が求められる研究の健全性・公正性)、「研究セキュリティ」の全体像 ● 全体像におけるサイバーセキュリティの位置づけと具体的な脅威認識 ● 具体的なインシデント事例
1-2		対象となる事業、情報の分類等	● 規制対象となっている対象の類型(例：政府資金活用の有無) ● 機微技術情報として扱う情報の類型
1-3		具体的な要求事項の内容	● 政府機関又は資金配分機関から大学・その他の研究機関及び研究者に課せられるセキュリティ要求事項 ● 上記要求事項を実施するにあたり指摘されている現状の課題
2-1	企業を対象にした取組	リスクに対する考え方	● 念頭に置くリスクの全体像 ● 全体像におけるサイバーセキュリティの位置づけと具体的な脅威認識 ● 具体的なインシデント事例
2-2		対象となる事業、情報の分類等	● 規制対象となっている対象の類型(例：政府資金活用の有無) ● 機微技術情報として扱う情報の類型
2-3		具体的な要求事項の内容	● 企業及び技術者に課せられるセキュリティ要求事項 ● 上記要求事項を実施するにあたり指摘されている現状の課題
3-1	対応事例	機微技術情報等漏えい後の対応事例	● 機微技術情報漏えい発覚後の一般的な対応の流れ ● 事案の概要、対応のタイムライン ● 行政機関及び司法機関の対応

- 調査結果

● 大学を対象にした取組

昨今、大学や研究機関からの大規模な機微技術情報の漏えい等を受けた研究インテグリティ、研究セキュリティ強化の世界的な潮流がある中で、欧米の双方にて対策の義務化を伴う取組が進められている。

＜米国政府による取組状況＞

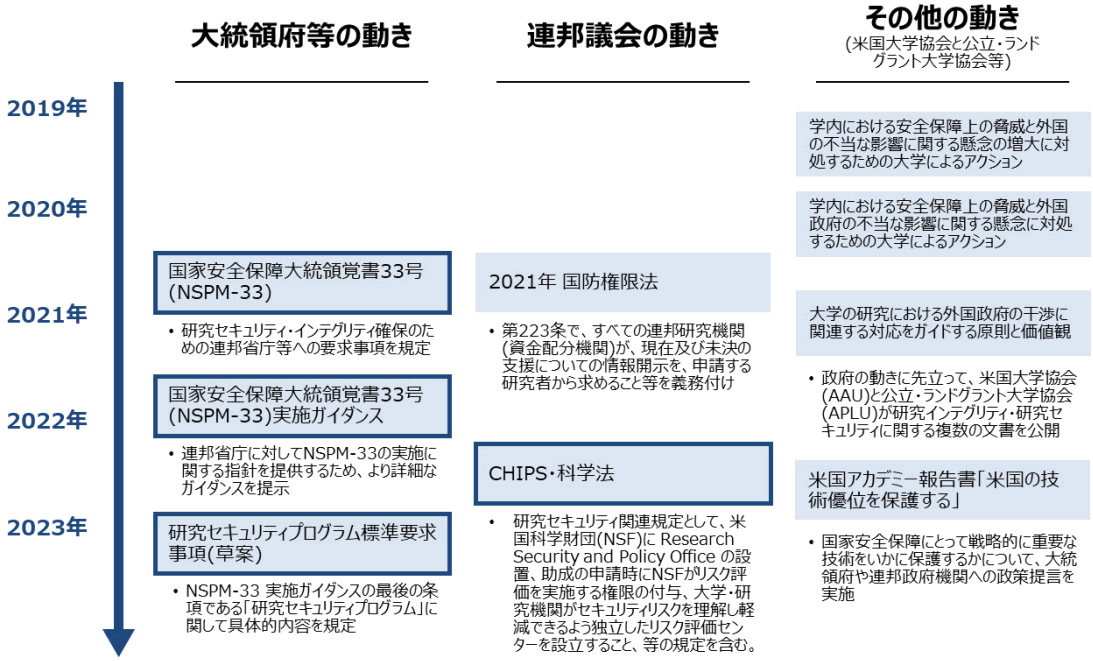
取組の背景

米国では、80 年代の国家安全保障決定 189 号(NSDD-189)に代表されるように、可能な範囲で、オープンサイエンス(科学の開放性)原則の優位性を確認してきた。

一方で最近では、2018 年に表面化した米中貿易摩擦からハイテク技術覇権争いにまで発展した議論の中で、オープンサイエンス原則が悪用され、国家安全保障の脅威になりかねないという問題が提起されており、開放性原則に制限をかける必要性をめぐる議論が、主要な連邦ファンディング機関や研究コミュニティを中心に改めて喚起されつつある。

近年の主な取組

「取組の背景」に示した動向を受け、研究活動に対する統制(研究セキュリティ・研究インテグリティ)について、2019 年から政府外での動きが現れ、2021 年以降に大統領府及び連邦議会でのルール形成が盛んに実施されている。



図表 2-6 米国における研究セキュリティ関連施策

中でも連邦政府による主要な動きとして、トランプ前政権の政権交代直前である 2021 年 1 月 14 日に発出された「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」(National Security Presidential Memorandum-33(NSPM-33))[7] 及びそれに続くガイドライン、要求事項の策定が挙げられる。NSPM-33 では、「中華人民共和国を含む一部の外国政府は、開かれた科学的交流への相互献身を示しておらず、研究を行うためのコストとリスクを回避するために、米国及び国際的に開かれた研究環境を利用しようとし、それによって、米国、その同盟国、パートナーを犠牲にして、経済及び軍事競争力を向上させようとしている」と説明し、「米国政府が支援する研究開発(R&D)を、外国政府の干渉や搾取から守るための行動を指示する」としている。また、NSPM-33 に基づき、主に連邦政府から研究資金の配分を受けている大学又は研究機関が遵

守すべき具体的な対策を示す文書として、2022 年 1 月 4 日に、「NSPM-33 実施ガイダンス」(Guidance for Implementing National Security Presidential Memorandum 33(NSPM-33))[8]、2023 年 2 月 28 日に「研究セキュリティプログラム標準要件案(DRAFT Research Security Programs Standard Requirement)」[9]が公表されている。

特に、「研究セキュリティプログラム標準要件案」では、NSPM-33 の規定を踏まえ、サイバーセキュリティ対策を含む研究セキュリティプログラムを義務的に適用すべき組織の条件や、具体的なサイバーセキュリティ要件等が示されており、覚書の公開(現状草案の段階)から 1 年以内の要求適合が求められる。

＜標準要件案の適用対象＞

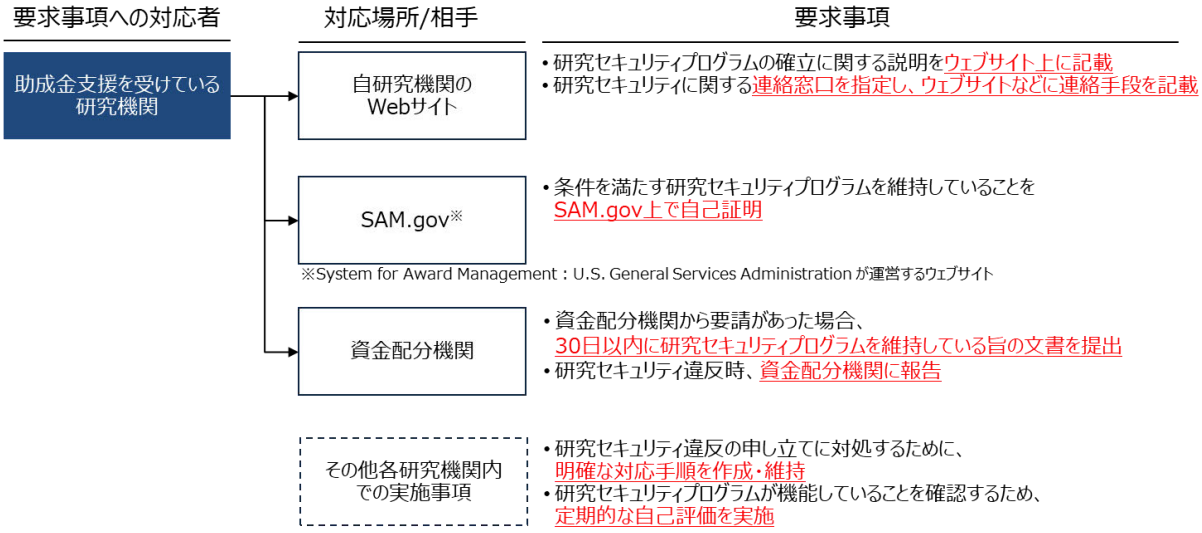
過去 2 会計年度連続で、連邦科学技術支援を年間 5,000 万ドル以上受けている研究機関

※ 大学のような研究組織で、その構成部分(例えば、学科、附属研究センター、学校)が、合計で年間少なくとも 5,000 万ドルの連邦科学技術支援を受ける場合に適用される。研究組織が相互に連結された研究組織のネットワーク(例：公立大学システム)の一部である場合、この要件は、個別に年間 5,000 万ドル以上の連邦科学技術支援を受けているネットワーク内の個々の組織にのみ適用される。

＜標準要件案に対して大学・研究機関側で必要な対応＞

上記の条件を満たす大学・研究機関は、自組織の Web サイトにて確立した研究セキュリティプログラムに関する説明及び当該テーマに関する連絡窓口に関する情報を掲載する必要がある。また、当該研究セキュリティプログラムでは、後述するサイバーセキュリティ要件を遵守する必要がある。

さらに、対象の大学・研究機関は、資金配分機関から要請があった場合、30 日以内に研究セキュリティプログラムを維持している旨の文書を提出する義務や、当該プログラムへの違反が発覚したい際に資金配分機関へと報告する義務が課せられる。



図表 2-7 標準要件案に対して大学・研究機関側で必要な対応

＜大学・研究機関に課せられるサイバーセキュリティ要件＞

- 情報システムの正規の利用者に対して、ソーシャル・エンジニアリングの脅威やサイバー侵害の認識と対応を含め、定期的なサイバーセキュリティに関する意識向上トレーニングを実施する。
- 情報システムへのアクセスを、正規の利用者、正規の利用者の代理として行動するプロセス又は機器(他の情報システムを含む)に限定する。
- 情報システムへのアクセスを、正規のユーザーが実行できるトランザクション及び機能に制限する。
- 外部情報システムへの接続を確認し、その利用を管理・制限する。

- 一般にアクセス可能な情報システムに掲載又は処理される非公開情報を管理する。
- 情報システムの利用者、利用者の代理となるプロセス又は機器を識別する。
- アクセスを許可する前提条件として、利用者、プロセス、又は機器の身元を認証(又は検証)する。
- 情報システムの外部境界及び重要な内部境界において、組織の通信(組織の情報システムによって送受信される情報)を監視、制御、及び保護する。
- 内部ネットワークから物理的又は論理的に分離された、一般にアクセス可能なシステムコンポーネント用のサブネットワークを導入する。
- ランサムウェアやその他のデータインテグリティ攻撃メカニズムから科学データを保護する。
- 情報及び情報システムの欠陥を適時に特定し、報告し、修正する。
- 組織の情報システム内の適切な場所で、悪意のあるコードからの保護を提供する。
- 新しいリリースが利用可能になった場合、悪意のあるコード保護メカニズムを更新する。
- 情報システムの定期的なスキャン及び、外部ソースからのファイルがダウンロード又は実行される際にリアルタイムスキャンを実行する。

ここで紹介したような研究セキュリティに関する上位ルールの策定は、主に大統領府 科学技術政策局(OSTP)が担っている。また、定められたルールに基づき、資金配分機関(NSF、NIH、DARPA 等)は、条件を満たす大学・研究機関において「研究セキュリティプログラム」が確立・運用されているかを確認する責任がある。

＜EU 政府による取組状況＞

取組の背景

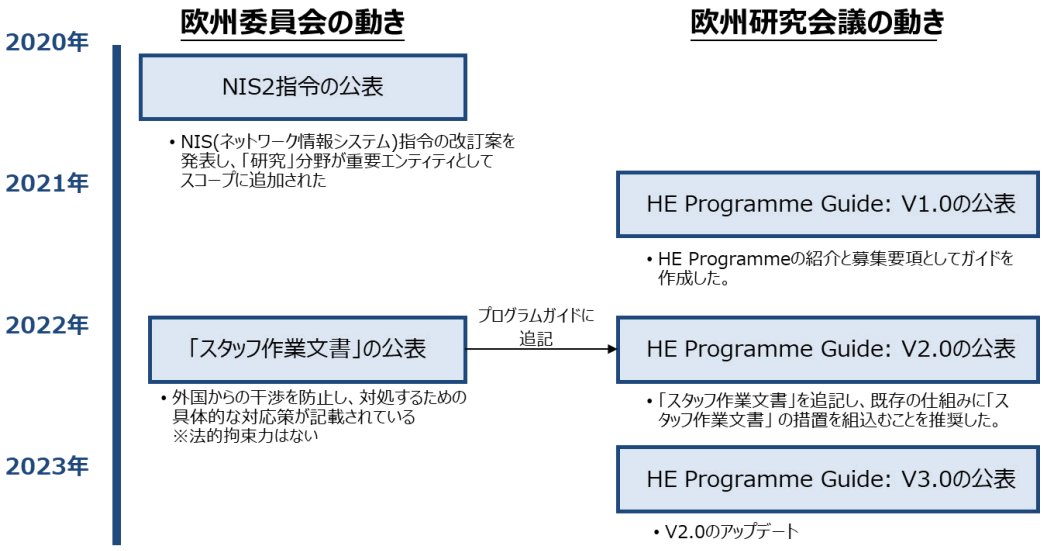
優れた研究の実施のためには国際協力が必須であるが、地政学的リスクが高まる今日の情勢の下では、EU が主導的地位に立ち、多国間主義、開放主義、相互主義を促進することが必要と考えられている。こういった中で、EU は外国の干渉から高等教育機関や研究実施機関を守るためのガイドラインの策定に取り組んでおり、EU 加盟国及び高等教育機関や研究実施機関、研究助成機関等が協力し、2022 年 1 月に「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書(以下、「スタッフ作業文書」という)」[10] を公表した。

近年の主な取組

上記の動向を受け、欧州委員会は欧州連合国や大学・研究機関、及び Horizon Europe Programme(以下、HE Programme という)への応募機関に対して、可能な限り「スタッフ作業文書」を既存の仕組みの中に組み込むことを推奨している。また、資金配分機関である欧州研究会議(ERC)は HE Programme に申請する機関に対して既存の仕組みに「スタッフ作業文書」の措置を組み込むことを推奨している。こうした研究セキュリティに関する方針の策定は主に欧州委員会内の研究・イノベーション総局が担っている。

また、「研究」分野を NIS2 指令における重要エンティティに指定する等、研究活動を通じて機微な

情報を取り扱い得る領域のサイバーセキュリティ強化にも取り組んでいる。



図表 2-8 EU における研究セキュリティ関連施策

＜スタッフ作業文書におけるサイバーセキュリティ関連規定＞

「スタッフ作業文書」において、「サイバーセキュリティ」は、「価値観」、「ガバナンス」、「パートナーシップ」とともに海外からの干渉への対応策の４カテゴリーの内の１つを構成している。

サイバーセキュリティについては、以下のように 3 つの要求事項が示され、それぞれについて具体的な対策が提示されている。

1. サイバーセキュリティリスクの認知を向上する。
   - 機密コンピューティング(confidential computing)を含む、利用可能で実装されているすべてのデータ保護技術に関するトレーニングを開発し、セミナーを開催する。
   - 研究者、学生、事務・支援スタッフに対し、サイバー衛生(cyber hygiene)に関する教育・訓練を行い、リスクを特定し、サイバー攻撃を回避・対処する方法を知ってもらう。
   - サイバー攻撃が疑われる場合に適用するわかりやすいエスカレーションプロセスを開発・伝達し、報告されたインシデントをトリアージするための単一の連絡窓口を周知する。
   - サイバーセキュリティリスクのトップ 10 リストの維持と伝達を行う。
   - サイバーセキュリティインシデントを説明するベストプラクティスを掲載したニュースレターを定期的に発行する。

2. 海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、防止する。
   - オープンソースインテリジェンス調査を定期的に設定・実行し、異常な行動にフラグを立てるアラート機能を作成する。
   - 研究者、事務・支援スタッフの審査手順を策定する。
   - サイバーセキュリティ認証を受けた機器を調達し、機密コンピューティングを含むデータセットの機密保護ソリューション(confidentiality protection solutions)の開発に投資する。
   - 必要なレベルに応じた物理的なアクセス制御を実施する。
   - オフィス/企業活動クラスターにおいて、OS とインストールされたアプリケーションの集中管理アプローチを開発し、ローカル管理権(LAR)を無効化及び削除する。
   - 重要なサービスやリポジトリにアクセスするための二要素認証を有効にし、既知の悪意あるウェブサイトや侵害するウェブサイトへのアクセスを禁止するブロックリストを維持・実施する。

3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う。
   - 教訓を共有し、共有ブラックリスト、評価システム、データベースを更新することにより、状況認識能力を向上させる。
   - 影響を受ける当事者と対応に必要な人物の双方が参加する明確なプロセスを含む、インシデント対応計画を策定する。セキュリティインシデント管理成熟度モデル(SIM3)等のインシデント処理モデルから慣行や要素を採用する。
   - フォレンジック準備機能を導入し、対応にかかる時間を短縮する。
   - 違反したスタッフの懲戒処分を行い、その際、デジタル調査の証拠も含める。
   - インシデントに、法執行機関、国家情報・セキュリティ機関、知的財産局、データ保護当局を関与させる。

なお、欧州研究会議(ERC)は、2022 年 4 月 15 日に、HE Programme のプログラムガイドにて、プログラム申請者に対し 、既存の仕組みに「スタッフ作業文書」 の措置を組み込むことを推奨している。

＜NIS2 における「研究」分野の取扱い＞

2022 年 12月に官報へ掲載され、2024 年 10月18日より施行予定の NIS2 指令において、適用対象となる「重要エンティティ」に「研究」が追加されていることを受け、同セクターに属する事業者や団体は以下に例を示す要件の遵守を求められる。

□ リスク管理(21 条)
- リスクマネジメント及び情報セキュリティ対策
- インシデントハンドリング
- ビジネス継続性
- サプライチェーンセキュリティ
- ネットワークやシステムのセキュリティ
- サイバーセキュリティリスクマネジメントの効率性評価
- サイバー衛生の実施及びサイバーセキュリティ教育
- 暗号技術の活用
- アクセスコントロール等の人的セキュリティ
- 多要素認証の活用

□ 報告義務(23 条)
- インシデント通報(24 時間以内に早期警告、72 時間以内にインシデント通知)

＜英国政府による取組状況＞

取組の背景

英国の大学は世界中のパートナーと密接に連携しており、英国の研究の半分以上は国際連携によるものとされる。国際共同研究は英国の科学的発展に対して重要な役割を果たしている。

そのような認識を踏まえ、2019 年、ビジネス・エネルギー・産業戦略省(BEIS)は、英国が長期的な国際研究・イノベーションのパートナーとして選ばれるための目標を策定した。

国際的な研究協力が盛んに展開する一方、アカデミアや産業界が行う研究活動を通じた技術流出により、国家安全保障に重大なリスクを与えることが英国政府の安全保障部門により認識されている。

近年の主な取組

上記の動向を受け、2019 年、英国政府の国家安全保障機関である国家インフラ保護センター

(Centre for the Protection of National Infrastructure: CPNI)と国家サイバーセキュリティセンター(National Cyber Security Centre: NCSC)が国内の大学、研究機関に対して、「Trusted Research」イニシアチブ [11] を展開し、関連ガイダンスとして「Trusted Research Guidance for Academics」[12] を発行した。



図表 2-9 英国における研究セキュリティ関連施策

その後、英国の大学協会である UUK(Universities UK)は、2020 年 10 月、外国による敵対的な干渉から守り、学問の自由を促進するために教育機関が取るべき配慮や対策について、詳細なガイドラインである「Managing risks in internationalization: Security related issues」[13] を公表した。こちらは、大学として研究インテグリティを理解し、既存のガイドライン「Trusted Research Guidance for Academia」[14] を補完するものとされている。

加えて、資金配分機関である UKRI(UK Research and Innovation)は、2021 年 8 月、国際共同研究のデューディリジェンスに関して、UKRI のファンディングを受ける機関への要求事項を定めた「Trusted Research and Innovation Principles」(UKRI 文書)を公表した。UKRI から資金提供を受けている組織は、同文書に示された原則を採用し、これらの原則に合致する管理及び対策を実施したことを証明できるようにする必要がある。これは、新規の助成金と既存の助成金に適用される。

＜UKRI 文書におけるサイバーセキュリティの位置づけ及び要求事項＞

同文書では、助成金申請機関が遵守すべき原則のカテゴリーとして、「パートナーの適正評価」、「情報・知識共有管理」、「商用への応用」という 3 つが提示されており、サイバーセキュリティは「情報・知識共有管理」における構成要素のひとつとして位置づけられている。

具体的には、「サイバー攻撃のリスクを軽減するには、スタッフと学生向けの広く公表されたガイダンスを含むセキュリティ意識向上及びトレーニングプログラムの一部として導入されたサイバーコントロールの開発を通じて達成される堅牢なサイバーセキュリティ文化が不可欠である」とされている。

＜UKRI 文書に示された原則の実装に必要なサイバーセキュリティ対策の例＞

UKRI 文書は原則の提示に留まり、具体的な対策の例示は必ずしも含まれておらず、当該情報を求める際は他の文書を参照する必要がある。

例えば、前述した「Trusted Research Guidance for Academia」では、研究者の安全確保に

資する対策として以下のようなものが示されている。

- サイバーセキュリティ
  - 強力な個別のパスワードを使用してメールを保護する(メールアカウントの保護)
  - 最新のソフトウェアとアプリのアップデートをインストールする
  - 2 段階認証をオンにする
  - パスワードマネージャの利用
  - データのバックアップ
  - ランダムな 3 つの単語を使用した解読困難なパスワードの作成

- USB ドライブ利用時の注意
  - USB ドライブのソースがどの程度信頼できるかの考慮
  - 設定又はシステム環境設定を通じた、「自動実行」無効の確認
  - USB ドライブ上のデータへのアクセス前におけるウイルス対策ソフトによる自動スキャンの実行
  - 情報を共有する必要がある場合は、代替手段 (クラウド ストレージ、電子メール、専用のコラボレーション プラットフォーム等) を検討する

- フィッシング攻撃に対する防御
  - フィッシング詐欺が電子メールで使用するテクニックを理解する
  - フィッシングメールをクリックした場合、インシデント報告先に迅速な報告を行う

● 企業を対象にした取組

営業秘密保護や不正アクセス禁止法制を擁しつつ、事業者間においては契約による保護を中心としているという全体的な枠組みは日本を含めて各国で共通していた。

他方、特に米国では営業秘密保護等について多数の訴訟が提起されており、法制度等の運用の面で日本との差異が明確に見られた。

＜米国政府による取組状況＞

米国では、価値あるデータは営業秘密によって保護することが基本であり、連邦法によりサポートされる。アメリカの現行法において各法令がパッチワークのような状態であり、重複性もあるが、ロバスト性の高い保護を実現している。

図表 2-10 米国における企業を対象としたデータ保護法制の概要 [9]

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、営業秘密関連法、その他現行法、契約等によってロバスト性の高い保護を実現している。一方で、契約関係にない第三者による不正取得等に対する懸念もある。	不正行為法リステイトメント	○		コンピュータ犯罪取締法(刑法第1030条)		○	懲罰的損害賠償	連邦著作権法(インターネット上のコンテンツを対象としたデジタルミレニアム著作権法)	-
	連邦経済スパイ法(EEA)		○						
	統一営業秘密法(UTSA)	○							
	連邦営業秘密保護法(DTSA)	○							

営業秘密は、長く州法におけるコモン・ローにより保護されてきたが、連邦刑事法において営業秘密の保護を強化するため、1996 年に連邦経済スパイ法が制定された。また、連邦法としては、刑事的救済のみが取り扱われ、民事的救済はもっぱら州法によっていたが、2016 年に連邦営業秘密保護法(DTSA)が制定されたことで連邦レベルでも民事的救済を求めることが可能となった。

さらに、コンピュータ犯罪取締法(刑法第 1030 条)では、コンピュータに対する不正なアクセス行為と、コンピュータ及びデータへ損害を与える行為を連邦レベルで規制している。

これらの法制のうち、特に営業秘密保護に係るものについて、これまで実施されてきた不正競争防止法の改正もあり、内容面では日米間で大きな差異は必ずしも見られないが、運用面では、提起される訴訟の件数、提起される違反行為の内容、原告による申し立ての認容率等、多数の差異がある。[16]

＜EU 政府による取組状況＞

EU においてもデータの保護は契約による保護を基本としており、第三者からの不正取得に対しては営業秘密保護指令やデータベース保護指令により、欧州各国の現行法で対応することとなっている。

図表 2-11 EU における企業を対象としたデータ保護法制の概要 [15]

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあるという考え	営業秘密保護指令	○		－	－	－	モデル契約開発中	データベース保護指令(著作権と独自の権利による保護)	単一デジタル市場戦略

中でも、営業秘密は非技術的なものを含めたイノベーションや競争力のために重要であるにもかかわらず、現状において欧州域内における不統一な保護状況が国を超えた研究開発や知識の流通を阻害しているとの認識が示されている。2016 年に採択された営業秘密保護指令は、営業秘密保護について、共通の定義を提供し、営業秘密侵害に該当する行為と、しない行為を明確にしている。

評価としては、新たなデジタル経済に対応する意図で策定されたものではなく、自動生成されるデータやリアルタイムのデータに適用するのには無理がある場合があるといった批判的なものと、欧州域内でハーモナイズが図られることは望ましい」といった好意的なものがある。

＜英国政府による取組状況＞

データの保護はコモン・ローでの保護が原則となっており、機密情報が侵害された場合は民事的な救済措置を請求することができる。また、機密情報が侵害された際、窃盗や著作権侵害に当たる場合は刑事的措置も可能となる。なお、不正アクセスがなされた場合はコンピュータ不正使用法により刑事罰が執行される。

図表 2-12 英国における企業を対象としたデータ保護法制の概要 [15]

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、営業秘密(機密情報の保持)、競争法、コンピュータ不正使用法 等対応可能な範囲内で保護。	コモン・ロー	○	○	コンピュータ不正使用法(1条、3条)		○		データベース保護指令に基づく国内法	

経済的に価値のあるデータの保護は、第一義的にコモン・ローにより「機密情報(confidential information)」が保護され、これが侵害された場合には差止等、民事的な救済措置を請求することができる。

機密情報の保護については、刑事的救済措置はないものの、窃盗や著作権侵害にあたるとされる場合には刑事的措置を施すことが可能である。これに加えて、1989 年競争法によって「商業的にセン

シティブな情報(commercially sensitive information)」が保護され、救済手段として制裁金の支払等に加え、刑事的訴えが可能な場合もある。

- 機微技術情報流出後の対応事例

＜不正アクセス等に係る被疑者の訴追＞

これまで、外国から産業分野の知的財産等を標的としたサイバー活動が多数報告されているところ、表 2-12 に示すように司法省(DoJ)による訴追まで至ったケースが多数報告されている。

特に、それらのうち 2014 年に行われた APT1 に属するハッカー5 名の訴追を調査した。この事案は、米司法省がハッキング容疑で海外の政府当局者を訴追した初のケースとされており、前述したコンピュータ犯罪取締法(刑法 1030 条)や連邦経済スパイ法(1031 条)等への違反を根拠として 5 名が起訴された。

図表 2-13 外国の攻撃グループに対する DoJ の訴追事例 [17]

脅威グループ	概要	司法省の対応
APT1 (別名：Comment Crew, Comment Panda)	2013年2月のレポートでMandiantが初めて明らかにした人民解放軍第61398部隊に関連するサイバー脅威グループであり、少なくとも141の組織から数百テラバイトのデータを盗んでいる。司法省がサイバースパイ行為で外国を刑事告発した初めてのケースとなった。	2014年、司法省がAPT1のハッカー5人を、米国企業に対するサイバースパイ行為で起訴
APT3 (別名：UPS Team, Gothic Panda, TG-0110, Boyusec, Buckeye)	MSSPとして知られる中国のサイバーセキュリティ企業に関連するサイバー脅威グループ。APT3は、航空宇宙、防衛、建設、エンジニアリング、ハイテク、電気通信、運輸分野の組織を標的としている。シマンテックによると、2015年以降、APT3は米国を拠点とする被害者を標的とすることから、香港の政治組織にシフトしている。	2017年、司法省は、金融、エンジニアリング、テクノロジー業界の企業を商業利益のためにハッキングしたとして、ハッカー3人を起訴
APT10 (別名：Menupass Team, Stone Panda, POTASSIUM, Red Apollo, Cicada, CVNX)	中国の国家安全保障上の目標を支援するため、外国政府だけでなく、建設・エンジニアリング、航空宇宙、電気通信企業を標的としてきた MSS に関連するサイバー脅威グループ。APT10は、エンジニアリング、工業製造、小売、エネルギー、製薬、通信、政府産業などの顧客の情報を入手するために、米国やその他の国の多数のMSPを侵害した世界的なサイバースパイキャンペーンである「Operation Cloud Hopper」を実行した。	2018年、司法省は、MSPと45社以上のテクノロジー企業を標的とした10年以上にわたる世界的なコンピュータ侵入キャンペーンに関連して、APT10のメンバー2人を起訴
APT26 (別名：Tur-bine Panda)	MSSの江蘇支部に関連するサイバー脅威グループで、航空宇宙、防衛、エネルギー分野を標的としたサイバースパイキャンペーンを行ってきた。2019年、CrowdStrikeは、同社がTurbine Pandaと呼ぶこのグループが、2010年から2015年にかけて、中国国産旅客機C919の部品を製造する複数の外国企業からIPを窃取していたことを明らかにした。	2018年、司法省は、民間旅客機に使用されるターボファンエンジンに関する情報を含む、機密データ、知的財産、及び機密情報の窃盗を共謀したとして、MSS江蘇支社の諜報部員2名を起訴
APT40 (a.k.a. Kryp-tonite Panda, GAD-OLINIUM, BRONZE MOHAWK, TEMP. Periscope, Levia-than)	MSS海南支社のフロント企業である海南湘敦科技発展有限公司に関連するサイバー脅威アクターで、中国の海軍近代化プログラムを促進する可能性が高い国家主導のスパイ活動を行っている。APT40は、米国、カナダ、欧州、中東、一帯一路構想諸国にわたり、政府、企業、大学を標的として、海洋研究を含む幅広い産業にわたるIPを提供している。APT40はHAFNIUMと関連しているか、重複している可能性がある。	2021年、司法省は、2011年から2018年にかけて実行された感染症研究を含む知財を標的とした世界的なコンピュータ侵入キャンペーンに関連して、APT40のメンバーを起訴

＜経済制裁の実施＞

機微技術情報の漏えいが顕在化、又は疑われる場合において、欧州理事会による制裁措置(例：関与者の資産凍結、直接・間接の資金提供の禁止)が発動されたケースが複数確認された。

図表 2-14 欧州理事会による経済制裁の発動例

制裁対象	概要	欧州理事会の対応
ロシア連邦軍参謀本部情報総局(GRU)	**ロシアの軍事スパイ組織** 2018年10月に起こったOPCW(化学兵器禁止機関:本部,オランダ ハーグ市)に対するハッキング未遂事件に関与している疑い	**制裁措置の発動** EU加盟国への入国およびトランジットの禁止および全ての資産の凍結が主な内容となる。またEU市民および企業が、制裁対象者に対し直接的・間接的に資金提供を行うことは禁止される (EU理事会が2019年5月に採択した規則2019／796に基づく措置)
Chosun Expo	**北朝鮮のハッキンググループ・APT38のフロント企業** APT38は世界中の銀行から数十億円もの現金を不正に引き出していた	
Huaying Haitai	**中国政府が支援するハッキンググループ・APT10のフロント企業** 世界各国のマネージドサービスプロバイダ(MSP)を標的として、軍事組織を含む多くの企業の知的財産や機密情報を盗み出すハッキング作戦「Operation Cloud Hopper」を展開していた	

・ まとめ

これまでの調査結果に関連する情勢を補足し、「機微技術保有組織のサイバーセキュリティの確保」に関する我が国の現状と課題について以下のように取りまとめた。

[我が国の現状]

機微な技術情報を取扱う研究機関は近年継続的な脅威に晒されており、実際にインシデントが多数報告されているところ、欧米ではそのような機関に対するサイバーセキュリティその他に関する統制を強めているが、我が国には複数の観点で取組が不足しており、今後の国際的な研究協力等に支障が出るおそれもある。

- 産業技術総合研究所(2018 年)や宇宙航空研究開発機構(2023 年)におけるインシデントのように、機微な技術情報を取扱う研究機関(大学や企業の研究部門等を含む)を標的にした脅威が既に多数顕在化しており、今後も激化が進むと予想されている、
- 我が国では、企業を中心に機微な技術情報を含む営業秘密の保護を推進しており、訴訟件数や違反の内容に差異は見られるが、規定は米国等に相当する内容となっている。
- 他方、昨今国際的に研究セキュリティに係るルールメイキングが推進されており、欧米主要国の一部では、我が国よりも具体的かつ厳格な対策が進められている状況にある。今後、我が国でそれに相当する取組が進められない場合、適切な情報保全の不備を理由として国際的な研究協力等に支障が出るおそれもある。
  - 米国、EU、英国の資金配分機関は、研究セキュリティに係る取組の一環として、募集要項で助成金申請者に対してサイバーセキュリティの確保を要求している。
  - EU の NIS2 指令では「研究」が重要インフラを構成する業種として指定されており、一定のサイバーセキュリティ対策の実施を要求するとともに、機微技術情報の漏えいを含むサイバーインシデントの当局への報告義務(米国でも類似の規定が見られる)が課される予定。

[上記を踏まえた我が国の課題]

1. 海外の動向も念頭に置いた、大学や研究機関におけるセキュリティマネジメント向上
2. 上記の我が国の仕組みと欧米の制度との相互運用性確保による国際的な研究活動の推進におけるリスクの低減

3 CPSF 等に基づく国際規格(TS 等を含む)の推進

3.1 本事業項目の目的

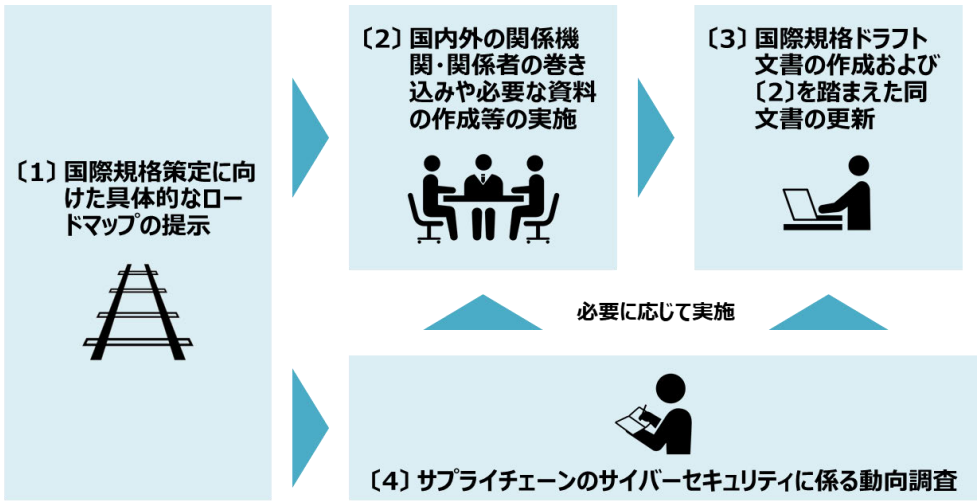
本事業では、日本企業の競争力強化に寄与する国際的なルールを形成していくことを目的とし、ルール形成を構成する一要素になりうる CPSF 等をベースにした国際標準化を推進した。

3.2 本事業項目の実施内容

本事業では、以下の(1)～(4)を実施内容として整理した上で、まず、国際規格策定に向けたロードマップを策定した。その後、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理に関する国際的なルール形成の状況を調査しつつ、サイバーセキュリティに関する国際的なフレームワークについて、CPSF の考え方をベースにしたものが採用されるよう必要な働きかけ・検討を行った。

＜本事業項目の実施内容＞

(1) CPSF 等に基づく国際規格策定に向けた具体的なロードマップの提示
(2) 国内外の関係機関・関係者の巻込みやそのために必要な資料の作成等
(3) 国際規格ドラフト文書の作成及び(2)の結果を踏まえた同文書の更新
(4) サプライチェーンのサイバーセキュリティ確保を目的とした国際規格、ガイドライン、フレームワーク、政策文書等の調査



図表 3-1 本事業項目の実施プロセス(概要)

3.3 本事業項目の実施結果

3.3.1 国際規格策定に向けたロードマップの策定

（１） 前提：主要な国際標準化機関とその標準策定プロセス

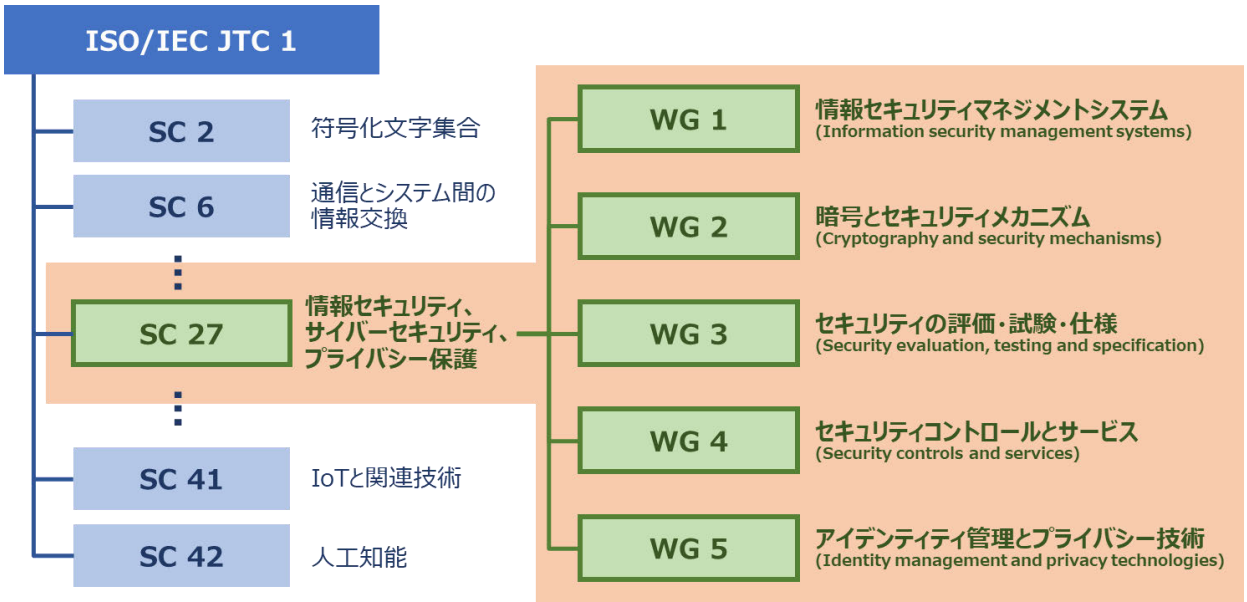
一般に国際規格とは、国際標準化機関で制定される規格を指す。代表的な国際標準化機関としては、ISO(国際標準化機構)が電気・電子・通信分野を除く幅広い分野の国際規格を制定しており、IEC(国際電気標準会議)は電気・電子分野の国際規格を、ITU(国際電気通信連合)は通信分野、放送・情報技術分野の国際規格を制定している [18]。また、情報技術の標準化について、ISO と IEC は共同で JTC 1(Joint Technical Committee 1)を設立、運用している。

具体的な規格策定プロセスは主体となる国際標準化機関や策定される文書の種別(例：IS/TS/TR)によって異なることから、ロードマップの策定にあたっては CPSF 等に基づく国際規格の策定を行う機関や委員会、策定する文書の種別を特定し、参照されている標準的な規格策定プロセスを確認する必要がある。

■ CPSF 等に基づく国際規格の策定を行う機関や委員会

CPSF 等に基づく国際規格策定の推進にあたっては、これまでの事業において、上記のうち JTC 1 内の SC 27(Sub-Committee 27)[19] にて規格化のプロジェクトを立ち上げている。図 1.3-1 に示すように、SC 27 には以下 5 つの作業部会(WG)が存在する。

- WG 1 (Information security management systems)
  情報セキュリティマネジメントシステム(ISMS)実装における要求事項や、セクター毎のガイドライン等を策定している。
- WG 2 (Cryptography and security mechanisms)
  暗号アルゴリズム、エンティティ認証等のセキュリティ基盤技術の標準化を進めている。
- WG 3 (Security evaluation, testing and specification)
  IT 製品や情報システムのセキュリティ評価に関連した規格の開発・保守を行っている。
- WG 4 (Security controls and services)
  ISMS を組織内で実装するための補助となる規格の開発・保守を行っている。
- WG 5 (Identity management and privacy technologies)
  ID 管理、生体認証、プライバシーに関する規格の開発・保守を行っている。



図表 3-2 JTC 1/SC 27 の構成

なお、CPSF 等に基づく規格策定に係る具体的なプロジェクトは、ISO/IEC 5689 とナンバリングされ、上記のうち WG 4 (セキュリティコントロールとサービス)で推進されている。SC 27/WG 4 では、IoT をはじめとする情報システムを構成する新興の製品やソリューションのセキュリティに関する規格開発を実施しており、CPS(Cyber-physical system)という IoT(Internet of Things)とも関連した概念を

取り扱うのにより適している。

■ 策定する文書の種別と規格策定プロセス

国際規格策定に向けたロードマップを策定する上では、JTC 1/SC 27/WG 4 を含む、ISO/IEC における国際標準策定プロジェクトが、一般的に、表 1.3-1 のようなプロセスで推進される点を考慮する必要がある[20]。

No.1.「予備段階」は、目標期日を確定できない業務項目について適用するもので、新業務項目提案(NP)の推敲や初回原案の作成に用いられる段階である。

No.2.「提案段階」は、新しい国際標準の開発を提案する段階である。すなわち、予備段階で検討した NP に対して投票を実施し、提案先の委員会(TC、SC 又は WG)の投票 P メンバーの過半数による賛成及び 5 か国以上の積極的な貢献の表明が得られた場合、新プロジェクトを登録できる。

No.3「作成段階」では、当該プロジェクトを担当する委員会の指名するエキスパートが作業原案(WD)を作成する。規格を技術仕様書(TS: Technical Specification)又は技術報告書(TR: Technical Report)として提案する場合、「作成段階」の最後に規定された割合の投票 P メンバーからの承認 を得て、No.6「承認段階」へと移行することができる。

規格を国際規格(International Standard)として提案する場合、No.3「作成段階」に続いて、技術的内容について合意に達するよう、各国代表団体からのコメントを検討する No.4「委員会段階」を実施する。

すべての技術的問題が解決し、委員会原案(CD)を照会原案(DIS)として回付することが承認され、中央事務局によって登録された時点で、「委員会段階」は終了する。

No.5「照会段階」では、中央事務局から 4 週間以内に、すべての国代表団体に原案が回付され、5 か月投票にかけられる。

続く No.6「承認段階」では、中央事務局は、2 か月投票のために最終国際規格案(FDIS)をすべての国代表団体に回付する。FDIS は、投票 P メンバーの 3 分の 2 以上が賛成で、反対が投票総数の 4 分の 1 以下の場合に承認され、No.7「発行段階」にて国際標準として発行される。

図表 3-3 ISO/IEC におけるプロジェクトの各段階と関連文書

プロジェクトの段階		関連文書	
		名称	略語
1	予備段階	予備業務項目(Preliminary work item)	PWI
2	提案段階	新業務項目提案(New work item proposal)	NP
3	作成段階	作業原案(Working draft(s))	WD
4	委員会段階	委員会原案(Committee draft(s))	CD
5	照会段階	照会原案(Enquiry draft)	DIS
6	承認段階	最終国際規格案(Final draft international standard)	FDIS
7	発行段階	国際規格(International standard)	ISO/IEC

（２） CPSF 等に基づく国際規格策定に向けたロードマップ

ISO/IEC における規格策定プロセスや実際に策定される文書の種別、JTC 1/SC 27/WG 4 における実際の議論の状況等を踏まえ、CPSF 等に基づく国際規格策定に向けたロードマップを以下のとおり作成した。なお、ここでは、策定する文書の種別が「技術仕様」(TS)である場合を想定し、2024 年 3 月時点での議論の状況も加味した上でロードマップの具体化を行った。

A. 2024 年 3 月時点までの経過

2023 年 2 月及び 4 月に実施された会合での決定事項に基づき、同年 7 月 13 日から 10 月 5 までの期間で NP 投票を実施した。投票結果は、賛成 27 か国(うち、積極貢献を表明した国が 8 カ

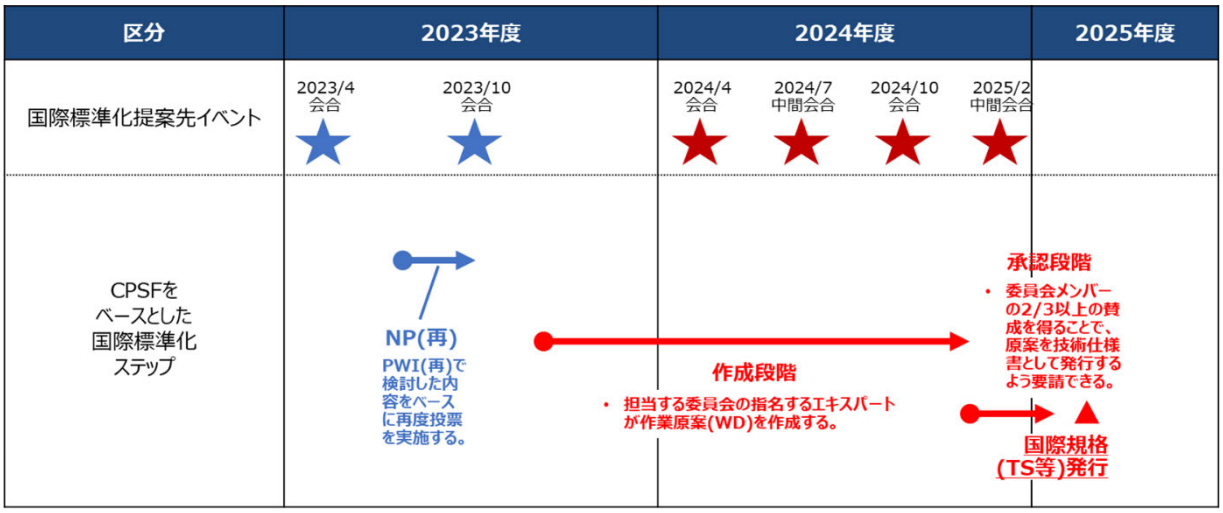
国)、反対 1 か国、棄権 27 か国であり、賛成多数かつ積極貢献を表明する国が 5 カ国以上であったため、本案件は可決となった。期間中に実施した働きかけの状況等については、「国内外の関係機関・関係者の巻込み」を参照されたい。

NP 投票可決後、エディタにて作業ドラフトの第 1 版を作成し、2023 年 12 月 26 日から翌年 1 月 31 日までの期間で SC 27/WG 4 エキスパート内の意見募集を行い、1 カ国(ドイツ)からのコメントを得た。こちらのコメントへの対応及び今後の検討の進め方について、2024 年 4 月に予定されている WG 会合にて議論される。

B. 今後の見通し

本案件は、現時点で技術仕様書(TS)として策定することを前提に検討が進められている。そのような場合、現在実施している「作成段階」の検討を行い、参加者の合意の下、規定された割合の投票 P メンバーからの承認を得て、「承認段階」及び「発行段階」へと移行することができる。

今後、本案件は「作業段階」にて SC 27/WG 4 レベルで WD の詳細について検討を進める。具体的には、エディタにてエキスパートからの意見を反映した原案を作成し、エキスパート間で 1～2 か月程度の意見募集を行った上で、提出された意見に基づき会合にて修正内容を合意し、次回の原案に反映していくというプロセスを繰り返し実施する。本案件では、今後 3 回程度そのようなサイクルを推進し、内容について合意を得た後、2024 年度中に DTS(Draft Technical Specification)投票へ進め、承認段階へ移行することを想定する。

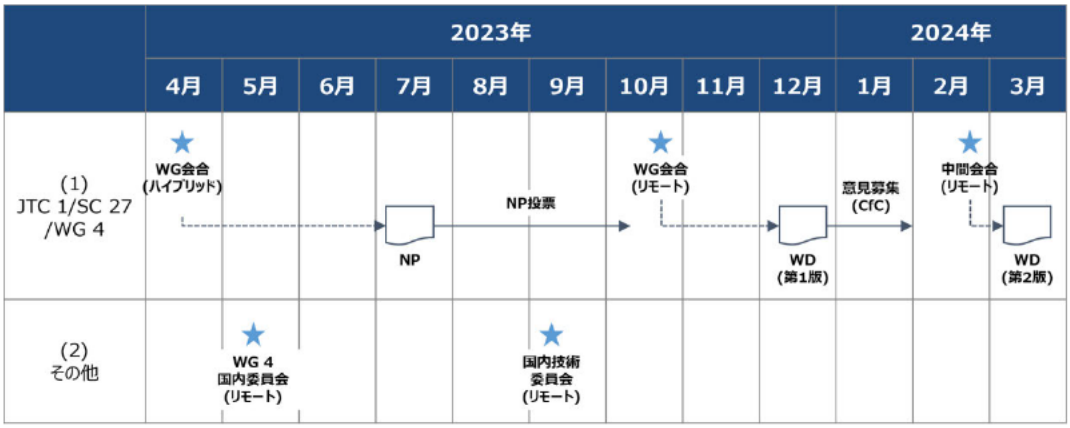


図表 3-4 CPSF 等に基づく国際規格策定に向けたロードマップ

3.3.2 国内外の関係機関・関係者の巻込み

前節で検討したロードマップ等を踏まえ、CPSF 等に基づく国際規格の策定を目指し、JTC 1/SC 27/WG 4、その他の関係機関・関係者に対して実施した巻込みについて詳述する。

本節以下では、今年度事業にて実施した国内外の関係機関・関係者との議論の状況について、図 1.3-3 にて示すように、(1) JTC 1/SC 27/WG 4、(2) その他(主に国内での働きかけ等)という 2 つの観点から整理した。



図表.3-5 国内外の関係機関・関係者との意見交換の状況

（1） JTC 1/SC 27/WG 4 における国際的な議論の状況

前述したように、JTC 1/SC 27/WG 4 では、2023 年 2 月の中間会合及び 4 月の WG 会合(米国 Redmond での現地開催とオンライン開催の併用によるハイブリッド形式)にて ISO/IEC PWI 5689 について NP 投票に進める点を合意し、7 月 13 日から 10 月 5 までの期間で NP 投票を実施した。今回の投票においては、前回 NP 投票時のように、賛成票は十分確保できているにもかかわらず積極貢献を表明する国の数が不足するという事態を防ぐため、特に前回投票時に賛成だったが積極貢献を表明しなかった国及び棄権票を投じた国のエキスパートに対して、個別の働きかけを行った。

図表 3-6 NP 投票実施中の主な働きかけの状況

対象国	前回結果	示された反応	今回結果
 ドイツ	賛成	サポートをするとのことだが、国内委員会で反対が出た場合、押し通せるかは不明。	賛成
 フランス	棄権	Antonio を介して、国内の SC27/WG4 担当と連携し、支援の回答を得た。	賛成＋積極貢献
 ルクセンブルク	賛成	4 月の Redmond 会合でも接触。支援について了承。	賛成＋積極貢献
 韓国	賛成	国際会合にて接触し、支援することを約束。WG5 の担当からもプッシュいただくよう依頼。	賛成＋積極貢献
 アメリカ	棄権	9 月の米国内の会議で調整を行う予定。支援について了承。	賛成＋積極貢献
 シンガポール	棄権	支援可能な状況であるとの返信あり。	賛成＋積極貢献

主な働きかけの内容や反応は表 3-6 に示すとおりだが、NP 投票では上記に日本とベルギーを加えた計 7 カ国の積極貢献の表明を得た結果、本案件は可決となった。また、投票時、日本に加え、オース

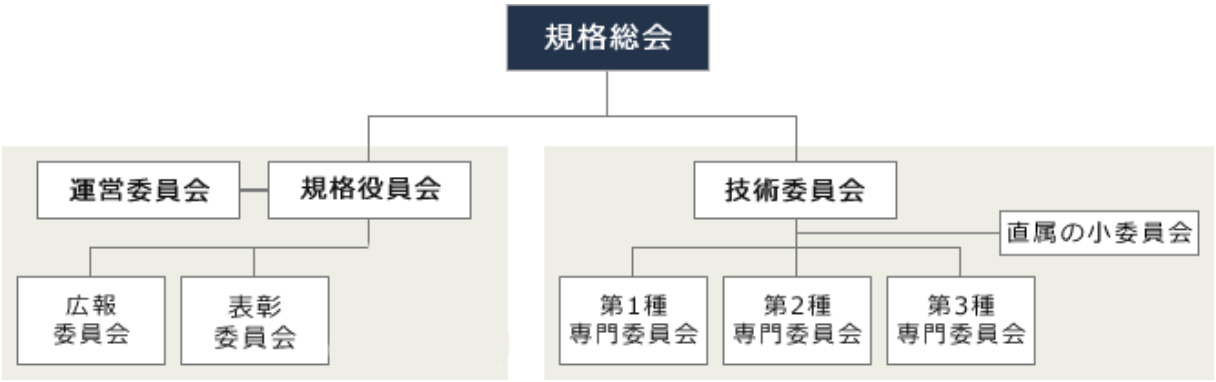
トラリア、カナダ、アメリカ、インドの計 5 カ国からコメントが提出された。
投票結果判明後の 10 月下旬に開催された WG 会合では、NP 可決後の本案件の進め方について議論があり、以下の合意がなされた。

- エディタは、NP 投票で各国から受け取ったコメントを註に記載し、本会合後 2 週間以内に WD 第 1 版を作成する。
- WD 発行後、SC 27/WG 4 はエキスパートにコメントを求める。
- ISO/IEC JTC 1/SC 41 (Internet of Things and Digital Twin) に WD に関するコメントを求める。
- WD に対するコメントに基づき、エディタは、次回の WG 4 会合(2024 年 4 月を目途に開催)より以前に中間会合を開催する。

上記で示されたエキスパートへのコメント募集は、2023 年 12 月 26 日から翌年 1 月 31 日まで実施され、前述のとおり、ドイツからコメントを得た。こちらのコメントへの対応及び今後の検討の進め方について、2024 年 4 月に予定されている WG 会合にて議論される。

（2） その他(主に国内での働きかけ等)

(1)で述べたものに加え、国内でも必要な働きかけを行った。ここでは特に、NP 投票等における日本国内の審議について述べる。
今回の NP 投票では提案国である日本も賛成に加えて積極貢献を表明したが、投票にあたっては SC 27/WG 4 国内小委員会の親会にあたる情報規格調査会 [21] 内の SC 27 専門委員会(第 1 種専門委員会の一部を構成)及び技術委員会の承認を得る必要がある。



図表 3-7 情報規格調査会の組織 [22]

本案件においては、SC 27 専門委員会内でメール審議を行った後に 2023 年 9 月 4 日に開催された技術委員会の場で必要な説明を行い、委員からの承認を得た。

3.3.3 CPSF 等に基づく国際規格(案)の作成

これまでに述べたように、ISO/IEC WD 5689 は、NWIP 投票にて可決され、WD の段階にある。本委託事業では、現在審議されている WD 第 1 版を含む CPSF 等に基づく国際規格(案)の作成を推進した。

3.3.4 サプライチェーンのサイバーセキュリティに係る動向調査

本事業項目では、これまでに述べた国際規格を直接的に推進する活動に加え、それを補助する目

的で、米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的としたリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関係する国際規格、ガイドライン、フレームワーク、政策文書等の調査を行った。今回の調査にて対象とした文献の一覧を以下に示す。

図表 3-8 調査対象文献一覧

No.			対象文献	発行/審議団体
1	ISMS 関連標準の動向	1-1	ISO/IEC 27000 シリーズ	ISO/IEC JTC 1
		1-2	ISO/IEC CD 27017	ISO/IEC JTC 1
2	IoT セキュリティ関連標準の動向	2-1	ISO/IEC 27402:2023	ISO/IEC JTC 1
		2-2	ISO/IEC CD 27404	ISO/IEC JTC 1

4 ガイドライン等の普及・啓発の推進

4.1 本事業項目の目的

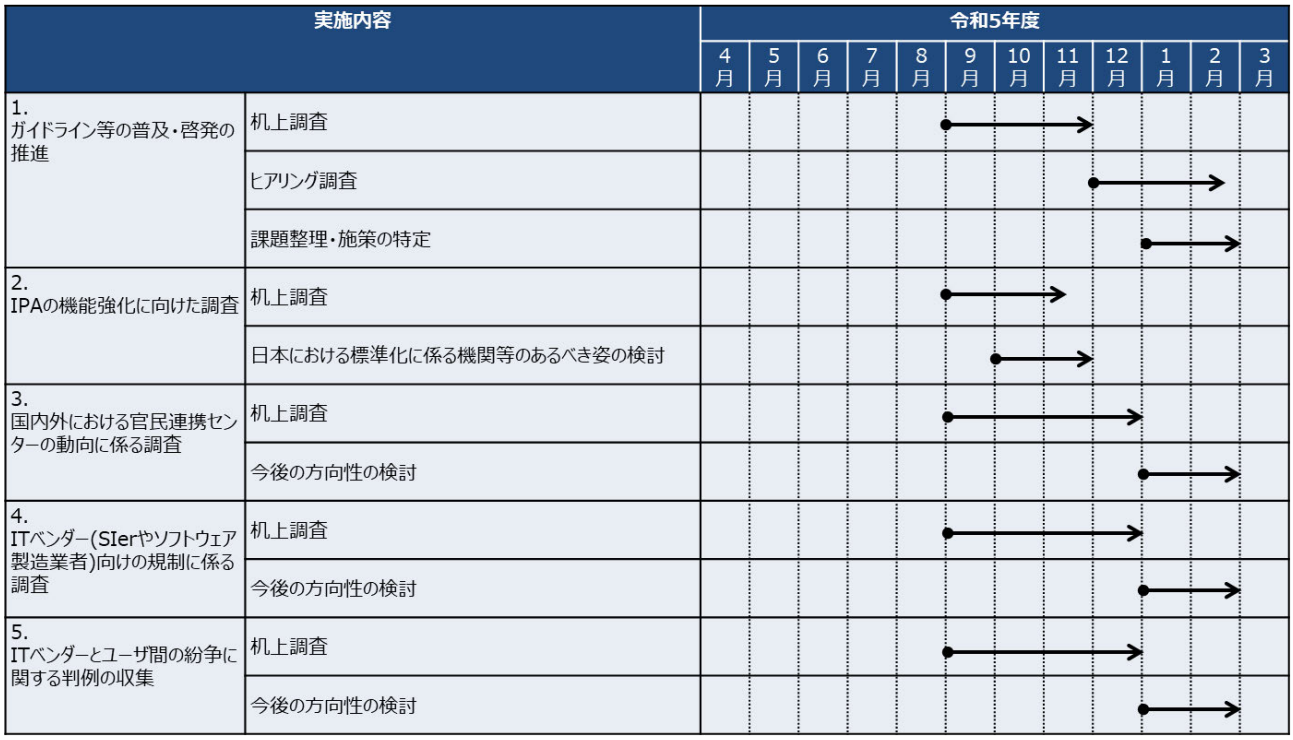
本事業項目では、CPSF に基づくガイドラインやその他のサイバーセキュリティに係る基準・標準等の普及・啓発の推進について、様々な産業界での普及・拡大を進めることを目的とした。

4.2 本事業の実施内容

貴省担当者との相談の上、上記目的を達成するための具体的な事業内容を、以下の 1～5 とした。

＜本事業項目の実施内容＞

1. ガイドライン等の普及・啓発の推進
2. IPA の機能強化に向けた調査
3. 国内外における官民連携センターの動向に係る調査
4. IT ベンダー(SIer やソフトウェア製造業者)向けの規制に係る調査
5. IT ベンダーとユーザー間の紛争に関する判例の収集



図表 4-1 本事業項目の実施スケジュール

4.3 本事業項目の実施結果

4.3.1 ガイドライン等の普及・啓発の推進

本項では、CPSF に基づくガイドライン及びユースケースを含む政府機関が公開するガイドライン等の認知・利用拡大を推進していく上での現状と課題等を整理及び、それに係る貴省、IPA 及び民間団体等との役割分担の明確化を図ることを目的として、以下の流れで調査を行った。

① 机上調査
② ヒアリング調査
③ 課題整理・施策の特定

具体的な調査項目及び項目ごとのリサーチクエスチョンは以下のとおり。

図表 4-2 調査項目及びリサーチクエスチョン

調査項目	リサーチクエスチョン
1. 調査の目的等	
1.1. 調査の目的	-
1.2. 推進スケジュール	-
2. 中小企業を対象としたガイドライン等の普及・啓発に関する取組の現状	
2.1. 中小企業における情報セキュリティ対策状況の実態	● 既存ガイドライン(CPSF 関連の他、経営ガイドライン、中小企業ガイドライン等)はどの程度認知又は活用されているか。 ● 認知又は利用している場合、認知経路や利用の理由(きっかけ)は何か。
2.2. 政府や関連団体による普及・啓発に関する取組の現状	● CPSF 関連又はそれ以外のガイドライン等の普及・啓発に向けて活動する主体にはどのようなものがあり、具体的に誰に何を行っているか。 ● それぞれの取組はどの程度効果を上げているか。 ● 成功している取組の優れた点とその要因は何か。 ● 目的の実現に向けて、政府・行政機関又は民間団体はどのような問題に直面しているか。
3. 中小企業を対象としたガイドライン等の普及・啓発に関する課題・施策	
3.1. ガイドライン等の普及・啓発に関する課題	● 2 章で特定された現状に対して、ヒト/モノ/カネ/情報のそれぞれの観点から達成すべき課題は何か。 ※分析観点については仮のもの ● 上記のうち、全体で共通する課題及び、CPSF に基づくガイドラインに特有の課題にはどのようなものがあるか。 ● 特定された課題にアプローチする際に想定されるリスクや懸念点にはどのようなものがあるか。
3.2. 普及・啓発に関連する国内外の取組	● 海外又は国内(サイバーセキュリティ以外の領域)では日本で想定されるものと同様の課題に対して、どのような施策を講じているか。 ● 当該施策が効果を上げていると考えられる場合、その要因は何か。
3.3. CPSF に基づくガイドラインの普及・啓発に関する施策の方向性	● CPSF に基づくガイドライン等の普及において効果及び実行可能性の観点から望ましい施策は何か。

① 机上調査

図表 4-2 で示す調査項目のうち、「2-1.中小企業における情報セキュリティ対策状況の実態」及び「2-2.政府や関連団体による普及・啓発に関する取組の現状」はヒアリング調査に先駆けて机上にて調査を行った。

◆中小企業における情報セキュリティ対策状況の実態

既往アンケート調査[26,28]の再分析を中心に、中小企業の基本動向及び、ガイドライン等の普及に係

る情報収集の状況、ガイドライン等の認知・利活用の状況等を含む 9 項目について結果を整理した。以下では結果のサマリを示す。

i. 中小企業の動向に関する基本データ
- 建設業や製造業、情報通信業等の対象業種又は地域という観点のいずれでも小規模企業が最も多く、次いで中小企業(小規模企業を除く)、大企業の数が多い。

ii. IT 投資・サイバーセキュリティ関連投資額
- 直近 3 期の IT 投資額について、67.8%の中小企業が 100 万円未満、17.5%が 500 万円未満と回答。
- 直近 3 期の情報セキュリティ投資額について、82.3%が 100 万円未満、8.2%が 500 万円未満であり、6.0%がわからないと回答。

iii. サイバーセキュリティに係る脅威状況・認識
- 中小企業の約 36%が一年以内にサイバー攻撃の被害を受けたと回答している。
- セキュリティに係る組織体制は、「組織的には行っていない」の割合が最も高く 49.2%である。
- 回答企業の約 4 割が 5 名以下の事業者であることを考えれば妥当な結果と解釈されている。

iv. 具体的なサイバーセキュリティ対策状況
- 導入済セキュリティ製品・サービスは、「ウイルス対策ソフト・サービスの導入」の割合が最も高く 77.2%、次いで「ファイアウォール(35.6%)」、「VPN(17.1%)」となっている。
- セキュリティ業務の外部委託は、「委託していない」の割合が最も高く 58.7%となっている。次いで、「わからない(11.3%)」、「ウイルス監視サービス(10.8%)」となっている。
- ガイドライン準拠の支援を行うコンサルティングサービスの利用は、2.8%と極めて少数。

v. 情報収集の実施状況
- 中小企業では「機会があれば情報を収集している」が最も多く選択されており、「常時情報を収集している」割合は 3 割以下である。
- 4 割強が業界団体から、2/3 程度が IT 業者から情報を取得している一方、社外セミナーへの参加やメディア記事の参照は、上記と比較すると限られている。
- ヒアリングでは、IT 事業者から自社に必要で具体的なアドバイスが提供されること、業界団体から提供される情報の内容と当社の実態が合っていない等の意見があった。

vi. ガイドライン等の認知状況/利用状況
- 中小企業の中で比較的規模の大きい企業にあっても、認知度は経営ガイドラインで 29.9%、ISMS で 35.1%、その他はほぼ 10%以下にとどまる。
- 中小企業の中で比較的規模の大きい企業にあっても、利用率は経営ガイドラインで 13.0%、ISMS で 10.4%、その他は 3%以下にとどまる。
- IPA が実施する活動の認知度について、「知っているものはない」の割合が最も高く 69.8%となっている。次いで、「中小企業の情報セキュリティ対策ガイドライン(14.1%)」、「SECURITY ACTION(5.8%)」となっている。

vii. ガイドライン等の認知/利用のきっかけ・動機
- インターネット、IT 関連事業者、業界団体が中小企業による CPSF 認知のきっかけとされる。一方で、メディア記事や社外セミナー等による普及効果は薄い。
- 経営ガイドラインにおいても基本的な状況は CPSF と同様だが、ISMS と NIST CSF では社外の IT 関連事業者経由で認知を得たという割合が相対的に高い。
- 全体を通じて、自社内又は業界団体、IT 関連事業者の呼びかけが主な活用のきっかけとされ、内外のセキュリティ事故はきっかけとしてあまり機能していない。大企業においては、経営ガ

イドラインや ISMS、NIST CSF の普及にあたって、取引先や IT 関連事業者が一定の役割を果たしている。

viii. ガイドライン等を活用していない理由
- 大企業と比較して人材不足や手順や参照先の不明確さを多く選択している。
- 従業員 50 名未満の中小企業の 23.9%、50～100 名の 20.0%が利用の必要性を感じていない。

ix. ガイドライン等の活用において直面している課題
- 課題はガイドラインにより様々だが、推進人材の不足、予算の制約や不明確な進め方という課題は共通する。ヒアリングでは、金銭支援策に関する要望が多かった。
- 約半数以上が、解説文書や詳細なガイドラインの公開を要望している。
- 50 名未満の 30.4%、50~100 名の 23.3%、100~300 名の 16.9%が要望は特にないと回答している。

◆政府や関連団体による普及・啓発に関する取組の現状

政府や関連団体によるガイドライン等の普及・啓発に関する取組の現状を整理するため、以下の条件を設定し、調査対象を整理した。

1. 産業サイバーセキュリティ研究会及び TF、SWG にて作成したガイドラインに限定せず、政府機関(例:経産省、IPA 等)や民間団体が策定したセキュリティに係るガイドラインの普及・啓発に関する取組を対象とする。
2. ただし、上記ガイドラインうち、民間企業単体が自発的に実施するセキュリティの普及・啓発に関する取組は対象外とする。

上記条件に基づき特定した具体的な調査対象は以下のとおりである。

図表 4-3 調査対象となる対象ガイドライン等

No	大分類	小分類	普及啓発の実施主体	対象ガイドライン/制度
1	全国規模	政府主導	貴省・IPA	中小企業の情報セキュリティ対策ガイドライン
2			貴省・IPA	SECURITY ACTION(中小企業の情報セキュリティ対策ガイドライン)
3			貴省・IPA	サイバーセキュリティ経営ガイドライン
4			貴省・IPA	制御システムのリスク分析ガイド
5			貴省・IPA	IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド
6		民間主導	制御システムセキュリティセンター(CSSC) 等	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
7			Edgecross コンソーシアム等	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
8			JEITA 等	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン
10	地域規模		ITC ちば経営応援隊/IT コーディネータ協会	中小企業の情報セキュリティ対策ガイドライン等

No	大分類	小分類	普及啓発の実施主体	対象ガイドライン/制度
11			関西サイバーセキュリティネットワーク	同上
12			名古屋商工会議所	同上

調査結果のサマリは以下のとおり。

- 全国規模の政府主導による取組

貴省・IPA が主導する全国規模の取組について、主体/取組の概要、取組の優れた点とその要因、取組の成果の観点から調査した。貴省・IPA が各関連団体と連携し取組を実施することで、一定の効果がみられている。一方で、中小企業の全体数からみるとまだまだガイドライン普及の余地があると言える。

図表 4-4 調査結果

対象ガイドライン/制度	調査項目	No.	調査結果
中小企業の情報セキュリティガイドライン	主体/取組の概要	1-1	● 貴省・IPA が各地の経済産業局等と協力してセミナー・演習にて周知。 ● 貴省・IPA が企業側の自発的な活用を支援するための各種補助コンテンツ(概要資料、動画)を作成。 ● 貴省がガイドラインに対応した認定制度(SECURITY ACTION)を創設することで利用を促進。
	取組の優れた点とその要因	1-2	● 地域の経済産業局と協力することで、中小企業がより自分ごととして捉えやすくしている。 ● セミナー・演習の参加費用を抑えることで、中小企業がより参加しやすくしている。
	取組の成果(例:ガイドラインの普及割合)	1-3	● 中小企業を広く対象とした調査にて、認知率は 14.1%、利用率は 6.1%(どちらも 2021 年調査時点)と 2 割をどちらも下回っており、十分普及しているとは言えない。
SECURITY ACTION	主体/取組の概要	2-1	● 貴省・IPA が業界団体(例:JNSA)と連携してセミナーを実施。ただし、補助金申請の要件に含まれている場合があり、地方自治体も普及の一翼を担う。 ● 貴省が、セキュリティガイドラインを認証制度の要件に組み込み、その認証の取得を補助金交付の要件とすることで、ガイドラインの利用を促進。
	取組の優れた点とその要因	2-2	● 費用的な負担がある場合に認証取得が進みにくいより小規模な企業においても、補助金の申請要件とすることで、SECURITY ACTION の取得を促進させることができる。
	取組の成果(例:ガイドラインの普及割合)	2-3	● 中小企業における制度の認知率は 5.8%、利用率は 1 つ星を宣言した企業で 2.6%、2 つ星を宣言した企業で 0.7%(全て 2021 年調査時点)にとどまっており、十分に普及しているとは言えない。

対象ガイドライン/制度	調査項目	No.	調査結果
サイバーセキュリティ経営ガイドライン	主体/取組の概要	3-1	● 貴省・IPA がセキュリティプレゼンター制度等を通じて民間企業や人材を活用しつつ、普及啓発活動を実施。ただし、セキュリティプレゼンター制度は本ガイドラインの普及のみを対象にしていない点に留意。 ● 貴省・IPAが企業側の自発的な利用を支援するため、プラクティス集の策定や可視化ツールの無償公開を実施。
	取組の優れた点とその要因	3-2	● 具体的なセキュリティ対策を実装の際に企業がプラクティス集を活用可能。 ● また、IT 担当者は可視化ツールを活用することで、費用をかけず経営者層に対して問題提起が可能
	取組の成果(例:ガイドラインの普及割合)	3-3	● 大企業を含む製造業者を対象にした調査にて、認知率は 29.9%、利用率は13.0%(どちらも2022年調査時点)であり、中小企業を中心に過半数以上の事業者から認知を得られていない。
制御システムのリスク分析ガイド	主体/取組の概要	4-1	● 貴省・IPA が、セミナーやガイドラインを活用したリスク分析ワークショップにてガイドラインを周知。 ● 貴省・IPA が、ガイドラインの補足資料、活用の手引き等の補助資料を作成。 ● IPA が、重要インフラ事業者を対象にしてガイドラインを活用した支援を実施。(及びそのフィードバックの反映)
	取組の優れた点とその要因	4-2	● セミナーにおいて、3 種類(入門編/応用編/管理者向け)の動画を提供することによって、知識や立場が異なる各受講者に対応可能。 ● IPA が無料でリスクアセスメントの支援を行うことによって、一定の質を担保しつつ直接ガイドラインを普及させることが可能。
	取組の成果(例:ガイドラインの普及割合)	4-3	● 大企業を含む貴省が所管している業界団体(製造業)の会員企業を対象とした調査(調査においてはリスク分析の参考資料として本ガイドラインを提示)において、そもそもリスク分析を実施していない企業は47.4%にのぼるため、 少なくとも約半数の企業が本ガイドラインを利用していない
IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド	主体/取組の概要	5-1	● 貴省・IPA が、関連団体(日本商工会議所、中小企業基盤整備機構、全国中小企業団体中央会、SC3)と連携を行い、普及啓発活動を実施。 (HP・メールマガジン等を通じた案内、セミナー等における案内、各都道府県を通じた地域の中小企業への周知) ● 貴省・IPA が、ガイドラインの概要版、経営者向け概要版を作成。
	取組の優れた点とその要因	5-2	● 各業界団体の HP でのガイドラインを紹介することで、貴省 HP のみでの紹介に比べて、幅広い企業が認知する可能性が高まる。 ● 鳥取県サイバーセキュリティ対策ネットワークや高松商工会議所等のより地域企業に近い団体における HP での紹介が可能となり、より自分ごととして中小企業が捉えやすくなる。

対象ガイドライン/制度	調査項目	No.	調査結果
	取組の成果(例:ガイドラインの普及割合)	5-3	- (公開(2023/6/6)から調査時点で 5 ヶ月程度経過。普及期間が少ないため)

- 全国規模の民間主導による取組

産業サイバーセキュリティ研究会における各サブワーキンググループにて作成されたガイドライン(ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン/工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン/スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン)を対象として調査を行った。中小企業と関係の深い業界団体(例:商工会議所)に対して各種ガイドラインの普及啓発に係る働きかけを行っている事例がみられた。しかし、業界団体を通じた取組において、同じ業界であっても、貴省が策定したガイドラインの普及啓発に積極的な団体とそうではない団体がみられ、横の連携において課題がみられた。

図表 4-5 調査結果

項目	調査結果
普及啓発の支援を依頼する対象	● 貴省が策定した分野別のガイドラインは様々なステークホルダーが想定読者となるため、関連する業界団体も多岐にわたるとともに、他省庁が管轄する業界団体も含まれ得る。[ビルガイドライン、スマートホームガイドライン] ● 中小企業への普及啓発を目的として、中小企業と関係の深い業界団体(例:商工会議所)に対して働きかけを行っている事例がみられた。[IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド]
普及啓発の支援を行う団体(例:業界団体)の取組	● 業界団体を通じた取組において、同じ業界であっても、貴省が策定したガイドラインの普及啓発に積極的な団体とそうではない団体がみられた。 [ビルガイドライン、スマートホームガイドライン] ● ガイドライン策定の段階で深く関わっている業界団体(例:JEITA、CSSC)においては、積極的な取組(例:ガイドラインを踏まえた個別ガイドラインの策定)がみられた。具体的には貴省が策定したガイドラインに関連するガイドラインを各業界団体が作成している。 [ビルガイドライン、スマートホームガイドライン] ● 業界団体が独自にガイドラインを策定する場合があり、その際には普及啓発に係る業界団体独自のチャネルを活用している。[日本建設業連合会のセキュリティガイドライン、CCDS の製品分野別セキュリティガイドライン] ● 業界内で強い立場(例:建設業界における元請企業)にある企業が業界独自のガイドラインの普及啓発に取り組んでいる事例がみられた。[日本建設業連合会のセキュリティガイドライン]

- 地域規模の取組

中小企業の情報セキュリティ対策ガイドライン等の積極的な普及啓発を行う団体を対象としてその取組内容について調査を行った。セミナーを中心として普及啓発活動をしており、参加している中小企業に対しては一定の効果があったとされている。一方で、中小企業の全体数からみるとまだまだガイドライン

普及の余地があると言える。

図表 4-6 調査結果

対象団体	調査項目	No.	調査結果
ITC ちば経営応援隊	主体/取組の概要	1-1	<ガイドラインの普及に係る取組> ● 地域コミュニティ連絡会を設置した 3 地域と連携してセミナーを開催。 <上記以外の取組> ● 貴省関東経済産業局の委託事業において社内の現状分析、情報セキュリティ規程案の策定等の直接的な支援を実施。 ● また、他団体(例:全国中小企業団体中央会)の各種研修において、講師を務め事例等を紹介。
	取組の優れた点とその要因	1-2	<ガイドラインの普及に係る取組> ● 他地域の連絡会参加者にセミナー開催を告知してもらうことで、多くの企業にガイドライン等を周知することが可能。 ● IT コーディネータ協会と連携することによって、より小規模の企業(10 名～50 名以下)に対して支援や情報の提供を行うことができている。
	取組の成果	1-3	<ガイドラインの普及に係る取組> ● 令和 3 年度のセミナーの申込者数は 2 回合計で 300 件以下となっている。中小企業の数は茨城県で約 8 万、千葉県で約 12 万、長野県で約 7 万であることから、効果は限定的となっている。
関西サイバーセキュリティネットワーク	主体/取組の概要	2-1	<ガイドラインの普及に係る取組> ● 中小企業の情報セキュリティ対策ガイドラインに基づいたリスク分析ワークショップを開催。 <上記以外の取組> ● 地域コミュニティ形成のため相談窓口の設置やサイバーセキュリティ専門家の派遣を実施。 ● また、地域コミュニティに向けてサイバー攻撃の現状やセキュリティ対策をセミナーにて紹介。
	取組の優れた点とその要因	2-2	<ガイドラインの普及に係る取組> ● サイバーインシデント演習やリスク分析ワークショップを開催することによって、地場の企業が自分ごととして捉えやすくなる。
	取組の成果	2-3	<ガイドラインの普及に係る取組> ● 関西圏の地域セキュリティコミュニティの存在を認知している団体は 6.3%であり、そもそも、地域セキュリティコミュニティの存在が知られていない。なお、ワークショップの定員は 40 名。
Pit-Nagoya(名古屋商工会議所の取組を含む)	主体/取組の概要	3-1	<ガイドラインの普及に係る取組> ● 中小企業の情報セキュリティ対策ガイドラインを活用した対策をセミナーにて紹介。 ● 自工会/部工会が策定したガイドラインをセミナーにて紹介。 <上記以外の取組> ● IT 化にむけた相談窓口の設立や中小企業と IT 企業のマッチング支援を実施。 ● お助け隊サービスで得た知見を踏まえて、セキュリティサービスを提供。

対象団体	調査項目	No.	調査結果
	取組の優れた点とその要因	3-2	<ガイドラインの普及に係る取組> ● ガイドラインに則った対策内容についてセミナーを行うことによって、中小企業はガイドラインの認知に加え具体的なセキュリティ対策を進めやすくなる。 ● 自工会の担当者と連携することで自工会のみの周知と比較して幅広い企業に対してガイドラインを普及させることが可能。

② ヒアリング調査

図表 4-2 で示す調査項目のうち、「2-1.中小企業における情報セキュリティ対策状況の実態」及び「2-2.政府や関連団体による普及・啓発に関する取組の現状」について、関係者からより詳細な情報を直接取得し、以後の分析のインプットとするため、ヒアリング調査を実施した。ヒアリングの対象団体数及び質問内容は以下のとおり。

図表 4-7 ヒアリング対象及び質問カテゴリー

No	分類	団体数	質問カテゴリー
1	中小企業	5	● 中小企業におけるセキュリティに関する認識及び情報収集/提供の状況 ● 政府が公開するセキュリティガイドライン等の認知・利用
2	IT 事業者	6	● 中小企業におけるセキュリティに関する認識及び情報収集/提供の状況 ● 政府が公開するセキュリティガイドライン等の認知・利用
3	CPSF に基づくガイドラインに関連する業種のビジネス団体	5	● 中小企業におけるセキュリティに関する認識及び情報収集/提供の状況 ● CPSF に基づくガイドライン等の認知・利用
4	中小企業を対象に含んだセキュリティ対策の普及啓発に関する取組を行う団体	5	● 中小企業におけるセキュリティに関する認識及び情報収集/提供の状況 ● 政府が公開するセキュリティガイドライン等の認知・利用

各事業者・団体から聴取した内容については、質問項目ごとに取りまとめを行った後で、後の分析のため以下の 5 つの分類にしたがって整理した。

図表 4-8 調査結果整理の観点

No	大分類	中分類	
1	政府における取組	1.1	ガイドラインの策定・整理
		1.2	ガイドラインの普及
		1.3	ガイドライン関連活動のガバナンス
2	政府と支援機関間における取組	2.1	政府から支援機関への働きかけ
3	支援機関における取組	3.1	継続的なリソースの確保
		3.2	支援対象の拡大
4	支援機関と中小企業間における取組	4.1	支援機関から中小企業への働きかけ
5	中小企業における取組	5.1	必要性の認識

No	大分類	中分類	
		5.2	リソースの確保

上記 5 つの観点に基づく整理結果は下表に示すとおり。

図表 4-9 ヒアリング結果

No	中分類	ヒアリング結果
1-1	ガイドラインの策定・整理	**○ヒアリングにおける指摘に見る現状** **中小企業のサイバーセキュリティ対策推進における各種ガイドライン等の位置づけ** • 今回ヒアリングを行った団体の多くが、CPSF に基づく分野別ガイドライン等が中小企業にとって高度に感じられる場合があると回答。 • 中小企業の現状を踏まえれば、「中小企業の情報セキュリティ対策ガイドライン」や「サイバーセキュリティ経営ガイドライン」の普及促進に努めるべきであり、分野別ガイドライン等はその先にあるものと位置づけられる。[政府機関、業界団体等] **各種ガイドライン等の活用促進に向けた取組の推進** **◆対策等に関する具体的な記載の拡充** • 活用促進に向けては、対策基準(チェックシート等)やガイドラインを踏まえた具体的なセキュリティ対策の整理が有効ではないか。 • 中小企業ガイドラインは公表当初(2016 年、2017 年頃)よりバージョンアップされており具体的になってはきているが、ガイドラインの記載内容は依然として抽象的であり、企業側の具体的なアクションにつながりにくい。[IT 事業者] **◆理解しやすいコンテンツの作成と周知** • (ビル)オーナーが内容を理解することによって、プロパティマネージメント会社へ指示がなされるため、オーナーにとって理解が容易なもの(例:漫画)があるとよい。 **◆ガイドライン群の整理** • ガイドも色々あり、どれを使っていいのか分からないという声があるので、整理し分かりやすくしてほしい。[IT 事業者] • 中小企業からはこれらのガイドラインの差分について聞かれることがあるが、明確に回答できていない。[IT 事業者] • 業界ごとのガイドラインの普及も適当とは思うが、業界共通の事項と業界固有の事項の整理を適切に行うべき。[業界団体等] • 示された対策のうち、どこまでを実装すべきか悩む場合がある。また、ガイドラインに示された対策の位置づけ(推奨/義務)について質問を受けることがある。明確に示していただけるとありがたい。[IT 事業者] **国際標準の活用による相互運用性の確保** • 工場セキュリティの取組においては、IEC 62334 等の国際標準をベースとして国内におけるルール作りを推進いただきたい。また、工場セキュリティ向上の全体像を構想した上で、その一部として国際標準の活用、例えば IEC 62443 の 2-3、2-4、3-3 を踏まえた JIS 化を検討いただけるとよい。 日本国内における先進的な業界(例:自動車業界)の規格が国際標準と連携できると、他業界へ横展開がしやすいのではないか。[業界団体等]

No	中分類	ヒアリング結果
1-2	ガイドラインの普及	**○ヒアリングにおける指摘に見る現状** **専門家による伴走の必要性** • 中小企業の情報セキュリティ対策ガイドラインを含め、中小企業単体による適用ではなく専門家による伴走支援が必要 [地域コミュニティ全般] • 経営ガイドラインについて、ITベンダーでガイドラインをかみ砕いた上で、中小企業等へお伝えしている。[地域コミュニティ] **DX 等とバンドルした普及の推進** • DX で生産性向上、販路拡大等をしたいという話は担当者にも通じやすく、IT システム導入にセキュリティをバンドルすることも重要 [業界団体等] • 政府機関には DX に伴うセキュリティの必要性についてより広範にアナウンスいただきたい。[地域コミュニティ] **動機づけによる任意の対策実施の支援** • 補助金があることによって、オーナー側に必要性を説明するセキュリティ会社やコンサルタント会社が営業しやすくなると考えられる。また、IT 導入補助金のような単年度の支援というよりは複数年にわたる支援が必要ではないかと考える。[業界団体等] • 一部業界で上流の意識が高いところ(自工会等)では、下流の中小企業も意識している(せざるを得ない)。このアプローチは有効だと考えるが、上流の意識改革から必要であり、それをどのように進めるのかが課題。監督省庁等の働きかけが重要だと考える。[業界団体等] • サイバーセキュリティお助け隊は有効な取組と認識している一方で取組範囲が限定的であるため、さらにサービスが充実するとよい。 [政府機関、地域コミュニティ] **強制力のある施策の必要性** • 自動車、金融及び医療関連業界でガイドラインが業種の達成指標として機能している例があるが、それら以外の業種では十分活用されているとは言えない。[IT 事業者] • ガイドラインが現状調達要件等にもなっていないため、インセンティブが無いことから、対策の必然性がなく、次の段階としてより強制力の強い制度を導入し、それに見合う支援施策を検討すべき。[業界団体等] • ガイドラインに掲載している対策には一定の優先順位をつけている。しかし、特定の企業が優先度の高い対策を調達基準としているという実態が必ずしもあるわけではなく、対策の実施有無をチェックする手段も乏しいため、活用があまり進んでいないものと認識している。[業界団体等]
1-3	ガイドライン関連活動のガバナンス	**○ヒアリングにおける指摘に見る現状** • 中小企業ではガイドラインに記載されている事項の理解もあまりできていない実態があるのではないか。また、ガイドラインの存在自体が中小企業に伝わっておらず、策定したままにするのではなく、策定後のモニタリングも策定者が責任をもって行うべきではないかと思う。[業界団体等] • IPA、商工会議所、東京都、TAMA 協会等各団体が似たような取組を行っており、バラバラになっている。政府に音頭をとっていただき取組を全体として最適化していただけるとよい。[地域コミュニティ]

No	中分類	ヒアリング結果
2-1	政府から支援機関への働きかけ	**〇ヒアリングにおける指摘に見る現状** **団体等の横のつながりの欠如** • 一部を除き、セキュリティに係る大きなイベントは開催されておらず、横のつながりが希薄。業界団体は会員企業に対して簡単に連絡をとることができる一方で、外部の業界団体とは連絡がとりにくい。仮に特定の業界向けの普及活動を行おうとしても、アクセスポイントがわからない。 • 既存の枠組みとして SC3 があるが、セキュリティに関する専門家集団となっており、普及啓発の部分での連携には必ずしも適さない。 • 通常接点を持つ事業者は既にセキュリティに対して一定の問題関心を有する事業者に限られることから、DX やセキュリティ対策を進めようとする際にセキュリティについても関心が芽生えつつある層を捕まえてニーズを把握するところを政府等には期待したい。[以上、業界団体等] **支援機関に対する政府の支援** • 政府に期待する事項：IPA が情報セキュリティ対策について、さまざまなリソースを提供しているが、必ずしも現場に浸透しているとは言い難い状況。IPA と我々のような中小企業支援機関が、予算面、活動面で連携して普及活動を進められるような支援スキームを希望する。[地域コミュニティ] • 支援機関向けの補助金があるとよい。[地域コミュニティ、IT 事業者] • 地域での地道な普及啓発は定量的・即効的な効果は見えづらいが、長期スパンで裾野を広げていく活動を支援いただきたい。[地域コミュニティ] • サイバーセキュリティ経営ガイドラインが公開された際に、セミナーでの紹介を経産省へ依頼したことがあるが、ガイドラインの公開とあわせて、都度セミナーを開催しているわけではない。政府機関側からセミナーでの紹介をもちかけていただけるとありがたい。[地域コミュニティ] **中小企業等の取引先、親会社等への支援** **◆取引先からの働きかけ促進** • 弊社としても抱えている中小企業向けのサイバーセキュリティ対策の底上げ活動を費用持ち出しで行っているが、狙われやすい中小の会社ほど意識が低く、対策費用もかけられない。我々のように企業として仕入先を支えようとしている企業にも、国レベルの支援や同業者共同での底上げ活動が必要。取引先を持つ上位企業の費用負担について補助の検討をお願いしたい。 • 契約条件に入れたいところだが、下請け法の関係もありなかなか難しい状況。仕入れ先に強制力を持たせられるよう、牽引をお願いしたい。[以上、IT 事業者] **◆親会社からの働きかけ促進** • 総務、経理、IT を兼務している担当者に専門知識を学んでもらうことは難しいため、親会社側にセキュリティ対策やその責任を負わせる仕組みがあるとよい。弊グループでは可能なものはシェアードサービスを導入しシステムを共通化することで、子会社のセキュリティを強化している。ただし、親会社と子会社は別会社となるため、利益供与に該当するかについて考慮が必要。親会社のセキュリティ基準に準拠したシステムを子会社は導入することとなるため、コスト高となり得る。したがって、費用上の配慮があると子会社も参加しやすくなると考えられる。(ただし、税務上の配慮が必要)[以上、IT 事業者]

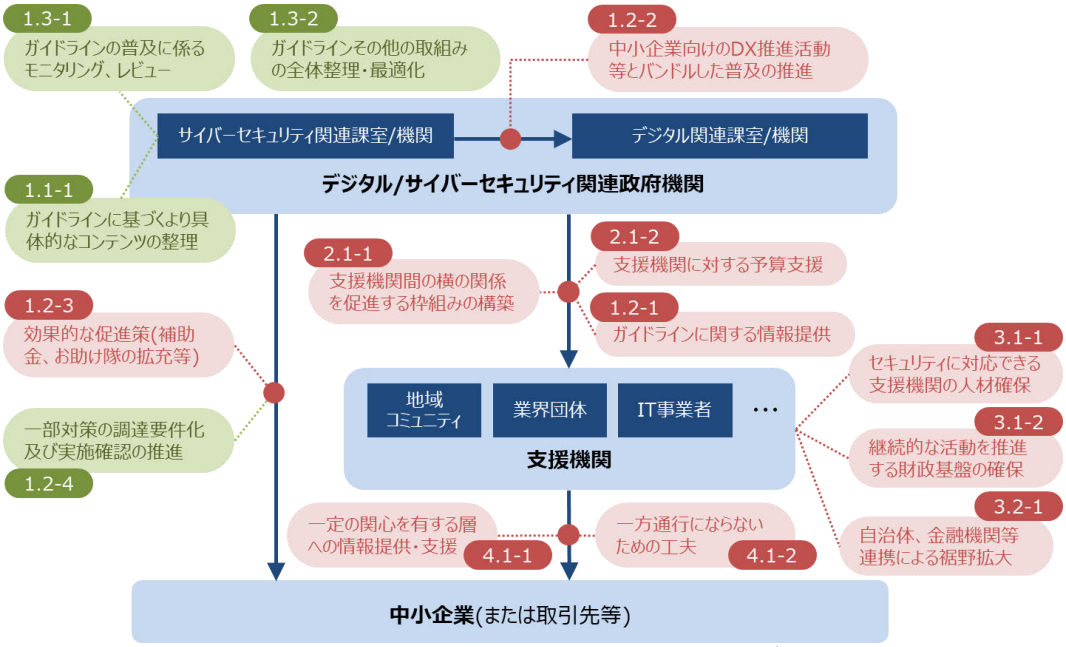
No	中分類	ヒアリング結果
3-1	継続的なリソースの確保	**〇ヒアリングにおける指摘に見る現状** • サイバーセキュリティの重要性は理解しているが、商工会議所における経営指導員の年齢層が高く対応が難しい場合や、県内のサイバーセキュリティ人材が不足しているケースがある。 • 専門家を個別に派遣する場合には費用が多くかかるため、集合研修を有効活用することが重要と考える。[以上、地域コミュニティ]
3-2	支援対象の拡大	**〇ヒアリングにおける指摘に見る現状** **業界団体間の連携による支援の拡大** • セキュリティ系団体は、非 IT 系を含む民間団体(商工団体、金融機関、業界団体(自工会、金型組合等))との連携に課題あり。 • ビルや工作機械は、業界内の大多数の事業者が所属しているため、他団体との連携の必要性を感じていない。 • スマートホームや制御機器では複数のステークホルダーが絡むため、団体連携は積極的に行っている。他方、これらの団体は大企業が中心で中小企業の参画がほとんど無い。 • 地域コミュニティは、商工会議所をはじめ、地域の経済団体等と連携している。経済団体等と連携したセミナーを実施することで、互いの会員企業等への情報普及が図れる。また各団体に対し「出前講座」の枠組みにより様々な有識者を派遣することで連携を図っている。 **民間企業との連携による支援の拡大** • 複数の地域コミュニティが、支援拡大を図るため、自治体や地域金融機関と連携したチャネル開拓を実施している。具体的には、セミナー開催(融資先に行う経営支援サービスの一環)、金融機関からの支援先の紹介がなされている。 • また、セミナーの開催等にあたって IT ベンダーとの連携を行った事例もあった。地域コミュニティ内で他地域の情報が十分得られない場合、IT ベンダーと連携する形で進めているとのことであった。 • セキュリティベンダーやセキュリティコンサルに委託する費用が高いため、お抱えの事業者へ依頼を行うと考えられる。適切に設定を行えていないケースがあるため、お抱えの事業者にもセキュリティについて学んでいただくことが重要と考えられる。具体例等を示すことでかかる事業者が適切なセキュリティ実装を行えるレベルまで教育支援を行うことが大切。[IT 事業者]

No	中分類	ヒアリング結果
4-1	支援機関から中小企業への働きかけ	**○ヒアリングにおける指摘に見る現状** **◆サイバーセキュリティに対して関心の低い層に対する働きかけ** • 多数の団体からセキュリティに係る課題認識を持つ中小企業がそもそも少ない点が指摘されている。そういった企業に対しては、まずセキュリティ対策そのものの必要性から説く必要があり、機運を高めてから、具体的なガイドラインの存在やその中身を説明する、何かと抱き合わせにするか景品を出す等の施策が提案された。 • その際、DX によって将来像を描くと同時にサイバーセキュリティの重要性を理解いただくことが重要。 • また、意識啓発の方法についても、同じ情報提供をするだけでは聞き手に対する効果がさらに薄くなる可能性がある点が指摘された。 **◆サイバーセキュリティに対して一定の関心がある層に対する働きかけ** • 関心を持って参加する企業には、ガイドラインの内容をいかに分かりやすく説明できるか(例を用いる等)が課題。 • ワークショップや演習等の参加型の形式は多数の団体から有効であった旨の意見があった。 **◆IT 導入補助金と関連した働きかけ** • サイバーセキュリティお助け隊導入を IT 導入補助金の加点要素にしていただいた結果、申請する業者から問い合わせが増加し、契約件数が増えた経緯がある。ただし、導入から利用料の補助が切れる 1 年後にサービスを解約した企業が多くみられた。 • IT 導入補助金制度の条件に該当する事業者に対して、サイバーセキュリティお助け隊サービスと併せて制度の案内を行っているが、中小企業が独力で IT 導入補助金を申請することは難しい。 • 販売パートナーは、中小企業が興味をもっているシステムに関する情報を積極的に中小企業へ提供しているようである。営業活動の一環として補助金に関する情報を中小企業へ提供しているようであるが、セキュリティに特化した情報はあまり提供していないようである。[以上、IT 事業者] **◆効果的な周知・啓発方法** • サイバーセキュリティ単体で集客の期待はあまりない一方で、大規模イベント(CEATEC)を活用したセミナーについては、多くの参加がある。 • 中小企業はセミナー等の情報を随時チェックしていないため、プッシュ型の案内の方がリアクションを期待できる。[地域コミュニティ] • ガイドラインの周知を行う際には、FAX での案内送付、ポスター等を活用した普及啓発も重要。[業界団体等] • 地域の名士企業が取組に前向きになると、地域の企業も取組に前向きになるケースがある。つながりを広げていくためには、影響力がある人やそのネットワークを見極めることが重要となる。セキュリティ単体での働きかけは難しいため、セキュリティに対する優先順位をあげてもらうための働きかけを行いつつ、各企業と WIN-WIN の関係を構築することが重要である。[IT 事業者] • 依頼を受けて SC3 の会合にて講演を行ったが、地域によってセキュリティに対して積極的な地域とそうでない地域がみられる。 • 後者は、政府等の推進主体が地域のキーマンと出会えていない可能性があるため、各地区に普及を進める(説得する)人を配置するべきではないか。キーマンと会うために地方を行脚する体制があるとよい。また、業界の横のつながりを活用することや商工会議所の若いメンバ(青年会等)にアプローチすることも有効と考えられる。[中小企業]

No	中分類	ヒアリング結果
5-1	必要性の認識	**〇ヒアリングにおける指摘に見る現状** **◆サイバーセキュリティに対する関心の低さ** • サイバー攻撃を受ける可能性が低いとの理由でセキュリティ対策を実施しない企業が存在する。特に、都市部と比較して地方ではその傾向が顕著。 • 能動的にセキュリティに関する情報収集を行っている企業は極めて少数である。(情報収集を行っていたとしても、補助金情報のみであったりする) [以上、IT 事業者] • ある中小企業の経営者は「うちにとられて困るものはないからリスクはない」とおっしゃっていた。このような場合は「明日 PC のデータが消えたときにお客さんに迷惑かからないか」と問いかけるようにして、リスクを伝えている。 • セミナーの案内はシステム部門に丸投げされることが多い。経営層もセキュリティについて理解が追いついていないため、セミナーに参加することは少ないのではないか。したがって、地方では、情報の内容よりも顔の見える関係での情報交換、特に情報の発信主体が重要となる。医療分野ではセキュリティに馴染みがない方が多いため、いい仲間といい情報に出会えるかが重要なポイントとなる。[以上、中小企業] **◆人材、予算等の不足** • 中小企業ではセキュリティ担当が設置されていたとしても兼務が多く、リソース(人や時間)が不足していることが原因の 1 つとして考えられる。情報提供はメール等で行うが、そもそも担当者が自席にいて PC を見ている時間も短いようである。 • サイバーセキュリティ対策には非常に費用がかかる(例:1 声 100 万円)というイメージが NHK の報道によってついてしまったことも、反応が薄い原因の 1 つ。 • セキュリティ人材の不足が課題である。セキュリティ人材の確保を進める一方で、弊グループではシェアードサービス等を導入することによって各社のセキュリティへの負担を軽減させる方向で進めている。 • セキュリティ人材が不足しているため、政府による育成の仕組みがあるとよい。個別の話になるが、弊社から人材を派遣している ICS-CoE の教育プログラムは企業側の負担が大きい。参加費用が大きいだけでなく、派遣した人材の業務が止まることも大きい。業務を続けながら学ぶことができる仕組みか、あるいは企業側のデメリットを補填する支援があるとよい。(例:業務をとめずに教育制度に参加できるような仕組み、派遣した人材の人件費を補填する仕組み、人材を派遣した企業に対して報奨金を提供する仕組み) **◆サイバーセキュリティに対する関心の高い企業の共通性** • サプライチェーン上位企業から説明を受けている企業や、上記に伴い、今後視察がある等の噂を聞いて取組始めている企業、過去に被害を受けた経験がある企業はセキュリティ対策の推進を積極的に行っている傾向にあり、実際にそのような企業から問い合わせをいただくことがある。しかし、被害を受けてない企業の関心は総じて低い。 • セキュリティ被害情報は被害企業から外に出ず、公にならないことがほとんどであり、同業他社でインシデントが生じていてもそれを知る由がない。 [以上、IT 事業者]

③　課題整理・施策の特定

机上調査及びヒアリング調査を踏まえて、CPSF に基づくガイドライン及びユースケース、その他のサイバーセキュリティ関連基準・標準等の認知・利用拡大を推進していく上での課題等を具体化した。具体化した課題は、それぞれの「効果の大きさ」及び「実施容易度」の 2 軸からスコアリングし、優先順位付けを行った。課題間の優先順位付けを行った結果、優先的に実施することとした課題(赤：優先度高となった課題、緑：優先度中となった課題)を、各主体間の関係の中にマッピングすると以下のようなイメージになると考えられる。



図表 4-10　優先的な課題のマッピング

まず、関連する政府機関内で取り組むべき課題としては、「中小企業向けの DX 推進活動等とバンドルした普及の推進」が挙げられる。サイバーセキュリティ対策は、事業や業務のデジタル化と並行して検討すべきものであり、「DX with Cybersecurity」実現のためには、DX 認定や各種補助金施策等の制度的な支援におけるサイバーセキュリティの位置づけ明確化やさらなる取組を喚起する仕組みの強化に加え、事業者や団体等に対する説明の場の共有等を通じてリーチできる範囲を拡大していくことが有効と考えられる。

また、中小企業個社に対する直接的な支援としては、従来から実施されている補助金等の「効果的な促進策」が行動変容のために重要と考えられる。貴省では、中小企業向けに IT 導入補助金等の仕組みを既に運用しているが、事業者・団体からは、当該制度でカバーされている製品・サービスの範囲拡大や助成額の向上等について意見があった。

他方、より広い範囲の中小企業へと取組を拡げていくためには、地域コミュニティや業界団体、IT 事業者等の支援機関による取組を喚起することも重要と考えられる。今回ヒアリングを行った地域コミュニティ等の活動は有効性が認められる一方で、有志の持ち出しにより運営されている場合が多いことから財政面や人材面で課題を抱えていることが多く、それらの活動の持続可能性を確保するために「支援機関に対する予算支援」を行ったり、「支援機関間の横の関係を促進する枠組みの構築」を通じて全体の水準を向上させる取組の優先度が高いと判定された。

＜施策の特定＞

これまでの分析にて取組推進の優先順位が高いとされた課題に対して今後講じ得る施策(案)を具

体化した。施策(案)は、働きかける対象としてどの主体を想定するかにより以下の(A)～(C)に分類した。

A) デジタル/サイバーセキュリティ施策に係る政府内の連携措置
　A-1. DX 推進施策との連携
B) 中小企業個社(又は取引先等)を対象とする措置
　B-1. 個社への対策促進施策
　B-2. 取引先等への対策促進施策
C) 支援機関を通じた対策推進に向けた措置
　C-1. 個々の支援機関に対する支援措置
　C-2. 支援機関間の連携を促進し活用する措置

分類のそれぞれについて、ヒアリングでいただいた意見やその他の情報を加味し、以下のように今後に向けての推奨事項を整理した。

(A) デジタル/サイバーセキュリティ施策に係る政府内の連携措置

A-1. DX 推進施策との連携

政府内における DX 関連課室等との連携を通じて、様々なチャネルから中小企業又は支援機関に網羅的に働きかけを行い、DX 及びサイバーセキュリティについて役割を認識している支援機関や協力関係を結ぶことのできるキーマン(地域や業界において一定の発言力や影響力を有する個人又は団体であり、サイバーセキュリティに対して積極的な者)を増やすことが望ましい。働きかけの実施にあたっては、中小企業関係者でも理解が容易なコンテンツを整備しておくことも有効と考えられる。

また、制度面においては、B-1 で述べるように、国の制度を活用しながら DX を推進しようとする事業者が、並行してサイバーセキュリティ対策にも相応の投資を行うことを喚起できるような仕組みをさらに強化することが望ましい。

また、展開するガイドラインについても、複数あると中小企業にとっては取捨選択が難しくなるため、既にある程度の普及が見られる「中小企業の情報セキュリティ対策ガイドライン」及び関連するアセスメントツールを中心に、ベースラインとなるものに一本化することが望ましい。

参考となる海外事例

- 米国：NIST Cybersecurity Framework の普及に係る取組
  - NIST Cybersecurity Framework の製造業のプロファイル(NIST IR 8183)の作成/HP 上での公開
  - NIST Cybersecurity Framework のクイックスタートガイドの作成/HP 上での公開
- 米国：DHS/CISA による中小企業向けの取組(中小企業向けのガイドである CYBER ESSENTIALS の作成/スターターキットの無償公開/ウェビナーでの紹介)
- EU：ENISA による中小企業向けアセスメントツールの提供
- ドイツ：中堅企業向け IT セキュリティ移行拠点(TISiM)の構築

(B) 中小企業個社(又は取引先等)を対象とする措置

B-1. 個社への対策促進施策

現行の IT 導入補助金において、既に「サイバーセキュリティお助け隊」を軸とした支援措置が講じられているが、そのカバー範囲や補助額等に関して多数の事業者から意見を得たところ、今後に向けては以下のような施策を講じることが考えられる。

- 「サイバーセキュリティお助け隊」がカバーする範囲を、ライフサイクル全体を対象とするため、現行の端末監視やネットワーク監視及び付帯サービスから、他の製品/サービス分類も含めるよう拡張する。
- セキュリティ対策導入時に事業者への補助率を向上させる。

その際、製品・サービス範囲の拡大範囲として、例えば、各中小企業にて IPA 自社診断を実施の上、より多くの項目で求められている類型を制度に組込むことも想定される。(例：一般従業員向け教育・リテラシー教育、ポリシー管理・設定管理、入退室管理システム、コンサルティング(現状分析、ポリシー策定等)、個人認証用デバイス及びその認証システム、訓練(演習)等)

＜参考となる海外事例＞
- 米国：SBA によるサイバーセキュリティパイロットプログラムを通じた助成金の提供
- ドイツ：資金援助プログラム(go-digital、Digital Jetzt)の提供
- 韓国：韓国インターネット振興院(KISA)が運営する地方情報保護支援センターによる中小企業を対象としたサイバーセキュリティに関するサポートの提供

B-2. 取引先等への対策促進施策

B-1 で述べた中小企業個社への支援に加え、中小企業を含むサプライチェーンに対して一定のセキュリティ要件の実装を求め、その遵守状況に応じて取引先企業とともに改善策を講じようとする大企業や中堅企業(企業グループの親会社を含む)による取組を支援するような施策も中小企業の取組を喚起するにあたり有効と考えられる。

そのような取組を行うに当たって考慮すべき競争法に係る留意事項等を示したものとして、「サプライチェーン全体のサイバーセキュリティ向上のための 取引先とのパートナーシップの構築に向けて」が公表されているが、当該文書では「積極的に価格の交渉の機会を設け、取引の相手方と十分に協議を行い、サイバーセキュリティ対策の内容や費用負担の在り方を決定する」ことが求められているところ、独占禁止法や下請け法に抵触するリスクや金銭的障壁の軽減が必要と考えられる。

＜参考となる海外事例＞
- ドイツ：自動車業界における TISAX(Trusted Information Security Assessment Exchange)の取組

(C) 支援機関を通じた対策推進に向けた措置

C-1. 個々の支援機関に対する支援措置

今回机上調査やヒアリング調査を実施した支援機関の取組状況は様々であり、地域や業界によって取組の広さや深さに大きな差がある点が明らかになった。今後、個別の支援機関の取組を促進、喚起するため、優れた取組を行う地域や業界の事例を参照しながら、まずは目標を明確化した上で、現状の取組を評価し、改善及び取組状況のシェア等に向けた施策を講じる必要がある。

取組が進んでいない業界・地域に対しては、セキュリティ有識者(JNSA 等)が伴走して進めることも考えられる。

＜参考となる海外事例＞
- 豪州：産業・科学・エネルギー資源省による Cyber Security Connect and Protect Program の実施

C-2. 支援機関間の連携を促進し活用する措置

「支援機関」には様々な性質の組織が含まれ得るところ、それらを一括りにするのではなく、例えば以下のようにさらなる分類を行った上で現状と課題の整理を行うことが適当と考えられる。
- 企業に直接セキュリティ対策支援を行う支援機関
  普段から、企業と物理的に近い距離で活動し、地域の中堅・中小企業等に DX・サイバーセキュリティ関連の支援を提供する。
- セキュリティ対策支援をさらに促進させる支援機関
  地域のプラットフォームやハブ機能等として活動する存在や、地域の支援機関と協働する。ある特定の専門的知見・ノウハウをもって、上記機関と協働する。

上記で挙げたような類型の支援機関が効果的に連携することを通じて、B で述べたような中小企業に対する動機付けを通じたニーズの掘り起こしと並行して、「中小企業の情報セキュリティ普及推進協議会」等の既存体制も活用しつつ、リーチできる中小企業の幅を広げ、地域 IT ベンダー等の支援機関としての対応能力の向上を図っていくことが望ましい。

＜参考となる海外事例＞

・ 米国：NIST Small Business Cybersecurity Community of Interest(COI)の立ち上げ

4.3.2 IPA の機能強化に向けた調査

本項では、セキュリティガイドライン等策定に係る政府内での役割整理や規制的なアプローチの採用を含め、セキュリティガイドライン等の更なる普及の推進に係る検討を行うにあたり、必要な情報を収集することを目的として調査を行った。

① 調査内容

調査項目は以下のとおり。各調査項目は Web 等を活用し机上にて調査を行った。

図表 4-11 調査項目

調査項目	説明
1. 日米のサイバーセキュリティ政策推進体制の全体像	
1.1. 日米におけるサイバーセキュリティ政策に係る体制の全体像	日米それぞれで、行政機関、標準化機関、研究機関が入る全体像(関係図)を示す。
1.2. 各機関の役割と概要	全体像で示した日米の各機関について、個別に役割や概要の説明を付す。
2. 標準化機関の組織・機能面に関する日米比較	
2.1. 基本情報	各標準化機関について、組織としての基本情報を明確化し、比較する。
2.2. 他の政府機関との関係性	標準化機関として、規制等に係る行政機関及び研究機関との関わりのありよう(例：恒常的な連携関係、これまでの連携実績)を示す。
2.3. 官民連携の実施状況	標準化機関と民間部門との関わりが組織的になされているものについて、概要/予算・人員規模/推進 PJ と民間の参画状況/主要アウトプットを示す。
3. 標準化機関等から発行される文書体系等の日米比較	
3.1. 文書発行体と文書体系	ガイドライン等を発行する機関と当該機関から発行されるガイドライン(主にシリーズ化されているもの)の体系について、日米で比較を行う。
3.2. 近年の注力領域	標準策定の観点から日米それぞれで近年特に注力されている領域を示し、比較する。
4. 日本における標準化に係る機関等のあるべき姿の検討	
4.1. 組織・機能面のあるべき姿	-
4.2. 発行される文書体系等のあるべき姿	-

② 調査結果

以降、調査結果を以下の項目ごとに整理して提示する。

- 1.日米のサイバーセキュリティ政策推進体制の全体像
- 2.標準化機関の組織・機能面に関する日米比較
- 3.標準化機関等から発行される文書体系等の日米比較
- 4.日本における標準化に係る機関等のあるべき姿の検討

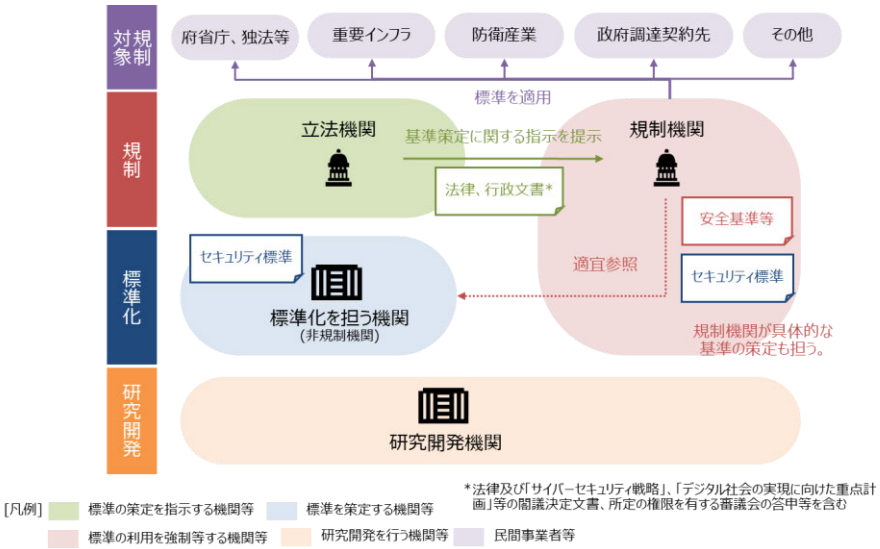
- 1.日米のサイバーセキュリティ政策推進体制の全体像

本項では、日米それぞれで、サイバーセキュリティ政策に関連して、行政機関、標準化機関、研究機関としてどのような関係機関があり、それぞれがどのような役割分担で施策の推進等を行っているのかを整理する。

まず、日本では、所掌対象となる業種その他のカテゴリーごとに監督省庁が存在しており、(実質的に)規制として機能する基準・標準については、業種等で共通する内容を示した手引き等を参照しつつ策定されているものもあるが、重要インフラ業種や防衛産業等と同様、既に監督省庁又はそれと深い関係を有する業界団体等により策定されていることが多い。

事業者に規制として課されるわけではないボランタリーな基準・標準については、これまで、貴省、総務省、IPA 等により策定されている。代表的な基準・標準として、「サイバーセキュリティ経営ガイドライン」(貴省・IPA)、「サイバー・フィジカル・セキュリティ対策フレームワーク」(貴省)、「テレワークセキュリティガイドライン」(総務省)等がある。

各業所管を行うにあたり、規制機関により、貴省や IPA で定めるボランタリーなガイドラインが参照されることは少なく、むしろ自らが策定している基準が主に参照されている。

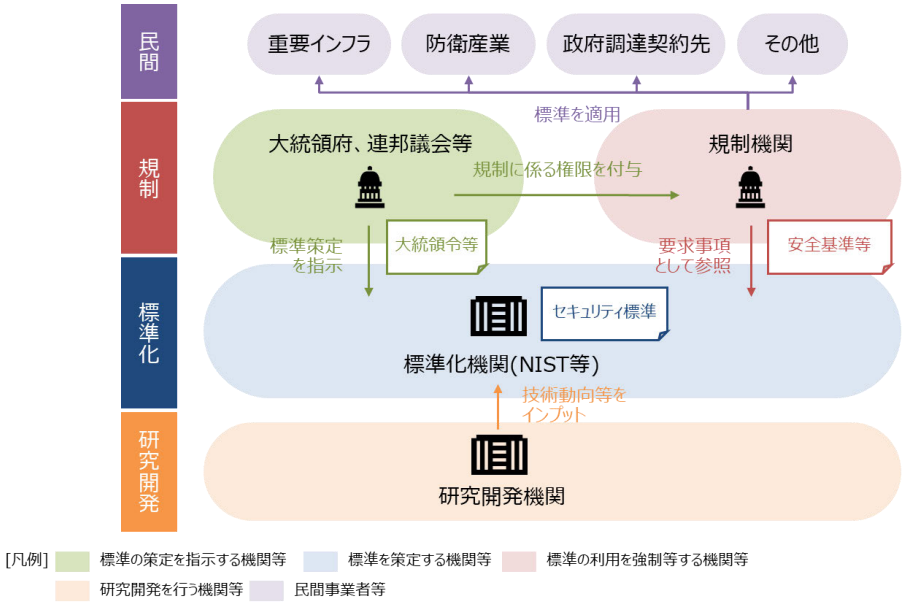


図表 4-12 日本政府における体制の全体像

一方、米国においても、所掌対象となる業種その他のカテゴリーごとに監督省庁が存在している点は共通しているが、特に政府調達(防衛調達を含む)において、NIST が策定した基準・標準が盛んに参照されている点に特徴がある。こうした役割分担を形成するにあたり、多くの場合、連邦法又は大統領令の中で NIST に対して基準・標準策定に関する権限を与えるという形式がとられている。例えば、2002 年に公布された連邦情報セキュリティマネジメント法(FISMA : Federal Information Security Management Act of 2002 FISMA : Federal Information Security Management Act of 2002)は、連邦政府機関が情報セキュリティを強化することを義務付け、

NIST に対しては、そのための規格やガイドラインの開発を義務付けている [28]。また、2021 年に発行された大統領令第 14028 号「国家サイバーセキュリティの向上」においては、ソフトウェアサプライチェーンのセキュリティ強化や IoT 製品のラベリングに関する各種ガイドラインの策定が支持されており、それらは政府調達等で活用されている。

さらに、その他、重要インフラ関係については CISA、機密情報管理については DoD にてガイドライン策定が行われている。



図表 4-13 米国政府における体制の全体像

日米間で大きな差異となっているのは、基準・標準の策定を担う機能やそれらと規制機関との関係のあり方であり、さらに言えば、米国ではそういった機能が個々の規制機関等と分離され NIST 等へ集約されており、そこで策定された基準・標準が監督機能等を担う機関に活用されている点(連邦法や大統領令による権限の付与等も含む)にあると考えられる。

- 2.標準化機関の組織・機能面に関する日米比較

<2.1 基本情報>

米国における NIST(コンピューターセキュリティ部/応用サイバーセキュリティ部)と同様、セキュリティ標準を策定する部署は IPA(デジタル基盤センター/セキュリティセンター等)と AIST(サイバー・フィジカル・セキュリティ研究センター等)においてもみられた。ただし、かかる組織においては役割や業務範囲が異なっており、NIST 法を通じて NIST(商務長官)には標準策定に係る権限が割り当てられている一方で、「情報処理の促進に関する法律」に係る業務範囲の中で標準策定について言及されておらず、日本における IPA には必ずしも権限が割り当てられているとは言えなかった。

予算・人員の規模の観点では、部署単位で比較した際に前述のセキュリティ標準の策定に係る部署において、NIST と IPA の人員数は同程度の可能性がある。しかし、取組面を比較すると、IPA や AIST で策定されているセキュリティ標準の数は NIST より少ない。また、詳細は後述するが、NIST が策定したセキュリティ標準は体系的に整理されていたが、IPA や AIST の標準は NIST と比較して体系的に整理されていなかった。

<2.2 他の政府機関との関係性>

米国及び日本において、セキュリティ標準について各省庁で協議・調整を行う場は存在する一方で、日本にはそのセキュリティ標準のニーズの特定や標準化の方針を決定する場がない可能性がある。

米国と日本において、プロジェクト単位で各標準機関が大学研究機関と連携する取組はみられる。また、セキュリティ標準策定に限定しなければ、NIST において大学研究機関と共同で専門の研究機関

を設立している事例もみられ、専門の研究機関において継続的な情報共有や研究開発を行えている可能性がある。

<2.3 官民連携の実施状況>
NCCoE とキャンパスサイバーを対象として、組織の位置づけ及び取組内容から比較を行った。

図表 4-14 比較結果

項目	比較結果
組織の位置づけ	● NCCoE は NIST(応用セキュリティ部)の一部門であり公的な組織における取組(プロジェクト単位で民間企業を募集)として位置づけられる一方で、キャンパスサイバーは企業(大企業、中小企業)、政府機関、研修機関、研究機関が参画する官民が共同で出資している組織として位置づけられる。 ● NCCoE では、NIST の予算の一部として予算が割り当てられており、キャンパスサイバーにおいては、国家サイバーセキュリティ戦略の枠組みから資金提供がなされている。 ● キャンパスサイバーでは、相乗効果を期待し 1 つの建物内で検討を実施。
取組内容	● NCCoE ではセクターごとにラボを設置し、実証環境を構築した上で、NIST が策定したセキュリティ標準の実践ガイドを作成している。 ● キャンパスサイバーでは各作業グループにおいて研究開発及びプロトタイピングのサポートを行っており、具体的なツール等を作成。 (例:知識、仕様書、データセット、技術構成要素の作成等。) ANSSI が公開した文書の中で、キャンパスサイバーが策定した文書やツール等は参照予定と明記されている。

● 3.標準化機関等から発行される文書体系等の日米比較

<3.1. 文書発行体と文書体系>
日本と米国における文書発行体及び文書体系について、「分野ごとのセキュリティ対策強制の有無」、「標準化機関等に対する標準策定指示のあり方」、「標準策定に係る政府内の役割分担」、「策定されている標準の体系化、量的な充実の程度」という 4 つの観点から比較を行った。結果の概要は以下のとおりである。

◆分野ごとのセキュリティ対策強制の有無
先述したとおり、米国では FISMA 等により政府機関及び調達先において一定のセキュリティ対策の実施を義務付けており、その後複数回の大統領令の公布を通じて、義務の範囲は管理された非機密情報(CUI)の保護やソフトウェアサプライチェーン対策等を含むように拡大している。また、重要インフラ保護に関しては、NIS 指令による一律の対策義務化を行う EU とは異なり、横断的な規制は敷かず、ボランタリーな取組の喚起が中心となっている。
他方、日本においても、サイバーセキュリティ戦略本部が決定する「政府機関等のサイバーセキュリティ対策のための統一基準群」への対応が政府機関等には求められており、米国の動向も捉えつつ、随時対策事項の改正を行っているが、ソフトウェアサプライチェーン等一部の対策については、現状では必ずしもリーチされていない場合がある。また、サイバーセキュリティ基本法に定めのあるように、重要インフラ事業者等においてサイバーセキュリティ対策の実施は努力義務とされており、横断的に強制力のある法規が必ずしも定義されているわけではないという点において米国と共通していると考えられる。

◆標準化機関等に対する標準策定指示のあり方
こちらも先述したように、米国では、連邦法又は大統領令にて、NIST 又は CISA 等その他の機関に対して所定の基準・標準の策定を求めるものがある。これらにおいては、基準・標準で扱う具体的な

内容、策定を担当する機関、指名された機関による対応の〆切等が明確に記載されている。
一方、日本では、強制力を伴う法規という形式よりも、「サイバーセキュリティ戦略」や「デジタル社会の実現に向けた重点計画」等の政策文書において標準化の対象となる要素を抽出したり、担当省庁が割り当てられることがあるものの、基準・標準の具体的な内容や策定期限が具体的に示されることは少ない。

◆標準策定に係る政府内の役割分担
米国の政府調達においては、行政管理予算局(OMB)が拘束力のある規則等の策定を担う一方、特に大統領令等にて権限の付与がなされているような場合に顕著であるが、規則を実際に履行する際に参照する具体的なガイドライン文書については NIST が策定を行っていることが多く、一定の役割分担がなされている。また、重要インフラ等の民間分野についても、政府調達分野ほど顕著ではないものの、Cybersecurity Framework に代表される NIST 標準が参照される傾向がみられる。
一方、日本においては、前述したように、監督業務を担う所管省庁又は関連する業界団体が、基準・標準の策定を担うケースが多く、それらの機関以外が策定したボランタリーな基準・標準が参照されることは少ない。

◆策定されている標準の体系化、量的な充実の程度
米国では、主に政府機関が利用することを想定した NIST 標準について以下のような体系化がなされている[29]。

・ FIPS
米国商務長官の承認を受けて、NIST が公布した情報セキュリティ関連の文書。主なターゲットは米国政府だが、推奨する管理策や要求事項、暗号化やハッシュ化、認証、デジタル署名及び LAN のセキュリティ等、分野別に、詳細な基準や要求事項、ガイドラインを示し、政府機関のみならず、民間企業にとっても、情報セキュリティ対策を考える上で有用とされる。調査実施時点で利用可能なものは 11 件。

・ Special Publication (SP) 800 シリーズ
SP 800 シリーズは、コンピューターセキュリティ部(CSD)が発行するコンピューターセキュリティ関係のレポート。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文だが、 内容的には、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応等、セキュリティに関し、幅広く網羅している。調査実施時点で利用可能なものは 176 件。

・ Special Publication (SP) 1800 シリーズ
NIST の一部門である NCCoE が募集し民間事業者が参画するコンソーシアムにて作成する文書。サイバーセキュリティ・コミュニティに対して、実用的で使用可能なサイバーセキュリティ・ソリューションを提示する。調査実施時点で利用可能なものは 26 件。

・ NISTIR
NIST の各内部機関がまとめたレポート。調査実施時点で利用可能なものは 264 件。

その他、CISA や各業関連機関から多数の文書が公開されているが、NIST でなされているようなあり方で必ずしも体系化されていないものもある。
日本では、NISC で策定されているものが政府統一基準群、重要インフラ関連規定としてまとめられているが、米 NIST が発行するものに対して量的な充実が見られるとは言えない。また、その他ボランタリーなガイドラインについては、対象者や対策分野等によって多数のシリーズが存在しており、必ずしも 1 つの体系をなしているわけではない。さらに、米国における SP 1800 に相当する具体的な実装方法まで言及する文書は、政府機関等から発行されるものとしては基本的に存在していない。

比較項目	米国	日本	両国の主な差異
分野ごとのセキュリティ対策強制の有無	• 政府システムについて、FISMA等で一定の対策を義務化 • 重要インフラ等について、横断的な規制はなく、ボランタリーな取組みの喚起が中心	• 政府システムについて、統一基準に則った対策を義務化 • 重要インフラ等について、対策の実施は努力義務と位置づけ※1	• ソフトウェア調達等の一部の領域を除き、日米で必ずしも大きな差異は見られない
標準化機関等に対する標準策定の指示のあり方	• 連邦法や大統領令にて、NIST等への具体的な指示を実施 • 標準化の主題だけでなく、策定主体や策定期限を明示しつつ指示がなされる	• サイバーセキュリティ戦略や重点計画において標準化の主題や担当省庁が示されていることがある • 主題や策定期限がの具体的に示されることは少ない	• 米国の大統領令にあるものと比較して、日本の法令や閣議決定文書等における基準等策定の指示は曖昧さを残すことが多い
標準策定に係る政府内の役割分担	• OMB等の規制機関が規則の策定等を担う一方、(特に大統領令等にて規定される場合)標準策定の多くはNISTへと委任	• 制度的な位置づけが明確な標準について、NISCや防衛省、総務省等の規制機関または業界団体が自ら標準策定を実施	• 対象とした基準策定は規制機関に集中しており、米国にあるような役割分担は希薄 • 強制基準にて自主的なガイドラインはほとんど参照されていない
策定されている標準の体系化、量的な充実の程度	• NISTで策定されるものについては、FIPS、SP 800、SP 1800等にシリーズ化されており、それぞれ11、176、26件の文書が利用可能 • 上記は政府機関だけでなく、民間からも参照されている	• NISCで策定されているものについては、政府統一基準群、重要インフラ関連規定にまとめられているが、文書数は比較的限定的 • その他自主的なものについては、多くがシリーズ化されていない	• SP 800等と比較して日本では具体的な手順・マニュアル等の整備は限定的 • SP 1800に相当する具体的な実装方法にまで言及する文書は日本には存在しない

図表 4-15 日米間の現時点での比較

<3.2. 近年の注力領域>

NIST では、「暗号」、「リスク管理の強化」、「実用的ソリューション」、「モノのインターネット」(IoT)、「産業用制御システム」、「人材教育・訓練」、「アイデンティティ・アクセス管理」という 7 つの領域における検討を優先的に推進 [30] している。日本においても主にサイバーセキュリティ戦略等で示されるように、

重点領域	米NISTの取組み	日本における主な取組み	日米の取組み比較
暗号 (Cryptography)	• 暗号アルゴリズムの設計と検証 • ポスト量子暗号(PQC)の標準化 • 軽量暗号の標準化	• 耐量子計算機暗号や量子暗号等に関する研究の推進や、その事業化・標準化等[複数省庁]	日米とも量子分野や軽量暗号に関する研究開発及び標準化の取組がなされている。
リスク管理の強化 (Enhanced risk management)	• リスク管理フレームワークの策定・改定と適用の促進(CSF、PF、RMF等)	• CPSF等に基づくガイドライン等の策定[経産省] • 行動計画の積極的改定[NISC] • 自治体ガイドライン推進[総務省]	日本では複数省庁にて多岐にわたる分野のガイドライン策定が分業されている。
実用的ソリューション (Practical solutions)	• NCCoEにおける官民パートナーシップの推進、SP1800シリーズの発行	• セキュリティ製品・サービスの有効性検証を行う基盤整備[経産省] • CYNEX[総務省/NICT]	日本でも環境整備が進められているが、SP1800シリーズのような標準化と連動した活動とはなっていない。
モノのインターネット (Internet of Things)	• IoT Device Cybersecurity Core Baselineの策定 • 連邦政府向けプロファイルの策定	• IoT製品に対するセキュリティ適合性評価制度構築[経産省]	日米ともIoT機器の認証・ラベリングの取組みが推進されるが、米国では政府調達関連の取組みも志向される。
産業用制御システム (Industrial Control Systems)	• SP 800-82 Rev.3の策定 • 実用的なソリューション例の開発 • CSF製造業プロファイルの策定	• 工場ガイドラインの策定[経産省] • システム等の信頼性を確認する技術検証体制整備[複数省庁]	日米ともガイドラインの策定に加え、ソリューション例の開発や技術検証等、実装面での支援も提供している。
人材教育、訓練 (Workforce education & training)	• NICE サイバーセキュリティ人材フレームワークの策定及び適用支援 • 全米のサイバーセキュリティ人材のニーズと供給の可視化	• 「プラス・セキュリティ」知識を補充できる環境整備 • 人材の流動性・マッチングに関する取組 等[複数省庁]	日米とも人材のニーズと供給の可視化、マッチングに関する取組がなされている。
アイデンティティ・アクセス管理 (Identity & access management)	• 「連邦職員の個人ID検証(PIV)」標準第3版の策定 • SP 800-63 第4版草案の策定	• 本人確認の手法に関するガイドライン策定等[デジタル庁]	日米ともにデジタルアイデンティティに関する取組みを行っているところ、PIV等のセキュリティクリアランスに係る標準化については米国が先行している。

図表 4-16 日米間の現時点での比較

国内でも複数の省庁が連携しつつ一定の取組が推進されているところ、主な差異としては、「リスク管理の強化」における複数省庁による分業(日本)、「実用的ソリューション」における標準化と結びついた製品・サービスの有効性検証(米国)、「モノのインターネット」や「アイデンティティ・アクセス管理」等で見られる政府調達の活用(米国)等があると考えられる。

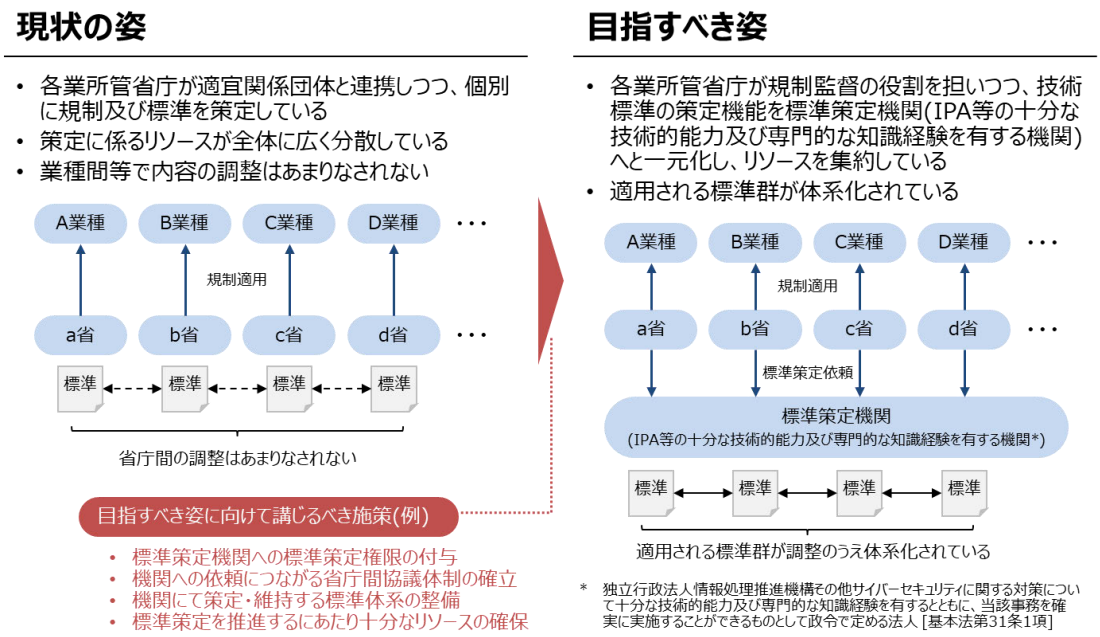
● 4.日本における標準化に係る機関等のあるべき姿の検討

<4.1.組織・機能面のあるべき姿>

これまでの調査結果から、日本においては各業所管省庁又は関連団体が個別に基準・標準の策定を行い、対する米国ではそのような機能のある程度が NIST に集約されており、連邦法又は大統領令による権限が付与されている。このような状況においては、基準・標準の策定に係るリソース(組織、人員、予算等)が全体に広く分散し、組織において定期的な人事異動等がなされる場合等では、必要なスキルやナレッジが当該組織内に十分に蓄積されないリスクもある。

また、複数存在する基準・標準の策定組織間で当該基準・標準の内容に関する調整が十分でない場合、本来すべての分野で求められるベースラインにあたる対策と分野等で固有の内容等がうまく峻別されず、事業者側で複数の基準・標準に対応が必要になる場合に不要な工数を要してしまう可能性もある。

そのため、現状各省庁で分散して実施されている標準策定業務の全部又は一部を IPA 等の十分な技術的能力及び専門的な知識経験を有する機関に一元化し、適用される標準群を体系化することで、サイバーセキュリティ関連の標準を策定・普及し、継続的に保守管理していく体制の確保を図ることが適切ではないかと考えられる。



図表 4-17 標準化機能等の強化を通じて実現したい姿

そのような変更を行うにあたり、情報処理の促進に関する法律に規定される IPA の業務(第 51 条)及び、サイバーセキュリティ基本法における基準の策定に関する権限(第 31 条第 1 項)について必要な改正を実施することで、サイバーセキュリティ関連の標準を策定・普及し、継続的に保守管理する上で IPA に必要な権限を付与する必要がある。

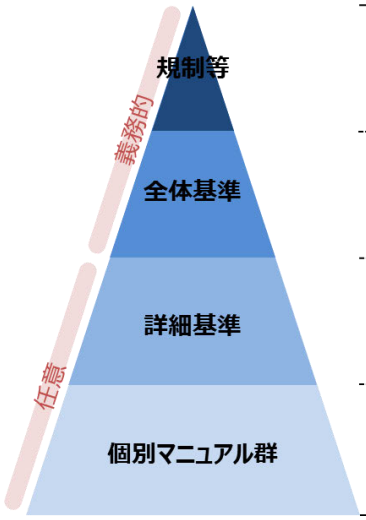
さらに、政府全体として今後策定すべき基準・標準について、方向性を議論し、合意する場を設ける必要がある。既存の会議体としては、サイバーセキュリティ対策推進会議(CISO 等連絡会議)も想定されるが、当該会議は政府機関におけるサイバーセキュリティ対策の推進が目的とされ、民間事業者も対象に含めたサイバーセキュリティ標準に係る検討がスコープとされていないため、新たに会議体を定義する等して、サイバーセキュリティ標準策定の方向性等に係る省庁間の協議体制を確立する必要があると考えられる。

<4.2.発行される文書体系等のあるべき姿>

策定される基準・標準を利用する事業者の立場からは、自身が必ず遵守しなければならない規制

及び求められる管理策、当該管理策を実装する際に参考となる技術的な情報や具体的なソリューション例が体系的に整理されていることが望ましい。それゆえ、セキュリティ標準の体系として、例えば、事業者に対策義務を課したりする「規制等」を頂点として、規制等の遵守に必要なハイレベルな要求事項を規定する「全体基準」、対策基準を全体としてより詳細に補完する「詳細基準」、対策基準や詳細基準に対応する対策の実装例等について個別具体的に解説する「個別マニュアル群」を整備していくことが望まれる。

上記で例を述べたような体系をより精緻に構想し、その中で具体的に基準・標準の策定等を進めていくにあたり、今後、日本においてこうした体系がどの程度整備されており、逆にどの程度整備が不十分な箇所があるのか等については、今後より具体的な分析が進められるべきである。



概要	具体例
特定の事業者に対して、一定のセキュリティ対策の実施を強制したり、推奨したりするもの	• サイバーセキュリティ基本法 14条 • 政府機関等のサイバーセキュリティ対策のための統一規範 • 各業法及び施行規則等
規制等の対象となっている事業者が遵守すべきハイレベルな要求事項を規定するもの	• 政府機関等のサイバーセキュリティ対策のための統一基準 • サイバーフィジカルセキュリティ対策フレームワーク(CPSF)
対策基準の遵守事項に対応した基本的な対策事項を例示したもの	• 政府機関等の対策基準策定のためのガイドライン • CPSFに係る分野別ガイドライン(ビル、スマートホーム、自動車、工場等)
対策基準や詳細基準に対応する対策の実装例等について個別具体的に解説したもの	• 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル • 政府機関等における情報システム運用継続計画ガイドライン

図表 4-18 セキュリティ標準体系の整備

③ まとめ

・ デジタル庁が公表した「デジタル社会の実現に向けた重点計画」の「ウ 標準の策定と活用の推進」において、「独立行政法人情報処理推進機構(IPA)について、米国国立標準技術研究所(NIST)も参考に、デジタル戦略等における基準・標準機関として位置づけ、これまでの情報処理推進に加え、国全体のデジタル社会形成の観点から、データ戦略に係る基準・標準の整備等を推進する」とされていることを背景に、標準策定機関が有する機能や整備されている基準・標準の体系等について、米 NIST をベンチマークとしつつ調査を実施し、結果を取りまとめた。

・ 調査結果及びそこから導かれる現状の問題と課題を踏まえ、今後「基準・標準の整備等を推進」するにあたって、その方向性の案として以下を提言した。

<u>組織・機能面のあるべき姿</u>

- ➢ 各省庁によるサイバーセキュリティ関連標準策定業務について、IPA 等の十分な技術的能力及び専門的な知識経験を有する機関への移管・一元化
- ➢ 上記を行うにあたり必要な法律その他の規則の改正
- ➢ 政府内でサイバーセキュリティ関連標準策定の方向性を議論するための会議体の設置・運営

<u>発行される文書体系等のあるべき姿</u>

- ➢ 事業者にとって利用しやすいサイバーセキュリティ関連の基準・標準に関する体系の構築
- ➢ 上記を構想・実装するにあたり必要な現状調査・分析の実施

4.3.3 国内外における官民連携センターの動向に係る調査

本項では、サイバーセキュリティを対象とした海外の官民連携センターの設置状況及びその内容についての情報収集を通じて、官民連携センターが持つ機能や特徴、機能を果たすための具体的な取組及びその取組の結果、民間企業に対するサポートの内容を理解することを目的として調査を実施した。

① 調査内容

調査対象は以下に示すように、欧米を中心に主要国から計 8 件を選定した。各調査項目は Web 等を活用し机上にて調査を行ったが、机上にて調査が難しい場合には、適宜有識者へヒアリングを実施して情報を補足した。

図表 4-19 調査対象一覧

No	地域	調査対象
1	米国	The National Cybersecurity Center of Excellence (NCCoE)
2		Mach37
3	欧州	The Cybersecurity Competence Centre
4	英国	Plexal Innovation Centre
5	オランダ	The European Network for Cyber Security
6	ロシア	Skolkovo Innovation Center
7	イスラエル	Cyberspark
8	韓国	国家サイバーセキュリティ協力センター

② 調査結果

米国や欧州等の地域ごとに取組を整理したサマリは以下のとおり。

- 米国では、NCCoE 及び Mach37 を対象として調査を行った。
  - NCCoE では、企業が共同で研究ができるようテスト施設を設置するとともに、テーマによって機密扱いのエリアをその施設に設け、出入りする人員に制限を設けた。また、政策的なテーマと結びついた研究テーマを設定することで、企業への参加のインセンティブを付与した。また、FFRDC(Federally Funded Research and Development Centers)の立場より、高度な知識を有する企業(MITRE)がセンターにおける民間企業の研究を支援することで、企業は専門的な知見を得つつ研究を行うことが可能となった。
  - Mach37 では、スタートアップ企業が投資家に対して研究成果に関するプレゼンテーションを行う場を設け、当該企業と投資家を結びつけるための仕組みを構築した点に特徴がみられた。
- EU・英国では、The Cybersecurity Competence Centre 及び Plexal Innovation Centre、The European Network for Cyber Security を対象として調査を行った。
  - The Cybersecurity Competence Centre では、かかるセンター単体ではなく欧州域内の各国の調整センターと協力して、強力なサイバーセキュリティ共同体を構築することを目的としている点に特徴がみられた。
  - Plexal Innovation Centre では、人材の調達や政府との密な連携が行いやすいよう、大学や政府との距離が近い場所にセンターを整備するとともに、かかる機関の専門人材から研究等に係るアドバイスを受けることができるようにしている点に特徴がみられた。
  - The European Network for Cyber Security では、民間企業において準備が難しい模擬環境を活用したプログラムを提供している。
- ロシアでは、Skolkovo Innovation Center を対象として調査を行った。行政的な権限が付与さ

れたスコルボ基金(当時大統領が評議会議長を務める)を設置し、研究を行う特別な管理区域を設定した上で、税制優遇措置や保険料率に関する優遇措置を実施した。特にこれらの施策は参加団体を募る目的で実施された。

- イスラエルでは、Cyberspark を対象として調査を行った。金銭面や人材面において特徴がみられた。金銭面では、政府補助金による広範なインセンティブや多額の部分的資金援助を用意し、例えば、現地のスタッフを採用する際、賃金に対して一定の割合で助成金を企業に対して支給した。また、人材面では、サイバー分野におけるプロジェクトマネージャーの採用支援やイスラエルに精通した専門のプロジェクトチームによる支援を実施している。
- 韓国では、国家サイバーセキュリティ協力センターを対象として調査を行った。合同分析室で分析したサイバー脅威情報は、公共機関を対象とした国家サイバー脅威インテリジェンス(NCTI)や民間企業を対象とした韓国サイバー脅威インテリジェンス (KCTI)を通じて、リアルタイムで共有している点に特徴がみられた。

分類	米国	EU・英国	ロシア
立地・設備面の特徴	• 航空関係であればシミュレーター、送電関係ではOT機器を設置し、企業が共同で研究ができるようテスト施設を設置。[NCCoE] • テーマ(例:安全保障)によってはclassifiedなエリアを設定。[NCCoE]	• 人材の調達や政府との密な連携が行いやすいよう、大学や政府との距離が近い場所に官民連携センターを配置。[Plexal Innovation Centre] • 大学の研究施設をテスト用設備として利用。[Plexal Innovation Centre]	• 行政的な権限が付与されたスコルボ基金(当時大統領が評議会議長を務める)を設けた上で研究を行う特別な管理区域を設定。 • 研究センター(テクノパーク)への人材提供の役割の機能を持つ大学(スコルテック)を設立。
内容面の特徴	• 政策的なテーマと結びついた研究開発テーマを設定。[NCCoE] • 共同研究で策定した文書を政府が公開し、お墨付きを与えることで、結果的にかかる文書が業界標準となる。[NCCoE]	• 民間企業において準備が難しい模擬環境を活用したプログラムを提供。[European Network for Cyber Security]	• 大企業による技術の調達及びスタートアップ企業による売上確保を目的として、大企業とスタートアップ企業のマッチングを実施。
金銭面の特徴	• スタートアップ企業が投資家に対して研究成果に関するプレゼンテーションを行う場を設け、スタートアップと投資家を結びつけるための仕組みを構築。[Mach37]	• 各社が無料で1対1の相談を実施できるようセンター側でファンドと提携。[Plexal Innovation Centre]	• 関係法令により、民間企業に対する税制優遇措置(法人税や固定資産税の減免)や保険料率(社会保険料の減免)に関する優遇措置を実施。
人材面の特徴	• FFRDC(Federally Funded Research and Development Centers)の立場より、高度な知識を有する企業(MITRE)がセンターにおける民間企業の研究を支援。[NCCoE]	• 大学研究機関やコンサルティング企業と協力することによって、かかる機関の専門人材から民間企業に対して、研究等にかかるアドバイスを提供。[Plexal Innovation Centre]	• メンターによる経営サポートに加えて複雑な行政手続き(知的財産登録や通関業務)を代行。 • 外国人労働者に対する労働許可の有効期間を延長。

図表 4-20 立地・設備/内容/金銭/人材面での比較(1/2)

分類	イスラエル	韓国
立地・設備面の特徴	• 人材の確保や各種手続き面でメリットがあるため、テック系の人材が多いテルアビブと官公庁が多いエルサレムに近いベエルシェバに設立。 • 施設は産業界の研究機関や大学と隣接した位置に設立。参画企業はかかる団体と日常的にアイディア交換が可能。	• IT系の企業が多くテック系の人材が多いテクノバレーに設立。テクノバレーは官公庁やテック系の大学が立地するソウルから20キロほどの距離に位置する。 • 合同分析室等を設立し、行政機関の職員とITベンダが合同で分析を実施。
内容面の特徴	• CyberSparkにR&Dセンターを設立する際に、サイバー分野での豊富な経験とイスラエルでの深い知識に基づいて、最適なチャネル(例:地元の起業家との合弁事業、多国籍企業との合弁事業の開始)を選別するための情報を提供。	• 合同分析室で分析したサイバー脅威情報は、公共機関を対象とした国家サイバー脅威インテリジェンス(NCTI)や民間企業を対象とした韓国サイバー脅威インテリジェンス (KCTI)を通じて、リアルタイムで共有。
金銭面の特徴	• 政府補助金による広範なインセンティブや多額の部分的資金援助を用意。例えば、現地のスタッフを採用する際、賃金に対して一定の割合で助成金を企業に対して支給。	• 請負事業者との契約条件等は管見の限り、確認できなかった。
人材面の特徴	• サイバー分野におけるプロジェクトマネージャーの採用支援やイスラエルに精通した専門のプロジェクトチームによる支援を実施。	• 常駐しているIT事業者の技術者を中心として、分析作業を実施。

図表 4-21 立地・設備/内容/金銭/人材面での比較 (2/2)

③ まとめ

これまでの調査結果に関連する情勢を補足し、「国内外における官民連携センターの動向」に関する我が国の現状と課題について以下のように取りまとめた。

[我が国の現状]

- 日本においては、一部強みを持つ技術(例:暗号)を除き、「シーズ」となるセキュリティ技術の研究が他の先進国と同等程度に進んでいるとは言えず、既に強みとなり得る技術を有していたとしても必ずしも国内で広く普及しているとは言えない状況にある。
- 結果として、事業者においては海外のセキュリティ技術を導入・運用する形態が主流となっており、コア技術に係るノウハウ・知見を蓄積することが難しい状況となっている。
- 開発した技術を事業者間で普及させるためには、顧客の視点や製品・サービスの品質について、ビジネス戦略上の判断や顧客目線を持ったアプローチが重要となる一方で、日本では、ビジネス戦略上の判断や顧客目線を持った民間事業者と大学や官公庁が連携できる場が豊富に整備されているとは言えない。
- 他方、欧米においては、例えば以下のような特徴をもつ物理的な産官学連携拠点を整備し、研究開発を行っている。日本においても産官学連携に係る物理的な拠点は一部整備されているものの、特にソフト面の支援等において欧米の取組と比較すると取組が十分とは言えない。
  - ハード面: 各団体が持ち込んだ設備を活用してテストを行うことが可能な施設を整備
  - ソフト面:専門人材・団体による研究開発の直接的な支援、参画団体間での速やかな情報共有・適切な進捗管理
- 産官学が連携を行う場として物理的な拠点を設けるメリット(例: 産官学間で速やかな情報共有や進捗管理が可能、各団体が持ち込んだ設備を活用してテスト可能)は大きく、日本においても参考とすべき点がある。

[上記を踏まえた我が国の課題]

- 民間企業によるノウハウの共有を通じた、事業化に直結する研究開発の推進
  (基礎的な研究による「シーズ」となる技術の創出そのものについては本課題では必ずしも対象としないものの、別途施策が講じられるべきと考える。)
  - 顧客にとって魅力的で品質の安定した製品・サービスにつながる技術の研究開発
  - 顧客に対して現実的な価格で提供可能な技術の研究開発

4.3.4 IT ベンダー(SIer やソフトウェア製造業者)向けの規制に係る調査

本項では、海外における IT ベンダーに対する規制の整理を通じて、IT ベンダーに対する具体的な要求や過失が発生した場合の行政機関による働きかけの手段の有無(及びその内容)等を理解することを目的として調査を実施した。

① 調査内容

以下のような特徴を持っている規制を調査対象とした。

- 政府から IT ベンダー等に対して直接的に課される/政府から重要インフラ事業者に課される規制が IT ベンダー等に間接的に課される
- サイバーセキュリティ対策の実施を求める規定が規制全体の一部又は全部を構成している

図表 4-22 調査対象一覧

No	地域	調査対象
1	米国	DFARS Clause252.204-7012
2		行政部門及び政府機関の長向けの覚書 (連邦政府機関が調達するソフトウェアに関してセキュリティ要件を定めるガイダンス)
3	欧州	NIS 指令
4		一般製品安全規則
5		EU 無線機器指令
6		民間航空機規則
7		自動車の型式承認規則
8		機械規則
9		製造物責任指令案
10		AI 規則案
11	英国	英国のサイバーレジリエンスを向上させるための法律案
12	中国	重要情報インフラセキュリティ保護条例
13	日本	PL 法

② 調査結果

適用対象や具体的な要求、IT ベンダーに対する具体的な働きかけの手段を整理したサマリは以下のとおり。

図表 4-23 調査結果(サマリ)

分類		調査結果
適用対象		● 対象外であったソフトウェア(単体)が対象に新たに含まれる可能性がある。なお、日本の PL 法ではハードウェアを伴わないソフトウェアは対象外となっている。 [製造物責任指令案]
具体的な要求	平常時の要求	● サイバーセキュリティの要素が改正にて新たに追加されている。しかし、要件レベルでの詳細化はなされておらず、他の標準を参照することとしている。 ● 上市前に自明でなかったとしても、脆弱性に対処するために必要なソフトウェア・セキュリティ・アップデートを提供しなかった場合、製造業者に責任が生じ得るとするルールが提案されている。成立した場合、非常に大きな影響があるため、注視が必要。[製造物責任指令案]
	異常時(インシデント等の発生時)の要求	● リスク管理義務や関連する要件を定めていることに加えて、重大なインシデントが発生した場合に、ベンダーに対して監督官庁等へ報告義務を課している場合がある。[NIS 指令] ● なお、EU サイバーレジリエンス法(注:本調査の対象外)においても、インシデントや脆弱性を発見した場合に、ベンダーに対して、例えば以下のような監督官庁やユーザーに対する報告義務(11 条)を課している。 ✓ 積極的に悪用された脆弱性を発見してから 24 時間以内に ENISA に通知する。 ✓ インシデントを認識してから 24 時間以内に ENISA に通知する。 ✓ インシデントの影響を緩和するための是正措置について遅滞なくユーザーに通知する。

分類			調査結果
働きかけの手段	金銭的な罰則を含まない働きかけ	事業者の監督について	● 訓練を受けた専門家による抜き打ち検査を含む、立入検査等の権限を監督官庁に認めているルールみられる。[NIS 指令] ● 注意喚起を含む、不遵守に対する状況の改善を要求する権限を監督省庁に認めているルールが見られる。[EU 無線機器指令、民間航空機規則]
		事業者に対する執行について	● 製品の市場投入又は市場での入手を禁止、一時停止、又は制限する措置を行う権限が監督官庁に認められている。[一般製品安全規則、EU 無線機器指令]
	金銭的な罰則を含む働きかけ		● 対象となる事業者の重要度によって、罰金額に差異を設けており、より重要度が高いと考えられる事業者における違反に対して、より多額の罰金を課している。[NIS 指令] ● また、対象となる事業者が同じであったとしても、遵守していない要件によって、罰金額に差を設けている。重要と考えられる対策要件を遵守しない事業者に対してより高額な罰金を課している。[AI 規則案] ● 規定内で金銭的な罰則を設けていなくとも、EU 加盟国によって設けられる可能性がある

また、今回の調査では、IT ベンダー向けの規制のうち製造物責任法に該当する規制において、各国で以下のような差異がみられた。

- 欧州における製造物責任指令案においては、対象に電子、デジタル製造ファイル、ソフトウェアが含まれている。また、製品が市場に投入された時点等に瑕疵が存在しなかった場合には免責されるが、安全性を維持するために必要なソフトウェアのアップデートやアップグレードが行われていない場合を除くとされている。
- 米国における第 3 次不法行為リステイトメントにおいては、製造物に組み込まれたソフトウェアは対象となる可能性がある。また、販売・供給時点において、製品が、製造上の欠陥を含むか、設計に欠陥が存在するか、又は指示・警告が不適切なために欠陥となる場合にはその製品は欠陥製品となる。
- 日本における製造物責任法においては、製造物に組み込まれたソフトウェアは対象となる可能性がある。また、その製造業者等が引き渡したときにおける科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかった場合、製造事業者の瑕疵となる可能性がある。
- 各国の製造物責任法において、欧州と米国/日本間で差異がみられた。欧州の製造物責任指令案は案の状態であることから今後変わり得るが、現時点でみられる主な差異は以下の 2 点と考えられる。
  - 米国と日本において対象外のソフトウェア(単体)が欧州では対象に含まれている。
  - 各国・地域ともに製品が市場で投入された時点で予期できなかった瑕疵や欠陥は免責されるが、欧州ではソフトウェアがアップデートされていない場合、免責されない。

比較項目	欧州	米国	日本	主な差異
対象法制度 (成立年度)	製造物責任指令案 (2022年9月案公表)	第3次不法行為リステイトメント(1998年公表)	製造物責任法 (1995年7月施行)	-
対象製品	• 製品とは、すべての動産を意味し、他の動産または不動物と一体化している場合も含む。 • 製品には、電子、デジタル製造ファイル、ソフトウェアが含まれる。	• 製品とは、使用または消費のために商業的に流通する有形動産を指す。 • 製造物に組み込まれたソフトウェアは対象となる可能性がある。	• 製造又は加工された動産 • 製造物に組み込まれたソフトウェアは対象となる可能性がある。	• 米国と日本において対象外のソフトウェア(単体)が欧州では対象に含まれている。 • 米国、日本では製造物に組み込まれる場合対象となる可能性。
免責事項	• 主に製品が市場に投入された時点等には存在しなかった場合には免責される。 • ただし、安全性を維持するために必要なソフトウェアのアップデートやアップグレードが行われていない場合は除く。	• 販売・供給時点において、製品が、製造上の欠陥を含むか、設計に欠陥が存在するか、または指示・警告が不適切なために欠陥となる場合にはその製品は欠陥製品となる。	• その製造業者等が引き渡したときにおける科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかった場合	• 各国・地域ともに製品が市場で投入された時点で予期できなかった瑕疵や欠陥は免責される。 • ただし、欧州ではソフトウェアがアップデートされていない場合、免責されない。

図表 4-24 各国の製造物責任法の比較

③ まとめ

これまでの調査結果に関連する情勢を補足し、「IT ベンダー(SIer やソフトウェア製造業者)向けの規制」に関する我が国の現状と課題について以下 A、B のように取りまとめた。

A. ソフトウェア製品のセキュリティの強化

[我が国の現状]
ソフトウェアを狙う脅威がますます高度化している中、防御に必要なユーザー及びベンダーの取組は十分になされているとは言えない

- IoT や DX の進展を通じて、これまで以上に様々な形で OSS 等を含むソフトウェアが利用されるようになっている一方、それらの脆弱性を悪用されるケースは後を絶たない。また、運用中のソフトウェアだけでなくソフトウェアサプライチェーンを狙った脅威が顕在化しつつあり、さらに高度化している。
- これらの対応には、ソフトウェアのユーザーによる対応だけでは不十分であり、開発等を行う製造業者による構想段階から運用段階に至るまでのライフサイクル全体の対応が必要となるが、現状それらが十分行われているとは言えない。

欧米では機器やソフトウェアの製造業者に対する取組が強まっており、我が国の対応が遅れた場合、将来的に海外へのビジネス展開に影響が出るおそれもある

- 欧米では、そのような関心から、機器やソフトウェアの製造業者に対する一定の対策の義務化(例：EU サイバーレジリエンス法)や責任の明確化(例：EU 製造物責任指令、米国家サイバーセキュリティ戦略)が盛んに議論されており、そのようなルールメイキングの動きが QUAD 等の国際的な枠組みを通じてグローバルで展開されつつある。
- 我が国でも「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」にて「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の策定や SBOM を活用した脆弱性管理の効率化に関する実証等の SBOM に係る取組の推進、「IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会」にて製品のセキュリティ向上に向けた制度構築(各種調達要件への組込みを含む)の議論が進められ

ているが、IoT 製品においては欧米の動向を踏まえた包括的な認証制度及びその展開に関する議論が行われている一方で、ソフトウェアのセキュリティ確保については、欧米でなされているような SBOM 以外の論点を含めた包括的な議論がなされているとは言えない。
- 我が国において欧米と相互運用性のあるルールを確立し、全体の水準を向上させる取組が行われない場合、欧米等の外国におけるルールへの対応やビジネス展開に支障が生じる可能性がある。

[上記を踏まえた我が国の課題]
1. 設計段階からの安全性の確保や継続的なセキュリティアップデートによる脆弱性対処等を通じた、高度化する脅威に対応できる安全なソフトウェアの提供促進
2. 上記の我が国の仕組みと欧米の制度との相互運用性確保による海外ビジネス展開におけるリスクの低減

B. IT サービスプロバイダーに課される責務

[我が国の現状]
昨今、外部 IT サービス経由での政府、重要インフラ等におけるインシデントが頻発しており、セキュリティマネジメントにおける委託先管理等の重要性が改めて認識されている
- 国内外で外部サービスの脆弱性等に起因するシステム侵害が多数報告されている。
- EU 及び英国では、CSP や MSP を重要インフラに指定する等し、一定のセキュリティマネジメントを最低限の実施事項として求めているところ、我が国ではそのような取組に端緒はついたものの、依然限定的である。
- EU 及び英国では、CSP や MSP を重要インフラに指定し、一定のセキュリティマネジメントを最低限の実施事項として求めている。
- 我が国においても経済安全保障推進法(基幹インフラ役務の安定的な提供の確保に関する制度)の制定等を推進してきたが、重要インフラ事業者等には CSP や MSP 等が含まれていない。
- 政府向けに ISMAP が制度化されているものの、重要インフラ事業者等にて同様の制度が十分活用されているわけではない。

[上記を踏まえた我が国の課題]
- マネージドサービスプロバイダー(MSP)やクラウドサービスプロバイダー(CSP)等のセキュリティ水準向上を通じた、より安全で信頼できる政府、重要インフラ等システムの実現。

4.3.5 IT ベンダーとユーザー間の紛争に関する判例の収集

本項では、IT ベンダーとユーザー間で実際に起きた紛争の判例を整理・分析することを通じて、システム開発や運用における両者の責任分界や、その明確化がおろそかになることによる弊害及び予め両者で契約等の中で講じておくべき対策を理解することを目的として調査を実施した。

① 調査内容

本項では、国内外の判例の分析に加え、個々の判例の性質に依存しない一般的な事項について調査した上で、IT ベンダーとユーザー間で責任分界が曖昧であった点が発生の一因とされているセキュリティインシデントに関する調査報告書等における現状の課題及び今後の改善施策等についても調査を行った。

図表 4-25 調査項目一覧

No	分類	調査項目	整理の観点等
1-1	一般的な事項	IT ベンダーとユーザー間での責任分界に係る法、ガイドライン等の規定	● 責任分界に係る既存規定の概要(例：民法上の債務不履行責任、不法行為責任、PL 法における製造物責任、等) ● ベンダーの債務の内容としてのセキュリティ対策
1-2		IT ベンダー側の過失が認められる/認められない場合とその根拠	● 契約書・仕様書に明記した対策の不実装 ● 契約書・仕様書に明記のない対策の不実装 ● 契約締結時点で脅威が既知の場合 ● 契約締結時点で脅威が未知の場合 ● IT ベンダーによる脆弱性の修補責任
1-3		脆弱性の原因が SIer 等の直接の委託先以外の主体(OSS 又は OSS 以外のサードパーティ製品開発ベンダー)にあった場合のベンダー責任のあり方	● 脆弱性の原因が OSS にあった場合の責任のあり方 ● 脆弱性の原因が OSS 以外のサードパーティ製品にあった場合の責任のあり方
1-4		セキュリティ対策不足が重過失となり得る場合の条件等	● IT ベンダー側の重過失が問われ得る際の判断条件 ● 代表的な判例
2-1	判例ごとの検討事項	事案の概要	● 関係する事業者のプロフィール ● 生じた被害及び係争上の争点
2-2		IT ベンダー側の過失が認められた/認められなかった具体例とその根拠	● IT ベンダーの過失として認定された事項 ● ユーザーの過失として認定された事項 ● 上記判断の具体的根拠
2-3		セキュリティ対策不足が重過失となった具体例とその根拠	● IT ベンダーの重過失とされた具体的事項 ● 上記判断の具体的根拠
2-4		賠償の範囲	● 事故対応・調査費用・お詫び関連 ● システム改修 ● 逸失利益、信用低下
3-1	対応事例	発注者及び IT ベンダー間の責任分界に係る示唆	● 報告書等で指摘された論点

② 調査結果

● 一般的な事項

<IT ベンダーとユーザー間での責任分界に係る法、ガイドライン等の規定>

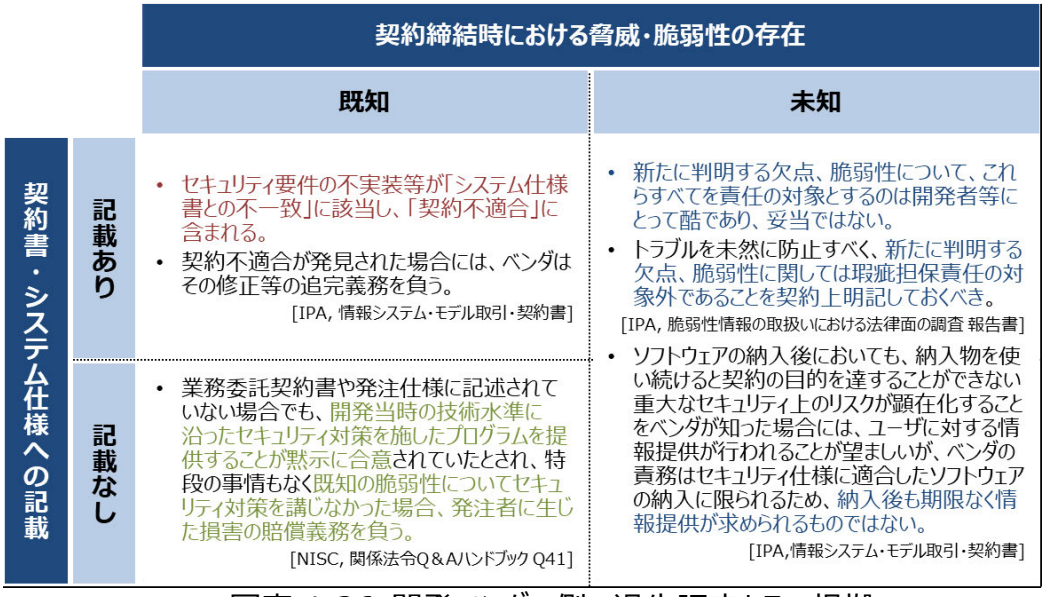
IT ベンダーとユーザー間の責任分界等に関しては、民法(第 415 条、第 562 条、第 644 条、第 709 条等)及び製造物責任法(第 3 条)において関連する規定が設けられているが、具体的な内容は双方で締結する契約(主に、請負又は準委任)に依拠することとなる。

対象の契約が請負契約か準委任契約かによって問題となり得る点は異なるが、例えば、受託業務の完成義務を負う請負契約においてユーザーに完成されたものとして引き渡された成果物が契約の内容に

適合しているかどうか、準委任契約において事務処理に関して善管注意義務が果たされているかどうかがポイントになる。

＜IT ベンダー側の過失が認められる/認められない場合とその根拠＞

セキュリティインシデント等が顕在化した後で、悪用された脆弱性に関して IT ベンダー側の契約不適合責任を検討するにあたり、①契約書やシステム仕様書に記載があるかどうか、②契約締結時に当該脅威・脆弱性の存在が認知されていたかが論点となり得る[31]。



図表 4-26 開発ベンダー側の過失認定とその根拠

システム等の納入後にセキュリティインシデントが起きた際、対策を施すことが仕様書等に明示されていたにもかかわらず対応していなかった場合に開発ベンダーが契約不適合責任及びその修正等の追完義務を負うことになる。他方で、契約締結当時あるいは納品時において未知の脅威が将来発生して攻撃を受けたというような場合に開発契約上の責任を負わせることは「開発者等にとって酷であり、妥当ではない」[32] とされているが、新たに判明する欠点、脆弱性に関しては瑕疵担保責任、契約不適合責任の対象外である旨を契約に明記すべきと考えられる。

問題となるのは、契約締結当時で既知の脅威に十分な対応を取っておらず、かつ仕様書にも記載がなかった場合のベンダー責任である。過去の判例(例：東京地判平 26.1.23 判時 2221-71)には、業務委託契約書や発注仕様に記述されていない場合でも、開発当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示に合意されていたとされ、特段の事情もなく既知の脆弱性についてセキュリティ対策を講じなかった場合、発注者に生じた損害の賠償義務を負うとされているものがある。ソフトウェアが提供時において通常備えられている「セキュリティ」を欠いている場合、開発ベンダーによる脆弱性の修補責任が生じ得る。

＜脆弱性の原因が SIer 等の直接の委託先以外の主体にあった場合のベンダー責任のあり方＞

本件については、「～情報システム・モデル取引・契約書～(受託開発(一部企画を含む)、保守運用)〈第二版〉」[33] に具体的な記載がなされている。

- 第三者ソフトウェア(商用パッケージソフト等)及び FOSS(Free and Open Source Software)の利用については、①当該ソフトウェアそのものの契約不適合に起因するリスク及び②システムとの組み合わせに起因するリスクが存在する。
- ベンダーが第三者ソフトウェア及び FOSS の契約不適合の有無を管理することは非常に困難である場合が多いが、取引のパターンとして、ユーザーが特定の製品を予め指定する場合、価格・機

能の条件を指定しその中からベンダーが選定する場合、ベンダーが自ら選定する場合があり、それぞれの場合でベンダーの責任の範囲が異なってくる。

- 第三者ソフトウェア及び FOSS 自体の契約不適合に起因するリスクは、当該第三者とユーザーとの契約で対処すべき問題である。但し、商用パッケージについて、ベンダーがサブライセンサーとなる権利を得て、ベンダー自身の商品ラインナップのひとつとしてユーザーにサブライセンスする場合は、ベンダーは当該ソフトウェアの契約不適合についても一定の範囲で責任を負うべき場合がある。
- 他方、ユーザーに第三者ソフトウェア及び FOSS の選定の知見等がなく、ベンダーがユーザーに導入の可否について判断機会及び判断を行うために、合理的に必要とされる情報を与えることなく自主的判断で選択した場合については、ベンダーも一定の責任を負う(特に、ベンダーは当該ソフトの選定(利用方法、機能上・利用上の制限、保証期間等)について、専門家としての情報提供義務を契約上の責任として負う。)。

＜セキュリティ対策不足が重過失となり得る場合の条件等＞

攻撃への対策を講じなかった場合の結果が容易に予見可能であり、対策そのものに多大な労力や費用がかかるものではないような場合、対策を怠ったベンダーの債務不履行責任は、重大な過失(重過失)があったものとされることがある。

結果の予見が容易に可能かという点については、悪用された脆弱性が未知のものであるか、既知のものである場合に業界の間で十分に認知されているものか等が考慮される。また、結果の回避が容易であるかという点については、効果のある対策が業界の間で十分に認知されており、その実施に多大な労力・時間・費用がかかるか等が考慮される。

重過失が認められる場合、重い賠償義務を負ったり、システム開発契約において合意していた損害賠償額の上限に関する規定等の免責条項の有効性について制限を受けたりする場合がある。

- 判例ごとの検討事項

セキュリティインシデント発生による損害に係るユーザー企業と IT ベンダーとの責任分界について争ったものとして、以下に示す国内判例 5 件、国外(米国)判例 3 件を調査対象とした。

国内判例

- 東京地判平 26.1.23 判時 2221 号 71 頁
- 東京地判平 30.10.26 判例集未登載
- 東京地判平 30.3.29(平 28 ワ 13202)
- 東京地判平 31.1.25(平 29 ワ 22870)
- 東京地判令元.12.20(平 29 ワ 6203)

海外判例(米国)

- Traveler`s Casual and surety Company of America v. Ignition Studios
- Solarwinds Corp
- Blackbaud

- 対応事例

近年発生したセキュリティインシデントに関する事故調査報告書等を参照し、特にユーザー事業者と IT ベンダー等の責任分界が問題とされたケースの有無や提案された対応策等について調査を行った。

特に医療業界で発生したインシデント(例：つるぎ町立半田病院、大阪急性期・総合医療センター)において、IT ベンダーの役割(又は医療機関との責任分界)を問い、対応の強化を求めるような論調がみられた。

③ まとめ

これまでの調査結果に関連する情勢を補足し、「IT ベンダー(受託開発ベンダー、運用ベンダー等)とユーザー間の紛争」に関する我が国の現状と課題について以下のように取りまとめた。

[我が国の現状]

受託開発ベンダー等と発注者との契約でもセキュリティに関する責任分界が明確に規定されず、双方が必要な対応を怠った結果、インシデントや訴訟提起が多数生じている

- これまでユーザーと受託開発ベンダー等との間においては、双方の責任分界を規定する上で契約が重要な位置づけであるところ、昨今の情勢変化を踏まえ、政府でも「情報システム・モデル取引・契約書（第二版）」における「セキュリティ仕様」に関する条項の見直し、「クラウドを利用したシステム運用に関するガイダンス」の策定等の取組を進めてきた。
- 他方、上記のような取組が進められているにもかかわらず、受託開発ベンダー・運用ベンダーと発注者との間で締結される契約等でサイバーセキュリティに関する責任分界が曖昧な状況が引き続き生じており、複数のインシデント調査報告書にて主要な事故原因とされ、改善が求められている。
- 上記と同様の理由で受託開発ベンダー・運用ベンダーと発注者との間で、特にベンダーが担うべき責任を問う形で多数の訴訟が提起されている。

[上記を踏まえた我が国の課題]

- 受託開発ベンダー・運用ベンダーと発注者との責任分界の明確化を通じた全体的なセキュリティ水準の向上

<参考文献>

1 貴省,” 第 8 回『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”, (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/008.html)

2 貴省,” 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン” (https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html)

3 貴省,” 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン【別冊：スマート化を進める上でのポイント】” 今後公開予定

4 IEC 62443 の以下の文書を参照
- IEC 62443-2-1:2010 (https://webstore.iec.ch/publication/7030)
- IEC 62443-3-3:2013 (https://webstore.iec.ch/publication/7033)

5 NIST SP 800-82 Rev.3 (https://csrc.nist.gov/pubs/sp/800/82/r3/final)

6 貴省,” 協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ Version 1.1” (https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework_1_1.pdf)

7 Presidential Memorandum on United States Government-Supported Research and Development National Security Policy (https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/)

8 NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, “GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT”, 2022 年 1 月, (https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf)

9 Subcommittee on Research Security National Science and Technology Council Office of Science and Technology Policy, ”DRAFT Research Security Programs Standard Requirement”, 2023 年 2 月, (https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf) (https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_3.pdf)

10 “Enhancing security through Research and Innovation”, 2021 年 12 月 15 日, (https://home-affairs.ec.europa.eu/news/enhancing-security-through-research-and-innovation-2021-12-15_en)

11 Trusted Research, (https://www.npsa.gov.uk/trusted-research)

12 Trusted Research Guidance for Academia, (https://www.npsa.gov.uk/trusted-research-academia)

13 Universities UK, “Managing risks in Internationalisation: Security related issues”, 2022 年 12 月, (https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation)

14 UK Research and Innovation, “UK Research and Innovation Trusted Research and Innovation Principles”, 2021 年 8 月, (https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf)

15 三菱 UFJ リサーチ&コンサルティング, “平成 2 9 年度産業経済研究委託事業 海外におけるデータ保護制度に関する調査研究 調査報告書”, 2017 年 11 月, (https://www.meti.go.jp/policy/economy/chizai/chiteki/keizaisanngyou29.pdf)

16 山根崇邦, “アメリカにおける営業秘密の保護(3・完)： 連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較”, 2021 年 4 月,

(https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/81694/1/59_02-Yamane.pdf)
17 U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, “2022 Annual Report to Congress”, (https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf)
18 貴省産業技術環境局基準認証ユニット“標準化実務入門(標準化教材)” “2.規格、標準とは”, 2016 年 1 月 7 日改定 (https://www.meti.go.jp/policy/economy/hyojun-kijun/katsuyo/jitsumu-nyumon/pdf/2015text_zenbun.pdf)
19 “ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection”, (https://www.iso.org/committee/45306.html)
20 参考文献 1 “第 3 節 JTC1”参照
21 情報規格調査会(ITSCJ)とは、「国際標準化機構(ISO)、国際電気標準会議(IEC)などの情報技術に関するデジュール標準である国際規格の審議及びこれに関する調査研究、国内規格の審議などを行い、情報処理及び電子計算機に関する標準化に寄与することを目的としている」国内の審議団体である。
22 一般社団法人 情報処理学会 情報規格調査会, “概要”, (https://itscj.ipsj.or.jp/itscj/about.html)
23 “IWA 39:2022 Gap analysis for standardization on sustainable and human-centred societies enabled with cyber physical systems”, (https://www.iso.org/standard/81618.html)
24 “IoT 製品・システムを安全に実装するための国際規格が発行されました”,2021 年 6 月 21 日 (https://www.meti.go.jp/press/2021/06/20210621004/20210621004.html)
25 ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines, (https://www.iso.org/standard/44373.html)
26 IPA, “中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 ―”, (https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf)
27 株式会社日立製作所, ”令和 4 年度サプライチェーン・サイバーセキュリティ対策促進事業(サイバー・フィジカル・セキュリティ対策フレームワークの利活用に関する調査) 調査報告書”, 2023 年 3 月, (https://www.meti.go.jp/meti_lib/report/2022FY/000524.pdf)
28 IPA, “情報セキュリティ向上のための米国の取組み”, 2007 年 8 月, (https://www.ipa.go.jp/security/reports/oversea/nist/fisma.html)
29 IPA, “【概要説明】 NIST 及び NIST 発行の情報セキュリティ関連文書”, 2005 年 8 月, (https://www.ipa.go.jp/security/reports/oversea/nist/nist_publications.html)
30 “NIST CYBERSECURITY & PRIVACY PROGRAM”, 2022 年 7 月, (https://www.nist.gov/system/files/documents/2022/07/21/Extended%20Cybersecurity%20Vitals%20Fact%20Sheet.pdf)
31 伊藤雅浩, “情報ネットワーク法学会研究大会 2019@関西大学”, 2019 年 11 月, (https://masahiroito.hatenablog.com/entry/2019/11/04/212356)
32 IPA, “情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書 改訂版”, 2019 年 3 月, (https://www.ipa.go.jp/archive/files/000072543.pdf)
33 情報システム・モデル取引・契約書(第二版), (https://www.ipa.go.jp/digital/model/model20201222.html)

<商標又は登録商標>
本調査事業では、各商品や各サービスを対象として各種調査や各種実証を推進したが、本調査報告書に記載されている各商品や各サービスは各社の商標又は登録商標である点にご留意いただきたい。

（様式２）

二次利用未承諾リスト

報告書の題名 令和5年度産業サイバーセキュリティ強靭化事業（サイバー・フィジカル・セキュリティ対策フレームワークの利活用に関する調査）調査報告書

委託事業名 株式会社日立製作所

受注事業者名 株式会社日立コンサルティング

頁	図表番号	タイトル
36	図表3 - 9	2024年2月時点で策定又は改定が予定されるISMSファミリー規格
37	図表3-10	現状版にて新たに追加されている管理策
40	図表3-12	ベースライン要求事項(本規格)の位置づけ
41	図表3-13	ISO/IEC 27402:2023の要求事項

別紙１

協調的なデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ

Version 1.1

経済産業省　商務情報政策局　サイバーセキュリティ課

令和 6 年 2 月 28 日

変更履歴

Version	変更年月日	変更箇所	変更内容
1.0	2022 年 4 月 8 日	-	新規作成
1.1	2024 年 2 月 28 日	添付 A	添付 A-5（ATM・金融端末の生産ラインにおける板金加工データの収集・加工）を追加

目次

1. 新たなデータマネジメントの在り方 4
1-1 CPSF における第 3 層（サイバー空間におけるつながり） 4
1-1-1 CPSF 概論 4
1-1-2 第 3 層の位置づけ 4
1-2 データの信頼性確保：データマネジメントの考え方の確立 5
1-3 本フレームワークの目的 7
1-4 本フレームワークの想定読者 9
2. 本フレームワークにおけるデータマネジメントのモデル 10
2-1 概要編 10
2-1-1 データマネジメントのモデル化の概要 10
2-1-2 リスク分析手順 12
2-2 詳細編 13
2-2-1 モデル化（「イベント」） 13
2-2-2 モデル化（「場」） 19
2-2-3 モデル化（「属性」） 20
3. 活用方法 22
3-1 サプライチェーンを構成するステークホルダー間での活用 22
3-2 ルール間のギャップの分析 24
添付 A ユースケース 25
A-1 POS データの分析 25
A-2 高齢者生活支援事業の提供 37
A-3 IaaS、PaaS、SaaS 等を利用してサービスを提供する例 50
A-4 国内で提供される IT サービスに関して、海外で開発や運用等を実施する例 64
A-5 ATM・金融端末の生産ラインにおける板金加工データの収集・加工 75
添付 B イベントごとのリスクの洗い出しのイメージ 91
B-1 イベントごとの典型的なリスクの記載方法等 91
B-2 イベントごとのリスクの洗い出しのイメージ 94

1. 新たなデータマネジメントの在り方

1-1 CPSFにおける第3層（サイバー空間におけるつながり）

1-1-1 CPSF概論

サイバー空間とフィジカル空間が高度に融合した産業社会においては、製品・サービスという価値を生み出す工程（サプライチェーン）が従来の定型的・直線的なものから、多様なつながりによる非定型的なものへと変化している。このような新たな価値創造過程（バリュークリエイションプロセス）のセキュリティ上の課題とその対策を整理することによって、新たな産業社会のセキュリティを確保していく考え方をまとめたものが、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）である。CPSF では、「バリュークリエイションプロセスのセキュリティ確保にあたっては、従来のサプライチェーンで想定されているマネジメントの信頼できる企業間のつながりによって付加価値が創造される領域を越えて、フィジカル空間の情報が IoT によってデジタル化され、データとしてサイバー空間に取り込まれ、そうしたデータがサイバー空間で自由に流通することで、多様なデータが新たなデータを生み出して付加価値を創出することや、新たに創出されたデータが IoT によってフィジカル空間にフィードバックされることで新たな製品やサービスを創出するという、新たな付加価値を創造するための一連の新たな活動を視野に入れる必要がある」とし、企業間のつながりに信頼性の基点を置く第 1 層、フィジカル空間とサイバー空間のつながりに信頼性の基点を置く第 2 層、サイバー空間におけるつながりに信頼性の基点を置く第 3 層という異なる 3 つの信頼性の基点を設定し、これらの基点を中心に経済社会全体のセキュリティ上の課題の洗い出しとその対策をまとめている。

1-1-2 第3層の位置づけ

あらゆるモノがネットワークにつながっていくことでサイバー空間が急激に拡大し、それらの間で行き交うデジタル化されたデータが爆発的に増大している。サイバー空間の中では、データが自由に流通し、物理的な距離に縛られることなくデータを入手して編集・加工したり、これまでは処理が容易ではなかった大量のデータを様々な切り口から分析してインテリジェンスを抽出したりするような、新たな価値を創造する活動が加速度的に広がっている。ネットワーク越しに提供される新たなサービスは、サーバなどの物理的な情報システムの上で展開されているが、その多くにおいてサービスを生み出す活動は物理上の特性ではなく論理によって実現され[1]、付

[1] 以前は特定のハードウェアでしか実現できなかった機能が、ミドルウェアの発達等により、ハードウェアの特性に縛られずにソフトウェアによって実現されるようになっている。

加価値を創造しているのは物理特性に依存しないデータである。データは基本的にシステムや組織に対して中立性を持つものであり、それが求められる規範等に則って適切に扱われることによって、自由に流通・活用される。こうした活動、サイバー空間におけるつながりが展開される場が第3層であり、ここでは、データがサイバー空間で付加価値を創出する基礎となる。

第3層におけるデータの生成・移転・加工等のライフサイクルの各工程には、第1層においてマネジメントの信頼性が確認された企業（組織）のみが関わる訳ではない。データのライフサイクルには様々な主体が関与し、関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、そのデータが関わったバリュークリエイションもまた価値をもたらすことはなく、有害な結果をもたらすことにもつながりかねない。例えば、サイバー空間から発信されたIoTシステムへの動作指令が誤った内容であるならば、第2層における“転写”する機能の信頼性を確保することに成功していたとしても、IoTシステムはサイバー空間から届いた誤った指令を“正しく”転写して忠実に動作することで物理的な損害を発生させてしまうかもしれない。

つまり、第3層においては、データそのものが正しいことが最も重要な前提であり[2]、付加価値の創出（バリュークリエイション）の基礎となるデータが、バリュークリエイションプロセスの信頼性を確保するための信頼性の基点でなければならない。

1-2 データの信頼性確保：データマネジメントの考え方の確立

CPSFは、サイバー空間とフィジカル空間が高度に融合した産業社会において動的に構成されるサプライチェーンをバリュークリエイションプロセスとして捉え、産業社会に対して3つの層を設定してこれに合わせて信頼性の基点を導入することで、動的かつ複雑な姿を見せるバリュークリエイションプロセスにおけるリスクを包括的に洗い出し、対応策を実施できるようにするためのフレームワークである。その中の第3層の位置づけは既に述べたとおりだが、データ自体に信頼性の基点を置いて包括的なセキュリティ対策を実施するためには、データのライフサイクル全体にわたってリスクを洗い出し、セキュリティ確保のための様々な措置を実施することが必要となる。

ここで留意すべきことは、第3層では信頼性の基点をデータに置いている一方、データのライ

---

[2] セキュリティの確保に向けては、データの機密性、完全性及び可用性を維持することが必要である。ここでは、そのうち、第三層におけるデータそのものが正しいこと（完全性）の重要性を特に強調して説明しているものであり、対策等を検討するにあたっては、機密性・完全性についても考慮する必要がある。

フサイクルは第3層の中に閉じるものではないということである。

CPSFでは、「第3層においては、サイバー空間のデータ及び、その加工・分析・保管という諸機能の信頼性を確保する」ことが必要であるとするとともに、「フィジカル空間からサイバー空間に転写されたデータは第2層の転写機能の信頼性を確保することによってデータの信頼性が確保されるが、サイバー空間では様々なデータが生成・編集・加工され、自由に流通し、かつ、こうした過程はマネジメントの信頼性が確認された企業（組織）によってのみ扱われるわけではない」とし、データが生成される場所については第3層ではなく第2層に属する場合があることを明確にし、第3層と第2層とを組み合わせることでデータ生成における信頼性を確保する考え方を示している。

つまり、データの信頼性を確保するためには、CPSFの第3層の考え方を基礎とした上で、そのコンセプトの適用範囲を拡張し、データを軸として、データの生成・取得から廃棄に至るライフサイクル全体を視野に入れた対応、つまり、データマネジメントの在り方に関する枠組みを設定することが必要になる。この枠組みでは、データのライフサイクルの各工程において発生する様々な形の“関与”をデータマネジメントとして捉え、これをモデル化することでデータに関わるリスクの洗い出しと対応策の整理を行うことになる。

この考え方で整理を進めていくにあたって、以下の3つの視点を押さえておく必要がある。

①データマネジメントについて確立した定義は存在しない。
②データの信頼性の観点からデータマネジメントを捉える場合、データに関与する主体の視点からではなく、データを軸に置く必要があり、データがライフサイクルの各工程においてどのような関与を受けるかという視点で整理すべきある。
③データマネジメントをデータのライフサイクルの各工程おいて発生する様々な関与の総体を意味するものと整理した場合、関与する主体は同一・単一の主体に限られるものではないことから、データマネジメントは複数の主体による協同的活動（Collective Action）になることを排除しない。

①の視点から導かれることは、データマネジメントという言葉に対する各人の理解は現時点では一致しているわけではないということである。

本フレームワークは、他の機関等において整理された既にあるデータマネジメントの定義を持ち込むのではなく、CPSFを基礎としてデータを軸においてセキュリティ対策を検討するために必要なデータマネジメントの考え方を示すものである。ここで示すデータマネジメントの考え

方を改めて共有することにより、これまで各組織や各国においてデータ管理に関する議論がなかなか噛み合わず、それぞれが整備したデータ管理に関するルール等の間の調整を図ることが難しかったところ、共通の尺度として本フレームワークを活用してデータマネジメントに関する共通の理解を得ることで、異なるデータ管理のルール等の間について、ルール間を跨いでデータが流通した場合でもデータのセキュリティが同じように確保されるために必要な調整を図ることが可能となる。

②の視点を強調しているのは、様々な団体等がこれまでに提示してきたデータマネジメントの考え方は「データという資産を組織が如何に生かすか」という視点で整理され、データのライフサイクル全般を捉えたものではないため、データの信頼性を包括的に確保するためのフレームとはなっていないことを明らかにする必要があるためである。

データの信頼性は、データが基本的に組織等からの中立性を持っていることを踏まえ、データを軸に置き、当該データの信頼性を確保するために求められる措置を整理して実施することで確保されるのであり、それに関与する主体の立場から整理された当該主体が実施すべき必要な措置は、データに対して本来求められる措置全体に対する部分的な措置でしかないことを改めて明確にする必要がある。

③の視点は、②の視点によってデータマネジメントが単一の主体によるマネジメントであるという考え方から解放されたことで、ライフサイクルの工程において関与する主体は一つのモノに限定されるのではなく、複数の主体が同時に関与し、かつ、関与する際に求められる措置も各主体によって異なることがあるということを明らかにするものである。この③の視点を導入することで、サービスを構成するシステムが複数のサービサーによって実現されるクラウドサービス（例えば、ユーザー企業A社が利用するB社のSaaSはC社のPaaSの上で展開し、C社のPaaSはD社のIaaSで展開されるようなケース）におけるデータの扱いを考える場合などにおいて各主体に求められることや、データがシステム等に対して基本的に中立性を持っていることを踏まえたゼロトラストの概念に基づくアーキテクチャを明確に整理することができることになる。

以上の3つの視点は、本フレームワークを理解するための基礎条件となるものであり、改めて、その重要性をここで強調しておきたい。

1-3 本フレームワークの目的

本フレームワークは、主体間を転々流通するデータの信頼性を確保することでバリュークリエイションプロセスが付加価値を生み出していくために、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そ

のセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とすることを目的としている。データのライフサイクルの各工程において直面するリスクは、単一の主体が実施可能な措置によって対応できるものに限定されるわけではないため、データのライフサイクルの工程に関与する主体がそれぞれ実施すべき措置を他の主体と協調して取り組むことによってデータのセキュリティを確保することが必要になる。なお、協調的な取組の一環として各主体においてそれぞれ行うべきとされた具体的な措置は、各主体のガバナンスのもとで適切に実施される必要がある。

したがって、本フレームワークは、単独の組織のマネジメントの在り方について整理したものではなく、データを軸においてそのリスクに対処するという観点から、データに関与する主体＝ステークホルダーが協調して、組織のガバナンスを含めた必要な措置を実施することを促進する枠組みとなる。

データのセキュリティを確保するために必要な措置自体については、これまでに公表されてきた情報セキュリティに関する様々な国際標準等が「データマネジメント知識体系（DMBOK）」として既にまとめられていることから、本フレームワークを使って洗い出されたリスクに対する措置はDMBOK等の既存文書を参照して具体的な措置内容を選択することが可能である。

また、本フレームワークは、データが置かれた環境におけるリスクを明らかにしてセキュリティを確保するという役割に加え、データの流通を促進するための環境を実現するために必要な条件を明確化する役割も果たすことが可能である。

本フレームワークは、データの置かれている状態を可視化することでリスクを洗い出し、リスクに対処するために関与する主体それぞれに求められる適切な措置を明確化する（as is の対策）が、この考え方を拡張し、データを異なった環境に遷移させようとする際にデータの状態がどのような条件を満たせば異なる環境でもセキュリティが確保され、問題なく遷移させることが可能となるかを明らかにする（to be の対策）ことができる。例えば、データ交換プラットフォームとなっている異なるシステムの間で、特別な措置を必要とせずに自由にデータ交換を行うことができる環境を実現するためには、システム間の機能連携のためのAPIを設定することに加え、両システムで共有するデータ交換のためのプロトコルを整備することが必要になるが、本フレームワークを活用することで、プロトコルの設計が容易になる。

また、本フレームワークの考え方が広く共有され、一般的な活動として定着すれば、影響力に違いのあるシステム間において強い立場にあるシステムがデータ交換に必要なプロトコルをブラックボックスにすることで当該システムに他のシステムを依存させようとする（「バンドルす

る」）ことを難しくさせ、オープン化された環境でデータ連携やシステムの組み合わせの自由を確保し、より効率的なデータ活用モデルを実現することが可能となる。

更に視野を広げると、データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしても活用することが可能である。

各組織が整備したデータ管理に関わる制度は、プライバシー保護や情報の機微性保持等のそれぞれの目的からデータ管理に関する条件や措置を設定しているが、制度間で自動的に調整する機能がないことから、制度ごとに条件等が異なることで事実上データが一つの制度の中に“囲い込まれる”ことになり、データの流通が妨げられていることが少なくない。国際的にも、個人情報保護を目的としながらも、同じ目的であるにも関わらず各国で制度的な条件や措置が異なり、事実上国境を跨いでデータを流通させることが困難になってしまっているようなケースが見られる[3]。

こうした制度で要求されているデータ管理に関する条件や措置は、同じ目的であるならばデータ管理についての条件や措置も同じ内容であるべきだが、実際には、データの状態に着目するのではなく、これに関わる主体を管理することを考慮して設定されたと思われることが少なくなく、このことが制度間のギャップをもたらしている。

本フレームワークは、データを軸にして、客体であるデータの状態を可視化し、データの状態が満たすべき条件や実施されている措置を明らかにするものであり、関与する主体の在り方などを過度に考慮することなく、データに対して本来求められる条件等を歪めることなく整理することが可能であることから、本フレームワークを活用して各国の制度間に存在するギャップ分析を行い、分析結果をモデル化し、データ流通を可能とするために必要なギャップの調整措置を明らかにすることが可能となる。

1-4 本フレームワークの想定読者

上記のとおり、本フレームワークは、データのセキュリティ確保のためのデータマネジメントを可能とする機能に加え、データを流通させるための環境を実現するための、データ遷移をする地点間のギャップの的確な分析を可能とする機能を持つものであり、データを管理する現場レベルでの活用から、データ管理に関する仕組みや制度設計、更に国際的なデータ共有の仕組み作

[3] 一方で、GDPR における「データポータビリティ権」など、制度がデータの囲い込みの手段ではなく、データの可搬性（ポータビリティ）を確保する役割を果たす場合もある。

りにまで活用することができるものである。

したがって、本フレームワークは以下のような者に活用してもらうことが期待される。

- 真正であり、適切なセキュリティを確保することが求められるデータを扱う者、特に、データを利活用して価値を創造するバリュークリエイションプロセスに参加する者
- データ利活用に関するサービスを提供する者
- データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者
- データに求められる条件として適切なトラストを保証することが必要な場合の適切な水準のトラストサービスを提供しようとする者
- データセキュリティに関わるガイドライン等のルール設定に関わる者

2. 本フレームワークにおけるデータマネジメントのモデル

2-1 概要編

2-1-1 データマネジメントのモデル化の概要

データは、目的を持って生成・取得され、それが転々流通し、その属性を変えながら様々な形で活用されて付加価値を生み出していく。データのライフサイクル全般にわたってセキュリティを確保することが、第3層における付加価値を創造する活動の鍵となる。そのため、本フレームワークでは、データを軸に置き、データのライフサイクルを通してデータの置かれている状態を可視化することにより、データのライフサイクル全般にわたってリスクベースでデータのセキュリティを確保するための取組を進められる環境の実現を目指している。

このアプローチの鍵となるのが、データの置かれている状態を可視化する方法であり、可視化の枠組みとして機能することになるデータマネジメントのモデルである。

本フレームワークでは、データマネジメントを「データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、データマネジメントを、データが有する性質である「属性」、データに対して特定の規範を共有する範囲である「場」、データの属性を生成・変化・維持などをする作用である「イベント」の3つの要素から構成されるモデルとして整理する。

この3つの要素を使ってデータの置かれた状態を可視化することにより、データに対してどのようなリスクが存在し、それに対してどう対処すべきか、ということを明確にすることができる。また、この3つの要素はそれぞれが相互に影響しあう関係にあるため、データが移転して要素の一つが変化することで他の要素も変化するという、状態の変化を連続的なものとして捉え、次に発生する変化の予見可能性を高めることにより、データマネジメントを行う際のポイントを

把握しやすくする。

3つの要素がどのような関係を持つか、整理する。

「属性」は、どのようなカテゴリに区分されるのか、どのような機密性が求められるのか、誰が権利を行使し得るのか等のデータの持つ性質であるが、この「属性」は、個人情報が匿名加工という作用を経て匿名加工情報になるように、データに対する作用（「イベント」）によって変化するものであるだけでなく、例えば、個人情報保護法[4]に基づいてデータがどのように扱われなければならないのか、特定組織の内部規程でデータのアクセス権者をどのように定めているか等の「場」の要求によって「属性」の内容が決められる部分が存在し、「属性」と「場」は相互に依存する関係にある。同様に、例えば、電気事業に関する法令では、電気事業者が持つ電気利用に関する顧客のデータを電気事業者以外の者が利用することを目的に電気事業者がデータを提供する場合に、電気事業者が行うべきデータの加工処理の内容が定められているように、データの存在する「場」がデータの「属性」を適切に管理するために特定の作用「イベント」を要求することが頻繁に発生する。したがって、「場」と「イベント」についても、それぞれ関連するものと捉えることが必要になる。

つまり、「属性」と「場」と「イベント」は相互に影響しあう関係にあり、それぞれが他の要素の影響を受けることなく独立して決定されることは限られた場合であり、「属性」、「場」が「イベント」によって変化する場合には、それぞれが関連して連続性を持つことになる。したがって、データのライフサイクルを連続的なデータの状態の変化とし、予見可能性に基づいて、次の状態に遷移する場合の3つの要素について許容される変化の内容や変化幅を捉えることができる本モデルを使うことで、データマネジメントにおいてより現実的かつ効率的な対処を検討するに際してその機能を発揮する。

また、本フレームワークの目的で述べたように、データのライフサイクルの各工程には複数の主体が関与することになり、ステークホルダーの間で共通の理解に基づいたデータマネジメントの取組が必要となるが、3つの要素によってデータの状態が可視化され、かつ、3つの要素の相互依存関係から、データの遷移によるデータの変化に関する一定の予見可能性が確保されることから、ステークホルダーの間で認識を共有しやすくなる。その結果、ステークホルダーの間では、共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を

[4] 本稿では、個人情報の保護に関する法律（平成十五年法律第五十七号）の略称として、「個人情報保護法」という表記を用いる。

実現していくことにつながっていく。

2-1-2 リスク分析手順

一連のバリュークリエイションプロセスに関わるステークホルダーが、共通の理解に基づいてそれぞれの主体が実施すべき措置の検討を進めるためには、当該バリュークリエイションプロセスにおけるデータに関わるリスクを洗い出し、主体間で認識を共有することが必要である。その際、「属性」、「場」及び「イベント」の3つの要素によってデータの状態を可視化することでリスクの洗い出しを行うことが可能となるが、その際には下記の4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化することで、データに関わるリスクの洗い出しと対応策の整理を実施することが可能となる。

STEP 1　データ処理フロー（「イベント」）の可視化

- まず、データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化する。
- その際、「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通するデータを扱う際の対策等を検討するには、検討の本質とは異なる場合があることから省略し、データの取扱に係るマネジメントのルールを提示し、それに従って取り扱っていることを示すことで代替することも考えられる。

STEP 2　必要な制度的な保護措置（「場」）の整理

- データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定する。その際、一つのデータに対して複数の「場」が重なり合う、つまり、データに対して様々な観点からの要求がなされることが考えられる。

STEP 3　「属性」の具体化

- 設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する。
- 場合によっては、データの「属性」を整理していく中で、本データが取り扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する。

STEP 4　「イベント」ごとのリスクポイントの洗い出し

- 設定された「場」という観点から、「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビューする。
- その際、機密性・完全性・可用性といったサイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要がある。

なお、上記のとおり、「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP 1～3については、お互いにフィードバックをかけながら検討されることが適切であると言える。すなわち、各ステップは不可逆的なものではなく、例えばSTEP 3を検討中に「イベント」の追加が必要であることが判明することもあり得る。その際にはSTEP 1に戻って当該必要な「イベント」を追加し、その状態でSTEP 2やSTEP 3を再度検討することで、「属性」、「場」、「イベント」が十分に整理し、その後にSTEP 4に進むことで、適切な形でリスクの洗い出しを実施することが可能になる。また、STEP 4までの取組が完了した後も、内外の要因により従前に特定した「属性」、「場」、「イベント」の内容が変更されることで、新たなリスクが出現したり、想定していた内容が変化したりすることが想定される。そのため、データ利活用のプロセスや関連する法制度等に何らかの変更を認識した場合、あるいは対象となるプロセスや扱われるデータの特性等を踏まえて設定された適切な間隔で、STEP 1からSTEP 3までの検討結果をレビューし、改めてリスクポイントの洗い出しを行うことが望ましい。

2-2 詳細編

2-1において、本フレームワークを用いたリスクの洗い出しの方法を概観してきたが、実際に本フレームワークを活用するにあたっては、「属性」、「場」、「イベント」を適切に設定することが肝要である。そこで、以下にモデル化やリスク分析の詳細を整理する。

ただし、特に「場」や「属性」に関しては、取り扱うデータの性質や、バリュークリエイションプロセスを構成するステークホルダーの性質によってその内容は多様であり、網羅的に示すことには困難が伴う。フレームワークの活用にあたっては、下記の記述を参考にしながら、組織等の実情を踏まえて必要な「イベント」、「場」、「属性」を設定し、リスクの洗い出しを実施する必要がある点に留意されたい。

2-2-1 モデル化（「イベント」）

データの属性を生成・変化・維持などをする作用である「イベント」に関しては、大きくは「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の5つに区分することが可能である。なお、それぞれの「イベント」ごとに考慮すべきリスクの例は、添付の形で示す。

- 生成・取得

  バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、センサーによる計測等の自動的な手段又は人手による入力等を介して生成・取得されることによってそのライフサイクルが始まる。

  これまでに、データが生成される場所については第3層ではなく第2層に属する場合があることを明確にし、第3層と第2層とを組み合わせることでデータ生成における信頼性を確保する考え方を示している。サイバー空間とフィジカル空間が高度に融合し、センサーによるデータの取得など、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの信頼性を検討する場合、センサー等によって物理的な情報がデータとして正しく転写されているかなど、従来はデータを管理する範疇に捉えられていなかった、データの生成に関わる機器・システムなどの信頼性についても検討する必要がある点に留意が必要である。例えば、第2層においてサイバー空間への転写が正しく行われるよう、セキュリティ侵害（例：ソフトウェアの改ざん）を受けていない信頼できるIoT機器によりデータを生成し、なりすましやネットワーク上での改ざん等がないようサーバ等へ正確に当該データを送信することを通じて、第3層において利活用するデータの信頼性をデータライフサイクルの初期段階から確保することが可能である。なお、本件に関しては、CPSFの第2層（サイバー空間とフィジカル空間のつながり）における信頼性の確保として、IoT機器・システムのセキュリティ・セーフティ対策を検討した「IoTセキュリティ・セーフティ・フレームワーク」でも触れられており、フレームワーク間で連動する構造になる。

本イベントにおいて考えられる代表的なリスクとして、計測結果が実際と異なる、計測機器をなりすまされる等の転写の失敗、システム障害等に起因する生成・取得の停止、不適切なプロセスによる個人情報の取得などが挙げられる。

- 加工・利用

生成・取得されたデータは必ずしもそのまま単純に付加価値を生み出すというわけではなく、何らかの作用を通じて付加価値を伴うものとなっていく。例えば、いわゆる生データか

ら、利用目的に合わせて抽出やトリミングなど様々な処理を行い、データを利用しやすくした上で、そのデータを閲覧したり、そのようなデータからAI等を利用することでインテリジェンスを抽出したりすることによって付加価値につながる。本フレームワークでは、このような付加価値を生み出すための作用を加工・利用と捉える。

なお、データの一部の項目や要素、レコードなどを、その分析過程や保管されたデータセットから取り除く作用については、加工の一形態として捉えるものとし、後述する廃棄とは区別して捉えるものとする。

また、データを保有しない者がデータにアクセスする作用（閲覧）については、付加価値を生み出すための作用である点から利用の一形態として捉えることが適切であるが、データを複製して共有することで閲覧させる場合には、複製元のデータを保有する移転元だけでなく、移転先もデータを管理することとなるため、リスクを洗い出すにあたっては移転・提供の要素を考慮に入れる必要がある。

本イベントにおいて、考えられる代表的なリスクは、データの目的外利用、不適切な加工などである。

- 移転・提供

サイバー空間とフィジカル空間が高度に融合した社会であるSociety5.0においては、様々な主体が動的にサプライチェーンを構成することになるが、その過程では、必ず組織を跨ぐ移転が行われる。企業間のつながりで固定的なサプライチェーンを構成する場合であっても、データの組織間の移転・提供は一定のリスクを孕むものとして慎重に処理されてきたが、サプライチェーンを動的に構成する場合には、その効果を最大限に引き出すためにはより自由にデータの移転・提供を実施できる環境にすることが求められ、その裏腹の関係として、リスクに対してもより効果的に対応することが求められることになり、そのための制度も含めた環境を整備しなければならない。

また、データの移転・提供は、一般にデータが複製されて移転元にデータが残ったまま移転先でもデータを管理することになる。そのため、加工・利用の説明において既に述べたとおり、データを保有しない者がデータにアクセスする作用（閲覧）については、リスクを洗い出すにあたっては移転・提供の要素を考慮に入れる必要がある。

なお、本フレームワークにおける移転・提供には、機器と機器、例えばサーバとクライアントの間でのデータの移転・提供も取り扱うこととする。これによって、悪意のある者によるネットワーク上での盗聴やデータの移転・提供に係るシステムの不具合等によるデータの損傷等

のリスクを捉えることが可能になる。

そこで、本フレームワークにおいては、対象となる移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という4つの単位で整理することとする。単一の移転・提供事象についてリスクやその他の留意事項を整理しようとする際、その具体的な方法等に応じて、同時に複数の単位が考慮され得る。これにより、技術的・非技術的なリスクを網羅的に識別するにあたり有用と考えられる。4 つの単位の概要や実際に考慮すべき事項は下記のとおり整理できる。

ー　国・地域

この単位においては、対象となる移転・提供事象に関連する国・地域及び、域外適用されるものも含めて当該国・地域におけるデータ保護関連の政策、法令、ガイドライン等を特定し、それらに係るリスクや対応に必要な手続き等を整理する。当該移転・提供事象が現に特定の法令等が適用される国・地域を越えて行われている、あるいは国・地域内の移転・提供であっても境界を越えているとみなせる方法（例：「みなし輸出」に該当する行為）で行われている場合に考慮すべき単位である。具体的には、個人情報保護関連法令における個人情報の越境移転や外為法等の輸出管理関連法令における技術情報等の輸出、海外のデータ保護法令における特定データの国内保存に関する規定や域外適用に関する規定等が該当し得る。検討にあたっては、それらに係るリスク（例：法令違反、社会的な信用の失墜）、適正な移転・提供実施のために必要な手続き（例：個人情報を日本から海外にある第三者に移転する際の本人同意の取得、本人への情報提供等）を含めて特定することが望ましい。

ー　組織・ヒト

この単位においては、対象となる移転・提供事象に関連する組織及びヒト、当該主体におけるデータ保護関連の方針、体制等を特定し、それらに係るリスクや必要となる対処等を整理する。当該移転・提供事象が、ある組織・ヒトからセキュリティポリシー等の異なる別の組織・ヒトへ行われる場合に考慮すべき単位である。同一の法人内のデータ移転・提供であったとしても、適用されるセキュリティポリシーが異なる部門（例：本社と生産拠点）間で行われる場合はこちらに該当する点に注意が必要である。例えば、ある組織から事業上有用なデータを他の組織に移転・提供する際、セキュリティ水準が相対的に低い組織・ヒトから重要なデータが漏えいするリスクが懸念されるため、移転先となる組織及び

ヒトに係るセキュリティ対策やその他のデータ保護措置の実施状況（例：ISMS認証等の取得有無）を確認する等の対処が特定され得る。

ー　システム・サービス

この単位においては、移転・提供を実行するシステム及び当該システムが提供する機能としてのサービス（用いられるプロトコル等を含む）、それらが備えるデータ保護機能を特定し、想定されるリスク（例：ネットワーク上での盗聴、送信元/送信先のなりすまし）や必要な対処を整理する。当該事象が、ネットワークを通じて機器間で電子的に行われる場合に考慮すべき単位である。データの移転・提供に用いられるシステム・サービスには、例えば、クラウドストレージ、電子メール、ファイル転送（例：FTP、HTTP）等、様々なものが含まれるが、現に移転・提供されるデータのカテゴリや価値（重要度）等を考慮して十分なセキュリティ等の水準を有している手法が利用されるべきである。例えば、クラウドストレージを用いてデータを移転・提供する際、クラウドストレージ側の脆弱性を悪用されデータが漏えいするリスクや、サービス利用者側の設定ミス等によりデータが外部からアクセス可能となるリスク等が想定されることから、事前に当該クラウドサービスにおけるセキュリティ機能の実装状況を確認する、サービス利用時に利用者側で実施すべき事項を文書化しておく等の対処が特定され得る。

ー　機器

この単位においては、移転・提供事象を実行する単体のシステムコンポーネント（例：サーバ、IoT機器、ネットワーク機器）及びそれらが備えるデータ保護機能を特定し、想定されるリスク（例：機器内の不正なコンポーネントを通じた意図しないデータ移転、サービス拒否攻撃等による機器の稼働停止）や必要な対処を整理する。当該事象が、ネットワーク又は可搬媒体等を通じて行われる場合に考慮すべき単位である。例えば、クラウドストレージを用いてデータを移転・提供する際、クラウドサービスにアクセスする端末が外部から不正アクセスされ、クラウドストレージのデータにアクセスされる等のリスクが想定されることから、当該端末を利用しようとする際の認証機能を強化する、同端末におけるエンドポイント向けのセキュリティ対策（例：マルウェア対策ソフトウェア、EDRの導入）を強化する等の対処が特定され得る。

前述のとおり、「イベント」をどの程度詳細に記述するかは、データフローの整理の目

的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通する場合のデータマネジメントを検討する際には省略されることも考えられる。

- 保管

保管については、他のイベントに付随して必ず生じる「イベント」である[5]。データはライフサイクルの様々な段階において、ネットワーク接続されたストレージ機器（オンプレミス、クラウドの双方を含む）、クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。データの取扱に関してリスクを洗い出し、セキュリティ対策を検討する上では、移転・提供、加工・利用されるデータとは異なるリスクが生じ得ることから、「イベント」の一類型として整理し、リスクの洗い出しを実施することが適切と考えられる。

- 廃棄

加工・利用されたデータは、ライフサイクルの終わりとして、適切に廃棄される必要がある。

なお、本フレームワークにおける廃棄は、データセット全体を使用不可能な状態とすることを指す[6]。データは自組織が直接的に管理する媒体だけでなく様々な媒体に複製され得るが、当該データのカテゴリや重要度等を勘案して、組織は当該データに対する権限や複製、配布等の状況について適切に管理する必要がある。元のデータを廃棄する際に、複製先のデータも含めて廃棄する必要がある場合には、関連するステークホルダーと協議する等、文脈に応じて適切な廃棄の取組を推進する必要がある。なお、個人の同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切である。

本「イベント」における代表的なリスクは、廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまう等が考えられる。

---

[5] 本稿では、データを長期保存する際に行われる「アーカイブ」も保管に含まれるものと捉える。

[6] データの「属性」や「場」の規範等によって、データの廃棄について、ハードディスク等の物理的な破壊や暗号化消去等の特定の方法を求めるのか、一般的な方法を許容するのか等、廃棄への要求水準は異なると考えられるため、個々の事情に応じて要求される適切な廃棄方法を実施することが重要である。

5つの「イベント」は、それぞれ重複する性質を持つ場合がある。例えば、国外にある他組織が公開しているデータを閲覧することは、データの加工・利用の性質を有するが、国・地域間及び組織間におけるデータの移転・提供という性質を内包する。さらに、自組織内における機器間での移転も含まれることから、目的に応じて適切に「イベント」を捉え、リスクの洗い出しを実施する必要がある。

2-2-2 モデル化（「場」）

前述のとおり、「場」はデータに対して特定の規範を共有する範囲と定義している。データに対する規範は、各国・地域等の法令によって定められているもの、組織で定められた内部規則、組織間で個別に取り交わされる契約などの様々な形態が存在し、取り扱うデータの性質や、データを利活用する所在地によっても設定される「場」は変わり得る。その際、現にデータが所在している国の法令のみならず、該当する場合は域外適用規定を有する他国の法令も含めて「場」として特定する必要がある点に留意が必要である。さらには、データの取扱に関して、特定のコミュニティにおいて暗黙のうちに共有されている共通認識（必ずしも明文化されていないものも含む）や、デジタルプラットフォーム等の利用規約も、「場」として機能していると言える。このように、「場」は、それぞれの状況や関係する者の事情などによって適用される形態等が異なることになり、一律に設定方法や形態が決まるものではない。そうした「場」に関するより具体的な検討は、今後の議論や事例の蓄積を通じて、精緻化されることが想定される。

対象となるデータ利活用プロセスに係るデータ保有者のようなステークホルダーが「場」の設定を行うにあたって、例えば、「場」を構成する重要な要素の一つに法令等があるが、必要な観点を漏らすリスクを低減しながら検討するためには、例えば下記のような4つのカテゴリから整理することで適切な設定につながると考えられる。4つのカテゴリは、「場」が、データに関して何らかの共通の取扱を求める法令等と連動して設定されることを背景に、データに共通の取扱を求める目的としてはどのようなものが考えられるか、という観点から整理している。なお、4つのカテゴリは一つの例であり、フレームワークを適用する対象が位置する文脈や重視する観点等により重複や漏れが生じる場合も想定されることから、必ずしも完全なものではない。

その際、「場」の要求に応じて設定される「属性」の例も併せて記載するので、「場」や「属性」の洗い出しに活用されたい。

- パーソナルデータの保護

・「場」の例：個人情報保護法（日本）、GDPR（欧州関係）、個人情報を取得する際に当該

個人が同意した利用目的

・規定される「属性」の例：カテゴリ（個人情報、匿名加工情報）、データ権利者、データ管理主体

- 知的財産（営業秘密を含む）保護

・「場」の例：不正競争防止法、著作権法、主体間の契約（NDA等）

・規定される「属性」の例：カテゴリ（営業秘密、限定提供データ）、開示範囲、データ権利者

- 機微技術管理

・「場」の例：外為法、米国輸出管理規則

・規定される「属性」の例：カテゴリ（輸出管理等対象技術）、開示範囲、データ管理主体

- 適切な社会機能の維持

・「場」の例：金融商品取引法（インサイダー取引）、各種守秘義務関係

・規定される「属性」の例：開示範囲

また、関連規定等の分類方法には、上記で示したものとは別の観点からまとめたものとして、以下の分類[7]がある。

- 情報を管理する事業者に管理責任を課す類型：情報を管理する者に対して当該情報に対する管理責任を負わせる類型の法制度であり、個人情報保護法における個人情報取扱事業者の義務等を含む。
- 不正行為者に法的責任を問う類型：不正行為者に対して法的責任を問う類型の法制度であり、不正競争防止法における営業秘密保護規定等を含む。

2-2-3 モデル化（「属性」）

「属性」は、対象データの法的なカテゴリや開示範囲、取得元から許容された利用目的等のデータが有する性質を示すものである。組織は、当該データの「属性」の整理を通じて、関連する利用上の制約を特定し、セキュリティを確保するために必要な措置を講ずることによって、データの適切な取扱を実現することが可能になる。かかるデータの「属性」の項目を網羅的に示すことは困難だが、代表的な「属性」やパラメータ、「属性」の整理のポイントを下記に示す。

なお、前述のとおり、「属性」は「場」の要求によってその内容が決められる部分が存在し、2-2-2においても「場」によって規定される「属性」の例を挙げている。整理した「場」に

[7] 経済産業省「情報セキュリティ関連法令の要求事項集」（2011 年 4 月）

関して、データに対する要求を検討し、関連する「属性」を適切に具体化することが重要である。

- カテゴリ

  特に「場」と連動して、データに対して特別な作用（「イベント」）を求める場合（個人情報・匿名加工情報、営業秘密・限定提供データなど）、カテゴリとして法令等における位置づけを整理する。

- 開示範囲

  民法上の契約や組織内規則も含め、データに定められている開示範囲を整理する。その際、組織内での取扱であっても、国・地域間での移転が伴う場合や、米国輸出管理法上のみなし輸出に該当する場合等、開示範囲の制限が複層的に適用される可能性がある点に留意する。

- 利用目的

  個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場合、データが主体間を転々として付加価値を生み出していく過程全体を通じて、当該利用目的の範囲内で取り扱われる必要があることから、「属性」として明示しておく必要がある。

- データ管理主体

  サプライチェーンが動的に構成される中、データに対して様々なプレーヤが関与することとなるが、法令上あるいは契約上、データフローのある時点において、データの管理に責任を負うべき主体が特定される。当該主体は、実際にサイバーセキュリティ対策を講じる際に、重要な推進主体となる。データを軸に置く本フレームワークにおいては、データが転々流通する過程で管理主体も移り変わるものであり、データが有する「属性」の一つとして取り扱う。なお、クラウドサービス等を利用する場合や、データの処理を外部委託等する場合等、管理主体が曖昧になるケースがあるため、データ管理主体を特定し、その変化を適切に捉えることは重要である。

- データ権利者

  データ管理主体とは別に、データに対して権利を有する主体が存在することがある。バリュークリエイションプロセスの中で、移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者（例：個人情報ならばデータ主体となる本人、事業上有用なデータならば権利元の組織）は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられる。例えば、個人情報保護法上の同意の取り下げや、著作権法等のライセンスに関する規定上の取扱、企業の競争力に関わるデータ（例：製品の設計データ、製造拠

点における機器・設備の稼働状況）を提供している場合等は、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

- 価値 （重要度）

  対象データの事業上の価値（重要度）を特定する。組織は、特定された価値の大きさに応じて、現に対象データを取り扱うシステムや組織に対して適切なリスク対応策を採用することが望ましい。価値の算定にあたっては、データのカテゴリや業種等に応じて様々な方法を適用することが可能だが、一例として、機密性、完全性、可用性の観点からデータ侵害によって生じ得る事業への影響の度合いを評価し、そのうち最大のものを評価値とするものがある。

- 媒体・保存先

  一般に、電子化されたデータは複製等が容易であるが、データのカテゴリや適用されるポリシーの内容等によっては、データを保管、加工・分析等するために利用している媒体やサービスを特定し、求められるセキュリティ水準を維持できるようにデータの所在を継続的に管理することが必要な場合がある。主な媒体・保存先の種別としては、可搬電子媒体、PC、モバイル端末、社内サーバ、社外サーバ（例：クラウドサービス）等がある。

- 利用期限

  法律や別途締結される契約、関連するポリシー等でデータの利用期限や利用完了後の遅滞ない廃棄、提供元への返還等が定められる場合、当該データ利用の開始日と終了日を特定し、利用期限を過ぎてもデータが利用可能なままとなっていないか等を管理することが必要となる。

3. 活用方法

3-1 サプライチェーンを構成するステークホルダー間での活用

本フレームワークの目的で述べたように、本フレームワークを活用することで、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することが可能になる。

バリュークリエイションプロセスに関わるステークホルダーの間で、複数の主体の協同的活動によって必要なセキュリティ対策を検討するにあたっては、データのライフサイクルの各工程において直面するリスクに関する認識を共有することが必要である。本フレームワークを活用してリスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と協議しながら取り組

むことによって、データの信頼性を確保することが期待される。

また、既に述べているように、データは基本的に中立性を有しており、バリュークリエイションプロセスにおけるデータとデータに関与する主体は切り離して考えるべきで、例えば流通しているデータの誤用や悪用はデータ自体の問題ではなく、それを行った主体の問題として理解することができる。したがって、バリュークリエイションプロセスに参加する各主体は、関係するステークホルダーの間で互いにデータ流通に係る条件を提示した上で契約等を締結、履行することで、本フレームワークで示す協同的活動における責任を果たすことができる。その上で、各主体において当該契約等が履行されているかは、監査等の方法で確認され得ることから、将来的には、経営者によるITガバナンス（デジタルガバナンス）の検討にも本フレームワークが活用されることが期待できる。

なお、本フレームワークにおいては、主体間を転々流通するデータに関するリスクの洗い出しに関する考え方を整理している。可視化されたリスクに対して、各主体が実施すべきセキュリティ対策は、これまでに公表されてきた情報セキュリティに関する様々な国際標準等において既にまとめられている。具体的な措置内容の選択にあたっては、既存の規格等を参照いただきたい。主な規格は次のとおり。

＜リスクマネジメントの全体プロセスを示すもの（例）＞

- ISO 31000:2019
- ISO/IEC 27001:2013
- NIST SP 800-30 Rev.1

＜全般的にセキュリティ対策要件等を示すもの（例）＞

- データマネジメント知識体系ガイド（DMBOK） 第2版
- ISO/IEC 27001:2013 附属書A, ISO/IEC 27002:2013
- NIST SP 800-53 Rev.5
- CPSF

＜各イベントのセキュリティ対策等の詳細を示すもの（例）＞

- 生成・取得：安全なウェブサイトの作り方　改訂第 7 版（生成・取得の手段としてウェブサイトを用いる場合）、NISTIR 8259 （生成・取得の手段としてIoT機器を用いる場合）
- 移転・提供：ISO/IEC 27033-1:2015, NIST SP 800-47 Rev. 1
- 加工・利用：AI・データの利用に関する契約ガイドライン 1.1版
- 廃棄：NIST SP 800-88 Rev.1

3-2 ルール間のギャップの分析

本フレームワークの目的のところで述べてきたように、本フレームワークは、データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしての活用も可能である。

例えば、欧州からの個人情報の移転に関して、GDPRに関するSchrems II 判決でプライバシーシールドが無効と判断された米国と、十分性認定を受けている我が国の差異について下記のように整理することが可能と考えられる。ここでは、状況を単純化するため、同一事業者の国外拠点への移転を想定し、事前に設定された利用目的の範囲内での移転であることとする。

欧州から日本への移転については、移転という「イベント」によって、「場」が欧州のGDPR等の法制度から、日本の個人情報保護法制の下に移る。その際、日本は十分性認定を取得していることから、欧州GDPRで求められているデータ保護が、日本の個人情報保護法制の下でも実質的に確保されていると考えられる。データの「属性」に関しては、データ管理主体に日本拠点が加わるのみであるが、関連する処理[8]に際して、GDPRの規定する個人データの適法な処理の要件が満たされていることを前提とすると、十分性認定により、データ管理主体の変化に関しては事前に認められ、許容されていると言える。

一方、欧州から米国への移転をGDPR等に定めのある適法な手段に基づいて行おうとする場合、データが米国に所在する状況では、「場」が米国の各種法制度に基づいたものに変化している。例えば、米国の法制度の下では、安全保障などを目的とした米国政府機関による監視の対象となる場合があることから、移転という「イベント」を経てデータの物理的な所在地が米国となることを通じて、データ「属性」に関して、データ管理主体の変化の他に、潜在的な開示範囲に米国政府が加わる形で「属性」が変化していると考えられる。このような状況も反映し、現状では、欧州から米国への個人データの越境移転を、欧州委員会が認めた標準的契約条項（SCC）の締結に基づいて実施することが求められている[9]。そのため、十分性認定に基づきかかる移転を行う日本と米国との間には、欧州からの個人データの越境移転に関するルール間のギャップが存在すると言える。

このように、データに関する「場」の変化や「属性」の変化を可視化することで、データの

[8] ここでの「処理」とは、GDPR における定義にならい、「自動的な手段であるか否かに関わらず、個人データ、または個人データの集合に対して行われる、あらゆる単一の作業、または一連の作業」を意味するものとする。

[9] なお、欧州から米国への移転・提供にあたって、SCC を利用する場合であっても、米国政府への開示に関する対応について、特に留意して実施する必要がある。

セキュリティの確保のために要求されている条件や措置の相違を把握することにつながる。

添付A ユースケース

A-1 POSデータの分析

直接的な消費者との接点を有する小売・流通業は、従来から他産業に比べ多様かつ大量のデータを保有し、顧客へのサービスの向上や効率化のため、販売・仕入れ等に付随して発生するデータの活用に取り組んできた。特に小売業が持つPOSデータ・ID-POSデータの活用が進んでいる。

また、実店舗と EC 等の融合を目指す「オムニチャネル」の取組も、各事業者にて環境整備が進められており、スマートフォンやソーシャルメディア（SNS）が普及したことで、消費者が様々な販売チャネルを活用して、新たな購買体験を経験することが可能になっている[10]。事業者は、それら複数のチャネルから収集されるデータをチャネルや部門ごとにばらばらに蓄積、活用するのではなく、統合的に活用することで、より効果的に取組を進めることができるとされている。

上記の背景を踏まえ、小売・流通業に係る本フレームワークのユースケースとして以下の流れによるデータの利活用プロセス（A-1内において、以下、「本ユースケース」という。）を取り上げる。

- 小売事業者X（X社）は、従来から国内各地に店舗を構える小売事業者で、現在は物理店舗とECサイトという複数のチャネルで商品を販売しており、会員証等を活用しながら購入者のID[11]と購入物等を紐づけられる形で販売データを収集している。
- 個々のチャネルから得られたデータは他のデータと相互に連携できる形で個別に保管され、別途作成される各種マスターデータ（例：顧客マスタ[12]、商品マスタ）等も参照しながら、マーケティング用途等のニーズに応じて統合される。

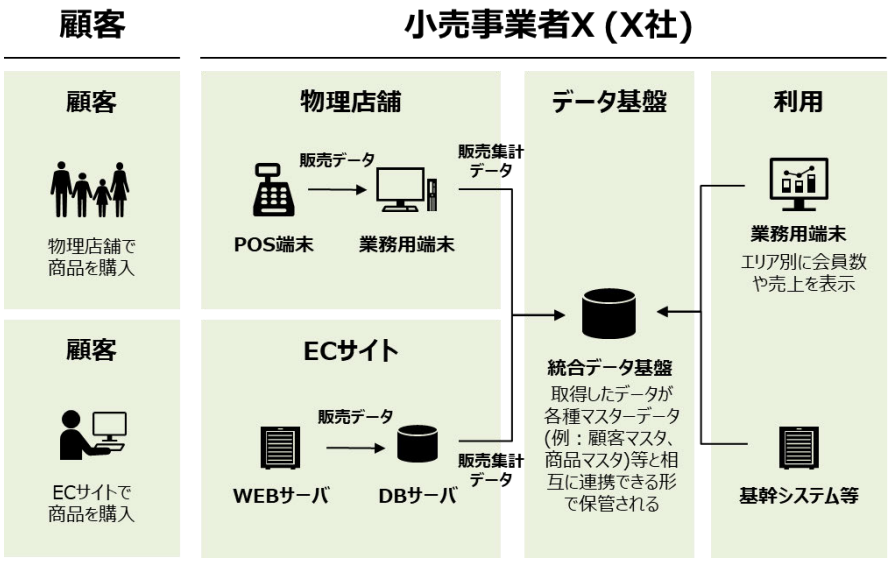
---

[10] 経済産業省 商務流通保安グループ「流通・物流分野における情報の利活用等に関する研究会　調査報告書」（2016 年 2 月）

[11] 本ユースケースでは、物理店舗と EC サイトで共通の会員 ID が利用されていると仮定する。

[12] X 社の顧客マスターデータを、本稿では「会員情報」（会員の氏名、性別、住所、連絡先等の情報を内容として含む）と呼称する。

- 統合されたデータは多種多様な用途で活用され得るが、ここでは事業者X自身がチラシ配布や広告表示等の広報の最適化を図るため、地図ソフトと連携してエリア別に会員数や売上を表示する事例を取扱う。



図A-1.1 対象プロセスの概要

小売・流通業におけるサプライチェーンには、図A-1.2に示すように、製造、中間流通、販売[13]等の段階があり、SPA（製造小売業）等の例外を除いて、それぞれ別の事業者がビジネスを行っている。小売・流通業におけるデータ利活用としては、取扱い製品の製造段階や中間流通段階を対象にしたものも想定されるが、本ユースケースにおいては、特に小売段階における販売データ等のマーケティング活動等への利用を扱うこととする。



図A-1.2 小売・流通業のサプライチェーンにおける対象プロセスの位置づけ

X社が図A-1.1に示すようなデータ利活用の仕組みを今後整備しようとする際、又は既に整備

[13] 経済産業省 商務流通保安グループ「流通・物流分野における情報の利活用等に関する研究会　調査報告書」（2016 年 2 月）「5） 製・配・販連携によるサプライチェーンの高度化」等を参照

した仕組みを見直そうとする際に、関係部門（例：物理店舗部門、EC事業部門、情報システム部門）で連携しつつ全体として一貫性のあるセキュリティ対策等を実装するために、本フレームワークは活用され得る。その際、本ユースケースにおいて考慮すべきステークホルダーとして以下が挙げられる。

- 顧客：X社が運営する店舗から商品を購入する
  - 物理店舗を利用する顧客
  - ECサイトを利用する顧客
- X社：顧客が利用する店舗を管理・運営する
  - 物理店舗の管理・運用に係る部門
  - ECサイトの管理・運用に係る部門（EC事業部門）
  - 情報システム部門
  - マーケティング部門
- ITサービス事業者：X社からの委託を受けシステムの開発、運用等を行う

A-1-1 STEP 1　データ処理フロー（「イベント」）の可視化

- *まず、データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化する。*
- *その際、「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通するデータを扱う際の対策等を検討するには、検討の本質とは異なる場合があることから省略し、データの取扱に係るマネジメントのルールを提示し、それに従って取り扱っていることを示すことで代替することも考えられる。*

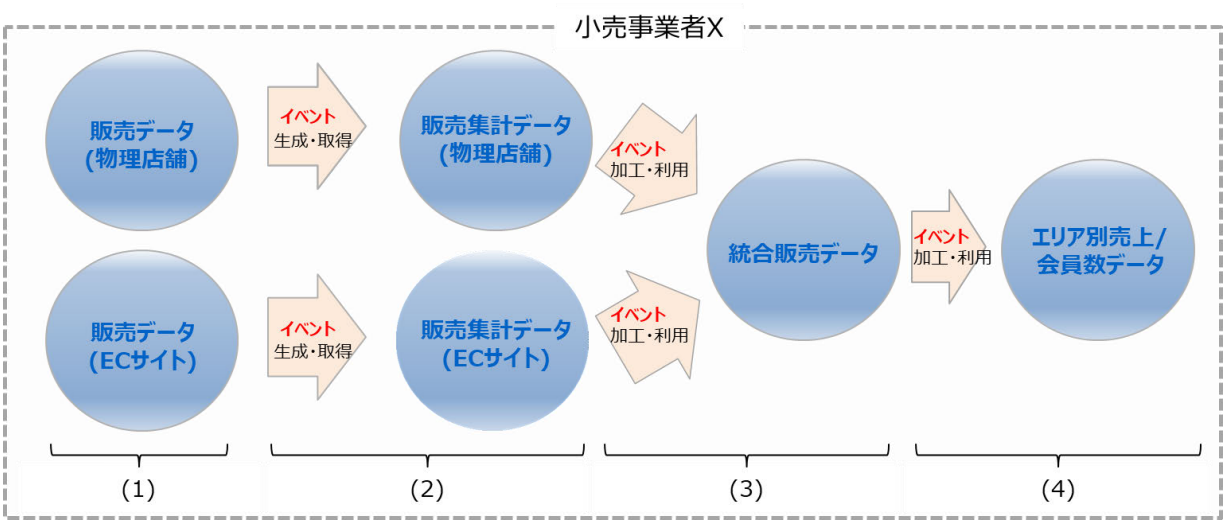
STEP 1は、生成・取得から廃棄に至るまでの一連のデータのライフサイクルにおいて、データがどのようなプロセスで利活用されるのかを理解する段階である。本ユースケースでは図A-1.1で示すように、以下のプロセスにより構成される。

(1) 物理店舗とECサイトという各販売チャネルにおいて顧客による購買が行われる都度、個別の「販売データ」が「生成・取得」される。「販売データ」には、販売の日時や店舗、購入された商品とその価格、個数等が含まれる。

(2) 「販売データ」は各店舗又はサイト等の単位で「販売集計データ」として蓄積される。

(3) 各店舗やサイト等で保管された「販売集計データ」は、X社の統合データ基盤に集約された後、複数の販売チャネルを連携させたマーケティング分析等の基盤となるよう、「統合販売データ」に「加工・利用」される。

(4) 「統合販売データ」は、チラシ配布等の広報の最適化を図るため、地図ソフトと連携して「エリア別売上/会員数データ」に「加工・利用」される。



図A-1.2 データ処理フローの可視化（POSデータの分析）

なお、図A-1.2では割愛しているが、（1）から（4）という4つの段階からなる上記プロセスにおいて、各種データの適時かつ適法な利用に資するよう、「販売集計データ」、「統合販売データ」、「エリア別売上/会員数データ」は業務用端末や各種データベースに中長期的に保管され、あらかじめ設定した利用期限の終了とともに適切な手法を通じてレコード単位で削除、又はデータセット単位で廃棄される。データの保管や廃棄に係る要件はSTEP 3にてデータの管理に資する「属性」を特定する際の重要なインプットとなるため、可能であればSTEP 2やSTEP 3において特定しておくことが望ましい。

また、図A-1.2に示すプロセスとは別途、X社はECサイト上の会員登録画面や物理店舗に設置された申込用紙への記入等を通じて顧客から会員情報を「生成・取得」しており、共通する会員ＩＤに基づいて当該情報と各種販売データを突合することで、個人情報としての「統合販売データ」等へと「加工・利用」している。この際、申込用紙等を通じて各物理店舗にて取得された会員情報は、個人情報保護の観点から各店舗や各地域の支社では保管されず、本社情報システム部門が管理する統合データ基盤にて集中的に管理されるという運用を想定する。

「生成・取得」や「加工・利用」等の「イベント」をどの程度詳細に記述するかは、データ

フロー整理の目的に応じて調整されるが、ここでは、データの管理水準や対策の内容に少なからず影響するデータの「属性」である事業上の重要度やカテゴリ（例：個人情報の該当性）を変化させるものや、「信頼境界」[14]を構成すると考えられるものを抽出した。

A-1-2 STEP 2　必要な制度的な保護措置（「場」）の整理

- *データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定する。その際、一つのデータに対して複数の「場」が重なり合う、つまり、データに対して様々な観点からの要求がなされることが考えられる。*

STEP 2は、STEP 1で特定された一連のデータ利活用プロセスに対して、「場」としてどのようなデータの保護に係るルール（規範）が課せられ得るかを理解する段階である。本ユースケースにおいて、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

（1）割賦販売法/PCI DSS[15]：物理店舗やECサイトでの決済にクレジットカードを用いる場合、割賦販売法第35条の16により加盟店たるX社は、クレジットカード番号等に該当する「販売データ」等の適切な管理や自らの委託先に情報管理に係る指導等を行うことが義務づけられている。実務上の指針とされる「クレジットカード・セキュリティガイドライン」では、具体的な管理として、カード情報を保持しない非保持化又はカード情報を保持する場合はPCI DSS準拠のいずれかの対応が必要とされる。

（2）個人情報保護法：各種チャネルにおける「販売データ」等は会員ＩＤにより個々の顧客を識別しており、それ単体では特定の個人を識別できるものではないが、統合データ基盤等において別途会員情報と突合等されることで個人データに「加工・利用」される。X社内部の情報管理規則において各物理店舗等において個人データを取扱わないこととしている場合、会員情報を扱う統合データ基盤等に対して物理店舗の担当者その他の関係者からのアクセスができないようにする等して、「販売データ」等を他の情報と容易に照合できないようにする必要がある。なお、X社が個人データ（例：「販売集計データ（ＥＣサイト）」、「統合販売データ」）を管理する場合、利用目的の明確化・利用目

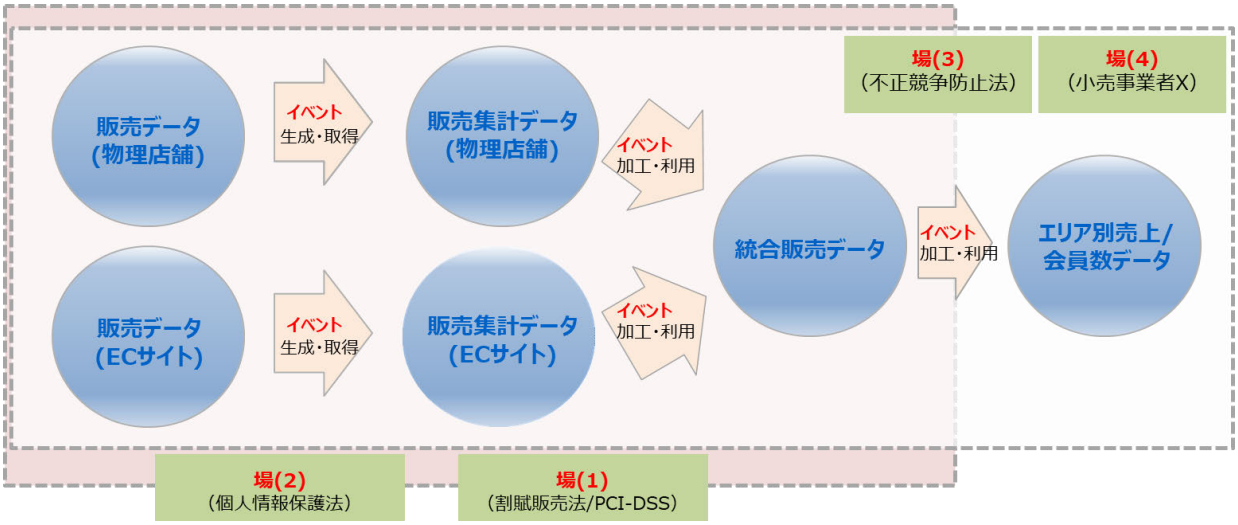
[14] 脅威分析の一環で作成されるデータフロー・ダイアグラム（DFD）において特定される、管理している組織やインターフェイスが変わる場所に引く境界線のことを指す。

[15] 加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定されたセキュリティ基準 ”Payment Card Industry Data Security Standard” を指す。

的による制限、安全管理措置、第三者提供時の手続等の個人情報保護法において個人情報取扱事業者の義務として定められる各種の規律を遵守する必要がある。

（3）不正競争防止法：X社が収集し、保管する「販売集計データ」や「統合販売データ」等は通常、事業上の価値が高い情報であって、「営業秘密」として不正な取得、使用、開示から法的な保護を受けられるよう管理することが一般的と考えられる。

（4）X社内部の情報管理規則



図A-1.3 必要な制度的な保護措置の整理（POSデータの分析）[16]

A-1-3 STEP 3 「属性」の具体化

- *設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する。*
- *場合によっては、データの「属性」を整理していく中で、本データが取り扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する。*

STEP 3は、STEP 2にて特定されたデータの保護に係るルール（場）の効果的・効率的な遵守に資するデータの「属性」を特定する段階である。内容を特定すべき「属性」項目のうち主なものは本文2-2-3に示したとおりだが、STEP 2で特定される「場」と強く関連したものが多く含まれる。各「属性」項目のパラメータを設定するにあたり考慮することが望ましいルール

[16] 図中には必ずしも記載されていないが、物理店舗や EC サイトの運営にあたり、必ずしも明文化していないが担当部署等において共有されているルールも特定されるべき「場」として含まれ得る。

は以下のとおりと考えられる。

表A.1-2 「属性」の検討において考慮すべきルール（場）

		割賦販売法等	個人情報保護法	不正競争防止法	X 社内部情報管理規則
カテゴリ	パーソナルデータ保護	○	○		
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的			○		
データ管理主体		○	○		○
データ権利者		○	○		
価値（重要度）		○	○	○	○
媒体・保存先			○		○
利用期限		○	○		○

本ユースケースにて取扱われるデータの多くは個人データに該当するため、「利用目的」や「利用期限」、「開示範囲」の適切な設定と遵守状況のモニタリング等は特に重要になる。「利用目的」や「利用期限」は会員規約等における規定を参照して具体化しつつ、「開示範囲」はNeed to knowの原則[17]やNeed to useの原則[18]に従い、営業秘密管理上の「秘密管理性」を満たすためにも社内でも関係者のみに限定することが望ましい。上記の事項を考慮して具体化した本ユースケースで取り扱うデータがとり得るパラメータの例を以下に示す。

[17] それぞれの職務を実施するために必要な情報へのアクセスだけが認められるべきという考え方

[18] それぞれの職務、業務を実施するために必要な IT 機器、アプリケーション、手順、部屋等へのアクセスだけが認められるべきという考え方

表A-1.1 本ユースケースにて取扱うデータの「属性」パラメータ例

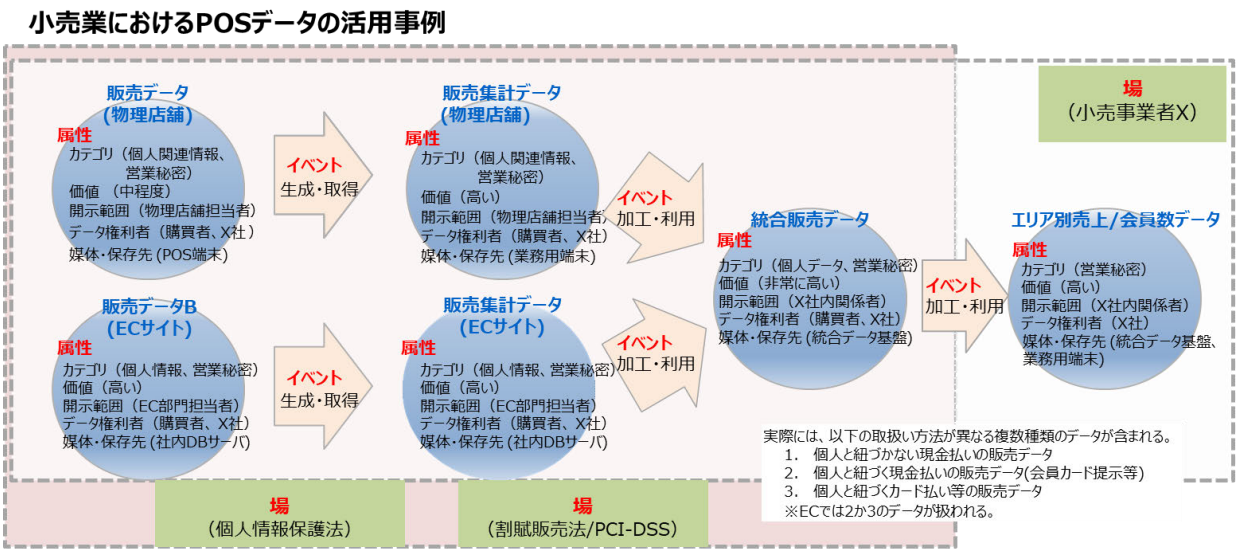
		販売データ（物理店舗）	販売集計データ（物理店舗）	統合販売データ	エリア別売上/会員数データ
カテゴリ	パーソナルデータ保護	個人関連情報 等	個人関連情報 等	個人データ	統計情報（非個人情報）
	知的財産（営業秘密を含む）保護	営業秘密	営業秘密	営業秘密	営業秘密
	…	…	…	…	…
開示範囲		X 社内[19]	X 社内	X 社内	X 社内
利用目的		• 売買契約の履行 • 各種アフターサービスの実施 • 商品企画、開発	左記と同様	左記と同様	広報活動の効率化
データ管理主体		各物理店舗	各物理店舗	情報システム部門	情報システム部門、マーケティング部門
データ権利者		購買者、X 社	購買者、X 社	購買者、X 社	X 社
価値（重要度）		中程度	高い	非常に高い	高い
媒体・保存先		POS 端末（店舗に所在）	業務用端末（店舗に所在）	社内サーバ（統合データ基盤）	社内サーバ、業務用端末
利用期限		会員契約終了から 5 年	（各レコード単位で）会員契約終了から 5 年	左記と同様	特になし

「カテゴリ」としては、「場」として設定されている複数のルールに対応して、取扱うデー

[19] 本ユースケースでは X 社内で複数の部門が利活用に関与するが、当該部門間での責任分界を明確にするため、実際の資産管理にあたっては部門や役割等のより詳細な単位で開示範囲の記載を行うことが望ましい。

タが個人情報保護法における「個人関連情報[20]」、「個人データ」又は「非個人情報」、不正競争防止法における「営業秘密」として管理すべきデータに該当すると特定できる。その際、個人情報保護や営業秘密保護等の異なる体系による複数の類型が同一のデータに適用され得る点について留意する必要があるが、この中でも特に、個人情報保護法における位置づけが利活用プロセスの中で変化しており、データごとに異なる管理が必要となっている点を確実に認識する必要がある[21]。

上記では表形式でデータとその属性の一覧を提示したが、データ利活用プロセスの全体におけるデータの属性の変化とイベントとの関係をより俯瞰的に示すために、図A.1-4のように、STEP 2までに作成している図に属性を記入する方法も効果的と考えられる。



図A.1-4 「属性」の提示方法の例

[20] 生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。（個人情報保護法第 26 条の 2（第 1 項））Cookie 等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴や、ある個人の商品購買履歴・サービス利用履歴が事例として挙げられる。

[21] 例えば、POS 端末にて生成された段階では個々の「販売データ」は必ずしも特定の個人を識別可能な情報とは言えないが、店舗内の業務用端末に格納される「販売集計データ」は、同端末にて管理される会員情報と照合することで容易に特定の個人を識別し得るデータとなる。

A-1-4 STEP 4 「イベント」ごとのリスクポイントの洗い出し

- *設定された「場」という観点から、「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビューする。*
- *その際、機密性・完全性・可用性といったサイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要がある。*

A-1-4-1 「イベント」ごとのリスクポイントの洗い出し

STEP 4は、STEP 3までに理解したデータ利活用プロセスにおいて、セキュリティ及び関連する法制度等の観点からいかなるリスクが想定されるかを特定する段階である。セキュリティの保護に係る観点（機密性、完全性、可用性）及び関連する法制度等の観点（パーソナルデータ保護、知的財産（営業秘密を含む）保護）から、例として、本ユースケースのうち、図A.1-4に示す「販売集計データ（ECサイト）」の「生成・取得」及び付随する「保管」のプロセスに関して以下のようなリスクを想定することができる[22]。下記と同様の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

表A.1-2 「販売集計データ（ECサイト）」の「生成・取得」及び「保管」にて想定されるリスクの例

大分類	中分類	「販売集計データ」の「生成・取得」及び「保管」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 販売集計データが保管された社内 DB サーバが悪意ある第三者により不正アクセスされ、同データが漏えいする。 ● 社内サーバに保管された販売集計データが、正規の従業員により故意に持ち出される。
	完全性	● 正規ユーザーへのなりすましにより、不正な商品取引が実施される。 ● 社内サーバに保管された販売集計データが、正規の従業員により故意に改ざんされる。

[22] 考慮すべきリスク（脅威）を網羅的に抽出する際に適用できる既存の枠組み等については、添付 B を参照されたい。

	可用性	● サービス妨害攻撃等により EC サイトにおける取引が一時的に停止する。 ● 販売集計データが保管された社内サーバがマルウェアに感染し、同データが暗号化される等して利用できない。 ● EC サイト運用に係る設備や機器に不具合が生じ、取引が一時的に停止する。 ● 地震や津波等の自然災害により EC サイト運用に係る設備や機器に被害が生じ、取引が一時的に停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 規約等において生成・取得する販売データの利用目的が明確に示されていない、又は利用の実態と対応していない。 ● 販売集計データを取扱う従業員を適切に監督していない。
	知的財産（営業秘密を含む）保護	● 販売集計データが悪意のある第三者により不正な手段で取得され、開示、使用される。
	・・・	・・・

なお、リスクを特定した後で、かかるリスクの低減に資する「属性」項目を再度レビューし、必要に応じてSTEP 3の成果に追加等することができる。

A-1-4-2 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて、X社は自社のデータ利活用の具体的な姿やその中に潜むリスクを適切に理解し、継続的にリスク管理を改善するための基礎を強化することができる。具体的に示唆される改善の内容は、X社による現状のデータ管理の実態に応じて多岐にわたると考えられるが、例えば以下が含まれる可能性がある。

- 各物理店舗等におけるデータ取扱いに対するガバナンス強化

  国内に多数存在する各物理店舗においては「販売データ」や「販売集計データ」といった個人に関連する情報を取扱うものの、統合データ基盤やECサイト等とは異なり、一律の高度なデータ保護水準を確保することが難しい場合も想定される。本ユースケースでは、そうした懸念に対応するため、各物理店舗では別途収集される会員情報との照合をせず、各店舗では個人データの取扱いをしないこととしているが、かかる管理をより確実なものとすべく、各物理店舗の個人利用に関するニーズを確認したうえで、統合データ基盤で管理される会員情報に対する各物理店舗等によるアクセス状況のレビュー、アクセス制御ポリ

シーその他の運用規定のレビュー等を行うことが具体的な施策として検討され得る。

- マーケティング部門等におけるデータ利用の実態を踏まえた保護施策の検討
  図A-1.2に示されている利用形態に限らず、統合データ基盤にて管理される「統合販売データ」等の利用実態や自社の個人情報保護方針や会員規約等の記載事項（例：利用目的に関する条項）との対応状況を確認し、当初提示していた利用目的との乖離が存在する、あるいは将来的に予想される場合に、例えば以下のような施策を検討することが可能と考えられる。

ー 個人情報保護方針や会員規約等における関係規定（例：利用目的に関する条項）の改定、顧客への通知、その他の必要な手続きの実施
ー 「統合販売データ」等の仮名加工情報、匿名加工情報への加工及び利用

A-2 高齢者生活支援事業の提供

昨今、消費者向け製品のIoT化に伴い、家電やウェアラブル、センサー等の多様な機器で生活情報を収集できるようになっており、「子育て世代、高齢者、単身者など、様々なライフスタイル／ニーズにあったサービスをIoTにより実現する新しい暮らし[23]」と定義されるスマートホームが急速に普及していくと見込まれている。

かかるスマートホームの実現に向けた具体的な取組の例として、宅内や施設内から収集したデータを活用した高齢者生活支援サービスの提供が挙げられる。高齢者向けの生活支援に関しては、かねてより住まい・医療・介護・予防・生活支援が一体的に提供される「地域包括ケアシステム」の実現が標榜されてきたが、在宅高齢者の生活実態や健康状態を正確に把握するデータが不足していることもあり、高齢者を支えるサービスが質・量ともに不足している点が課題だと認識されてきた。

上記の背景を踏まえ、スマートホーム分野に係る本フレームワークのユースケースとして、複数の事業者が保有するデータを活用した高齢者生活支援事業（A-2内において、以下、「本ユースケース」という。）を取り上げる[24]。

- 一般的な戸建て住宅や有料老人ホーム等に設置される多数の機器群を通じて、高齢者の生活や健康の状況に関するデータが生成され、各機器ベンダー（A社～D社）の運用するサーバに蓄積される。
- 各機器ベンダーは一定の収益を得る代わりに、第三者（プラットフォーム事業者）の運用するデータ基盤に各々が収集したデータを提供する。各機器ベンダーから提供されたデータは特定の個人を特定できない形でデータ基盤上に集約され、高齢者の生活リズム情報や安否情報というより高次なデータへと加工される。
- 高齢者の生活リズム情報や安否情報等のデータは、必要に応じてサービス事業者等に第三者提供され、データ主体の個人と紐づけたうえでより高度な支援サービスの提供等に活用される。サービス事業者等は、見守りサービス等の提供のため、各種機器から取得したデータを特定の住まい手に紐づけて取扱う点や機器から取得したデータの利活用プロセス等

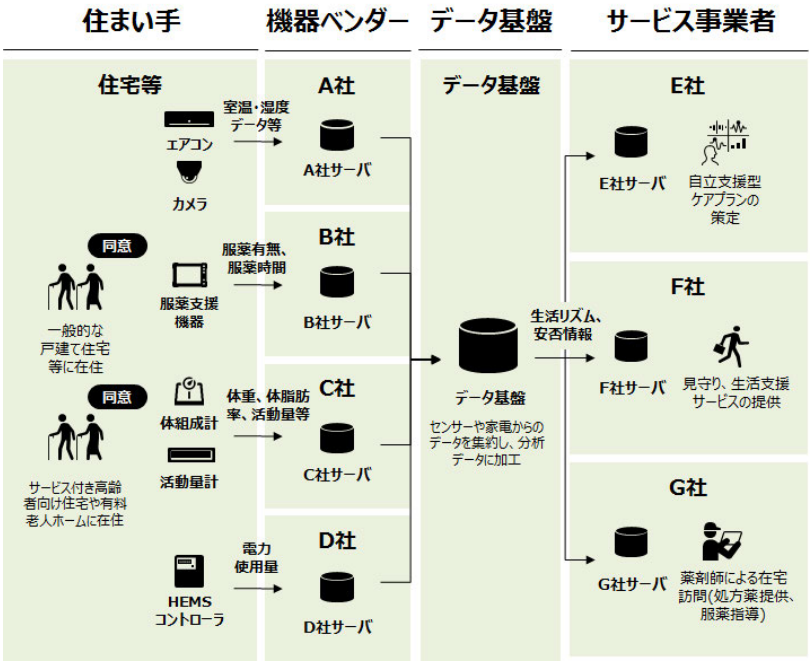
---

[23] 『「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました』（https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html）

[24] 本ユースケースに係る詳細については、「２０１８年度成果報告書　IoT を活用した新産業モデル創出基盤整備事業　研究開発項目 ⑥IoT 技術を活用したライフデータの高度利用システムの開発　IoT 家電・センサーからのライフデータによる高齢者の生活サポートサービス基盤の研究開発」を参照されたい。

についてあらかじめ同意を取得しているものとする。

- サービスの提供に直接的又は間接的に関わる機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている。



図A-2.1 対象プロセスの概要

本ユースケースにおいては、以下に示すとおり非常に多数のステークホルダーが存在しているが、取り扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、データの利用に係るサプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

- 住まい手：日常生活の中で各種IoT機器・サービス等を利用し、それに伴って生成される自身に関するデータを同意等の適切な手続きを経たうえで事業者に提供する。
  - 一般的な戸建て住宅等に在住する高齢者
  - サービス付き高齢者向け住宅や有料老人ホームに在住する高齢者
- 機器ベンダー（A社～D社）：宅内や施設内に設置されている機器を製造・販売し、本人同意等の適切な手続きを経たうえで各々運用中の機器から取得したデータを収集し、管理している。
  - A社：エアコンや見守りカメラ等の家庭用IoT機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
  - B社：処方薬の服薬有無や服用時間等をセンシングする服薬支援機器を製造・販売

し、収集したデータを自社サービスで活用することに加え、プラットフォーム事業者にも提供する。

- C社：体組成計や活動量計等のヘルスケア機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
- D社：スマートメータが実装された家庭向けに電力使用状況を可視化するサービスを提供し、収集したデータをプラットフォーム事業者にも提供する。

- プラットフォーム事業者：各住宅、施設に設置した機器等からのデータを集約し、適宜加工・分析等を実施する。
- サービス事業者（E社～G社）：プラットフォーム事業者からデータの提供を受け、より高度な高齢者支援サービスの提供等に活用する。

このような組織横断的なデータ利活用の仕組みを整備しようとする際、本フレームワークの活用を通じて、コンソーシアム等の場においてステークホルダー間でデータのライフサイクルの各工程において想定されるリスクに関する認識を共有し、各主体がそれぞれ実施すべき対策について他の主体と協議していく試みをより円滑なものとすることが望まれる。

A-2-1 STEP 1　データ処理フロー（「イベント」）の可視化

本ユースケースにおけるデータ処理フローは図A-2.2で示すように、以下のプロセスにより構成される。

(1) 高齢者の在住する宅内又は施設内に設置された機器類から、同意等の適切な手続きを経たうえで各種データが「生成・取得」され、各機器ベンダー（A社～D社）の管理するサーバへと「移転・提供」された後、「統合データ」として蓄積、保管される。これらのデータは取得時から各機器の識別情報に紐づけられ、当該機器が誰の住宅等に設置されているかは機器ベンダーからはわからないものとする。煩雑となるため図では割愛しているが、以下に示すように、宅内、施設内には複数の事業者が提供する多数の機器が設置されている。利活用上の需要に基づいて設置機器は増減する可能性があるが、住まい手や各機器ベンダー等は機器構成の変更を把握し、適切に管理することが望ましい。

表A-2.1 主な設置機器と収集データ

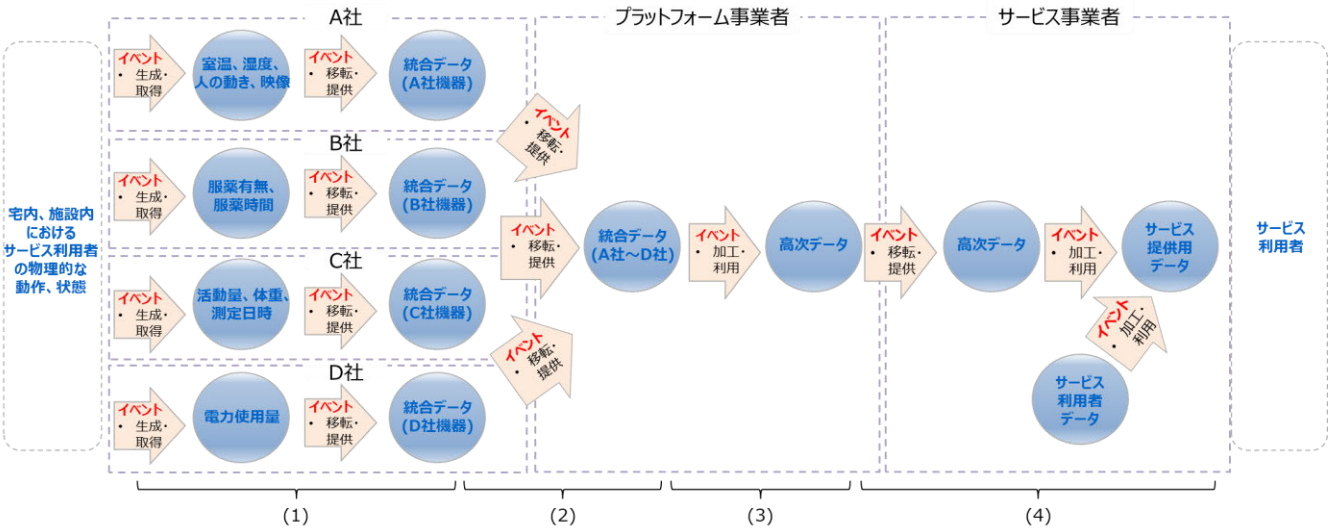
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動

		き）
	コミュニケーションカメラ	室温、人の動き、映像
B社	服薬支援機器	服薬有無、服薬時間
C社	活動量計	活動量、歩数
	体組成計	体重、測定日時
D社	HEMSを用いた電力使用量集約基盤	電力使用量

(2) 各機器ベンダーが保有する「統合データ」は、プラットフォーム事業者が運営するデータ基盤に「移転・提供」され、統合、保管される。統合データは、機器の識別情報に紐づく利用者識別情報に基づき管理されており、当該データから個人を識別することはできないように構成されているものとする。組織横断的なデータ利活用の仕組みを整備するという本検討の趣旨を踏まえ、ここでは、各機器ベンダーが個別に行う自社保有データの活用はフローから省略し、事業者間でのデータ移転・提供により焦点を当てることとする。

(3) 各社から提供を受けデータ基盤に集約された「統合データ」は、サービス提供事業者の利用に適する「高次データ」（例：生活リズム情報、安否情報）に「加工・利用」される。なお、（2）、（3）のプロセスにおいて、取扱うデータと特定の個人への紐づけは行われないものとする。

（4）「高次データ」は、プラットフォーム事業者から提供先事業者のサービス内容や個別の求め応じて必要な情報を検討したうえで「移転・提供」され、サービス事業者が別途保有しているサービス利用者データと突合され、「サービス提供用データ」に「加工・利用」される。



図A-2.2 データ処理フローの可視化（高齢者生活支援事業の提供）

A-2-2 STEP 2　必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、取扱うデータが「個人に関連した情報」である点や当該データが複数の事業者に提供され得る点等を考慮すると、例えば下記のルールや各社の必ずしも明文化されていないルール等が「場」として特定され得る。

（1）個人情報保護法： 本ユースケースで利用されるデータは住まい手（ここでは高齢者）という「個人に関する情報」であり、最終的に元の住まい手に対してサービスを提供するため、サービス事業者にて特定の個人を識別できるように加工されることから、個人情報保護法における「個人データ」又は「個人関連情報」等に該当すると考えられる[25]。「サービス提供用データ」が「個人データ」であるため、サービス事業者が個人情報取扱事業者に該当することに加えて、各機器ベンダーにより収集されるデータやプラットフォームに集約される「統合データ」は、匿名的な利用者識別情報や機器識別情報に基づいて必ずしも特定の個人に紐づかない形で管理されていることを仮定しているため、「個人データ」ではなく「個人関連情報」等に該当すると考えられる。当該データは提供先のサービス事業者において個人データとして取得されることが容易に想定されるため、各機器ベンダー及びプラットフォーム事業者においては、個人関連情報取扱事業者

[25] 対象のデータが、個人情報保護法上のいかなる情報の類型に属するかは、改正個人情報保護法の動向も踏まえつつ、適用主体において慎重な検討が必要である。

として本人からの同意取得の確認、提供元における記録等の義務が生じる点に留意が必要である。一方で、本ユースケースにおける想定とは異なって、各機器ベンダー又はプラットフォーム事業者が保有する「統合データ」が「個人データ」として管理され、サービス事業者に提供される場合、個人情報保護法第２３条第５項に示される事由に基づき、コンソーシアムに参加する事業者間で円滑に当該個人データの提供がなされるよう、例えば以下のような仕組みを導入することも想定される[26]。

- 委託（法第23条第5項第1号関係）
  提供元事業者（機器ベンダーやプラットフォーム事業者）が、利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部をサービス事業者等へ委託することを通じて、当該個人データの提供先を「第三者」に該当しないものとする。
- 共同利用（法第23条第5項第3号関係）
  機器ベンダー、サービス事業者等において共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称を、あらかじめ、本人に通知等することを通じて、当該個人データの提供先を「第三者」に該当しないものとする。

（2）機器利用規約：住まい手と各機器ベンダーとの間で締結される。本ユースケースにて収集されるデータはそれ単体では必ずしも「個人データ」に該当するわけではないが、住まい手からデータの取扱い（例：機器から取得したデータのプラットフォーム事業者への提供）等が規定された規約に対して同意を得ることも想定される。

（3）データ提供契約：本ユースケースでは、プラットフォーム事業者を介して各機器ベンダーとサービス事業者とのデータの流通がなされることで高度なサービスを高齢者に提供することが想定されている。データの流通には営業秘密の漏えいやプライバシーの侵害等のリスクが想定されるが、適切な契約上・技術上の措置を採ることによって各々の役割と責任分界を明確にしつつ、リスクの最小化に寄与できるとされている[27]ことから、以下２種類のデータ提供事象について、事業者間及び住まい手も含めた形で様々な条件等

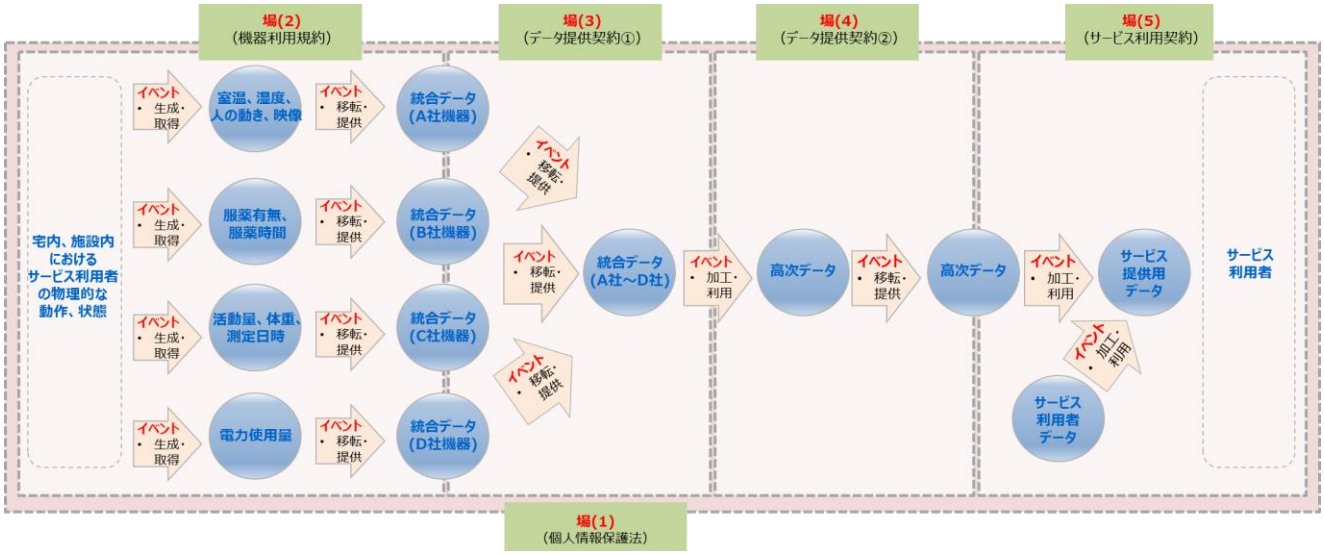
[26] 具体的な規定等については、「個人情報の保護に関する法律についてのガイドライン（通則編）」の「3-4-3 第三者に該当しない場合（法第 23 条第 5 項・第 6 項関係）」等を参照されたい。

[27] 契約にて考慮すべき事項の詳細については、「AI・データの利用に関する 契約ガイドライン 1.1 版」の「第 6 「データ共用型（プラットフォーム型）」契約（プラットフォームを利用したデータの共用）」を参照されたい。

を協議し、合意する必要がある。

- 機器ベンダーからプラットフォーム事業者への提供（図A-2.3における場（３））
  - プラットフォーム事業者に対してどのような内容のデータを提供するか
  - プラットフォーム事業者がどのような目的・方法で提供データを利用できるか
  - プラットフォーム事業者による加工処理等により生じる派生データの利用権限その他の成果物の取扱いはいかなるものか
- プラットフォーム事業者からサービス事業者への提供（図A-2.3における場（４））
  - 機器ベンダーから提供を受けたデータのうち、提供される予定のサービスの内容等を踏まえて、どの内容を個別のサービス事業者に提供するか
  - 各サービス事業者がどのような目的・方法でデータ、サービスを利用できるか
  - サービス事業者による加工処理等により生じる派生データの利用権限その他の成果物の取扱いはいかなるものか

（4）サービス利用契約：住まい手と各サービス事業者との間で締結され、サービスの内容や提供期間に加え、取得する個人データの取扱いに係る条項を含む。本ユースケースでは、サービス事業者が個別に取得する個人データに加えて、機器ベンダーが提供する多数の機器から住まい手に関するデータを取得することから、住まい手から見て全体のデータ利活用プロセスについて透明性を確保できるような説明を伴っていることが望ましい。



図A-2.3 必要な制度的な保護措置の整理（高齢者生活支援事業の提供）

A-2-3 STEP 3　「属性」の具体化

前STEPにて特定した「場」を踏まえ、各種データの管理に資する属性を特定する。本ユースケースにおいては、高齢者という個人に関する情報を取り扱うことから、属性の検討に際しても個人情報保護法制はまず参照されるべきルールとなる。加えて、開示範囲やデータ管理主体、利用期限等の事業者間の責任分解にも関連する内容を特定する際には、当事者間で締結される各種契約・規約が有用である。

表A-2.2 「属性」の検討において考慮すべきルール（場）

		個人情報保護法	機器利用規約	データ提供契約	サービス提供契約
カテゴリ	パーソナルデータ保護	○			
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○	○	○	○
データ管理主体			○	○	○
データ権利者		○	○	○	○
価値（重要度）			○	○	○
媒体・保存先			○	○	○
利用期限			○	○	○

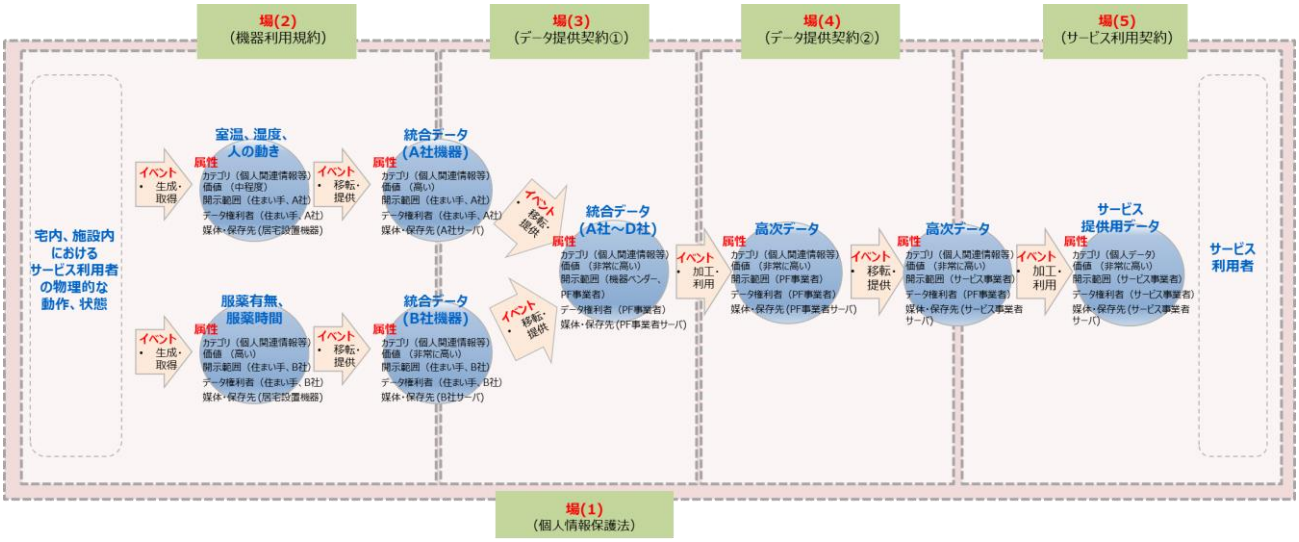
本ユースケースにて取扱われるデータの多くは個人データ又は個人関連情報等に該当する。機器から収集したデータは、別途利用者データ等と突合されない場合は「カテゴリ」が個人関連情報等に該当すると考えられるが、第三者提供先において個人データとなることが想定されるかどうか、その場合に本人同意が得られていることが確認できているかどうかが重要となるため、後述するように、上記に示した属性項目とは別途同意の取得状況等が管理されていることが望ましい。上記の事項を考慮して具体化した本ユースケースで取り扱うデータがとり得るパラメータの例を以下に示す。

表A-2.3 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		統合データ（A 社）	統合データ（A 社～D 社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産（営業秘密を含む）保護	営業秘密（A 社）	営業秘密 等[28]（PF 事業者）	営業秘密 等（PF 事業者）	営業秘密（サービス事業者）
	…	…	…	…	…
開示範囲		A 社内	PF 事業者内	PF 事業者内	サービス事業者内
利用目的		• 取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A 社	PF 事業者	PF 事業者	サービス事業者
データ権利者		住まい手、A 社	住まい手、機器ベンダー、PF 事業者	住まい手、PF 事業者	住まい手、サービス事業者
価値（重要度）		高い	非常に高い	非常に高い	非常に高い
媒体・保存先		A 社サーバ	PF 事業者サーバ	PF 事業者サーバ	サービス事業者サーバ
利用期限		特になし	データ提供契約終了から 1 年	データ提供契約終了から 1 年	サービス提供期間終了まで

[28] 表 A-2.3 のデータのうち、特定の事業者間で共有されるものについては、不正競争防止法上の「限定提供データ」に該当する場合も想定される。

上記では表形式でデータとその属性の一覧を提示したが、データ利活用プロセスの全体におけるデータの属性の変化とイベントとの関係をより俯瞰的に示すために、STEP 2までに作成している図に属性を記入すると図A.2-4のようになる。



図A.2-4 「属性」の提示方法の例

A-2-4 STEP 4 「イベント」ごとのリスクポイントの洗い出し

A-2-4-1 「イベント」ごとのリスクポイントの洗い出し

ここまでで特定したデータ利活用フローや認識すべきルール（場）、データの管理に資する属性の内容を踏まえ、本ユースケースのうち、図A.2-2に示す各機器ベンダーが保有する「統合データ」の「移転・提供」プロセスに関して以下のようなリスクを想定することができる。下記と同様の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

前述したように、本フレームワークでは、対象の移転・提供事象について、４つの単位（国・地域・組織・人、システム・サービス、機器）の単位でリスクを整理することが可能としているが、本ユースケースにおいては一例として以下のようなリスクが特定され得る。

＜国・地域＞

- 国や地域をまたがるデータの移転・提供は想定していないため、非該当

＜組織・ヒト＞

- 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。
- プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。

＜システム・サービス＞

- 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。

＜機器＞

- 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。

表A.2-4 各機器ベンダー「統合データ」のPF事業者への「移転・提供」にて想定されるリスクの例

大分類	中分類	各機器ベンダーが保有する「統合データ」の PF 事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤の API を無作為に呼び出すような DoS 攻撃を行い、プラットフォーム事業者サーバの処理が停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。 ● プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。
	知的財産（営業秘密	● 各社の統合データが悪意のある内外の主体により不正な手段で取得され、開示、使用される。

	を含む）保護	
	・・・	

なお、本ユースケースのように提供先において高度なサービス提供等のために個人関連情報等が個人データとして取得されることが想定される場合、「機密性」や「パーソナルデータ保護」等の観点でより影響度の大きいリスクが顕在化する可能性がある。そのようなリスクには、通常サイバーセキュリティの文脈で着目される外部の攻撃者によるデータ漏えい等だけでなく、正規の事業者によるデータの不正利用（意図的なものと非意図的なものの双方を含む）が含まれる。本ユースケースでは、関連する規定を考慮すると、A-2-3にて述べたものに加えて、当該データの処理に関する同意の取得状況、有効性等を管理すべき属性として指定し、関連する組織等のポリシーやシステムに管理の仕組みを設計・構築等することでプライバシー保護に係るリスクの低減に資することが想定される。

A-2-4-2 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて明らかになったように、本ユースケースでは様々な機器によるデータの収集からその加工、最終的な利用に至るまで多数の事業者が関与しており、そのように複雑なビジネス構造には事業者間の相互依存性等に根差す特有のリスクも想定される。こういった体制が事前に予見されている、又は現に行われている場合、コンソーシアム等の枠組みを活用して、参画する各社が相互に連携してリスクを低減する試みを進めることが有効になると考えられる。そこで必要になる対策は、複雑なデータ利活用の実態を踏まえれば非常に多岐にわたると考えられるが、例えば以下が含まれる可能性がある。

- 複雑なデータ利活用プロセスに配慮した利用目的の提示や同意の取得等
  本ユースケースのような多数の機器、サービス、事業者が関与する複雑なビジネス構造の中では、データ主体である住まい手に対してデータ利活用プロセスの透明性を確保することがより困難なものとなる。本ユースケースにおいて健康状態や詳細な行動ログ等の機微なデータが活用されるという点も踏まえれば、最悪の場合、サービスの継続に係る課題につながる可能性もある。そのようなデータ利活用の透明性に関連したリスクを低減するためには、データ主体（ここでは高齢者を含む住まい手）に対する、各事業者の役割を含む

サービスの全体像及びデータ主体が得られる効用や、統合的な個人データ等の取扱いポリシーの提示、それらに関する理解しやすい説明等が重要である。一方で、それらの取組は事業者やサービスの利用者に一定の負担をかけるものだが、いわゆる「同意疲れ」等の問題も指摘されていることから、そのような負担にも配慮した方法が検討されることが望ましい。

- 機微なデータの生成・取得に関連し得る各種IoT機器におけるセキュリティ等の確保
  本ユースケースでは、特にデータの「生成・取得」段階において、エアコンや服薬支援機器、活動量計等の製造者の異なる多数の機器が利用される。それらのデータが集約され、統合的に処理される情報システムのセキュリティ管理は従来から課題視される傾向にあるが、一方でそれらのデータを生成・取得する末端のIoT機器については、それらがデータの信頼性を確保しようとするにあたり重要な構成要素であるにもかかわらず、セキュリティ等の確保に向けた対処は未だ途上にある場合が多いと考えられる。機器によっては個人に関する比較的機微なデータを取扱う可能性があることから、想定されるリスクやその程度を踏まえつつ、各機器ベンダーにおいて適切な水準のセキュリティ対策を実装し、それらを取りまとめる事業者やサービス利用者はその旨を確認することが望ましい。

A-3　IaaS、PaaS、SaaS等を利用してサービスを提供する例

デジタル技術を活用した価値創出の推進が社会的な課題と認識される中、重要な基盤技術の一つとしてクラウドコンピューティング技術に注目が集まっており、ますます多くの利用者がクラウドサービスを利用するようになっている。かかるサービスの適切な利用を通じて、利用者は費用負担や導入にかかる時間的コストの効率化、セキュリティ水準や技術革新対応力、柔軟性の向上等のメリットが得られると考えられている[29]。

従来から課題として認識されていたセキュリティ水準等の懸念が、クラウドインフラのセキュリティ向上や利用者支援機能の充実等を通じて低減されてきた一方で、サービス提供者と利用者との間の責任分界に対する認識が不十分であることに起因するクラウド利用者自身の設定ミス等によるインシデントの増加、システムの複雑化に伴うデータの地理的所在等の透明性の不足等の課題が残存している点が指摘されている[30]。

上記の背景を踏まえ、事業者間の責任分界の明確化やデータフローの透明性確保に資する検討の例として、クラウドサービスを利用した以下の流れによるデータの利活用プロセス（A-3内において、以下、「本ユースケース」という。）を取り上げる。

- サービス・物販事業を運営するA社は、従来から行っている物理店舗を通じた製品・サービスの提供に加え、近年は会員用ポータルサイトの構築や顧客管理サービス（SaaS）の利用等を通じた更なる顧客価値の向上に取り組んでいる。
- 顧客はA社の運用するポータルサイトに登録、ログインした上で画像・動画データを自身のPCやスマートフォンにダウンロード等できる。また、顧客はポータルサイト経由で、関連する商品を購入することもできる。従来、画像・映像はA社従業員がCDやDVD等の媒体にコピーしたうえで顧客に郵送等していたが、本システムの導入により顧客への画像・映像の受け渡しにかかる工数が大幅に削減され、顧客としても撮影した画像・動画データを複数の端末から閲覧でき、自らの趣向に合わせて加工したりダウンロードしたりできる等のメリットが得られる。
- A社のポータルサイトはB社の提供するPaaS（Webアプリ開発・運用基盤）上に構築され

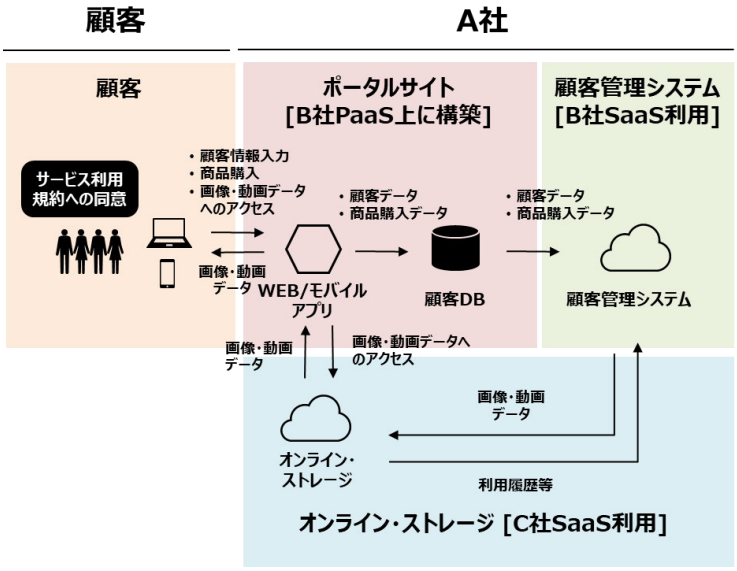
---

[29] 『政府情報システムにおけるクラウドサービスの利用に係る基本方針』（https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20210330kihon.pdf　）

[30] クラウドサービス利用にかかわるリスクに関しては、経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版附属書」の「A（参考）クラウドサービス利用にかかわるリスク」、Cloud Security Alliance (CSA)「クラウドの重大セキュリティ脅威 11 の悪質な脅威」」等を参照。

ており、そこで取得される会員情報や商品購入情報等はポータルサイトを構成する顧客DBに格納されるだけでなく、B社より別途SaaSとして提供され商品の販売管理等を行うA社顧客管理システムにも共有される。

- A社は、顧客が画像・動画データをC社の提供するSaaSを利用した自社のオンライン・ストレージにアップロードする。上述のとおり、顧客はポータルサイト経由で同ストレージにアクセスし、画像・動画データをダウンロードしたり、加工したりすることができる。データのダウンロード等の履歴は顧客管理システムに定期的に共有される。



図A-3.1 対象プロセスの概要

本ユースケースでは、A社がPaaSやSaaS等の性質の異なる複数のクラウドサービスを利用しているが、A社が上記のスコープにて適切な水準のセキュリティ等の信頼性を確保しようとする際に、考慮すべきステークホルダーとして以下が挙げられる。

- 顧客：A社が提供するポータルサイトにアクセスし、画像・動画データの加工、ダウンロードや関連商品の購入を行う。
- A社：サービス・物販事業等を業として行い、顧客価値を高めるための試みとしてクラウドサービスカスタマ[31]としてB社やC社から提供される各種クラウドサービスを利用しつつポータルサイトや顧客管理システム等を構築、運用している。

[31] クラウドサービスカスタマ（cloud service customer）とは、「クラウドサービスを使うためにビジネス関係にあるパーティ」を指す。(ISO/IEC 17789:2014) クラウド利用者とも呼ばれる。

- クラウドサービスプロバイダ[32]：A社に各種のクラウドサービスを提供する事業者
  - B社：ポータルサイト向けにWebアプリ開発・運用基盤をPaaSとして、顧客管理システム・サービスをSaaSとしてA社に提供する。
  - C社：画像・動画データを格納するオンライン・ストレージサービスをSaaSとしてA社に提供し、ピアクラウドサービス[33]としてB社の提供するサービスの基盤となっているIaaSも別途提供している。
- クラウドサービスパートナー：B社PaaS上にポータルサイトを構築することに加え、各サービス間の連携部分を開発する。

上記に示すように、本ユースケースではクラウドサービスカスタマであるA社と直接契約するB社が当該契約上は第三者であるC社のIaaSを利用してPaaSやSaaSを提供しているという「クラウドサプライチェーン」がある。クラウドサービスのサービスモデルの分類[34]を参照しつつ、本ユースケースにおけるクラウドサービス提供に係るサプライチェーンの概要を示したものが図A-3.2である。一般にこうしたクラウドサプライチェーンにおいては、以下のような課題が生じ得る[35]ために、クラウドサービスプロバイダ及びクラウドサービスカスタマの双方において適宜情報開示や適切な契約等に基づく監査の実施等の対策[36]を行うことが望ましい。

- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、配下に存在する PaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。
- 障害が要因となり事業活動に何らかの損害が生じた場合に事業者間で責任分界があいまい

---

[32] クラウドサービスプロバイダ（cloud service provider）とは、「クラウドサービスを利用できるようにするパーティ」を指す。(ISO/IEC 17789:2014)

[33] ピアクラウドサービス（peer cloud service）とは、「一つのクラウドサービスプロバイダのクラウドサービスであって、他の一つ以上のクラウドサービスプロバイダのクラウドサービスの一部として使用されるクラウドサービス」を指す。(ISO/IEC 17789:2014)

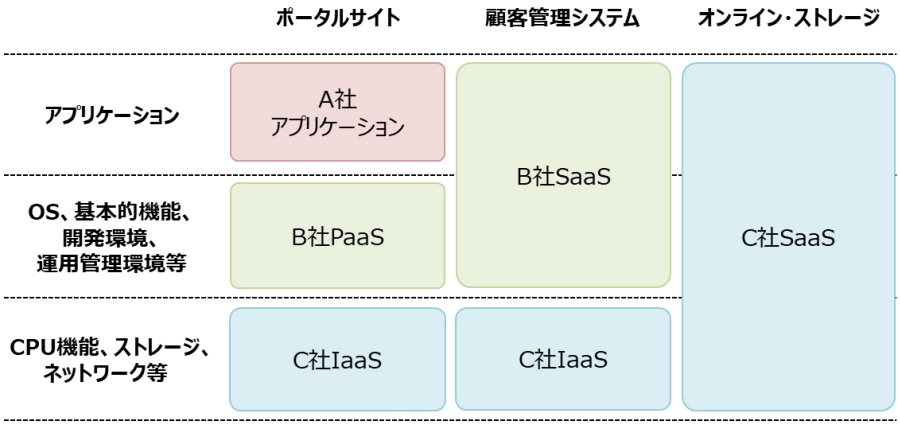
[34] サービスモデルの分類を定義する主な文献として、米国国立標準技術研究所（NIST）「NIST によるクラウドコンピューティングの定義」や各府省情報化統括責任者（ＣＩＯ）連絡会議決定「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等を参照

[35] 経済産業省「クラウドセキュリティガイドライン活用ガイドブック 2013 年度版」

[36] 具体的な取組みの例として、ホワイトペーパーの活用、確認等によるクラウドセキュリティ認証制度（例：ISMS クラウドセキュリティ認証、政府情報システムのためのセキュリティ評価制度（ISMAP））の認証基準への対応状況の確認や、既存の監査報告書（例：SOC2 報告書）の活用、個別の調査等による確認が挙げられる。

になりやすい。

- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、カスタマの意図に反する状態に陥ってしまう。



図A-3.2　クラウドサービス提供に係るサプライチェーンの概要

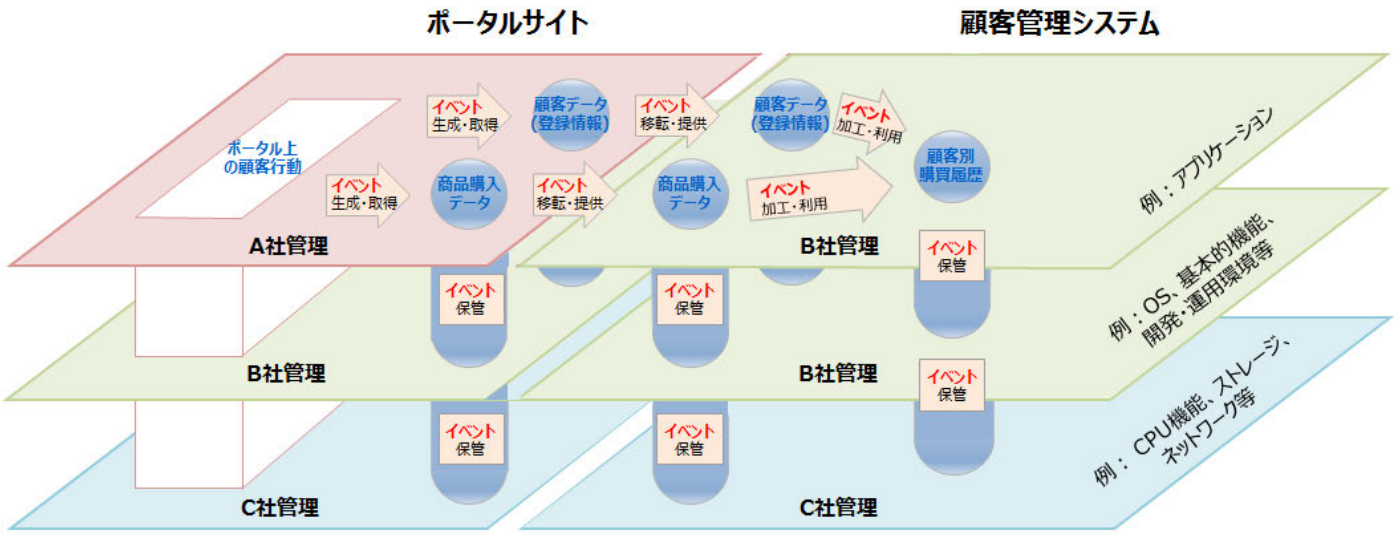
A-3-1 STEP 1　データ処理フロー（「イベント」）の可視化

本ユースケースにおけるデータ処理フローは図A-3.3で示すように、以下のプロセスにより構成される。本節以降では、特に（2）のプロセスについて、データ処理フローの可視化、必要な制度的な保護措置（「場」）の整理等を行う。

(1) 適切な契約等に基づいて、顧客の画像・動画データが「生成・取得」され、A社従業員によりC社の提供するオンライン・ストレージへ「移転・提供」され、「保管」される。画像・動画データは、顧客からの求めに応じて「加工・利用」（オンライン・ストレージ上での画像編集等）されたうえで顧客所有の端末（PC、スマートフォン等）に「移転・提供」される。

(2) ポータルサイト上では顧客による自身のデータの入力や製品等の注文、その他の行動に応じて、「顧客データ」、「商品購入データ」等が「生成・取得」され、顧客DBに格納される。当該データは、適時にB社が提供する顧客管理システムに「移転・提供」され、A社内の個別のニーズに応じてA社従業員により「加工・利用」される。フローを可視化する際は、ポータルサイトはC社がIaaSとして提供する物理・仮想インフラ（CPU機能、ストレージ、ネットワーク等）上にOS、開発環境、運用環境等を整備したB社PaaS上に構築されている点に留意する必要がある。

前述したように、本ユースケースのように複数の事業者のサービスからなるサプライチェーンを編成したクラウドサービスを利用する場合、その複雑性等に起因する特有のリスクが想定される。そのため、データ処理フローや必要な制度的な保護措置（「場」）を整理し、想定されるリスクを可能な限り網羅的に特定しようとする際には、必要に応じて、クラウドサプライチェーンの透明性の確保や責任分界の明確化という観点から、多層的なサービスの提供体制を踏まえた検討を実施することが望ましい。サービスの多層性を表現する際の観点は様々なものが考えられ得るが、図A-3.3では、一例として図A-3.2と同様の分類に基づいて、①アプリケーション、②OS、基本的機能、開発・運用環境等、③CPU機能、ストレージ、ネットワーク等の３つの異なる観点から各社の責任分界を含む「場」を示し、それらが一体となってデータ処理（イベント）を実施している態様を記述している。



図A-3.3 データ処理フローの可視化イメージ（IaaS、PaaS、SaaS等を利用したサービス）

A-3-2 STEP 2　必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、顧客データ等が個人データに該当する点や、当該データを処理、管理するシステムが複数のクラウドサービスを組み合わせて実現されている点等を考慮すると、例えば下記のルールや各社の必ずしも明文化されていないルール等が「場」として特定され得る。

（1）A社サービス利用規約等：A社は顧客との間でポータルサイトの利用等に関連して規約を設定し、同意を得る必要がある。規約又は別途定められる個人情報保護方針等にはサービスの内容や利用に際しての禁止事項、免責事項等に加え、氏名、住所、連絡先等の

顧客データ（登録情報）や画像・動画データの保護に関する規定が含まれるべきである。かかる規定は、本ユースケースにおいて該当する個人データを取扱うすべてのプロセスにおいて遵守されるべきものである。

（2）個人情報保護法：A社が顧客から取得する顧客データや結果として取得される顧客別購買履歴は個人データに該当すると考えられることから、A社は個人情報取扱事業者に課せられる規律を遵守する必要がある。また、A社によるB社及びC社提供クラウドサービスの利用が、個人データの第三者提供に該当するかどうか（B社及びC社が個人情報を取扱うかどうか）、該当する場合はそれがB社又はC社への「委託」にあたるか、本人からの同意を得る必要があるか[37]、当該提供行為が「外国にある第三者への提供」にあたるかどうか等を確認し、その結果に応じて適切な管理を行うことが必要となる。本ユースケースにおいては、①ポータルサイトの開発・運用に関連して利用されているB社及びC社のサービス、②顧客管理システムの開発・運用に関連して利用されているC社サービスでは、サーバに保存された個人データを取り扱わない旨を契約条項により定め、適切にアクセス制御を行っているものと想定する。

（3）各種クラウドサービス利用規約：本ユースケースにおけるA社の各種システムはB社及びC社が提供するクラウドサービスを利用して開発・運用されているが、前述したクラウドサプライチェーンやそれに係るリスクを踏まえた検討を行う場合、関連するクラウドサービス利用規約等を「場」として特定することが望ましい。ここで、特定されるべき規約等としては例えば以下があると考えられる。

- A社がポータルサイトを運用するために必要なA社とB社、及びB社とC社とのサービス利用規約（それぞれを、「B社PaaS利用規約」、「C社IaaS利用規約」と呼ぶ）
- A社が顧客管理システムを利用するために必要なB社の規約（B社SaaS利用規約）、

---

[37] クラウドサービスの利用が、「本人の同意が必要な第三者提供」または「委託」に該当するかどうかは、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準になるとされる。その際、クラウドサービスプロバイダが、個人データを取り扱わないこととなっている場合としては、「契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等」が想定される。当該クラウドサービスプロバイダが、個人データを取り扱わないこととなっている場合には、個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はないとされる。［個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A Q7－53］

及びB社に物理・仮想インフラ（CPU機能、ストレージ、ネットワーク等）を提供するC社の規約（C社IaaS利用規約）

- A社のポータルサイトと顧客管理システムとのデータ連携機能（B社提供）の運用に係る契約

また、上記規約等により規定される各組織のセキュリティに関する役割と責任を明確化しておくことが望ましい。例えば、A社がB社の提供する顧客管理システム（SaaS）を利用する際、各種ハードウェアやOS、ミドルウェア、アプリケーションへの脆弱性対応等の各種セキュリティ対策についてはB社又はC社が担うが、SaaSを利用する端末におけるセキュリティ対策やファイルの開示範囲等の設定、社員等のアカウント管理、認証・認可等の対策は一般的にA社側で実施する必要がある。自組織の役割と責任、その履行状況等を正確に把握できないことは、意図せざるセキュリティインシデントの発生につながり得るものであり、関係者のそれぞれにおいて慎重に検討、対処されることが望ましい。

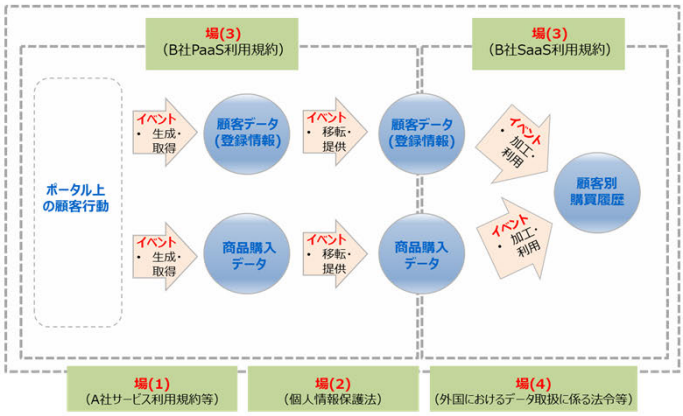
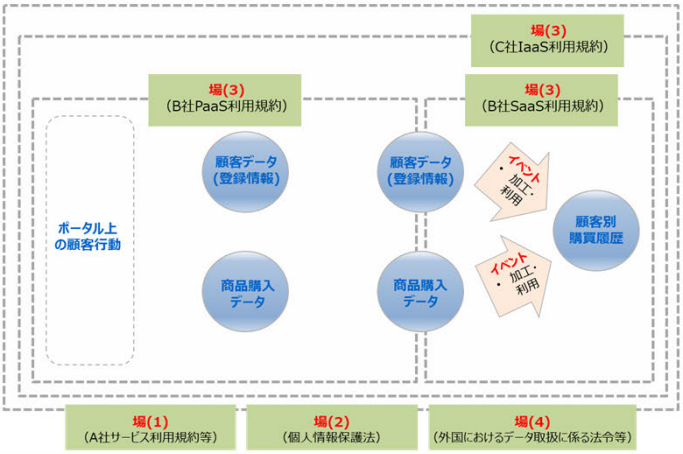
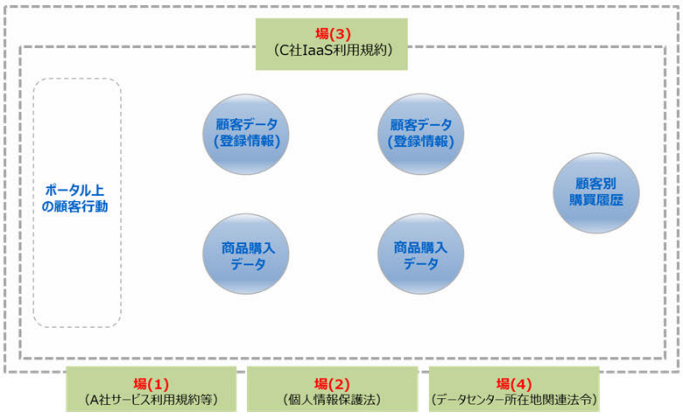
（4）データセンター所在地関連法令（外国におけるデータ取扱に係る法令等）：

インターネット経由でクラウドサービスが提供される場合、サービス運用コスト等の関係でデータセンターが海外に所在しているケースが珍しくないが、当該サービスの提供者及び利用者が「場」を明確にするという観点からは、セキュリティインシデント等の事象が発生した際にどの国の法律に基づき、どの国の裁判所の判断を仰ぐ必要があるのかを認識することが重要である。私法[38]関係はクラウドサービスカスタマとクラウドサービスプロバイダとのサービス提供契約等において準拠法の指定条項や合意裁判管轄条項が含められていることが一般的である。一方で、公法関係は原則として属地主義が採用されるため、クラウドサービスカスタマのデータがデータセンター所在国の捜査機関により捜索押収される等の想定外のリスクが顕在化する恐れもあり、その場合は本ユースケースにおけるあらゆるステークホルダー（例：A社、A社サービスを利用する個人）が影響を被り得る。上記に関連して、A社及びB社におけるクラウドサービス等の利用に際しては、外国におけるデータ取扱に係る法令等に関連して具体的な争訟リスクが予見されるかどうかも考慮して、データセンターの所在地を含めたサービスの検討がなされる

[38] ここで、公法とは、「国家と私人との法律関係」を規律する法であり、私法は「私人と私人との法律関係」を規律する法を指すものとする。

ことが望ましい。

図A-3.4において、上記で特定した（1）から（4）の場を、図A-3.2に示した各事業者の責任分界を念頭に置きつつ、関連する事業者ごとに各々の立場から整理している。なお、図中におけるイベントの記載有無は、対象の事業者が当該イベントの実施に対して責任を有しているかどうかを示している。

事業者ごとの観点を踏まえた整理	必要な制度的な保護措置の整理例（IaaS、PaaS、SaaS等を利用したサービス）
A社から見た整理	
B社から見た整理	
C社から見た整理	

図A-3.4 必要な制度的な保護措置の整理例（IaaS、PaaS、SaaS等を利用したサービス）[39]

[39] 図中の破線部はポータルサイト及び顧客管理システムで同一の規範が適用され得る範囲を示し、実線部は両者で別個の規範が適用され得る範囲を示している。

A-3-3 STEP 3 「属性」の具体化

本ユースケースにおいては、顧客本人又は関連する人物が映った画像・動画データを取り扱うことから、A-2と同様に属性の検討に際して個人情報保護法制はまず参照されるべきルールとなる。加えて、データの開示範囲やデータ管理主体、利用期限等の利用上の制約に係る事項を特定する際には各種クラウドサービス利用規約の条項、媒体・保存先の適切性等を検討する際にはデータセンター所在地関連法令等を参照することが有用である。

表A-3.1 「属性」の検討において考慮すべきルール（場）

		A 社サービス利用規約等	個人情報保護法	各種クラウドサービス利用規約	データセンター所在地関連法令
カテゴリ	パーソナルデータ保護	○	○		
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	
利用目的		○	○	○	
データ管理主体		○	○	○	
データ権利者		○	○		
価値（重要度）		○	○		
媒体・保存先				○	○
利用期限		○		○	

上述したとおり、顧客データや商品購入データ、画像・動画データがいずれも個人データに該当することから、データ権利者は顧客自身となり、A社は個人情報取扱事業者の義務の一環として顧客からの「開示等の請求等」[40]に適切に対応する必要がある。また、顧客管理システムの開発・運用に関連して利用されているC社サービスでは、サーバに保存された個人データ

[40] 個人情報の保護に関する法律（最終改正：令和 2 年 6 月 12 日法律第 44 号）第 32 条を参照

を取り扱わない旨を契約条項により定め、適切にアクセス制御を行うとされていることから、実質的にデータへアクセスし、一定の管理責任を有しているA社、B社をデータ管理主体として設定している。なお、本ユースケースのように複数のクラウドサービスプロバイダが分業して特定のサービスが提供される場合、A社のようなクラウドサービスカスタマはC社のような事業者を必ずしも認知せずサービスを利用する状況になり得る。特に、関連する法制度や組織内のポリシー等でデータの所在地に制約を課しているようなケースでは、契約前にクラウドサービスプロバイダ（本ユースケースにおいてはB社）に対して情報の開示を要求し、下記の媒体・保存先に相当するデータの所在地等に関する情報を収集しておく必要がある。

表A-3.2 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		顧客データ[41]	商品購入データ	画像・動画データ
カテゴリ	パーソナルデータ保護	個人データ	個人データ	個人データ
	知的財産（営業秘密を含む）保護	A 社の営業秘密	A 社の営業秘密	-
	…	…	…	…
開示範囲		A 社、顧客	A 社、顧客	A 社、顧客
利用目的		• 顧客への各種サービスの提供 • 顧客からの問合せへの対応 • 顧客への広告・メールマガジンの送付		• 顧客への各種サービスの提供
データ管理主体		A 社、B 社	A 社、B 社	A 社
データ権利者		顧客	顧客	顧客
価値（重要度）		高い	高い	高い
媒体・保存先		B 社 SaaS（C 社 IaaS）	B 社 SaaS（C 社 IaaS）	C 社 SaaS
利用期限		会員契約終了から 2 年	会員契約終了から 2 年	撮影後 2 年間

[41] A-3-3 では、「顧客データ」及び「商品購入データ」として、A 社顧客管理システム内に保管されているデータを専ら取り扱う。「顧客データ」には、識別子、認証情報、住所、氏名、メールアドレス等を含む。

A-3-4 STEP 4　「イベント」ごとのリスクポイントの洗い出し

A-3-4-1 「イベント」ごとのリスクポイントの洗い出し

STEP 3までの検討事項を踏まえ、以下では本ユースケースのうち、図A.3-4に示すA社がB社により提供される顧客管理システム上で取扱う「顧客データ」の「加工・利用」及び「保管」のプロセスに関して以下のようなリスクを想定することができる。A-1及びA-2と同様、下記の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

表A.3-3 顧客管理システムにおける「顧客データ」の「加工・利用」「保管」で想定されるリスク（例）

大分類	中分類	A 社が B 社により提供される顧客管理システム上で取扱う「顧客データ」の「加工・利用」及び「保管」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある外部の主体がパスワードリスト攻撃等により A 社従業員になりすまし、顧客管理システムに保管された顧客データを外部に漏えいさせる。 ● 悪意のある外部の主体が顧客管理システム（B 社 SaaS）の脆弱性を悪用して顧客管理システムに不正アクセスし、顧客データを外部に漏えいさせる。 ● A 社従業員による B 社 SaaS のアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に顧客データが開示される。 ● 国内又は国外の司法機関等からの求めに応じて共同利用しているサーバ等の押収がなされる際、十分な保護が必要な顧客データが開示される。
	完全性	● 悪意のある内外の主体によりアプリケーションが改ざんされ、顧客データの処理にあたって不正な処理が行われる。 ● 悪意のある内外の主体により保管中の顧客データが改ざんされる。
	可用性	● 悪意のある第三者が B 社 SaaS に対して DoS 攻撃を行い、A 社システムを含む多数のカスタマ向けの処理が停止する。 ● 悪意の有無を問わず、B 社 SaaS 又は C 社 IaaS に対して過度のトラフィックが集中し、急激なピーク負荷がかかることで、A 社システムを含む多数のカスタマ向けの処理が停止する。

関連する法制度等に係る観点	パーソナルデータ保護	● A 社又は B 社の正規の利用者により、顧客に通知された利用目的以外の用途で顧客データが利用される。 ● A 社の担当者等により B 社に対する必要かつ適切な監督が十分行われない。
	知的財産（営業秘密を含む）保護	● 顧客データが正当な手段によりデータを取得した悪意のある内外の主体（B 社従業員を含む）により不正の利益を得る目的、又は A 社に損害を加える目的で使用される。
	・・・	

なお、本ユースケースのように、クラウドサービスカスタマにおいて、サービス提供に係るクラウドサービスプロバイダが個人データを取り扱わないことを契約で取り決める場合は、自社が取り扱う個人データとして安全管理措置を講じる必要がある。また、外国で個人データを取り扱う場合に該当する場合[42]には、当該国における個人情報保護に関する制度等を把握した上で安全管理措置を講じる必要がある。そのため、表A-3.2で示す属性項目以外に「取扱い国」等の項目を設け、当該国における個人情報保護に関する制度等を把握する必要がある。また、この検討等に必要な情報を収集するため、クラウドサービスプロバイダ等との間の契約において、情報の開示を求める等して、データセンター所在地等を把握できるようにしておくことが望ましい。なお、保有個人データを外国で取り扱う場合には、「保有個人データの安全管理のために講じた措置」として、クラウドサービスプロバイダ及び当該データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を公表等する必要がある。

A-3-4-2 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて明らかになったように、本ユースケースでは、クラウドサービスカスタマが、複数の事業者がサプライチェーンを

[42] 外国にある支店・営業所に個人データを取り扱わせる場合や外国にあるクラウドサービスプロバイダの提供するクラウドサービスを利用し、その管理するサーバに個人データを保存する場合（日本国内に所在するサーバに個人データが保存される場合においても同様）等には、外国で個人データを取り扱う場合に該当する。
https://www.ppc.go.jp/files/pdf/2109_APPI_QA_4ejj3t.pdf

構成して提供するサービスを含め、機能別に複数のクラウドサービスを利用しており、そこではオンプレミスでシステムを構築し、運用する際とは異なる複数のリスクが想定される。そのようなリスクに対してA社及び関連する事業者が実施できる対応策として、例えば以下が挙げられる。

- データの物理的な所在に関する透明性の確保
  ポータルサイトの運用が既に行われているかにかかわらず、顧客データや商品購入データ等が現に保管されるデータセンターの所在地がフレームワークの適用段階で明確でない場合、A社は直接のサービスの提供者であるB社（ポータルサイト、顧客管理システム）及びC社（オンライン・ストレージ）の担当者にかかる情報の開示を求め、自社のサービス利用規約等における規定との整合やデータセンター所在地の法制度等をさらに調査し、確認したうえで、顧客の知り得る状態にしておく必要がある。

- 自社の責任分界の明確化及び運用状況のレビュー
  クラウドサービスの提供又は利用においては、オンプレミスでの管理とは異なり、クラウドサービスカスタマ及びクラウドサービスプロバイダの間でセキュリティやコンプライアンスに係る管理責任が分担されており、双方が自身の責任を果たしつつ適宜必要な情報開示等を行うことで全体として適切な管理が実現されることとなっている。このような管理のあり方は、「責任共有モデル」と呼ばれる場合がある[43]。本ユースケースにおいて、A社はSaaSやPaaS等、責任範囲が異なる複数のサービスを利用しているが、前述したように、クラウドサービスカスタマとしてのA社が責任を果たすべきアプリケーションの運用管理やアクセス権限等のセキュリティ設定が不十分な状態となることで、顧客データ等のセキュリティが侵害される恐れがある。そのようなカスタマ側の管理に起因するリスクを低減するため、A社では、STEP 2で明確化された事業者間の責任分界をさらに具体化する形で、それぞれのクラウドサービス利用において自社にて実施が必要な管理策（例：クラウドサービスにアクセスする端末の保護、アクセス権限の管理）を改めて洗い出し、運用支援ツール等も活用しつつその履行状況をレビューすることが望ましい。

---

[43] クラウドサービスプロバイダとクラウドサービスカスタマの責任の相違を表現しようとする際、プロバイダが責任を有するのが「クラウドのセキュリティ」(Security ‘of’ the Cloud)であり、カスタマが責任を有するのが「クラウドにおけるセキュリティ」(Security ‘in’ the cloud)と言い表すことがある。（https://aws.amazon.com/jp/blogs/news/rethinksharedresponsibility/）

A-4 国内で提供されるITサービスに関して、海外で開発や運用等を実施する例

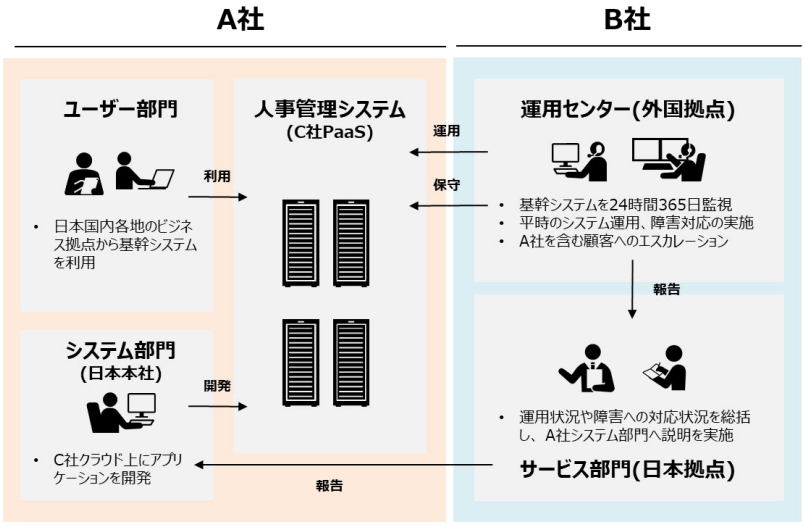
デジタルトランスフォーメーション（DX）の実現等、デジタル技術の高度な活用を通じた事業等の変革の重要性が社会的に認められている一方で、高度な専門性を必要とするITシステムの開発や保守、運用等の業務に対して、自社で人的リソースを確保しそれらを内製化するのが困難なケースが広く見られる。そのような場合、長期的には自社でリソースを確保することも志向しつつ、かかる業務を適切に外部委託することで、ユーザー事業者は質の高いサービスを享受しつつ、それ以外の業務に対するリソースを確保しやすくなるとされている。さらに、IT関連のアウトソーシングに関しては、従前から事業のグローバル化への対応やコスト削減等の観点から海外に拠点を置く事業者への委託がしばしば行われている。

一方、国内ではなく国外で事業上有用な技術情報等のデータや個人データを取扱う際には、一般に個人情報保護や技術情報に係る輸出管理等の側面から十分な注意を払う必要がある。データが組織や国・地域の境界を越えて取扱われることが施行される昨今において、かかる課題は従前よりさらに重要なものになっていると考えられる。

上記の背景を踏まえ、海外で事業上のデータを取扱うことが想定される場合における、当該データに対する適切な管理の検討に資する例として、以下の流れによるプロセス（A-4内において、以下、「本ユースケース」という。）を取り上げる。

- A社は国内にて全国的に事業を展開する事業者で、従来は複数あるグループ会社ごとにシステムを構築、運用し、適宜本社へのデータ共有を実施していたが、グループ内人材のタレント管理から人事・給与まであらゆる人事業務をクラウドで行うため、全社的に統合されたシステムをC社の提供するクラウドサービスを利用して構築している。
- A社は上記システムのうち自身で責任を有する部分の運用をB社に委託している。具体的には、B社にてヘルプデスク（問合せ対応）や常時監視、障害対応、必要に応じてアドオン機能の開発等を行う。

- B社の運用センターは外国に設けられており、ITシステムの運用に対して高い専門性を有するスタッフが24時間365日対応を行っている。本社に所在するA社システム部門へ運用状況や障害への対応状況を報告等する場合は、運用センターからの報告を受け、B社日本拠点のスタッフが実際の対応を実施する。



図A-4.1 対象プロセスの概要

本ユースケースにおいて、A社が全体的なセキュリティ等の管理を行うにあたり、考慮すべきステークホルダーとして以下が挙げられる。

- A社： 日本各地に事業拠点を有する事業者であり、全社共通の人事管理システムをC社クラウドサービス上に構築、運用する。
- B社： A社からの委託を受け、過去に人事管理システムの構築を支援し、そこで得た知見も活用しつつ、外国の運用センターを活用してA社人事管理システムに係る運用・保守業務等を行う。
- C社： A社にクラウドサービスを提供する。

A-4-1 STEP 1　データ処理フロー（「イベント」）の可視化

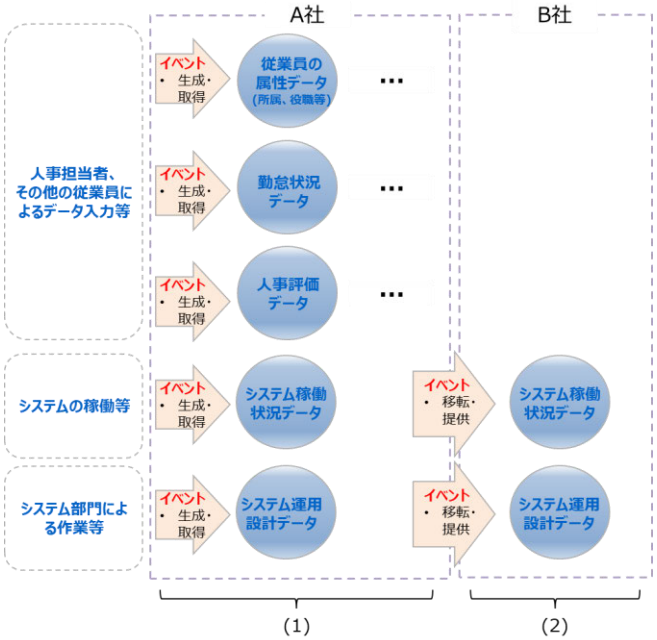
本ユースケースにおけるデータ処理フローは図A-3.2で示すように、以下のプロセスにより構成される。

(1) 人事担当者やその他の従業員等の人事管理システムのユーザー部門の入力により、各種人事管理関連データ（図A-4.2では、従業員の属性データ、勤怠状況データ、人事評価データを記載しているが、これらに限定されない）が「生成・取得」される。これらのデータは、例えば給与計算のような従来からの用途だけでなく、人材育成や離職率低下等の目的で

「加工・利用」され得る[44]。また、上記の一連のシステム利用を通じて、システム稼働状況データが継続的に「生成・取得」される。

(2) システム稼働状況データや、運用管理等に必要なデータ（システム運用設計データ等）は運用保守の委託先であるB社に「移転・提供」され、サービス提供のために活用される。なお、少なくとも下記に挙げるような平時の運用業務を実施するにあたっては、B社は各種人事管理関連データの提供を受けないものとする。

- 各種アプリケーションのパフォーマンス管理
- 人事管理システムを対象にした修正パッチの配布、適用
- A社システム部門経由で行う問合せ対応、障害発生時の調査、対応



図A-4.2 データ処理フローの可視化

（国内で提供されるITサービスに関して、海外で開発や運用等を実施する例）

A-4-2 STEP 2　必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、顧客データ等が個人データに該当する点や、当該データを処理、管理するシステムが複数のクラウドサービスを組み合わせて実現されている点等を考慮する

[44] こうした「加工・利用」の在り方は多様であり得るが、その点への考慮は本ユースケースの本旨とは異なることから、図 A-4.1 では詳述しない。

と、例えば下記のルールや各社の必ずしも明文化されていないルール等が「場」として特定され得る。

（1）個人情報保護法：A社は機密性の高い人事データを保有しているため、個人情報取扱事業者に課せられる義務の遵守が求められる。さらに、A社以外の適用範囲を考慮するうえでは、委託先となるB社やC社が、契約内容から見てA社から個人データの提供を受けているのかという点について明確化がなされる必要がある。その際、A-3でも記載したように、委託先の事業者がシステム内の個人データを取り扱うこととなっている場合には、個人データを提供したことになり、本人同意の取得、又は委託契約の締結等による正当性の確保を行う必要がある。なお、上記の場合はA社から委託先に対して個人情報保護法第20条に基づき自らが講ずべき安全管理措置と同等の措置が講じられるよう監督を行う[45]必要がある点にも留意する必要がある。一方で、委託先の事業者が、契約条項において個人データを取り扱わない旨を規定している場合、適切にアクセス制御を行っている場合等であれば、B社やC社へ個人データが提供されたことにはならない[46]。その場合は、B社やC社のような委託先にて個人データが取扱われていないことを確実にしたうえで、A社自身が自ら果たすべき適切な安全管理措置を講じる必要がある[47][48]。

（2）輸出管理関係法令[49]：一般に、各社の貨物の輸出、技術情報（例：設計書、ソースコード、運用ツール）等の非居住者（日本に定住していない外国人及び日本人）への提供の

---

[45] 個人情報の保護に関する法律についてのガイドライン（通則編） 3-3-4 委託先の監督（法第 22 条関係）

[46] 個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A』 Q7－53

[47] 同 Q7－54

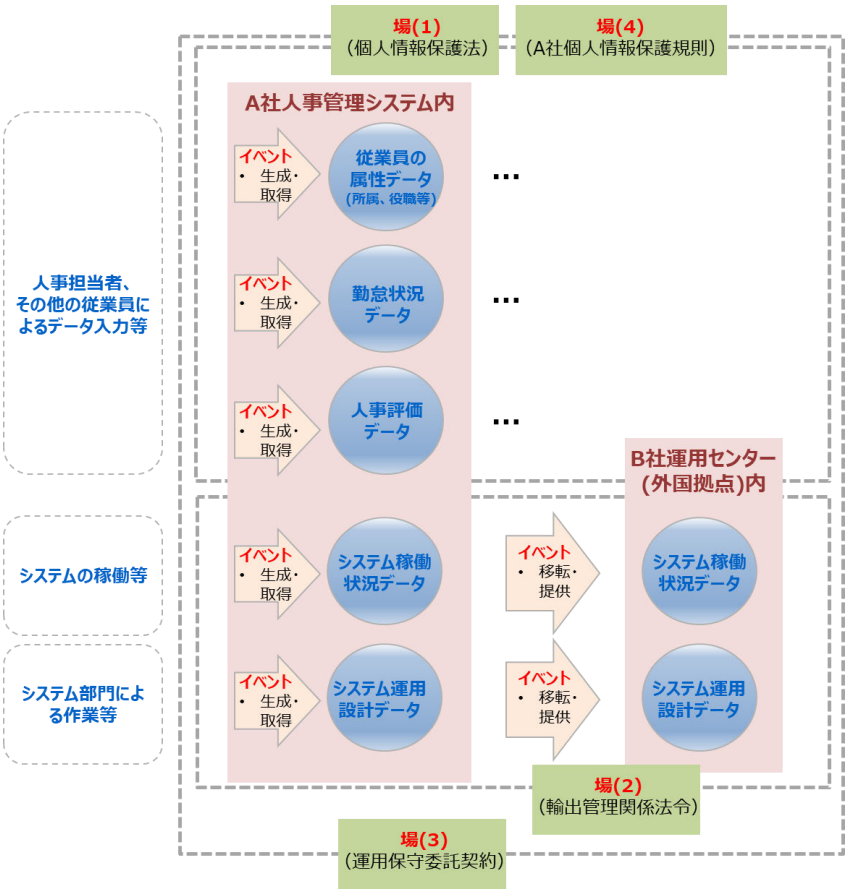
[48] B 社や C 社が契約上個人データを取り扱わないこととなっている場合、個人情報取扱事業者となる A 社は、外国において個人データを取り扱うこととなるため、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理措置の一環として、クラウドサービスプロバイダ（ここでは B 社）が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要がある。それが困難な場合、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となるべき情報を本人の知り得る状態に置く必要がある。（同 Q10－25 を参照）

[49] 日本における輸出管理関係法令に関するより詳細な情報については、経済産業省 貿易経済協力局 貿易管理部 安全保障貿易検査官室「安全保障貿易管理ハンドブック（第 10 版）」等の資料を参照されたい。

際には、貨物又は技術情報等の提供が外国為替及び外国貿易法（外為法）による輸出規制の対象に該当するかどうかを判定し、必要に応じて所管省庁から許可を得る等の手続きを実施する必要がある。本ユースケースでは、システム運用設計データのような役務の実施に必要なデータのほか、該当する場合は運用ツールの提供、現地での指導等が輸出管理の対象となり得る。A社及びB社は、あらかじめ輸出管理に必要な社内の手続きを整備しておき、取引前や出荷時に輸出の可否を審査、確認する必要がある。

（3）運用保守委託契約：A社とB社の間で委託業務の仕様やその他の事項について取り決めておくものであり、例えば、A社従業員の個人情報をB社は業務の実施にあたり取扱わない点、A社技術情報等の取扱い（例：秘密保持契約）等について明確に規定する必要がある。

（4）A社個人情報保護規則



図A-4.3 必要な制度的な保護措置の整理例

（国内で提供されるITサービスに関して、海外で開発や運用等を実施する例）

A-4-3 STEP 3 「属性」の具体化

本ユースケースにおいては、A社が人事管理のために自社の従業員に関するデータを取り扱うことから、カテゴリや開示範囲等の検討に際して、属性項目の検討に際して個人情報保護法制の参照が必要と考えられる。また、従業員に係るデータの利用目的やデータ管理主体、媒体・保存先や利用期限の特定にあたっては、社内の個人情報保護規則が有用な材料となるだろう。さらに、A社とB社間の運用保守委託契約からは各データの開示範囲（取扱いの有無を含む）や媒体・保存先、利用期限等に関する規定を得ることが可能と考えられる。

表A-4.1 「属性」の検討において考慮すべきルール（場）

		個人情報保護法	輸出管理関係法令	運用保守委託契約	A社個人情報保護規則
カテゴリ	パーソナルデータ保護	○			○
	知的財産（営業秘密を含む）保護			○	○
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○			○
データ管理主体		○			○
データ権利者		○			○
価値（重要度）		○			○
媒体・保存先			○	○	
利用期限		○		○	○

図A-4.2及び図A-4.3にて特定したデータのうち、従業員の属性データ、システム稼働状況データ、システム運用設計データの3つについて、表A-4.2にて各種属性項目のパラメータを示している。前述したように、従業員の属性データは個人データに該当し、利用目的の特定や安全管理等の個人情報取扱事業者の義務がA社に課せられる。A社自身の従業員を対象とした個人情報保護規則を参照し、開示範囲や利用目的、データ権利者（及び権利者たる従業員が行使でき

る権利の内容）、利用期限等の属性項目を具体化することができる。また、人事管理システムはC社が提供するPaaS上に構築されていることから、媒体・保存先としてC社PaaSを特定することができる。A社とC社の契約では、C社では個人データを取扱わないと規定していることから、開示範囲をA社内として、現にそのような管理が行われるようアクセス制御等を適切に行う必要がある。

従業員の属性データとは異なり、システム稼働状況データやシステム運用設計データは、B社においてもC社と同様に個人データが取扱われないこととなっていることも踏まえ、現に個人データを含まないデータとして管理されるべきである。また、C社に同様にB社対しても、従業員に関するデータを含むA社が管理する各種個人データに対するアクセスが適切に制御され、その状態が継続的に維持・管理される必要がある[50]。契約に基づいてB社に移転・提供されるシステム稼働状況データやシステム運用設計データ等は、運用保守委託契約を参照し、対象システムの運用、保守業務の実施や障害対応の実施等の目的で、委託契約の期間中に限り利用され、当該期間終了後に適切な手法で廃棄される。

表A-4.2 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		従業員の属性データ	システム稼働状況データ	システム運用設計データ
カテゴリ	パーソナルデータ保護	個人データ	非個人情報	非個人情報
	知的財産（営業秘密を含む）保護	A 社の営業秘密	A 社の営業秘密	A 社の営業秘密
	…	…	…	…
開示範囲		A 社内	A 社システム部門、B 社運用担当者	A 社システム部門、B 社運用担当者
利用目的		• 人事、給与の計算、決定、支払	• 対象システムの運用、保守業務の実施 • 障害対応の実施	• 対象システムの運用、保守業務の実施 • 障害対応の実施

[50] 個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A』 Q5－35 等を参照

	• 入社、退職、勤怠、その他の雇用管理 • 従業員の健康管理 • 会社から従業員への連絡等	• 障害の再発防止、運用の更なる効率化に向けた対策等の検討	
データ管理主体	A 社	A 社、B 社	A 社、B 社
データ権利者	A 社、従業員	A 社	A 社
価値（重要度）	非常に高い	高い	非常に高い
媒体・保存先	C 社 PaaS	B 社端末、C 社 PaaS	B 社端末
利用期限	雇用契約期間中	委託契約期間中	委託契約期間中

A-4-4 STEP 4 「イベント」ごとのリスクポイントの洗い出し

A-4-4-1 「イベント」ごとのリスクポイントの洗い出し

STEP 3までの検討事項を踏まえ、以下では本ユースケースのうち、図A.4-2及び図A.4-3に示す「システム運用設計データ」の「移転・提供」及びその後の「保管」のプロセスに関して以下のようなリスクを想定することができる。データの移転・提供過程にて想定されるリスクは用いられる技術的手段により異なることが想定されるが、ここでは当該移転・提供行為が外部クラウドストレージサービス（SaaS）を利用して行われるとしてリスクを抽出している。なお、以下では、上記データの「移転・提供」が技術情報の外国への「輸出」に該当し得ることに鑑み、「関連する法制度等に係る観点」として、「機微技術管理」を新たに加えている。

対象の移転・提供事象について、4 つの単位（国・地域・組織・人、システム・サービス、機器）の単位でリスクを整理することを通じて、一例として以下のようなリスクが特定され得る。

＜国・地域＞

- パーソナルデータ保護の観点については、システム運用設計データに個人に関する情報が含まれていないことを前提とすれば、非該当
- システム運用設計データが現に移転・提供される以前に、A社内で実施される輸出管理

関連手続きにおいて、技術情報の提供に係る輸出管理上の懸念が認められるかどうかの確認がなされない。

＜組織・ヒト＞

- 悪意のある海外拠点のB社従業員により、USBメモリの挿入等を通じてシステム運用設計データが不正に外部に持ち出される。

＜システム・サービス＞

- A 社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体にシステム運用設計データが開示される。
- 悪意のある第三者が A 社の業務端末と外部クラウドストレージサービスを提供するサーバとの間の通信に介入し、データを改ざんする。

＜機器＞

- 外部クラウドストレージサービスを提供するサーバがマルウェアに感染し、システム運用設計データの移転・提供に遅延が生じる。

表A.4-3 「システム運用設計データ」の「移転・提供」及びその後の「保管」で想定されるリスク（例）

大分類	中分類	「システム運用設計データ」の「移転・提供」及びその後の「保管」で想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある外部の主体が A 社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納されたシステム運用設計データに不正アクセスされる。 ● A 社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体にシステム運用設計データが開示される。 ● 悪意のある外部の主体が B 社の保有する運用・保守用の端末に不正アクセスし、システム運用設計データに不正アクセスする。 ● 悪意のある海外拠点の B 社従業員により、USB メモリの挿入等を通じてシステム運用設計データが不正に外部に持ち出される。
	完全性	● 悪意のある第三者が A 社の業務端末と外部クラウドストレージサービスを提供するサーバとの間の通信に介入し、データを改ざんする。

	可用性	● 外部クラウドストレージサービスを提供するサーバがマルウェアに感染し、システム運用設計データの移転・提供に遅延が生じる。
関連する法制度等に係る観点	パーソナルデータ保護	● システム運用設計データに個人に関する情報が含まれていないことを前提とすれば、該当なし。
	知的財産（営業秘密を含む）保護	● システム運用設計データが悪意のある内外の主体（例：外部の攻撃者、B 社の従業員）により不正な手段で取得され、開示、使用される。
	機微技術管理	● システム運用設計データが現に移転・提供される以前に、A 社内で実施される輸出管理関連手続きにおいて、技術情報の提供に係る輸出管理上の懸念が認められるかどうかの確認がなされない。

A-4-4-2 今後のデータ管理の高度化に向けた課題の検討

前述のフレームワーク適用プロセスからわかるように、本ユースケースでは、事業者（A社）が外部の事業者の支援を受けつつ構築した人事管理システムという汎用的なシステムの運用を、コスト削減や品質の向上等を目的として、海外に保守拠点を有する外部の事業者（B社）に委託するケースを取扱った。このような場合、多くの個人データを取扱う人事管理システムそれ自体を保護するだけでなく、そこで取扱われる従業員に関するデータやシステムの運用に係るデータの移転・提供に係るガバナンスを確保すること等が特有の課題となる。そのような課題に対してA社及び関連する事業者が実施できる対応策として、例えば以下が挙げられる。

- B社からA社データへのアクセス状況のレビュー
  前述のとおり、B社はA社の管理する個人データを取扱うことはないとされているが、前提となる契約等の条項が継続的に遵守されていることを確実にする必要がある。例えば、委託される業務内容に個人データを用いて情報システムの不具合を再現させ検証する等の個人データを取扱い得るものが含まれていないこと、かかる条項が含まれていない場合に現にB社拠点から個人データへのアクセスが行われていないことを確認すること（例：付与されているアカウントやアクセス権限の分析、契約期間中のアクセスログのレビュー）が対処として想定される。

- B社海外拠点におけるセキュリティマネジメントの確認

  B社はA社の従業員等に関する個人データを取扱うことはないものの、システム運用設計データやシステム稼働状況データ等のA社にとって事業上の価値があるデータを自社の拠点にて取扱う。昨今、本ユースケースにおけるB社のような委託先や海外支社等において、相対的にセキュリティ管理が行き届いていないことに起因して、外部からの攻撃や内部不正、その他のヒューマンエラー等による情報漏えい等の事例が報告されている点を踏まえると、A社とB社との委託契約等においてフレームワークの適用を行う際にかかるリスクへの対応が十分になされていない場合は、A社からB社に対して自社と同等の管理水準を達成するためのより具体的な安全管理策を規定し、書面又は監査等により遵守状況を確認したりする等の施策が有用と考えられる[51]。

[51] 業務委託先等に対するセキュリティ管理策に関しては、JIS Q 27002:2014 の「15.1 供給者関係における情報セキュリティ」における各種実施策等も参照されたい。

A-5 ATM・金融端末の生産ラインにおける板金加工データの収集・加工

近年、IoT化や自動化を通じて個別の機械やデバイスの稼働データを利活用する流れが広がっている中、利活用の対象となるデータの種類は多種多様になっており、データの性質に応じた管理が求められてきている。例えば、工場内においてデバイスの稼働データだけではなく、従来想定されていなかった映像データや画像データ等の個人情報等にも該当し得るデータを利活用することも想定される。従来対象としていなかった範囲のデータの取扱いについても考慮が必要となってきており、事業者ではより慎重な検討を求められるようになる可能性がある。

本章ではスマート工場分野に係る本フレームワークのユースケースとして、日本国内のATM・金融端末の生産工場において、板金加工工程に係る作業を可視化し業務効率化に役立てることを目的とする工場の製造部門によるデータ取得、加工プロセス（A-5内において、以下、「本ユースケース」という。）を取り上げる。

- ATM・金融端末の生産工場における調達、部材加工、組み立て、試験の4つのステップのうち、部材加工作業をデータ取得の対象とする。
- 作業員は曲げ加工機（ベンダー）を活用して板金を加工する。作業現場では、例えば以下のデータ[52]を取得、加工する。
  - 作業現場において作業員を監視するネットワークカメラにて取得した映像データ[53]
  - 曲げ加工機（ベンダー）のモータに取り付けられた電流センサーにて取得したセンサーデータ[54]
- 図A-5.1に示すプロセスにてデータを取得、加工する。

(1) 作業員を監視するネットワークカメラにて映像データを取得し、工場内に設置されたデータ保存用サーバに保存する。同様に、曲げ加工機（ベンダー）のモータに取り付けられた電流センサーにてセンサーデータを取得し、同じデータ保存用サーバに保存する。

(2) データ保存用サーバにて映像データ等を圧縮処理する。

(3) 圧縮処理した映像データ及びセンサーデータを社内クラウドへ定期的に自動でアップロードする。

(4) 社内クラウド上でビジネスインテリジェンスツールを活用しプロファイル化（例:ID付

[52] 本ユースケースでは取り扱わないが、生産管理データは別途社内クラウドにアップロードされプロファイル化されているものとする。

[53] 映像データは斜め上から作業員を撮影し作業員の顔や手元が映ったデータを指す。

[54] 設備の駆動モータ電流値データを指す。

与）を行う。

(5) IDによって紐づけられた映像データやセンサーデータ、生産管理データを社内クラウドのアプリケーションを通じて確認する。ただし、現時点で現場改善を目的としたデータの利活用を想定しており、社外への公開は想定していない。

- クラウドサービスのデータセンターは日本国内に設置されているものとする。
- 本ユースケースでは、新規でシステム構築を行うとともに、工場内の制御システムとは接続しないことを想定する。

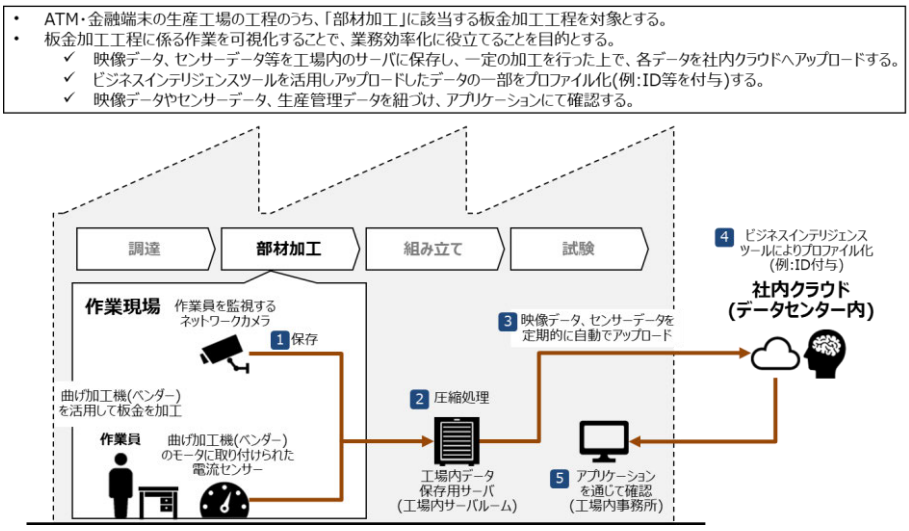


図 A-5.1 対象プロセスの概要

本ユースケースにおいて考慮すべきステークホルダーとして以下が挙げられる。

- ATM・金融端末の生産工場の製造部門:ATM・金融端末を生産するとともに、生産工場内のシステム部門及び本社における情報システム部門と協力して、作業員による現場作業の可視化、効率化を行う。
- ATM・金融端末の生産工場の情報システム部門:外部のITベンダーと契約を行い、工場内データ保存用サーバの導入・管理を行う。また、生産工場内のセキュリティ対策を主に担当する。
- ITベンダー:ATM・金融端末の生産工場に対してデータ保存用サーバやネットワークカメラ、電流センサー等からなるシステム一式を提供する。なお、ネットワークカメラや電流センサーはITベンダーが他の事業者から調達する。
- 本社における情報システム部門:外部のクラウドサービスプロバイダと契約を行い、社内クラウド及びビジネスインテリジェンスツールの導入・管理を行う。

- クラウドサービスプロバイダ:日本国内にデータセンターを保有し、クラウドサービスを本社の情報システム部門へ提供する。クラウドサービスにはビジネスインテリジェンスツールの提供が含まれる。

A-5-1. STEP1 データ処理フロー（「イベント」）の可視化

本ユースケースでは図A-5.2に示すように、以下のプロセスにより構成される。

(1) 作業現場に設置されたネットワークカメラから映像データ、曲げ加工機（ベンダー）のモータに設置された電流センサーよりセンサーデータを生成・取得する。

(2) 取得されたデータは、工場内のLANを通じて工場内のデータ保存用サーバに保存される。

(3) 工場内のデータ保存用サーバに保存されたデータは圧縮処理され、定期的に自動で社内クラウドへ移転・提供される。

(4) 社内クラウド内のデータは、ビジネスインテリジェンスツールを通じてプロファイル化（例:ID付与）される。[55]

(5) 付与されたIDによって映像データ、センサーデータ、生産管理データが紐づけられる。生産工場の製造部門は、例えば不良品が発生した際の作業状況を確認する。作業員は別途管理されている作業管理簿、出勤管理表等によって特定されているものとする。

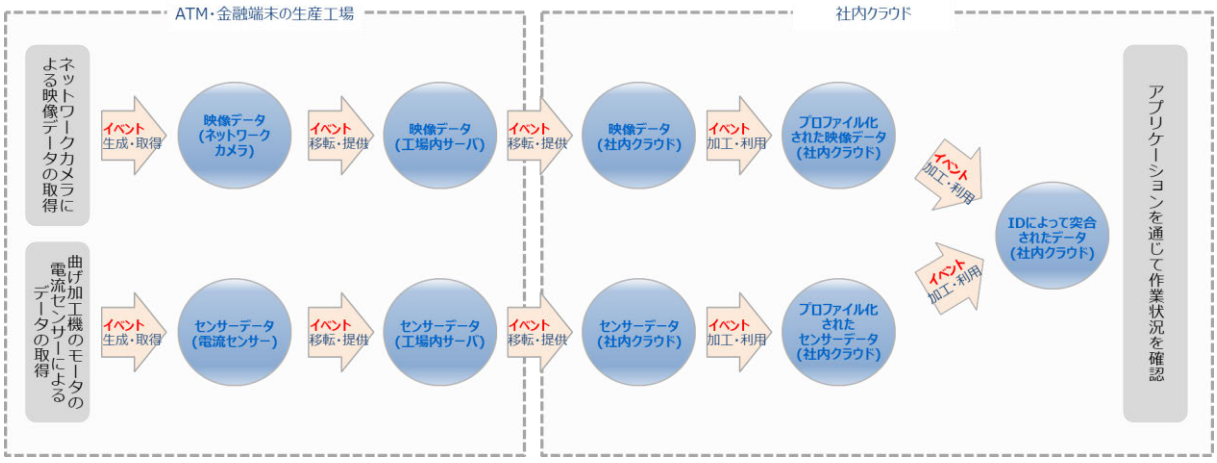


図 A-5.3 データ処理フローの可視化

[55] 「プロファイル化された映像データ」とは、斜め上から撮影され作業員の顔や手元が映ったデータにIDが付与され、センサーデータや生産管理データと紐づけできる状態となったデータを指す。

A-5-2. STEP2 必要な制度的な保護措置（「場」）の整理

STEP2では、STEP1で特定された一連のデータ利活用プロセスに対して、「場」としてどのようなデータの保護に係るルール（規範）が課せられ得るかを理解する段階である。本ユースケースにおいて、取り扱うデータの性質を考慮すると、例えば、以下に示すルールが「場」として特定され得る。

(1) 不正競争防止法:不正競争防止法[56]とは、不正競争の防止、不正競争に係る差止め・損害賠償に関する措置を示すもの。生産工場内の保存用サーバに格納されたカメラデータ及びセンサーデータと社内クラウドに格納されたカメラデータ、センサーデータプロファイル化されたデータは営業秘密の要件となる有用性、秘密性管理性、非公知性を満たすよう管理されるべきであり、営業秘密に該当することによって、かかるデータの侵害が民事的阻止や刑事的措置の対象となる。

(2) 個人情報保護法:ネットワークカメラにより取得されるデータは作業員の全体像を映すものである。作業員の向きによっては個人を特定可能な顔特徴データ等が取得されることがあることから、映像データの取扱いにあたっては、個人情報取扱事業者の義務を遵守しなければならない。

- 個人情報の利用目的
- 不適正利用の禁止
- 個人データの管理（データ内容の正確性の確保/安全管理措置/従業員の監督/委託先の監督）
- 個人データの漏えい等の報告
- 個人データの第三者への提供
- 個人関連情報の第三者提供の制限等
- 保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等

(3) 工場の情報セキュリティ管理規程:工場で取り扱う情報のセキュリティを保護するために定められたルールをまとめた文書。例えば、以下の対策を講じる必要が生じる。

- 「情報資産管理台帳」に記載した上で、情報資産の機密性に沿って取り扱うデータに対して評価を行う。
- 評価に基づき設定された「情報資産管理台帳」の利用者範囲を踏まえて、必要最低限の

[56] 経済産業省「不正競争防止法」
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/unfaircompetition_textbook.pdf

アクセス権を付与する。

(4) クラウドサービスの利用規約: クラウドサービスプロバイダが提供する利用規約。利用規約では、例えばクラウド上のデータを活用した違法行為または不正行為が禁止されている。

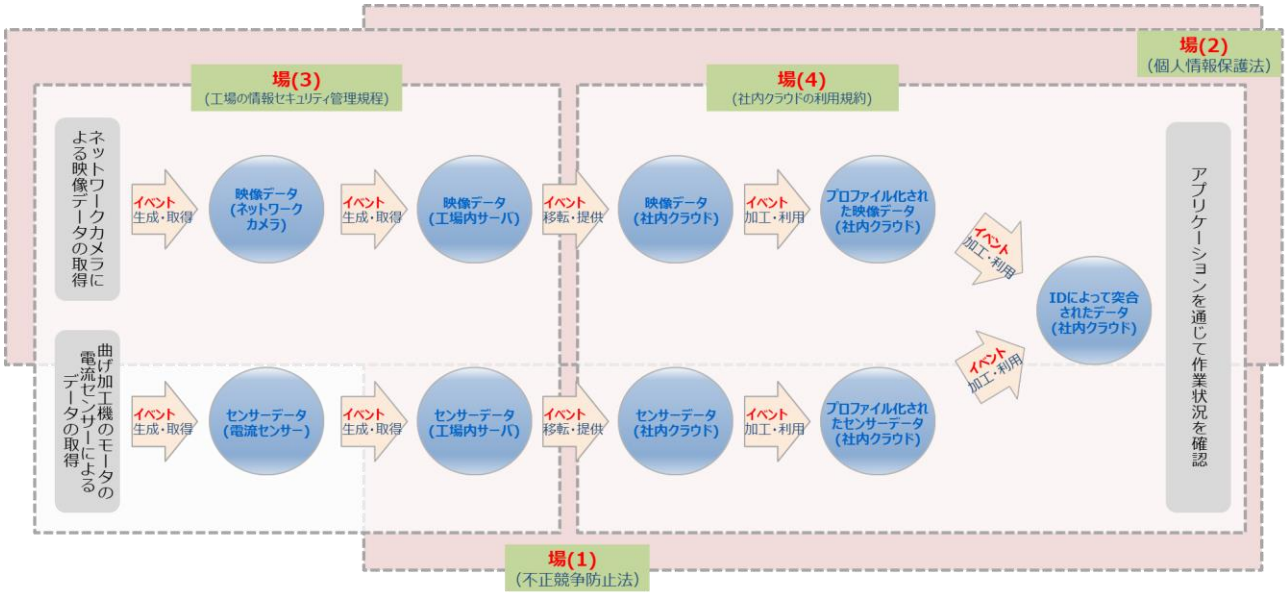


図 A-5.4 必要な制度的な保護措置の整理

他方、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer 1.0」（以下、「工場ガイドライン」）では、「業務内容や業務重要度などを考慮しつつ、同等の水準のセキュリティ対策が求められる領域として、ゾーンを設定する」としている。また、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer 1.0 別冊：スマート化に向けた対策ポイント」では、「ゾーン内・ゾーン間の考え方について、経済産業省「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」が参照可能である」としている。

工場システムにおけるゾーン設定にあたって、DMFの考え方を参考にすることができることから、本ユースケースではデータに着目[57]した上でその考え方を紹介する。

DMFでは、データマネジメントを「場」、「属性」、「イベント」の3つの要素から構成されるモデルとして整理している。そのうち「場」を「ゾーン」に、「イベント」を「業務」（処

[57] 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0 別冊：スマート化に向けた対策ポイント」では、ゾーンごとのセキュリティリスクを検討する際の視点として「データの値」を例にあげていることから、本ユースケースではデータに着目をしてゾーン等を設定した。

理）に置き換えた上で対応関係を整理した。

- 「場」:「ゾーン」に相当（例:生産工場ゾーン（作業現場、サーバルーム、工場内事務所）、社内クラウドゾーン）
- 「イベント」:「業務」（処理）に相当（例:製造データの取得/サーバに保存）

STEP1及びSTEP2での整理結果を工場システムの文脈で再整理した結果を以下に示す。

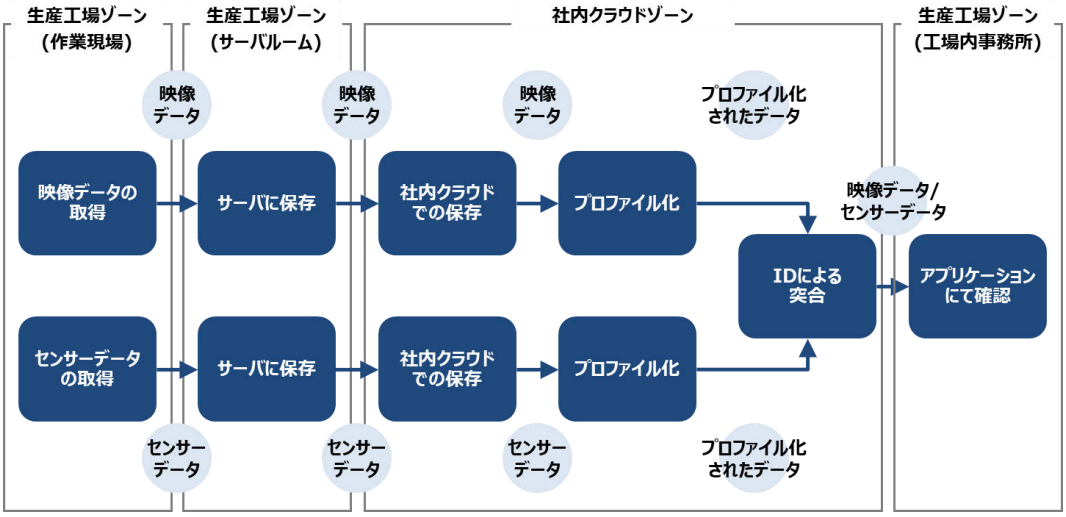


図 A-5.5 制御システム環境における DMF の考え方を踏まえた整理結果

A-5-3. STEP3 「属性」の具体化

STEP3では、STEP2にて特定されたデータの保護に係るルール（場）の効果的・効率的な遵守に資するデータの「属性」を特定する。

本ユースケースでは、STEP2までに特定した以下のデータを扱う。

- 映像データ（ネットワークカメラ内）
- 映像データ（保存サーバ内）
- プロファイル化された映像データ
- センサーデータ（電流センサー内）
- センサーデータ（保存サーバ内）
- プロファイル化されたセンサーデータ

表A-5.1 本ユースケースで扱うデータの「属性」パラメータ例

		映像データ(ネットワークカメラ内)	映像データ(保存サーバ内)	プロファイル化された映像データ	センサーデータ(電流センサー内)	センサーデータ(保存サーバ内)	プロファイル化されたセンサーデータ
カテゴリ	パーソナルデータ保護	個人情報を含む	個人情報を含む	個人情報を含む	-	-	-
	知的財産・営業秘密保護	-	事業者の営業秘密を含む	事業者の営業秘密を含む	-	事業者の営業秘密を含む	事業者の営業秘密を含む
	…	…	…	…	…	…	…
開示範囲		生産工場の製造部門	生産工場の製造部門	生産工場の製造部門及び情報システム部門、本社の情報システム部門	生産工場の製造部門	生産工場の製造部門	生産工場の製造部門及び情報システム部門、本社の情報システム部門
利用目的		作業の可視化に伴う業務効率化					
データ管理主体		生産工場を保有する事業者					
データ権利者		生産工場を保有する事業者/作業員	生産工場を保有する事業者/作業員	生産工場を保有する事業者/作業員	生産工場を保有する事業者	生産工場を保有する事業者	生産工場を保有する事業者
価値（重要度）		高い	高い	非常に高い	高い	高い	非常に高い
媒体・保存先		ネットワークカメラ	ATM・金融端末の生産工場/社内クラウド	社内クラウド	電流センサー	ATM・金融端末の生産工場/社内クラウド	社内クラウド
利用期限[58]		映像データを取得後２年間	映像データを取得後２年間	映像データを取得後２年間	-	-	-

A-5-4. STEP4 「イベント」ごとのリスクポイントの洗い出し

A-5-4-1. 「イベント」ごとのリスクポイントの洗い出し

本STEPでは、これまでの検討を踏まえて、対象のプロセス内でデータ取扱いに関連して想定

[58] 個人情報保護法では個人情報の保存期間や廃棄すべき時期について規定されていないが、事業者では利用期限を２年間と設定した。ただし、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するとした。

されるリスクを洗い出し、当該リスクのうち主なものを対象として有効と考えられるデータ管理策の検討を実施した。

全体のプロセスを以下に示す4つのイベントに分割して分析を行った。

- 映像データの生成・取得及び「社内クラウド」への移転・提供
- センサーデータの生成・取得及び「社内クラウド」への移転・提供[59]
- 映像データをプロファイル化する際の加工・利用
- センサーデータをプロファイル化する際の加工・利用

映像データの生成・取得及び「社内クラウド」への移転・提供の際には、ネットワークカメラから保存用サーバまでのネットワーク、及び保存用サーバから社内クラウドまでのネットワーク、そこで扱われる映像データが機密性、完全性、可用性の観点からセキュリティ観点の分析対象となり得る。

また、法制度等の観点からは、パーソナルデータ保護や知的財産・営業秘密保護を目的として、利用目的の逸脱や第三者への提供時の手続きの不備がリスクとして特定され得る。

表 A-5.2 映像データの生成・取得及び「社内クラウド」への移転・提供

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	● 「映像データ」が、生産工場内のネットワーク又は生産工場及び社内クラウド間のネットワーク上で内部犯行者又は外部の攻撃者に傍受され、漏えいする。
		マルウェア感染	● 「映像データ」がマルウェアに感染したネットワークカメラ又は保存用サーバから不正な送信先へ共有される。
	完全性	なりすまし	● ネットワークカメラが不正な機器になりすまされ、工場内データ保存用サーバにおいて正確でない「映像データ」が生成・取得される。

[59] 「映像データ」及び「センサーデータ」をデータ保存用サーバから社内クラウドへ同時に移転・提供する場合、容易に照合可能となることから、「センサーデータ」も個人情報になり得る点にご留意いただきたい。

大分類	中分類	脅威分類	想定されるリスク
		改ざん	● 「映像データ」が、生産工場内のネットワーク上や生産工場と社内クラウド間のネットワーク上で、内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	● ネットワークカメラがマルウェアに感染して稼働停止し、「映像データ」を生成・取得できない。 ● 保存用サーバがマルウェア感染して稼働停止し、社内クラウドへ移転・提供できない。
		システムの不具合	● 「映像データ」の生成・取得に係るネットワークカメラ又は保存用サーバに故障等の不具合が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	違法な手段によるデータ取得	● 「映像データ」を取得する事業者が、データの利用目的等の必要事項を作業員に対して明確に示していない、又は利用の実態と対応した形で提示していない。
			● 作業員以外の人物（例:視察の目的で来訪した本社社員）が映り込んだ「映像データ」が適切な処理を経ることなく、工場内データ保存用サーバ及び社内クラウドに蓄積される。
		許諾等のない第三者提供	● 事業者が、事前の本人同意取得又はオプトアウトに係る手続（委託、共同利用等を含む）等の実施なしに、保存用サーバ内の「映像データ」を分析等の目的で第三者の事業者に提供する。
		利用しないデータの消去漏れ	● 利用目的が達成され予め定めた保存期間（2年間）を過ぎたとしても、「映像データ」が消去されずに、保存用サーバに残り管理されない状態となる。
	知的財産・営業秘密保護	違法な手段によるデータ取	● 事業者における悪意のある従業員又は退職者を含む第三者が、保存用サーバ内の「映像データ」を

大分類	中分類	脅威分類	想定されるリスク
		得	不正な方法（窃取、詐欺、強迫、その他の不正な手段）で取得している。

センサーデータの生成・取得及び「社内クラウド」への移転・提供の際には、映像データと同様にネットワークカメラから保存用サーバまでのネットワーク、及び保存用サーバから社内クラウドまでのネットワーク、そこで扱われるセンサーデータが機密性、完全性、可用性の観点からセキュリティ観点の分析対象となり得る。

しかし、センサーデータにはパーソナルデータが含まれないため、パーソナルデータ保護に係るリスクは必ずしも想定されない。

表 A-5.3 センサーデータの生成・取得及び「社内クラウド」への移転・提供

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	● 「センサーデータ」が、生産工場内のネットワーク又は生産工場及び社内クラウド間のネットワーク上で内部犯行者又は外部の攻撃者に傍受され、漏えいする。
		マルウェア感染	● 「センサーデータ」がマルウェアに感染した保存用サーバから不正な送信先へ共有される。
	完全性	なりすまし	● 電流センサーが不正な機器になりすまされ、工場内データ保存用サーバにおいて正確でない「センサーデータ」が生成・取得される。
		改ざん	● 「センサーデータ」が、生産工場内のネットワーク上や生産工場と社内クラウド間のネットワーク上で、内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	● 保存用サーバがマルウェア感染して稼働停止し、社内クラウドへ移転・提供できない。
		システムの不具合	● 「センサーデータ」の生成・取得に係る電流センサー又は保存用サーバに故障等の不具合が生じ、処理

大分類	中分類	脅威分類	想定されるリスク
			が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	違法な手段によるデータ取得	● 事業者における悪意のある従業員又は退職者を含む第三者が、保存用サーバ内の「センサーデータ」を不正な方法（窃取、詐欺、強迫、その他の不正な手段）で取得している。

映像データをプロファイル化する際の加工・利用時には、社内クラウド及び社内クラウド上で稼働するビジネスインテリジェンスツール、そこで扱われる映像データが機密性、完全性、可用性の観点からセキュリティ観点の分析対象となり得る。

また、法制度等の観点からは、パーソナルデータ保護や知的財産・営業秘密保護の観点から、加工の結果として生成されるデータの取扱いがリスクとして特定され得る。

表 A-5.4 映像データをプロファイル化する際の加工・利用

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	● 加工・利用過程において、権限のない内外の主体により対象となるデータの全部又は一部が不正アクセスされ、「映像データ」が特定され、漏えいする。
	完全性	改ざん	● 悪意のある内外の主体により社内クラウドのビジネスインテリジェンスツールの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	● 悪意のある内外の主体により、意図的に「映像データ」のプロファイル（例:ID）が改ざんされる。

大分類	中分類	脅威分類	想定されるリスク
		システムの不具合	● 社内クラウドを構成する設備や機器の一部に故障等による障害や誤作動が発生する。
	可用性	サービス不能	● サービス妨害攻撃、マルウェア感染等により、社内クラウドを構成する設備や機器が一時的に停止する。
		システムの不具合	● 過度の処理リクエスト等により、社内クラウドを構成する設備や機器が一時的に停止する。
		自然災害等	● 地震や津波等の自然災害により、社内クラウドを構成する設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	提供先での目的外利用	● 必要な手続きを含むことなく、事前に作業員へ通知したものとは異なる目的で「映像データ」が利用される。
		利用しないデータの消去漏れ	● 利用目的が達成され予め定めた保存期間（2年間）を過ぎたとしても、「映像データ」が消去されずに、社内クラウドに残り管理されない状態となる。
	知的財産・営業秘密保護	提供先での目的外利用	● 正当な手段によりデータを取得した悪意のある内外の主体（退職者を含む）により、不正な利益を得る目的で「映像データ」が使用される。

センサーデータをプロファイル化する際の加工・利用時には、社内クラウド及び社内クラウド上で稼働するビジネスインテリジェンスツール、そこで扱われるセンサーデータが機密性、完全性、可用性の観点からセキュリティ観点の分析対象となり得る。

しかし、センサーデータにはパーソナルデータが含まれないため、法制度等の観点からは、パーソナルデータ保護に係るリスクは必ずしも想定されない。

表 A-5.5 センサーデータをプロファイル化する際の加工・利用

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	● 加工・利用過程において、権限のない内外の主体により対象となるデータの全部又は一部が不正アクセスされ、「センサーデータ」が特定され、漏えいする。
	完全性	改ざん	● 悪意のある内外の主体により社内クラウドのビジネスインテリジェンスツールの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	● 悪意のある内外の主体により、意図的に「センサーデータ」のプロファイル（例:ID）が改ざんされる。
		システムの不具合	● 社内クラウドを構成する設備や機器の一部に故障等による障害や誤作動が発生する。
	可用性	サービス不能	● サービス妨害攻撃、マルウェア感染等により、社内クラウドを構成する設備や機器が一時的に停止する。
		システムの不具合	● 過度の処理リクエスト等により、社内クラウドを構成する設備や機器が一時的に停止する。
		自然災害等	● 地震や津波等の自然災害により、社内クラウドを構成する設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用	● 正当な手段によりデータを取得した悪意のある内外の主体（退職者を含む）により、不正な利益を得る目的で「センサーデータ」が使用される。

A-5-4-2. 今後のデータ管理の高度化に向けた対策の検討

本節では、前節で特定されたリスクを適切に低減、管理し、データ管理の高度化を実現するために実施され得る対策を検討する。

リスクの大きさは、リスクが顕在化した場合の影響の度合い及び起こりやすさから算出するが、本ユースケースでは起こりやすさを正確に考慮することが難しいため、影響の度合いの大きさからリスクの大きさを算出する。製造業/工場では、安全確保（S：Safety）、事業／生産継続（BC：Business Continuity）、品質確保（Q：Quality）、納期遵守・遅延防止（D：Delivery）、コスト低減（C：Cost）の価値が重視されていることから、これらを侵害するものをリスクが大きいと判断する。また、間接的にコスト低減（C：Cost）を阻害する可能性のあるコンプライアンスリスクもリスクが大きいものとみなす。

ここでは、以下のリスクを大きいリスクとした上で、生じ得る結果を特定した。

表 A-5.6 リスクと生じ得る結果

リスク	生じ得る結果
社内クラウドで加工・利用する際の「映像データ」及び「センサーデータ」の改ざん	「センサーデータ」と「映像データ」に誤ったIDが割り振られ、「センサーデータ」と「映像データ」が誤って紐づけをされることによって、仮に不良品が発生した場合の原因特定に時間を要する。その結果、納期遅延が生じ、最悪の場合、事業/生産継続に影響を与え得る。
社内クラウドのビジネスインテリジェンスツールの設定等の改ざん	
社内クラウドへ移転・提供する際の「映像データ」やプロファイル化された「映像データ」の漏えい	個人情報の流出によって、対応にかかるコストが生じる。最悪の場合、対象の従業員に対する損害賠償が生じ得る。
社内クラウドから「映像データ」やプロファイル化された「映像データ」の漏えい	

上記で特定したリスクに対する対策の方向性を検討する。本ユースケースにおいて生じるリスクとそのリスクに対して講じる対策の関係性は以下の通り。なお、「保存用サーバから社内クラウドへ転送する際のセキュアなネットワークの利用」及び「セキュアなクラウドサービスの利用」にて示す対策の一部は、工場ガイドラインの「3.2.2.ステップ 2-2 想定脅威に対するセキュリティ対策の対応づけ」で示された対策を参照した。

表 A-5.7 リスクに対して講じる対策

リスク	対策	参考となる工場ガイドラインにおける対策
社内クラウドで加工・利用する際の「映像データ」及び「センサーデータ」の改ざん	セキュアなクラウドサービスの利用	(1)システム構成面での対策 ① ネットワーク
社内クラウドのビジネスインテリジェンスツールの設定等の改ざん	セキュアなクラウドサービスの利用	(1)システム構成面での対策 ① ネットワーク
社内クラウドへ移転・提供する際の「映像データ」やプロファイル化された「映像データ」の漏えい	保存用サーバから社内クラウドへ転送する際のセキュアなネットワークの利用	(1)システム構成面での対策 ③ 業務プログラム・利用サービスにおけるセキュリティ対策
	「映像データ」及びプロファイル化された「映像データ」の適切な取扱い	-
社内クラウドから「映像データ」やプロファイル化された「映像データ」の漏えい	セキュアなクラウドサービスの利用	(1)システム構成面での対策 ① ネットワーク
	「映像データ」及びプロファイル化された「映像データ」の適切な取扱い	-

上記の検討結果から、本ユースケースにおけるリスクに対して講じる対策は以下の3つとする。

- 保存用サーバから社内クラウドへ転送する際のセキュアなネットワークの利用
- セキュアなクラウドサービスの利用
- 「映像データ」及びプロファイル化された「映像データ」の適切な取扱い

- 保存用サーバから社内クラウドへ転送する際のセキュアなネットワークの利用
  保存用サーバから社内クラウドへデータを転送する際には、工場ガイドラインの（1）システム構成面での対策 ① ネットワークにおけるセキュリティ対策を参照するものとする。

- セキュアなクラウドサービスの利用

  社内クラウドは外部のサービスを利用するため、具体的なセキュリティ対策の実施主体は提供するITベンダーとなる。ここでは、工場ガイドラインの（1）システム構成面での対策 ③ 業務プログラム・利用サービスにおけるセキュリティ対策に示された観点を参照して、セキュアなクラウドサービスを利用するものとする。

  - セキュリティに関する仕様が提示されているか
  - セキュリティに関する設定項目の設定値が記載されているか
  - セキュリティ被害の影響に関する取決めが記載されているか

- 「映像データ」及びプロファイル化された「映像データ」の適切な取扱い

  「映像データ」及びプロファイル化された「映像データ」の可視化の主な目的は社内の業務効率化である。また、仮に「映像データ」の作業員の顔をマスキングしたとしても、他の情報（例:作業管理簿、出勤管理表）と容易に突合可能であることから、匿名加工を行うのではなく個人情報として適切に管理することが求められる。したがって、例えば、以下のような対策を実施することが求められる。[60]

  ＜個人情報取扱事業者が具体的に講じなければならない措置＞

  - 工場内サーバ及び社内クラウドに対する物理的安全管理措置（個人データを取り扱う区域の管理/機器及び電子媒体等の盗難等の防止/電子媒体等を持ち運ぶ場合の漏えい等の防止/個人データの削除及び機器、電子媒体等の廃棄）
  - 工場内サーバ及び社内クラウドに対する技術的管理措置（アクセス制御/アクセス者の識別と認証/外部からの不正アクセス等の防止/外部からの不正アクセス等の防止）
  - 不適正利用の禁止

---

[60]仮に匿名化を行う場合には、「映像データ」及び「プロファイル化された映像データ」を加工し、個人情報に含まれる個人識別符号の全部を削除することにより、特定の個人を識別することができないようにする必要がある。具体的な対策として、抽出元のカメラ画像や個人識別符号等特定の個人を識別することができる情報と容易に照合することができないことを前提として、例えば個人情報識別符号である顔をマスキングすることや作業員をシルエット画像に置き換えることが考えられる。読者においては、既存のガイドラインとして個人情報保護委員会が公表する「個人情報の保護に関する法律についてのガイドライン（通則編）」(2023 年 12 月一部改正)や「「個人情報の保護に関する法律についてのガイドライン」 に関する Q&A」(2023 年 12 月更新)、「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」(2023 年 3 月)等を参考にしつつ各自判断されたい。

添付B イベントごとのリスクの洗い出しのイメージ

B-1 イベントごとの典型的なリスクの記載方法等

本章では、フレームワークの適用を行う事業者等が、自身のデータ利活用プロセスにおいて想定されるリスクを特定するにあたり、考慮することが望ましい典型的なリスクや有効な対策要件（例）を列挙する[61]。

表B.1-1　添付Bにおけるイベントごとの典型的なリスクの記載方法

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	生成・取得されるデータがネットワーク上で悪意のある内部犯行者又は外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護

B-2では、表B-1に示す様式に沿って、イベント類型（生成・取得、加工・利用、移転・提供、保管、廃棄）ごとに対象となる機能、資産の例を示したうえで、典型的なリスクを列挙する。その際、「リスク」の記述に該当する「想定されるセキュリティインシデント等（例）」に加え、特定するリスクの網羅性やスコープをより明確なものとするため、以下に概要を示す事項を併記している。

- 保護の観点

  「想定されるセキュリティインシデント等（例）」を特定する際に、考慮すべき保護の観点を提示している。かかる観点には、セキュリティの保護に関わるもの（機密性、完全性、可用性）と関連する法制度等に関わるもの（パーソナルデータ保護、知的財産（営業秘密を含む）保護等）が含まれる。
- 脅威主体の区分

  対象となるデータ利活用プロセスに対して（多くの場合ネガティブな）影響を及ぼし得る脅威の主体を以下の4つに分類している。

[61] 個々の適用ケースで特定され得るリスクはここで列挙されるものに必ずしも限定されない。

表B.1-2　脅威主体の区分（例）[62]

脅威主体の区分	概要
アドバーサリ （悪意のある主体）	サイバー資源（すなわち、電子的形態の情報、情報及び通信技術、ならびにそれらの技術によって提供される通信及び情報処理能力）に対する組織の依存を利用しようとする個人、グループ、組織、又は国家。一般的には、外部からのサイバー攻撃又は物理的な攻撃、内部犯行等が含まれる。
偶発的	日々の責務を実施する過程で必ずしも悪意のない個人が取る誤ったアクション（ヒューマンエラー等を含む）。
構造上	老化、リソースの枯渇、又は予測されたオペレーティングパラメータを超えるその他の状況に起因する、機器の故障、環境制御の失敗、又はソフトウェアの不具合。
外部環境上	組織が依存するが、組織のコントロールの範囲外である重要インフラに対する自然災害、及びそれらのインフラの故障。

フレームワークの適用主体は、サイバー攻撃等を行う悪意のある内外の主体（アドバーサリ）だけでなく、正規の従業員等によるヒューマンエラー（偶発的）や自然災害、インフラの故障等も含め、可能な限り網羅的な観点から、自身のデータ利活用プロセスに対する脅威を担い得る主体とそれによるリスクを特定することが望ましい。

- 脅威

上記区分の主体により担われ得る具体的な脅威を記載する。ここでは、脅威を洗い出すための手法の一つであるSTRIDEを基礎としつつ、生成・取得や加工・利用等に関わり得るIoT機器等の性質やアドバーサリ以外の主体による脅威も考慮して、追加の脅威類型（マルウェア感染、不正改造、誤使用[63]、システム等の不具合、自然災害等）を含めて提示している[64]。

---

[62] NIST Special Publication 800-30 Revision 1（IPA 訳）における「付録 D 脅威源 脅威事象を開始することができる脅威源の分類体系」を参照し、適宜追記等を実施

[63] 「誤使用」として、ここでは専ら、使用者に悪意のないものを指す。

[64] 経済産業省サイバーセキュリティ課「機器のサイバーセキュリティ確保のための セキュリティ検証の手引き　別冊 1 脅威分析及びセキュリティ検証の詳細解説書」における「STRIDE によって抽出されない可能性が高い」脅威の記述も踏まえ、アドバーサリ（悪意のある主体）以外の脅威主体による脅威類型を適宜追加している。

表B.1-3　STRIDEによる脅威の分類例

脅威	内容
なりすまし	コンピューターに対し、他の利用者や機器を装うこと。
改ざん	権限なしでデータを改ざんし、データの完全性を失わせること
否認	利用者が、あるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報漏洩	アクセス権限を持たない個人に情報が公開されること
サービス不能	正規のユーザーがサーバやサービス等にアクセスできないこと ※DDoS 攻撃やジャミングによるサービス妨害など
権限の昇格	権限のない利用者がアクセス権限を得ること

表B.1-4 本稿にて追加で定義している脅威の分類例

脅威	内容
マルウェア感染	他の機器への汚染源になる。ランサムウェア等により業務妨害を受けること
不正改造	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれること
誤使用	機器が利用者により事前に意図しない用途等で使われること
システム等の不具合	機器の故障、環境制御の失敗、又はソフトウェアの不具合が生じること
自然災害等	地震や津波、豪雨等の自然現象及び、電気、通信、給水、ガス等の外部のユーティリティの不具合によりデータ利活用プロセスに負の影響が及ぶこと

- 有効な対策要件（例）

特定されたリスクを低減するために有効と考えられる対策要件の例を、以下に示す参照文献との対応関係とともに記載している。参照文献としては、すべてのイベント類型に関連する内容を持つ「一般」と、各イベント類型にある程度特化した内容を持つものを扱う。

＜一般＞

- CPSF
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and

Organizations

- データマネジメント知識体系ガイド（DMBOK） 第2版

＜生成・取得＞

- 安全なウェブサイトの作り方　改訂第７版
- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

＜移転・提供＞

- SP 800-47 Rev. 1 Managing the Security of Information Exchanges
- ISO/IEC 27033-1:2015 Information technology – Security techniques – Network security – Part 1: Overview and concepts

＜加工・利用＞

- AI・データの利用に関する契約ガイドライン 1.1版

＜廃棄＞

- SP 800-88 Rev. 1 Guidelines for Media Sanitization

また、保護の観点として、パーソナルデータ保護や知的財産（営業秘密を含む）保護を参照しているインシデント等に対しては、参照文献として、以下に例示する各種法令に係るガイドライン文書との対応を示している。

＜パーソナルデータ保護＞

- 個人情報の保護に関する法律についてのガイドライン（通則編）
- 個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）
- 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）

＜知的財産（営業秘密を含む）保護＞

- 営業秘密管理指針

B-2 イベントごとのリスクの洗い出しのイメージ

本節では、表B.1-1に示した様式に沿って、イベント類型（生成・取得、加工・利用、移

転・提供、保管、廃棄）ごとに対象となる機能、資産の例を示したうえで、典型的なリスクや有効な対策要件（例）を示す。

B-2-1 データの生成・取得過程におけるリスクの洗い出しのイメージ

センサーによる計測や人手による入力等によるデータの生成・取得は、データライフサイクルの初期段階を構成しており、以降の利活用プロセスにおけるデータの信頼性を確保するうえで重要な位置を占めている。生成・取得は様々な手段で実行され得るため、実際のリスクアセスメントはその方法を具体的に特定したうえで実施することが望ましいが、以下では、様々な手法等に対して共通に適用し得るものとして、対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を示す。

＜対象となる機能＞

- フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能
- 上記のほか、オンラインシステム等への直接の入力や使用履歴の収集等により、データを生成・取得する機能

＜対象となる資産＞

- データの生成・取得に係る設備や機器（例：センサー、Webサーバ、業務用端末）
- 上記に接続するネットワーク

表B.2-1 データの生成・取得過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	生成・取得されるデータがネットワーク上で悪意のある内部犯行者又は外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護
				通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	生成・取得されるデータがマルウェアに感染した機器・設備等から不正な送信先へ共有される。	情報漏えい	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
				外部向き通信の監視、対処
	偶発的	データの生成・取得に係る設備や機器に不適切な設定	情報漏えい	機器・サービスの初期設定及び設定等の変更管理

		がなされており、データが本来想定していない主体から閲覧できるようになっている。		ユーザー、機器、サービス等に対する適切な水準の認証の実施 通信経路、端末の挙動等の監視、対処
完全性	アドバーサリ（悪意のある主体）	（特に人手のデータ入力が行われる場合） 正規ユーザーへのなりすましにより、不正確なデータが生成・取得される。	なりすまし	ユーザー、機器、サービス等に対する適切な水準の認証の実施 入力値の検証
	アドバーサリ（悪意のある主体）	データ生成元の機器を不正な機器によりなりすまされ、正確でないデータが生成・取得される。	なりすまし	機器等が設置された物理的環境におけるアクセス制御 機器等が設置された物理的環境の監視 通信経路、端末の挙動等の監視、対処 入力値の検証
	アドバーサリ（悪意のある主体）	稼働中のデータ生成元の機器が不正改造され、正確でないデータが生成・取得される。	不正改造	機器等の物理的耐性の強化 機器等が設置された物理的環境におけるアクセス制御 機器等が設置された物理的環境の監視
	アドバーサリ（悪意のある主体）	悪意のある従業員又は第三者の物理的な攪乱により、データ生成元の機器から正確でないデータが生成・取得される。	なりすまし	入力値の検証 機器等が設置された物理的環境の監視
	アドバーサリ（悪意のある主体）	正規の機器から生成・取得されたデータがネットワーク上で傍受され、改ざんされる。	改ざん	暗号化等による通信経路の保護 データの完全性、真正性保護
	構造上	品質や信頼性の低い IoT 機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する。	システム等の不具合	運用時の機器・システムの真正性確認
	偶発的	（特に人手のデータ入力が行われる場合） 正規ユーザーの誤入力により、不正確なデータが生成・取得される。	誤使用	入力値の検証
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃等によりデータの生成・取得に係る	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保

		設備や機器が一時的に停止する。		通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	センサー等の設備や機器がマルウェアに感染して稼働が停止し、データを生成・取得できない。	マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	データの生成・取得に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの生成・取得に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	偶発的	データ取得先の組織が、生成・取得するデータの利用目的をデータ元の個人に対して明確に示さしていない、又は利用の実態と対応して提示していない。	不十分なコンプライアンス	データ取得時の利用目的等の提示
	偶発的	データ取得先の組織が、偽り等の不正の手段により個人情報を取得している。	不十分なコンプライアンス	正当な手段によるデータの取得
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	悪意のある従業員又は退職者を含む第三者が、紙等で管理されている営業秘密を不正な方法（窃取、詐欺、強迫、その他の不正な手段）でデータとして取得している。	情報漏えい	秘密管理性を確保した営業秘密等の管理
	偶発的	他社から転職者等を受け入れる場合、その転職者が持ち込むデータの中に、他社の営業秘密等が含まれる等、意図せぬ形で他社の営業秘密等を取得してしまう。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保

B-2-2 データの加工・利用過程におけるリスクの洗い出しのイメージ

データは生成・取得して保管するだけでは必ずしも付加価値を生み出すわけではなく、何

らかの加工・利用を通じて付加価値をもたらす。他方、加工・利用過程に何らかの障害が発生すれば、データの信頼性、ならびにデータの利活用から得られるはずだったメリットを大きく損なわせる可能性があることから、他のイベントと同様、リスクを正しく認識し、適切に対処することが重要である。以下にて、加工・利用過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を示す。

＜対象となる機能＞

- データを加工・分析する機能

＜対象となる資産＞

- データの加工・利用に係る設備や機器（例：サーバ、業務用端末、それらにインストールされたソフトウェア資産）

表B.2-2 データの加工・利用過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	加工・利用過程において、悪意のある内外の主体により対象となるデータの全部又は一部が正当な権限なく参照され、自社又は他社の機密データが特定される。	情報漏えい	暗号化等による加工・利用過程の保護
	偶発的	アプリケーションやデータベース等におけるアクセス制御等の設定ミスにより本来保護が必要なデータが外部から閲覧可能となってしまう。	情報漏えい	最小権限の原則による権限の割り当て
				機器・サービスの初期設定及び設定等の変更管理
完全性	アドバーサリ（悪意のある主体）	悪意のある内外の主体によりアプリケーションが改ざんされ、データの処理にあたって不正な処理が行われる	改ざん	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て
				継続的なアプリケーションのセキュリティ管理
	アドバーサリ（悪意のある主体）	悪意のある内外の主体により意図的に加工・利用の結果として生じるデータの全体又は一部が改ざん又は削除される。	改ざん	適切な要員、サービスの選定
				自組織及び委託先等における要員のセキュリティ確保
				通信経路、端末の挙動等の監視、対処

	偶発的	正規の従業員が悪意なく誤って加工・利用の結果として生じるデータの全体又は一部を変更又は削除する。	誤使用	適切な要員、サービスの選定
				自組織及び委託先等における要員のセキュリティ確保
				機器、通信機器、回線等の冗長化及びバックアップの確保
	構造上	データの加工・利用を行う設備や機器の一部に障害や誤動作が発生し、集約結果の完全性が損なわれる。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃、マルウェア感染等によりデータの加工・利用に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
			マルウェア感染	脆弱性対応プロセスの整備、実行
				入力値の検証
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	過度の処理リクエスト等によりデータの加工・利用に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの加工・利用に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	アドバーサリ（悪意のある主体）	従業員により必要な手続きを踏むことなく、事前にデータ取得元の個人へと通知した目的とは異なる目的でデータが利用される。	不十分なコンプライアンス	利用目的等による加工・利用の制限
	アドバーサリ（悪意のある主体）	元の個人情報の本人を識別する目的で、仮名加工情報や匿名加工情報を他の情報と照合する。	不十分なコンプライアンス	仮名加工情報や匿名加工情報に対する識別行為の禁止
	偶発的	個人情報を仮名加工情報や匿名加工情報にする際に行う加工が法令等により定められる要求を満たした方法で適切に行われない。	不十分なコンプライアンス	仮名加工情報、匿名加工情報の適正な加工
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	正当な手段によりデータを取得した悪意のある内外の主体（退職者を含む）により、不正の利益を得る目的	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保
				通信経路、端末の挙動等の監視、対処

		又は権利元に損害を加える目的でデータが使用される。		
	偶発的	従業員により必要な手続きを踏むことなく、事前に提供元の組織人と合意した利用条件（利用目的、利用権限等）とは異なる方法でデータが利用される。	不十分なコンプライアンス	利用目的等による加工・利用の制限

B-2-3 データの移転・提供過程におけるリスクの洗い出しのイメージ

近時、ますます多くのデータが生成・取得、加工・利用される中で、データに由来するメリットを最大限享受するために、組織内あるいは複数の組織間でデータを共有（移転・提供）することの重要性が認識されている。一方で、移転・提供が主に行われるネットワーク上は、加工・利用や保管の過程とは異なるリスクや脅威が想定される場でもあり、それらを正しく認識し、対処することが重要である。移転・提供過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

- データを送受信する機能

＜対象となる資産＞

- データの移転・提供に係る設備や機器（例：ネットワーク、ネットワーク機器、サーバ、業務用端末）

表B.2-3 データの移転・提供過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	データが移転・提供に係るネットワーク上で悪意のある第三者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護
	アドバーサリ（悪意のある主体）	データがマルウェアに感染した機器・設備等から不正な送信先へ移転・提供される。	マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入

			情報漏えい	外部向き通信の監視、対処
	アドバーサリ（悪意のある主体）	データが正規の送信先になりすました不正な送信先へ移転・提供される。	なりすまし	暗号化等による通信経路の保護
				通信経路、端末の挙動等の監視、対処
	偶発的	データが悪意のない正規の利用者により本来想定されていない送信先へ移転・提供される。	情報漏えい	通信経路、端末の挙動等の監視、対処
				外部向き通信の監視、対処
完全性	アドバーサリ（悪意のある主体）	データが移転・提供に係るネットワーク上で悪意のある第三者に傍受され、改ざんされる。	改ざん	暗号化等による通信経路の保護
				データの完全性、真正性保護
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
				通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	データの移転・提供に係る設備や機器がマルウェアに感染し、データを移転・提供できない。	マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	偶発的	法令に基づく場合等の特定の事由に該当しない場合に、事前の本人同意取得又はオプトアウトに係る手続等の実施なしに、個人データを第三者に提供する。	不十分なコンプライアンス	第三者提供に係る正当な根拠の確保
	偶発的	個人データの第三者提供を行う際に、提供を行う側、提供を受ける側のいずれか又は双方において記録の作成、確認の実施が行われない。	不十分なコンプライアンス	第三者提供時の記録・確認の実施

	偶発的	個人データを外国にある第三者提供に提供する際、本人同意の取得、適切な情報提供等の遵守すべき手続きが実施されない。	不十分なコンプライアンス	外国にある第三者へのデータ提供時に必要な手続きの実施
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	悪意のある従業員又は退職者を含む第三者が、不正取得行為（窃取、詐欺、強迫、その他の不正な手段）により取得した営業秘密を移転・提供する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	アドバーサリ（悪意のある主体）	不正取得行為が介在したことを、移転・提供先が故意にもしくは重過失により知らないで営業秘密を取得する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	偶発的	移転・提供元が不正取得行為の介在について善意・無重過失で営業秘密を取得していても、取得後に不正取得行為の介在について悪意・重過失に転じ、当該営業秘密を第三者に開示する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	アドバーサリ（悪意のある主体）	移転・提供元から営業秘密を示された場合、不正の利益を得る目的で、又は、その保有者に損害を加える目的で、その営業秘密を開示する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	偶発的	従業員又は退職者が、自社の管理する営業秘密をそうとは認識せずに外部の事業者等に開示する。	不十分なコンプライアンス	営業秘密を企業内外で共有する場合の秘密管理性の確保

B-2-4 データの保管過程におけるリスクの洗い出しのイメージ

データは、ライフサイクルの様々な段階において、外部サービス（クラウドストレージを含む）やネットワーク接続されたストレージ機器、クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。データの利活用が活発に行われ、蓄積されるデータの種類や量がますます増加する中で、大規模なデータストレージ及び保

管されるデータはますます重要な保護対象となっている。かかる過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

- データを保管する機能

＜対象となる資産＞

- 各種データ処理に関連しデータを保管し得る設備や機器（例：サーバ、業務用端末、長期保存用の媒体）

表B.2-4 データの保管過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	外部の攻撃者により、弱いパスワード、ソフトウェアの脆弱性等が原因でデータを保管する機器・システムが外部から不正アクセスされ、データが漏えいする。	情報漏えい	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て
				保管されたデータ等の暗号化
				脆弱性対応プロセスの整備、実行
				外部向き通信の監視、対処
	アドバーサリ（悪意のある主体）	悪意のある従業員や退職予定者、外部委託先の従業員等により、データを保管する機器・システムがアクセスされ、保護すべきデータが漏えいする。	情報漏えい	自組織及び委託先等における要員のセキュリティ確保
				機器等が設置された物理的環境の監視
				保管されたデータ等の暗号化
				通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	外部の攻撃者や悪意のある内外の従業員等により、データを保管する媒体（例：端末内の HDD や SSD、USB メモリや CD、DVD 等の可搬媒体）が盗難されたり、不正に読み出されたりする。	情報漏えい	機器等が設置された物理的環境におけるアクセス制御
				保管されたデータ等の暗号化
				機器等が設置された物理的環境の監視
	偶発的	データの保管に係る設備や機器に不適切な設定がなされており、保管データが本来想定していない主体から	情報漏えい	機器・サービスの初期設定及び設定等の変更管理
				保管されたデータ等の暗号化

		閲覧できるようになっている。		通信経路、端末の挙動等の監視、対処
		国内又は国外の司法機関等からの求めに応じて共同利用しているサーバ等の押収がなされる際、十分な保護が必要なデータが開示される。	情報漏えい	データを処理、保管するサーバ等設備の所在地の確認
完全性	アドバーサリ（悪意のある主体）	悪意のある内外の主体により意図的に保管データの全体又は一部が改ざん又は削除される。	改ざん	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て
				データの完全性、真正性保護
	アドバーサリ（悪意のある主体）	マルウェア感染等により保管データの全体又は一部が改ざん又は削除、破壊される。	マルウェア感染	機器・サービスの初期設定及び設定等の変更管理
				脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	偶発的	正規の従業員（自社又は外部委託先等）が悪意なく誤って保管データの全体又は一部を変更又は削除する。	非意図的な誤使用	機器、通信機器、回線等の冗長化及びバックアップの確保
	構造上	外部委託先等が運用するものを含め、データを保管する設備や機器の一部に障害や誤動作が発生し、保管データの全体又は一部が損なわれる。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃、マルウェア感染等によりデータの加工・利用に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
			マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	外部委託先等が運用するものを含め、データを保管する設備や機器の一部に障害や誤動作が発生し、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの保管に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	偶発的	事業者が保有し、利用する個人データの内容が事実でないという理由で、本人か	不十分なコンプライアンス	本人からの求めに応じた保有個人データの訂正・利用停止等

		ら訂正や削除を求められた際の対応が十分に行われない。		
	偶発的	事業者が保管する個人データに対して、適切な安全管理策（従業員の監督、委託先の監督を含む）が講じられていない。	不十分なコンプライアンス	個人データに対する安全管理措置の実施
	偶発的	既に必ずしも利用しなくてもよい状況となっている個人データが不必要に保持又は利用されている。	不十分なコンプライアンス	データの遅滞ない消去
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	悪意のある外部の攻撃者、従業員又は退職予定者等により、営業秘密として管理される保管データがアクセスされ、データが外部へ漏えいする。	情報漏えい	ユーザー、機器、サービス等に対する適切な水準の認証の実施 最小権限の原則による権限の割り当て 通信経路、端末の挙動等の監視、対処
	偶発的	他社より提供を受けた営業秘密情報等について、利用期限が過ぎているにもかかわらず、別途許可等を得ることなく保管されたままとなっている。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保 データの遅滞ない消去
	偶発的	自社の保有する知的財産等に外部の知的財産等が混入（コンタミネーション）し、他社の知的財産等情報を不用意に使用・開示してしまう。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保 他社の秘密情報等の分離管理

B-2-5 データの廃棄過程におけるリスクの洗い出しのイメージ

様々な目的で利活用されたデータは、データの上書きや媒体の物理破壊、ディスク全体の暗号化等の適切な方法により廃棄され、復元できない状況とされることでそのライフサイクルを終える。かかる過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

-

＜対象となる資産＞

- 各種データ処理に関連しデータを保管し得る設備や機器（例：サーバ、業務用端末に

おける記憶媒体）

表B.2-5 データの廃棄過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	外部の攻撃者や悪意のある従業員等により、事業者が利用を終了し、十分でない方法により廃棄されたデータが不正に復元される。	情報漏えい	適切な要員、サービスの選定
				適切な方法によるデータ及び媒体の廃棄
	アドバーサリ（悪意のある主体）	悪意のある従業員又はデータの廃棄を委託された事業者の従業員により、廃棄を予定していたデータが外部に開示される。	情報漏えい	適切な要員、サービスの選定
				データ及び媒体廃棄の履行確認
	偶発的	廃棄作業を委託する場合に、委託先が確実に削除又は廃棄したことについて証明書等を取得していない等の原因で事実を確認することができない	不十分なコンプライアンス	データ及び媒体廃棄の履行確認
完全性	偶発的	記憶媒体等を処分する際に、本来は廃棄すべきでないデータまで廃棄してしまう。	誤使用	機器、通信機器、回線等の冗長化及びバックアップの確保

B-2-6 対策要件（例）と参照ガイドライン

B-2-1からB-2-5にて示した有効な対策要件（例）について、データの信頼性確保に係る取組を進めていく際の参考情報として、各種参照ガイドラインとの対応関係を以下に示す。なお、有効な対策要件（例）は、適用主体においてリスク管理のプロセスが一とおり整備されていることを前提に、リスク対応の段階において実施すべき「防御」や「検知」に係る主な対策要件を記載している。

表B.2-6 対策要件（例）と参照ガイドライン

対策	適用対象イベント	参照ガイドライン
適切な要員、サービスの選定	加工・利用、廃棄	・CPSF Ver.1.0 CPS.SC-4, CPS.SC-5 ・ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.2.1 ・NIST SP 800-53 Rev. 5 PS-7, SR-5, SR-6 ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第５．２(1)，(9), 第６．４（1），(5) ・NIST SP 800-88 Rev. 1 4.7 Verify Methods
自組織及び委託先等における要員のセキュリティ確保	加工・利用、保管	・CPSF Ver.1.0 CPS.GV-1, CPS.SC-5, CPS.AT-1, CPS.AT-2 ・ISO/IEC 27001:2013 A.6.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.15.1.1 ・NIST SP 800-53 Rev. 5 AT-1, AT-2, AT-3, AT-4, PS-7, SA-9, SA-16, SA-21 ・DAMA-DMBoK（第7章） 5.4 アウトソーシングにおけるデータセキュリティ ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第５．２(1)，(9), 第６．４(1)，(5)
ユーザー、機器、サービス等に対する適切な水準の認証の実施	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.AC-1, AC-4, AC-9 ・ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 ・NIST SP 800-53 Rev. 5 AC-2, AC-3, AC-7, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 ・DAMA-DMBoK（第7章） 3.3 アイデンティティ管理技術 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Logical Access to Interfaces ・安全なウェブサイトの作り方 改訂第７版 1.4 セッション管理の不

		備、1.11 アクセス制御や認可制御の欠落、2.5 パスワードに関する対策 ・AI・データの利用に関する契約ガイドライン データ編 第５．２(1) , (9), 第６．４ (1), (5) ・ISO/IEC 27035-1:2015 8.4 Identification and authentication ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
最小権限の原則による権限の割り当て及び認可の実施	加工・利用、保管	・CPSF Ver.1.0 CPS.AC-5, CPS.AC-9 ・ISO/IEC 27001:2013 A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 ・NIST SP 800-53 Rev. 5 AC-1, AC-3, AC5, AC-6, AC-24 ・DAMA-DMBoK（第7章） 2.3.5.3 データセキュリティの管理と保守 ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第５．２(1) , (9) , 第６．４ (1) , (5)
暗号化等による通信経路の保護	生成、取得、移転・提供	・CPSF Ver.1.0 DS-23 ・ISO/IEC 27001:2013 A.13.2.1, A.13.2.3 ・NIST SP 800-53 Rev. 5 CA-3, SC-8, SC-11, SC-12, SC-13 ・DAMA-DMBoK（第7章） 3.2 HTTPS ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Data Protection ・安全なウェブサイトの作り方 改訂第７版 2.3 ネットワーク盗聴への対策 ・ISO/IEC 27035-1:2015 7.2.2 Information on current/planned networking, 8.8 Cryptographic based services ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
保管されたデータ等の暗号化	保管	・CPSF Ver.1.0 DS-3 ・ISO/IEC 27001:2013 A.10.1.1 ・NIST SP 800-53 Rev. 5 SC-28

暗号化等によるデータの加工・利用過程の保護	加工・利用	-
データの完全性、真正性保護	移転・提供、保管	・CPSF Ver.1.0 CPS.DS-11, CPS.CM-4CPS.DS-10, CPS.CM-3 ・ISO/IEC 27001:2013 A.13.2.3, A.14.1.2, A.14.1.3A.12.2.1, A.12.5.1, A.14.2.4 ・NIST SP 800-53 Rev. 5 SC-16, SI-7SI-3, SI-7 ・DAMA-DMBoK（第7章） 2.3.5.3 データセキュリティの管理と保守3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・ISO/IEC 27035-1:2015 7.2.2 8.8 Cryptographic based services ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
適切な方法によるデータ及び媒体の廃棄	廃棄	・CPSF Ver.1.0 CPS.DS-6, CPS.IP-6 ・ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 ・NIST SP 800-53 Rev. 5 MP-6 ・DAMA-DMBoK（第7章） 4.7 ドキュメントのサニタイズ ＜より詳細なガイドライン＞ ・NIST SP 800-88 Rev. 1 4 Information Sanitization and Disposition Decision Making
データ及び媒体廃棄の履行確認	廃棄	・ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 ・NIST SP 800-53 Rev. 5 MP-6 ＜より詳細なガイドライン＞ ・NIST SP 800-88 Rev. 1 4.7 Verify Methods, 4.8 Documentation
機器・サービスの初期設定及び設定等の変更管理	生成、取得、保管	・CPSF Ver.1.0 CPS.AM-1, IP-1, IP-2, .PT-2 ・ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4 ・NIST SP 800-53 Rev. 5 CM-2, CM-7, CM-8, CM-11, PE-20 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Device Identification, Device Configuration ・NISTIR 8259B Documentation, Education and Awareness

運用時の機器・システムの真正性確認	生成、取得	・CPSF Ver.1.0 CPS.DS-13 ・ISO/IEC 27001:2013 A.11.2.4 ・NIST SP 800-53 Rev. 5 SA-10, SI-7
継続的なアプリケーションのセキュリティ管理	加工・利用、移転・提供	・CPSF Ver.1.0 CPS.DS-10, CPS.DS-13, CPS.IP-2, CPS.MA-1 CPS.CM-3 ・ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.1, A.14.2.4, A.14.2.5 ・NIST SP 800-53 Rev. 5 CM-2, CM-5, SI-3, SI-7 ・DAMA-DMBoK（第7章） 3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第５．２(9), 第６．４（5） ・ISO/IEC 27035-1:2015 ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan, 3.3 Maintaining the Information Exchange
端末、ネットワーク上におけるマルウェア対策の導入	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.DS-10, CPS.CM-3 ・ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.2.4 ・NIST SP 800-53 Rev. 5 SI-3, SI-7 ・DAMA-DMBoK（第7章） 3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Cybersecurity State Awareness ・NISTIR 8259B Information and Query Reception ・安全なウェブサイトの作り方 改訂第７版 2.1.1 OS やソフトウェアの脆弱性情報を継続的に入手し、脆弱性への対処を行う、2.6 WAF によるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第５．２(9), 第６．４（5）
脆弱性対応プロセスの整備、実	生成、取得、	・CPSF Ver.1.0 CPS.RA-1, CPS.RA-2, CPS.IP-10, CPS.MA-1,

行	移転・提供、加工・利用、保管	CPS.CM-7 ・ISO/IEC 27001:2013 A.6.1.4, A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.3 ・NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SI-2, SI-4, SI-5 ・DAMA-DMBoK（第7章） 4.2 セキュリティパッチの即時適用 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 4, Activity 5, Activity 6 ・NISTIR 8259A Device Configuration, Software Update ・NISTIR 8259B Information Dissemination ・安全なウェブサイトの作り方 改訂第 7 版 2.1.1 OS やソフトウェアの脆弱性情報を継続的に入手し、脆弱性への対処を行う ・AI・データの利用に関する契約ガイドライン データ編 第５．２(4)，(9)，第６．４（5） ・ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management ・NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange
機器等が設置された物理的環境におけるアクセス制御	生成、取得、保管	・CPSF Ver.1.0 CPS.AC-2 ・ISO/IEC 27001:2013 A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8 ・NIST SP 800-53 Rev. 5 PE-2, PE-3, PE-4, PE-5 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
機器等が設置された物理的環境の監視	生成、取得、保管	・CPSF Ver.1.0 CM-2 ・ISO/IEC 27001:2013 A.11.1.2, A.11.2.5, A.11.2.6 ・NIST SP 800-53 Rev. 5 CA-7, PE-3, PE-6, PE-8, PE-20 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
機器等の物理的耐性の強化	生成、取得	・CPSF Ver.1.0 CPS.DS-8 ・ISO/IEC 27001:2013 A.8.2.3, A.10.1.2, A.11.1.4, A.11.1.5, A.11.2.1

		・NIST SP 800-53 Rev. 5 SR-9, SR-11 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
ネットワークの分離等によるデータフローの制御	移転・提供	・CPSF Ver.1.0 CPS.AM-4, CPS.AC-7, CPS.CM-1 ・ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 ・NIST SP 800-53 Rev. 5 AC-4, CA-3, CA-9, SC-7 ・DAMA-DMBoK（第7章） 3.5 ファイアウォール（予防） ＜より詳細なガイドライン＞ ・ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management ・NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange
通信経路、端末の挙動等の監視、対処	生成、取得、移転・提供、加工・利用	・CPSF Ver.1.0 CM-1, CM-5, CM-6 ・ISO/IEC 27001:2013 A.12.4.1, A.12.4.2 ・NIST SP 800-53 Rev. 5 AU-12, AU-13, AU-14, CA-7, PE-21, SC-7, SI-4 ・DAMA-DMBoK（第7章） 2.3.5.3 データセキュリティの管理と保守、3.4 侵入検知と防止ソフトウェア、3.5 ファイアウォール ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Cybersecurity State Awareness ・NISTIR 8259B Information and Query Reception ・安全なウェブサイトの作り方 改訂第 7 版 2.6 WAFによるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第５．２(1)，(9)，第６．４(1)，(5) ・ISO/IEC 27035-1:2015 8.2.4 Network monitoring, 8.5 Network audit logging and monitoring ・NIST SP 800-47 Rev.1 3.3.3 Maintaining the Information Exchange
入力値の検証	生成、取得、	・CPSF Ver.1.0 CPS.CM-3

	加工・利用	・ISO/IEC 27001:2013 A.12.2.1 ・NIST SP 800-53 Rev. 5 SI-10 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・安全なウェブサイトの作り方 改訂第 7 版 1.1 SQL インジェクション、1.2 OS コマンド・インジェクション、1.3 パス名パラメータの未チェック／ディレクトリ・トラバーサル、1.10 バッファオーバーフロー、2.6 WAF によるウェブアプリケーションの保護プリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第５．2 (1) , (9) , 第６ 4 (1) , (5)
外部向き通信の監視、対処	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.DS-9 ・ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.13.1.1, A.13.2.1 ・NIST SP 800-53 Rev. 5 AC-4, SC-7, SI-4 ・DAMA-DMBoK（第7章） 2.3.5.1 機密レベルの割り当て、2.3.5.2 規制対象カテゴリの割り当て、2.3.5.3 データセキュリティの管理と保守、3.6 メタデータの追跡 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・安全なウェブサイトの作り方 改訂第 7 版 2.6 WAFによるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第５．2 (1) , (9) , 第６．4 (1), (5)
データ取得時の利用目的等の提示	生成、取得	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-1-1 利用目的の特定, 3-1-2 利用目的の変更, 3-3-2 要配慮個人情報の取得, 3-3-3 利用目的の通知又は公表, 3-3-4 直接書面等による取得, 3-3-5 利用目的の通知等をしなくてよい場合
正当な手段によるデータの取得	生成・取得	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-3-1 適正取得（法第17条第1項関係）

第三者提供に係る正当な根拠の確保	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-1 第三者提供の制限の原則（法第 23 条第 1 項関係）, 3-4-2 オプトアウトによる第三者提供（法第 23 条第 2 項～第 4 項関係）, 3-4-3 第三者に該当しない場合（法第 23 条第 5 項・第 6 項関係）, 3-4-4 外国にある第三者への提供の制限（法第 24 条関係） ・個人情報保護法ガイドライン（外国にある第三者への提供編）全般
第三者提供時の記録・確認の実施	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-5 第三者提供に係る記録の作成等（法第 25 条関係）, 3-4-6 第三者提供を受ける際の確認等（法第 26 条関係） ・個人情報保護法ガイドライン（第三者提供時の確認・記録義務編）全般
外国にある第三者へのデータ提供時に必要な手続きの実施	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-4 外国にある第三者への提供の制限（法第24条関係） ・個人情報保護法ガイドライン（外国にある第三者への提供編） 全般
仮名加工情報、匿名加工情報に対する識別行為の禁止	加工・利用	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-1-3 利用目的による制限（法第16条第1項関係）, 3-1-4 事業の承継（法第16条第2項関係）, 3-1-5 利用目的による制限の例外（法第16条第3項関係） ・個人情報の保護に関する法律についてのガイドライン （匿名加工情報編） 3-6 識別行為の禁止（法第 36 条第 5 項、第 38 条関係）
仮名加工情報、匿名加工情報の適正な加工	加工・利用	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編）2-8　匿名加工情報（法第2条第9項関係） ・個人情報の保護に関する法律についてのガイドライン （匿名加工情報編） 3-2 匿名加工情報の適正な加工（法第 36 条第 1 項関係
本人からの求めに応じた保有個	保管	＜より詳細なガイドライン＞

人データの訂正・利用停止等		・個人情報保護法ガイドライン（通則編）　3-5-3 保有個人データの訂正等（法第29条関係）, 3-5-4 保有個人データの利用停止等（法第30条関係）, 3-5-5 理由の説明（法第31条関係）, 3-5-6 開示等の請求等に応じる手続（法第32条関係）
個人データに対する安全管理措置の実施	保管	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編）3-3-2 安全管理措置（法第20条関係）, 3-3-3 従業者の監督（法第21条関係）, 3-3-4 委託先の監督（法第22条関係）
データの遅滞ない消去	保管	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-3-1 データ内容の正確性の確保等（法第19条関係）
秘密管理性を確保した営業秘密等の管理	生成、取得、移転・提供	＜より詳細なガイドライン＞ ・営業秘密管理指針 2．秘密管理性について（2）必要な秘密管理措置の程度＜
営業秘密を企業内外で共有する場合の秘密管理性の確保	移転・提供	＜より詳細なガイドライン＞ ・営業秘密管理指針 2．秘密管理性について（4）営業秘密を企業内外で共有する場合の秘密管理性の考え方
他社の秘密情報等の分離管理	保管	＜より詳細なガイドライン＞ ・営業秘密管理指針 2．秘密管理性について（4）営業秘密を企業内外で共有する場合の秘密管理性の考え方
データを処理、保管するサーバ等設備の所在地の確認	保管	-

別紙２　ガイドライン等の普及・啓発に係る調査

© Hitachi, Ltd. 2024. All rights reserved.

目次

1. はじめに …… 2
   1-1. 調査の目的 …… 3
   1-2. 調査の全体像と推進スケジュール …… 6

2. 中小企業に対するガイドライン等の普及・啓発に関する取組みの現状 …… 9
   2-1. 中小企業における情報セキュリティ対策状況の実態 …… 10
   2-2. 政府や関連団体による普及・啓発に関する取組みの現状 …… 35
   2-3. 中小企業及び支援機関等を対象としたヒアリング調査 …… 60

3. 中小企業を対象としたガイドライン等の普及・啓発に関する課題・施策 …… 69
   3-1. 中小企業を対象としたガイドライン等の普及・啓発に関する課題 …… 70
   3-2. 普及・啓発に関連する国内外の取組み …… 77
   3-3. 中小企業を対象としたガイドライン等の普及・啓発に資する施策 …… 100

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

1. はじめに

© Hitachi, Ltd. 2024. All rights reserved.

1-1. 調査の目的

© Hitachi, Ltd. 2024. All rights reserved.

本調査の目的(1/2)

- 本調査項目は、仕様書に記載の内容も踏まえ、CPSFに基づくガイドライン及びユースケース等の認知・利用拡大を推進していく上での現状と課題等を整理及び、それに係る経済産業省、IPA及び民間団体等との役割分担の明確化を図ることを目的とするものと認識する。

仕様書の記載

- CPSFに基づくガイドライン等の普及・啓発の推進について、様々な産業界での普及・拡大を進めることを目的とし、普及・啓発活動を推進する。具体的には、様々な産業界におけるCPSFやこれに連なるガイドラインやユースケース等の認知・普及の拡大に向けた課題の調査や対策の検討を実施する。具体的な調査項目や実施内容については、担当者と協議の上で決定することとし、研究会等での議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。
- 加えて、CPSFに基づき整備が進んでいるガイドラインやユースケース等の認知・拡大を推進していく上での現状と課題等を整理し、調査報告書にまとめる。調査報告書の具体的な内容については担当者と協議の上で決定する。

直近の問題意識

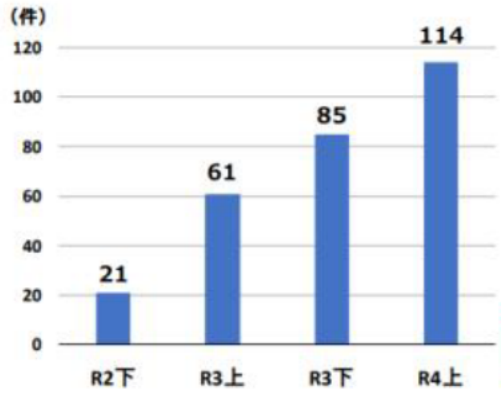
- ガイドラインの策定及び普及に係る権限をIPAに付与・移管していくことを予定しており、移管後のMETIとIPA、または民間団体との役割分担等も視野に入れて検討を行う。

© Hitachi, Ltd. 2024. All rights reserved.

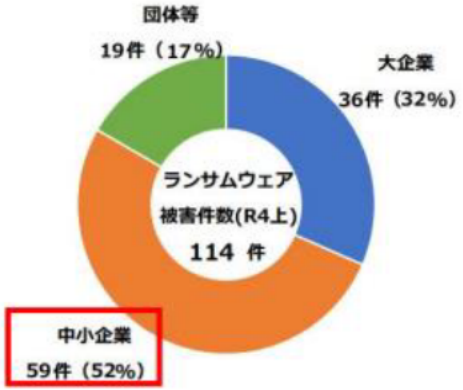
本調査の目的(2/2)

- 近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。
- 本調査では、CPSFに基づくガイドライン等の主たる普及・啓発対象として中小企業を念頭に置き、上記課題の解決に資するべく検討を進める。

- 企業等における**サイバー被害（ランサムウェア被害）**の警察庁への報告件数は**右肩上がりに増加中**。
- 被害件数(114件)の内訳は、大企業が36件（32%）に対して、**中小企業は59件（52%）と過半数超**。

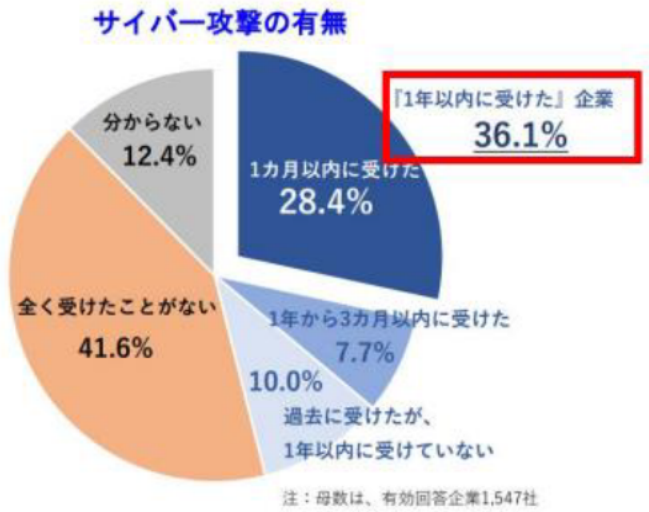


企業・団体等における
ランサムウェア被害の報告件数



ランサムウェア被害企業等の
規模別件数

中小企業の約36%が1年以内にサイバー攻撃の被害



[出典] 中小企業が取り組むべきセキュリティ対策のいろは
https://www.ipa.go.jp/security/sc3/activities/chushoWG/images/07/02_iroha.pdf

© Hitachi, Ltd. 2024. All rights reserved.

1-2. 調査の全体像と推進スケジュール

© Hitachi, Ltd. 2024. All rights reserved.

ガイドライン等の普及・啓発に係る調査の全体像

HITACHI
Inspire the Next

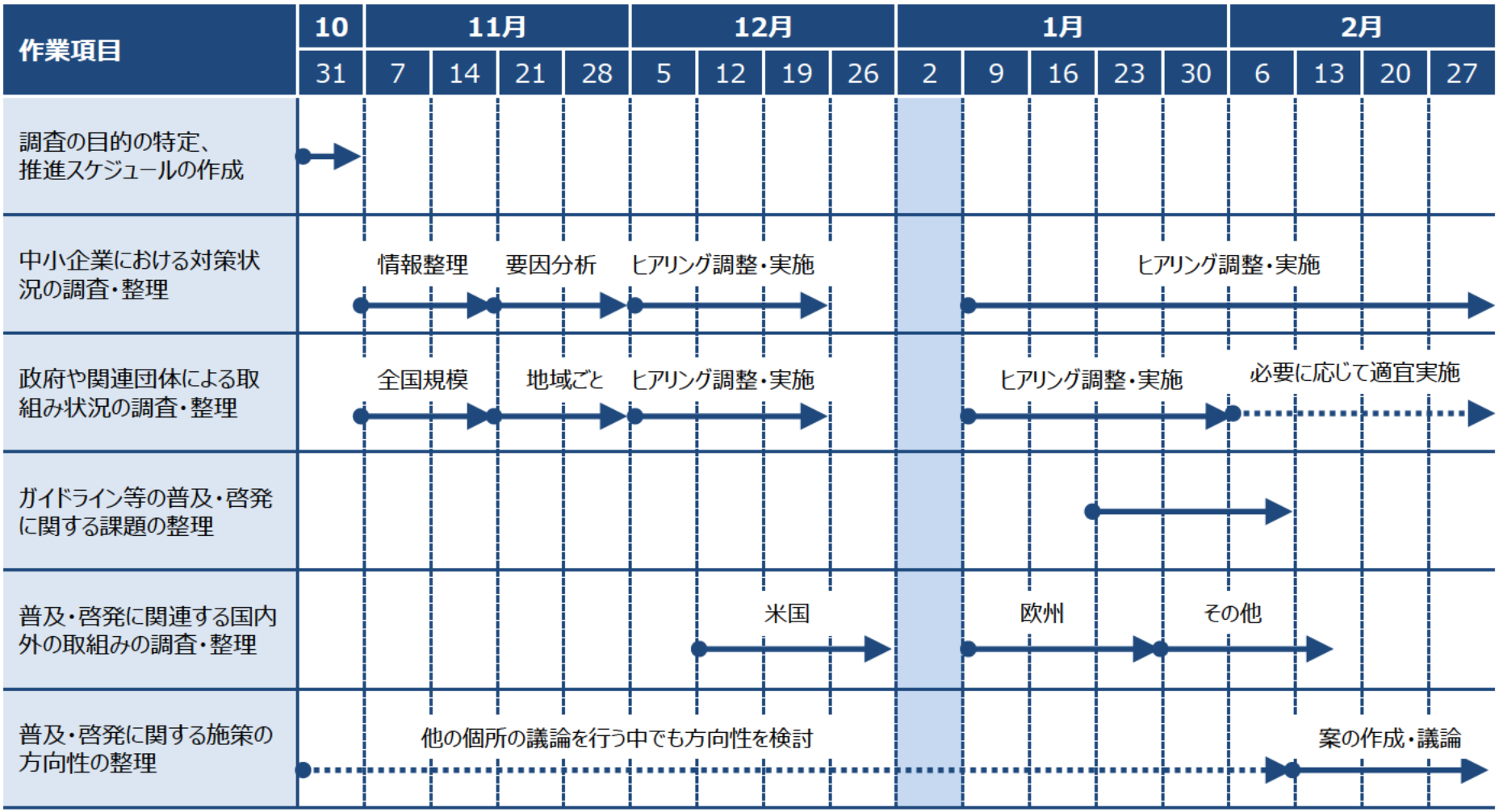
- 2023年10月24日に実施した定例会議にて、本調査を下記の項目に基づき実施する点を合意した。
- その後、ヒアリング調査の実施(2-3)等の変更を施しつつ、2章以降の調査を行った。

1. 調査の目的等		
1-1	調査の目的	-
1-2	推進スケジュール	-
2. 中小企業を対象としたガイドライン等の普及・啓発に関する取組みの現状		
2-1	中小企業における情報セキュリティ対策状況の実態 2-1-1 ガイドライン等の普及及びセキュリティ対策の状況 2-1-2 普及及び対策推進を妨げていると考えられる要因	• 既存ガイドライン(CPSF関連の他、経営ガイドライン、中小企業ガイドライン等)はどの程度認知または活用されているか。 • 認知または利用している場合、認知経路や利用の理由(きっかけ)は何か。
2-2	政府や関連団体による普及・啓発に関する取組みの現状 2-2-1 政府機関主導の全国規模の取組み 2-2-2 民間団体主導の全国規模の取組み 2-2-3 地域単位での取組み	• CPSF関連またはそれ以外のガイドライン等の普及・啓発に向けて活動する主体にはどのようなものがあり、具体的に誰に何を行っているか。 • それぞれの取組みはどの程度効果を上げているか。 • 成功している取組みの優れた点とその要因は何か。 • 目的の実現に向けて、政府・行政機関または民間団体はどのような問題に直面しているか。
3. 中小企業を対象としたガイドライン等の普及・啓発に関する課題・施策		
3-1	ガイドライン等の普及・啓発に関する課題	• 2章で特定された現状に対して、ヒト/モノ/カネ/情報のそれぞれの観点から達成すべき課題は何か。 ※分析観点については仮のもの • 上記のうち、全体で共通する課題及び、CPSFに基づくガイドラインに特有の課題にはどのようなものがあるか。 • 特定された課題にアプローチする際に想定されるリスクや懸念点にはどのようなものがあるか。
3-2	普及・啓発に関連する国内外の取組み	• 海外または国内(サイバーセキュリティ以外の領域)では日本で想定されるものと同様の課題に対して、どのような施策を講じているか。 • 当該施策が効果を上げていると考えられる場合、その要因は何か。
3-3	CPSFに基づくガイドラインの普及・啓発に関する施策の方向性	• CPSFに基づくガイドライン等の普及において効果及び実行可能性の観点から望ましい施策は何か。

© Hitachi, Ltd. 2024. All rights reserved.

推進スケジュール

- 10月最終週から具体的な検討に取り掛かり、2月末を目途に報告書のとりまとめを行った。
- 内容は机上調査を中心としつつ、12月から翌年2月にかけて事業者・団体等へのヒアリングを実施した。



※ヒアリング調査等の一部を3月初旬にわたって実施した。

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2. 中小企業に対するガイドライン等の普及・啓発に関する取組みの現状

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2-1. 中小企業における情報セキュリティ対策状況の実態

© Hitachi, Ltd. 2024. All rights reserved.

現状調査結果のサマリ (1/2)

HITACHI
Inspire the Next

調査項目		調査結果の概要
i	中小企業の動向に関する基本データ	**日本に所在する企業の大多数が中小企業に該当** • 建設業や製造業、情報通信業等の対象業種または地域という観点のいずれでも小規模企業が最も多く、次いで中小企業(小規模企業を除く)、大企業の数が多い。
ii	IT投資・サイバーセキュリティ関連投資額	**ほとんどの場合、中小企業のIT/セキュリティ投資は100万円未満と少額** • 直近3期のIT投資額について、67.8%の中小企業が100万円未満、17.5%が500万円未満と回答。 • 直近3期の情報セキュリティ投資額について、82.3%が100万円未満、8.2%が500万円未満であり、6.0%がわからないと回答。
iii	サイバーセキュリティに係る脅威状況・認識	**多数の中小企業がサイバー攻撃の被害に遭っている一方、組織的対策を未実施** • 中小企業の約36%が一年以内にサイバー攻撃の被害を受けたと回答している。 • セキュリティに係る組織体制は、「組織的には行っていない」の割合が最も高く 49.2%。回答企業の約4割が5名以下の事業者であることを考えれば妥当な結果と解釈されている。
iv	具体的なサイバーセキュリティ対策状況	**ウイルス対策ソフト・サービスの導入以上の対策を行っている中小企業(特に小規模企業)は少なく、ガイドライン準拠の支援を行うサービスの利用は2.8%と極めて少数** • 導入済セキュリティ製品・サービスは、「ウイルス対策ソフト・サービスの導入」の割合が最も高く77.2%、次いで「ファイアウォール(35.6%)」、「VPN(17.1%)」となっている。 • セキュリティ業務の外部委託は、「委託していない」の割合が最も高く58.7%となっている。次いで、「わからない(11.3%)」、「ウイルス監視サービス(10.8%)」となっている。 • ガイドライン準拠の支援を行うコンサルティングサービスの利用は、2.8%と極めて少数。
v	情報収集の実施状況	**情報収集を常時できている中小企業は3割程度である中、多くは業界団体やIT業者からの情報提供を活用** • 中小企業では「機会があれば情報を収集している」が最も多く選択されており、「常時情報を収集している」割合は3割以下である。 • 4割強が業界団体から、2/3程度がIT業者から情報を取得している一方、社外セミナーへの参加やメディア記事の参照は、上記と比較すると限られている。 • ヒアリングでは、IT事業者から自社に必要で具体的なアドバイスが提供されること、業界団体から提供される情報の内容と当社の実態が合っていない等の意見があった。

© Hitachi, Ltd. 2024. All rights reserved.

現状調査結果のサマリ (2/2)

HITACHI
Inspire the Next

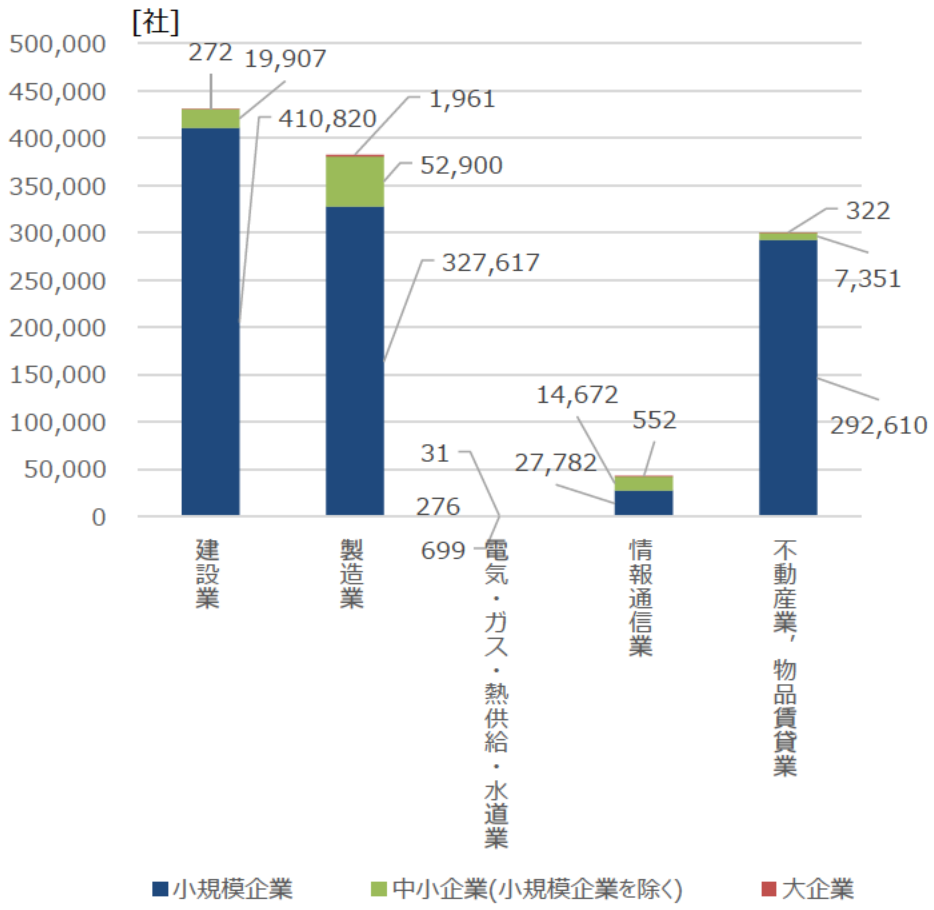
調査項目		調査結果の概要
vi	ガイドライン等の認知状況/利用状況	**全般的によく認知・利用されているとは言えない状況の中、CPSFに基づくガイドライン等の認知・利用状況は未だ低調** • 中小企業の中で比較的規模の大きい企業にあっても、認知度は経営ガイドラインで29.9%、ISMSで35.1%、その他はほぼ10%以下にとどまる。 • 中小企業の中で比較的規模の大きい企業にあっても、利用率は経営ガイドラインで13.0%、ISMSで10.4%、その他は3%以下にとどまる。 • IPAが実施する活動の認知度について、「知っているものはない」の割合が最も高く69.8%となっている。次いで、「中小企業の情報セキュリティ対策ガイドライン(14.1%)」、「SECURITY ACTION(5.8%)」となっている。
vii	ガイドライン等の認知/利用のきっかけ・動機	**CPSF等認知の主なきっかけは、インターネット、IT関連事業者、業界団体** • インターネット、IT関連事業者、業界団体が中小企業によるCPSF認知のきっかけとされる。一方で、メディア記事や社外セミナー等による普及効果は薄い。 • 経営ガイドラインにおいても基本的な状況はCPSFと同様だが、ISMSとNIST CSFでは社外のIT関連事業者経由で認知を得たという割合が相対的に高い。 • 利用のきっかけとしては、全体を通じて、自社内または業界団体、IT関連事業者の呼びかけが主な活用のきっかけとされ、内外のセキュリティ事故はきっかけとしてあまり機能していない。大企業においては、経営ガイドラインやISMS、NIST CSFの普及にあたって、取引先やIT関連事業者が一定の役割を果たしている。
viii	ガイドライン等を活用していない理由	**ガイドラインを活用しない理由として、人材不足や手順や参照先の不明確さを多く選択** • 大企業と比較して人材不足や手順や参照先の不明確さを多く選択している。 • 従業員50名未満の中小企業の23.9%、50～100名の20.0%が利用の必要性を感じていない。
ix	ガイドライン等の活用において直面している課題	**推進人材の不足、予算の制約や不明確な進め方が利用上の課題** • 課題はガイドラインにより様々だが、推進人材の不足、予算の制約や不明確な進め方という課題は共通する。ヒアリングでは、金銭支援策に関する要望が多かった。 • 約半数以上が、解説文書や詳細なガイドラインの公開を要望している。 • 50名未満の30.4%、50~100名の23.3%、100~300名の16.9%が要望は特にないと回答している。

© Hitachi, Ltd. 2024. All rights reserved.

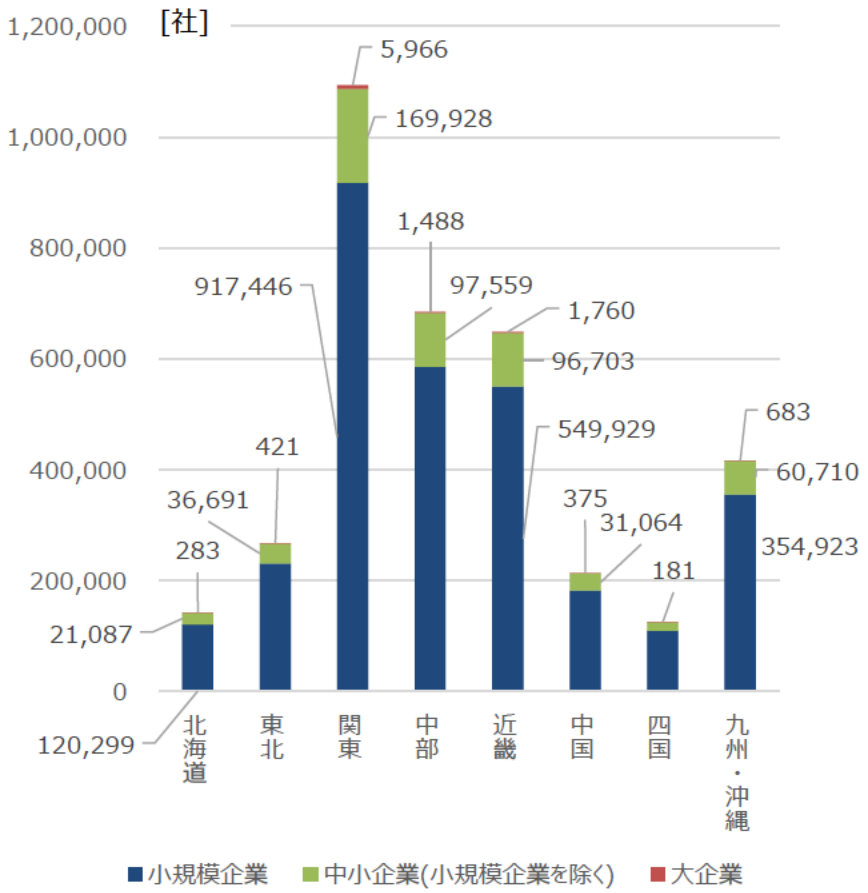
i. 中小企業に関する基本データ

- 対象とする業種または地域いずれにおいても中小企業(小規模企業含む)が圧倒的多数を占めている。

産業ごとの規模別企業数 (2016年)



地域ごとの規模別企業数 (2016年)



[出典] 中小企業庁「中小企業の企業数・事業所数」より日立作成

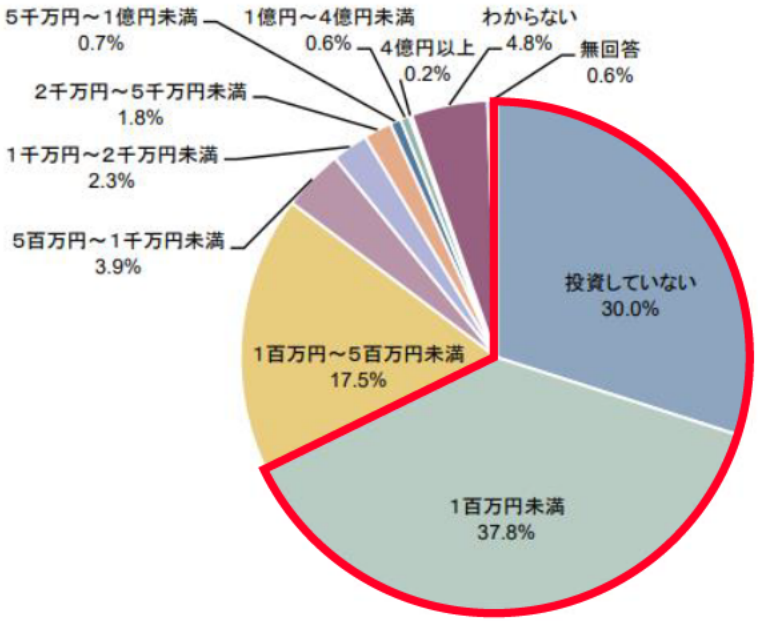
© Hitachi, Ltd. 2024. All rights reserved.

ii. 中小企業におけるIT投資・サイバーセキュリティ関連投資額

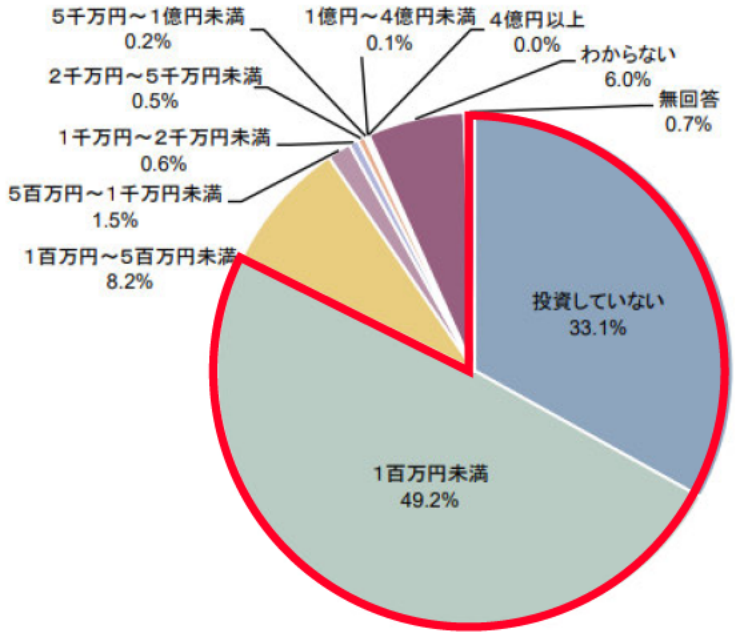
HITACHI Inspire the Next

- 直近3期のIT投資額について、67.8%の中小企業が100万円未満、17.5%が500万円未満と回答。
- 直近3期の情報セキュリティ投資額について、82.3%が100万円未満、8.2%が500万円未満であり、6.0%がわからないと回答。

直近3期のIT投資額



直近3期の情報セキュリティ対策投資額



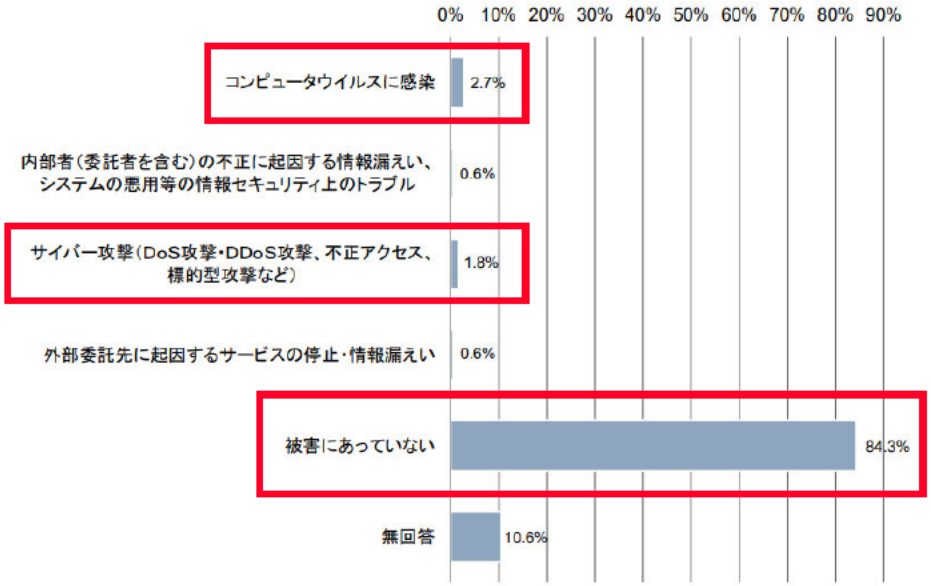
[出典] 2021年度中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 ―
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

© Hitachi, Ltd. 2024. All rights reserved.

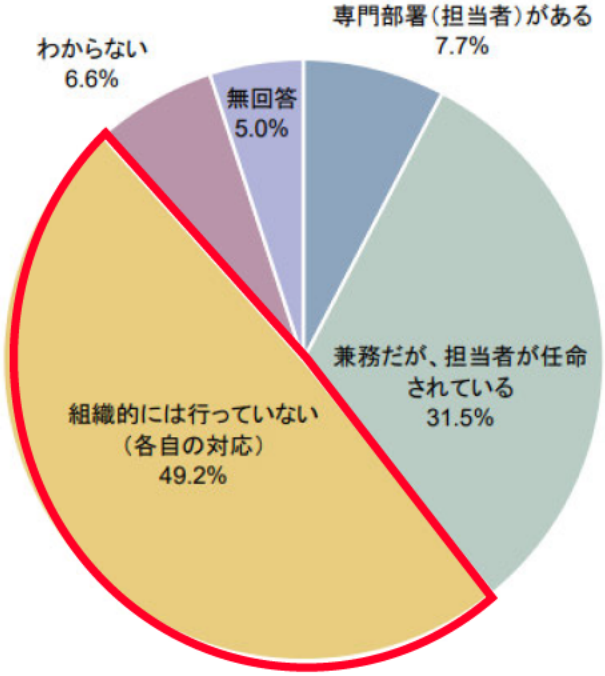
iii. サイバーセキュリティに係る脅威状況・認識

- 84.3%の中小企業が直近1年で「被害にあっていない」と回答しており、「コンピュータウイルスに感染(2.7%)」、「サイバー攻撃(DoS攻撃・DDoS攻撃、不正アクセス、標的型攻撃など)(1.8%)」は少数。
- セキュリティに係る組織体制は、「組織的には行っていない(各自の対応)」の割合が最も高く 49.2%となっている。回答企業の約4割が5名以下の事業者であることを考えれば妥当な結果と解釈されている。

セキュリティ被害の有無



中小企業における組織体制



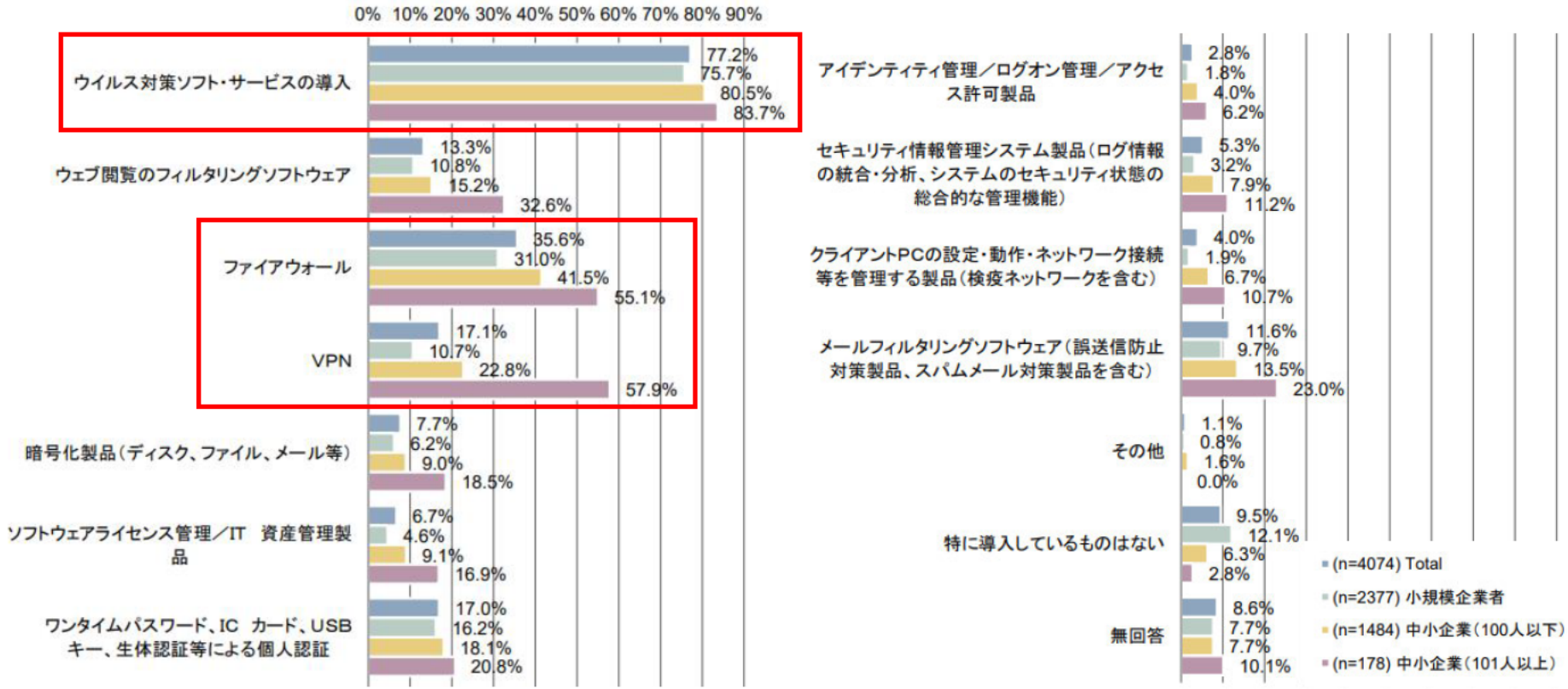
[出典] 2021年度中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 ―
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

© Hitachi, Ltd. 2024. All rights reserved.

iv. 具体的なサイバーセキュリティ対策状況

- 導入されている情報セキュリティ関連製品やサービスとして、「ウイルス対策ソフト・サービスの導入」の割合が最も高く77.2%となっている。次いで、「ファイアウォール(35.6%)」、「VPN(17.1%)」となっている。

情報セキュリティ関連製品やサービスの導入状況



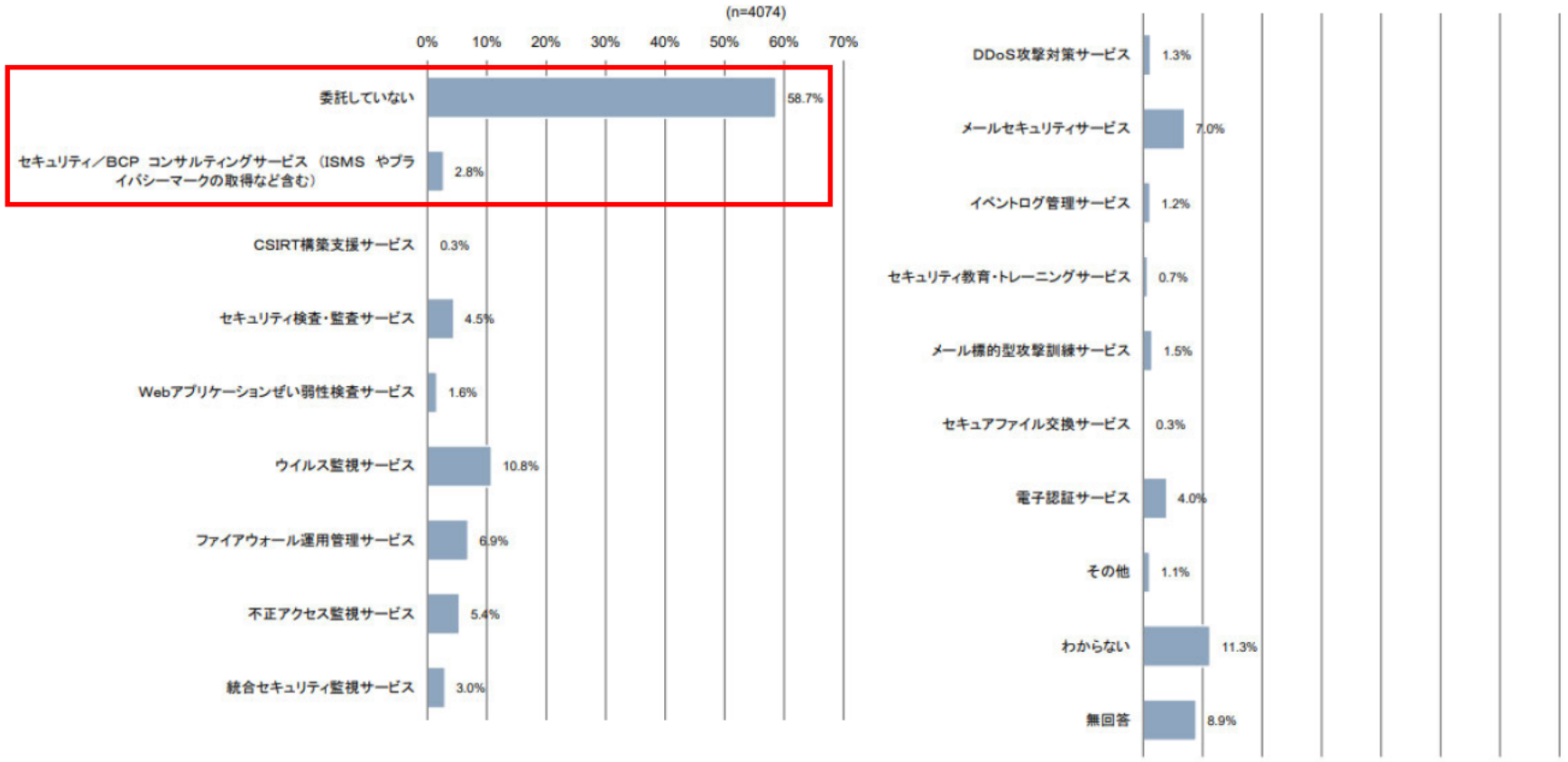
[出典] 中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 ―
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

© Hitachi, Ltd. 2024. All rights reserved.

iv. 具体的なサイバーセキュリティ対策状況

- 情報セキュリティ業務の外部委託について、「委託していない」の割合が最も高く58.7%となっている。次いで、「わからない(11.3%)」、「ウイルス監視サービス(10.8%)」となっている。
- ガイドライン準拠の支援を行うコンサルティングサービスの利用は、2.8%と極めて少数。

情報セキュリティ業務の外部委託の状況・内容



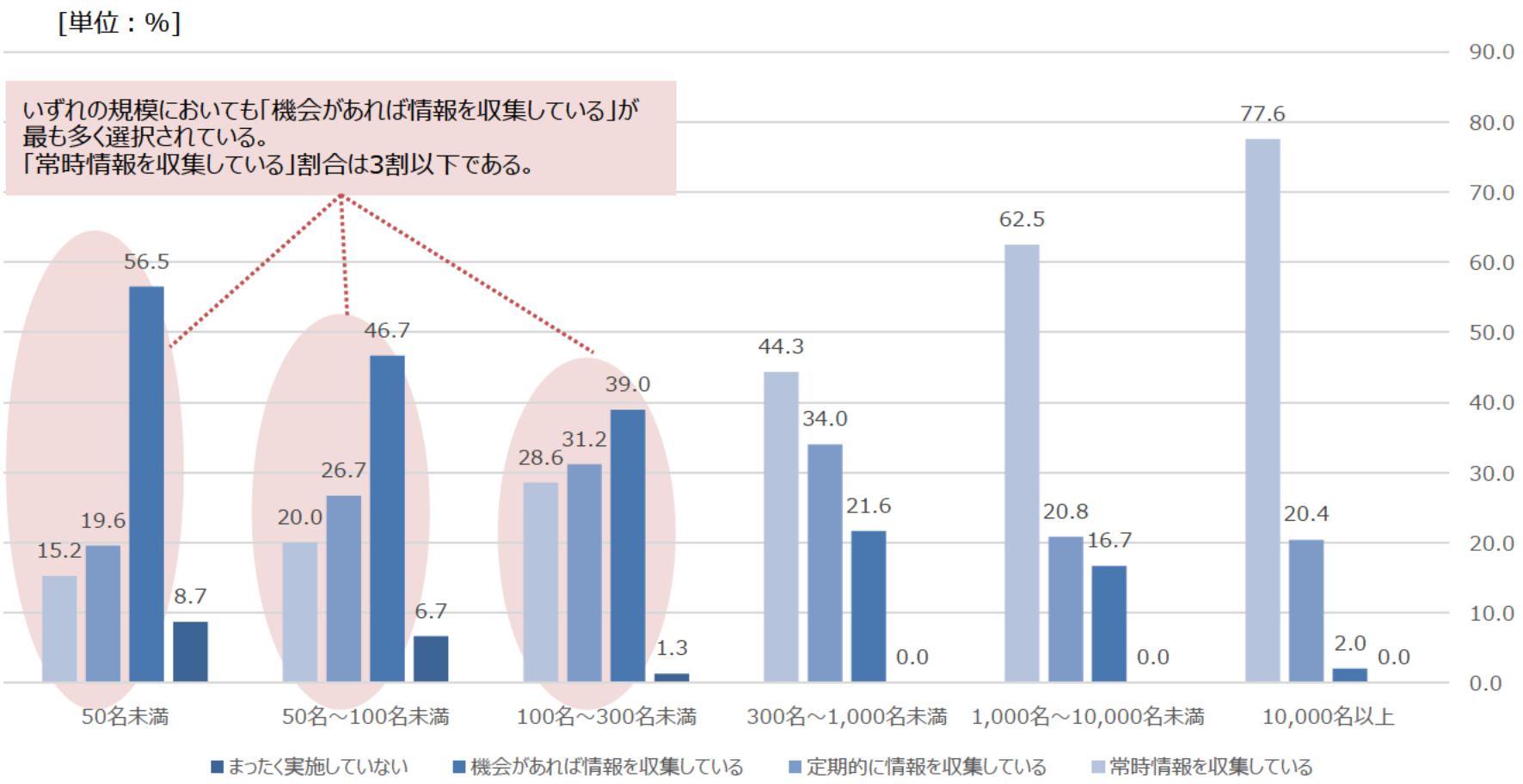
[出典] 中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 ―
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

© Hitachi, Ltd. 2024. All rights reserved.

v. 情報収集の実施状況

- 大企業では「常時情報を収集している」が最も多い一方で、中小企業では「機会があれば情報を収集している」が最も多く選択されており、「常時情報を収集している」割合は3割以下である。

従業員規模ごとの情報収集頻度



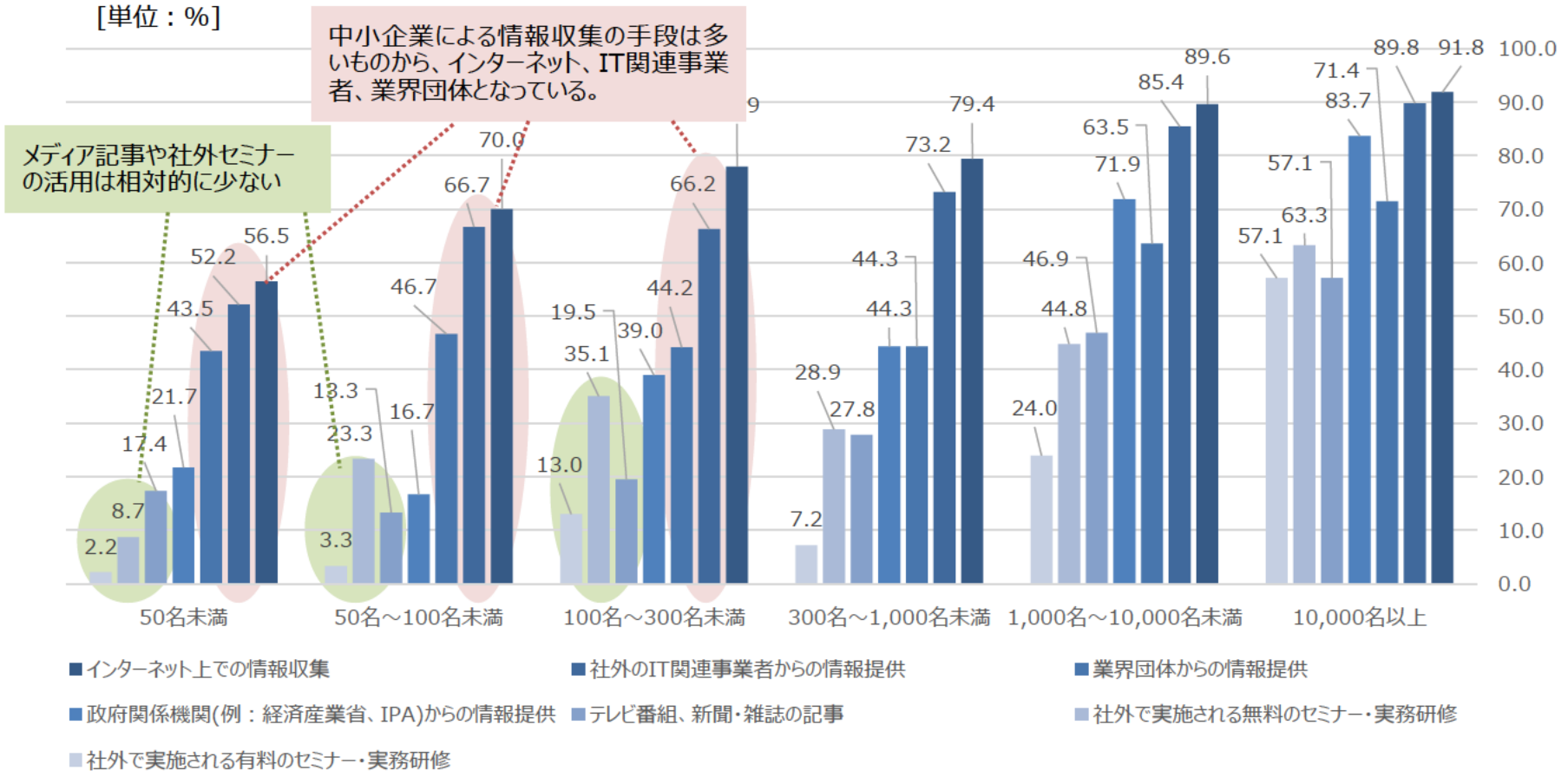
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

v. 情報収集の実施状況

- 4割強の中小企業が業界団体から、2/3程度の中小企業(50名以上)がIT業者から情報を取得している。
- 社外セミナーへの参加やメディア記事の参照は、上記と比較すると実施が限られている。

従業員規模ごとの情報収集手段



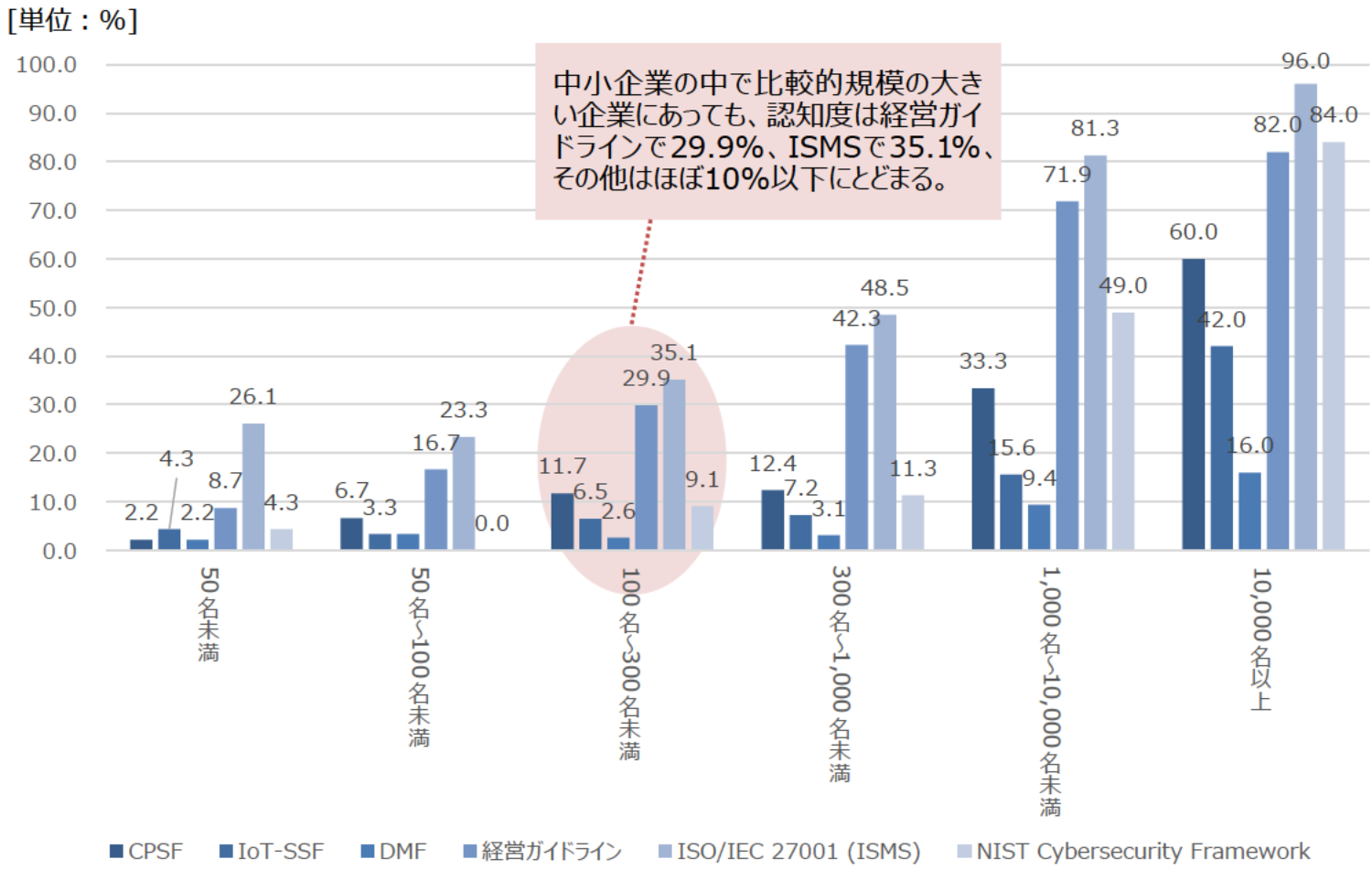
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vi. ガイドライン等の認知状況/利用状況

- 中小企業の中で比較的規模の大きい企業にあっても、認知度は経営ガイドラインで29.9%、ISMSで35.1%、その他はほぼ10%以下にとどまる。

従業員規模ごとのガイドラインの認知状況



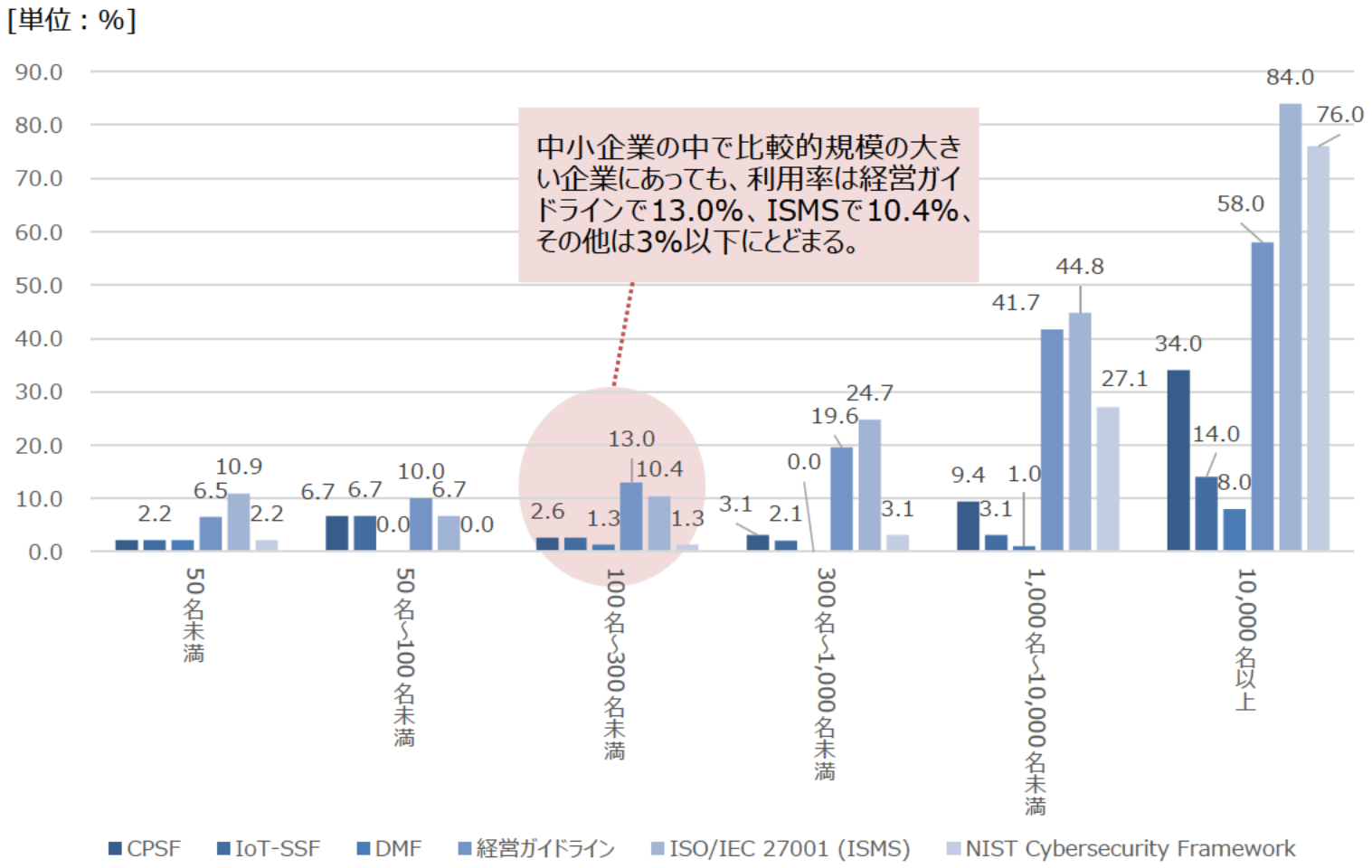
[出典] 昨年度実施のアンケート調査分析資料より

© Hitachi, Ltd. 2024. All rights reserved.

vi. ガイドライン等の認知状況/利用状況

- 中小企業の中で比較的規模の大きい企業にあっても、利用率は経営ガイドラインで13.0%、ISMSで10.4%、その他は3%以下にとどまる。

従業員規模ごとのガイドラインの利用状況



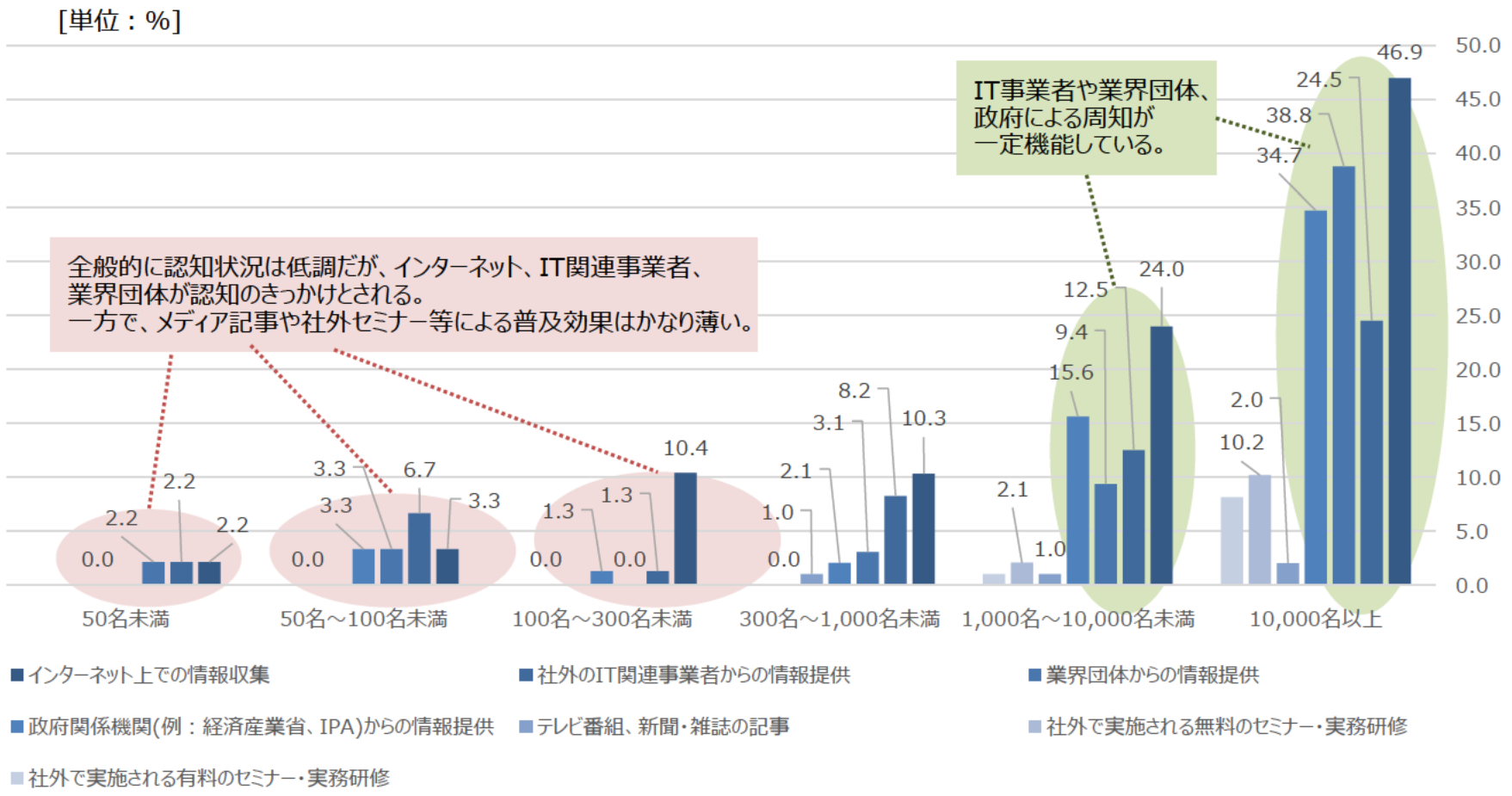
[出典] 昨年度実施のアンケート調査分析資料より

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 全般的に中小企業のCPSF認知状況は低調だが、インターネット、IT関連事業者、業界団体が認知のきっかけとされる。一方で、メディア記事や社外セミナー等による普及効果はかなり薄い。

従業員規模別のCPSF認知のきっかけ



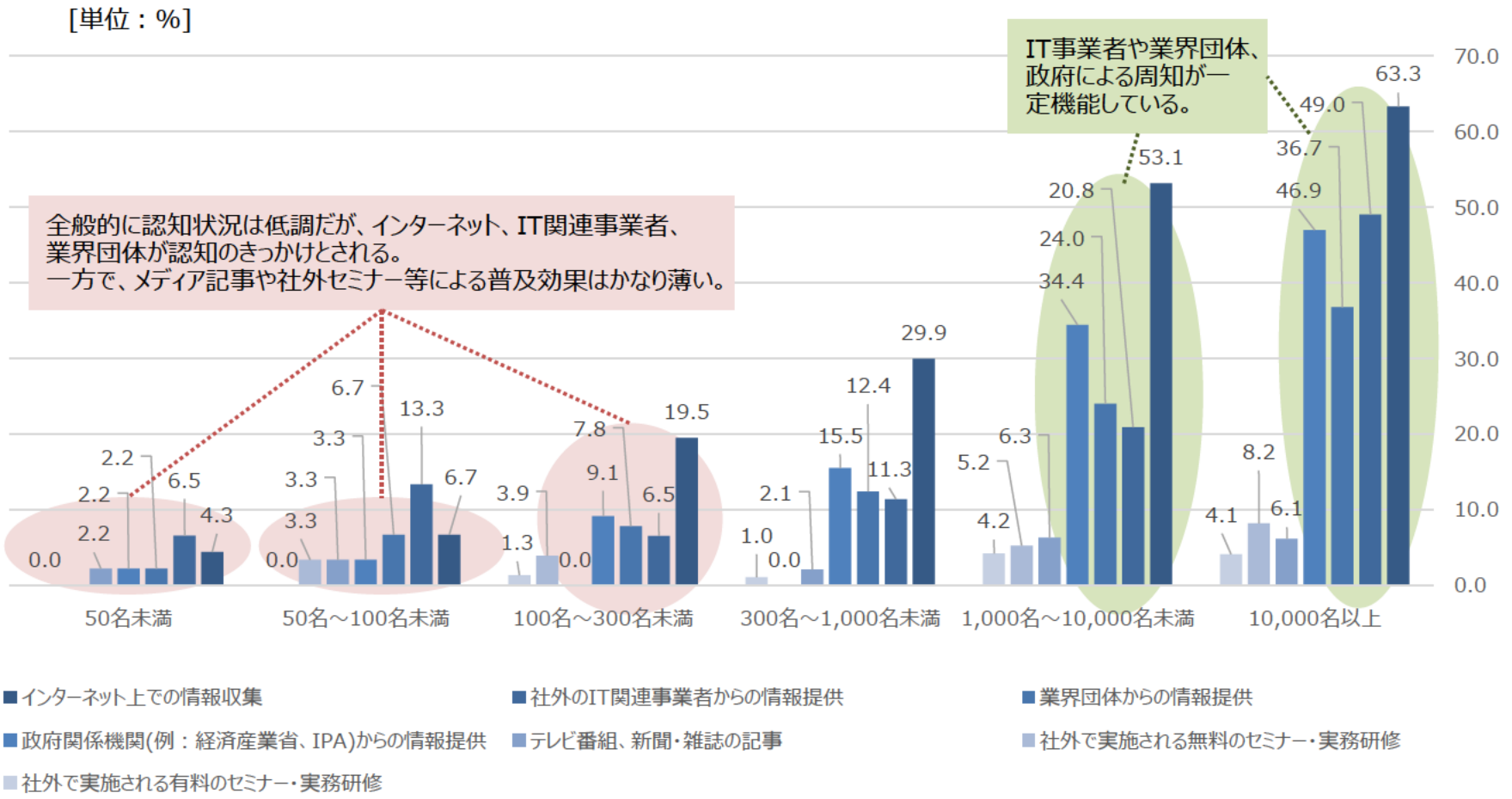
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 全体的な数値はより高い水準を示すものの、経営ガイドラインにおいても、基本的にはCPSFと同様の傾向がみられる。

従業員規模別の経営ガイドライン認知のきっかけ



[出典] 昨年度実施のアンケート調査結果を日立にて再分析

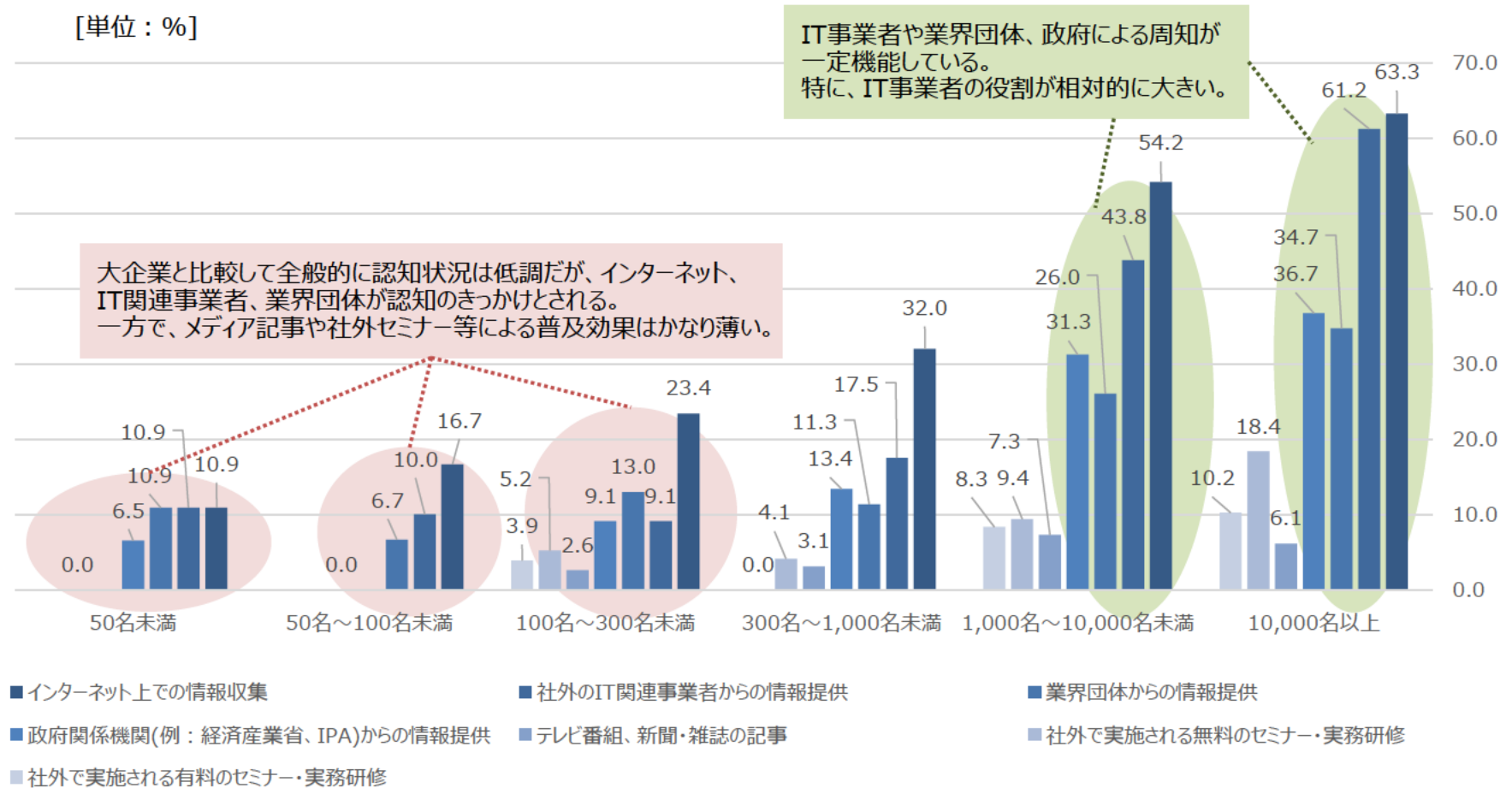
© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

HITACHI
Inspire the Next

- ISMSにおいては、経営ガイドラインの場合よりも、社外のIT関連事業者経由で認知を得たという割合がさらに高い。

従業員規模別のISO/IEC 27001(ISMS)認知のきっかけ



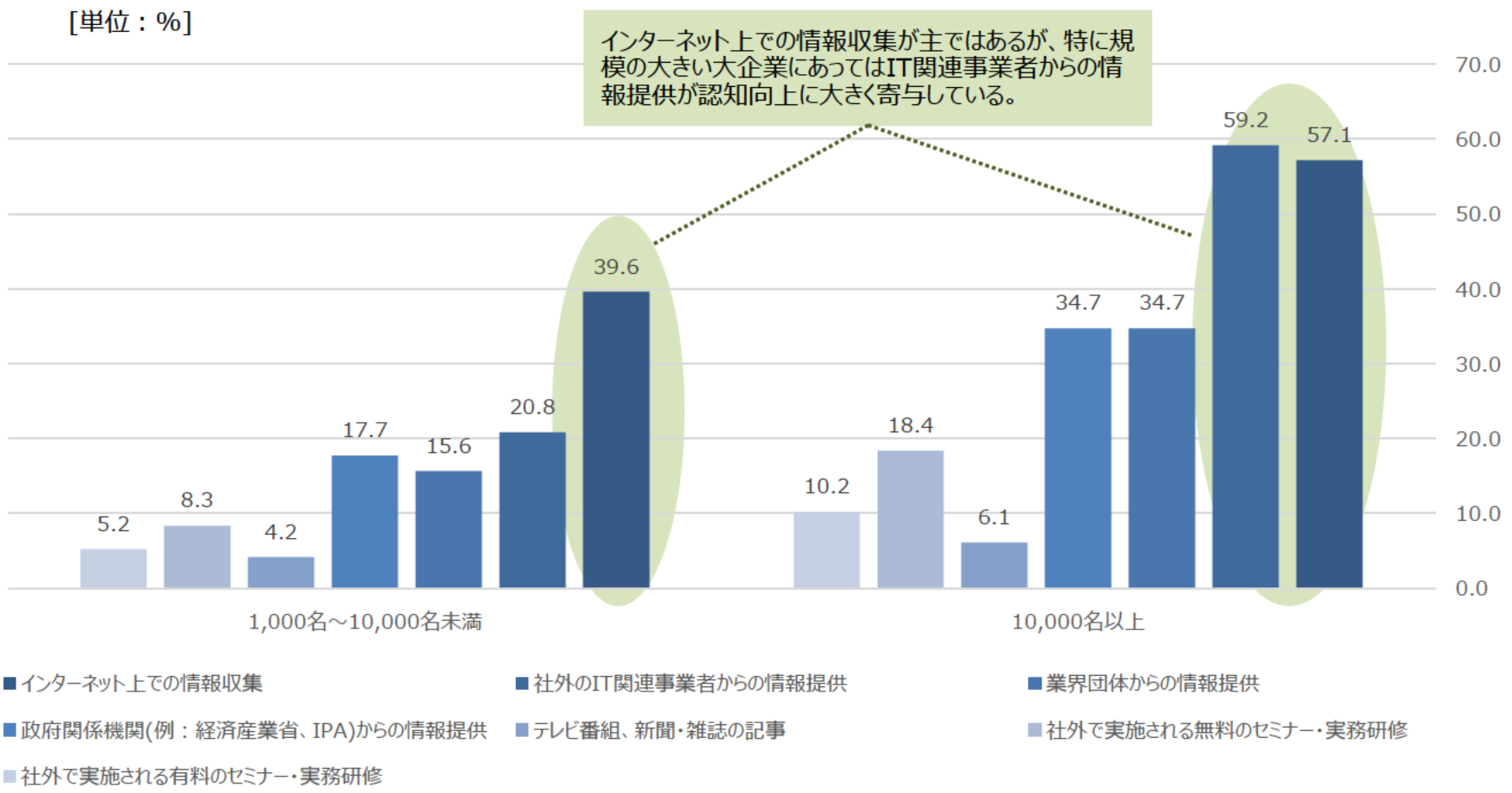
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- インターネット上での情報収集が主ではあるが、特に規模の大きい大企業にあってはIT関連事業者からの情報提供が認知向上に大きく寄与している。

従業員規模別のNIST CSF認知のきっかけ



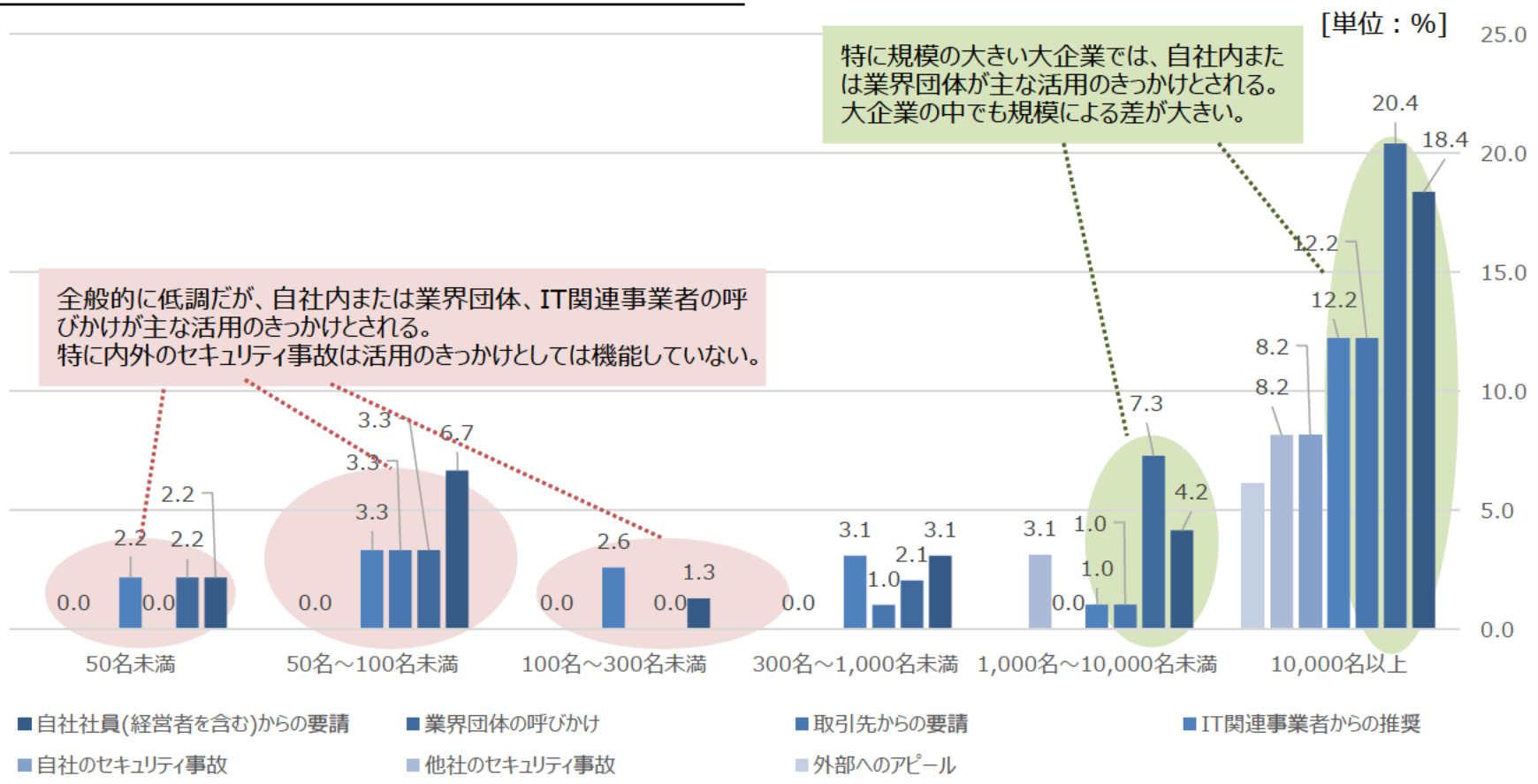
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 全般的に低調だが、自社内または業界団体、IT関連事業者の呼びかけが主な活用のきっかけとされる。
- 内外のセキュリティ事故はCPSF活用のきっかけとしてはあまり機能していない。
- 大企業の中でも10,000名以上の数値が飛びぬけており、規模による差が大きい。

従業員規模別のCPSF活用理由



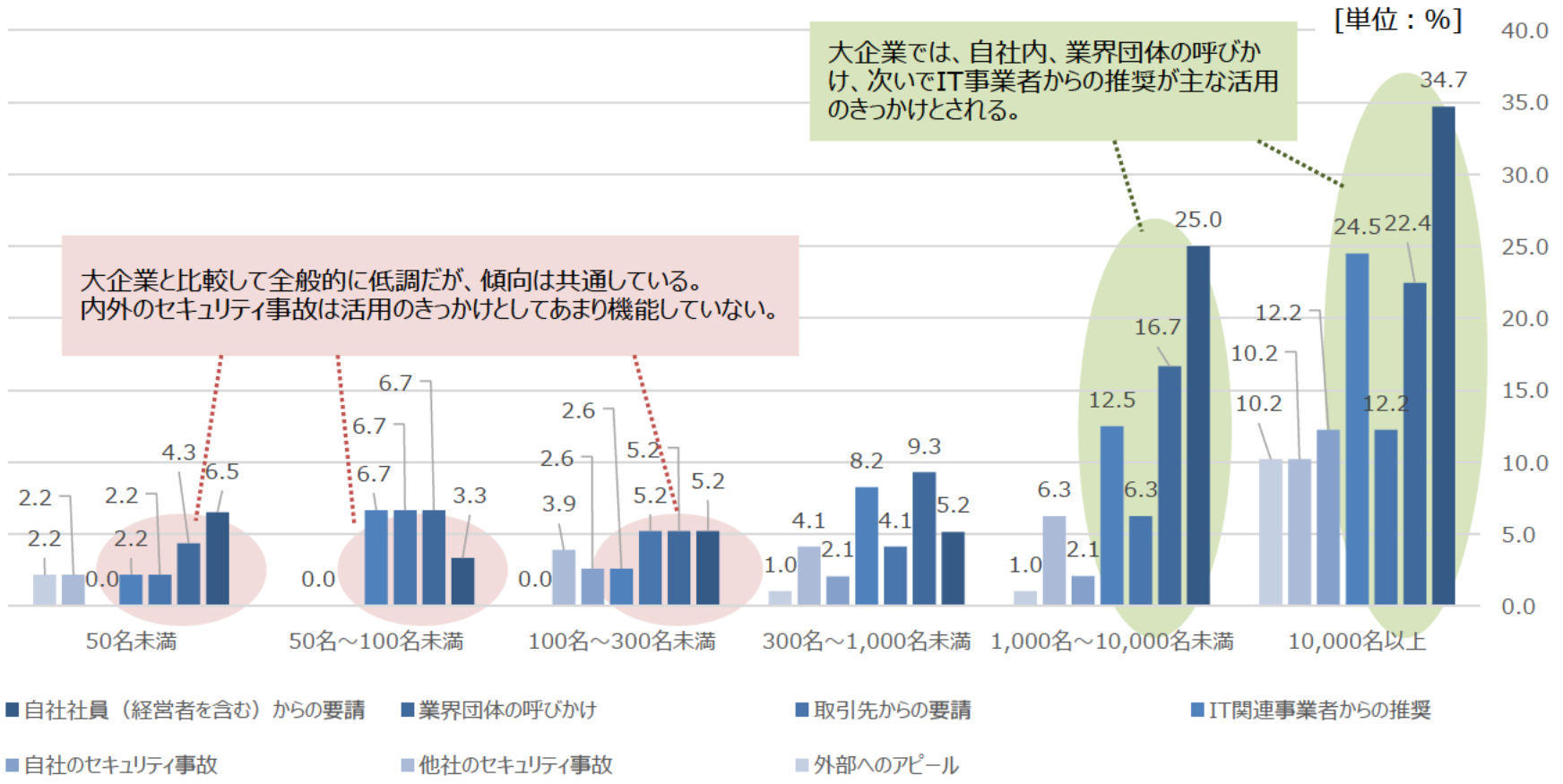
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 大企業では、自社内、業界団体の呼びかけ、次いでIT事業者からの推奨が主な活用のきっかけとされる。中小企業では大企業と比較して全般的に数値が低調だが、回答傾向は大企業と共通している。
- 内外のセキュリティ事故は活用のきっかけとしてあまり機能していない。

従業員規模別の経営ガイドライン活用理由



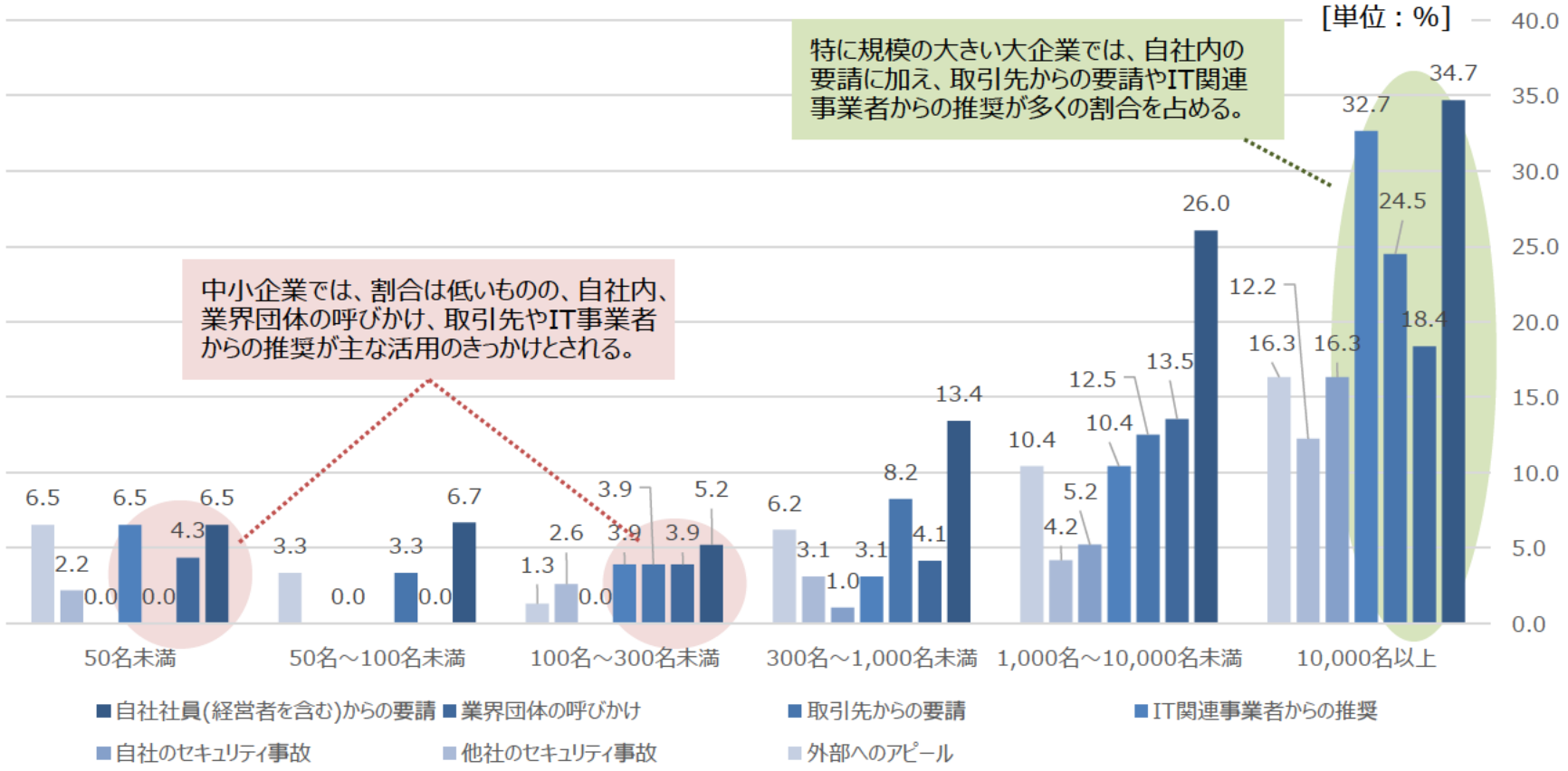
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 中小企業では、割合は低いものの、自社内、業界団体の呼びかけ、取引先やIT事業者からの推奨が主な活用のきっかけとされる。
- 大企業では、自社内の要請に加え、取引先からの要請やIT関連事業者からの推奨が多くの割合を占める。

従業員規模別のISO/IEC 27001(ISMS)活用理由



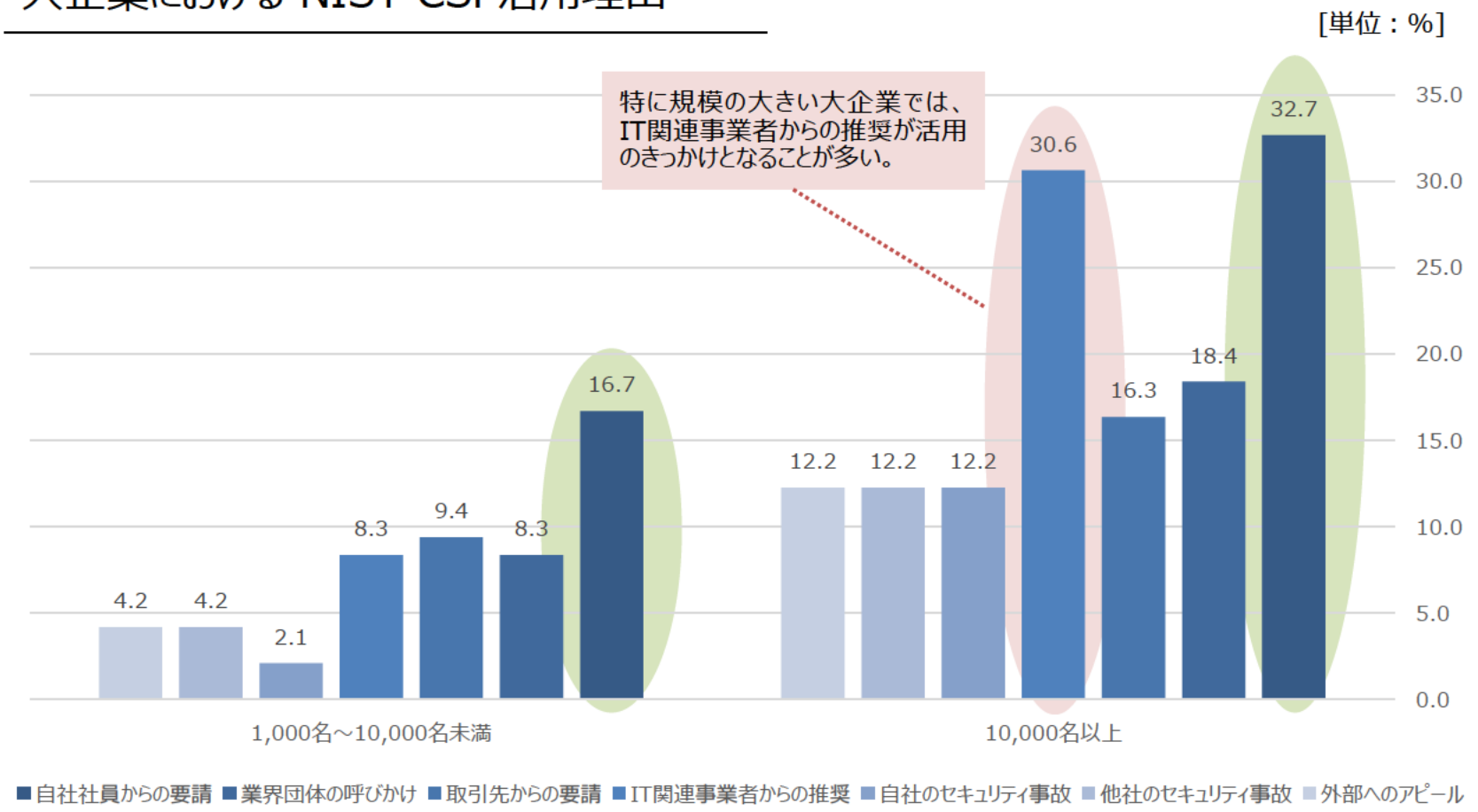
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

vii. ガイドライン等の認知/利用のきっかけ・動機

- 自社社員からの要請が主たるきっかけである点は他と共通するが、特に規模の大きい大企業では、IT関連事業者からの推奨が活用のきっかけとなることも多い。

大企業における NIST CSF活用理由



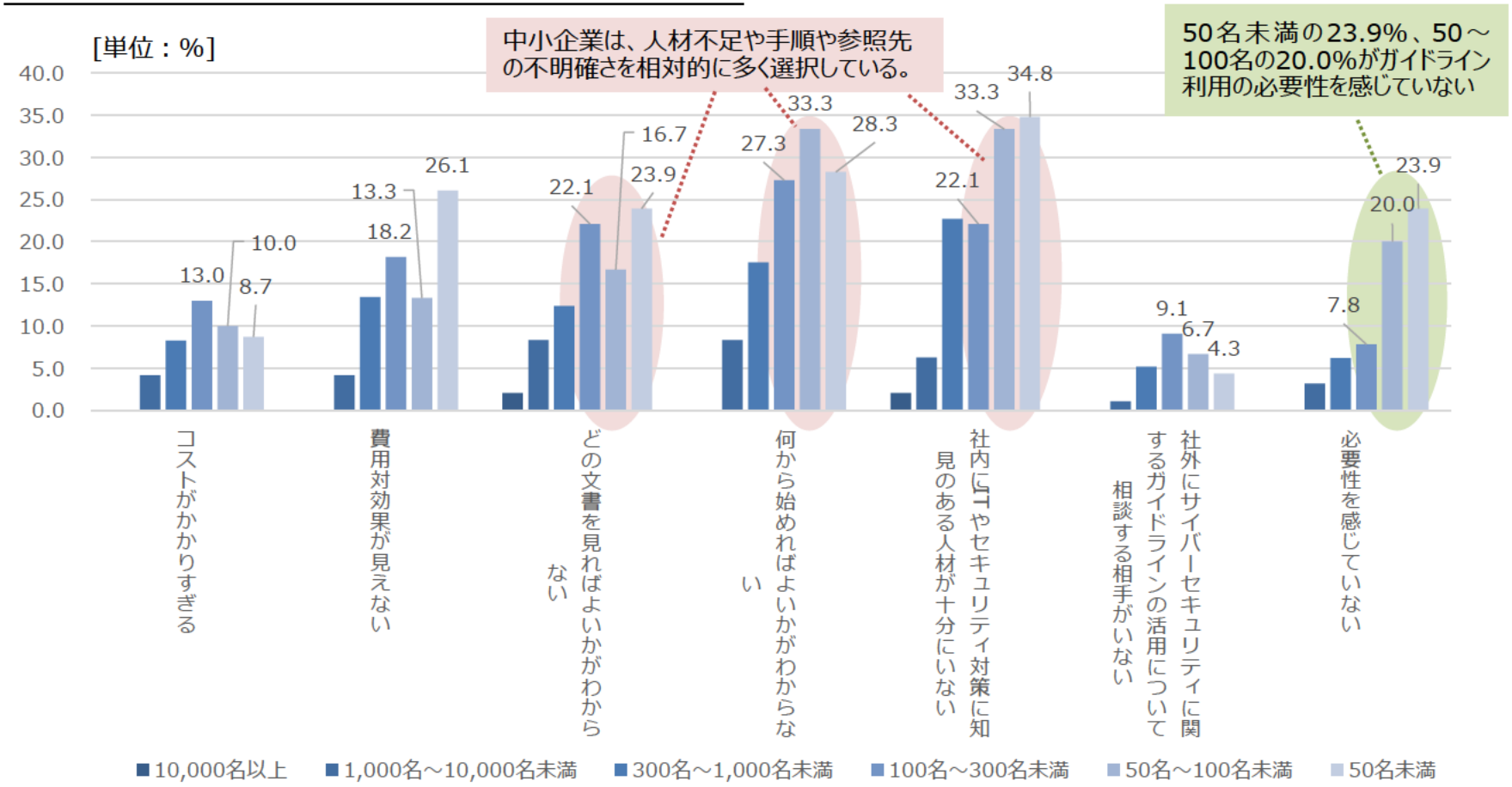
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

viii. ガイドライン等を活用していない理由

- 中小企業は、大企業と比較して人材不足や手順や参照先の不明確さを相対的に多く選択している。
- 従業員50名未満の中小企業の23.9%、50～100名の20.0%が利用の必要性を感じていない。

従業員規模別のガイドライン未利用理由



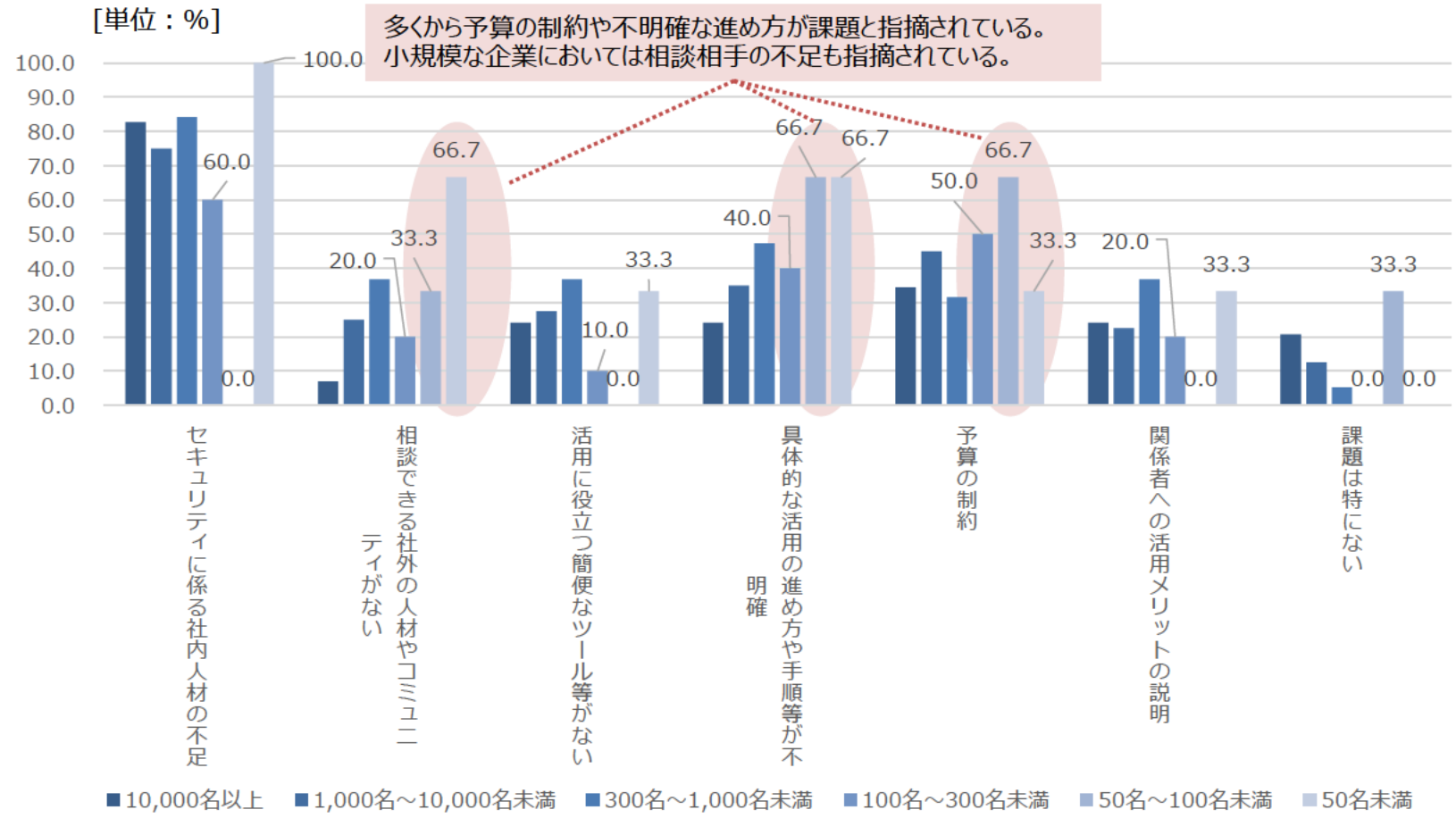
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

ix. ガイドライン等の活用において直面している課題

- 多くの中小企業から予算の制約や不明確な進め方が主な課題と指摘されている。
- また、小規模な企業においては相談相手の不足も上記と同様の水準で課題と指摘されている。

ガイドライン利用の課題(経営ガイドライン)



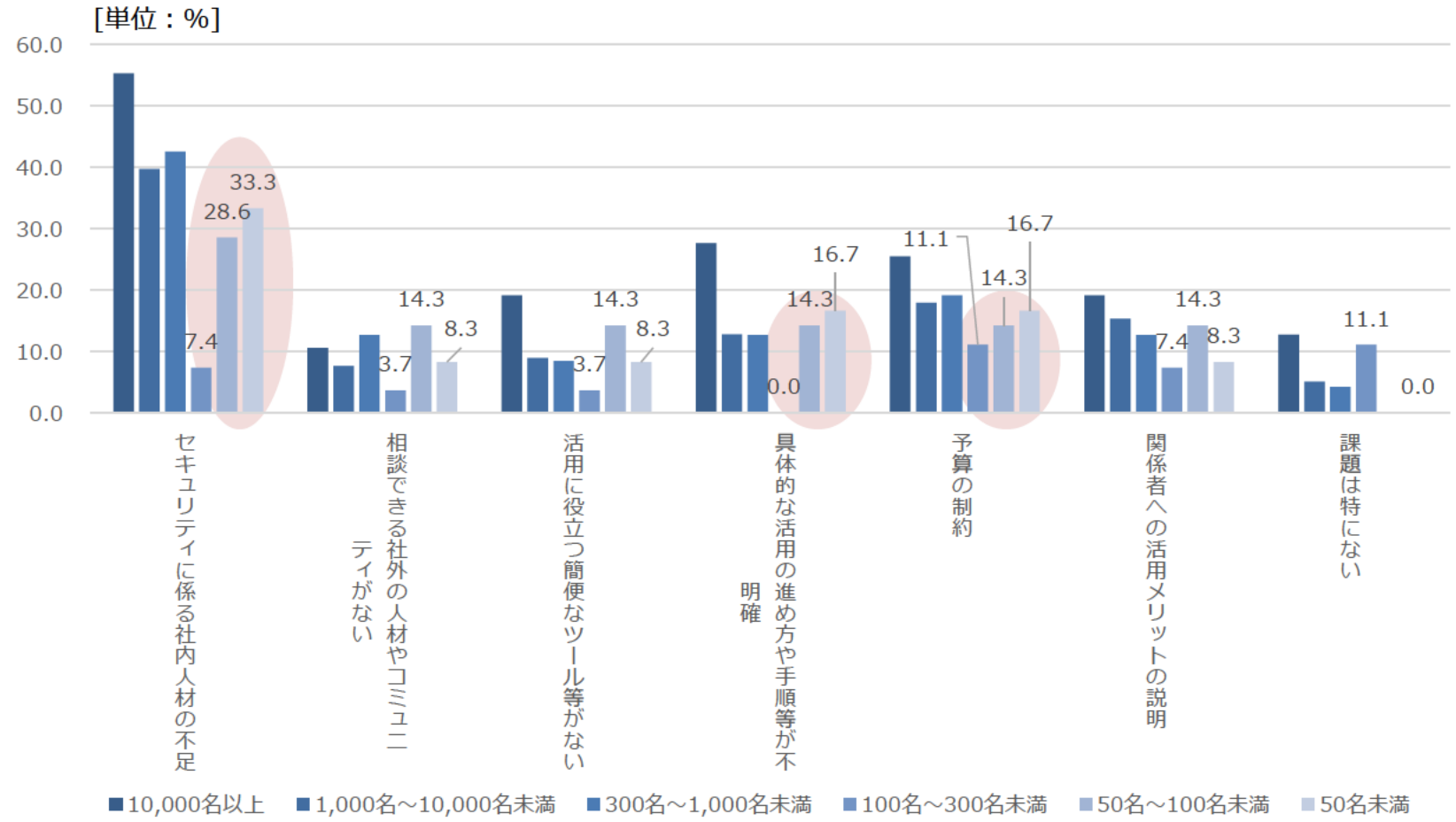
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

ix. ガイドライン等の活用において直面している課題

- 社内人材の不足に加えて、多くの中小企業から予算の制約や不明確な進め方が主な課題と指摘されている点は経営ガイドラインと共通している。

ガイドライン利用の課題(ISMS)



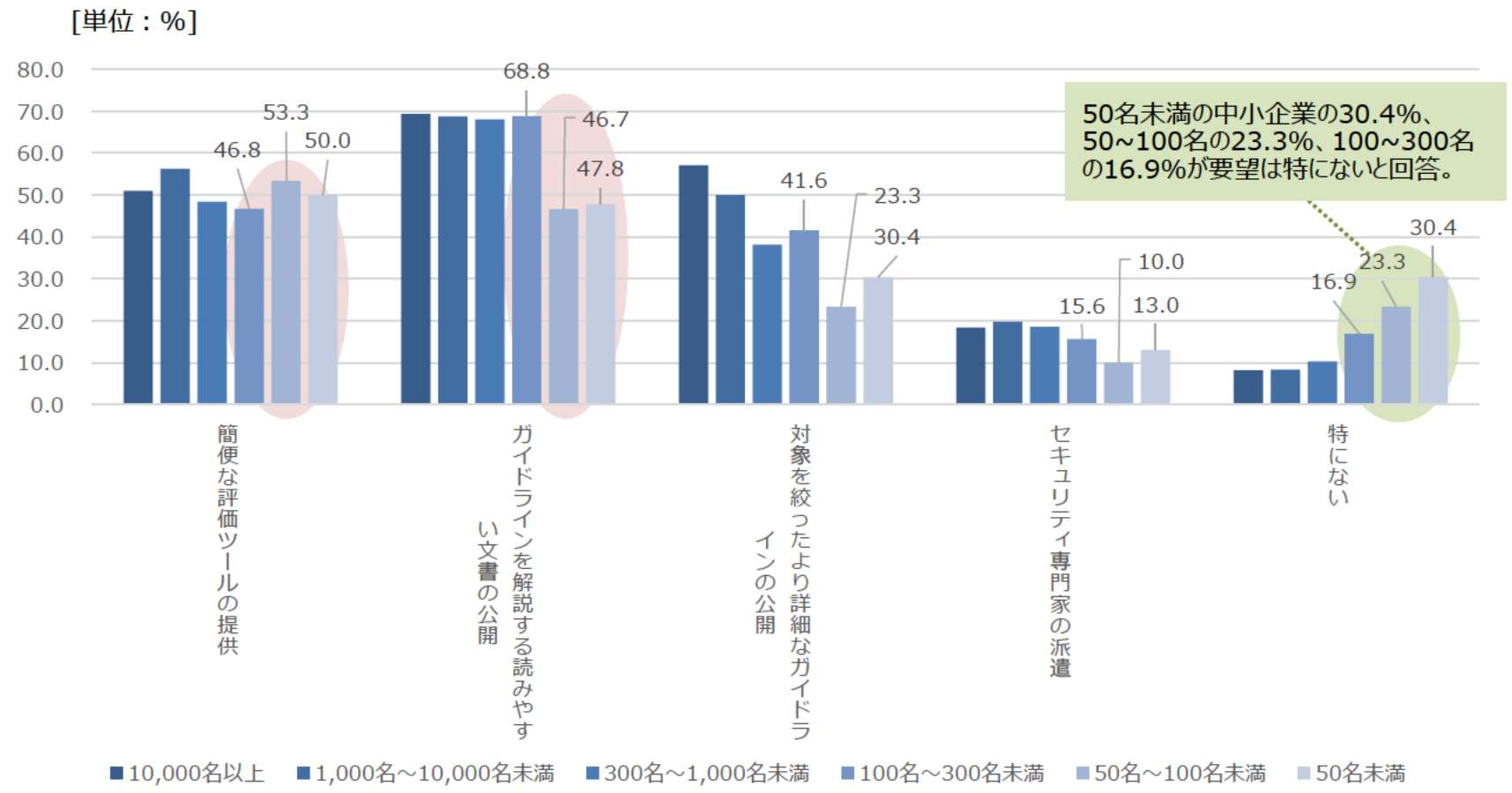
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

ix. ガイドライン等の活用において直面している課題

- 約半数以上の中小企業が、解説文書や詳細なガイドラインの公開を要望している。
- 50名未満の30.4%、50~100名の23.3%、100~300名の16.9%が要望は特にないと回答している。

従業員規模別の政策要望



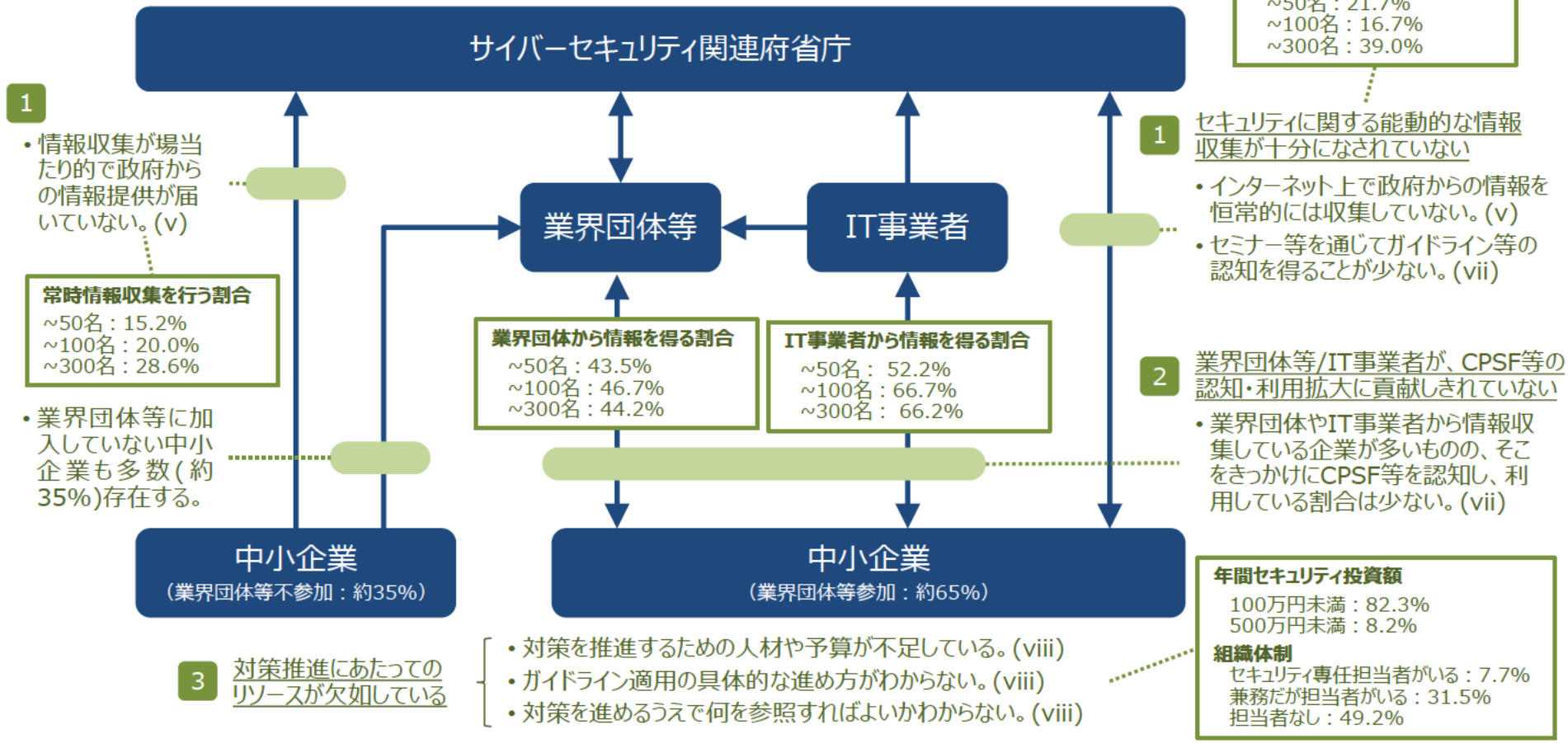
[出典] 昨年度実施のアンケート調査結果を日立にて再分析

© Hitachi, Ltd. 2024. All rights reserved.

普及及び対策推進を妨げていると考えられる要因

HITACHI
Inspire the Next

- これまでの調査結果に鑑み、普及及び対策推進に関する現状及び普及を妨げていると考えられる要因を以下のように整理した。
  1. 中小企業においてサイバーセキュリティに関する能動的な情報収集が十分になされていない
  2. 主要な情報の出し手である業界団体等またはIT事業者が、CPSF等の認知・利用拡大に貢献しきれていない
  3. 中小企業では対策推進にあたってのリソース(ヒト・モノ・カネ・情報)が欠如している



© Hitachi, Ltd. 2024. All rights reserved.

2-2. 政府や関連団体による普及・啓発に関する取組みの現状

© Hitachi, Ltd. 2024. All rights reserved.

2-2 の全体像

- 調査・整理事項として、ガイドライン等の普及・啓発に関する取組みを全国規模(2-2-1,2-2-2)の取組みと地域規模(2-2-3)で調査した。

2-2-1. 政府機関主導の全国規模の取組み

- ガイドラインごとに普及状況に関する取組みについて、以下を整理した。
  - i. 主体/取組みの概要
  - ii. 取組みの優れた点とその要因
  - iii. 取組みの成果(例:ガイドラインの普及割合)
- 政府機関の取組みにおいて、生じている問題・課題を整理した。

2-2-2. 民間団体主導の全国規模の取組み

- ガイドラインごとに普及状況に関する取組みについて、以下を整理した。
  - i. 主体/取組みの概要
  - ii. 取組みの優れた点とその要因
  - iii. 取組みの成果(例:ガイドラインの普及割合)
- 民間団体の取組みにおいて、生じている問題・課題を整理した。

2-2-3. 地域単位での取組み

- ガイドラインごとに普及状況に関する取組みについて、以下を整理した。
  - i. 主体/取組みの概要
  - ii. 取組みの優れた点とその要因
  - iii. 取組みの成果(例:ガイドラインの普及割合)
- 公共機関及び民間団体における地域規模の取組みにおいて、生じている問題・課題を整理した。

© Hitachi, Ltd. 2024. All rights reserved.

現状調査結果のサマリ (1/2)

調査項目		中小企業の情報セキュリティガイドライン	SECURITY ACTION	サイバーセキュリティ経営ガイドライン
i	主体/取組みの概要	• 貴省・IPAが各地の経済産業局等と協力してセミナー・演習にて周知。 • 貴省・IPAが企業側の自発的な活用を支援するための各種補助コンテンツ(概要資料、動画)を作成。 • 貴省がガイドラインに対応した認定制度(SECURITY ACTION)を創設することで利用を促進。	• 貴省・IPAが業界団体(例:JNSA)と連携してセミナーを実施。ただし、補助金申請の要件に含まれている場合があり、地方自治体も普及の一翼を担う。 • 貴省が、セキュリティガイドラインを認証制度の要件に組み込み、その認証の取得を補助金交付の要件とすることで、ガイドラインの利用を促進。	• 貴省・IPAがセキュリティプレゼンター制度等を通じて民間企業や人材を活用しつつ、普及啓発活動を実施。 • 貴省・IPAが企業側の自発的な利用を支援するため、プラクティス集の策定や可視化ツールの無償公開を実施。
ii	取組みの優れた点とその要因	• 地域の経済産業局と協力することで、中小企業がより自分ごととして捉えやすくしている。 • セミナー・演習の参加費用を抑えることで、中小企業がより参加しやすくしている。	• 費用的な負担がある場合に認証取得が進みにくいより小規模な企業においても、補助金の申請要件とすることで、SECURITY ACTIONの取得を促進させることができる。	• 具体的なセキュリティ対策を実装する際に企業がプラクティス集を活用可能。 • また、IT担当者は可視化ツールを活用することで、費用をかけず経営者層に対して問題提起が可能。
iii	取組みの成果(例:ガイドラインの普及割合)	• 中小企業を広く対象とした調査にて、認知率は14.1%、利用率は6.1%(どちらも2021年調査時点)と2割をどちらも下回っており、十分普及しているとは言えない。	• 中小企業における制度の認知率は5.8%、利用率は 1つ星を宣言した企業で2.6%、2つ星を宣言した企業で0.7%(全て2021年調査時点)にとどまっており、十分に普及しているとは言えない。	• 大企業を含む製造業者を対象にした調査にて、認知率は29.9%、利用率は13.0%(どちらも2022年調査時点)であり、中小企業を中心に過半数以上の事業者から認知を得られていない。

© Hitachi, Ltd. 2024. All rights reserved.

現状調査結果のサマリ (2/2)

調査項目		制御システムのリスク分析ガイド	IoT機器を開発する中小企業向け製品セキュリティ対策ガイド
i	主体/取組みの概要	• 貴省・IPAが、セミナーやガイドラインを活用したリスク分析ワークショップにてガイドラインを周知。 • 貴省・IPAが、ガイドラインの補足資料、活用の手引き等の補助資料を作成。 • IPAが、重要インフラ事業者を対象にしてガイドラインを活用した支援を実施。(及びそのフィードバックの反映)	• 貴省・IPAが、関連団体(日本商工会議所、中小企業基盤整備機構、全国中小企業団体中央会、SC3)と連携を行い、普及啓発活動を実施。(HP・メールマガジン等を通じた案内、セミナー等における案内、各都道府県を通じた地域の中小企業への周知) • 貴省・IPAが、ガイドラインの概要版、経営者向け概要版を作成。
ii	取組みの優れた点とその要因	• セミナーにおいて、3種類(入門編/応用編/管理者向け)の動画を提供することによって、知識や立場が異なる各受講者に対応可能。 • IPAが無料でリスクアセスメントの支援を行うことによって、一定の質を担保しつつ直接ガイドラインを普及させることが可能。	• 各業界団体のHPでのガイドラインを紹介することで、貴省HPのみでの紹介に比べて、幅広い企業が認知する可能性が高まる。 • 鳥取県サイバーセキュリティ対策ネットワークや高松商工会議所等のより地域企業に近い団体におけるHPでの紹介が可能となり、より自分ごととして中小企業が捉えやすくなる。
iii	取組みの成果(例:ガイドラインの普及割合)	• 大企業を含む貴省が所管している業界団体(製造業)の会員企業を対象とした調査(調査においてはリスク分析の参考資料として本ガイドラインを提示)において、そもそもリスク分析を実施していない企業は47.4%にのぼるため、 少なくとも約半数の企業が本ガイドラインを利用していない。	- (公開(2023/6/6)から調査時点で5ヶ月程度経過。普及期間が少ないため)

© Hitachi, Ltd. 2024. All rights reserved.

中小企業の情報セキュリティガイドライン関連の普及・啓発(1/2)

HITACHI
Inspire the Next

- 中小企業の情報セキュリティガイドラインを対象とした普及啓発の取組みは一定の効果はあげているものの、まだまだその認知率及び利用率は高いとは言えない。

主体/取組みの概要

実施主体	取組み(例)
対象	• 中小企業の情報セキュリティガイドライン
実施主体	• 貴省(各地の経済産業局を含む)・IPA
取組み内容(例)	• ガイドラインを活用したセミナー・演習の開催(次頁参照) • 補助コンテンツの作成(例:ガイドラインの概要資料/ガイドラインに係る映像コンテンツの作成) • 認証制度(SECURITY ACTION)の要件に対するガイドラインの組み込み

取組みの優れた点とその要因

- **セミナー・演習の開催**
  - ✓ 地域の経済産業局と協力して普及啓発を行うことで、中小企業がより自分ごととして捉えることが可能。
  - ✓ 1名あたり参加費は1000円となっており、リソースが乏しい中小企業にとって参加しやすい。
- **補助コンテンツの作成(概要資料/映像コンテンツ)**
  - ✓ 要点を簡単に理解できるため、多忙な経営者(もしくはIT担当者)が効率良くガイドラインの概要を把握可能。
- **認証制度への組込み**
  - ✓ 認証制度に組み込むことで、中小企業に対してかかる文書に記載された情報セキュリティ対策の実施を促すことが可能。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ 動画コンテンツは約2.6万回再生(2023年10月時点、2021年3月から約2年半の期間)されており、中小企業の1%に満たないため、閲覧した企業は限られている。そもそも、興味を持っていない企業に対して、動画自体が届かない可能性もある。
  - ✓ SECURITY ACTIONを取得した企業は2023年10月の時点(2017年4月の制度開始から6年半)で約30万件に上る。一方で、中小企業のうちの8.3%であり、取得している企業は全体からみれば必ずしも多いとは言えない。
- **ガイドラインの普及に係る成果**
  - ✓ ガイドラインの普及に係る取組みを実施しているものの、認知率は14.1%、利用率は6.1%(2021年調査時点)であり広く普及しているとは言えない。

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

中小企業の情報セキュリティガイドライン関連の普及・啓発(2/2)

HITACHI
Inspire the Next

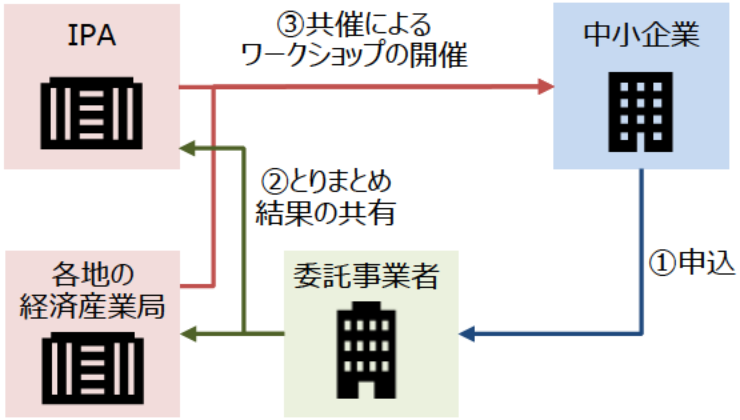
- IPA及び各地域経済産業局は、全国の会場にて中小企業のIT担当者、セキュリティ担当者を対象として、ガイドラインを活用したワークショップを開催。

プログラムの概要

- 中小企業のIT担当者、セキュリティ担当者を対象として、IPA及び各地の経済産業局、委託事業者が「中小企業の情報セキュリティガイドライン」をもとに、ワークショップを開催。

時間	内容
対象者	中小企業のIT担当者、セキュリティ担当者
参加料	1,000円/1名
場所	全国22か所程度
定員	40名程度(※1)

■ステークホルダー



プログラムの詳細(プログラム例)

- 合計3時間のプログラムにおいて、「中小企業の情報セキュリティ対策ガイドライン」にあるリスク分析の一連の流れについて仮想企業を舞台に体験。

時間	内容
14：00～ 15：00(60分)	・リスク分析の全体像と作業手順 【演習1】情報資産の洗い出し どのような情報資産があるか洗い出して重要度を判断する
15：00～ 15：05(5分)	休憩
15：05～ 15：45(40分)	【演習2】リスク値の算定 優先的・重点的に対策が必要な情報資産を把握する
15：45～ 15：50(5分)	休憩
15：50～ 16：50(60分)	【演習3】情報セキュリティ対策の決定 リスクの大きな情報資産に対して必要とされる対策を決める
16：50～ 17：00(10分)	まとめ 質疑応答

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

SECURITY ACTION関連の普及・啓発

HITACHI
Inspire the Next

- 本件取得がIT導入補助金の要件に組み込まれたことによって、SECURITY ACTIONの宣言が進んでいるが、中小企業全体からみるとSECURITY ACTIONの認知率及び利用率は依然として高いとは言えない。

主体/取組みの概要

実施主体	取組み(例)
対象	• SECURITY ACTION
実施主体	• 貴省・IPA
取組み内容(例)	• IT導入補助金の申請への組み込み • HPでの取得企業の紹介/制度の概要資料作成(取得理由、取組み内容　等) • 業界団体(例:JNSA)と連携したセミナーの開催

取組みの優れた点とその要因

- **IT導入補助金の申請への組み込み**
  - ✓ 費用的な負担がある場合に認証取得が進みにくいより小規模な企業においても、取得を促進させることが可能。
- **HPでの取得企業の紹介**
  - ✓ 企業における認証取得理由や具体的なセキュリティ対策を示すことによって、宣言を検討している企業が参考にすることが可能。
- **業界団体(例:JNSA)と連携したセミナーの開催**
  - ✓ 業界団体と協力することでより広範囲の企業に対して周知を実施することが可能。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ SECURITY ACTIONの宣言を行うきっかけのうち、1番多い回答は「補助金を申請する際の要件となっていた」であり、77.0%(2018年度調査時点)にのぼる。SECURITY ACTION 宣言が補助金申請の要件となっている点が取得の大きな理由となっている。
  - ✓ SECURITY ACTIONを取得した企業のうち1名～20名規模の企業は58.7%(2018年度調査時点)と約半数以上を占めている。上記に加えて、第三者認証ではなく自己宣言とすることによって、費用的な負担がある場合には取得が進みにくいより小規模な企業においても宣言が進んでいる。(※)
- **制度(SECURITY ACTION)の普及に係る成果**
  - ✓ 制度の認知率は5.8%、利用率は 1つ星を宣言した企業で2.6%、2つ星を宣言した企業で0.7%(全て2021年調査時点)にとどまっており、普及しているとは言えない。

※ 各地方自治体においても、各種補助金申請の際にSECURITY ACTION 宣言を求めている場合がある点にご留意いただきたい。

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

サイバーセキュリティ経営ガイドライン関連の普及・啓発

HITACHI
Inspire the Next

- 他文書と比較した際、ガイドラインの関連文書の策定や関連ツールの公開、勉強会の開催等により普及啓発の取組みは一定程度の効果を上げている一方で、まだまだ企業側での利用には至っていない可能性。

主体/取組みの概要

実施主体	取組み(例)
対象	• サイバーセキュリティ経営ガイドライン
実施主体	• 貴省・IPA
取組み内容(例)	• ガイドラインに沿った文書の策定(例:プラクティス集、付録F)/関連ツール(サイバーセキュリティ経営可視化ツール)の無償公開 • 企業を支援するセキュリティプレゼンター(※1)の育成を目的とした勉強会の開催 • 一般企業を対象としたガイドラインの適用方法に関するセミナーの開催

取組みの優れた点とその要因

- **ガイドラインに沿った文書の策定/関連ツールの無償公開**
  - ✓ サイバーセキュリティ経営ガイドラインを実践する際に参考となる手順等が示されたプラクティス集(※2)は、企業側で具体的なセキュリティ対策を実装する際に活用可能。
  - ✓ IT担当者は可視化ツールの評価結果を経営会議にて報告でき、費用をかけず経営者層に対して問題提起が可能。
- **セキュリティプレゼンターの育成を目的とした勉強会の開催**
  - ✓ 中小企業支援に役立つ情報セキュリティ対策資料をIPAが提供し勉強会を企画することで、セキュリティプレゼンターによる自発的な普及啓発活動を期待できる。なお、中小企業向け全般の取組みである点に留意いただきたい。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ セキュリティプレゼンターの登録者数は1757名(2023年11月時点)であり、約358万社ある中小企業の数に対して十分な数が登録させているとは言えない。
- **ガイドラインの普及に係る成果**
  - ✓ 企業規模ごとの認知率、利用率は以下の通り。(どちらも2022年調査時点。2-1参照) 一番高い100名～300名未満の企業であっても利用率は2割以下となっており、企業での利用は進んでいない。ただし、「ガイドラインはセキュリティ対策が進んでいる企業では有効ではない」との指摘があり、認知していたとしてもそもそもガイドラインの利用を必要としない企業が存在する点に留意が必要。
    - ➢ 50名未満 :認知率は8.7%、利用率は6.5%
    - ➢ 50名～100名未満 :認知率は16.7%、利用率は10.0%
    - ➢ 100名～300名未満 :認知率は29.9%、利用率は13.0%

※1 SECURITY ACTION等も対象にしており、サイバーセキュリティ経営ガイドラインのみを対象とした制度ではない点に留意いただきたい。
※2 プラクティス集は「サイバーセキュリティ経営ガイドラインVer2.0実践のための経営プラクティス集」を指す。

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

制御システムのリスク分析ガイド関連の普及・啓発

HITACHI
Inspire the Next

- IPA自ら積極的に普及啓発を実施している一方で、普及啓発に係る取組の波及効果は限定的。
- 少なくとも製造業において約半数の企業がリスク分析を実施しておらず本ガイドラインを利用していない。

主体/取組みの概要

実施主体	取組み(例)
対象	• 制御システムのリスク分析ガイド
実施主体	• 貴省・IPA
取組み内容(例)	• セミナーの開催(参加者の演習を含まない。)/ガイドラインを活用したリスク分析ワークショップの開催(参加者の演習を含む。) • 実施例、補足資料、活用の手引き等の補助資料の作成 • 重要インフラ事業者を対象にしたIPAによる支援とそのフィードバックの反映

取組みの優れた点とその要因

- **対象ガイドラインのセミナーの開催/対象ガイドラインを活用したリスク分析ワークショップの開催**
  - ✓ セミナーにおいて、3種類(入門編/応用編/管理者向け)の動画を提供することによって、知識や立場が異なる各受講者に対応可能。
- **実施例、補足資料、活用の手引き等の補助資料の作成**
  - ✓ 実施例は、企業側が自力でリスク分析を行う際に活用可能。
- **重要インフラ事業者を対象にしたIPAによる支援**
  - ✓ IPAが無料で支援することによって、一定の質を担保しつつ直接ガイドラインを普及させること可能。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ 現在まで開催されたセミナーは2018年から計10回であり、定員から算出した参加人数の最大は約2,500名。制御システムを保有すると考えられる製造業において約17万の事業者(2021年時点)がいることを考慮すると、IPAが開催するセミナーの直接効果は限られている。
  - ✓ 重要インフラ事業者を対象としたIPAによる支援では、重要インフラ分野のうち数業界の各1～2事業者を対象としており、リソース等の問題から対応可能な数が限られている。また、重要インフラ分野に指定されたユーザは大企業である可能性が高く、中小企業に対しても支援が行われていない可能性。
- **ガイドラインの普及に係る成果**
  - ✓ 大企業を含む貴省が所管している業界団体(製造業)の会員企業を対象とした調査において、そもそもリスク分析を実施していない企業は47.4%にのぼる。(調査においてはリスク分析の参考資料として本ガイドラインを提示) 約半数の企業が本ガイドラインを利用していない。

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

IoT機器を開発する中小企業向け製品セキュリティ対策ガイド関連の普及・啓発

- 公表されてから期間が短いため普及状況は把握できないものの、中小企業関連団体と連携して普及啓発を実施。

主体/取組みの概要

実施主体	取組み(例)
対象	• IoT機器を開発する中小企業向け製品セキュリティ対策ガイド
実施主体	• 貴省・IPA
取組み内容(例)	• 関連団体(日本商工会議所、中小企業基盤整備機構、全国中小企業団体中央会、SC3)との連携 (HP・メールマガジン等を通じた案内、セミナー等における案内、各都道府県を通じた地域の中小企業への周知) • 概要版、経営者向け概要版の作成

取組みの優れた点とその要因

- **関連団体(日本商工会議所、中小企業基盤整備機構、全国中小企業団体中央会、SC3)との連携**
  - ✓ 各団体のHPでのガイドラインを紹介することで、貴省HPのみでの紹介に比べて、幅広い企業が認知する可能性が高まる。
  - ✓ 鳥取県サイバーセキュリティ対策ネットワークや高松商工会議所等のより地域企業に近い団体におけるHPでの紹介が可能となり、より自分ごととして中小企業が捉えやすくなる。なお、具体的な取組みは明らかになっていないが、SC3内のWGにて今後取組みが明らかになる可能性がある。
- **概要版、経営者向け概要版の作成**
  - ✓ 経営者向け概要版(1枚)において、簡潔に内容を伝えることで、忙しい中小経営層に対しても利用を促進できる可能性。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ 日本商工会議所に所属、もしくは関連する団体のうち、以下の団体において取組みを実施。
    - □ 高松商工会議所(HP上で紹介)
    - □ 豊田商工会議所(HP上で紹介)
    - □ 市川商工会議所(関連団体(市川市塩浜協議会)に対して、ガイドライン策定のメール案内を実施)
    - □ 鳥取県サイバーセキュリティ対策ネットワーク(※1)(HP上で紹介)
- **ガイドラインの普及に係る成果**
  - ✓ - (公開(2023/6/6)から調査時点で5ヶ月程度経過。普及期間が少ないため)

※1 鳥取県商工会議所連合会をはじめとして、鳥取県内の19の団体が参画

[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

現状調査結果のサマリ

- ガイドラインの普及啓発を支援する団体とその取組みについて以下の観点から整理した。
  1. 普及啓発の支援を依頼する対象
  2. 普及啓発の支援を行う団体(例:業界団体)の取組み

項目		調査結果
1	普及啓発の支援を依頼する対象	・貴省が策定した分野別のガイドラインは様々なステークホルダーが想定読者となるため、関連する業界団体も多岐に渡るとともに、他省庁が管轄する業界団体も含まれ得る。[ビルガイドライン、スマートホームガイドライン] ・中小企業への普及啓発を目的として、中小企業と関係の深い業界団体(例:商工会議所)に対して働きかけを行っている事例がみられた。[IoT機器を開発する中小企業向け製品セキュリティ対策ガイド]
2	普及啓発の支援を行う団体(例:業界団体)の取組み	・業界団体を通じた取組みにおいて、同じ業界であっても、貴省が策定したガイドラインの普及啓発に積極的な団体とそうではない団体がみられた。 [ビルガイドライン、スマートホームガイドライン] ・ガイドライン策定の段階で深く関わっている業界団体(例:JEITA、CSSC)においては、積極的な取組(例:ガイドラインを踏まえた個別ガイドラインの策定)がみられた。具体的には貴省が策定したガイドラインに関連するガイドラインを各業界団体が作成している。 [ビルガイドライン、スマートホームガイドライン] ・業界団体が独自にガイドラインを策定する場合があり、その際には普及啓発に係る業界団体独自のチャネルを活用している。[日本建設業連合会のセキュリティガイドライン、CCDSの製品分野別セキュリティガイドライン] ・業界内で強い立場(例:建設業界における元請企業)にある企業が業界独自のガイドラインの普及啓発に取り組んでいる事例がみられた。[日本建設業連合会のセキュリティガイドライン]

© Hitachi, Ltd. 2024. All rights reserved.

ビル業界におけるガイドラインの普及に関連する団体

- ビル業界では、設計・建設段階と運用段階でセキュリティ対策の実施主体となるステークホルダーが異なるため、段階ごとにガイドラインの普及啓発に関連する業界団体も異なる。
- ビル業界の企業(主に中小企業)に対してガイドラインを普及する際には、それぞれの団体に対して働きかけを行うことが考えられる。

	設計・建設時	運用時
セキュリティ対策の実施主体(例)	• ビルオーナー(デベロッパー、自治体を含む) • 設計事務所 • ゼネコン/サブコン • 個別システム事業者	• ビルオーナー(デベロッパー、自治体を含む) • ビル管理会社
ガイドラインの普及に関連する団体と既存の取組み(例)	• **日本建設業連合会** ✓ 建設業(協力会社も対象に含む)における情報セキュリティ関連ガイドラインの発行・普及 ✓ 建設現場で利用する情報セキュリティ啓発ツール等を作成 • **元請企業(ゼネコン)** ✓ 協力会社向けのサイバーセキュリティ対策に関するセミナーの開催 ✓ サプライヤー向けのセキュリティ相談窓口の設置	• **日本ビルヂング協会連合会** ✓ 貴省が策定したビルガイドライン(※)をHP上にて紹介 • **全国ビルメンテナンス協会** ✓ サイバーセキュリティシステムを含むセキュリティに係る展示会の開催 ※「ビルガイドライン」は「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版」を指す。

建設業の協力会社は、企業規模や職種が多岐に亘っているため、管理に苦労している。合わせて、一次協力会社は弊社の目が届くが、その下は二次、三次、四次と重層構造になっている点も管理が難しいところ。



ゼネコンの社員

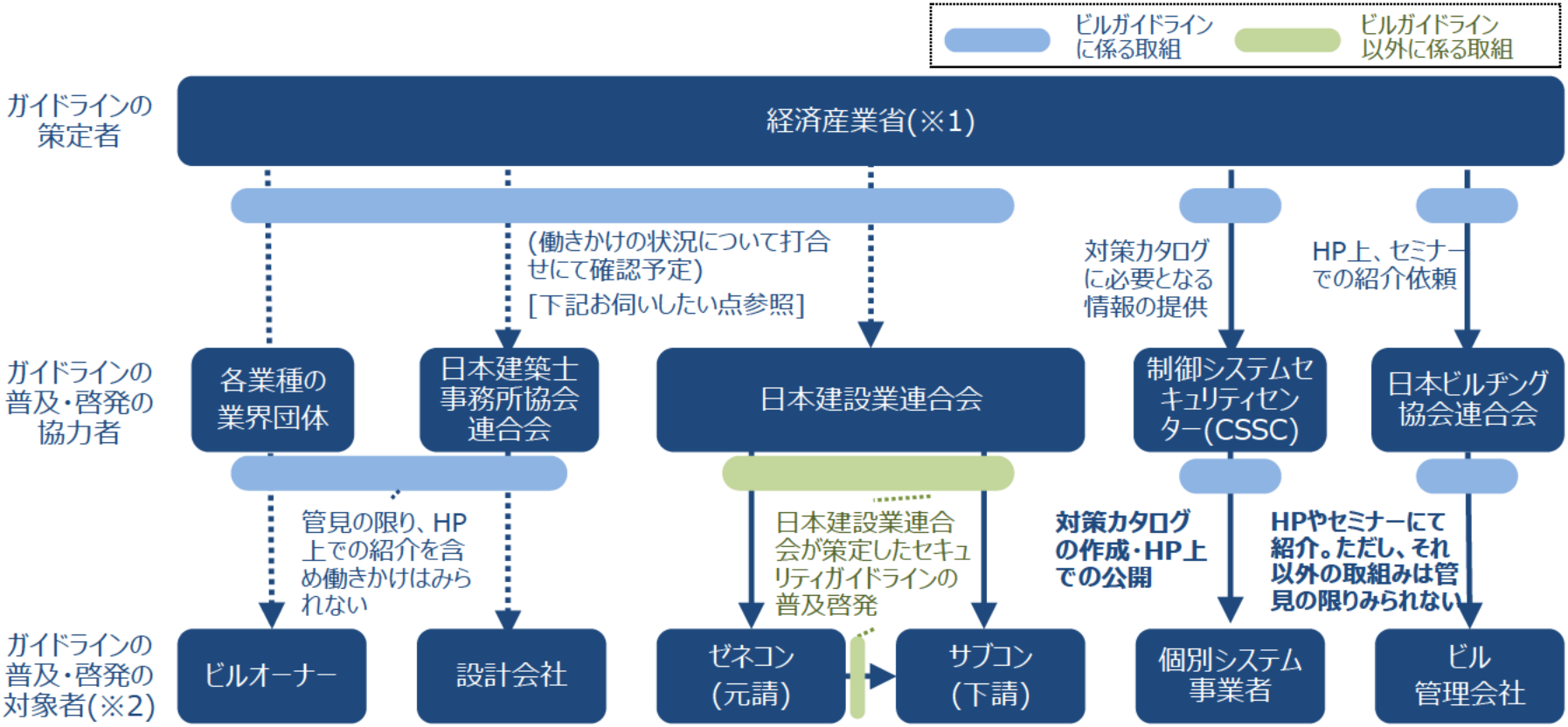
[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

ビル業界におけるガイドラインの普及啓発に係る取組み

HITACHI
Inspire the Next

- 制御システムセキュリティセンター(CSSC)及び日本ビルヂング協会連合会を除いて、ビルガイドラインに係る普及啓発活動に巻き込めている業界団体はない可能性。



※1 経済産業省上のHPでの紹介の記載は省略している。
※2「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第２版」の想定読者のうち、「テナント」や「サービスプロバイダ」、「セキュリティベンダ」の記載は省略。

[参考]貴省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第２版」
(https://www.meti.go.jp/policy/netsecurity/wg1/bill_gideline_2.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

スマートホーム業界においてガイドラインの普及に関連する団体

- スマートホーム業界では、設計・建築段階と運用段階でセキュリティ対策の実施主体となるステークホルダーが異なる。
- 業界団体(例:JEITA、CCDS)は、設計時・建築段階と運用段階におけるセキュリティ対策の実施主体を対象としたガイドラインを策定した上で、各実施主体に対してガイドラインの普及啓発活動を実施。

	設計・建築時	運用時
セキュリティ対策の実施主体(例)	• 住まい手 • スマートホームを供給する事業者 • IoT機器の事業者	• 住まい手 • スマートホーム向けのサービス事業者(例:クラウド事業者) • メンテナンスやサポートを行う事業者/IoT機器を遠隔から管理する事業者
ガイドラインの普及に関連する団体と既存の取組み(例)	• **電子情報技術産業協会(JEITA)** ✓ JEITA内のスマートホーム部会が、貴省と連携し「スマートホームの安心・安全に向けた サイバー・フィジカル・セキュリティ対策ガイドライン」を策定 ✓ 「スマートホームIoT データプライバシーガイドライン」を策定 ✓ スマートホームに関連する事業者向け及び住まい手向けにパンフレットを作成。HP上にて公開 • **重要生活機器連携セキュリティ協議会(CCDS)** ✓ 「CCDS製品分野別セキュリティガイドライン スマートホーム編」を策定 ✓ CCDSにおけるサーティフィケーションプログラムの実施 • **住宅生産団体連合会** ✓ 住宅生産団体連合会内の「IoT等先進技術活用WG」がJEITAやCCDS、家電製品協会と連携	

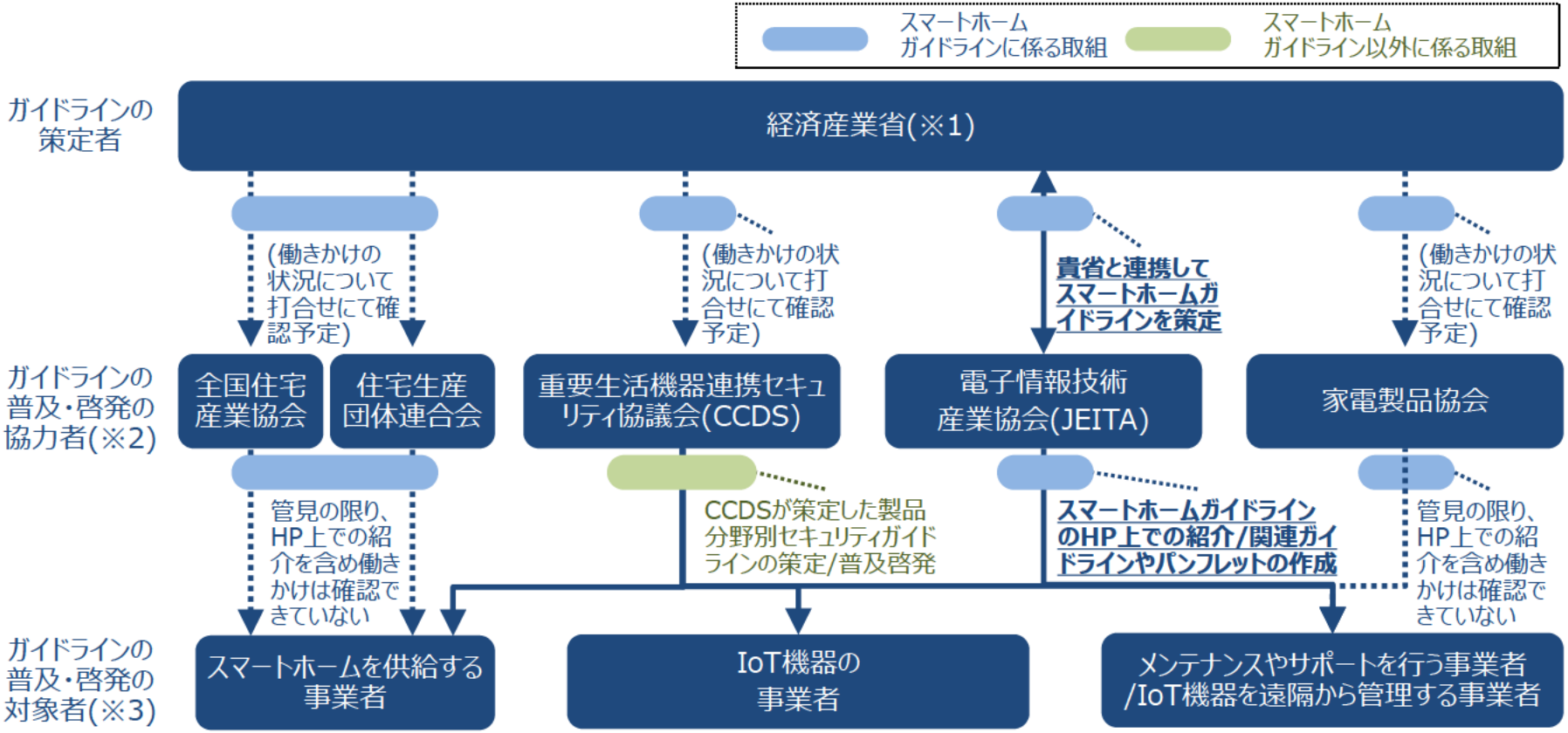
[参考]各種公開資料を参考に筆者作成

© Hitachi, Ltd. 2024. All rights reserved.

スマートホーム業界においてガイドラインの普及啓発に係る取組み

HITACHI
Inspire the Next

- パンフレットの作成や関連ガイドライン策定を行うなど、貴省と連携して「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定したJEITAが積極的な取組みを実施。



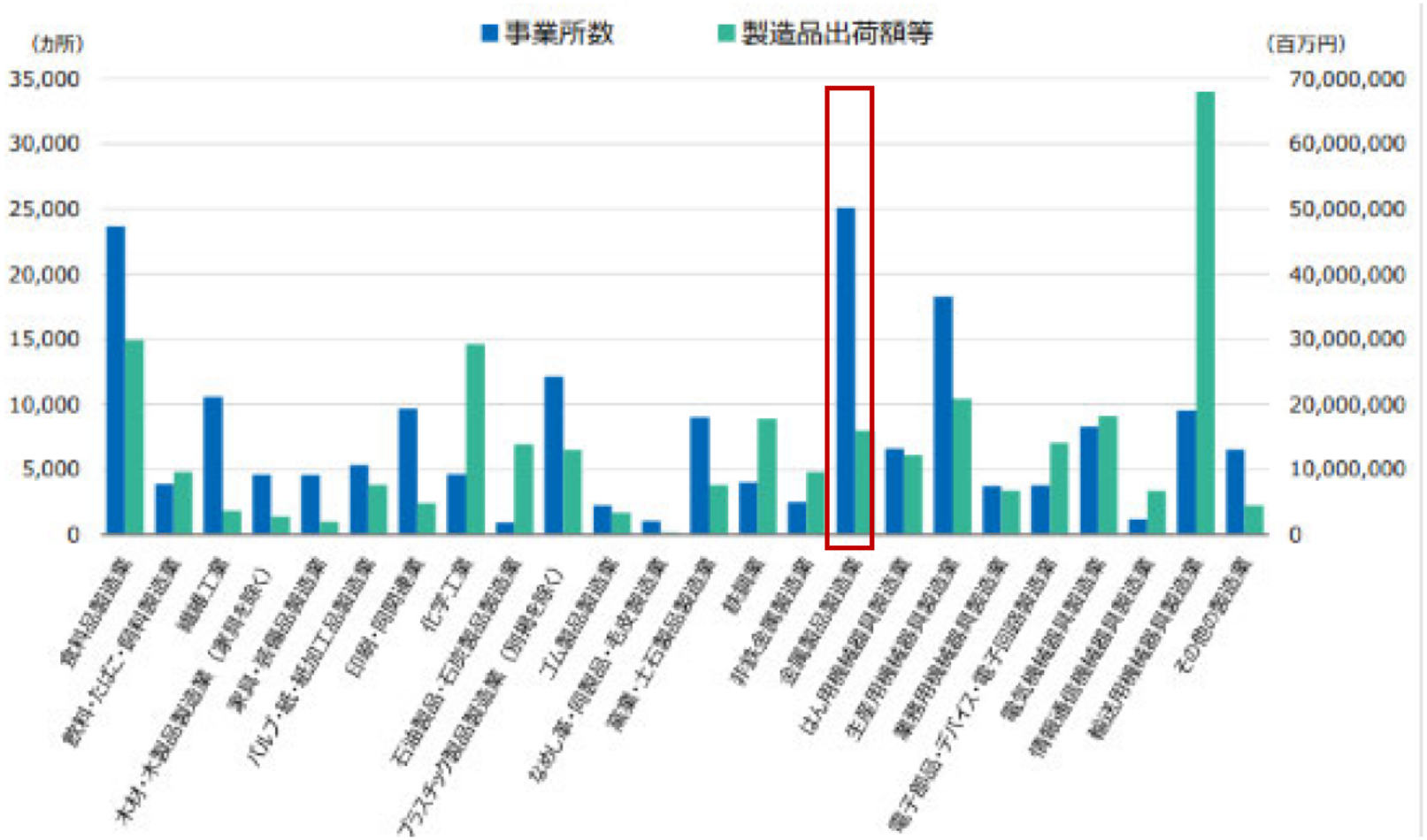
※1 経済産業省上のHPでの紹介の記載は省略している。
※2 戸建てを主な対象とした上で住宅関連の業界団体のうち、「全国宅地建物取引業協会連合会」や「全日本不動産協会」、「不動産流通経営協会」は対象外とした。また、IoT機器に関連する業界団体として、産業サイバーセキュリティ研究会 WG1に関連する業界団体を対象とした。
※3 「スマートホームの安心・安全に向けた サイバー・フィジカル・セキュリティ対策ガイドライン」の想定読者のうち、「スマートホーム向けのサービス事業者(例:クラウド事業者)」や「住まい手」、「スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社」、「スマートホーム化された賃貸住宅の所有者や管理受託会社」の記載は省略。

[参考]貴省「スマートホームの安心・安全に向けた サイバー・フィジカル・セキュリティ対策ガイドライン」
(https://www.meti.go.jp/press/2021/04/20210401005/20210401005-1.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

工場業界においてガイドラインの普及啓発に係る取組み

- 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の対象となる製造業のうち、事業所数が最も多い金属製品製造業を対象として調査を実施。



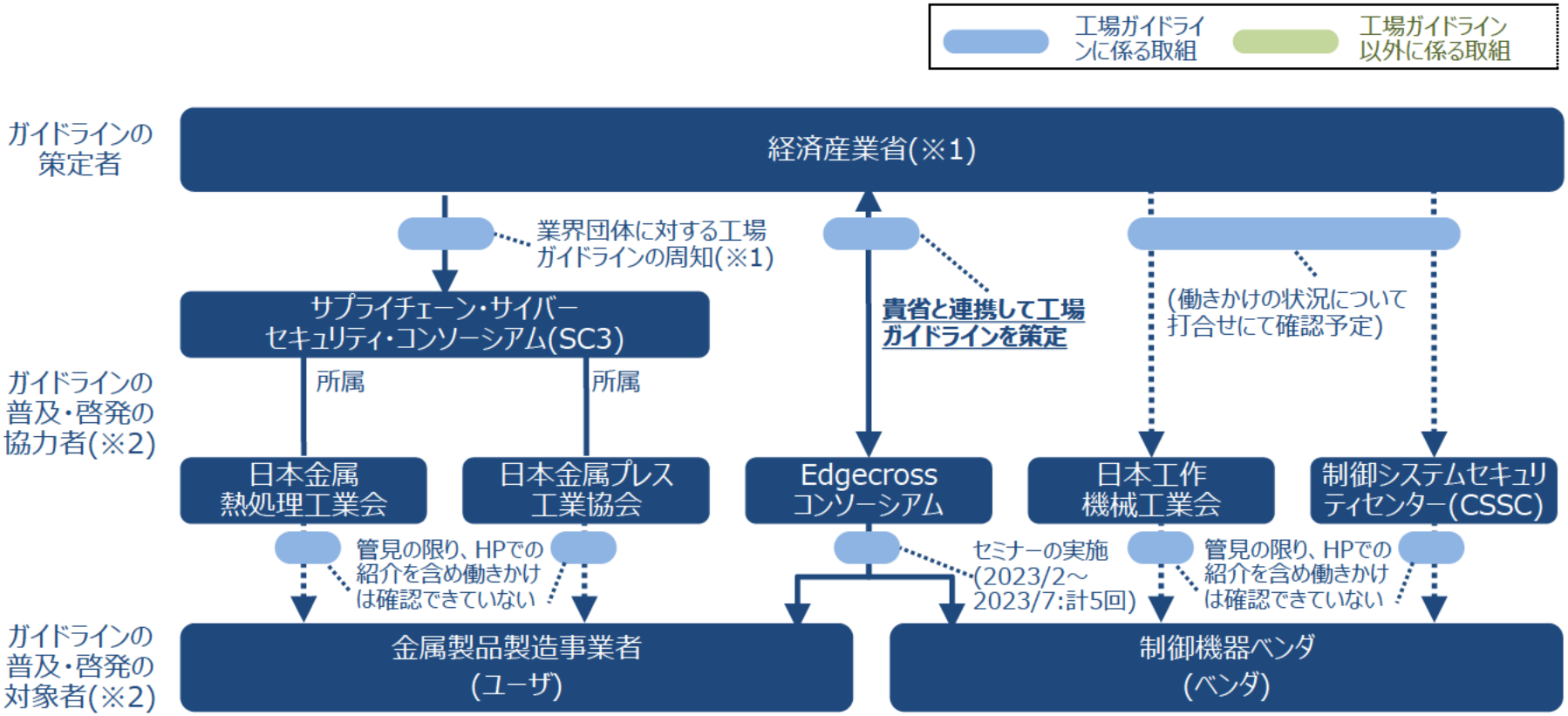
[参考]貴省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」
(https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

工場業界においてガイドラインの普及啓発に係る取組み

HITACHI
Inspire the Next

- Edgecrossコンソーシアムのように積極的に普及啓発の取組みを行っている団体がみられた一方で、工場SWGの委員が所属する団体であっても必ずしも普及啓発に積極的ではない団体がみられた。



※1 第6回 産業サイバーセキュリティ研究会 WG1 工場SWG 資料6「工場システムのセキュリティ普及啓発に関する取組」より
※2 工場SWGの委員の所属している団体として、「日本工作機械工業会」及び「制御システムセキュリティセンター(CSSC)」を今回の調査対象とした。

[参考]貴省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」
(https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

地域単位での取組み/現状調査結果のサマリ

HITACHI
Inspire the Next

調査項目		ITCちば経営応援隊	関西サイバーセキュリティネットワーク	Pit-Nagoya(名古屋商工会議所の取組みを含む)
i	主体/取組みの概要	<ガイドラインの普及に係る取組> • 地域コミュニティ連絡会を設置した3地域と連携してセミナーを開催。 <上記以外の取組み> • 貴省関東経済産業局の委託事業において社内の現状分析、情報セキュリティ規程案の策定等の直接的な支援を実施。 • また、他団体(例:全国中小企業団体中央会)の各種研修において、講師を務め事例等を紹介。	<ガイドラインの普及に係る取組> • 中小企業の情報セキュリティ対策ガイドラインに基づいたリスク分析ワークショップを開催。 <上記以外の取組み> • 地域コミュニティ形成のため相談窓口の設置やサイバーセキュリティ専門家の派遣を実施。 • また、地域コミュニティに向けてサイバー攻撃の現状やセキュリティ対策をセミナーにて紹介。	<ガイドラインの普及に係る取組> • 中小企業の情報セキュリティ対策ガイドラインを活用した対策をセミナーにて紹介。 • 自工会/部工会が策定したガイドラインをセミナーにて紹介。 <上記以外の取組み> • IT化にむけた相談窓口の設立や中小企業とIT企業のマッチング支援を実施。 • お助け隊サービスで得た知見を踏まえて、セキュリティサービスを提供。
ii	取組みの優れた点とその要因	<ガイドラインの普及に係る取組> • 他地域の連絡会参加者にセミナー開催を告知してもらうことで、多くの企業にガイドライン等を周知することが可能。 • ITコーディネータ協会と連携することによって、より小規模の企業(10名～50名以下)に対して支援や情報の提供を行うことができている。	<ガイドラインの普及に係る取組> • サイバーインシデント演習やリスク分析ワークショップを開催することによって、地場の企業が自分ごととして捉えやすくなる。	<ガイドラインの普及に係る取組> • ガイドラインに則った対策内容についてセミナーを行うことによって、中小企業はガイドラインの認知に加え具体的なセキュリティ対策を進めやすくなる。 • 自工会の担当者と連携することで自工会のみの周知と比較して幅広い企業に対してガイドラインを普及させることが可能。
iii	取組みの成果	<ガイドラインの普及に係る取組> • 令和3年度のセミナーの申込者数は2回合計で300件以下となっている。中小企業の数は茨城県で約8万、千葉県で約12万、長野県で約7万であることから、効果は限定的となっている。	<ガイドラインの普及に係る取組> • 関西圏の地域セキュリティコミュニティの存在を認知している団体は6.3%であり、そもそも、地域セキュリティコミュニティの存在が知られていない。なお、ワークショップの定員は40名。	<ガイドラインの普及に係る取組> • (セミナーでの集客状況については今後、ヒアリングにて確認予定。)

© Hitachi, Ltd. 2024. All rights reserved.

ITCちば経営応援隊 / ガイドラインの普及啓発に係る取組み

HITACHI
Inspire the Next

- 貴省関東経済産業局の委託事業において、 IPAと連携して中小企業の情報セキュリティガイドラインやSECURITY ACTIONを紹介。各地域の連絡会と協力してセミナー開催の告知を行うことで一定の効果はみられたが、全体からみると効果は限定的となっている。

主体/取組みの概要

実施主体	取組み(例)
対象	• 中小企業の情報システムセキュリティガイドライン • SECURITY ACTION
実施主体	• ITCちば経営応援隊(特定非営利活動法人で地域SECUNITYの1つ。関連団体は商工会議所、ITコーディネータ協会、千葉県産業振興センター)
取組み内容(例)	• SECURITY ACTIONや中小企業の情報セキュリティガイドライン等の普及啓発セミナーの実施(※1)

取組みの優れた点とその要因

- **SECURITY ACTIONや中小企業の情報セキュリティガイドライン等の普及啓発セミナーの実施**
  - ✓ 地域コミュニティ連絡会を設置した3地域(茨城県、千葉県、長野県)を対象としてセミナーを実施することとともに、連絡会参加者にセミナー開催の告知に協力してもらうことによって、多くの企業にガイドライン等を周知することが可能。

※1 令和3年度貴省関東経済産業局の委託事業内で実施。セミナーでは、サイバーセキュリティお助け隊の事例紹介や民間企業におけるセキュリティの動向紹介を同時に実施。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ 委託事業内で地域コミュニティ連絡会を設置した3地域(茨城県、千葉県、長野県)を対象に普及啓発セミナーは2回実施。受講申込者数は前年度比で2倍になっているものの、2回合計での申込者数は300件以下となっている。中小企業の数は茨城県で約8万、千葉県で約12万、長野県で約7万であることから、必ずしも多数の事業者にリーチができているとは言えない。
    - 第1回[オンライン配信]:受講申込者数140名・同時接続最大件数97件
    - 第2回[オンライン配信]:受講申込者数146名・同時接続最大件数115件
  - ✓ 委託事業が終了した令和4年度にもサイバーセキュリティセキュリティセミナーを継続的に実施(2回開催)し、自走化に向けて取り組む。

[参考] 貴省経済産業局「令和３年度中小企業サイバーセキュリティ対策促進事業(サイバーセキュリティ及び情報セキュリティに関する地域コミュニティ形成事業)」(https://www.meti.go.jp/policy/netsecurity/secunity_practice_2.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

ITCちば経営応援隊 / ガイドラインの普及啓発以外の取組み

HITACHI
Inspire the Next

- 委託事業のもとセキュリティ対策に係る直接的な支援を行うとともに、他団体における各種研修ではITCちば経営応援隊の職員が講師を務め、ガイドラインを参考に事例を紹介。

中小企業へのコンサルティング

- ITコーディネータ協会からの委託において、支援を希望する団体に対して伴走型コンサルティングを実施。

項目	支援内容(例)
藤恵工業への支援 (従業員11名)	• 1)ウィルス対策ソフトやパスワード設定などの基本的対策の徹底、2)情報セキュリティ対策の社内ルールの整備、3)従業員の情報セキュリティ対策意識の向上などの課題に対して、社内の現状分析、重点対策課題の整備、情報セキュリティ基本方針の確認、情報セキュリティ規程案の策定、改善実施計画の策定を支援。
マルウへの支援 (従業員40名)	• 「5分でできる自社診断」や「リスク分析シート」の作成を通じ社内のセキュリティ対策の現状を把握、関連規定類のチェックとセキュリティ対策実施計画書を策定し、本年度の対応計画を作成。

他団体における研修での登壇

- 他団体の各種研修において、ITCちば経営応援隊の職員が講師を務め事例等を紹介。

項目	内容
研修での事例の紹介	全国中小企業団体中央会及びその会員向けの情報セキュリティ、情報管理やDXに関する研修において、講師を務める。 IPAの「情報セキュリティ10大脅威2022」や「中小企業の情報セキュリティ対策ガイドライン」、貴省の「秘密情報の保護ハンドブック」を参考に、受講者の興味・ニーズに合うように選択、具体的な事例を紹介。

[参考] ITCちば経営応援隊「活動の記録 第12報2022年４月～2023年３月」
(https://npo-chiba-keiei-oentai.org/wp/wp-content/uploads/2023/09/2f0905c0266b7b4458d8624668d215e8.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

関西サイバーセキュリティネットワーク/ ガイドラインの普及啓発に係る取組み

HITACHI Inspire the Next

- 官民の様々なステークホルダーを巻き込み取組みを行うことでより地場の企業が自分ごととして捉えやすくなっている一方で、現時点で関西圏の地域セキュリティコミュニティの認知度は低く、ガイドラインの周知活動に伴う効果は限定的となっている。

主体/取組みの概要

実施主体	取組み(例)
対象	• 情報システムセキュリティガイドライン及び中小企業のためのセキュリティインシデント手引き
実施主体	• 関西サイバーセキュリティネットワーク
取組み内容(例)	• 「中小企業の情報セキュリティ対策ガイドライン」に基づいたリスク分析ワークショップの開催(参加費1,000円/名)(※1)

取組みの優れた点とその要因

- **サイバーインシデント演習の実施/リスク分析ワークショップの開催**
  - ✓ 近畿経済産業局、近畿総合通信局、一般財団法人関西情報センターが参画する関西サイバーセキュリティネットワークがサイバーインシデント演習やリスク分析ワークショップを開催することによって、地場の企業が自分ごととして捉えやすくなる。

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ 近畿圏(近畿2府5県)の中小企業を対象とした関西サイバーセキュリティネットワークによるアンケート調査(令和2年度時点)によると、関西圏の地域セキュリティコミュニティの存在を認知している団体は6.3%であり、そもそも、地域セキュリティコミュニティの存在が知られていない。
  - ✓ リスク分析ワークショップの定員は40名であった。また、「サイバーセキュリティ地域別セミナー」は複数回開催されているもののガイドラインの紹介はみられなかった。大阪府における中小企業は27万社あることを考慮すると効果は限定的である可能性が高い。

※1 2022年度に「サイバーセキュリティ地域別セミナー」を計7回を実施しているものの、アジェンダを見る限りのガイドラインの紹介は確認できなかった。

[参考]関西サイバーセキュリティ・ネットワーク事務局「関西サイバーセキュリティ・ネットワークの取組」
(https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/outline_k-sec-net.pdf)
貴省近畿経済産業局「「令和2年度中小企業サイバーセキュリティ対策促進事業（関西サイバーセキュリティ促進強化事業）」関西におけるサイバーセキュリティ対策の実態把握(アンケート調査結果)」
(https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/210317press_report2.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

関西サイバーセキュリティネットワーク/ ガイドラインの普及啓発以外の取組み(1/2)

HITACHI Inspire the Next

- 関西サイバーセキュリティネットワークでは、中小企業のセキュリティ対策推進を目的として積極的に取組みを実施。一方で、ガイドラインの普及啓発を目的とした取組みは少ない可能性。

令和4年度の主な取組み

分類	主な取組み ※赤字下線はガイドラインの普及啓発に係る取組(想定)
サイバーセキュリティ人材の発掘・育成	• サイバーセキュリティ・リレー講座（初級者向け） • サイバーセキュリティスクール(ゲーム編)（若手人材向け） • サイバーセキュリティスクール(CTF編)（若手人材向け）
地域におけるコミュニティ形成の支援／情報発信	• サイバーセキュリティ地域別セミナー(2府5県、計7回) • サイバーセキュリティカフェ(地域における情報発信) • サイバーセキュリティ専門家派遣事業(出前講座) • サイバーインシデント演習 in大阪 • 令和4年度情報セキュリティセミナー

令和4年度以前の主な取組み

分類	主な取組み ※赤字下線はガイドラインの普及啓発に係る取組(想定)
サイバーセキュリティ人材の発掘・育成	• 情報セキュリティ・マネジメントセミナー(年2回) • サイバーセキュリティフォーラムin 福井(中小企業向け)
地域におけるコミュニティ形成の支援／情報発信	• サイバーセキュリティ相談窓口の見える化 • 地域セキュリティコミュニティ形成支援 • 情報発信事業 ✓「新型コロナ対策としてのセキュリティ」 ✓「テレワークを行う上での中小企業との経営者の心構え5箇条」 ✓「地域のキーパーソンに聞く ～経営課題としてのセキュリティ～」
中小企業等の実態把握	• サイバーセキュリティ実態調査（アンケート調査） • サイバーセキュリティ実態調査（ヒアリング調査）

[参考]関西サイバーセキュリティ・ネットワーク事務局「関西サイバーセキュリティ・ネットワークの取組」
(https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/outline_k-sec-net.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

関西サイバーセキュリティネットワーク/ ガイドラインの普及啓発以外の取組み(2/2)

HITACHI Inspire the Next

- 地域コミュニティの形成に向けて積極的に取組みを行うとともに、地域コミュニティに対してはセミナーやHPを通じてサイバーセキュリティの取組みや相談を行うための連絡先等の情報を発信。

地域におけるコミュニティ形成の支援

- 地域コミュニティ形成のため、サイバーセキュリティ専門家を派遣するとともに相談が行えるよう座談会等を企画。

項目	支援内容(例)
サイバーセキュリティ専門家派遣事業	• 地域企業支援や産業振興、IT化をサポートしている地方自治体や業界団体において、地域やグループ内の中小企業に対するセキュリティ意識啓発に苦慮している団体を対象にサイバーセキュリティ分野の専門家を派遣。 • セキュリティ専門人材バンクに登録された有識者、ベンダ、コンサル、NPO等のセキュリティ専門家が講演を行う。
サイバーセキュリティカフェ	• 地方都市における中小企業等のサイバーセキュリティ担当者を対象に、サイバー攻撃の現状やセキュリティ対策などのミニ講演とあわせ、質問や相談を気軽にできる座談会を会場とオンラインのハイブリッドで開催。

地域におけるコミュニティへの情報発信

- セミナーやHPを通じてサイバーセキュリティの取組みや相談を行うための連絡先等の情報を発信。

項目	支援内容(例)
サイバーセキュリティ地域別セミナー	• 近畿2府5県で各1回ずつ、サイバーセキュリティ月間(2月1日～3月18日)に合わせて、サイバーセキュリティの取組機運向上及び域内関係者間のつながりを深めることを目的とした地域別セミナーを計7回開催。 <プログラム> ①有識者による基調講演、②セキュリティソリューション提供事業者、③地元のセキュリティの取り組み紹介、④情報処理安全確保支援士によるセキュリティコンサル事例紹介、⑤府県警察による被害事例紹介、⑥サイバー保険の紹介等
サイバーセキュリティ相談窓口	• サイバーセキュリティに関する相談先がわからないという中小企業が相談しやすい環境を整える目的で、相談窓口をリスト化し、ホームページで情報発信を行う。 • 産業支援機関や警察などの公的機関を中心としたリストを掲載した上で、拡充予定。

[参考]関西サイバーセキュリティ・ネットワーク事務局「関西サイバーセキュリティ・ネットワークの取組」
(https://www.kansai.meti.go.jp/2-7it/k-cybersecurity-network/outline_k-sec-net.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

Pit-Nagoya / ガイドラインの普及啓発に係る取組み

HITACHI
Inspire the Next

- Pit-Nagoya(名古屋商工会議所)では、活発にガイドラインの普及啓発活動を実施。また、セミナーでは貴省(IPA)が策定したガイドラインの他にも「自動車産業サイバーセキュリティガイドライン」を紹介。

主体/取組みの概要

実施主体	取組み(例)
対象	• 中小企業の情報セキュリティ対策ガイドライン、サイバーセキュリティ経営ガイドライン　等[名古屋商工会議所] • 自動車産業サイバーセキュリティガイドライン[名古屋商工会議所]
実施主体	• Pit-Nagoya(名古屋商工会議所)
取組み内容(例)	• 中小企業の情報セキュリティ対策ガイドラインを活用した対策の紹介[名古屋商工会議所]](※1) • 東京商工会議所と連携した経営ガイドラインや対策の紹介[名古屋商工会議所] (※2) • セミナーでの自工会/部工会が策定したガイドラインの紹介[名古屋商工会議所]

取組みの優れた点とその要因

- **情報セキュリティ対策ガイドラインを活用した対策の紹介**
  - ✓ 中小企業の情報セキュリティ対策ガイドラインに則った対策内容についてセミナーを行うことによって、中小企業はガイドラインを認知するとともに、具体的なセキュリティ対策を進めやすい。
- **東京商工会議所と連携した経営ガイドラインやセキュリティ対策の紹介**
  - ✓ 商工会議所のネットワークを活用することによって、セミナーを広く普及させることが可能。その結果、ガイドラインを必要としている企業に案内が届く可能性が高くなる。
- **セミナーでの自工会/部工会が策定したガイドラインの紹介**
  - ✓ 自工会の担当者と連携し、商工会議所がセミナーを実施することによって、自工会のみの周知と比較してより幅広い企業に対してガイドラインを普及させることが可能。

※1 2024/1/26実施予定
※2 2023/11/29実施予定

取組みの成果

- **普及啓発に係る取組みの成果**
  - ✓ ガイドラインの普及啓発にあたって、様々なガイドラインを対象としたセミナー活動を実施中。
  - ✓ また、開催予定の取組みも多く、現在進行形でガイドラインの普及啓発活動を実施。

[参考] 名古屋商工会議所「モノづくり企業が押さえるべき情報セキュリティ対策セミナー」
(https://www.nagoya-cci.or.jp/event/files/annnaijyo_HP.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

Pit-Nagoya / ガイドラインの普及啓発以外の取組み

HITACHI
Inspire the Next

- 共同事務局を担うNTT西日本及び日立システムズとともに、 Pit-Nagoyaは中小企業におけるIT化を支援する過程で各種サービスを提供するとともに、サイバーセキュリティお助け隊事業の経験を活かし、中小企業に対してセキュリティサービスを提供。

IT化を支援するサービス

- コンソーシアム会員に対して、セキュリティに限定せずIT導入に係る各種サービスを提供。

サービス	内容
中小企業・IT企業の相談窓口	• 中小企業のIT導入などについて、相談窓口を設置。
ITサービス一覧化・マッチング促進	• コンソーシアム会員のIT企業一覧から中小企業の課題にマッチした企業、サービスを探せるよう検索サービスを提供。
事業共有・セミナー情報の 一覧化	• コンソーシアム会員のIT企業が発信する最新の情報を一覧化し提供。

セキュリティに関するサービス

- サイバーセキュリティお助け隊事業の経験を活かし、中小企業に対して有償サービスを提供。

項目	内容
サービス内容	**(1) セキュリティ機器設置** • UTMの設置、通信の監視 **(2) 運用管理サポート** • サポートセンターによる常時監視。その他、問合せ対応、遠隔でのウイルス駆除、レポート配信(月に1回) • UTMの故障やインシデント時の駆け付けサポート **(3) サイバーリスク保険** • 情報漏洩時の損害賠償・費用負担への保険提供
費用	標準パック(上記(1)～(3)を含む) • (1-10台) 11,000円/台・月 • (50台以上) 14,300円/台・月 • (100台以上) 22,000円/台・月

[参考] 名古屋商工会議所「Pit-Nagoya セキュリティのサービス開始について」
(https://www.nagoya-cci.or.jp/pr/newsrelease20210803/21p.pdf)

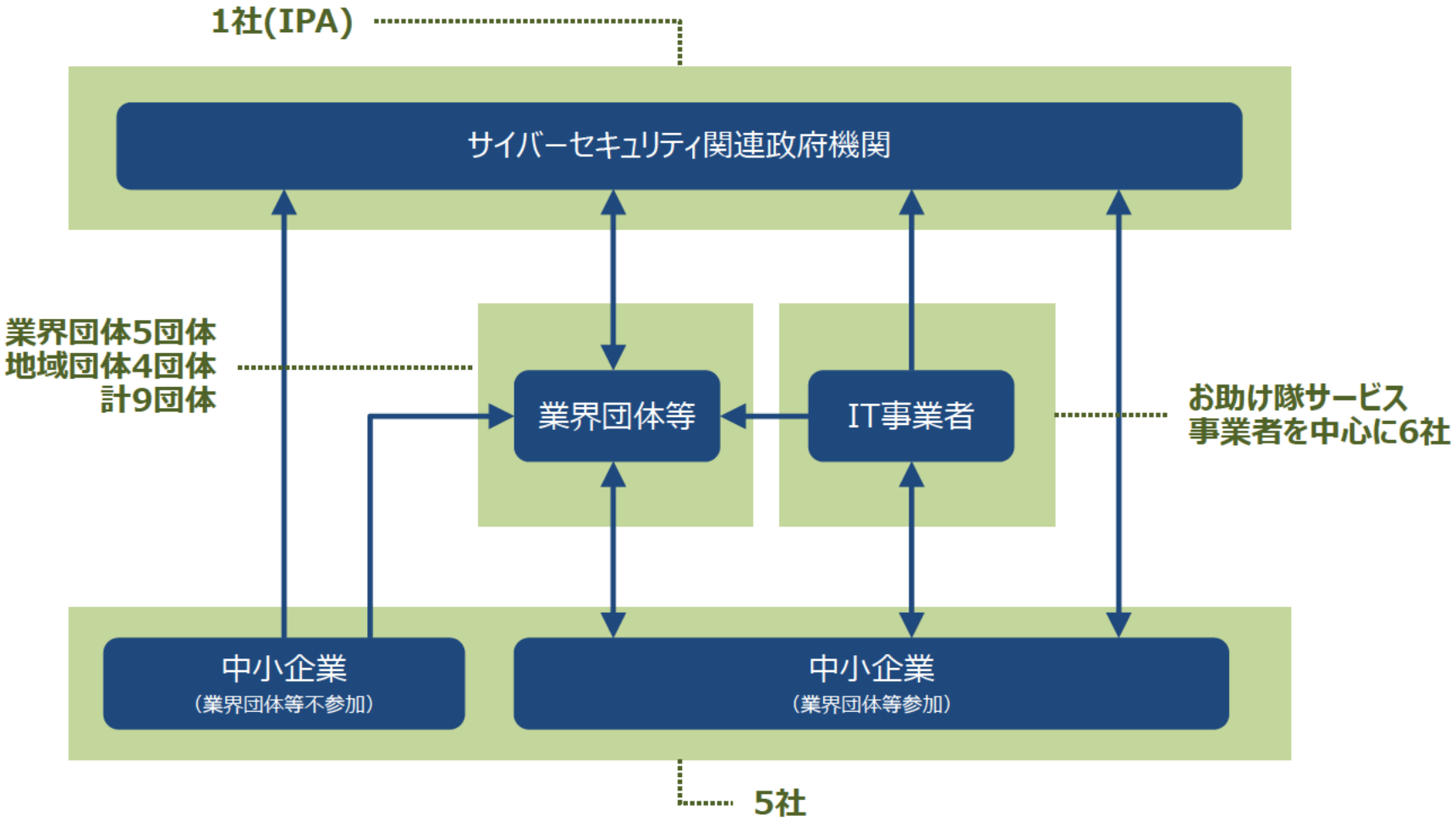
© Hitachi, Ltd. 2024. All rights reserved.

2-3. 中小企業及び支援機関等を対象とした ヒアリング調査

© Hitachi, Ltd. 2024. All rights reserved.

ヒアリング調査の実施状況

- これまで、サイバーセキュリティ関連政府機関(IPA)及び業界団体等(業界団体、地域コミュニティ)、中小企業にサイバーセキュリティ製品・サービスを提供するIT事業者及び中小企業(計21団体)に対してヒアリングを実施した。



© Hitachi, Ltd. 2024. All rights reserved.

調査結果整理の観点

HITACHI
Inspire the Next

- 前記ヒアリング調査での聴取内容に基づき、主体別の取組みという観点から、以下の5分類に分けて現状や課題の整理を行った。

大分類		中分類	
A	**政府における取組み**	A.1	ガイドラインの策定・整理
		A.2	ガイドラインの普及
		A.3	ガイドライン関連活動のガバナンス
B	**政府と支援機関間における取組み**	B.1	政府から支援機関への働きかけ
C	**支援機関における取組み**	C.1	継続的なリソースの確保
		C.2	支援対象の拡大
D	**支援機関と中小企業間における取組み**	D.1	支援機関から中小企業への働きかけ
E	**中小企業における取組み**	E.1	必要性の認識
		E.2	リソースの確保

© Hitachi, Ltd. 2024. All rights reserved.

A.1 ガイドラインの策定・整理に関する主なご意見

HITACHI
Inspire the Next

A. 政府における取組み

A.1 ガイドラインの策定・整理

○ヒアリングにおける指摘に見る現状

中小企業のサイバーセキュリティ対策推進における各種ガイドライン等の位置づけ

- 今回ヒアリングを行った団体の多くが、CPSFに基づく分野別ガイドライン等が中小企業にとって高度に感じられる場合があると回答。
- 中小企業の現状を踏まえれば、「中小企業の情報セキュリティ対策ガイドライン」や「サイバーセキュリティ経営ガイドライン」の普及促進に努めるべきであり、分野別ガイドライン等はその先にあるものと位置づけられる。[政府機関、業界団体等]

各種ガイドライン等の活用促進に向けた取組みの推進

◆対策等に関する具体的な記載の拡充

- 活用促進に向けては、対策基準(チェックシート等)やガイドラインを踏まえた具体的なセキュリティ対策の整理が有効ではないか。
- 中小企業ガイドラインは公表当初(2016年、2017年頃)よりバージョンアップされており具体的になってはきているが、ガイドラインの記載内容は依然として抽象的であり、企業側の具体的なアクションにつながりにくい。[IT事業者]

◆理解しやすいコンテンツの作成と周知

- (ビル)オーナーが内容が理解することによって、PM会社へ指示がなされるため、オーナにとって理解が容易なもの(例:漫画)があるとよい。

◆ガイドライン群の整理

- ガイドも色々あり、どれを使っていいのか分からないという声があるので、整理し分かりやすくしてほしい。[IT事業者]
- 中小企業からはこれらのガイドラインの差分について聞かれることがあるが、明確に回答できていない。[IT事業者]
- 業界ごとのガイドラインの普及も適当とは思うが、業界共通の事項と業界固有の事項の整理を適切に行うべき。[業界団体等]
- 示された対策のうち、どこまでを実装すべきか悩む場合がある。また、ガイドラインに示された対策の位置付け(推奨/義務)について質問を受けることがある。明確に示していただけるとありがたい。[IT事業者]

国際標準の活用による相互運用性の確保

- 工場セキュリティの取組みにおいては、IEC 62334等の国際標準をベースとして国内におけるルール作りを推進いただきたい。また、工場セキュリティ向上の全体像を構想したうえで、その一部として国際標準の活用、例えばIEC 62443の2-3、2-4、3-3を踏まえたJIS化を検討いただけるとよい。日本国内における先進的な業界(例:自動車業界)の規格が国際標準と連携できると、他業界へ横展開がしやすいのではないか。[業界団体等]

© Hitachi, Ltd. 2024. All rights reserved.

A.2 ガイドラインの普及等に関する主なご意見

HITACHI
Inspire the Next

A. 政府における取組み

A.2 ガイドラインの普及

○ヒアリングにおける指摘に見る現状

専門家による伴走の必要性

- 中小企業の情報セキュリティ対策ガイドラインを含め、中小企業単体による適用ではなく専門家による伴走支援が必要 [地域コミュニティ全般]
- 経営ガイドラインについて、ITベンダでガイドラインをかみ砕いた上で、中小企業等へお伝えしている。[地域コミュニティ]

DX等とバンドルした普及の推進

- DXで生産性向上、販路拡大等をしたいという話は担当者にも通じやすく、ITシステム導入にセキュリティをバンドルすることも重要 [業界団体等]
- 政府機関にはDXに伴うセキュリティの必要性についてより広範にアナウンスいただきたい。[地域コミュニティ]

動機づけによる任意の対策実施の支援

- 補助金があることによって、オーナー側に必要性を説明するセキュリティ会社やコンサルタント会社が営業しやすくなると考えられる。また、IT導入補助金のような単年度の支援というよりは複数年にわたる支援が必要ではないかと考える。[業界団体等]
- 一部業界で上流の意識が高いところ(自工会など)では、下流の中小企業も意識している(せざるを得ない)。このアプローチは有効だと考えるが、上流の意識改革から必要であり、それをどのように進めるのかが課題。監督省庁などの働きかけが重要だと考える。[業界団体等]
- サイバーセキュリティお助け隊は有効な取組みと認識している一方で取組み範囲が限定的であるため、更にサービスが充実するとよい。 [政府機関、地域コミュニティ]

強制力のある施策の必要性

- 自動車、金融及び医療関連業界でガイドラインが業種の達成指標として機能している例があるが、それら以外の業種では十分活用されているとは言えない。[IT事業者]
- ガイドラインが現状調達要件などにもなっていないため、インセンティブが無いことから、対策の必然性がなく、次の段階としてより強制力の強い制度を導入し、それに見合う支援施策を検討すべき。[業界団体等]
- ガイドラインに掲載している対策には一定の優先順位をつけている。しかし、特定の企業が優先度の高い対策を調達基準としているという実態が必ずしもあるわけではなく、対策の実施有無をチェックする手段も乏しいため、活用があまり進んでいないものと認識している。[業界団体等]

A.3 ガイドライン関連活動のガバナンス

○ヒアリングにおける指摘に見る現状

- 中小企業ではガイドラインに記載されている事項の理解もあまりできていない実態があるのではないか。また、ガイドラインの存在自体が中小企業に伝わっておらず、策定したままにするのではなく、策定後のモニタリングも策定者が責任をもって行うべきではないかと思う。[業界団体等]
- IPA、商工会議所、東京都、TAMA協会等各団体が似たような取組みを行っており、バラバラになっている。政府に音頭をとっていただき取組みを全体として最適化していただけるとよい。[地域コミュニティ]

© Hitachi, Ltd. 2024. All rights reserved.

B.1 政府から支援機関への働きかけに関する主なご意見

HITACHI
Inspire the Next

B. 政府と支援機関間における取組み

B.1 政府から支援機関への働きかけ

○ヒアリングにおける指摘に見る現状

団体等の横のつながりの欠如

- 一部を除き、セキュリティに係る大きなイベントは開催されておらず、横のつながりが希薄。業界団体は会員企業に対して簡単に連絡をとることができる一方で、外部の業界団体とは連絡がとりにくい。仮に特定の業界向けの普及活動を行おうとしても、アクセスポイントがわからない。
- 既存の枠組みとしてSC3があるが、セキュリティに関する専門家集団となっており、普及啓発の部分での連携には必ずしも適さない。
- 通常接点を持つ事業者は既にセキュリティに対して一定の問題関心を有する事業者に限られることから、DXやセキュリティ対策を進めようとする際にセキュリティについても関心が芽生えつつある層を捕まえてニーズを把握するところを政府等には期待したい。[以上、業界団体等]

支援機関に対する政府の支援

- IPAが情報セキュリティ対策について、さまざまなリソースを提供しているが、必ずしも現場に浸透しているとは言い難い状況。IPAと我々のような中小企業支援機関が、予算面、活動面で連携して普及活動を進められるような支援スキームを希望する。[地域コミュニティ]
- 支援機関向けの補助金があるとよい。[地域コミュニティ、IT事業者]
- 地域での地道な普及啓発は定量的・即効的な効果は見えづらいが、長期スパンで裾野を広げていく活動を支援いただきたい。[地域コミュニティ]
- サイバーセキュリティ経営ガイドラインが公開された際に、セミナーでの紹介を経産省へ依頼したことがあるが、ガイドラインの公開とあわせて、都度セミナーを開催しているわけではない。政府機関側からセミナーでの紹介をもちかけていただけるとありがたい。[地域コミュニティ]

中小企業等の取引先、親会社等への支援

◆取引先からの働きかけ促進

- 弊社としても抱えている中小企業向けのサイバーセキュリティ対策の底上げ活動を費用持ち出しで行っているが、狙われやすい中小の会社ほど意識が低く、対策費用もかけられない。我々のように企業として仕入先を支えようとしている企業にも、国レベルの支援や同業者共同での底上げ活動が必要。取引先を持つ上位企業の費用負担について補助の検討をお願いしたい。
- 契約条件に入れたいところだが、下請け法の関係もありなかなか難しい状況。仕入れ先に強制力を持たせられるよう、牽引をお願いしたい。[以上、IT事業者]

◆親会社からの働きかけ促進

- 総務、経理、ITを兼務している担当者に専門知識を学んでもらうことは難しいため、親会社側にセキュリティ対策やその責任を負わせる仕組みがあるとよい。弊グループでは可能なものはシェアードサービスを導入しシステムを共通化することで、子会社のセキュリティを強化している。ただし、親会社と子会社は別会社となるため、利益供与に該当するかについて考慮が必要。
- 親会社のセキュリティ基準に準拠したシステムを子会社は導入することとなるため、コスト高となり得る。したがって、費用上の配慮があると子会社も参加しやすくなると考えられる。(ただし、税務上の配慮が必要)[以上、IT事業者]

© Hitachi, Ltd. 2024. All rights reserved.

C.1 継続的なリソースの確保等に関する主なご意見

HITACHI
Inspire the Next

C. 支援機関における取組み

C.1 継続的なリソースの確保

○ヒアリングにおける指摘に見る現状

- サイバーセキュリティの重要性は理解しているが、商工会議所における経営指導員の年齢層が高く対応が難しい場合や、県内のサイバーセキュリティ人材が不足しているケースがある。
- 専門家を個別に派遣する場合には費用が多くかかるため、集合研修を有効活用することが重要と考える。[以上、地域コミュニティ]

C.2 支援対象の拡大

○ヒアリングにおける指摘に見る現状

業界団体間の連携による支援の拡大

- セキュリティ系団体は、非IT系を含む民間団体(商工団体、金融機関、業界団体(自工会、金型組合など))との連携に課題あり。
- ビルや工作機械は、業界内の大多数の事業者が所属しているため、他団体との連携の必要性を感じていない。
- スマートホームや制御機器では複数のステークホルダーが絡むため、団体連携は積極的に行っている。他方、これらの団体は大企業が中心で中小企業の参画がほとんど無い。
- 地域コミュニティは、商工会議所をはじめ、地域の経済団体等と連携している。経済団体等と連携したセミナーを実施することで、互いの会員企業等への情報普及が図れる。また各団体に対し「出前講座」の枠組みにより様々な有識者を派遣することで連携を図っている。

民間企業との連携による支援の拡大

- 複数の地域コミュニティが、支援拡大を図るため、自治体や地域金融機関と連携したチャネル開拓を実施している。具体的には、セミナー開催(融資先に行う経営支援サービスの一環)、金融機関からの支援先の紹介がなされている。
- また、セミナーの開催等にあたってITベンダーとの連携を行った事例もあった。地域コミュニティ内で他地域の情報が十分得られない場合、ITベンダーと連携する形で進めているとのことであった。
- セキュリティベンダやセキュリティコンサルに委託する費用が高いため、お抱えの事業者へ依頼を行うと考えられる。適切に設定を行えていないケースがあるため、お抱えの事業者にもセキュリティについて学んでいただくことが重要と考えられる。具体例等を示すことでかかる事業者が適切なセキュリティ実装を行えるレベルまで教育支援を行うことが大切。[IT事業者]

© Hitachi, Ltd. 2024. All rights reserved.

D.1 支援機関から中小企業への働きかけに関する主なご意見

HITACHI Inspire the Next

D. 支援機関と中小企業間における取組み

D.1 支援機関から中小企業への働きかけ

○ヒアリングにおける指摘に見る現状

◆サイバーセキュリティに対して関心の低い層に対する働きかけ

- 多数の団体からセキュリティに係る課題認識を持つ中小企業がそもそも少ない点が指摘されている。そういった企業に対しては、まずセキュリティ対策そのものの必要性から説く必要があり、機運を高めてから、具体的なガイドラインの存在やその中身を説明する、何かと抱き合わせにするか景品を出す等の施策が提案された。
- その際、DXによって将来像を描くと同時にサイバーセキュリティの重要性を理解いただくことが重要。
- また、意識啓発の方法についても、同じ情報提供をするだけでは聞き手に対する効果が更に薄くなる可能性がある点が指摘された。

◆サイバーセキュリティに対して一定の関心がある層に対する働きかけ

- 関心を持って参加する企業には、ガイドラインの内容をいかに分かりやすく説明できるか(例を用いる等)が課題。
- ワークショップや演習等の参加型の形式は多数の団体から有効であった旨の意見があった。

◆IT導入補助金と関連した働きかけ

- サイバーセキュリティお助け隊導入をIT導入補助金の加点要素にしていただいた結果、申請する業者から問い合わせが増加し、契約件数が増えた経緯がある。ただし、導入から利用料の補助が切れる1年後にサービスを解約した企業が多くみられた。
- IT導入補助金制度の条件に該当する事業者に対して、サイバーセキュリティお助け隊サービスと併せて制度の案内を行っているが、中小企業が独力でIT導入補助金を申請することは難しい。
- 販売パートナーは、中小企業が興味をもっているシステムに関する情報を積極的に中小企業へ提供しているようである。営業活動の一環として補助金に関する情報を中小企業へ提供しているようであるが、セキュリティに特化した情報はあまり提供していないようである。[以上、IT事業者]

◆効果的な周知・啓発方法

- サイバーセキュリティ単体で集客の期待はあまりない一方で、大規模イベント(CEATEC)を活用したセミナーについては、多くの参加がある。
- 中小企業はセミナー等の情報を随時チェックしていないため、プッシュ型の案内の方がリアクションを期待できる。[地域コミュニティ]
- ガイドラインの周知を行う際には、FAXでの案内送付、ポスター等を活用した普及啓発も重要。[業界団体等]
- 地域の名士企業が取組みに前向きになると、地域の企業も取組みに前向きになるケースがある。つながりを広げていくためには、影響力がある人やそのネットワークを見極めることが重要となる。セキュリティ単体での働きかけは難しいため、セキュリティに対する優先順位をあげてもらうための働きかけを行いつつ、各企業とWIN-WINの関係を構築することが重要である。[IT事業者]
- 地域によってセキュリティに対して積極的な地域とそうでない地域がみられる。
- 後者は、政府等の推進主体が地域のキーマンと出会えていない可能性があるため、各地区に普及を進める(説得する)人を配置するべきではないか。キーマンと会うために地方を行脚する体制があるとよい。また、業界の横のつながりを活用することや商工会議所の若いメンバ(青年会など)にアプローチすることも有効と考えられる。[中小企業]

© Hitachi, Ltd. 2024. All rights reserved.

E 中小企業における取組みに関する主なご意見

HITACHI
Inspire the Next

E. 中小企業における取組み

○ヒアリングにおける指摘に見る現状

◆サイバーセキュリティに対する関心の低さ

- サイバー攻撃を受ける可能性が低いとの理由でセキュリティ対策を実施しない企業が存在する。特に、都市部と比較して地方ではその傾向が顕著。
- 能動的にセキュリティに関する情報収集を行っている企業は極めて少数である。(情報収集を行っていたとしても、補助金情報のみであったりする) [以上、IT事業者]
- ある中小企業の経営者は「うちにとられて困るものはないからリスクはない」とおっしゃっていた。このような場合は「明日PCのデータが消えたときにお客さんに迷惑かからないか」と問いかけるようにして、リスクを伝えている。
- セミナーの案内はシステム部門に丸投げされることが多い。経営層もセキュリティについて理解が追いついていないため、セミナーに参加することは少ないのではないか。したがって、地方では、情報の内容よりも顔の見える関係での情報交換、特に情報の発信主体が重要となる。医療分野ではセキュリティに馴染みがない方が多いため、いい仲間といい情報に出会えるかが重要なポイントとなる。[以上、中小企業]

◆人材、予算等の不足

- 中小企業ではセキュリティ担当が設置されていたとしても兼務が多く、リソース(人や時間)が不足していることが原因の1つとして考えられる。情報提供はメール等で行うが、そもそも担当者が自席にいてPCを見ている時間も短いようである。
- サイバーセキュリティ対策には非常に費用がかかる(例:1声100万円)というイメージがNHKの報道によってついてしまったことも、反応が薄い原因の1つ。
- セキュリティ人材の不足が課題である。セキュリティ人材の確保を進める一方で、弊グループではシェアードサービス等を導入することによって各社のセキュリティへの負担を軽減させる方向で進めている。
- セキュリティ人材が不足しているため、政府による育成の仕組みがあるとよい。個別の話になるが、弊社から人材を派遣しているICS-CoEの教育プログラムは企業側の負担が大きい。参加費用が大きいだけでなく、派遣した人材の業務が止まることも大きい。業務を続けながら学ぶことができる仕組みか、あるいは企業側のデメリットを補填する支援があるとよい。(例:業務をとめずに教育制度に参加できるような仕組み、派遣した人材の人件費を補填する仕組み、人材を派遣した企業に対して報奨金を提供する仕組み)

◆サイバーセキュリティに対する関心の高い企業の共通性

- サプライチェーン上位企業から説明を受けている企業や、上記に伴い、今後視察がある等噂を聞いて取り組み始めている企業、過去に被害を受けた経験がある企業はセキュリティ対策の推進を積極的に行っている傾向にあり、実際にそのような企業から問い合わせをいただくことがある。しかし、被害を受けてない企業の関心は総じて低い。
- セキュリティ被害情報は被害企業から外に出ず、公にならないことがほとんどであり、同業他社でインシデントが生じていてもそれを知る由がない。[以上、IT事業者]

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

3. 中小企業を対象としたガイドライン等の普及・啓発に関する課題・施策

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 中小企業を対象としたガイドライン等の普及・啓発に関する課題

© Hitachi, Ltd. 2024. All rights reserved.

課題の評価指標(1/2)

HITACHI
Inspire the Next

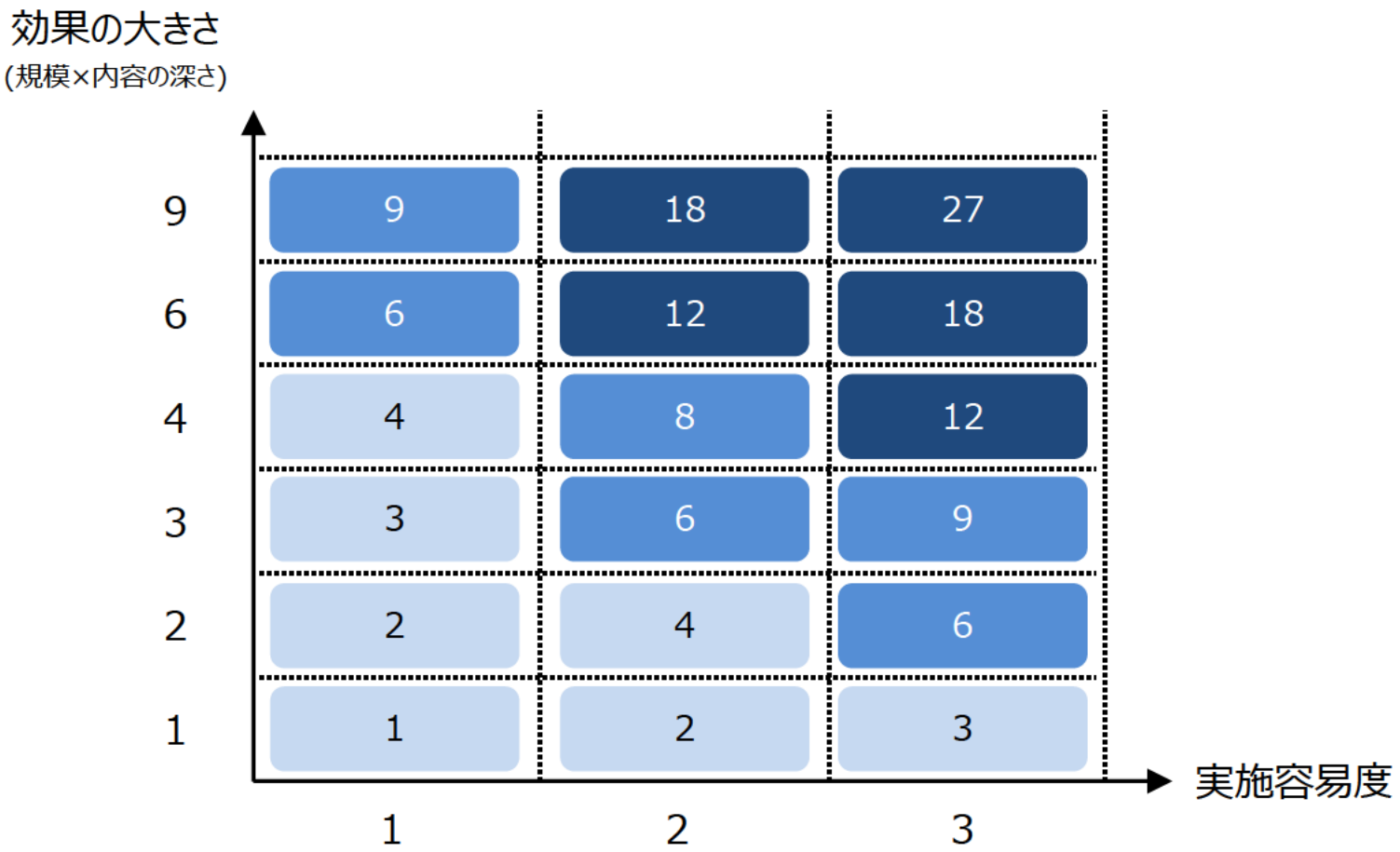
- 前回の指摘を踏まえ、課題間の優先度をよりはっきりとさせるため、効果の大きさを「支援規模」と「支援内容の深さ」に分けつつ、「実施難易度」を「実施容易度」とした。

分類	観点	評価	評価の目安	点数
効果の大きさ	**支援規模**	**H**igh	対策の必要性はあるものの意識が高くない多くの中小企業や、支援機関に対して働きかけることができる	3
		Moderate	対策の必要性はあるものの意識が高くない中小企業や、支援機関に対して、範囲(地域/業界等)を限って働きかけることができる	2
		Low	対策の必要性はあるものの意識が高くない中小企業や、支援機関に対して必ずしも働きかけることはできない	1
	支援内容の深さ	**H**igh	セキュリティ対策に一定の関心を払う中小企業の多くが、より高度な対策を推進することに寄与する。	3
		Moderate	セキュリティ対策に一定の関心を払う特定の属性(地域/業界等)を有する中小企業が、より高度な対策を推進することに寄与する。	2
		Low	セキュリティ対策に一定の関心を払う中小企業の多くが、より高度な対策を推進することには必ずしも寄与しない。	1
実施容易度		**H**igh	過去事例や取組みの具体的な受け皿があり、実施にあたり大きな困難は想定されない	3
		Moderate	過去事例や取組みの具体的な受け皿はあるが、実施にあたりある程度の困難(関係者の反対、多大な予算等)が想定される。	2
		Low	過去事例や取組みの具体的な受け皿が乏しく、実施にあたり大きな困難(関係者の反対、多大な予算等)が想定される。	1

© Hitachi, Ltd. 2024. All rights reserved.

課題の評価指標(2/2)

- 効果が大きく、実施難易度が低いものほど課題としての優先順位が高くなる。
- 「優先度高」とした課題について次頁以降赤枠で、「優先度中」としたもののうち比較的得点が大きいもの(8点または9点)について緑色で囲った。



[凡例] ：優先度高 ：優先度中 ：優先度低

© Hitachi, Ltd. 2024. All rights reserved.

ガイドライン等の普及・啓発に関する課題の評価(1/2)

HITACHI
Inspire the Next

小分類	課題	効果の大きさ		容易度	評点
		規模	深さ		
1.1 ガイドラインの策定・整理					
中小企業のサイバーセキュリティ対策推進における各種ガイドライン等の位置づけ明確化	中小企業の対策推進ロードマップにおけるCPSF関連ガイドライン等の位置づけ明確化	L (単体では裾野拡大なし)	M (普及には別の取組みが必要)	H (基礎となる素材が既存)	6
セキュリティ一般ではなく、「CPSFに基づくガイドライン」の普及を目指す場合は必須と考えられる。	ガイドライン間の差分明確化	L (単体では裾野拡大なし)	M (普及には別の取組みが必要)	H (必要な作業は機械的)	6
	中小企業向けのガイドラインと国際標準とのアライメント確保	L (単体では裾野拡大なし)	M (普及には別の取組みが必要)	H (必要な作業は機械的)	6
CPSF関連ガイドライン等の活用促進に向けたコンテンツの作成	ガイドラインに基づくより具体的なコンテンツの整理(簡易版コンテンツ等)	M (啓発コンテンツは一定の効果)	M (普及には別の取組みが必要)	M (ある程度の検討が必要)	8
1.2 ガイドラインの普及					
ガイドラインの普及に向けたより効果的な周知活動の推進	政府から支援機関(IT事業者/地域コミュニティ)に対するガイドラインに関する情報提供	M (支援機関に広く発信可)	M (普及には別の取組み要)	H (部分的には既に実施)	12
	中小企業向けのDX推進活動等とバンドルした普及の推進(例：チャネルの共有)	H (DX推進企業へ広く周知可)	M (高度な対策を含めれば可)	H (連携先は局内に既存)	18
ガイドラインに基づく対策実装の動機付け	一部対策の調達要件化及び実施確認の推進	H (広く対策を強制可能)	H (高度な対策も強制可能)	L (関係各位の負担が大)	9
	中小企業の実態に即した効果的な促進策(補助金、お助け隊の拡張を含む)	H (直接的に対策を促進)	H (直接的に対策を促進)	M (基礎となる事例が既存)	18

© Hitachi, Ltd. 2024. All rights reserved.

ガイドライン等の普及・啓発に関する課題の評価(1/2)

HITACHI
Inspire the Next

小分類	課題	効果の大きさ		容易度	評点
		規模	深さ		
1.3 ガイドライン関連活動のガバナンス					
ガイドライン関連活動のガバナンス強化	ガイドラインの普及に係るモニタリング、レビューを行う仕組みの構築	M (レビュー観点に組込み可)	M (レビュー観点に組込み可)	M (WGまたはSC3を活用？)	8
	政府機関及び支援機関におけるガイドラインその他の取組みの全体整理・最適化	M (整理の観点に組込み可)	M (整理の観点に組込み可)	M (関係者間の調整が一定必要)	8
2.1 政府から支援機関への働きかけ					
支援機関等による横断的枠組みの構築	普及活動等について支援機関間の横の関係を促進する枠組みの構築(例：SC3)	H (機関間の横の広がりに期待)	H (全体の水準向上にも寄与)	M (SC3活用？)	18
個々の支援機関に対する支援	支援機関に対する予算面の支援 (複数年度の事業も含む)	H (継続的な活動による拡大)	H (継続的な活動による深化)	M (各地に受け皿や実績あり)	18
3.1 支援機関における継続的なリソースの確保					
デジタル/サイバーセキュリティに対応できる支援機関側の人材の確保 (あるいはデジタル/サイバーセキュリティに対応できる外部機関との連携確立)		H (支援機関の取組促進)	H (人材は対策普及の基礎)	M (セキュリティプレゼンタ等が既存)	18
継続的なコミュニティ活動を推進するための財政基盤の確保		H (資金は活動運営の基礎)	H (資金は活動運営の基礎)	M (これまで政府から支援実績あり)	18

© Hitachi, Ltd. 2024. All rights reserved.

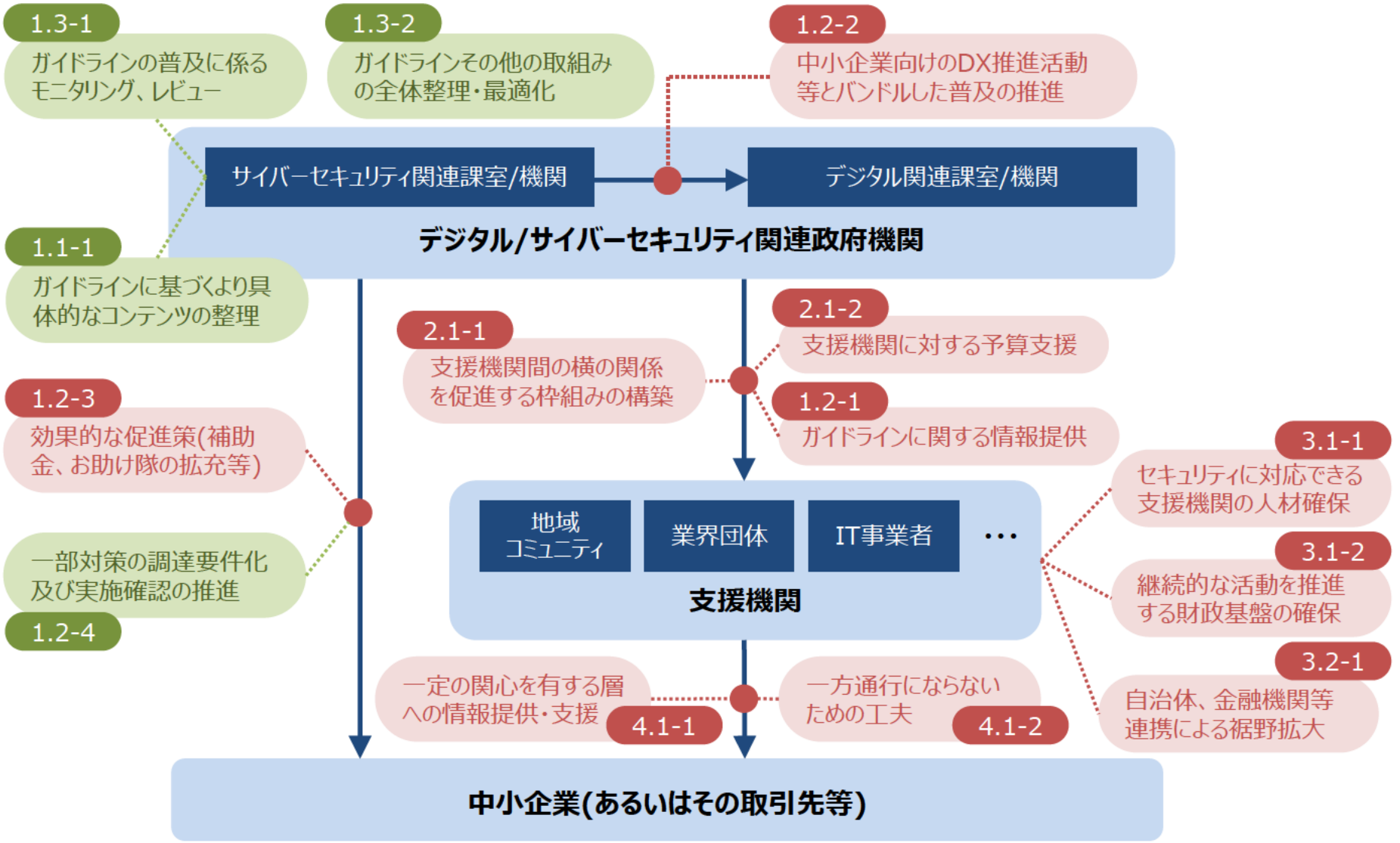
ガイドライン等の普及・啓発に関する課題の評価(2/2)

HITACHI
Inspire the Next

小分類	課題	効果の大きさ		容易度	評点
		規模	深さ		
3.2 支援対象の拡大					
業界団体・地域コミュニティ内外の連携枠組みの構築	自治体や商工団体、金融機関との連携等による裾野の拡大	H (支援規模拡大を促進可)	M (普及には別の取組み要)	M (各地に事例が存在)	12
4.1 支援機関から中小企業への働きかけ					
継続的かつ効率的なプッシュ型/プル型の情報提供・支援の推進	関心が薄い層への情報提供・支援(DXと合わせた必要性の説明等)	H (支援対象拡大を促進)	M (ステップアップには別取組み要)	L (これまでできていない)	6
	一定の関心を有する層への情報提供・支援(例を用いたわかりやすい説明等)	M (対象拡大には別取組み要)	H (対策水準向上に寄与)	M (部分的には既に実施)	12
	一方通行にならないための工夫(フォローアップセミナーの実施等)	M (既存対象へ支援強化)	H (対策水準向上に寄与)	M (部分的には既に実施)	12

© Hitachi, Ltd. 2024. All rights reserved.

優先的な課題のマッピング



© Hitachi, Ltd. 2024. All rights reserved.

3-2. 普及・啓発に関連する国内外の取組み

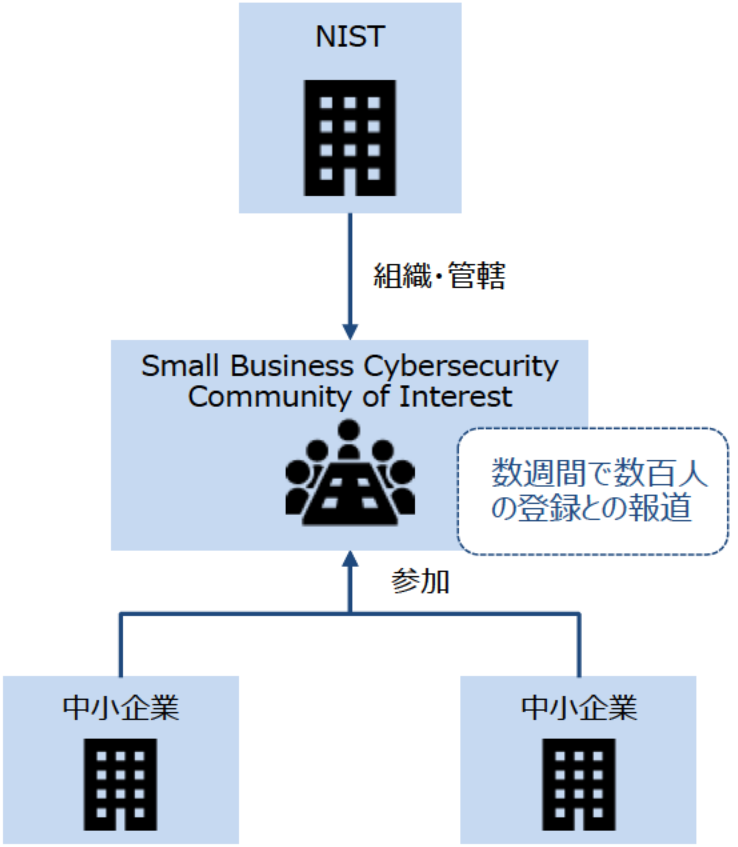
© Hitachi, Ltd. 2024. All rights reserved.

米国の事例 / NIST Small Business Cybersecurity Community of Interest(COI)の立ち上げ

- NISTは、中小企業向けのコミュニティを立ち上げ、バーチャルミーティングを通じてガイドラインを含むコンテンツの紹介・配信を実施。

主体/取組みの概要

実施主体	内容
実施主体	• NIST
設立時期	• 2023年4月
背景	• 中小企業のニーズや能力に適したガイダンスは不足している一方で、広く情報であふれているため、中小企業はセキュリティ確保のために重要な事項を知ることが困難になっている。
目標	• 利害関係者の間でアイデアやリソースを交換し、繁栄するビジネスを成長させ維持するためのサイバーセキュリティの知識、スキル、能力を向上させるサイバーセキュリティのガイダンスと実践を促進する。 • 中小企業コミュニティが直面するサイバーセキュリティとプライバシーに関する共通の課題とニーズについて議論を深める。 • 中小企業の所有者/ベンダが、NISTのリソースや取り組みが開発される際に、直接意見を交換できる場を提供する。 • 他の所有者/ベンダやNISTと協力し、このグループが必要かつ適切と判断した新たなサイバーセキュリティリソースを開発する。
取組み内容(例)	• 毎月または四半期ごとにバーチャルミーティングを開催し、NISTにおける中小企業に関連のイベント、リソース(例:NIST IR 8183の更新情報)、イニシアチブに関する最新情報を定期的を提供。 • NISTはCOIから小規模企業から中小企業のセキュリティに関する問題について情報を収集。



[参考] NIST "Join Our NEW NIST Small Business Cybersecurity Community of Interest!"
https://www.nist.gov/itl/smallbusinesscyber/about-contact-us/subscribe

© Hitachi, Ltd. 2024. All rights reserved.

米国の事例 / SBA /サイバーセキュリティパイロットプログラムを通じた助成金の提供

- SBAはサイバーセキュリティパイロットプログラムを通じて、メリーランド州政府に助成金を提供。
- メリーランド州政府は中小企業に対して募集を行った上で、採用企業に対して助成を実施。

主体/取組みの概要

本事例は、必ずしもガイドラインの普及啓発の取組みではないが、トレーニングの過程で各種ガイドラインが活用される可能性。

応募要件(メリーランド州における要件)

- 従業員50人以下の企業
- 業種:小売、レストラン、金融、医療、製造業
- 事業段階:製品またはサービスによる収益を伴う事業段階に達していること(事業開始後3年未満)
- 知識レベル:事業の全従業員がこの必須トピックに関する研修を修了し、また、このトピックに関するテストに合格することにより、基本レベルの知識を証明できること



助成内容(メリーランド州における助成内容) (※)

- サイバーセキュリティシステムのセキュリティスキャンの実施
- 全従業員を対象とした<u>サイバーセキュリティトレーニングの提供</u>(選ばれた従業員は、その知識レベルに合わせたトレーニング、業界特有のトレーニングを提供)
- <u>1事業者あたり1万ドル</u>を上限に、セキュリティ・スキャンで特定された<u>ハードウェアとソフトウェアを供給・設置</u>

※ 助成内容に示された「サイバーセキュリティシステム」「(セキュリティ・スキャンで特定された)ハードウェアとソフトウェア」の具体的な内容は述べられてない。しかし、資金提供を行うSBAボルチモア地区のディレクターは、「メリーランド州の600万社以上の中小企業は、サイバー犯罪者が欲しがる情報を持っているが、大企業のようなセキュリティインフラが不足しているため、魅力的な標的」と述べており、セキュリティインフラの導入等が本プログラムの主な目的の1つとなっている。したがって、前述の2つの用語はセキュリティインフラとなり得るシステムを指していると考えられる。

[参考] Maryland Commerce “Maryland Commerce Awarded Federal Grant to Assist Small Businesses with Cybersecurity Training” https://commerce.maryland.gov/media/maryland-commerce-awarded-federal-grant-to-assist-small-businesses-with-cybersecurity-training

© Hitachi, Ltd. 2024. All rights reserved.

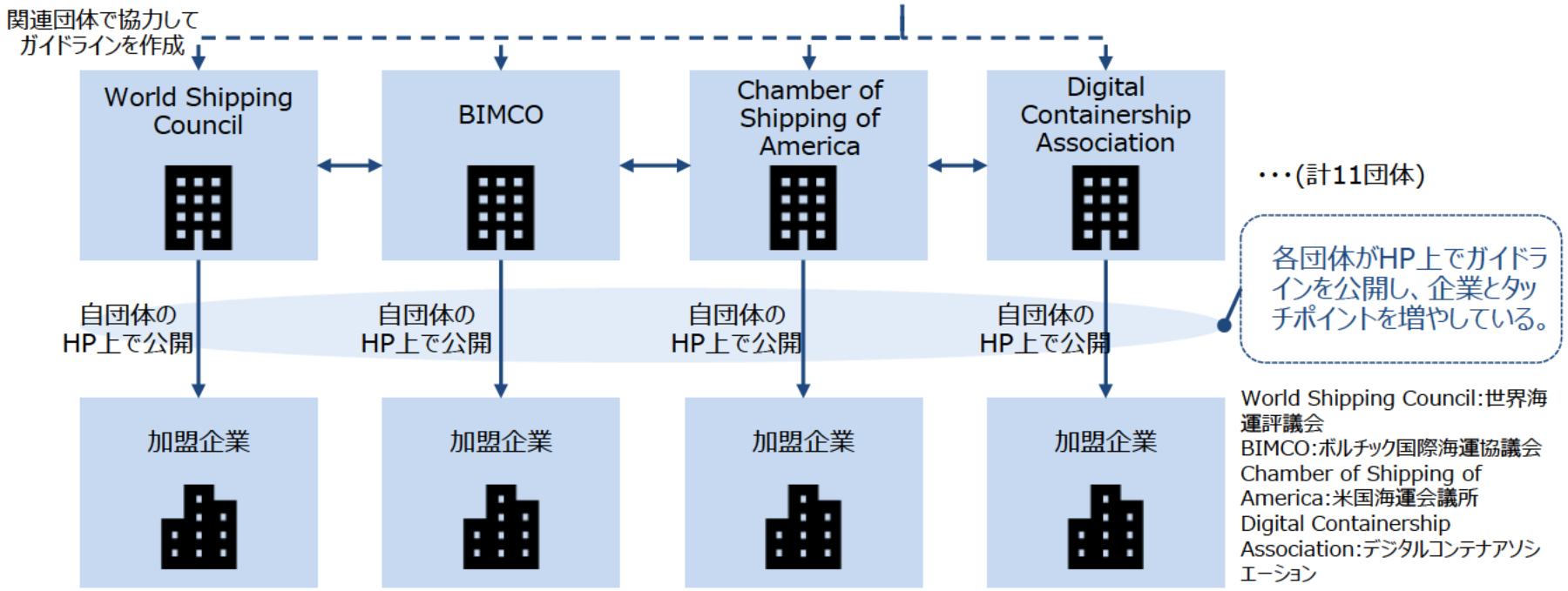
米国の事例 / 世界海運評議会(World Shipping Council)等の取組み

- ガイドラインをより普及させるために、関連する業界団体で協力して作成したガイドラインを各団体がHP上で公開し、企業とのタッチポイントを増やしている。

主体/取組みの概要

船舶のサイバーセキュリティガイドライン
(THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS Ver4.0)(2022/6/1)

- 船員、環境、貨物、船舶の安全とセキュリティ向上を目的として、適切なサイバーリスク管理戦略の策定方法をガイド
- NIST CSFに準拠、沿岸警備隊(U.S. Coast Guard)が作成したプロファイルを使用可能
- なお、IMO(国際海事機関)は決議MSC.428(98)にて、船舶の安全管理システムにサイバーリスク管理を組み込むことを義務付けられている。本ガイドラインではそのリスク管理方法をガイドラインで示す。



World Shipping Council:世界海運評議会
BIMCO:ボルチック国際海運協議会
Chamber of Shipping of America:米国海運会議所
Digital Containership Association:デジタルコンテナアソシエーション

[参考] World Shipping Council" Protection against cyber crimes."
https://www.worldshipping.org/security

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/現状認識

HITACHI
Inspire the Next

- 予算や知識、人材の不足からセキュリティ投資は後回しにされている、政府等が発行するガイドラインについても中小企業向けの内容に必ずしもなっていない等、EUでも日本と概ね共通した問題が指摘されている。

※ 赤字部分は既往調査結果と整合するもの、青字部分は新たな観点を含み得るものを示す。

分類	項目	指摘されている課題
政府による取組みの課題	中小企業に特化したガイダンスの不在	• ほとんどの既存文書は専門的な対応が可能な大企業を対象としている。 • ISO 27001:2013におけるマネジメントシステムの設計、実装、運用、改善は、多くの中小企業にとって、理解や実装に外部の専門家の支援が必要である。 • 中小企業が対応力を高めるために導入できる基準はいくつかあるが、導入に時間がかかる。 • ヒアリング対象の中小企業は、政府等の発行するガイドラインを認知していなかったり、多くの資料が背後にある理論を強調するに留まり、実践的なガイドラインを提供していないと主張していた。
中小企業による取組みの課題	対策予算の不足	• サイバーセキュリティ対策には、さまざまな側面からの投資が必要となるうえ、高度なファイアウォールやSIEM等の高度なサイバーセキュリティソリューションは大規模な投資となる。 • サイバーセキュリティが成熟した組織にとって有用な、多種多様な能力を提供する高度なソリューションは、中小企業が提供されるソリューションを理解しておらず、利用されないことが多い。
	専門知識と人材の不足	• 中小企業では、従業員に複数の役割を割り当て、専任の担当者を置くことが少ないが、多くのサイバーセキュリティ・ソリューションは、適切な実装・管理に専門的なIT知識を必要とする。 • ベンダーは、自社製品がデフォルトで安全であることを保証し、製品の管理が非技術者にとって比較的簡単であることを保証するべき。
	外部支援の不在	• 専門人材を直接雇用していない場合、外部の専門家の支援に投資する必要があるが、多くの中小企業には外部の専門家を雇うような余裕はなく、中小企業の上級管理職は自分自身の知識や同僚ネットワークから得た知識に頼っている。
	セキュリティ投資なきオンライン移行	• 多くの中小企業が事業の全部または一部をインターネットで提供するように転換したが、変化を急ぐあまり、多くの中小企業は、セキュリティ対策に時間や資金を投資しなかった。
	不十分なセキュリティ保護	• 70%以上の中小企業がエンドポイントウイルス対策、バックアップ、ファイアウォール、ソフトウェア更新等の基本的な対策を実施している一方、従業員に対する意識向上トレーニング、ロギングによる検知活動、可搬媒体の管理等を実施するのは30%以下である。

[参考] Cybersecurity for SMEs - Challenges and Recommendations
https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/ENISAによる推奨事項

HITACHI
Inspire the Next

- 前頁に示した現状の課題を踏まえ、以下に示す6つの取組みを進める必要があると整理している。
- 取組みには、的を絞ったガイドライン・テンプレートの提供や価格面に対処するようなものが含まれている。

項目		推奨事項 ※ 赤字部分は既往調査結果と整合するもの、青字部分は新たな観点を含み得るものを示す。
1	**幅広いサイバーセキュリティ推進** (PROMOTE CYBERSECURITY AT LARGE)	• 企業団体と連携した中小企業の経営者、従業員等への意識向上キャンペーンの実施 • 多くの中小企業はこうしたキャンペーンに参加しないか、効果的に届いていないため、今後のキャンペーンは、中小企業をターゲットとしてより焦点を絞ったものにする必要
2	**的を絞ったガイドライン・テンプレートの提供** (PROVIDE TARGETED GUIDELINES AND TEMPLATES)	• 中小企業にとって使いやすく、明確で構造化されたガイドライン、計画、手順、演習の作成 • 現実的で具体的な例、簡単な用語、容易に翻訳できる言語を含むグッドプラクティスハンドブックの作成 • ガイドライン、演習、手順等のために、中小企業の代表機関、公共部門組織及び利害の対立がない場合にはサイバーセキュリティ企業との協力による官民協力の提案
3	**中小企業に焦点を当てたサイバーセキュリティ標準の策定** (CREATE SME FOCUSED CYBERSECURITY STANDARDS)	• 大企業向けであり、必ずしも中小企業向けではない既存サイバーセキュリティ標準の採用方法について、中小企業に合わせたガイダンスや実施ガイドを作成 • 標準化委員会への参加から最終的な標準の使用・採用まで、標準のライフサイクルの全段階における中小企業の参加を確保
4	**リスク管理フレームワークの活用強化** (BOLSTER USE OF RISK MANAGEMENT FRAMEWORKS)	• 専門知識がなくても実施しやすく、中小企業向けに拡張可能なリスク管理枠組みの設計、普及(例：オランダのVNO-NCWの中小企業向けサイバーリスクガイド) • 当該リスクフレームワークの利用促進、その適用方法に関する指示の提供
5	**サイバーセキュリティを安価に** (MAKE CYBERSECURITY AFFORDABLE)	• 適切なサイバーセキュリティに関する助言またはガイドラインへのアクセス改善 • 中小企業のサイバーセキュリティ態勢強化のための資金提供 • 中小企業1社あたりのセキュリティソリューションの価格を引き下げるためのツールを提供する(より効果的な調達方法とシステムの使用、需要のプール等)。
6	**ISACの創設促進** (PROMOTE THE CREATION OF ISACS)	• 中小企業のISAC参加促進(特に中小企業セクターを対象としているもの)

[参考] Cybersecurity for SMEs - Challenges and Recommendations
https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/ENISA中小企業向けガイダンス

HITACHI
Inspire the Next

- 2021年6月、ENISAは12項目からなる中小企業向けガイダンスを公表。

No.	項目	提示された対策の概要
1	優れたサイバーセキュリティ文化の涵養	• 経営者への責任帰属 • サイバーセキュリティポリシーの提示、定期的なサイバーセキュリティ監査の実施 • GDPRに基づくデータ保護の実施
2	適切なトレーニングの提供	• 全従業員を対象とした定期的なサイバーセキュリティ意識向上トレーニングの実施 • サイバーセキュリティ管理責任者に対する専門的なトレーニングの実施
3	効果的なサードパーティ管理の確保	• すべてのベンダー、特に機密データにアクセスできるベンダーに対する積極的な管理、合意されたセキュリティレベルの維持
4	インシデント対応計画の策定	• 正式なインシデント対応計画の策定、明確なガイドライン、役割、責任の文書化
5	システムへのセキュアなアクセス	• パスフレーズ(3以上の文字種をランダムに組合せた文字列)または強固なパスワードの推奨
6	セキュアな機器	• ソフトウェアのパッチ適用と最新状態の維持 • アンチウイルスソリューションの導入、電子メールとウェブの保護ツール使用、データの暗号化
7	セキュアなネットワーク	• ファイアウォールの導入 • リモートアクセスツールの定期的な見直し、接続先の制限、強固な認証の実施
8	物理セキュリティの改善	• 重要な情報が保管されている場所に対する適切な物理的管理の実施
9	セキュアなバックアップ	• 定期的なバックアップの取得(可能な限り自動化)、定期的なデータ復元テストの実施 • 本番環境外での暗号化した上でのバックアップ保管
10	クラウドの活用	• クラウドプロバイダーと契約する前の特有のリスクに対する考慮 • EU/EEA域外へのデータ移転に関する法律や規制の遵守確認
11	セキュアなオンラインサイト	• ウェブサイトに対する定期的なセキュリティ・テストの実施
12	情報の探索と共有	• サイバー犯罪に関する同業者等への情報共有

[参考] Cybersecurity guide for SMEs - 12 steps to securing your business
https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/ENISA中小企業向けアセスメントツール

HITACHI
Inspire the Next

- ENISAは中小企業のサイバーセキュリティ対策状況を可視化するためのWebアセスメントツールを提供。
- 回答データはENISAに適宜匿名化されたうえで提供される。

中小企業向け自己評価モジュール

ビジネスプロファイル
(Business Profile)

- 基本的な属性情報について回答を求める。[7項目]
  - 企業規模
  - セキュリティ支出規模
  - 業種
  - 利用している外注サービス
  - アプリケーション内製の有無
  - 想定されるビジネス影響の程度

成熟度
(Maturity Level)

- 一般的なセキュリティ対策の実施状況について回答を求める。[39項目]
  - 資産インベントリの整備
  - サイバーセキュリティトレーニングの実施
  - 社内における技術担当者の有無
  - 外部事業者へのリスク評価の実施
  - 個人データの保護状況
  - インシデント対応計画の策定　等
- 総合結果は、Foundational/Advanced/Expertの3分類で示され、ヒト/プロセス/技術という対策カテゴリごとにスコアが示される。

改善行動計画
(Improvement Action Plan)

- 上記の回答結果に基づいて、改善に向けた行動計画を作成する。

ベンチマーク
(Benchmark)

- 類似事業者における対策状況と自社のものを比較する。

[参考] Cybersecurity Maturity Assessment for Small and Medium Enterprises
https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/団体等による取組み(GEIGER)

- GEIGERは、中小企業がサイバーセキュリティ、データ保護、プライバシーに関するリスクを認識し、これらのリスクを軽減するための支援を受けることができるソリューションを開発するイノベーション・プロジェクトである。
- このプロジェクトは、セキュリティ専門家、サイバーレンジ、国立サイバーセキュリティセンターと協力し、中小企業がサイバー脅威を認識するのに役立つサイバーセキュリティの「ガイガーカウンター」であるGEIGERを開発した。中小企業はウェブやスマートフォンでGEIGERを使用することができ、企業にとっての現在のリスクのレベルを動的に表示する。



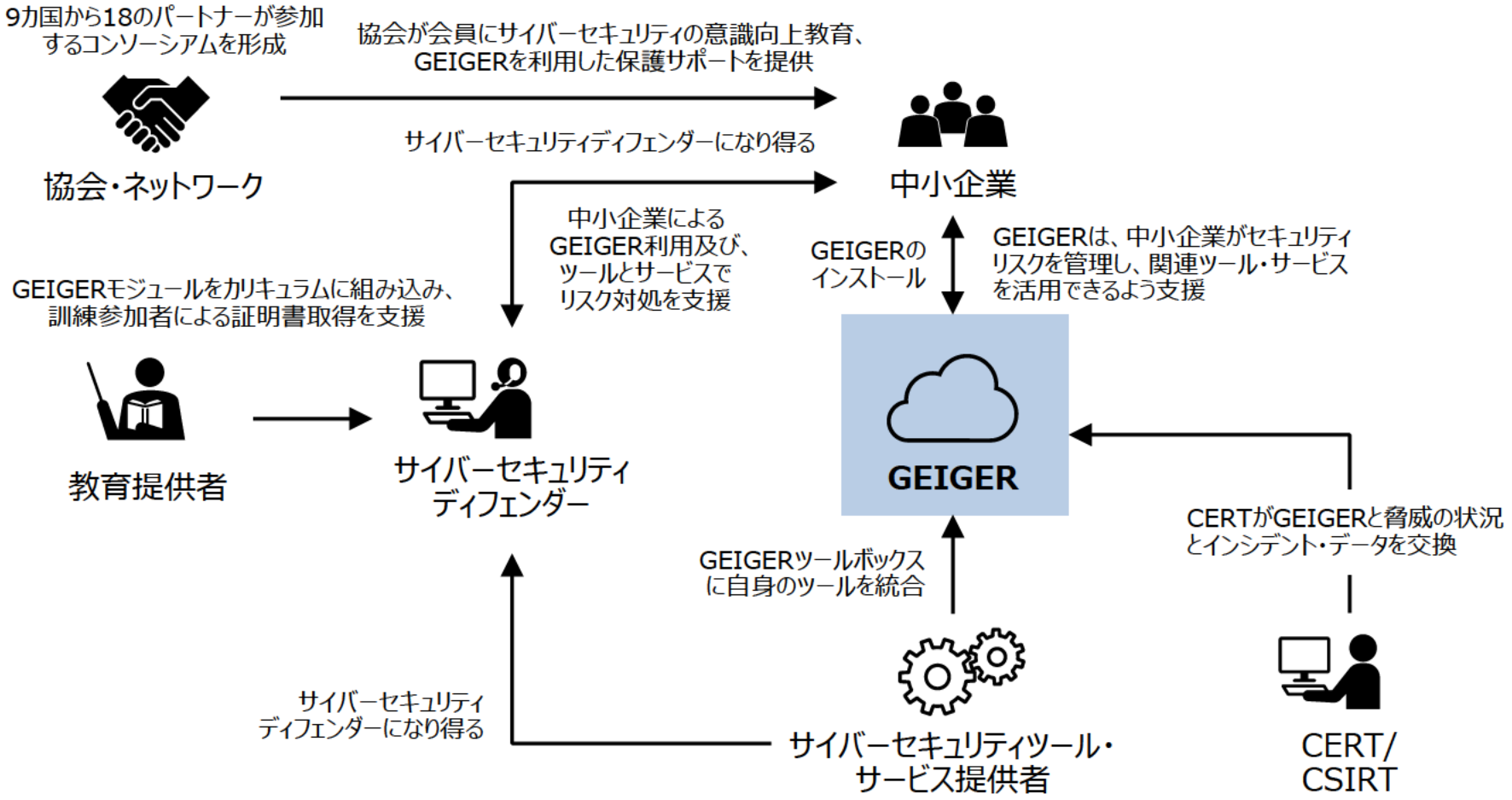
- 中小企業のリスクとインシデント検知をインシデント・データベース(GEIGERクラウド)の実装を加速することで実現する。
- 中小企業が利用するサービスとしてのGEIGERには、以下が含まれる。
  - ✓ GEIGERインジケータ
    誰でも簡単に自分自身のリスクと他者との比較を理解できる指標。
    リスク低減のための推奨事項がスコアの算定に使用される。
    結果は匿名化されたうえでCERT/CSIRTやセキュリティ関係協会へ共有され得る。
  - ✓ GEIGERツールボックス
    リスクを迅速に低減するための推奨事項、ツール、ガイダンス等を示す。

[参考] Easy and affordable cybersecurity solution for small businesses
https://project.cyber-geiger.eu/

© Hitachi, Ltd. 2024. All rights reserved.

EUにおける取組み/団体等による取組み(GEIGER)

- ツールによる要求事項準拠の評価を行うだけでなく、関係機関とも連携して対策水準向上に資するエコシステムを形成する。



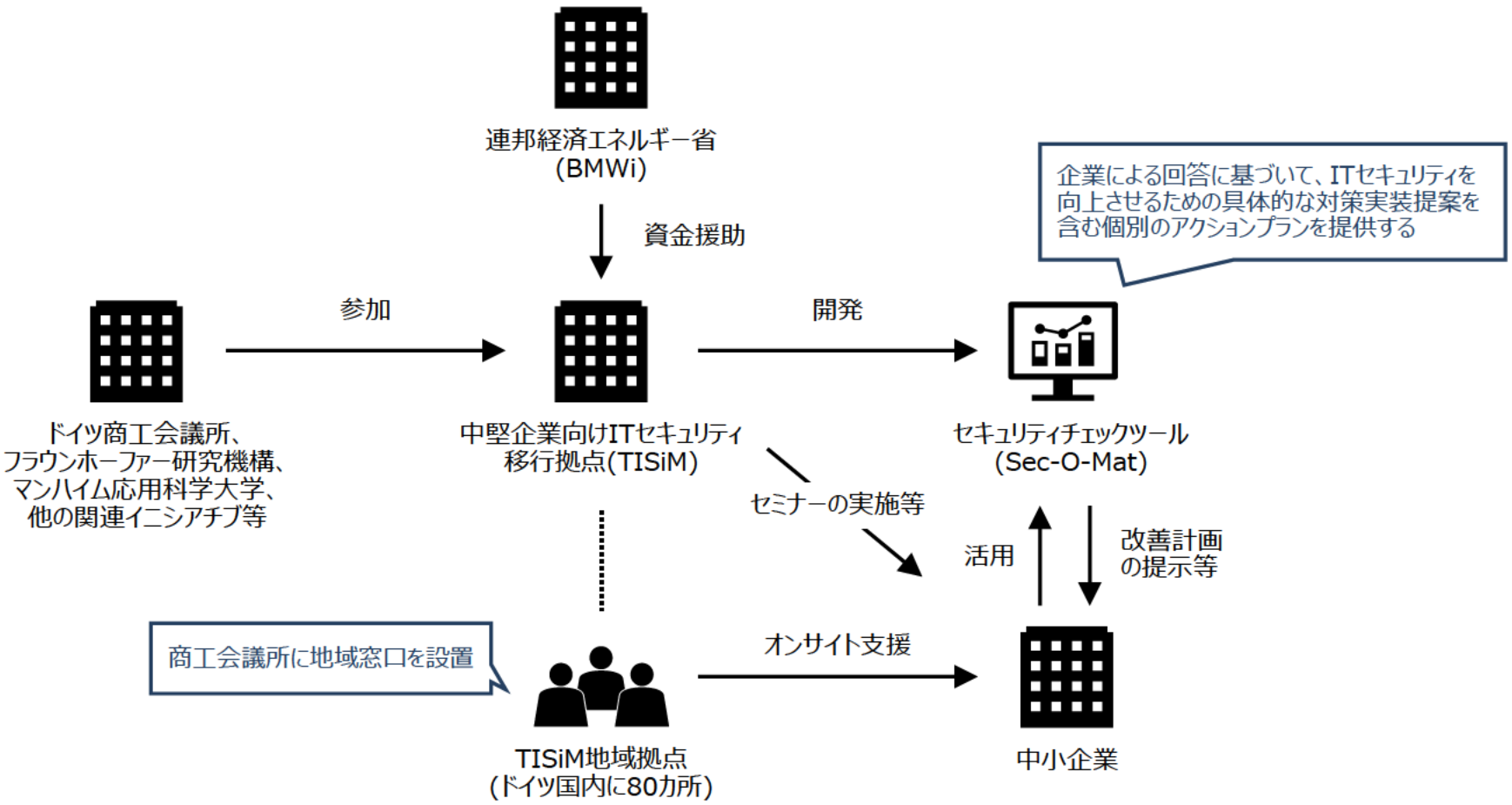
[参考] Easy and affordable cybersecurity solution for small businesses
https://project.cyber-geiger.eu/

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/中堅企業向けITセキュリティ移行拠点(TISiM)

HITACHI
Inspire the Next

- 中堅企業向けITセキュリティ移行拠点(TISiM)は、産学が参加するコンソーシアムであり、連邦経済エネルギー省(BMWi)が資金提供し、地域にも展開するエコシステムを形成している。



[参考] BMWi: TISiM stärkt sichere Digitalisierung in Mittelstand und Handwerk
https://www.tisim.de/bmwi-tisim-staerkt-sichere-digitalisierung-in-mittelstand-und-handwerk/
More cyber security for medium-sized businesses
https://www.fokus.fraunhofer.de/en/fokus/news/tisim_2020_10

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/資金援助プログラム(go-digital)

HITACHI
Inspire the Next

- go-digital資金調達プログラムは、「デジタル化戦略」、「ITセキュリティ」、「デジタルビジネスプロセス」、「データリテラシー」、「デジタル市場開発」という5つのモジュールに関して、認定コンサルティング会社によるコンサルティング及び実装サービスの最大50%を助成する。

支援対象

- 以下を満たす企業
  - 従業員数が100人未満
  - 年間売上高または前年度の年間貸借対照表合計が2,000万ユーロ以下
  - ドイツの恒久的施設または支店

支援モジュール

- 「デジタル化戦略」、「ITセキュリティ」、「デジタルビジネスプロセス」、「データリテラシー」、「デジタル市場開発」の5つのモジュールからなり、認定コンサルティング会社によるターゲットを絞ったコンサルティング及び実装サービスを提供

ITセキュリティに関する具体的な支援内容

- ITセキュリティに役立つすべてのコンサルティング及び実装が、資金提供の対象となる。
- 「ITセキュリティ」モジュールの目的は、中小企業や熟練した貿易業者に、ITセキュリティレベルとデータ保護を向上させる方法について適格なアドバイスを提供することである。このモジュールで中小企業に助言する際には一般的な保護目標を達成するための措置を運用手順とビジネスプロセスに統合する必要がある。これは、既存または新たに計画されたデジタル対策/運用ICTインフラストラクチャのリスクとセキュリティ分析(脅威と潜在的な脆弱性の評価)の後に行われる。
- コンサルティング・サービスには、1日あたりの最大コンサルティング料1,100ユーロ(税別)の50%が助成される。資金提供額の上限は16,500ユーロ。

[参考] Förderprogramm "go-digital"
https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html
Häufig gestellte Fragen zum Förderprogramm "go-digital"
https://www.bmwk.de/Redaktion/DE/FAQ/go-digital/faq-go-digital.html

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/資金援助プログラム(go-digital)

- 補助金を利用したい企業は地域に適したコンサルタント、当該コンサルタント(企業)の詳細、連絡先、サービス範囲に関する背景情報をオンラインですばやく検索できる。
- マップは継続的に更新され、補足される。

ベルリン周辺に所在する認定コンサルタントの分布

01 Digital Age GmbH
Königswinterer Straße 286 , 53227 Bonn

1A! DIGITAL GmbH
Heidplätzchen 1 A , 51789 Lindlar

3 Plus Solutions GmbH & Co. KG
Auf Häpelt 17 , 66822 Lebach

3iMedia GmbH
Johann-Georg-Schlosser-Straße 14 , 76149 Karlsruhe

4RAUM.DIE AGENTUR GbR
Schillerstraße 23 , 78713 Schramberg

7 Hills Neo GmbH
Rüdesheimer Str. 12 , 53175 Bonn



[参考] interaktive Beraterlandkarte
https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/Karten/Beratersuche-go-digital/SiteGlobals/Forms/Formulare/beratersuche-go-digital-formular.html

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/資金援助プログラム(Digital Jetzt)

- Digital Jetztプログラムでは、モジュール1及びモジュール2内のITセキュリティへの投資に対する助成率を引き上げている。

支援モジュール

- モジュール1「デジタル技術への投資」：指定されたデジタル技術(主にサードパーティ・サービス)及び関連するプロセスや実装への投資を支援
- モジュール2「従業員の資格への投資」：従業員がデジタル技術に対応するための資格対策への投資を支援

ITセキュリティに関する具体的な支援内容

- モジュール1の最大資金枠は、企業規模(常勤換算従業員数)ごとに分けられる。
  - 従業員50人以下:最大50%
  - 従業員250人以下：最大45%
  - 従業員499人まで：最大40%
- モジュール2の最大資金枠は、企業規模(常勤換算従業員数)によって分類される。
  - 従業員50人以下：最大40%
  - 従業員250人以下：最大35%
  - 従業員499人以下：最大30%
- データ保護を含むITセキュリティに重点を置いた研修と技術への投資については、5%の追加補助が得られる。
- 個々の企業に対する資金提供の上限は5万ユーロだが、バリューチェーンやネットワークにおける複数企業による投資の場合は、申請者1人当たり10万ユーロに増額される。

[参考] „Digital Jetzt“– Förderung für die Digitalisierung des Mittelstands
https://www.bmwk.de/Redaktion/DE/Dossier/digital-jetzt.html
Publikation:Richtlinie zum Förderprogramm „Digital jetzt – Investitionsförderung für KMU“
https://www.bmwk.de/Redaktion/DE/Downloads/P-R/richtlinie-zum-foerderprogramm-digital-jetzt-investitionsfoerderung-kmu.pdf?__blob=publicationFile&v=1

© Hitachi, Ltd. 2024. All rights reserved.

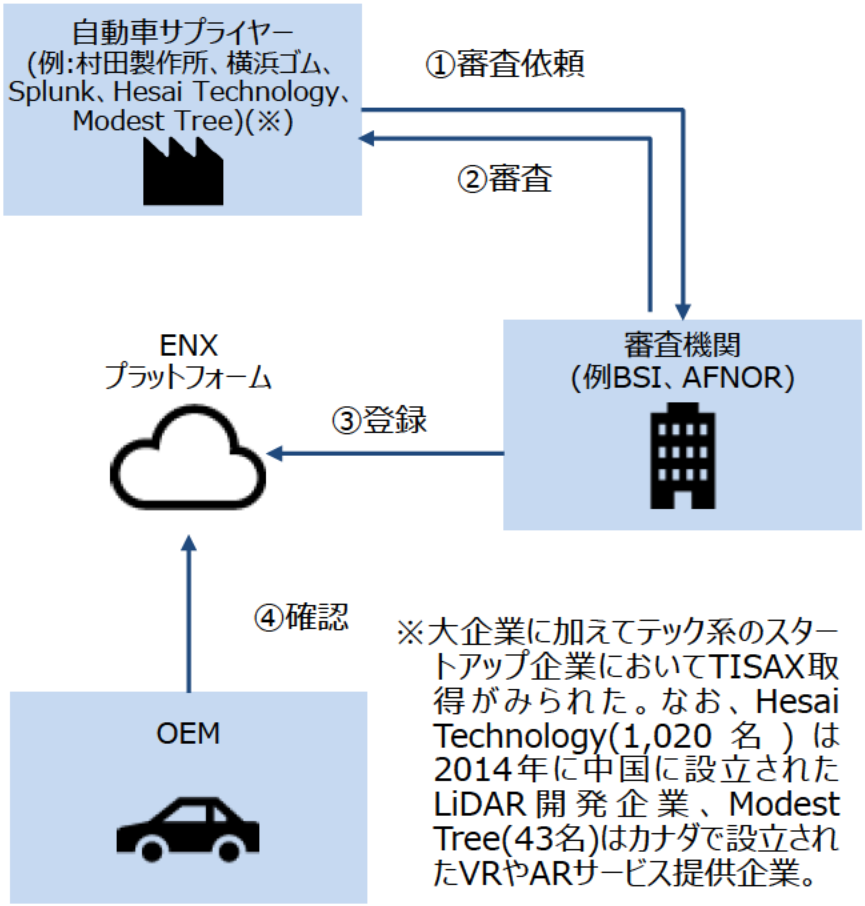
ドイツにおける取組み/ドイツ自動車工業会の取組み(1/3)

HITACHI
Inspire the Next

- ドイツ自動車工業会(VDA)が主体となり確立されたTISAX(Trusted Information Security Assessment Exchange)は自動車サプライヤーにおけるセキュリティ管理状況を審査する制度。

主体/取組みの概要 [TISAX(Trusted Information Security Assessment Exchange)]

実施主体	内容
実施主体	• VDA(ドイツ自動車工業会)によって確立 • European Network Exchange(ENX) Associationによって運用
対象	• OEMとの取引を希望し、情報セキュリティ管理水準を満たしていることを証明する必要のある企業(例:自動車部品サプライヤー)
開始時期	• 2016年開発 • 2017年運用開始
目的	• 自動車サプライチェーン全体の信頼を醸成するため ✓ 自動車業界において共通の情報セキュリティ評価と評価結果の共有 ✓ パートナー企業への機密情報の安全な共有を確実にするための共通の評価および交換メカニズムを提供
求められるセキュリティ基準	• ISO/IEC 27001等の規格に基づいて作成 • 自動車産業サプライチェーン特有の情報セキュリティの仮想的、物理的、社会的側面を包含
参加企業数	• 3,000社以上のTISAX参加企業(OEMおよびTISAX® 認定サプライヤー)



※大企業に加えてテック系のスタートアップ企業においてTISAX取得がみられた。なお、Hesai Technology(1,020 名) は2014年に中国に設立されたLiDAR 開 発 企 業 、Modest Tree(43名)はカナダで設立されたVRやARサービス提供企業。

[参考] ENX "TISAXについて"
https://portal.enx.com/en-US/TISAX/

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/ドイツ自動車工業会の取組み(2/3)

HITACHI
Inspire the Next

- 自動車サプライヤーによる自己評価結果に対する審査の有無や審査の内容によって、アセスメントが3段階に分かれる。

アセスメントレベル

審査機関
TISAX審査を実施できる機関は、ENX協会が契約した審査機関とされている。審査機関は自動車サプライヤーが自由に選択可能であるが、審査機関よりTISAX導入に係るコンサルティングを受けている場合には、かかる企業を審査機関として選択することはできない。

アセスメントレベル1 (AL1)
自動車サプライヤーは自己評価を行うが、審査機関は<u>その内容を確認しない。</u>

アセスメントレベル2 (AL2)
自動車サプライヤーは自己評価を行う。審査機関は<u>その内容を確認する。</u>

アセスメントレベル3 (AL3)
自動車サプライヤーは自己評価を行う。審査機関は<u>その内容を検証する。</u>

AL2では、審査機関は自動車サプライヤーが行った自己評価結果を検証せず、<u>証跡等の存在の有無について確認を行う。</u>
一方で、AL3では審査機関は自己評価結果やその証跡等が<u>主張通りのものであるかを検証する。</u>

[参考] ENX協会"TISAX参加企業のためのハンドブック"
https://www.enx.com/handbook/tph-jp.html

© Hitachi, Ltd. 2024. All rights reserved.

ドイツにおける取組み/ドイツ自動車工業会の取組み(3/3)

HITACHI Inspire the Next

- TISAXを取得していないことが自動車サプライヤーにとって不利に働くことやTISAX導入に係るコンサルティング企業費用が補助対象となることがTISAX普及の一因となっていると考えられる。

制度が普及した要因(例)

OEM調達要件への追加

- OEMの調達要件にTISAX取得が追加される場合があり、OEMとの取引を希望する企業にとって、TISAXを取得していないことがビジネス上不利になる可能性。

フォルクスワーゲン
(PwC「TISAX認証取得支援サービス」より)



- 新規取引時や自社とデータを交換する可能性がある場合には、取引先にTISAXの取得を義務付けている。

大手自動車
システムサプライヤー
(NEDO報告書(※1)より)



- 自動車業界では、TISAX取得企業のみを調達先とする傾向がある。
- TISAXを取得していないことから調達を回避した。

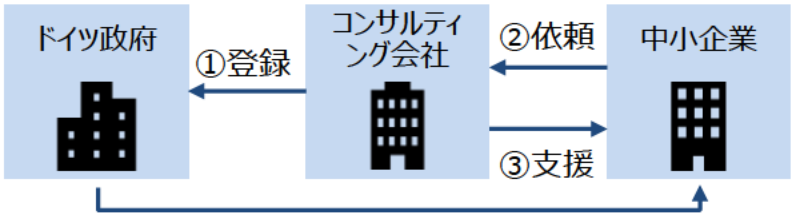
※1:NEDO「『サイバー・フィジカル・セキュリティ対策基盤』に関わる動向調査報告書」(2019年3月)

補助金の支給

- TISAX導入に係るコンサルティング費用が連邦経済・気候保護省(BMWK)が提供する中小企業を対象としたgo-digital資金援助プログラム(ITセキュリティ)の対象(※2)となり、取得のハードルが下がった。

■go-digital資金援助プログラムの全体像

- 条件(例:従業員100人未満、前年度の年間売上2,000万ユーロ以下、ドイツ国内に支店等を有する)を満たす中小企業に対してTISAX導入に係るコンサルティング費用を補助



補助率50%、コンサルタント料金のうち、1日最大1,100ユーロ(最大30日間/6ヶ月あたり)の補助金を支給

※2:IPM AUTOMOTIVE GMBH「TISAX® FREIGABE」にて、プログラムの対象となる旨が説明。(https://www.ipma-group.com/wp-content/uploads/2020/12/IPMA_TISAX_12_2020_DE.pdf)

[参考] BMWK "Häufig gestellte Fragen zum Förderprogramm "go-digital""
https://www.bmwk.de/Redaktion/DE/FAQ/go-digital/faq-go-digital.html

© Hitachi, Ltd. 2024. All rights reserved.

韓国における取組み/韓国インターネット振興院(KISA)の取組み(1/2)

HITACHI
Inspire the Next

- 韓国インターネット振興院(KISA)が運営する地方情報保護支援センターは、中小企業を対象としてサイバーセキュリティに関するサポートを行っている。地方情報保護支援センターは一定の金額を負担し、全体の費用(上限あり)が支援センターの負担額が超える場合には、超過分を中小企業側が負担する。

主体/取組み内容

実施主体	取組み(例)
実施主体	地方情報保護支援センター ※韓国インターネット振興院(KISA)が運営。KISAは、国家行政機関である未来創造科学部配下の準政府機関 ※クラウドベースのセキュリティサービス支援も併せて実施
場所	全国10か所
対象	中小企業 (募集企業数は600) ※募集期間:2022/5/2～10/31
費用	コンサルティング費:550万ウォン(約60万円)＋セキュリティソリューション費:660万ウォン(約73万円) ※コンサルティング費のうち500万ウォン、セキュリティソリューション費のうち540万ウォンは政府が負担し、超過分は企業が負担する。
支援企業	セキュリティ関連企業8社(F1セキュリティ/セキュリティハブ/A3セキュリティ/CAS/シードジェネレーション/FIN SECURITY/ソマンサ/L&Jテック)

プロセス

1	**応募・選考**	• 応募受付・対象者の選定(コンサルティング、セキュリティソリューションのどちらか一方だけを選択不可)
2	**コンサルティングの実施**	• セキュリティ関連企業による情報セキュリティコンサルティング ※詳細は確認できなかったが、現状調査の意味で使用されていると思料
3	**結果報告**	• セキュリティ関連企業はコンサルティング結果を報告し、中小企業へアクションプランを提案
4	**セキュリティソリューションマッチング**	• セキュリティ関連企業によるセキュリティソリューションの選定・導入
5	**フォローアップ**	• セキュリティ関連企業による実施点検・満足度調査 ※使用有無確認のため、セキュリティ関連企業は接続記録等の確認が可能

[参考] KISA"정보보호 컨설팅 지원사업 소개"
https://risc.kisa.or.kr/consulting/consultingIntro.do

© Hitachi, Ltd. 2024. All rights reserved.

韓国における取組み/韓国インターネット振興院(KISA)の取組み(2/2)

HITACHI
Inspire the Next

- セキュリティソリューションには、サイバーセキュリティお助け隊サービスで提供されていない分野(情報流出防止、パスワード/認証、バックアップ環境の構築等)でのソリューションが含まれている。
- ただし、サイバー保険や相談窓口、かけつけサービスは提供されていない。

セキュリティソリューション(セキュリティサービスを含む)提供分野

分野(※1) ※赤字下線はお助け隊サービスにて提供されているサービスを示す		機能	[参考] お助け隊サービスとの比較(※2)
ネットワーク	ファイアウォール(ネットワークファイアウォール、UTMなど)、侵入防止システム(IPS)/DDoS遮断システム、VPN、ネットワークアクセス制御、無線ネットワークセキュリティなど	企業ネットワークに認可されていない変更、破壊からネットワーク上の情報を保護	○ (お助け隊にて一部提供あり)
システム（端末）	マルウェア/ランサムウェア対応、スパム遮断ソリューション、APT対応、エンドポイント検知及び対応(EDR)など	許可のないユーザーファイル、フォルダ、機器などの使用制限	○ (お助け隊にて一部提供あり)
情報流出防止	DBセキュリティ/DBパスワード、セキュリティUSB、デジタル著作権管理(DRM)、DLP(ネットワークDLP、端末DLPなど)など	デジタルコンテンツの違法コピー及び流通防止、内部機密情報の漏洩検知及びブロック	- (お助け隊での提供がない可能性)
パスワード/認証	公開鍵基盤構造(PKI)、次世代認証(FIDO、DID、IDoT)など	情報アクセス者の資格や内容の検証手段の提供	- (お助け隊での提供がない可能性)
セキュリティ管理(バックアップ等)	脆弱性分析システム、バックアップ/復旧管理システムなど	非認可アクセスからネットワーク、システム、アプリケーションサービスの保護	- (お助け隊での提供がない可能性)

※1 提供されれている52の製品は韓国のベンダから提供されている。なお、「カリフォルニア情報技術株式会社」は韓国の企業として判断。(2023/1/16時点)
※2 本事業では、お助け隊サービスにて提供されているサイバー保険や相談窓口、かけつけサービス等は提供されていない。

[参考] KISA"정보보호 컨설팅 지원사업 소개"
https://risc.kisa.or.kr/consulting/consultingIntro.do

© Hitachi, Ltd. 2024. All rights reserved.

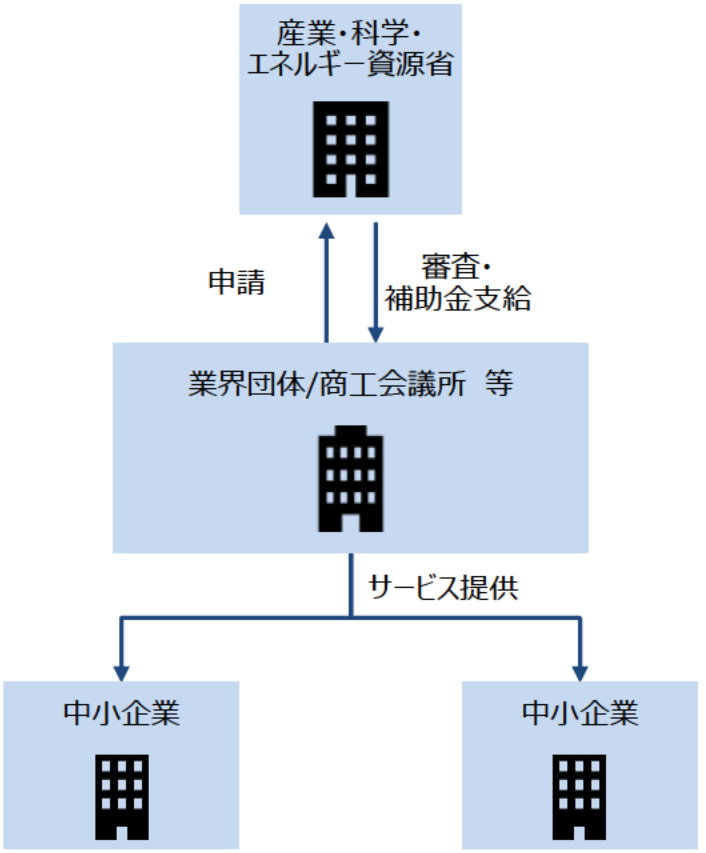
豪州における取組み/豪産業・科学・エネルギー資源省の取組み(1/3)

HITACHI
Inspire the Next

- 豪州では、Cyber Security Connect and Protect Programが実施され、中小企業にサービスを提供する商工会議所や業界団体等(希望団体のみ)に対して補助金が提供された。

主体/取組みの概要 [Cyber Security Connect and Protect Program]

実施主体	内容
実施主体	• 産業・科学・エネルギー資源省
実施時期	• 2020/10/26募集開始(2020/11/30募集締切)
目的	• 信頼できるアドバイザーを通じて、中小企業のサイバーセキュリティリスクに対する意識を高める。 • サイバーセキュリティリスクに対処するための中小企業の行動を促進させる。 • サイバーセキュリティの知識と能力の移転を含め、中小企業のサイバーセキュリティ能力を向上させる。
補助対象団体	• 中小企業にビジネスアドバイザリーサービスを提供する信頼できる組織(例:商工会議所、業界団体)
補助対象となる支出	• PJ活動のために直接雇用された人員の給与と人件費 • 外注費 • PJに直接関係する専門スタッフの採用または契約に関する費用 • PJに直接関係するコンピューター機器およびソフトウェアの購入 • ワークショップ、専門能力開発、ネットワーキング・イベント・フォーラム、およびコースの開発・実施費用(主要参加者の旅費を含む) • PJ等を実施するために必要な宿泊費および交通費(国内エコノミー旅行) • PJ支出の独立監査の費用
補助金額	• 総額830万豪ドル(1社あたり10万豪ドル～75万豪ドル)



サイバーセキュリティ戦略2020にて、中小企業におけるリソース不足、専門知識不足が指摘され、中小企業にサービスを提供する商工会議所等を対象としたCyber Security Connect and Protect Programの実施が明記された。

[参考] business.gov.au “Funding for business advisors to improve cyber security awareness and capabilities of SMEs”
https://businesschamberqld.com.au/membership/business-ready-qassure/

© Hitachi, Ltd. 2024. All rights reserved.

豪州における取組み/豪産業・科学・エネルギー資源省の取組み(2/3)

HITACHI
Inspire the Next

- 評価基準を踏まえて、中小企業における意識や能力を向上させるために実施する内容を申請者は提示する必要がある。また、補助期間終了後もプロジェクトを維持させるための戦略を提示する必要がある。

評価基準と申請者が提示すべき内容

評価基準	申請者が提示すべき内容
評価基準1 プロジェクトが中小企業のサイバーセキュリティをどのように改善するか。(50点)	a. プロジェクトが多様なニーズにどのように対応するかを含め、幅広い中小企業への能力と知識の移転を通じて、どのようにサイバーセキュリティに対する意識を高め、能力を向上させるか。 b. 申請者のアプローチにより、中小企業がサイバーセキュリティリスクに対処するための直接的な行動をどのように起こすか。 c. 直接または中小企業アドバイザーを通じて、現在の会員や顧客ベース以外の中小企業も含め、プロジェクトが対象とする中小企業の数。 d. 補助金期間終了後もプロジェクトの成果を維持するための戦略。
評価基準2 プロジェクトを遂行するための能力、キャパシティ、リソースを有するか。(25点)	a. 類似プロジェクトの管理実績と、管理職や技術職を含む適切なスキルと経験を持つ人材。 b. 業界、サイバーセキュリティ団体、その他の専門家とのパートナーシップをどのように活用し、中小企業のニーズを満たすようにするか 。 c. スコープ、実施計画、時間、予算、リスクに対応するプロジェクト管理計画。
評価基準3 助成金がプロジェクトにどのような影響を与えるか。(25点)	a. プロジェクトの規模および意図する成果に関して、要求される資金額がどのように正当化されるか 。 b. 補助金がなければプロジェクトが進行しなかった可能性を説明すること。助成金がプロジェクトにどのようなプラスの影響を与えるかを説明すること。

[参考] business.gov.au “Funding for business advisors to improve cyber security awareness and capabilities of SMEs”
https://businesschamberqld.com.au/membership/business-ready-qassure/

© Hitachi, Ltd. 2024. All rights reserved.

豪州における取組み/豪産業・科学・エネルギー資源省の取組み(3/3)

HITACHI
Inspire the Next

- 業界団体や大学を含め計14団体が採択され、1団体あたり10万豪ドル～75万豪ドルが提供された。

採択団体とプロジェクト名

採択団体(※)	プロジェクト名	補助額
IT Connexion Pty Ltd	サイバーセキュリティ意識向上トレーニング	25万豪ドル
Murray Hume Business Enterprise Centre Limited	企業向けサイバーセキュア	75万豪ドル
Loyal I.T. Solutions Pty. Ltd.	サイバー・セキュア・セントラル・コースト	45万6,258豪ドル
Hunter Business Centre Ltd	地域中小企業のためのサイバーセキュリティ文化プログラム	34万9,040豪ドル
Queensland Chamber Of Commerce And Industry Limited	CCIQAssure (サイバーセキュリティ認定プログラム)	73万8,500豪ドル 次頁にて紹介
Cybercx Pty Ltd	中小企業向けCyber123	75万豪ドル
Caravan Industry Association Of Australia Limited	オーストラリアのキャラバンおよびキャンピング業界におけるサイバー意識向上トレーニング	36万4,500豪ドル
Western Sydney University	オズ・サイバーセキュリティ・エイド・センター OCAC	74万5,920豪ドル
The Project Lab Pty Ltd	中小企業向けのサイバーアップ	64万1,434豪ドル
Business Enterprise Centre (Darwin Region) Incorporated	サイバーセーフ	21万9,596豪ドル
Real World Technology Solutions Pty Ltd	中小企業、慈善団体、先住民ビジネスにおけるサイバーセキュリティレジリエンス	75万豪ドル
First Focus IT Pty Limited	中小企業の経営幹部向けのサイバーセキュリティ教育パッケージを開発・提供	33万9,780豪ドル
Concept Data Pty Ltd	SAビジネスサイバーセキュリティアドバイザリーサービス	18万8,721豪ドル
Belmont Business Enterprise Centre Inc	MYビジネス・インキュベーター ©CYBER SECURITY トレーニング＆メンタリング・プロジェクト	27万4,900豪ドル

※Pty Ltdとは非公開株式有限責任会社を示し、日本における非上場の株式会社に近いとされている。

[参考] business.gov.au “Cyber Security Business Connect and Protect Successful applicants”
https://business.gov.au/grants-and-programs/cyber-security-business-connect-and-protect/grants-recipients

© Hitachi, Ltd. 2024. All rights reserved.

豪州における取組み/豪クイーンズランド商工会議所の取組み

- クイーンズランド商工会議所は支給された補助金によって、既存のプログラムの拡大を検討。既存のプログラムに対して新たにセキュリティに関する資格認定を追加することで、セキュリティに取り組む中小企業におけるビジネスチャンスが拡大する可能性があるとしている。(具体的な内容は今後明らかになる可能性)

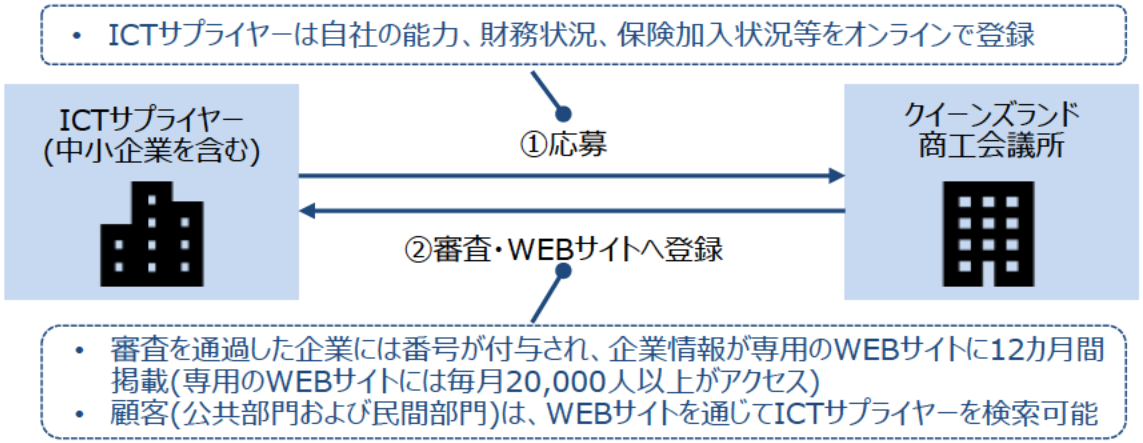
新たに開発予定

<具体的な内容(例:提供される監査、要件)は今後明らかになる可能性>

- オンライン・プログラム、トレーニング・イベント、一般的なサイバー・セキュリティ・リスクに対する認識を高めるための監査等を中小企業へ提供予定。
- 中小企業が大規模な供給契約を確保できるよう既存のプログラムに、サイバー・セキュリティの資格認定を追加予定。

既存のプログラム[QAssure]

- クイーンズランド商工会議所によって開発および管理されており、ICTサプライヤー(中小企業を含む)と、そのサービスを求める公共および民間部門の組織を結び付けることを目的とされる。プログラムに参加するために、中小企業は少なくとも年間432豪ドルを支払う必要。



V

セキュリティへの取組みが認められた中小企業のビジネスチャンスが拡大することで、中小企業全体のセキュリティへのモチベーションが向上する可能性

[参考] business.gov.au “Funding for business advisors to improve cyber security awareness and capabilities of SMEs”
https://businesschamberqld.com.au/membership/business-ready-qassure/
Business Chamber Queensland” Business Chamber Queensland”
https://businesschamberqld.com.au/membership/business-ready-qassure/

© Hitachi, Ltd. 2024. All rights reserved.

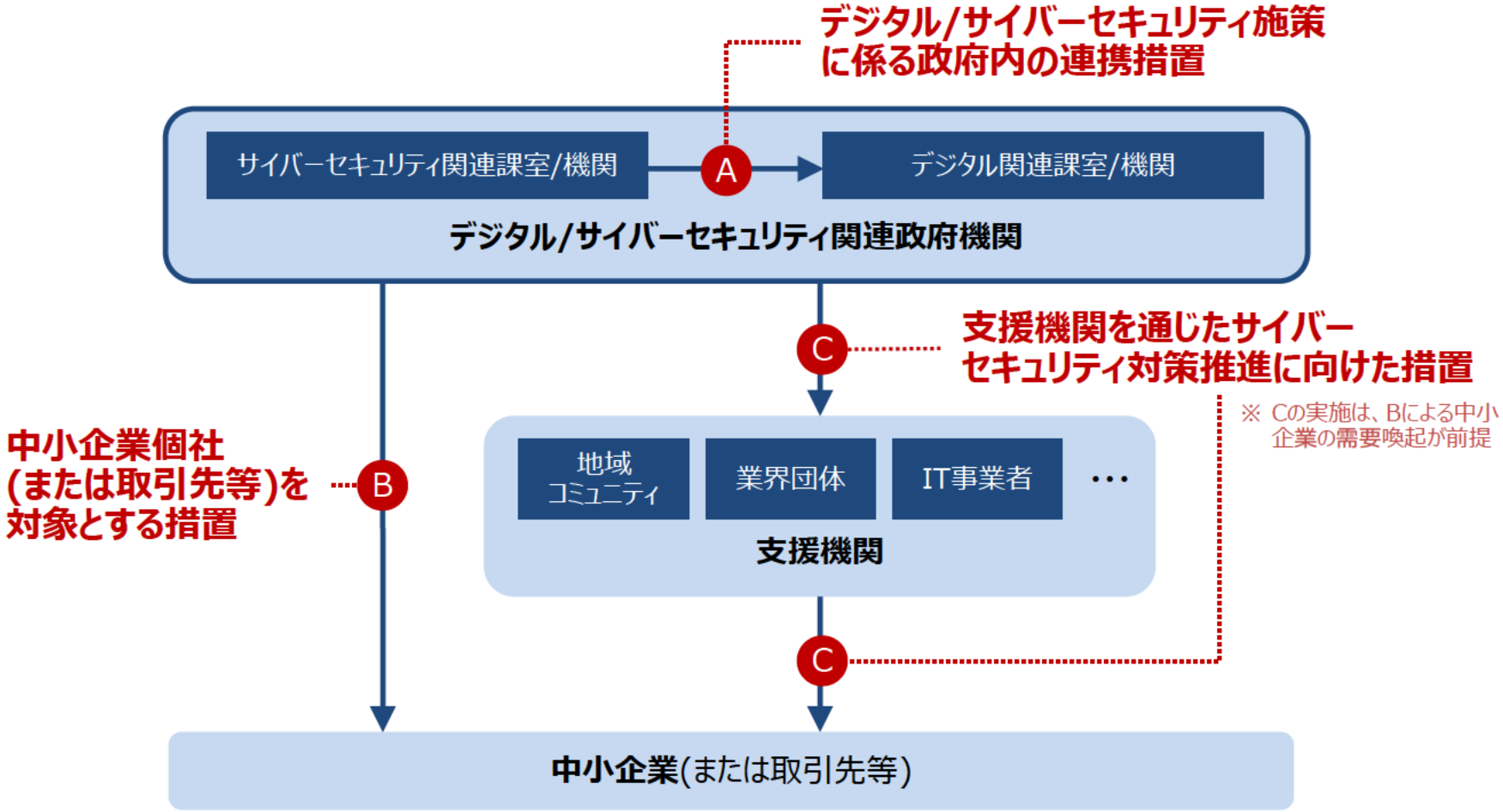
HITACHI
Inspire the Next

3-3. 中小企業を対象としたガイドライン等の普及・啓発に資する施策

© Hitachi, Ltd. 2024. All rights reserved.

普及・啓発に資する施策の類型

- 普及・啓発に資する政府施策を、主体間の関係性という観点から以下の3類型に分類した。
  - A) デジタル/サイバーセキュリティ施策に係る政府内の連携措置
  - B) 中小企業個社(または取引先等)を対象とする措置
  - C) 支援機関を通じたサイバーセキュリティ対策推進に向けた措置

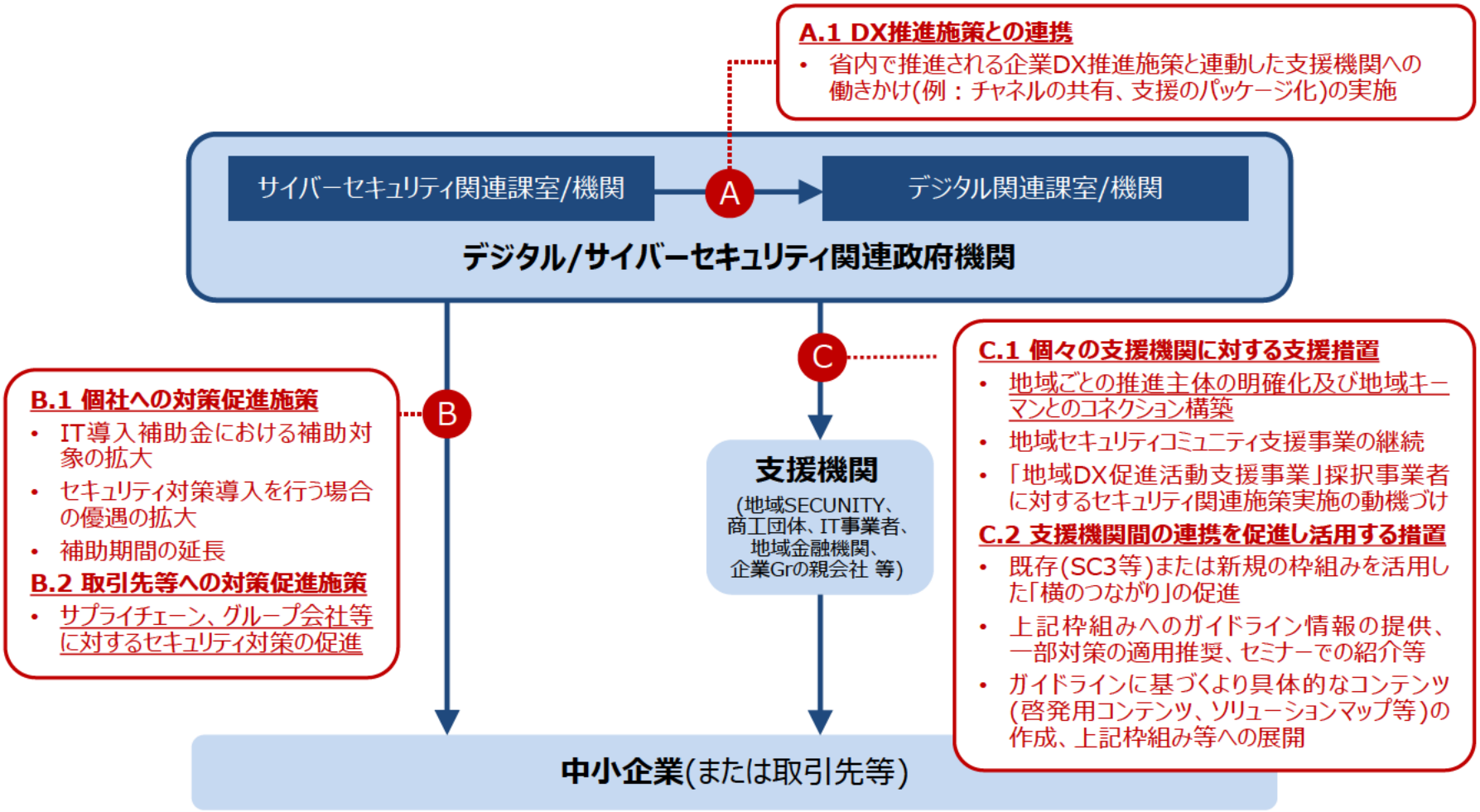


© Hitachi, Ltd. 2024. All rights reserved.

普及・啓発に資する施策のマッピング

HITACHI
Inspire the Next

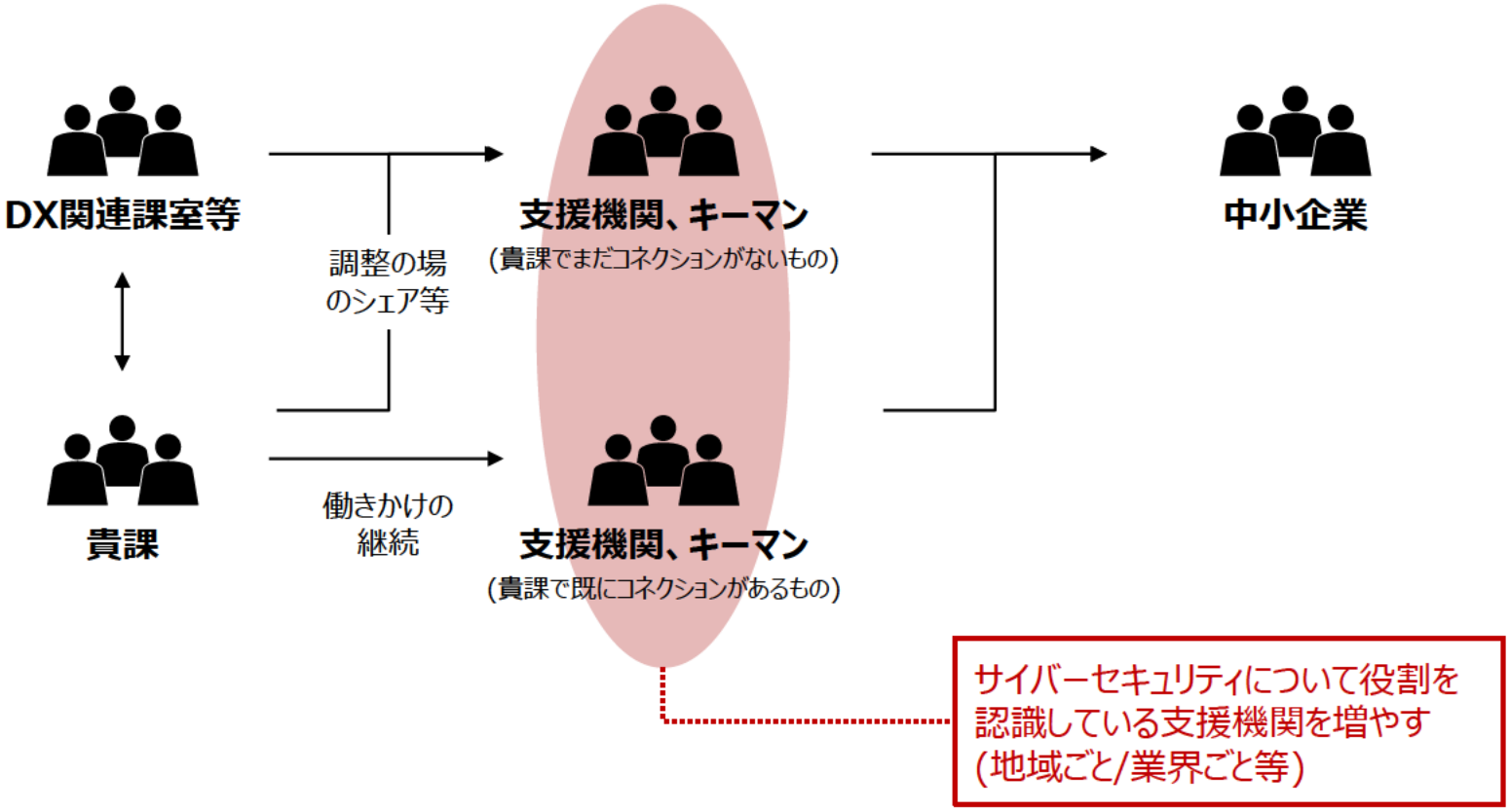
- 施策類型A~Cのそれぞれについて、課題に基づく施策例を検討した。
  - A) デジタル/サイバーセキュリティ施策に係る政府内の連携措置：DX推進施策との連携
  - B) 中小企業個社(または取引先等)を対象とする措置：個社への対策促進施策、取引先等への対策促進施策
  - C) 支援機関を通じた対策推進に向けた措置：個々の支援機関に対する支援措置、支援機関間の連携を促進し活用する措置



© Hitachi, Ltd. 2024. All rights reserved.

A.1 デジタル/サイバーセキュリティ施策に係る政府内の連携措置

- 政府内におけるDX関連課室等との連携を通じて、サイバーセキュリティについて役割を認識している支援機関や協力関係を結ぶことのできるキーマンを増やすことが望ましい。
- キーマンの特定や働きかけの実施にあたっては、非デジタル関係部局との連携も有効と想定される。
- また、展開するガイドラインについても、複数あると中小企業にとっては取捨選択が難しくなるため、ベースラインとなるものに一本化することが望ましい。



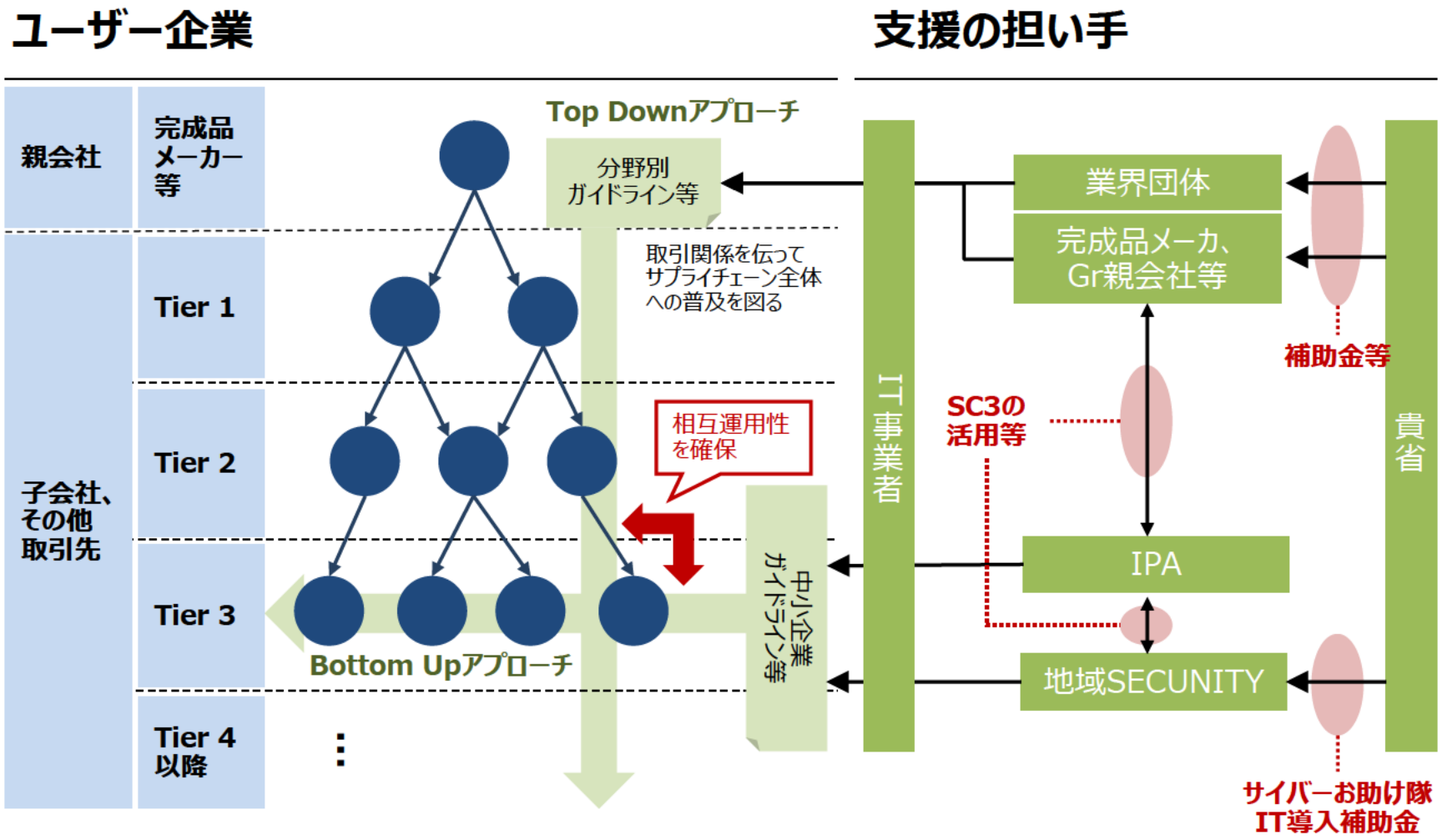
[参考] 第6回 支援機関を通じた中堅・中小企業等のDX支援の在り方に関する検討会
https://www.meti.go.jp/shingikai/mono_info_service/dx_support/pdf/006_03_00.pdf

© Hitachi, Ltd. 2024. All rights reserved.

B. 中小企業個社または取引先等を対象とする措置/アプローチ(案)

HITACHI
Inspire the Next

- Top Downアプローチとして業界団体や完成品メーカ・Gr親会社等、Bottom Upアプローチとして地域SECUNITYや中小企業個社への支援を通じて、中小企業のセキュリティ水準向上を図ってはどうか。



© Hitachi, Ltd. 2024. All rights reserved.

B.1 中小企業個社を対象とする措置/補助金制度の改善(1/2)

HITACHI
Inspire the Next

- 「サイバーセキュリティお助け隊」に限定されている利用可能範囲について、ライフサイクル全体を対象としつつ、他の製品/サービス分類も含めるよう拡張することに加え、セキュリティ対策導入時の補助率向上等のインセンティブ付与を通じてDX with Cybersecurityの更なる推進を図ってはどうか。

メインツールと組み合わせて、**オプションとして「サイバーセキュリティお助け隊サービス」**を申請可能。

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠		デジタル化基盤導入枠				セキュリティ対策推進枠
	A類型	B類型	デジタル化基盤導入類型			複数社連携IT導入類型	
補助額	5万円～150万円未満	150万円～450万円以下	会計・受発注・決済・ECソフト：50万円	会計・受発注・決済・ECソフト：50万円超～	PC・タブレット等：～10 / レジ・券売機等：～20	(1)デジタル化基盤導入類型の対象経費（左記同様） (2)消費動向等分析経費（上記(1)以外の経費） ※1 50万円×参画事業者数 補助上限：(1)+(2)で3,000万円 事務費・専門家費 補助上限：200万円	5万円～100万円
補助						)デジタル化基盤導入類型と同様 (2)・(3) 2/3以内	1／2以内
補助対象経費	クラウド利用料（最大２年分）、導入関連費		ハードウェア購入費				「サイバーセキュリティお助け隊」利用料（最大2年分）
	オプションとして「サイバーセキュリティお助け隊」を申請した場合、利用料1年分（「サイバーセキュリティお助け隊」導入は加点要素）						

1. 利用可能な製品・サービス範囲の拡大
   (例：サイバーセキュリティお助け隊サービスの拡充)
2. IPA自社診断結果に基づく製品・サービスの導入
3. セキュリティ対策導入時の補助率向上(例：5~10%UP)

- **DX with Cybersecurityの更なる推進**
- **自社のリスクプロファイルに応じたより広範な製品/サービスの導入**

[出典] 第9回 産業サイバーセキュリティ研究会 ワーキンググループ2（経営・人材・国際）資料3
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/009_03_00.pdf

© Hitachi, Ltd. 2024. All rights reserved.

B.1 中小企業個社を対象とする措置/補助金制度の改善(2/2)

HITACHI
Inspire the Next

- 製品・サービス範囲の拡大範囲として、例えば、各中小企業にてIPA自社診断を実施のうえ、より多くの項目で求められている類型を制度に組込むこととしてはどうか。
(例：一般従業員向け教育・リテラシー教育、ポリシー管理・設定管理、入退室管理システム、
コンサルティング(現状分析、ポリシー策定等)、個人認証用デバイス及びその認証システム、訓練(演習)等)

製品・サービス類型	登場数	製品・サービス類型	登場数
一般従業員向け教育・リテラシー教育	7	DLP（情報漏えい対策）	2
ポリシー管理・設定管理	6	端末接続制御(ネットワーク検疫)	
入退室管理システム	5	ネットワーク脆弱性診断	
コンサルティング(現状分析、ポリシー策定等)	4	バックアップ製品	
個人認証用デバイス及びその認証システム		個人認証用生体認証デバイス及びその認証システム	
訓練（演習）		アクセス許可・シングルサインオン（SSO）	
アイデンティティ・アクセス管理製品	3	インテリジェンス情報提供	1
暗号化		セキュリティ人材向け教育	
ウイルス対策	2	外部接続デバイス制御	
EDR		記憶媒体の廃棄装置	
ファイアウォール		ログ管理	
UTM		IT資産管理	
セキュアウェブゲートウェイ		データ管理（復旧・削除・検索）	
メール・セキュリティ対策		インシデント対応・フォレンジック	

[出典] IPA「新・5分でできる！情報セキュリティ自社診断」の対策で製品を探す
https://sg.jnsa.org/topic/60/

© Hitachi, Ltd. 2024. All rights reserved.

B.2 取引先、Gr親会社等を対象とする措置

HITACHI
Inspire the Next

- 「グループ・ガバナンス・システムに関する実務指針(グループガイドライン)」への追記や「サプライチェーン全体のサイバーセキュリティ向上のための 取引先とのパートナーシップの構築に向けて」公表などは既に行われているところ、独占禁止法や下請け法に抵触するリスクや金銭的障壁の軽減が必要ではないか。

独占禁止法または下請法上問題となる行為

取引の対価の一方的決定	• 取引上の地位が相手方に優越している事業者が、サイバーセキュリティ対策の要請を行い、対策の実施によって取引の相手方に生じるコスト上昇分を考慮することなく、一方的に著しく低い対価を定める場合には、独占禁止法上問題となる。
セキュリティ対策費の負担の要請	• 取引上の地位が相手方に優越している事業者が、対策費などの名目で金銭の負担を要請し、当該セキュリティ対策費の負担額及びその算出根拠等について取引の相手方との間で明確になっておらず、取引の相手方にあらかじめ計算できない不利益を与えることとなる場合や、取引の相手方が得る直接の利益等を勘案して合理的であると認められる範囲を超えた負担となり、取引の相手方に不利益を与えることとなる場合には、独占禁止法上問題となる。
購入・利用強制	• 取引上の地位が相手方に優越している事業者が、対策の実施の要請に際して、合理的な必要性がないにもかかわらず、自己の指定する商品の購入や役務の利用を強制する場合には、独占禁止法上問題となる。 • 例えば、取引の相手方が、対策実施の要請を受け、新たなサービスを利用する必要がないにもかかわらず、自己の指定する事業者が提供するより高価なセキュリティサービスを利用することを要請し、利用させることは、独占禁止法上問題となる。

懸念緩和に向けた措置(例)

<発注元企業が行うべき措置>

- 積極的に価格の交渉の機会を設け、取引の相手方と十分に協議を行い、サイバーセキュリティ対策の内容や費用負担の在り方を決定する。

<上記を支援する政策的措置(例)>

- サイバーセキュリティ対策の内容や費用負担に関する目安の明確化
- 要請される対策の実施にかかる発注元、発注先双方によるコスト負担の支援
(例：補助金の支出)

[出典] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて
https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

© Hitachi, Ltd. 2024. All rights reserved.

C.1 支援機関を通じた措置/個別機関の支援・連携の促進

- 個別の支援機関の取組みを促進、喚起するため、まずは目標を明確化した上で、現状の取組みを評価し、改善及び取組み状況のシェア等に向けた施策を講じる必要がある。
- 取組みが進んでいない業界・地域に対し、セキュリティ有識者・セキュリティ事業者団体が伴走して進めることも考えられる。

繰り返し実施

	1 目指す目標の明確化	2 現状の評価	3 改善施策の推進
課題	• 地域や業界等の軸で、当該領域において望まれる普及・啓発の取組みの目標を定義する。 • 団体による活動の内容等の視点に加え、普及の度合い等の成果(結果)の観点も含める。	• ①で規定したレベルに対して各地域または業界等の取組みがどの程度なされているかを評価する。	• 現状の評価に基づき、必要な施策を講じる。(予算的な支援を含む) • 取組み状況(優れているものだけでなく、幅広く実施)については、SC3等の横断的なコミュニティで適時報告する。
取組み例	• 優先地域・業界の特定 • 地域、業界ごとの推進主体の明確化 • 地域、業界ごとの普及、活動目標の設定	• 地域コミュニティや業界団体等に対するアンケート及びヒアリング調査 • 上記調査の結果に基づく評価の実施	• 地域キーマンの特定、アプローチの検討 • 働きかけの実施 • 横断的なコミュニティの組成、取組み状況の報告 • 優れた団体等の表彰等、アメにあたる施策の実施

© Hitachi, Ltd. 2024. All rights reserved.

C.2 支援機関間の連携を促進し活用する措置(1/2)

HITACHI
Inspire the Next

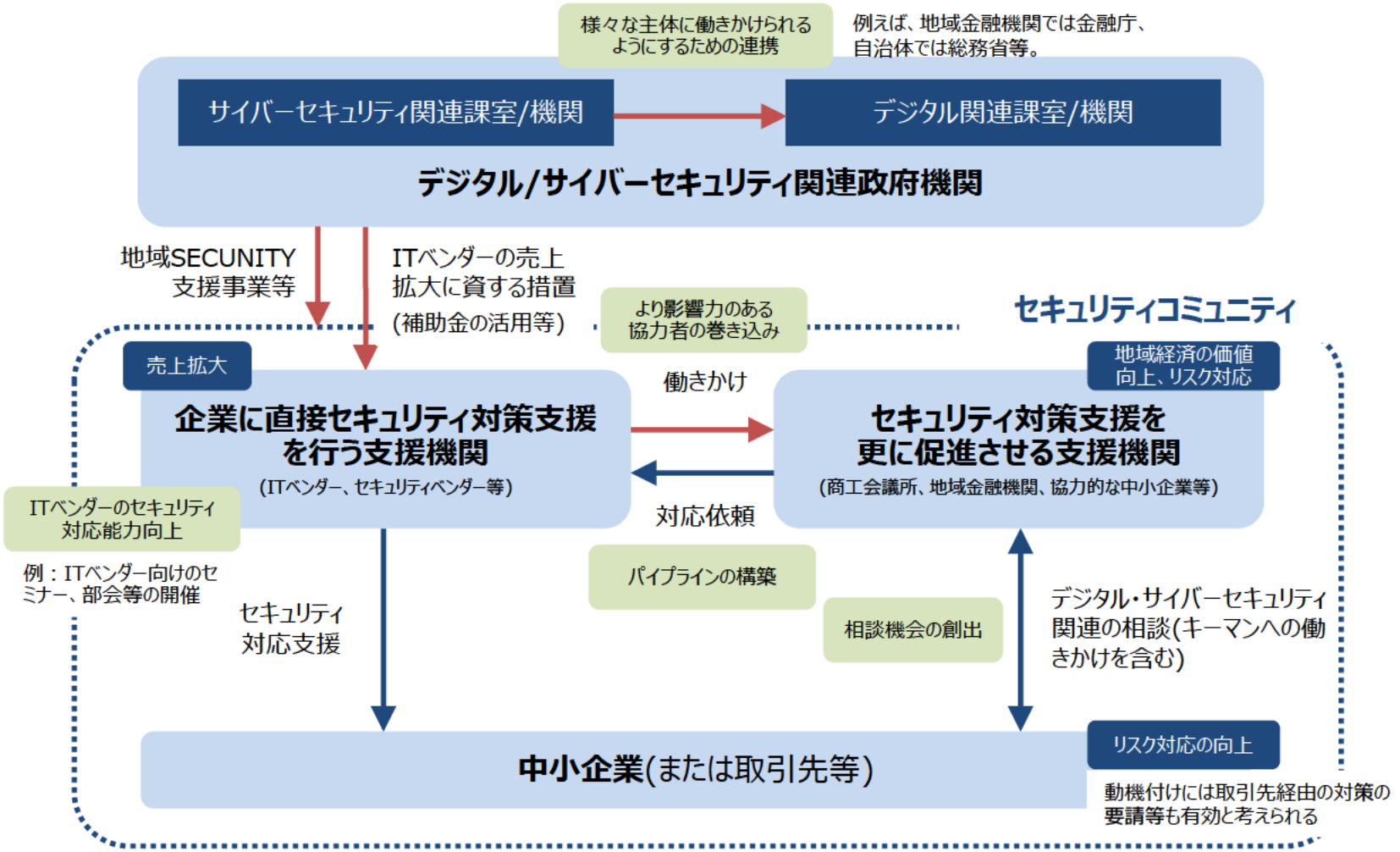
- これまで性質の異なる様々な機関を「支援機関」と一括りにしてきたが、より粒度の高い施策を検討する上ではさらなる分類を行ったうえで現状と課題の整理を行うことが適当。

類型	定義	具体的な機関(例)	中小支援における現状(仮説含む)
企業に直接セキュリティ対策支援を行う支援機関	• 普段から、企業と物理的に近い距離で活動し、地域の中堅・中小企業等にDX・サイバーセキュリティ関連の支援を提供する	ITベンダー	• これまでの実績から、地域の中小企業と直接チャネルを構築している • セキュリティに関する関心や知見が必ずしも高いとは言えない
		セキュリティベンダー	• 一部の例外を除いて、中小企業とは直接チャネルが構築できていない • 対策支援に必要な技術的能力を有する
セキュリティ対策支援を更に促進させる支援機関	• 地域のプラットフォームやハブ機能等として活動する存在や、地域の支援機関と協働する • ある特定の専門的知見・ノウハウを以て、上記機関と協働する	商工会議所	• これまでの実績から、地域の中小企業と直接チャネルを構築しており、経営支援や補助金の申請支援等を実施している • セキュリティ対策支援に特化した人員は基本的に擁していない
		地域金融機関	• これまでの実績から、地域の中小企業と直接チャネルを構築している • 一部の例外を除いて、サイバーセキュリティ対策を目的とした支援体制が十分に確立されているわけではない
		業界団体	• 所掌業界であれば中小企業とのチャネルを有しているケースがある • サイバーセキュリティ対策を目的とした支援体制が十分に確立されているかは団体により異なる
		協力的な中小企業	• 一部に存在し、他の企業に大きな影響力を有するケースもある。

© Hitachi, Ltd. 2024. All rights reserved.

C.2 支援機関間の連携を促進し活用する措置(2/2)

- 中小企業に対する動機付けを通じたニーズの掘り起こしと並行して、「中小企業の情報セキュリティ普及推進協議会」等の既存体制も活用しつつ支援機関間の連携を高めてリーチできる中小企業の幅を広げ、地域ITベンダー等の支援機関としての対応能力の向上を図っていくことが望ましい。



© Hitachi, Ltd. 2024. All rights reserved.


HITACHI
Inspire the Next

HITACHI
Inspire the Next

別紙３　IPAの機能強化に向けた国内外動向の調査

© Hitachi, Ltd. 2024. All rights reserved.

目次

1. 日米のサイバーセキュリティ政策推進体制の全体像 …… 2
2. 標準化機関の組織・機能面に関する日米比較 …… 5
3. 標準化機関等から発行される文書体系等の日米比較 …… 29
4. 日本における標準化に係る機関等のあるべき姿の検討 …… 49

© Hitachi, Ltd. 2024. All rights reserved.

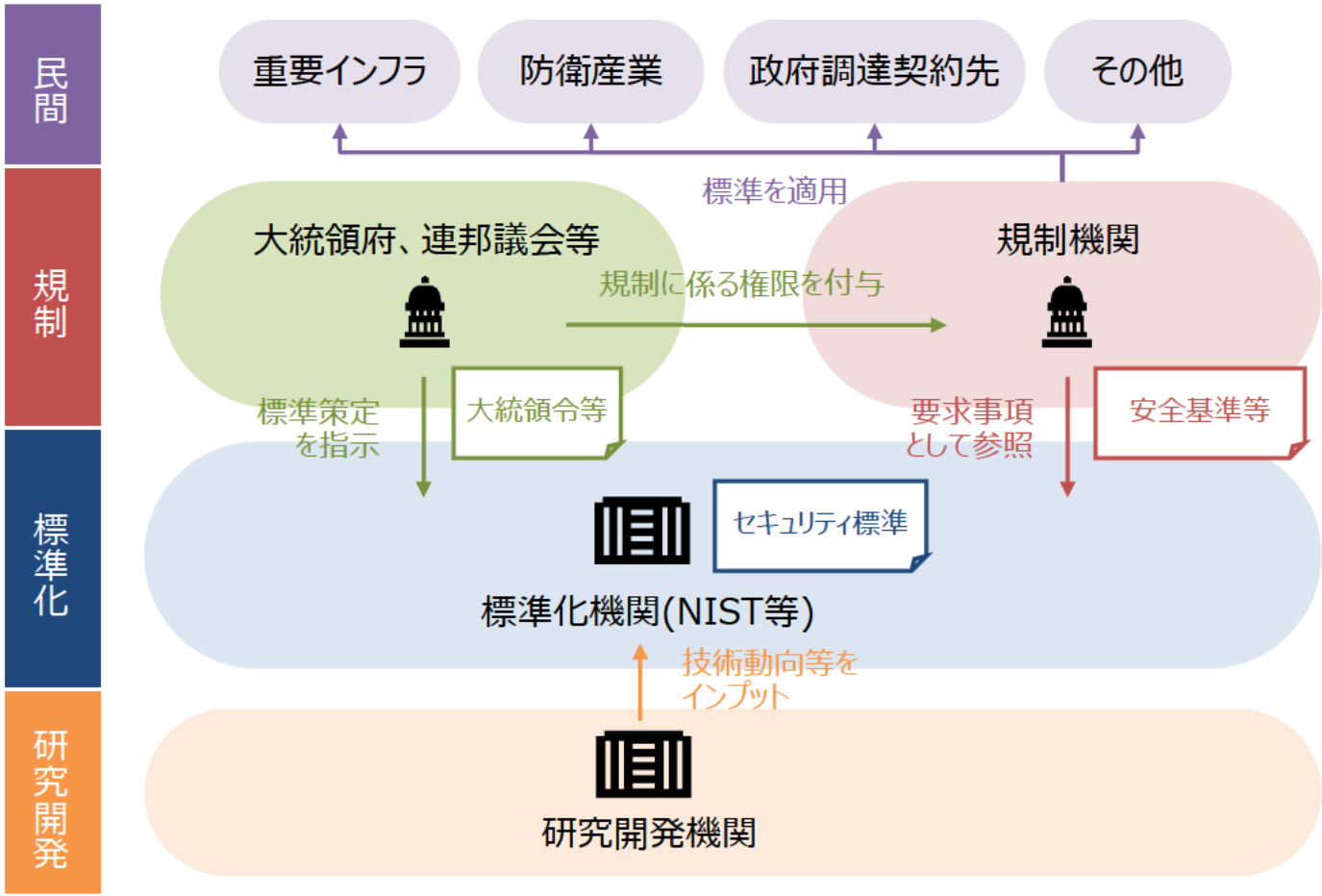
HITACHI
Inspire the Next

1. 日米のサイバーセキュリティ政策推進体制の全体像

© Hitachi, Ltd. 2024. All rights reserved.

1-1. 米国政府における機能間の関係性

- 米国立標準技術研究所(NIST)が策定した標準は、規制機関による引用を通じて、重要インフラ、防衛産業、政府調達等で適用されている。
- その他、サイバーセキュリティ・インフラセキュリティ庁(CISA)や国防総省(DoD)にて策定が行われている。

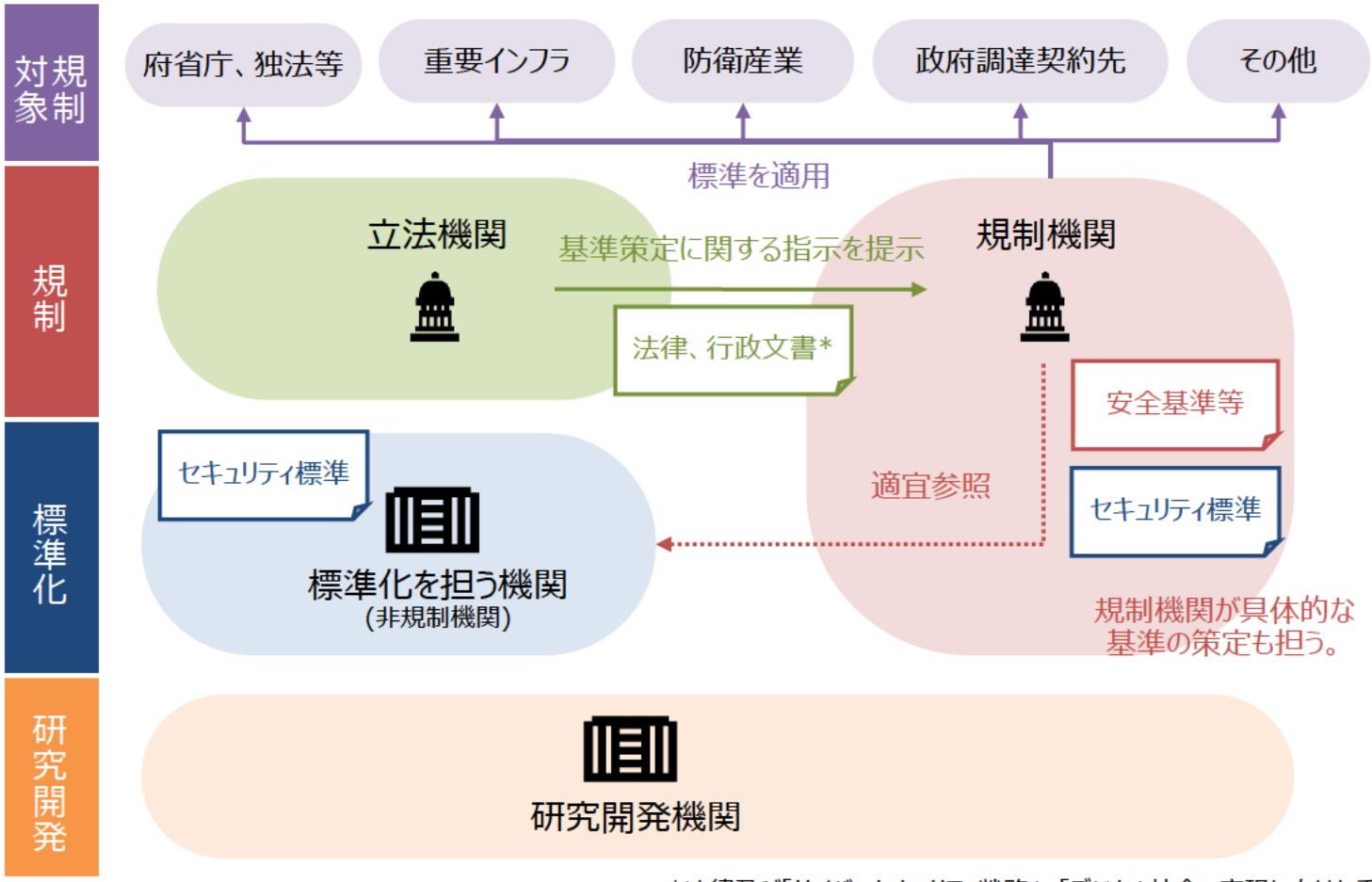


[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

© Hitachi, Ltd. 2024. All rights reserved.

1-2. 日本政府における機能間の関係性

- 日本では、規制機関たる防衛省や内閣官房(NISC)、総務省等が自ら基準を策定し、適用している。
- 規制機関による経済産業省や情報処理推進機構(IPA)で定めるボランタリーなガイドラインへの参照は限られている。



*法律及び「サイバーセキュリティ戦略」、「デジタル社会の実現に向けた重点計画」等の閣議決定文書、所定の権限を有する審議会の答申等を含む

[凡例] 標準の策定を指示する機関等　標準を策定する機関等
標準の利用を強制等する機関等　研究開発を行う機関等　民間事業者等

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2. 標準化機関の組織・機能面に関する日米比較

© Hitachi, Ltd. 2024. All rights reserved.

2-1. 組織編成と役割 / 基礎情報 (1/2)

HITACHI
Inspire the Next

- 情報処理推進機構(IPA)の機能強化に向けて、米国NISTや日本の産業技術総合研究所(AIST)を比較対象として調査を行った。

項目		日本 IPA	日本 AIST	米国 NIST
設立年度		2004年1月 (1970年～2004年は情報処理振興事業協会)	2001年4月 (1952年～2001年は工業技術院)	1901年1月 (1901年～1988年は国立標準局)
団体の位置づけ		独立行政法人	国立研究開発法人	米国商務省の所管組織
組織編成	**セキュリティの標準開発に関連する部署**	• **デジタル基盤センター** • **セキュリティセンター**	• **研究推進関連部署**(研究戦略企画部/**研究センター(7つの領域)**/TIA推進センター/量子・AI融合技術ビジネス開発グローバル研究センター/地域センター)	• **情報技術研究所**(応用計算数学部/**応用サイバーセキュリティ部**/**コンピュータセキュリティ部**/情報アクセス部/ソフトウェア・システム部/統計エンジアリング部)
	上記以外の部署	• デザインアーキテクチャ・デザインセンター • デジタル人材センター • 産業サイバーセキュリティセンター	• 組織運営関連部署(運営統括企画部/総務本部/ブランディング・広報部/イノベーション人材部/環境安全本部/セキュリティ情報化・推進部/つくばセンター) • 社会実装推進関連部署(㈱AIST Solutions) • 企画本部	• 通信技術研究所 • エンジアリング研究所 • 情報技術研究所 • 材料測定研究所 • 物理測定研究所 • NIST中性子センター • ナノスケール科学技術センター

© Hitachi, Ltd. 2024. All rights reserved.

2-1. 組織編成と役割 / 基礎情報 (1/2)

HITACHI
Inspire the Next

- 連邦情報処理規格(FIPS)や特別刊行物(SP)、省庁間報告(IR)を公表しているNISTのコンピュータセキュリティ部及び応用サイバーセキュリティ部に対応すると考えられる国内機関の部署として以下を想定した。
  - ✓ IPA:セキュリティセンター、デジタル基盤センター
  - ✓ AIST:サイバーフィジカルセキュリティ研究センター

セキュリティの規格開発に関連する部署

分類		部署	役割	主な成果物(例)
日本	IPA (※1)	セキュリティセンター	サイバー攻撃に関する情報の収集・分析・提供、情報セキュリティ対策の調査・分析と普及啓発、ITセキュリティ評価・認証制度の運営、暗号技術調査・評価、制御システムのマネジメントシステム適合性評価スキーム確立の支援を担う。	<セキュリティセンター> • サイバーセキュリティ経営ガイドライン • 中小企業の情報セキュリティ対策ガイドライン • 自動車の情報セキュリティへの取組みガイド
		デジタル基盤センター	データスペースの実現に向けた取組み、ソフトウェア開発手法の検討、DX推進に向けた取組み、未踏事業に伴う人材発掘・育成を担う。	<デジタル基盤センター> • つながる世界の開発指針
	AIST	サイバーフィジカルセキュリティ研究センター(※2)	社会が現在実際に直面しているセキュリティ課題に対し、それらを理論に裏打ちされた形で解決する技術(例:高機能暗号、ハードウェアセキュリティ、ソフトウェアアナリティクス)を研究開発する。	• ホワイトペーパー「サプライチェーンにおける信頼構築に向けて • 機械学習品質マネジメントガイドライン • 人工物メトリクスを用いた個体管理技術ガイダンス
米国	NIST	コンピュータセキュリティ部	米国の情報(システム)を保護するための標準、ガイドライン、仕組み、ツール、指標、実践を提供するために必要な研究、開発、アウトリーチ活動を行う	• Federal Information Processing Standards(FIPS) • Special Publications(SP) • Interagency or Internal Reports(IR)
		応用サイバーセキュリティ部	標準及びベストプラクティスのアウトリーチ活動や効率的な適用を行うことで実践的なサイバーセキュリティ/プライバシー政策を実行する。	

※1:2023/7/1の組織改編に伴いページを更新中であるため、内容が変わり得る。
※2:7つの領域のうち、情報人間工学領域の研究センターの1つ。

© Hitachi, Ltd. 2024. All rights reserved.

2-1. 組織編成と役割 / 予算・人員の規模

HITACHI
Inspire the Next

- IPAとAISTにおける全体の予算額及び人員数はNISTに及ばない。
- また、IPAにおける標準策定に携わる部署に在籍する人数はNISTより少なくなると見込まれる。

分類		予算	人員
日本	**IPA**	**167億円**(2022年度予算額)※1	**412人**※2 非常勤職員を除く
	AIST	**966億円**(2022年度予算額) ※3	**2916人**※4 非常勤職員を除く うち、サイバーフィジカルセキュリティ研究センター45人(2023/8時点、客員研究員、協力研究員、招聘研究員を除く)※5
米国	**NIST**	**14.7億ドル**(2022年度予算要求額)※6 [参考]1,911億円(1ドル=130円)	**約3400人**※7 うち、応用サイバーセキュリティ部及びコンピュータセキュリティ部の合計:235人(2023/8時点、NCCoEを除く)※8

注:管見の限り、セキュリティセンターとデジタル基盤センターの在籍人数は確認できなかった。
P11の組織編成を考慮すると、NISTの応用セキュリティ部及びコンピュータセキュリティ部の合計より少ないと考えられる。
[算定根拠]412人÷5部署(※9) ×2部署(セキュリティセンター、デジタル基盤センター)=165人

※1:IPA「令和4事業年度財務諸表 添付書類」決算報告書 法人合計 参照(https://www.ipa.go.jp/about/t6hhco000000iiqb-att/02tennpusiryou.pdf)
※2:IPA「令和4事業年度財務諸表」役員及び職員の給与の明細 参照(https://www.ipa.go.jp/about/t6hhco000000iipp-att/01zaihyou.pdf)
※3:AIST「財務諸表等 令和4年度」令和4年度決算報告書 参照(https://www.aist.go.jp/pdf/aist_j/zaimu/r4kakutei.pdf)
※4:AIST「財務諸表等 令和4年度」役員及び職員の給与の明細 参照(https://www.aist.go.jp/pdf/aist_j/zaimu/r4kakutei.pdf)
※5:サイバーフィジカルセキュリティ研究センター 研究員一覧から算出(https://www.cpsec.aist.go.jp/center/member.html)
※6:NIST "FY 2022: Presidential Budget Request Summary"(https://www.nist.gov/director/congressional-and-legislative-affairs/nist-appropriations-summary-1/fy-2022-presidential)
※7:米国検査院 "National Institute of Standards and Technology:Improved Workforce Planning Needed to Address Recruitment and Retention Challenges"(https://www.gao.gov/products/gao-23-105521#:~:text=The%20National%20Institute%20of%20Standards%20and%20Technology%20(NIST)%20has%20a,and%20technical%20(S%26T)%20staff.)
※8:NIST" Computer Security Division Staff"(https://www.nist.gov/staff/division/6021) "Applied Cybersecurity Division Staff" (https://www.nist.gov/staff/division/258356)より算出
※9:デジタルアーキテクチャセキュリティセンターデザインセンター、セキュリティセンター、社会基盤センター、IT人材育成センター、産業サイバーセキュリティセンターの計5部署

© Hitachi, Ltd. 2024. All rights reserved.

2-1. 組織編成と役割 / セキュリティ標準に係る取組みの概要

HITACHI
Inspire the Next

- NISTが策定するセキュリティ標準策定は法律的な要請に基づくものであり、他の規制において参照されているのに対して、IPAやAISTが策定するセキュリティ標準は必ずしも法律的な位置づけがなされておらず、必ずしも業法その他の規制要件と結び付けられていない。

分類		セキュリティ標準に係る取組みの内容	成果物(例)	
日本	IPA	• 「国家の安全保障／経済安全保障の確保への貢献」において、制御システムに係るリスク評価手法の浸透に向けて**制御システムのセキュリティリスク分析ガイド**や 中小企業のサイバーセキュリティ対策強化に向けた支援の強化として、**中小企業の情報セキュリティガイドライン**等を策定 • 「「誰も取り残さない」サイバーセキュリティの確保と各主体の自主的なセキュリティの取組を支えるインフラの提供」において、**サイバーセキュリティ経営ガイドラインの策定・更新やプラクティス集**を策定 • 「人材育成の推進とサイバー技術の活用促進」において、**TLS暗号設定ガイドライン等**を作成・更新	• サイバーセキュリティ経営ガイドライン • 中小企業の情報セキュリティ対策ガイドライン • 制御システムのセキュリティリスク分析ガイド • TLS暗号設定ガイドライン	セキュリティ標準を策定している一方で、法律的な位置づけはなされておらず、必ずしも規制に結び付いていない。
	AIST	• 以下の研究開発を行いつつ、**個別にホワイトペーパーやガイドライン**を策定 ➢ デジタルツイン技術、予測・計画・最適化技術、その結果に基づきフィジカル空間に働きかけるインタフェース技術を研究開発 ➢ サイバーフィジカルシステムのセキュリティ向上を目指したセキュリティ強化技術等を研究開発	• ホワイトペーパー「サプライチェーンにおける信頼構築に向けて • 機械学習品質マネジメントガイドライン • 人工物メトリクスを用いた個体管理技術ガイダンス	セキュリティ標準を策定している一方で、法律的な位置づけはなされていない。また研究開発分野と密接に関係。
米国	NIST	• 連邦情報セキュリティマネジメント法(FISMA)(2002年12月に制定) によって、連邦政府がFISMAに準拠するためにNISTが支援をすることを義務付けた。同法に従い、NISTは**FIPSやNIST SP 800シリーズ等**を策定。 • 作成した文書(例:SP800-171)は連邦政府の規制にて参照。	• FIPS • SP 800シリーズ(例:SP 800-53,SP800-171) • NIST IRシリーズ	策定したセキュリティ標準は法律的に位置づけられた上で、各省庁の規制において参照されている。

[参考] IPA「独立行政法人 情報処理推進機構 第五期中期計画」
(https://www.ipa.go.jp/about/disclosure/ps6vr7000000h6ln-att/5thplan.pdf)
国立研究開発法人産業技術総合研究所 中長期計画
(https://www.aist.go.jp/Portals/0/resource_images/aist_j/outline/middle_plan/chuchoukikeikaku5_rev4.pdf)
IPA「情報セキュリティ向上のための米国の取り組み」
(https://www.ipa.go.jp/security/reports/oversea/nist/fisma.html)

© Hitachi, Ltd. 2024. All rights reserved.

2-1. 組織編成と役割 / 小括

HITACHI
Inspire the Next

- NISTと同様、セキュリティ標準を策定する部署はIPAとAISTにおいてもみられる。
- 一方で、IPAやAISTにて策定されたセキュリティ標準には、法律的な位置づけがなされておらず必ずしも当該標準が規制等には結びついていない。
- また組織全体で比較した場合、IPA及びAISTに対して割り当てられている予算はNISTと比較して少ない。

比較項目	比較結果
組織編成と役割	• NIST(コンピューターセキュリティ部/応用サイバーセキュリティ部)と同様、**セキュリティ標準を策定する部署はIPA**(デジタル基盤センター/セキュリティセンター等)と**AIST**(サイバーフィジカルセキュリティ研究センター等)**においてもみられる。** • NIST法を通じてNIST(商務長官)標準策定に係る権限が割り当てられている一方で、IPAは「情報処理の促進に関する法律」に係る業務範囲の中で標準策定について言及されておらず、必ずしも権限が割り当てられているとは言えない。ただし、法律に記載されている業務等において必要な取組みとしてセキュリティ標準策定を行っている場合がある。(※1)
予算・人員の規模	• 組織単位で比較した場合、IPA及びAISTに対して割り当てられている**予算はNISTと比較して少ない**。(※2) • 部署単位で比較した場合、セキュリティ標準の策定に係る部署において**IPAの人員の数はNISTと同程度の可能性**がある。(※3)また、NISTの人員の内訳については、6割以上が科学エンジアリングスタッフであり、専門性の高い人員が割り当てられている。
取組みの概要	• **IPAやAISTで策定されているセキュリティ標準の数は、NISTと比較して少ない。**また、NISTのセキュリティ標準は体系的に整理されている一方で、**IPAやAISTの記載内容は必ずしも体系的に整理されているわけではない**。なお、詳しくは第三章にて詳述。 • また、NISTが策定しているセキュリティ標準(FIPSやSP 800シリーズ等)はは法律的な位置づけがなされており、各政府機関の規制において参照されている一方で、**IPAやAISTが策定したセキュリティ標準は必ずしも規制に結び付いていない**。

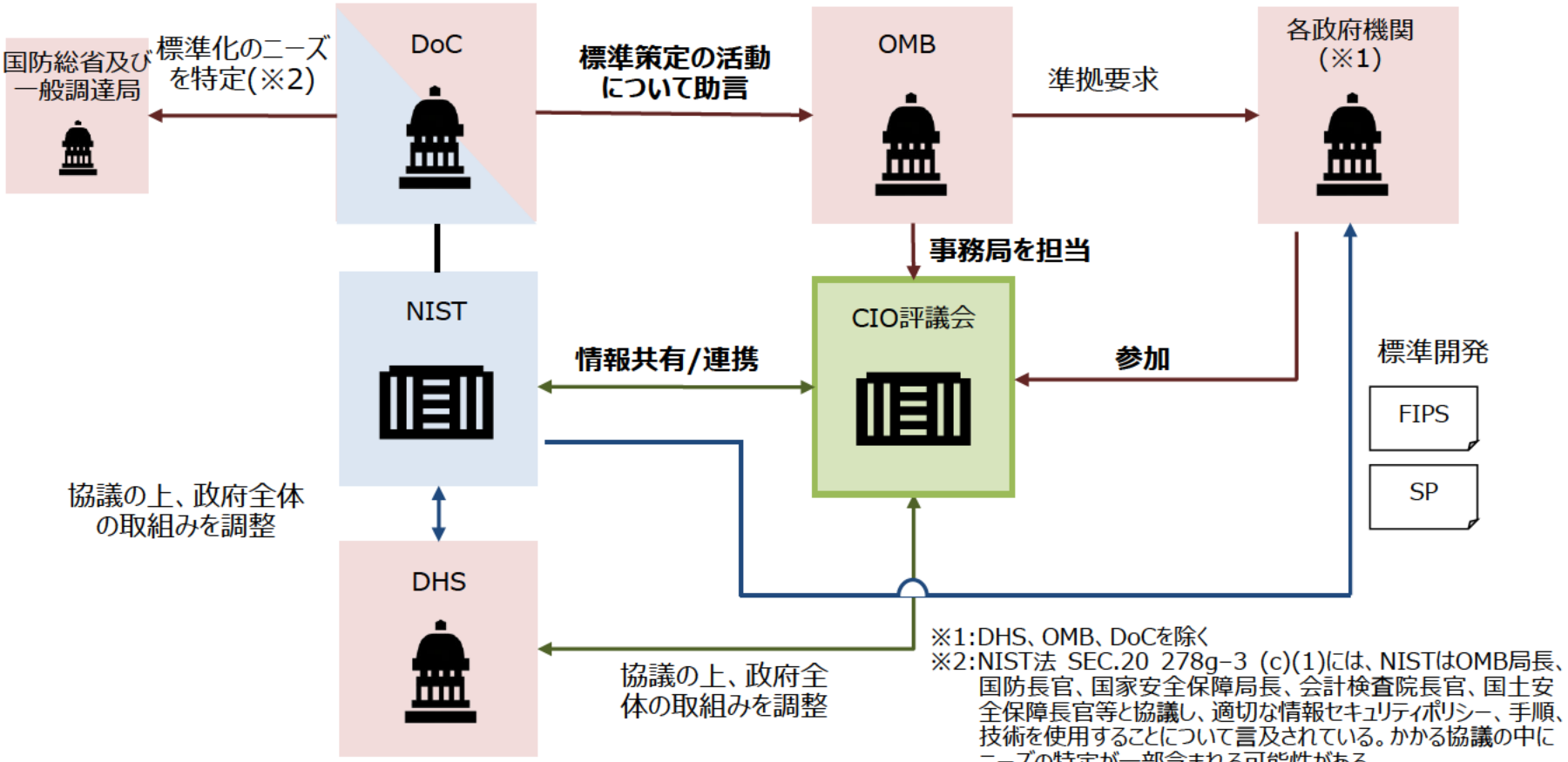
※1:「情報処理の促進に関する法律」第五十一条 (業務の範囲等)に記載がない場合であっても、例えば、セキュリティ標準の策定が含まれる場合がある点に留意いただきたい。例えば、「運用及び管理を行う者が異なる複数の情報処理システムの連携の仕組み並びに当該連携に係る運用及び管理の方法に関する調査研究並びにその成果の普及その他の当該連携を促進するために必要な取組を行うこと。」とされており、本業務の中でセキュリティ標準策定が含まれる可能性がある。
※2:現時点では、組織全体に割り当てられている予算額を比較。
※3:部署の人数計算は想定の数値である点にご留意いただきたい。

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 行政機関との関係性(米国)

HITACHI
Inspire the Next

- 行政管理予算局(OMB)が事務局を担当するCIO評議会が各政府機関やNISTと情報連携を行う。
  また、商務省(DoC)がOMBを通じて強いイニシアチブを発揮できる立場にある可能性。



[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

[参考] CIRCULAR NO. A-130 “Managing Information as a Strategic Resource”
(https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf)
U.S. Government Publishing Office“National Institute of Standards and Technology Act”
(https://www.govinfo.gov/app/details/COMPS-5388)

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 連邦最高情報責任者評議会(CIO Counsil) (1/2)

HITACHI
Inspire the Next

- 各関連機関の最高情報責任者等が参加する連邦最高情報責任者評議会(CIO評議会)は、標準やガイドラインを活用してIT標準に関する推奨事項を開発するため、適宜NISTと協力する。
- NISTIR7977に、NISTの標準開発においてCIO評議会及び委員会と連携する旨が記載。

NISTIR 7977

NISTIR 7977(NIST暗号標準とガイドラインの開発プロセス)にて、**NISTの標準開発においてCIO評議会及び委員会と連携する旨が記載されている。**

<抜粋(「5. 暗号コミュニティの参加」「連邦政府関係者」)>
連邦政府の最高情報責任者(CIO)評議会およびその委員会への参加は、NISTの暗号標準およびガイドラインに最も関心を持ち、その影響を受ける米国政府との直接的なつながりをNISTが確保するもう一つの方法である。

項目	内容
団体名	連邦最高情報責任者評議会 FEDERAL CHIEF INFORMATION OFFICERS COUNCIL(CIO Counsil:CIO評議会)
設立年度	1996年7月
説明	CIO評議会は、ITの設計や取得、開発、近代化、維持、使用、 共有、性能に関連する、**連邦政府の実務を改善するための省庁間フォーラム**。大統領令13011(連邦情報技術)に基づき設立、2002年電子政府法により成文化。
参加者	• 連邦最高情報セキュリティ責任者（CISO） • 情報規制庁(OIRA)長官 • **米国法典第31編第901条(b)(※)に記載されている各機関の最高情報責任者** • 情報機関の最高情報責任者 • 国土安全保障省の最高情報責任者 • 陸軍省、海軍省、空軍省の最高情報責任者（第3506条(a)(2)(B)に基づき最高情報責任者が指定されている場合） • 小規模代理店協議会代表2名 • CIO評議会が指定する米国のその他の役員または職員

[※] DoDやDoC、DHS等を含む24団体。詳細は(https://www.law.cornell.edu/uscode/text/31/901)参照

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 連邦最高情報責任者評議会(CIO Counsil) (2/2)

HITACHI
Inspire the Next

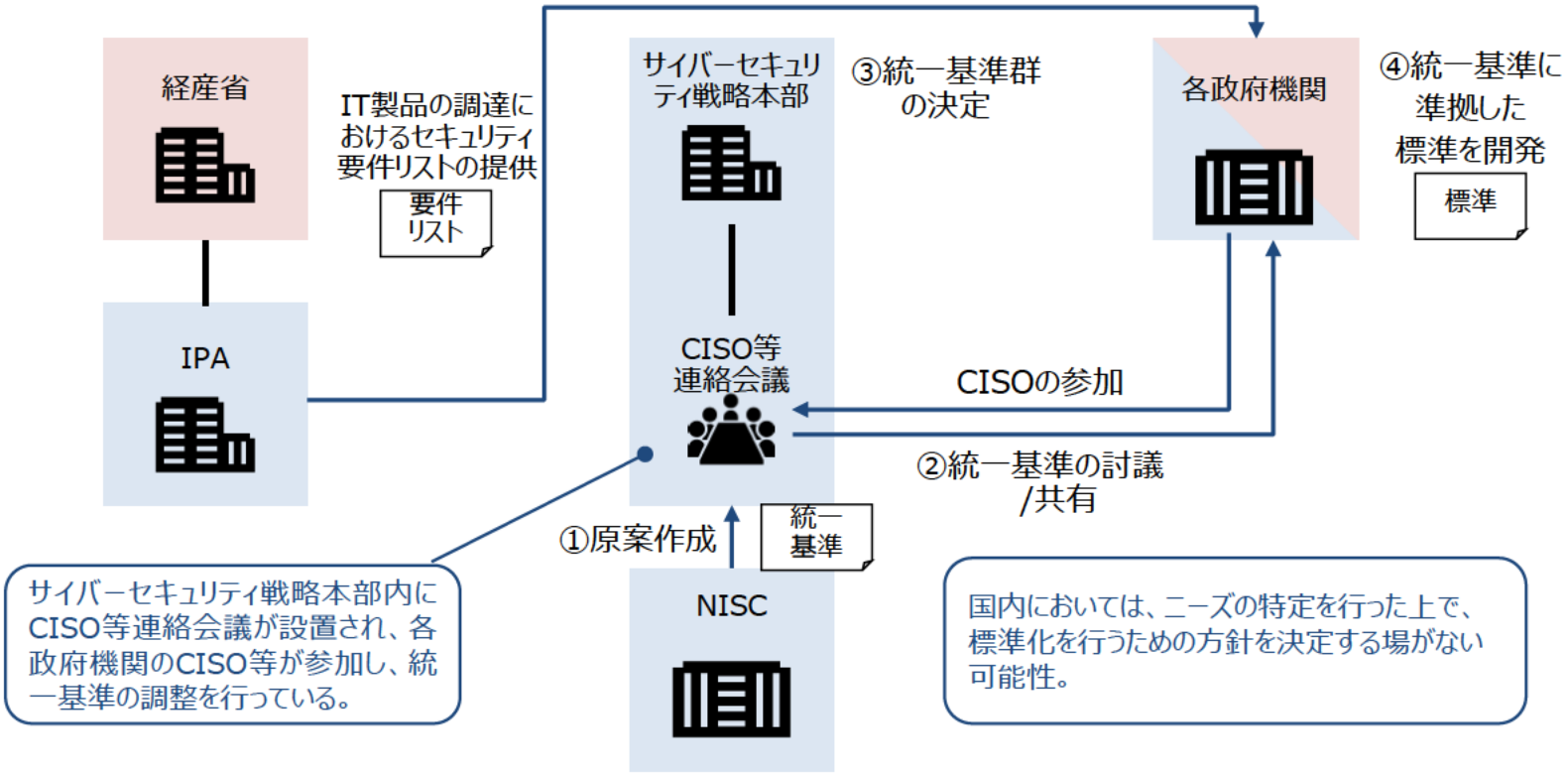
項目	内容
機能	1. 政府のIT管理ポリシーおよび要件について行政管理予算局(OMB)へ推奨を行う。 2. 情報技術とサイバーセキュリティ政策に関する政府全体の優先事項を定め、その実施を監視する。 3. ITマネジメントに関する教訓、アイデア、ベストプラクティス、革新的なアプローチを共有する。 4. 連邦CIOを支援し、ITの活用を通じて連邦政府のパフォーマンスを向上させるための複数省庁プロジェクトやその他の革新的イニシアチブの特定、開発、調整を行う。 5. ベストプラクティスの共有、知識の移転、連邦ITの課題に対処するための統一的なアプローチの開発を目的として、連邦政府機関のCIO間のコラボレーションとコミュニティ形成を促進する。 6. 第36章および2002年電子政府法のタイトルIIに基づき、各省庁による共通のIT管理パフォーマンス尺度の開発と使用を促進する。 7. 重複するIT投資を削減し、連邦政府内の省庁間でITリソースの効率的な利用を促進するため、省庁内ITポートフォリオ管理に関する協力の場としての役割を果たす。 **8. IT標準に関する推奨事項を策定するため、適宜NIST及びOMBと提携し、以下を活用して(商業)標準を最大限に利用する。** ✓ **相互接続性と相互運用性のための基準とガイドライン** ✓ **連邦政府の電子情報を分類し、技術の効率的な利用を可能にするための基準とガイドライン** ✓ **連邦政府のコンピュータ・システムの効率とセキュリティに関する基準とガイドライン** 9. 人事管理局と協力し、IT管理に関連する分野における連邦職員の雇用、訓練、分類、専門能力開発のニーズを評価し、対処する。 10. 米国アーキビストと協力し、連邦ITイニシアチブおよび活動によって連邦記録法がどのように効果的に対処できるかを評価する。 11. 連邦政府の最高財務責任者会議、連邦調達責任者会議、最高人事責任者会議、予算責任者諮問委員会、その他連邦政府内の主要グループ、産業界、学界、その他の連邦政府、部族政府、州政府、地方政府から、審議会の関心事項について適宜見解を求める。
委員会	• 実行委員会(The Executive Committee)にて、評議会の優先事項の設定、業務の監督と割り当て、評議会の業務成果と連邦IT構想との整合、評議会の運営と組織の管理、および審議会の意思決定機関としての役割を担う。実行委員会は月一開催。 • 評議会委員会(Council Committees)にて、特定の優先事項に焦点について議論。CISO会議(Chief Information Security Officer Council)、イノベーション委員会(Innovation Committee)、企業運営委員会(Enterprise Operations Committee)、ワークフォース委員会(Workforce Committee)からなる。

[参考] CIO Counsil"FEDERAL CHIEF INFORMATION OFFICERS COUNCIL CHARTER"
(https://www.cio.gov/assets/files/CIOC-Charter-Dec-2020.pdf)
NIST" NIST Cryptographic Standards and Guidelines Development Process"(NISTIR7977)
(https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 行政機関との関係性(日本)

- サイバーセキュリティ戦略本部内に設置され、各政府機関のCISO等が参加するサイバーセキュリティ対策推進会議(CISO等連絡会議)が統一基準の調整を実施。
- 他方、日本では広くニーズの特定を行い標準化の方針を決定する場が必ずしも設定されていない可能性。



[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

[参考]政府機関等のサイバーセキュリティ対策のための統一基準群（※）の概要）
(https://www.nisc.go.jp/pdf/policy/general/kijyungun-gaiyor5.pdf)
経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
(https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

[参考] CISO等連絡会議(概要)

HITACHI
Inspire the Next

- CISO等連絡会議にて、関係機関の最高情報セキュリティ責任者(CISO)等が情報連携を行いつつ、サイバーセキュリティ対策の推進を図っている。

分類	内容
目的	• 関係行政機関の最高情報セキュリティ責任者(CISO)等相互の緊密な連携の下、政府機関におけるサイバーセキュリティ対策の推進を図る
メンバー	• 推進会議は、議長、副議長、構成員及びオブザーバーをもって構成する。 • 議長は内閣官房副長官(事務)、副議長は内閣危機管理監及びデジタル監とする。 • 構成員及びオブザーバーは、本部長の指定する職にある関係機関の最高情報セキュリティ責任者(CISO)等とする。
組織	• 推進会議にサイバーセキュリティ対策推進専任審議官等会議(以下「専任審議官等会議」という。)を置く。専任審議官等会議は、関係機関の職員で議長の指定する職にある者によって構成する。 • 専任審議官等会議にサイバーセキュリティ対策推進会議幹事会(以下「幹事会」という。)を置く。幹事会は、関係機関の職員で議長の指定する職にある者によって構成する。

[参考]NISCサイバーセキュリティ対策推進会議等について
(https://www.nisc.go.jp/pdf/council/cs/taisaku-konkyo.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 調整方法の日米比較

HITACHI
Inspire the Next

- 日本では、広くニーズの特定を行った上で標準化を行うための方針を決定する場がない可能性。
- また、CISO等連絡会議ではIPAや他省庁が策定した標準に対する議論は行っていないため、議論を行う場がなく、団体間の調整を行うことができていない標準が存在する可能性。

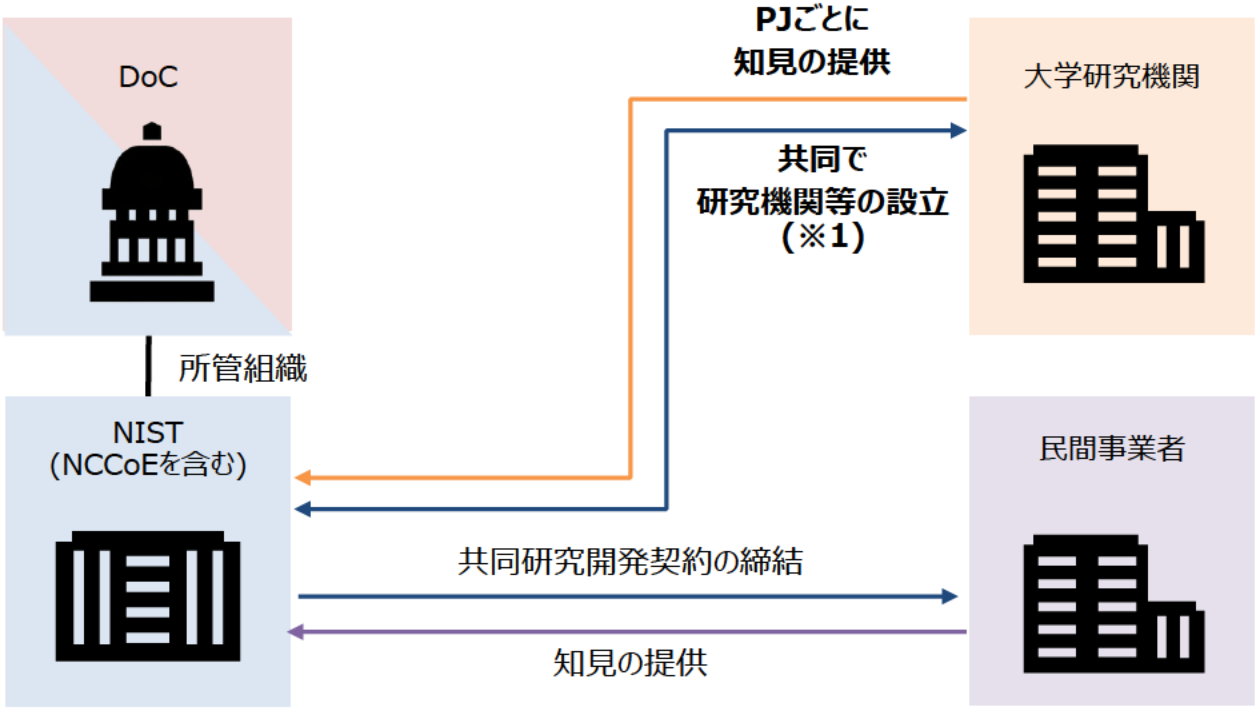
観点		米国	日本	考察
調整に用いられる場(where)		• CIO協議会	• サイバーセキュリティ戦略本部(CISO等連絡会議等を含む)	• 策定する標準について各関係省庁間で情報共有やレビュー等を行う場が存在する点で、米国と日本は共通する。 • 日本においては広くニーズの特定を行った上で、標準化の方針を決定する場がない可能性。
団体間での調整事項(what)		• 標準化のニーズ • 策定中の標準の内容	• 策定中の標準の内容	
団体間で政策の調整を行う方法(how)(※)	標準化のニーズに係る調整	• DoC(NIST)が国防総省や一般調達局と標準化のニーズを特定	-	• 各省庁のCIO(もしくはCISO)が参画し、策定中の標準について調整やレビュー等を行う点で米国と日本は共通。 • 日本では関係省庁が参画するCISO等連絡会議で、統一基準について検討を行う一方で、当会議体ではIPAや他省庁が策定した標準に対する議論を行っていないため、議論を行う場がなく、団体間の調整を行うことができていない標準が存在する可能性。
	策定する標準に関する調整	• DoC(NIST)が各省庁が参加するCIO評議会等にて情報共有/連携	• NISCが原案を作成した統一基準に対して、サイバーセキュリティ戦略本部内にて設置されたCISO等連絡会議にて調整を実施。 • ただし、CISO評議会ではIPAや他省庁が策定した標準について議論を行っていない。	

※公開されている情報が限定されているため、法律に記載されているレベルでの記載となっている点に留意されたい。

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 研究機関との関係(米国)

- NIST(及びNCCoE)は大学・研究機関とプロジェクトごとに協力しており、大学研究機関はNISTに対して専門的な知見を都度提供している。
- また、NISTにおいて大学研究機関と共同で専門の研究機関を設立し研究開発を行っている事例もある。人材面や金銭面で安定的な基盤があることによって、継続的に情報共有や研究開発を行えている可能性。



[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

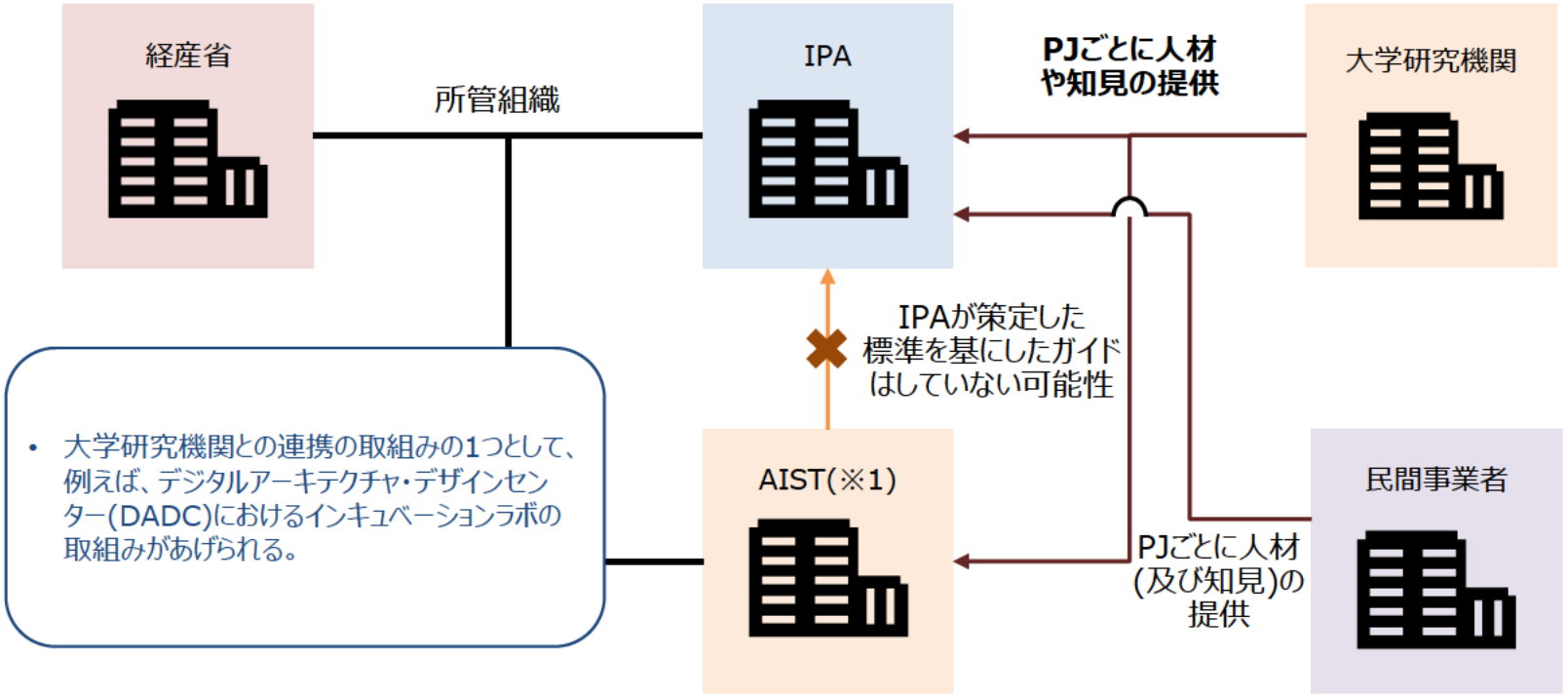
※1:セキュリティ標準策定に限らない点に留意いただきたい。。例えば、共同量子研究所内では、セキュリティ標準に関わり得る取組みとして量子暗号に係る研究を実施。

[参考] NIST" NATIONAL CYBERSECURITY CENTER OF EXCELLENCE(NCCOE)"
(https://www.nist.gov/itl/applied-cybersecurity/national-cybersecurity-center-excellence-nccoe)
CIRCULAR NO. A-130 "Managing Information as a Strategic Resource"
(https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 研究機関との関係(日本)

- 米国と同様、経産省は大学・研究機関とプロジェクトごとに協力しており、大学研究機関は経産省に対して人材や専門的な知見を都度提供している。
- 一方で、IPAと大学研究機関が共同で研究所を設立している事例はみられなかった。



[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

[参考]CPSEC「研究開発成果」(https://www.cpsec.aist.go.jp/achievements/)
IPA「サイバーセキュリティ経営可視化ツール」等
(https://www.ipa.go.jp/security/economics/checktool.html)

© Hitachi, Ltd. 2024. All rights reserved.

2-2. 行政機関・研究機関との関係性 / 小括

- 米国及び日本において、セキュリティ標準について各省庁で協議・調整を行う場は存在する一方で、日本にはトップダウン的に広くセキュリティ標準のニーズの特定や標準化の方針を決定する場がない可能性。
- 米国と日本において、プロジェクト単位で各標準機関が大学研究機関と連携する取組みはみられる。また、セキュリティ標準策定に限定しなければ、NISTにおいて大学研究機関と共同で専門の研究機関を設立している事例もみられ、専門の研究機関において継続的な情報共有や研究開発を行えている可能性がある。

比較項目	比較結果
2.2.1 行政機関との関係	• 米国及び日本においても、以下の通り**各省庁間でセキュリティ標準について協議・調整を行う場は存在**する。商務省(DoC)がOMB(及びCIO評議会)を通じてサイバーセキュリティ標準の策定方針について強いイニシアチブを発揮できる立場にある可能性。 ✓ 米国:CIO評議会 ✓ 日本:CISO等連絡会議 • 一方で、**日本ではニーズの特定を行い標準化の方針を決定する場がない可能性**。 • 米国では、大統領令を通じて特定のセキュリティ標準を期限つきで策定させる仕組みがみられる。
2.2.2 研究機関との関係	• 米国と日本において、各標準機関が大学研究機関と連携する取組みはみられる。 • 米国や日本おいても**プロジェクト単位で大学研究機関と連携がみられる。**また、セキュリティ標準策定に限定しなければ、**NISTにおいて大学研究機関と共同で専門の研究機関を設立し研究開発を行っている事例**もみられた。**人材面や金銭面で安定的な基盤があることによって、継続的に情報共有や研究開発を行えている可能性がある。**

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / NCCoEの基礎情報 (1/2)

HITACHI
Inspire the Next

- NCCoEは、民間企業を含むイノベーターと協力し標準ベースのセキュリティソリューションを提供する。

項目	内容
設立年度	• 2012年
規模 (人員/予算)	• NCCoE在籍メンバーは126名(2023年9月時点) • NCCoEプロジェクトにおける協力企業の累計数は396社(2021年実績) • センターを運営するための官民パートナーシップを確立するために1000万ドル(2012年/NIST予算)
設立目的	• 最先端のサイバーセキュリティ技術の導入を加速させることを目的とする。
ミッション/ビジョン	• **ミッション:**安全なテクノロジーの採用を加速する。(イノベーターと協力し、ビジネスニーズに対応する標準ベースのサイバーセキュリティ機能を提供する) • **ビジョン:**サイバーセキュリティを推進する(技術革新を促し、経済成長を促進する安全なサイバーインフラを提供する) • **目標:**実用的なサイバーセキュリティを提供する/サイバーセキュリティの採用率の向上させる/効果的なイノベーションを加速させる
主要なアウトプット	• NIST SP 1800シリーズ • 業界固有のサイバーセキュリティペーパー　等

NIST SP 1800シリーズ
NCCoEが募集し民間事業者が参画するコンソーシアムにて作成。サイバーセキュリティ・コミュニティに対して、**実用的で使用可能なサイバーセキュリティ・ソリューションを提示**。

<記載内容>
- ソリューションと機能の詳細な例
- 同じ最終結果を得るために複数の製品を使用する実証されたハウツーアプローチ
- あらゆる規模の組織に対する機能の実装に関するモジュール形式のガイダンス
- 組織が容易にソリューションを複製できるように、必要なすべてのコンポーネント、インストール、構成、および統合に関する情報

[参考] NIST Special Publication 1800-series General Information
(https://www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information)
NCCoE"Mission & Vision"
(https://www.nccoe.nist.gov/our-approach/mission-vision)

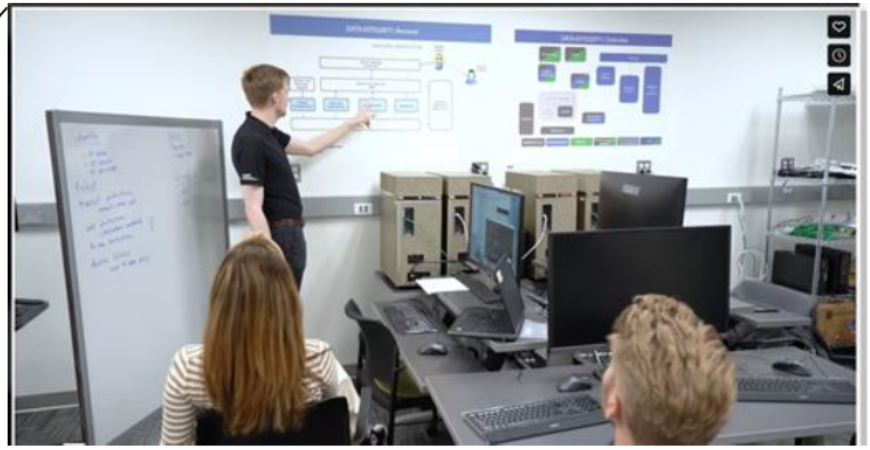
© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / NCCoEの基礎情報 (2/2)

HITACHI
Inspire the Next

- NCCoEではセクターごとにラボを設置し、実証環境を構築した上で各種課題に取り組んでいる。

ラボ	内容
データセキュリティラボ	ランサムウェア、データ侵害、その他の脅威に対する、企業におけるシステムの保護に取り組む。
エネルギーセクターラボ	送電網、石油・天然ガスパイプライン、その他のエネルギー・システムを動かすサイバー・フィジカル・システムの保護に取り組む。
ヘルスケアセクターラボ	医療機関のサイバーセキュリティを向上させるために、セキュアな技術の開発に取り組む
製造業ラボ	製造業におけるサイバーセキュリティの喫緊の課題に対処するための実践的なソリューション例の開発に取り組む
モバイルデバイスセキュリティラボ	組織によるモバイルデバイスの配備を改善し、最も差し迫ったサイバーセキュリティの課題に取り組む
・・・	NCCoEには20を超える応用サイバーセキュリティ・ラボがあり、実証環境を構築した上で、エンジニアが協力して、標準、ベストプラクティス、市販の技術を使ったサイバーセキュリティ・ソリューションの実証を行う。





(データセキュリティラボ内の)5Gプロジェクトでは、5Gに係るユースケースを調査した上で、実証環境にてデモンストレーションを行い、実際に機能していることを確認している。



(5Gプロジェクトに参画)
Intel マネージャー

[参考] NCCoE" Virtual Tours: Take a Look Inside the NCCoE"(https://www.nccoe.nist.gov/virtual-tours)
Youtube(https://www.youtube.com/watch?v=EXlQargmFL0)

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / NCCoEのプロジェクト (1/2)

- プロジェクトは、3つのプロセス(定義/収集/構築)からなる。
- 実証環境を提供するNCCoEに対して、民間事業者は対象製品の情報と専門知識を提供を行う。

プロジェクトのプロセス

Define 定義

- サイバーセキュリティの喫緊の課題を解決するために、産業界と業務範囲を定義
  - ✓ パブリック・コメントのためにプロジェクトの草案を発表
  - ✓ コメントを審査した上で、サイバーセキュリティの課題をアーキテクチャの草案とともに概説した最終版をウェブサイトに公開

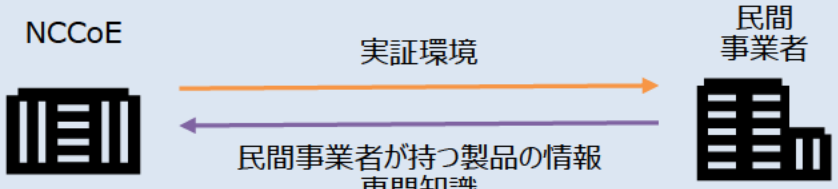
Assemble 収集

- サイバーセキュリティの課題に取り組むために、業界団体(民間事業者)、政府機関、学術機関からなるチームを編成
  - ✓ 連邦官報公告を発表し、協力の機会を告知する。
  - ✓ 協力者候補は、記入済みの関心表明書を提出する。(提出された関心表明書は先着順で受理)
  - ✓ 協力者がコンソーシアムに参加すると、共同研究開発契約に署名し、商業的に入手可能な製品と専門知識を提供。

Build 構築

- サイバーセキュリティの課題に対処するために、実用的で、使用可能で、再現可能な実装を構築
  - ✓ このフェーズでは、リファレンス・アーキテクチャを確定する。
  - ✓ 協力者は、各自の技術をインストールし設定するためのサポートを提供する。
  - ✓ また、相互運用性などの問題に対処するために、構築全体を通じてサポートを提供する。

NCCoEと民間事業者の関係性及び成果物例



【成果物例】
- NISTの標準で明らかになっているコンセプトや原則に則ったアーキテクチャ
- アーキテクチャに製品を当てはめた場合のソリューション例
- 具体的なソリューションの実装事例

[参考] NIST" NATIONAL CYBERSECURITY CENTER OF EXCELLENCE(NCCOE)"
(https://www.nccoe.nist.gov/our-approach/how-we-work)

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / NCCoEのプロジェクト (2/2)

HITACHI
Inspire the Next

- NIST SP 800-207「Zero Trust Architecture」のコンセプトや原則に則り、ゼロトラストアーキテクチャ(ZTA)ソリューションの例を実証することを目的として、PJ(IMPLEMENTING A ZERO TRUST ARCHITECTURE)が推進されている。

項目	内容
プロジェクトの目的	• 従来の一般的な企業ITインフラに適用されるZTAソリューションの例を実証すること。また、それらはNIST SP 800-207「Zero Trust Architecture」に文書化されているコンセプトと原則に従って設計され、展開される。
参画企業	• 24社(Appgate/AWS/Broadcom Software/Cisco/DigiCert/F5/Forescout/Google Cloud/IBM/Ivanti/Lookout/Mandiant/Microsoft/Okta/Palo Alto Networks/PC Matic/Ping Identity/Radiant Logic/SailPoint/Tenable/Trellix/Vmware/Zimperium/Zscaler)
アウトプット	• NIST SP 1800-35A: エグゼクティブサマリ (2nd Preliminary Draft) • NIST SP 1800-35B: アプローチ、アーキテクチャ、セキュリティの特徴 (3rd Preliminary Draft) • NIST SP 1800-35C: ハウツーガイド(3rd Preliminary Draft) • NIST SP 1800-35D: 機能デモンストレーション (3rd Preliminary Draft) • NIST SP 1800-35E: リスクコンプライアンスマネジメント (Preliminary Draft)
上記文書の想定読者と使用方法(※)	• **最高情報セキュリティ責任者や技術責任者などのビジネス意思決定者:** NIST SP 1800-35Aを使用して、このガイドの推進理由、サイバーセキュリティの課題、この課題を解決するためのアプローチ、およびこのソリューションが組織にどのような利益をもたらすかを理解することができる。 • **テクノロジー、セキュリティ、プライバシー・プログラム・マネージャー:** リスクを特定、理解、評価、軽減する方法に関心のあるマネージャーは、NIST SP 1800-35Bを使用することができる。また、NIST SP 1800-35Eでは、一般的な ZTA リファレンス設計の論理コンポーネントを、さまざまなサイバーセキュリティガイドラインや推奨プラクティス文書に記載されているセキュリティ特性にマッピングしている。 • **IT専門家:** アプローチを実装したいIT専門家は、NIST SP 1800-35Cを利用することができる。このガイドには、このプロジェクトの実装例を構築するための製品のインストール、構成、および統合に関する重要な手順が記載されており、これらの全部または一部を複製することができる。また、NIST SP 1800-35Dを使用することもできる。このガイドには、ZTAのセキュリティ機能を示すために定義されたユースケースと、各実装例でそれを実証した結果が記載されている。

※NIST SP 1800-35Bより引用

[参考] NCCoE" IMPLEMENTING A ZERO TRUST ARCHITECTURE"
(https://www.nccoe.nist.gov/sites/default/files/legacy-files/zt-arch-fact-sheet.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / CampusCyber (1/4)

HITACHI
Inspire the Next

- 2021年よりフランスにおいて企業や政府機関が連携し、キャンパスサイバーを設立。
- 相乗効果を生み出す目的で、企業、政府機関、研究機関等が1つの建物(13階)の中で検討を実施している点に特徴がみられる。

項目	内容
設立年度	• 2021年
設立場所	• フランス ピュトー
規模 (人員/予算)	• 企業(大企業、中小企業)、政府機関、研修機関、研究機関が参画(建物内で働く人は約2000人) • さまざまな分野から160以上の関係者が参加を表明。(2023年9月時点) • 5年間で4,000万ユーロ(約63億円)(※)を投入される。
設備	• 13階建ての建物 • プライベート及び共有ワークスペース面積合計17,000㎡
設立目的	• サイバーセキュリティコミュニティを統合し、これらの異なるアクター間のシナジーを発展させること
コンセプト/ミッション	• コンセプト:国内外の主要なプレーヤーが一堂に会するサイバーセキュリティの象徴的な場所。これにより、企業（大企業、中小企業）、政府機関、研修機関、研究機関、団体を同じ敷地内に迎えることができる。 • ミッション:デジタルセキュリティの利害関係者を同じ場所に集めて、社会を保護し、この分野でのフランスの卓越性を促進する。
活動の4つの柱	1. **オペレーション**:データを共有することで、すべての人がデジタル・リスクを使いこなす能力を強化する。 2. **フォーメーション**:エコシステムの全体的な技能向上のため、さまざまな対象者（公務員、職員、学生、再教育中の職員など）の初期研修および継続研修を支援。 3. **イノベーション**:技術革新を誘導し、経済構造への統合を強化するための、官民間のシナジー効果の開発。 4. **モビライゼーション**:革新的なイベントや交流のプログラム、そして信頼というデジタル社会の進化の発見に特化した、活気に満ちた開かれた場所。

[参考] Campus Cyber
(https://campuscyber.fr/#concept)
Paris La Défense“Campus Cyber”
(https://parisladefense.com/en/discover/towers/campus-cyber)

※ユーロ=157円で換算

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / CampusCyber (2/4)

HITACHI
Inspire the Next

- 研究開発およびプロトタイピングのサポートを行っており、NCCoEで作成しているような実践ガイドに留まらず具体的なツール等も作成している点に特徴がみられる。
- キャンパスサイバーでは、サイバーコモンズスタジオにて各作業グループが検討を行っている。

サイバーコモンズスタジオ

- ワーキンググループでテーマをまとめて調査する。
- **研究開発およびプロトタイピングのサポート**(例:知識、仕様書、データセット、技術構成要素の作成など)
- コモンズのガバナンスと運営を確立する。

作業グループ	内容
ポスト量子暗号	ポスト量子暗号の課題に対する認識を高め、暗号化の実装を俊敏なものへ導く。
フォーメーション	サイバー職業へのアクセスを促進・容易にし、職業を奨励し、職業に就く女性の数を増やす。
サイバー4トゥモロー	エコシステムの能力を強調し、持続可能な開発目標の課題を踏まえ、責任ある倫理的なデジタルの未来のための適切な対応を策定する。
暗号資産	暗号資産に関するサイバーセキュリティの視点を発展させ、サイバーセキュリティのための暗号資産の潜在的な用途を特定する。
意識改革	サイバーセキュリティに関する意識を高める革新的な方法を特定し、実施する。
危機管理と訓練	組織のサイバーレジリエンスを高める。
脆弱性管理	ソフトウェア、ソフトウェアパッケージ、ソフトウェアコンポーネント、インフラストラクチャに影響を与える脆弱性を特定して対処する。
AIとサイバーセキュリティ	人工知能が進歩を可能にするサイバーセキュリティの領域を分析する。
CTI(サイバー脅威インテリジェンス)	サイバー脅威インテリジェンスに関連したデータ共有のためのサイバーコモンズの構築と実施する。
アジャイルセキュリティ	アジャイルコンテキストでのセキュリティの実装を加速または有効にする。
リソースの共有	目的は、相互化可能なサービスを特定し、ガバナンスフレームワークを提案する。
期待	脅威の進化と対応の進化について集合的に反省する。

[参考] CAMPUS CYBER "COMMUNS"(https://campuscyber.fr/studios-des-communs/)
CAMPUS CYBER "Thèmes" (https://wiki.campuscyber.fr/Th%C3%A8mes)

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / CampusCyber (3/4)

HITACHI
Inspire the Next

- 公告によって結成された作業グループでは、7名～18名の人数が集まり手法やツールを開発する。

作業グループの概要 (例:危機管理と訓練作業グループ)

作業グループ	内容
参加者	• 非公開 (3ヶ月を超えない推奨期間で7人から18人のメンバーで構成するとされる。)
業務分野	• サイバーレジリエンスとサイバー危機管理の教義と方法 • 一般的なトレーニング方法論の開発 • 成熟度評価とサイバー危機管理専用のツールの開発
アウトプット	• **サイバー危機管理の教義と方法** ✓ 中小企業向けガイドとキット ✓ 高等教育向け標準トレーニング　等 • **危機管理ツールと評価** ✓ 成熟度指数と管理策のリスト ✓ **サイバー強靭性自己評価ツール** ✓ **警告・危機管理ツール**　等 • **研修** ✓ 訓練戦略 ✓ 演習シナリオ共有のための枠組み文書　等

作業グループのでの検討ステップ

ステップ	内容	
調査	• 課題の整理 • 公告	作業グループの組織前
説明	• 作業グループの構築 • 作業グループの立ち上げ	作業グループでの検討
実現	• 課題等の分析 • 成果物の開発	
運用	• 成果物のメンテナンス • 成果物の更新	コモンズでの統治

戦略文書や各種ガイドに加えて、
各種ツールを作成

[参考] CAMPUS CYBER " GT : CYCLE 3"
(https://campuscyber.fr/resources/gt-cycle-3/)
CAMPUS CYBER " Crise cyber et entraînement"
(https://wiki.campuscyber.fr/Crise_cyber_et_entra%C3%AEnement)

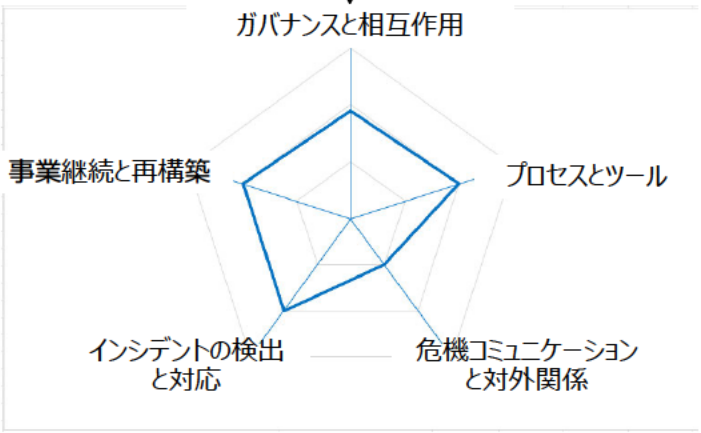
© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / CampusCyber (4/4)

- 「サイバー危機管理に関するガイド集」に基づいてANSSIが公開した自己評価ツールにおいて、自己評価結果から導かれた推奨事項における具体的な実装手法として、キャンパスサイバー(危機管理と訓練作業グループ)が開発したドキュメント等が紹介(予定)。
- 直接的ではないが、ANSSIが策定したセキュリティ標準の実装をキャンパスサイバーが一部支援。

サイバー危機管理に関するガイド集 (ANSSI) → **自己評価ツール (ANSSI)**

キャンパスサイバーの「危機管理と訓練」WGから公表されているドキュメント/ツールによって更新予定とされている。ただし、調査時点(2023/9/28)では未公表(※2)



アセスメント結果(抜粋)

分類	質問	成熟度 (※1)	次のステップ	利用可能なドキュメント/ツール
プロセスとツール	危機管理ユニットには、危機管理専用のデジタルツールがありますか?	1	危機ユニットには、オフラインでアクセスできる専用のデジタルツールがあります。	コンピュータ衛生ガイド、2017年:www.ssi.gouv.fr/guide/guide-dhygiene-informatique
…		…	…	…

推奨事項(抜粋)

※1:利用者の回答結果。0～3の4段階で判断
※2:キャンパスサイバーのドキュメントに加えて、ANSSIの「サイバー危機管理」コレクションのドキュメントによっても更新予定とされている。

[参考] ANSSI" PUBLICATION D'UN OUTIL D'AUTOÉVALUATION DE GESTION DE CRISE CYBER"
(https://www.ssi.gouv.fr/actualite/publication-dun-outil-dautoevaluation-de-gestion-de-crise-cyber/)

© Hitachi, Ltd. 2024. All rights reserved.

2-3. 官民連携の実施状況 / 小括

HITACHI
Inspire the Next

- NCCoEはNIST(応用セキュリティ部)の一部門であり公的な組織における取組み(プロジェクト単位で民間企業を募集)として、キャンパスサイバーは官民が共同で出資している組織における取組みとして位置づけられる。

項目	比較結果
組織の位置づけ	• NCCoEはNIST(応用セキュリティ部)の一部門であり**公的な組織における取組み(プロジェクト単位で民間企業を募集)**として位置づけられる一方で、キャンパスサイバーは企業(大企業、中小企業)、政府機関、研修機関、研究機関が参画する**官民が共同で出資している組織として位置**づけられる。 • NCCoEでは、NISTの予算の一部として予算が割り当てられており、キャンパスサイバーにおいては、国家サイバーセキュリティ戦略の枠組みから資金提供がなされている。 • キャンパスサイバーでは、相乗効果を期待し1つの建物内で検討を実施。
取組み内容	• NCCoEではセクターごとにラボを設置し、実証環境を構築した上で、NISTが策定した**セキュリティ標準の実践ガイドを**作成している。 • キャンパスサイバーでは各作業グループにおいて**研究開発およびプロトタイピングのサポートを行っており、具体的なツール等を作成**。 (例:知識、仕様書、データセット、技術構成要素の作成など。) ANSSIが公開した文書の中で、キャンパスサイバーが策定した文書やツール等は参照予定と明記されている。

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

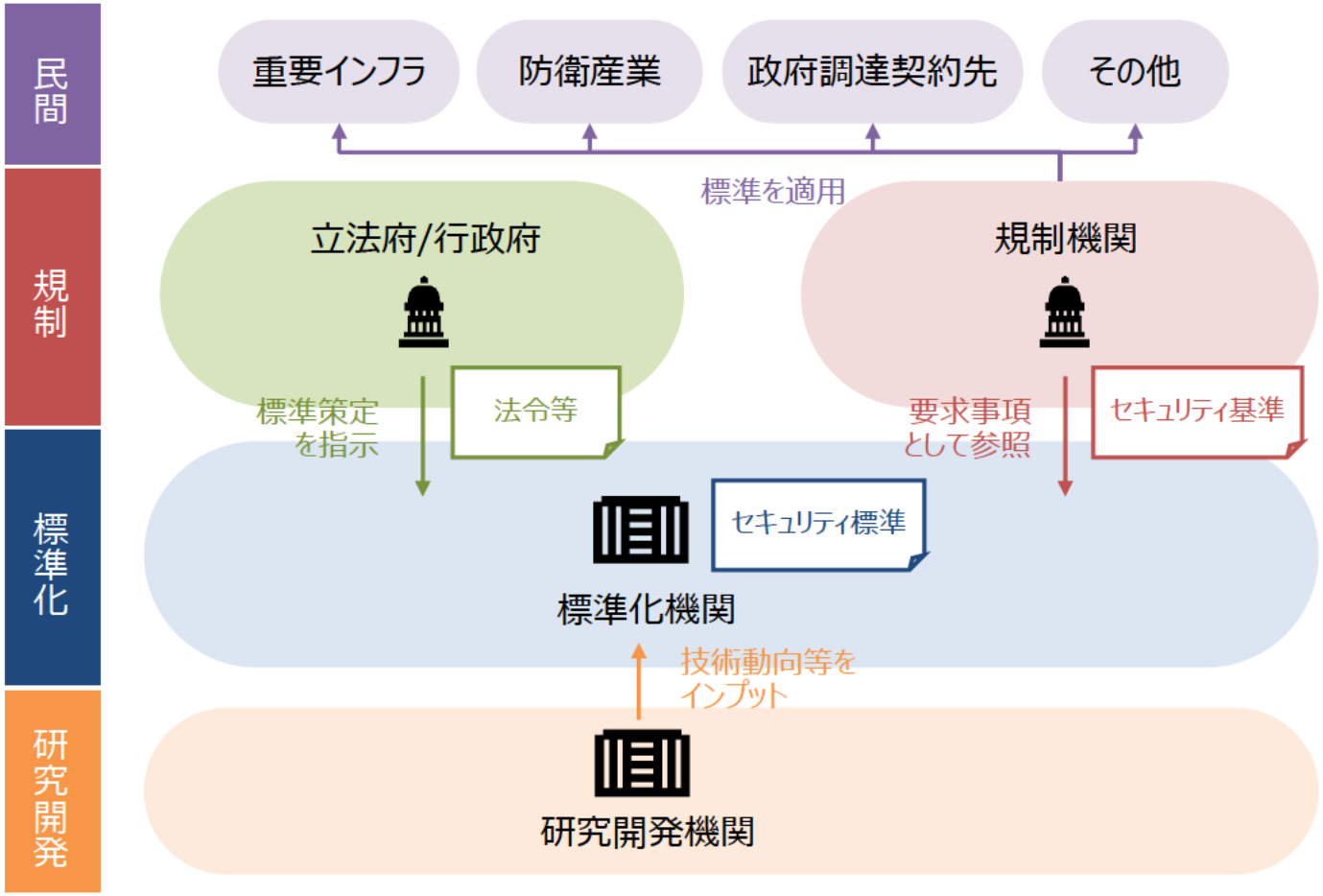
3. 標準化機関等から発行される文書体系等の日米比較

© Hitachi, Ltd. 2024. All rights reserved.

本章の分析に用いる参照モデル

HITACHI
Inspire the Next

- 本章にて米国及び日本の現状を整理するにあたり、以下の参照モデルをベースとして分析を行っていく。

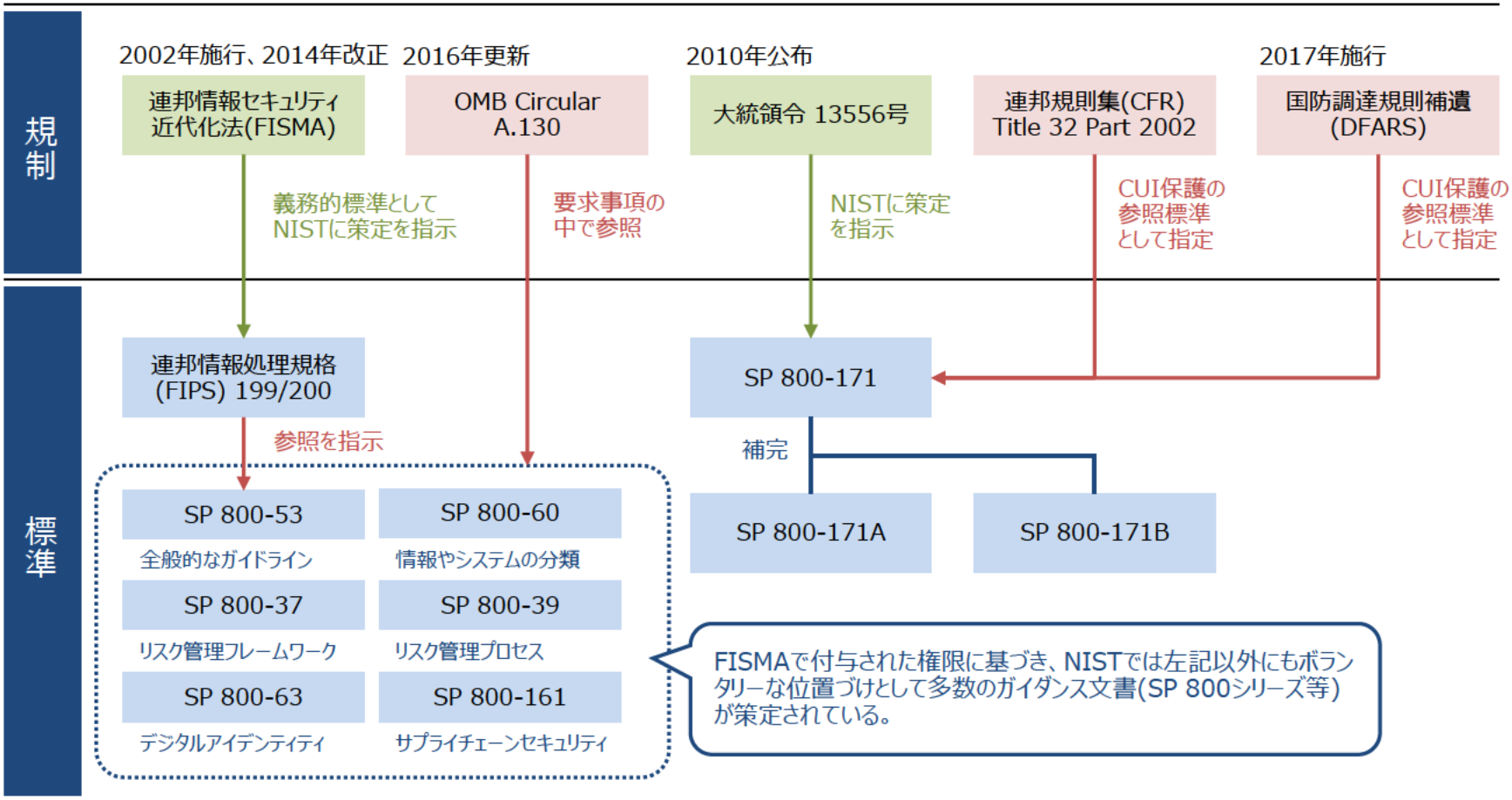


[凡例] 標準の策定を指示する機関等　標準を策定する機関等　標準の利用を強制等する機関等
研究開発を行う機関等　民間事業者等

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / 政府情報システム(米国)

- 2002年の連邦情報セキュリティ近代化法の規定に基づき、NISTでは政府情報システムの義務的なセキュリティ対策に必要な標準及び、ボランタリーな標準の策定を実施。
- 2010年には、大統領令 13556号が公開され、CUI保護に関する標準の策定がNISTに指示された。
- 法規制制定を大統領府、議会または規制機関が担い、標準策定をNISTが行うという分担がなされている。

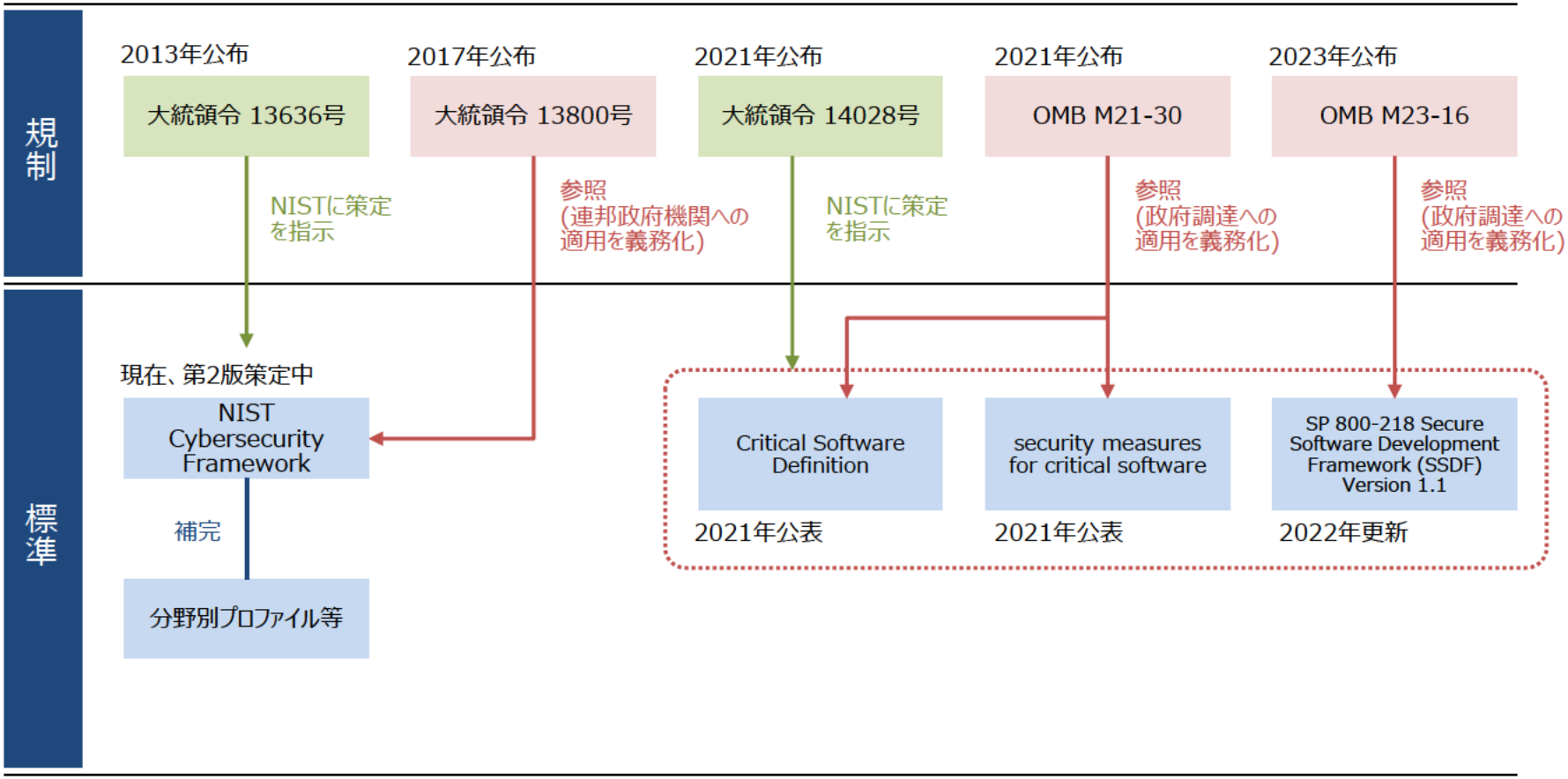


[凡例] NISTに標準の策定を指示するもの　策定された標準　標準の利用を強制等するもの

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / 重要インフラ・ソフトウェア(米国)

- 2013年に公布された大統領令 13636号に基づき、NIST Cybersecurity Frameworkが公開された。同文書は2017年の大統領令 13800号にて連邦政府機関への適用が義務化された。
- 2021年に公布された大統領令 14028号では、ソフトウェアサプライチェーン関連で多数の標準策定指示がNISTに対してなされた。そのうち重要ソフトウェアに関する標準とセキュアなソフトウェア開発慣行に関する標準は、OMB覚書にて連邦政府機関の対応が義務化されている。



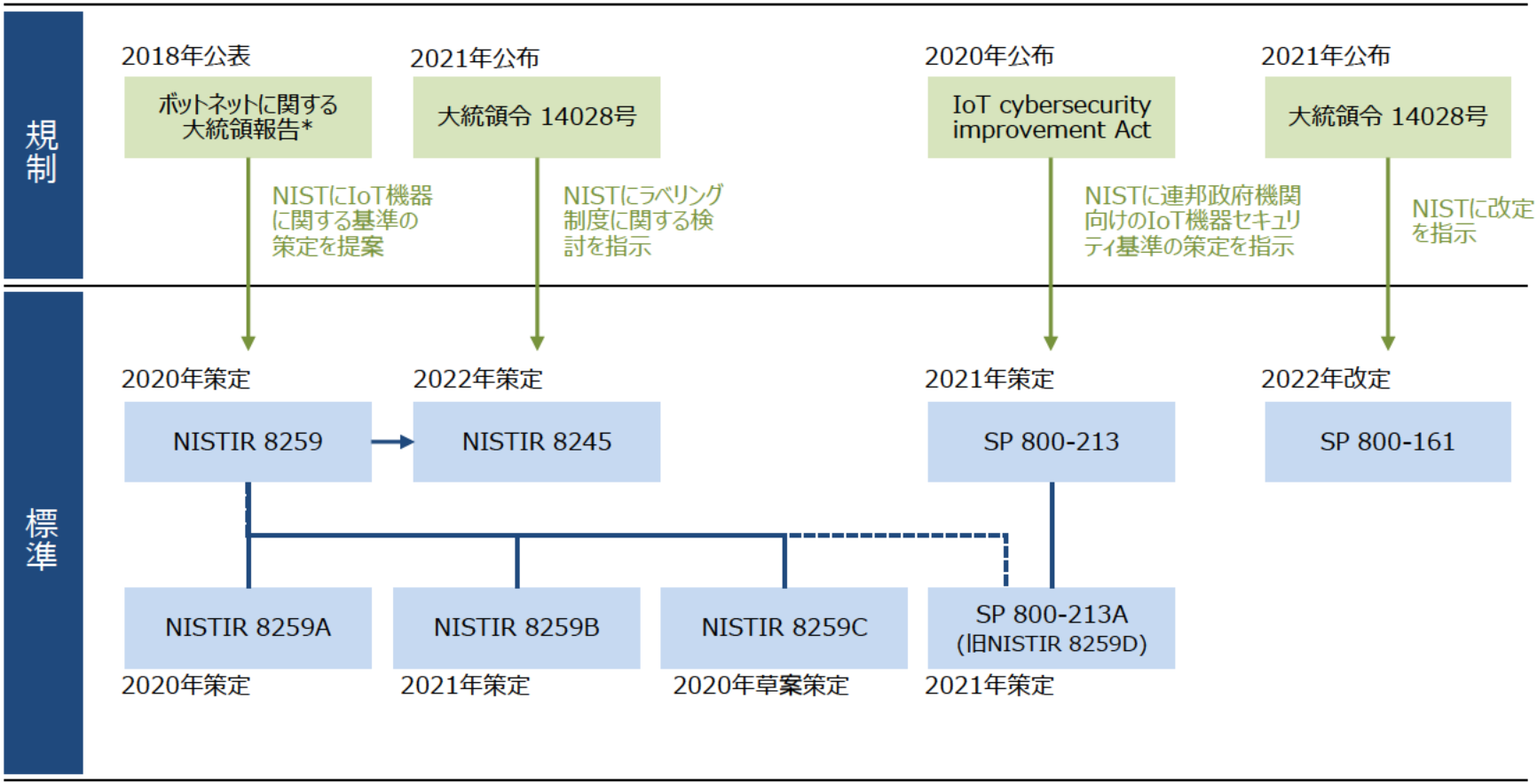
[凡例] NISTに標準の策定を指示するもの　策定された標準　標準の利用を強制等するもの

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / IoT製品・サプライチェーン(米国)

HITACHI
Inspire the Next

- IoT製品については、2018年のボットネットに関する大統領報告をきっかけにNISTIR 8259シリーズ文書が策定され、それらを参照する形でIoTサイバーセキュリティ改善法で指示された連邦政府機関向け基準や大統領令 14028号で指示された消費者IoT機器向けの基準が策定された。



* "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats"

[凡例] NISTに標準の策定を指示するもの　策定された標準　標準の利用を強制等するもの

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / FIPS・SP 800(米国)

HITACHI
Inspire the Next

- 前頁で紹介した文書体系において、すでに策定されている文書のうち主なものは以下の通り。

シリーズ	発行体	文書名	発行年
FIPS シリーズ*1	NIST	FIPS 140-3 暗号モジュールのセキュリティ要求事項	2019年
		FIPS 186-5 デジタル署名標準 (DSS)	2023年
		FIPS 197 先進的暗号標準 (AES)	2023年
		FIPS 198-1 鍵付きハッシュメッセージ認証コード (HMAC)	2008年
		FIPS 199 連邦政府の情報および情報システムに対するセキュリティ分類規格	2004年
		FIPS 200 連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項	2006年
		FIPS 201-3 連邦職員および委託業者のアイデンティティの検証	2022年
		FIPS 202 SHA-3規格：並べ替えベースのハッシュ関数及び拡張可能出力関数	2015年
SP 800 シリーズ*2	NIST	SP 800-18 連邦情報システムのセキュリティ計画策定に関する手引き	2006年
		SP 800-30 Rev.1 リスクアセスメント実施の手引き	2012年
		SP 800-37 Rev.2 情報システム・組織向けリスクマネジメントフレームワーク：セキュリティ及びプライバシーに対するシステムライフサイクルアプローチ	2012年
		SP 800-53 Rev.5 情報システム・組織向けのセキュリティ・プライバシー管理策	2020年
		SP 800-53A Rev.5 情報システム・組織向けのセキュリティ・プライバシー管理策の評価	2022年
		SP 800-53B 情報システム・組織向け管理策ベースライン	2020年
		SP 800-60 Vol.1 Rev.1 情報及び情報システムの種別とセキュリティ分類のマッピングに関する手引き	2008年
		SP 800-63-3 デジタルアイデンティティに関するガイドライン	2020年
		SP 800-171 Rev.2 非連邦システム・組織における管理すべき非格付け情報(CUI)の保護	2021年

*1: NISTページ上で利用可能なものは11件。(https://csrc.nist.gov/publications/search?sortBy-lg=Number+DESC&viewMode-lg=brief&ipp-lg=ALL&status-lg=Final&series-lg=FIPS)
*2: NISTページ上で利用可能なものは176件。(https://csrc.nist.gov/publications/search?keywords-lg=800-&sortBy-lg=Number+DESC&viewMode-lg=brief&ipp-lg=ALL&status-lg=Final&series-lg=SP)

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / SP 1800等(米国)

HITACHI
Inspire the Next

- 前頁で紹介した文書体系において、すでに策定されている文書のうち主なものは以下の通り。

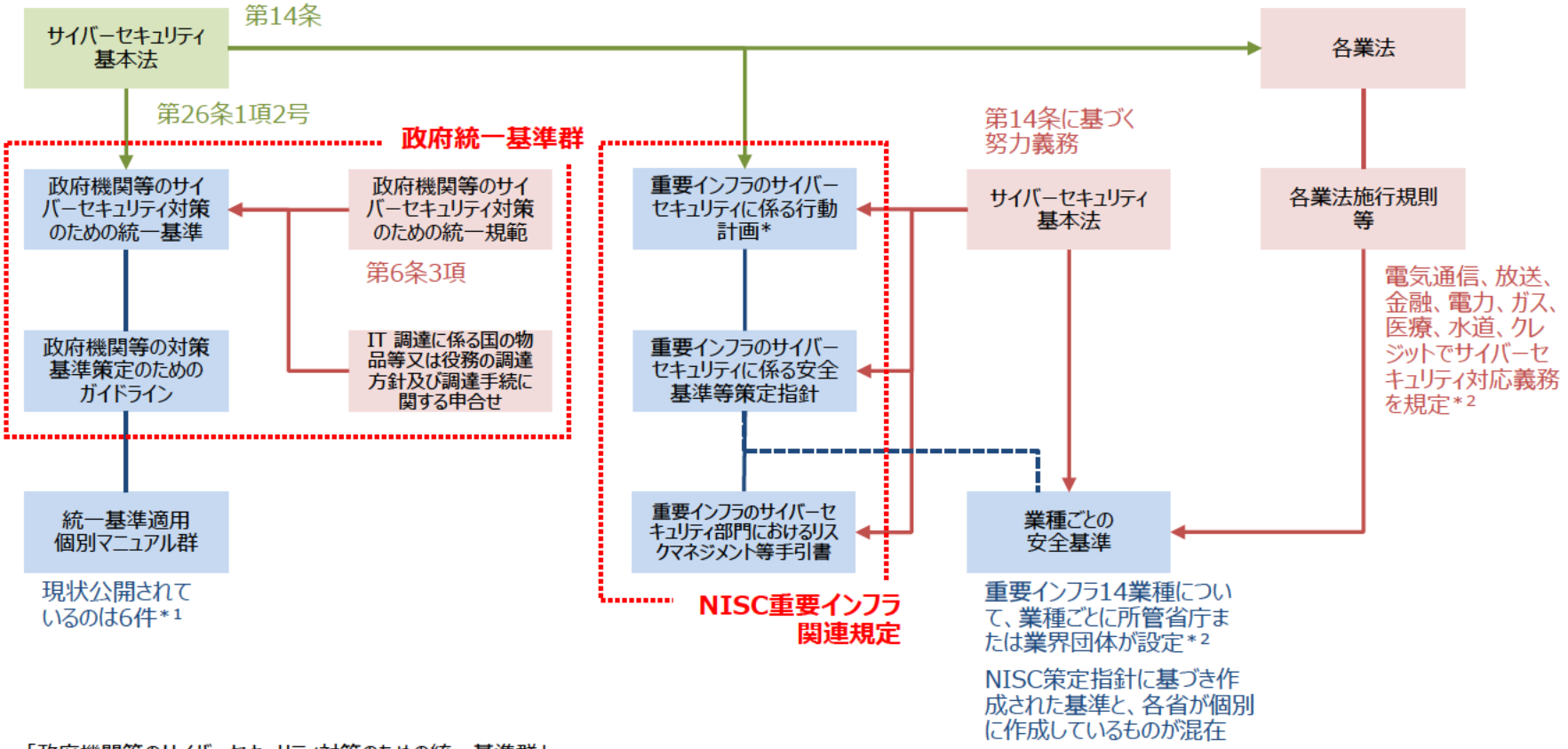
シリーズ	発行体	文書名	発行年
SP 1800 シリーズ*3	NIST NCCoE	SP 1800-1 モバイル端末上の電子健康記録(EHR)の保護	2018年
		SP 1800-2 電力設備向けのアイデンティティ・アクセス管理	2018年
		SP 1800-5 IT資産管理	2018年
		SP 1800-7 電力設備向けの状況認識	2019年
		SP 1800-8 医療提供組織におけるワイヤレス輸液ポンプの保護	2018年
		SP 1800-10 産業用制御システム環境における情報及びシステムの完全性の保護：製造業向けサイバーセキュリティ	2022年
		SP 1800-12 派生した個人識別検証(PIV)クレデンシャル	2019年
		SP 1800-17 電子商取引向けの多要素認証：リスクベースによる購入者向けのFIDO Universal 2nd Factor(U2F)の実装	2019年
		SP 1800-23 エネルギー業界の資産管理：電力設備・石油ガス産業向け	2020年
		SP 1800-32 分散型エネルギー資源の保護： 産業用IoTのサイバーセキュリティ事例	2022年
NISTIR*4	NIST	NISTIR 8200 IoTのための国際サイバーセキュリティ標準化の状況に関する省庁間報告書	2018年
		NISTIR 8202 ブロックチェーン技術の概要	2018年
		NISTIR 8228 IoTのサイバーセキュリティ・プライバシーリスク管理に対する考慮事項	2019年
		NISTIR 8240 NISTポスト量子暗号標準化プロセス第1ラウンドの現状報告	2019年
		NISTIR 8259 IoT機器製造者向けの基本的サイバーセキュリティ活動	2020年
		NISTIR 8397 ソフトウェアの開発者検証のための最低基準に関するガイドライン	2021年

*3: NISTページ上で利用可能なものは26件。(https://csrc.nist.gov/publications/search?keywords-lg=1800-&sortBy-lg=Number+DESC&viewMode-lg=brief&ipp-lg=ALL&status-lg=Final&series-lg=SP)
*4: NISTページ上で利用可能なものは264件。(https://csrc.nist.gov/publications/search?sortBy-lg=Number+DESC&viewMode-lg=brief&ipp-lg=ALL&status-lg=Final&series-lg=IR)

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / 基本法、各業法に係るもの(日本)

- 政府情報システム及び重要インフラ関連(業種特有のものを除く)の標準類は、サイバーセキュリティ基本法の規定に則り、NISCが中心となり策定されている。
- 一方で、各業法またはその施行規則等で参照され得る業種ごとの安全基準は、各業所管省庁または業界団体で策定されている。



*1 「政府機関等のサイバーセキュリティ対策のための統一基準群」
https://www.nisc.go.jp/policy/group/general/kijun.html

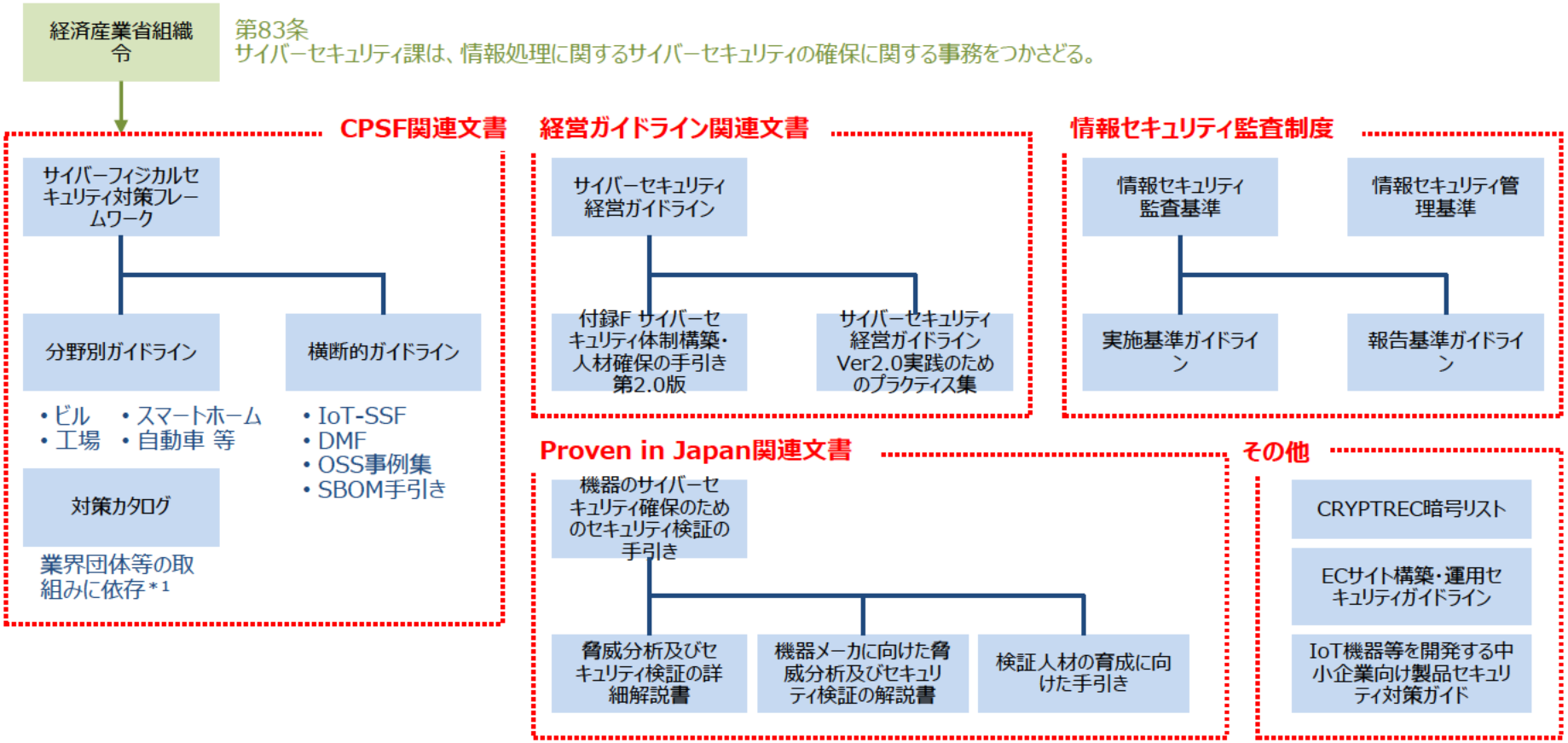
*2 「重要インフラにおける安全基準等の継続的改善状況等に関する調査について」(サイバーセキュリティ戦略本部 重要インフラ専門調査会(第33回))
https://www.nisc.go.jp/pdf/council/cs/ciip/dai33/33shiryou02.pdf

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 /経済産業省が発行するもの(日本)

HITACHI Inspire the Next

- 経済産業省組織令第83条に基づき、ユーザー事業者だけでなく、検証や監査等のセキュリティ関連サービスを提供する事業者も対象としたボランタリーな標準等が多数策定されている。
- 近年は、政府情報システムや重要インフラに必ずしも該当しない業種等における分野別ガイドラインや、IoTやソフトウェア等におけるセキュリティ確保に資する文書の策定に注力している。

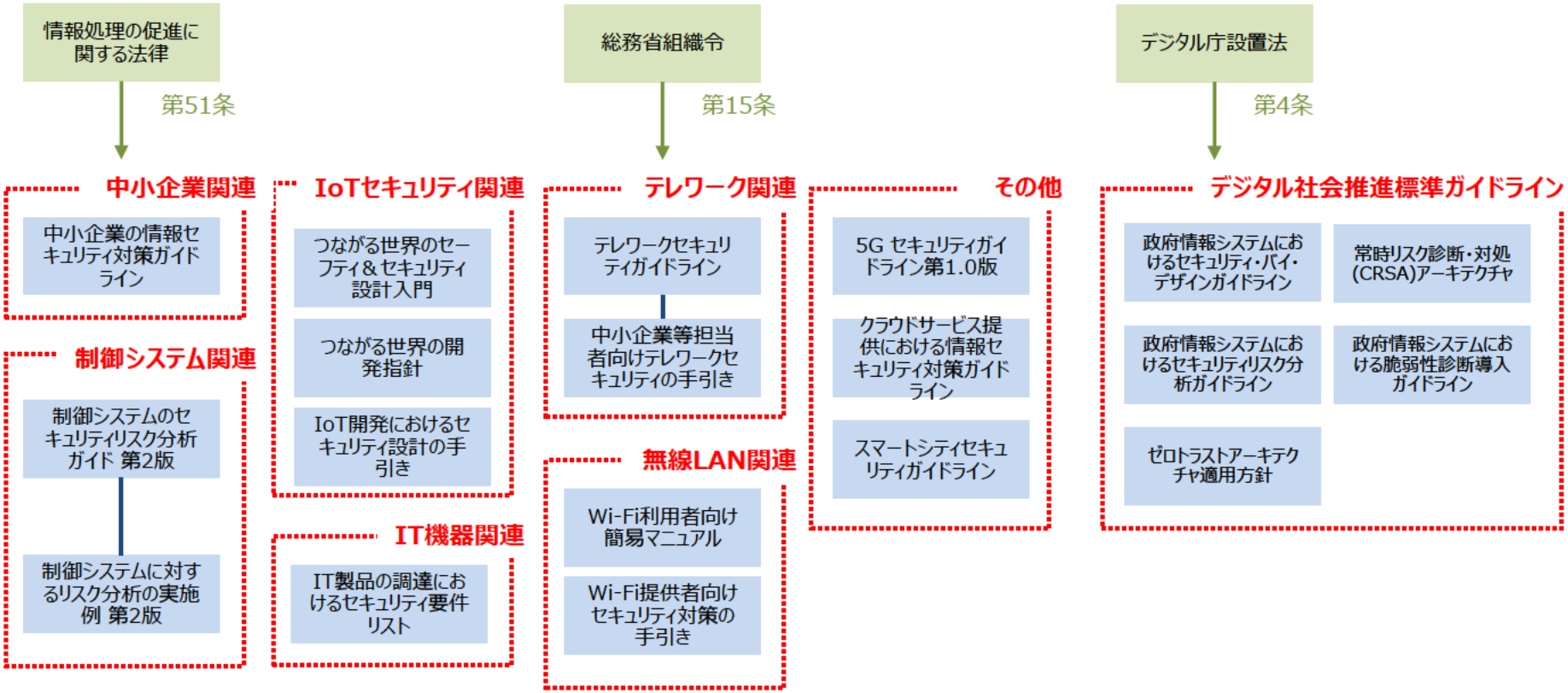


* 経済産業省の取組みについては、以下サイトから関連するものを抜粋
https://www.meti.go.jp/policy/netsecurity/index.html

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / その他(日本)

- NISC及び経済産業省以外にも、総務省やデジタル庁のようなサイバーセキュリティに係る事務を所掌する省庁からサイバーセキュリティ関連の標準が公開されている。
- 主に、総務省はテレワークや5G、無線LANを中心としたネットワーク関連、デジタル庁は政府情報システム関連の文書(デジタル社会推進標準ガイドライン)を策定している。



*1 IPAの取組みについては、以下サイトから関連するものを抜粋
https://www.ipa.go.jp/security/index.html

*2 総務省の取組みについては、以下サイトから関連するものを抜粋
https://www.soumu.go.jp/main_sosiki/cybersecurity/index.html

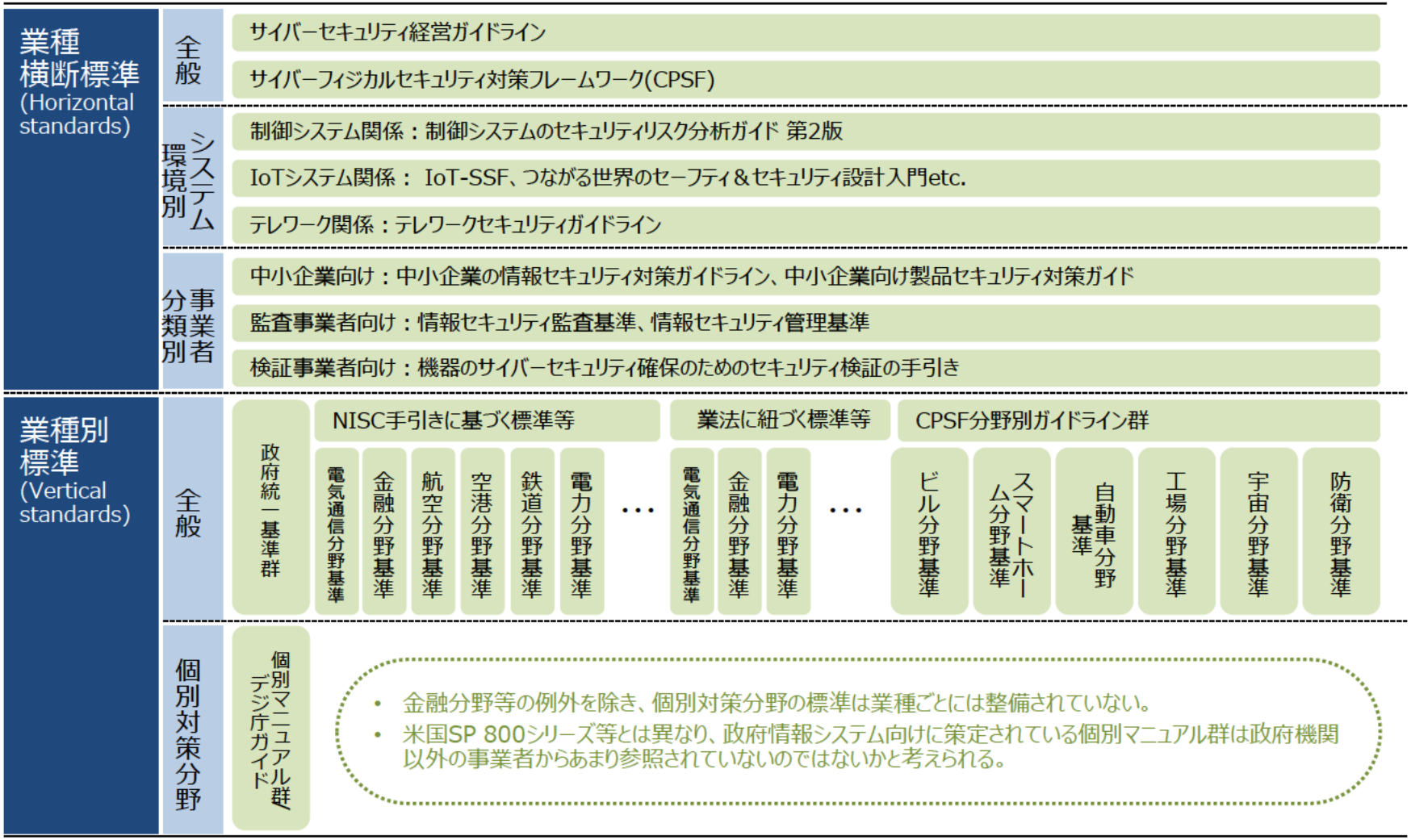
*3 デジタル庁の取組みについては、以下サイトから関連するものを抜粋
https://www.digital.go.jp/resources/standard_guidelines/#security

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / 既存標準等の暫定的整理

HITACHI
Inspire the Next

- これまで開発されてきた標準は、大きく分けて業種横断的な標準(Horizontal standards)と、業種別標準(Vertical standards)に分けられる。



© Hitachi, Ltd. 2024. All rights reserved.

[参考] 文献リスト(1/3)

HITACHI
Inspire the Next

- 前頁で紹介した文書体系において、すでに策定されているか、または策定中である文書のうち主なものは以下の通り。

分野	発行体	安全基準等の文書名	発行年 (最終改定)
政府機関等	内閣サイバーセキュリティセンター(NISC)	政府機関等のサイバーセキュリティ対策のための統一規範	2023年
		政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）	2023年
		政府機関等のサイバーセキュリティ対策の運用等に関する指針（令和3年度版）	2021年
		対策推進計画策定マニュアル	2023年
		政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書	2022年
		情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	2022年
		外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書	2016年
		政府機関等における情報システム運用継続計画ガイドライン	2021年
		スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	2016年
重要インフラ一般	NISC	重要インフラのサイバーセキュリティに係る行動計画	2022年
		重要インフラのサイバーセキュリティに係る安全基準等策定指針	2023年
		重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書	2023年
電気通信(放送、ケーブルテレビは略)	総務省	事業用電気通信設備規則	2023年
		情報通信ネットワーク安全・信頼性基準	2020年
	(一社)電気通信事業者協会安全・信頼性協議会	電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）	2023年

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 文献リスト(2/3)

HITACHI
Inspire the Next

- 前頁で紹介した文書体系において、すでに策定されているか、または策定中である文書のうち主なものは以下の通り。

分野	発行体	安全基準等の文書名	発行年 (最終改定)
金融	金融情報システムセンター(FISC)	金融機関等コンピュータシステムの安全対策基準・解説書	2023年
		金融機関等におけるセキュリティポリシー策定のための手引書	2008年
航空	国土交通省	航空分野における情報セキュリティ確保に係る安全ガイドライン（第５版）	2019年
鉄道	国土交通省	鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第４版）	2019年
電力	経済産業省	電気設備に関する技術基準を定める省令	2023年
		電気事業法施行規則第50条第２項の解釈適用に当たっての考え方	2023年
	(一社)日本電気協会	電力制御システムセキュリティガイドライン	2019年
		スマートメーターシステムセキュリティガイドライン	2019年
ガス	経済産業省	ガス事業法施行規則	2023年
	(一社)日本ガス協会	都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説	
政府・行政	総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン	2022年
医療	厚生労働省	医療法施行規則	2023年
		医療情報システムの安全管理に関するガイドライン（第6.0版）	2023年
水道	厚生労働省	水道施設の技術的基準を定める省令	2020年
		水道分野における情報セキュリティガイドライン（第４版）	2019年
物流	国土交通省	物流分野における情報セキュリティ確保に係る安全ガイドライン（第４版）	2019年
化学	石油化学工業協会	石油化学分野における情報セキュリティ確保に係る安全基準	2019年
クレジット	クレジット取引セキュリティ対策協議会	クレジットカード・セキュリティガイドライン【4.0版】	2023年
石油	石油連盟	石油分野における情報セキュリティ確保に係る安全ガイドライン	2020年

[参考] 文献リスト(3/3)

HITACHI
Inspire the Next

- 前頁で紹介した文書体系において、すでに策定されているか、または策定中である文書のうち主なものは以下の通り。(範囲を広げれば他にも多数あり)

分野	発行体	安全基準等の文書名	発行年 (最終改定)
IoT	経済産業省・総務省・IoT推進コンソ	IoTセキュリティガイドラインver1.0	2016年
	総務省	端末設備等規則	2023年
	総務省	端末機器の基準認証に関するガイドライン(第１版)	2020年
	経済産業省	サイバーフィジカルセキュリティ対策フレームワーク	2019年
	経済産業省	IoTセキュリティ・セーフティフレームワーク(IoT-SSF)	2020年
製造	経済産業省	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer1.0	2022年
ビル	経済産業省	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版	2023年
スマートホーム	経済産業省	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン	2021年
宇宙	経済産業省	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver1.1	2023年
自動車	経済産業省	自工会/部工会・サイバーセキュリティガイドライン V2.1	2023年

© Hitachi, Ltd. 2024. All rights reserved.

3-1. 日米における文書体系の整理 / 日米間の比較結果(サマリ)

HITACHI
Inspire the Next

- セキュリティ対策の強制状況は一部の例外を除いて大きな差異が見られなかった一方で、米国では標準策定の指示の具体性が高く、政府内での役割分担が明確であり、NISTを中心に多数の文書が策定されている点が大きな差異となっている。

比較項目	米国	日本	両国の主な差異
分野ごとのセキュリティ対策強制の有無	• 政府システムについて、FISMA等で一定の対策を義務化 • 重要インフラ等について、横断的な規制はなく、ボランタリーな取組みの喚起が中心	• 政府システムについて、統一基準に則った対策を義務化 • 重要インフラ等について、対策の実施は努力義務と位置づけ※1	• ソフトウェア調達等の一部の領域を除き、日米で必ずしも大きな差異は見られない
標準化機関等に対する標準策定の指示のあり方	• 連邦法や大統領令にて、NIST等への具体的な指示を実施 • 標準化の主題だけでなく、策定主体や策定期限を明示しつつ指示がなされる	• サイバーセキュリティ戦略や重点計画において標準化の主題や担当省庁が示されていることがある • 主題や策定期限がの具体的に示されることは少ない	• 米国の大統領令にあるものと比較して、日本の法令や閣議決定文書等における基準等策定の指示は曖昧さを残すことが多い
標準策定に係る政府内の役割分担	• OMB等の規制機関が規則の策定等を担う一方、(特に大統領令等にて規定される場合)標準策定の多くはNISTへと委任	• 制度的な位置づけが明確な標準について、NISCや防衛省、総務省等の規制機関または業界団体が自ら標準策定を実施	• 対象とした基準策定は規制機関に集中しており、米国にあるような役割分担は希薄 • 強制基準にて自主的なガイドラインはほとんど参照されていない
策定されている標準の体系化、量的な充実の程度	• NISTで策定されるものについては、FIPS、SP 800、SP 1800等にシリーズ化されており、それぞれ11、176、26件の文書が利用可能 • 上記は政府機関だけでなく、民間からも参照されている	• NISCで策定されているものについては、政府統一基準群、重要インフラ関連規定にまとめられているが、文書数は比較的限定的 • その他自主的なものについては、多くがシリーズ化されていない	• SP 800等と比較して日本では具体的な手順・マニュアル等の整備は限定的 • SP 1800に相当する具体的な実装方法にまで言及する文書は日本には存在しない

※1 第5次行動計画にて一定の体制整備の法的な必要性を改めて示唆

© Hitachi, Ltd. 2024. All rights reserved.

3-2. 標準化の優先領域 / NISTによる方向性(1/2)

HITACHI
Inspire the Next

- NISTでは、ポスト量子や軽量暗号、フレームワーク類を通じたリスク管理の強化、NCCoEにおける官民パートナーシップの推進を通じた実用的ソリューション、IoT関連のルール形成が優先的に推進されている。

重点領域	方向性	取組み例
暗号 (Cryptography)	技術の進歩がもたらすリスクから個人、企業、政府を守ることを目的として、暗号の健全な利用を促進するために、信頼できるツールとリソースを提供している。	• 暗号アルゴリズムの設計と検証 • ポスト量子暗号(PQC)の標準化 • 軽量暗号の標準化
リスク管理の強化 (Enhanced risk management)	急速に進化する脅威の状況と、企業レベルのビジネス要件を満たす必要性とのバランスを取らなければならない中で、サイバーセキュリティ・リスクを測定し、管理することを支援するために、NIST は関係者を招集して各種フレームワーク等を策定している。	• サイバーセキュリティと統合リスク管理(ERM)の統合を目的としたNISTIR 8286シリーズの策定 • Cybersecurity Framework 2.0への改定 • リスク管理フレームワーク(RMF)の適用推進 • プライバシーフレームワークの開発、適用推進 • サイバーセキュリティ・サプライチェーン・リスク管理(CSCRM)に関するガイドラインの策定 - SP 800-161 Rev.1の公開 - SP 800-218 Rev.1 SSDFの公開
実用的ソリューション (Practical solutions)	National Cybersecurity Center of Exellence(NCCoE)を、企業、政府機関、学術機関が連携して、企業の最も差し迫った実用的なサイバーセキュリティの問題に取り組む共同拠点として機能させる。	• NCCoEにおける官民パートナーシップの推進を通じた信頼性の高いネットワークやプラットフォームの構築 - マーケットリーダーやセキュリティ企業を含むコンソーシアムを通じて、標準とベストプラクティスを適用し、市販の技術を使用した適応可能なサイバーセキュリティ・ソリューションの例を開発 - セキュリティガイドライン(SP 1800シリーズ)の策定
モノのインターネット (Internet of Things)	コネクテッドデバイスのサイバーセキュリティを向上させるための標準、ガイドライン、関連ツールの開発と適用を支援している。	• セキュリティ管理をサポートするために一般的に必要とされる機能を定義するIoT Device Cybersecurity Core Baselineの策定 • 2020年12月に署名された法律に基づき連邦政府向けベースラインプロファイルを策定

[参考] NIST CYBERSECURITY & PRIVACY PROGRAM
(https://www.nist.gov/system/files/documents/2022/07/21/Extended%20Cybersecurity%20Vitals%20Fact%20Sheet.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3-2. 標準化の優先領域 / NISTによる方向性(2/2)

HITACHI
Inspire the Next

- 前頁の事項に加え、産業用制御システム、NICEイニシアチブを通じた人材教育・訓練、SP 800-63の改訂等を含むアイデンティティ・アクセス管理関連の標準策定も盛んに推進されている。

重点領域	方向性	取組み例
産業用制御システム (Industrial Control Systems)	ICS特有の性能、信頼性、安全性の要件に対応するための従来のITセキュリティ対策の調整方法についてのガイダンスを提供することで、悪意のある攻撃、機器の故障、その他の脅威に対するコンピュータ制御システムの脆弱性を業界が低減できるよう支援している。	• 一般的なICSサイバーセキュリティガイドとして、SP 800-82 Rev.3を策定中 • 製造業者がICSをデータ完全性攻撃等から保護できるよう、実用的なソリューション例を開発 • 分散型エネルギー資源システムと配電設備との間におけるデータ交換のセキュリティを向上させるために、エネルギー企業を支援 • NISTのサイバーセキュリティ・フレームワーク製造業プロファイルを策定、適用促進
人材教育、訓練 (Workforce education & training)	National Initiative for Cybersecurity Education (NICE) は、サイバーセキュリティの教育、訓練、人材育成に焦点を当てた政府、学界、民間セクターのパートナーシップであり、サイバーセキュリティ教育、訓練、人材育成の強固なネットワークとエコシステムを活性化し、促進している。	• NICE サイバーセキュリティ人材フレームワークの策定及び適用支援 • サイバーセキュリティ雇用ヒートマップを通じて、全米のサイバーセキュリティ人材の必要性と供給を可視化
アイデンティティ・アクセス管理 (Identity & access management)	データ保護、プライバシー、セキュリティの要として、適切な人、機器、データ、プロセスが適切なリソースに適切なタイミングでアクセスできるようにするための研究、ガイダンス、技術移行活動を行う。	• 連邦職員や請負業者向けの「連邦職員の個人ID検証(PIV)」標準の第3版を策定 • SP 800-63 (デジタルアイデンティティ・ガイドライン)の第4版草案を策定 • モバイル運転免許証(mDL)アプリケーションの国際標準への貢献、標準に基づくリファレンス実装の開発

[参考] NIST CYBERSECURITY & PRIVACY PROGRAM
(https://www.nist.gov/system/files/documents/2022/07/21/Extended%20Cybersecurity%20Vitals%20Fact%20Sheet.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3-2. 標準化の優先領域 / 日本における取組み(1/2)

HITACHI
Inspire the Next

- NISTの優先領域のそれぞれに対して、主にサイバーセキュリティ戦略等で示されるように、国内でも複数の省庁が連携しつつ一定の取組みが推進されている。

重点領域	日本での取組み(サイバーセキュリティ戦略等を参照)	
	主要担当省庁	標準化やそれに係る普及、研究開発等に係る取組み
暗号 (Cryptography)	NISC、内閣府、総務省、文部科学省、経済産業省	• 耐量子計算機暗号や量子暗号等に関する先進的な研究の推進や、その事業化・標準化等 • IoT 等のリソースの限られたデバイスにおいても適用可能な軽量な暗号技術の確立 • 量子通信・暗号に関する研究開発暗号技術の安全性・信頼性確保や普及促進等に関する検討(例：耐量子計算機暗号、軽量暗号等に関するガイドラインの作成)
リスク管理の強化 (Enhanced risk management)	経済産業省	• CPSF等に基づく産業分野別・産業横断的なガイドライン等の策定 • 機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼性の確保を図るための仕組みの構築
	NISC、重要インフラ所掌官庁	• 「重要インフラの情報セキュリティ対策に係る第4次行動計画」の積極的改定、官民連携に基づく重要インフラ防護の一層の強化
	総務省	• 「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づくセキュリティ対策の着実な実施
実用的ソリューション (Practical solutions)	経済産業省	• セキュリティ製品・サービスの有効性検証を行う基盤整備や実環境における試行検証 • 一定の基準を満たすセキュリティサービスの審査・登録・リスト化や政府機関における利用促進 • 検証ビジネスの市場形成に向けた、検証事業者の信頼性を可視化する取組の検討
	NISC、内閣府、総務省、経済産業省	• サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤構築 • IoT システム・サービス、サプライチェーン全体での活用に向けた基盤の開発・実証の取組について、様々な産業分野を念頭に置いた社会実装を促進 • 政府機関における新技術の活用に向けた技術検討の促進

[参考] サイバーセキュリティ戦略（閣議決定）
(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3-2. 標準化の優先領域 / 日本における取組み(2/2)

HITACHI
Inspire the Next

- NISTの優先領域のそれぞれに対して、主にサイバーセキュリティ戦略等で示されるように、国内でも複数の省庁が連携しつつ一定の取組みが推進されている。

重点領域	日本での取組み(サイバーセキュリティ戦略等を参照)	
	主要担当省庁	標準化やそれに係る普及、研究開発等に係る取組み
モノのインターネット (Internet of Things)	NISC、内閣府、総務省、文部科学省、経済産業省	• 不正なプログラムや回路が仕込まれていないことを確認するための検証技術の研究開発・実用化 • サイバー攻撃の観測・把握・分析技術や情報共有基盤の強化 • サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤構築
	経済産業省	• IoT製品に対するセキュリティ適合性評価制度構築に向けた検討の推進
産業用制御システム (Industrial Control Systems)	NISC、警察庁、総務省、経済産業省等	• IT システムやサービスの信頼性・安全性を確認するための技術検証体制の整備 • 情報共有・報告・被害公表の的確な推進、制御システムのインシデント原因究明機能の整備等
	NISC、総務省、文部科学省、経済産業省	• 実務者層・技術者層の育成に向けた資格制度の整備・改善、若年層向けのプログラムや制御系システムに携わる実務者を対象とするプログラムの実施、演習環境の提供、学び直しの促進
	経済産業省	• 工場セキュリティガイドラインの策定及び普及の推進
人材教育、訓練 (Workforce education & training)	NISC、総務省、経済産業省	• 「プラス・セキュリティ」知識を補充できる環境整備(例：先導的・基盤的なプログラムの提供、趣旨に適うプログラムを一覧化したポータルサイト等、法令への理解を深めるツール等の活用促進) • 企業・組織内での機能構築、人材の流動性・マッチングに関する取組(例：人材 ニーズに係る実態把握、実際のインシデントを踏まえた普及啓発、手引き資料の活用促進、企業・組織内での機能構築や人材の活躍等の先進事例の収集・整備、ポータルサイト等を通じた積極的な発信) • 地域における「共助」の取組や産業界と教育機関との連携促進・エコシステム構築
	NISC、総務省、文部科学省、経済産業省	• 社会全体でサイバーセキュリティ人材を育成するための共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう産学に開放
アイデンティティ・アクセス管理 (Identity & access management)	デジタル庁	• マイナンバーや法人 番号など個人・法人を一意に特定し識別する ID 制度や電子署名、商業登記電子証明書 など情報とその発信者の真正性等を保証する制度(例：行政手続におけるオンラインによる本人確認の手法に関するガイドライン)の企画立案、普及を推進

[参考] サイバーセキュリティ戦略（閣議決定）
(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3-2. 標準化の優先領域 / 取組み状況の比較

HITACHI
Inspire the Next

- 7つの重点領域に係る差異としては、複数省庁による分業(日本)、標準化と結びついた製品・サービスの有効性検証(米国)、政府調達の活用(米国)等があると考えられる。

重点領域	米NISTの取組み	日本における主な取組み	日米の取組み比較
暗号 (Cryptography)	• 暗号アルゴリズムの設計と検証 • ポスト量子暗号(PQC)の標準化 • 軽量暗号の標準化	• 耐量子計算機暗号や量子暗号等に関する研究の推進や、その事業化・標準化等[複数省庁]	日米とも量子分野や軽量暗号に関する研究開発及び標準化の取組がなされている。
リスク管理の強化 (Enhanced risk management)	• リスク管理フレームワークの策定・改定と適用の促進(CSF、PF、RMF等)	• CPSF等に基づくガイドライン等の策定[経産省] • 行動計画の積極的改定[NISC] • 自治体ガイドライン推進[総務省]	日本では複数省庁にて多岐にわたる分野のガイドライン策定が分業されている。
実用的ソリューション (Practical solutions)	• NCCoEにおける官民パートナーシップの推進、SP1800シリーズの発行	• セキュリティ製品・サービスの有効性検証を行う基盤整備[経産省] • CYNEX[総務省/NICT]	日本でも環境整備が進められているが、SP1800シリーズのような標準化と連動した活動とはなっていない。
モノのインターネット (Internet of Things)	• IoT Device Cybersecurity Core Baselineの策定 • 連邦政府向けプロファイルの策定	• IoT製品に対するセキュリティ適合性評価制度構築[経産省]	日米ともIoT機器の認証・ラベリングの取組みが推進されるが、米国では政府調達関連の取組みも志向される。
産業用制御システム (Industrial Control Systems)	• SP 800-82 Rev.3の策定 • 実用的なソリューション例の開発 • CSF製造業プロファイルの策定	• 工場ガイドラインの策定[経産省] • システム等の信頼性を確認する技術検証体制整備[複数省庁]	日米ともガイドラインの策定に加え、ソリューション例の開発や技術検証等、実装面での支援も提供している。
人材教育、訓練 (Workforce education & training)	• NICE サイバーセキュリティ人材フレームワークの策定及び適用支援 • 全米のサイバーセキュリティ人材のニーズと供給の可視化	• 「プラス・セキュリティ」知識を補充できる環境整備 • 人材の流動性・マッチングに関する取組 等[複数省庁]	日米とも人材のニーズと供給の可視化、マッチングに関する取組がなされている。
アイデンティティ・アクセス管理 (Identity & access management)	• 「連邦職員の個人ID検証(PIV)」標準第3版の策定 • SP 800-63 第4版草案の策定	• 本人確認の手法に関するガイドライン策定等[デジタル庁]	日米ともにデジタルアイデンティティに関する取組みを行っているところ、PIV等のセキュリティクリアランスに係る標準化については米国が先行している。

© Hitachi, Ltd. 2024. All rights reserved.

4. 日本における標準化に係る機関等のあるべき姿の検討

© Hitachi, Ltd. 2024. All rights reserved.

標準化機能等の強化を通じて実現したい姿

HITACHI
Inspire the Next

- 標準の策定・改定だけでなく、標準の普及及びそれと連動した産業創出に向けた動きを並行して講じていくことにより、策定標準を軸としたセキュリティ向上サイクルの確立を目指す。

1. 標準の策定・改定

サイバーセキュリティ関連の標準を策定し、継続的に保守管理していく体制を確保する

講じるべき施策の例

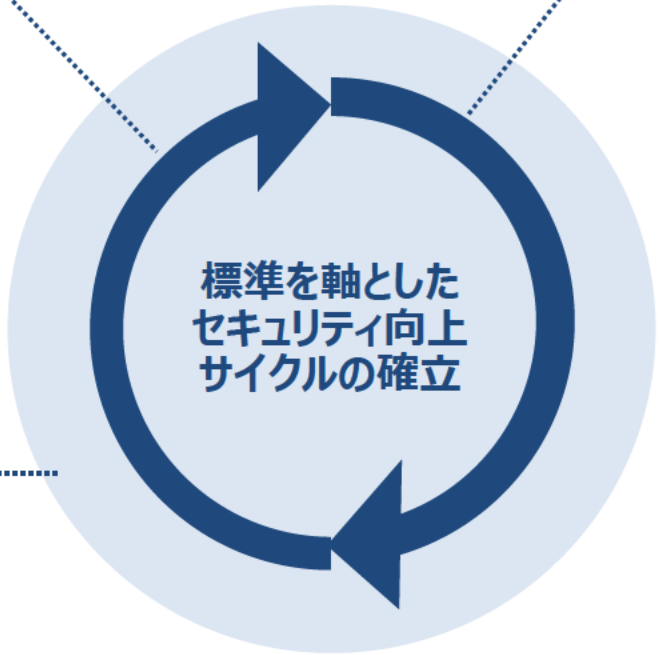
1-1. 法律上の措置を含めたセキュリティ標準策定機能の強化
1-2. セキュリティ標準に係る政府内での調整機能の確立
1-3. セキュリティ標準体系の整備

2. 標準の普及及びそれと連動した産業創出

策定された標準を官民に普及しつつ、標準準拠を支援する技術開発等を通じてデジタル産業基盤の強化を図る。

講じるべき施策の例

2-1. 標準準拠を促進する技術の開発や実証に係る官民連携の推進
2-2. 規制による強制またはボランタリーな対策の普及推進



3. リソースの確保・維持

1. 及び2. を実行するにあたり必要なリソース(予算、人員等)を継続的に確保・維持する。

講じるべき施策の例

3-1. セキュリティ標準の策定・維持を専門的に取扱う部門の設立
3-2. 当該部門に必要な予算及び人員の確保

© Hitachi, Ltd. 2024. All rights reserved.

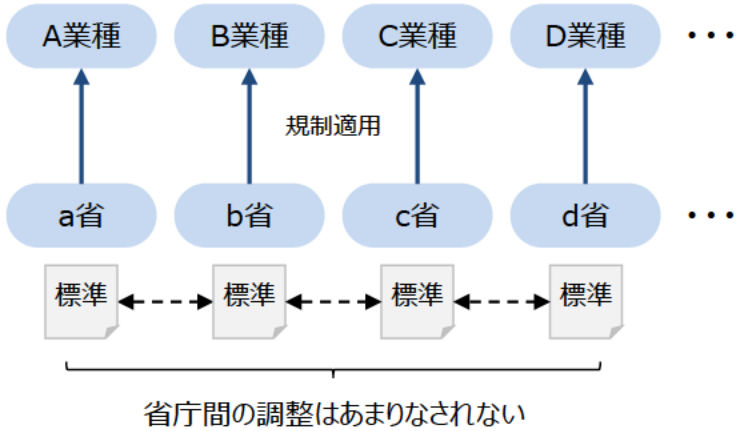
4-1. 標準の策定・改定 / 概要

HITACHI
Inspire the Next

- 現状各省庁で分散して実施されている標準策定業務をIPA等の十分な技術的能力及び専門的な知識経験を有する機関に一元化し、適用される標準群を体系化することで、サイバーセキュリティ関連の標準を策定・普及し、継続的に保守管理していく体制の確保を図る。

現状の姿

- 各業所管省庁が適宜関係団体と連携しつつ、個別に規制及び標準を策定している
- 策定に係るリソースが全体に広く分散している
- 業種間等で内容の調整はあまりなされない

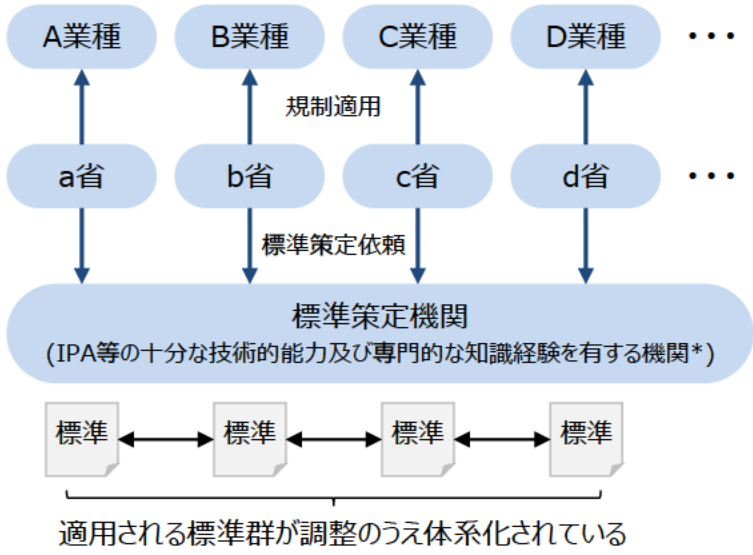


目指すべき姿に向けて講じるべき施策(例)

- 標準策定機関への標準策定権限の付与
- 機関への依頼につながる省庁間協議体制の確立
- 機関にて策定・維持する標準体系の整備
- 標準策定を推進するにあたり十分なリソースの確保

目指すべき姿

- 各業所管省庁が規制監督の役割を担いつつ、技術標準の策定機能を標準策定機関(IPA等の十分な技術的能力及び専門的な知識経験を有する機関)へと一元化し、リソースを集約している
- 適用される標準群が体系化されている



* 独立行政法人情報処理推進機構その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人 [基本法第31条1項]

© Hitachi, Ltd. 2024. All rights reserved.

4-1. 標準の策定・改定 / 標準策定機関(IPA)への権限付与

HITACHI
Inspire the Next

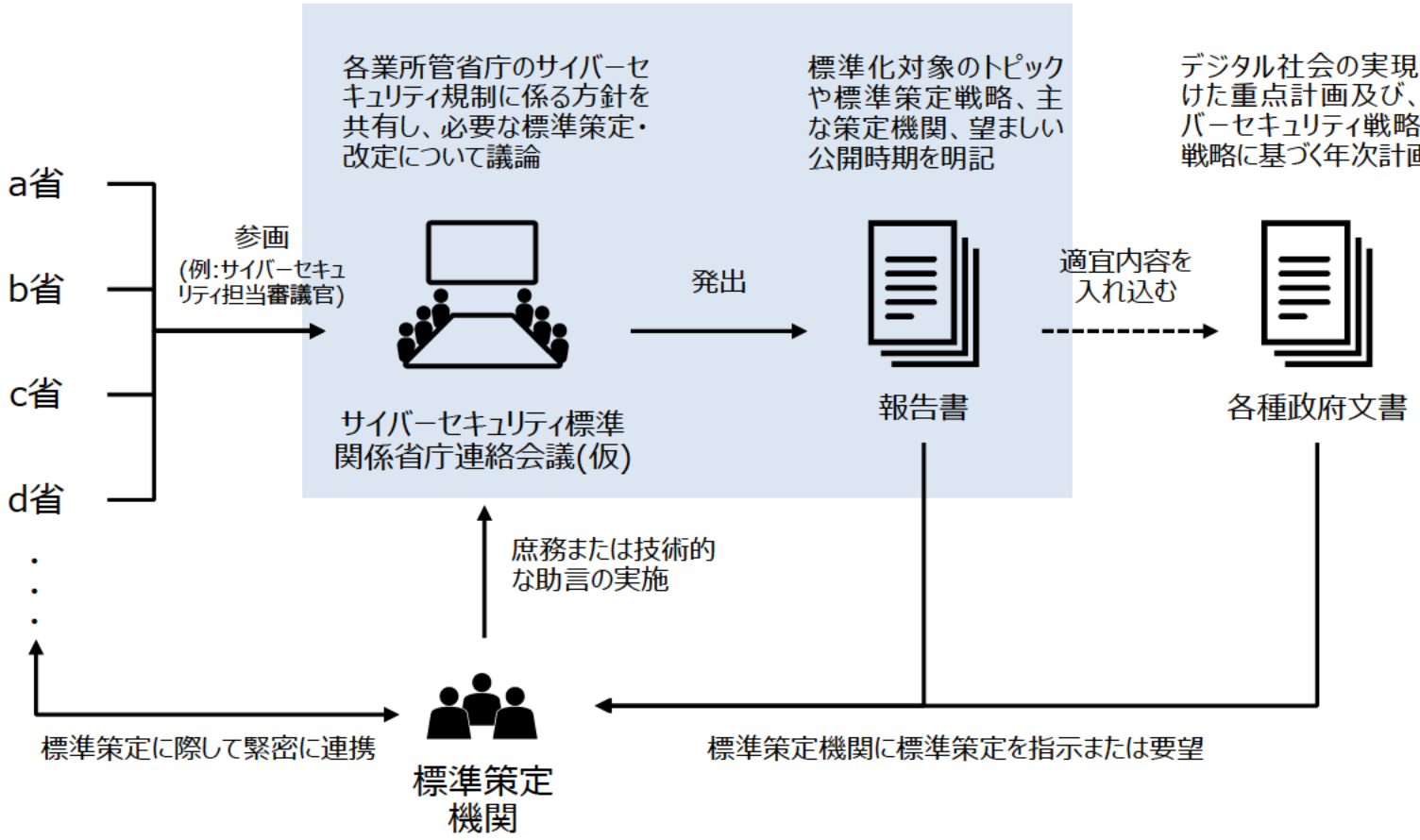
- 情報処理の促進に関する法律に規定されるIPAの業務及び、サイバーセキュリティ基本法における基準の策定に関する権限について必要な改正を実施することで、サイバーセキュリティ関連の標準を策定・普及し、継続的に保守管理するうえでIPAに必要な権限を付与する必要がある。

	現状	目指すべき姿
情報処理の促進に関する法律 (昭和四十五年法律第九十号)	• 「第四章　独立行政法人情報処理推進機構」の「第三節　業務等」にサイバーセキュリティに関する標準の策定及び改定等の維持に係る業務が位置づけられていない。 • 政府内でサイバーセキュリティ標準の策定や維持に係る調整を実施する際の役割(例：連絡会議の事務局)について規定されていない。	• 第51条(業務の範囲等)に新たな項を設け、サイバーセキュリティに関する標準の策定及び改定等の維持に係る業務を追記する。 • 第51条(業務の範囲等)に新たな項を設け、サイバーセキュリティ標準の策定や維持に係る調整を実施する会議体の庶務または技術的な助言等をIPAが担う旨を追記する。 ※ 上記のような会議体については、既存のCISO等連絡会議と同様に、サイバーセキュリティ基本法施行令第4条の規定に基づき、適宜設置され得る。
サイバーセキュリティ基本法 (平成二十六年法律第百四号)	• 国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成(第26条1項2号)について、サイバーセキュリティ戦略本部に権限が割り当てられている。 • 一方で、当該業務について、事務の委託(第31条)が規定されておらず、IPAに実施の権限が割り当てられていない。 • 重要インフラ事業者向けの基準の策定については、単に主体が「国」とされており、特定の機関等への権限付与は含まれていない。	• 第31条(事務の委託)第1項にて、「国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成」についてもIPA等の十分な技術的能力及び専門的な知識経験を有する機関に事務の一部を委託できるよう規定を改定する。 ※ 現状では、第26条1項2号に定めるサイバーセキュリティ戦略本部が担う事務のうち、IPAに委託できるのは「独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準に基づく監査に係るもの」に限られている。

© Hitachi, Ltd. 2024. All rights reserved.

4-1. 標準の策定・改定 / 省庁間の協議体制の確立

- 現状開催されているCISO等連絡会議では、政府機関におけるサイバーセキュリティ対策の推進が目的とされ、民間事業者も対象に含めたサイバーセキュリティ標準に係る検討がスコープとされていないため、新たに会議体を定義する等して、サイバーセキュリティ標準策定の方向性等に係る省庁間の協議体制を確立する必要がある。

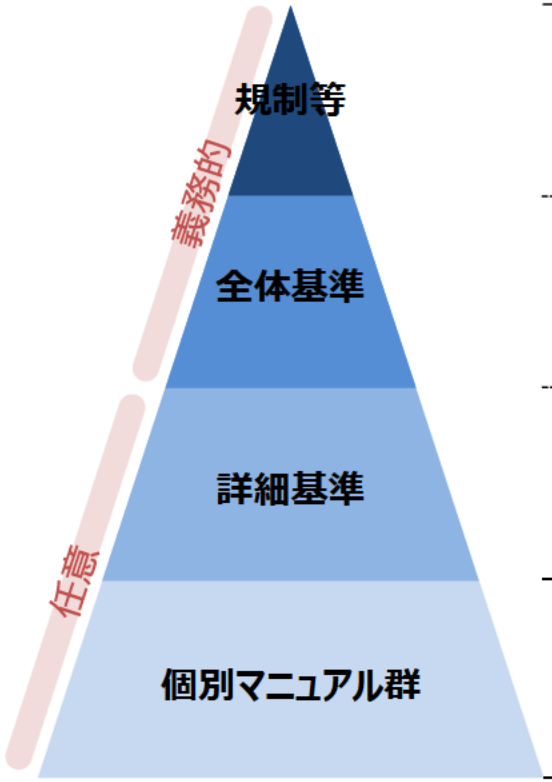


© Hitachi, Ltd. 2024. All rights reserved.

4-1. 標準の策定・改定 / セキュリティ標準体系の整備(1/3)

HITACHI
Inspire the Next

- セキュリティ標準の体系として、事業者に対策義務を課したりする「規制等」を頂点として、規制等の遵守に必要なハイレベルな要求事項を規定する「全体基準」、対策基準を全体としてより詳細に補完する「詳細基準」、対策基準や詳細基準に対応する対策の実装例等について個別具体的に解説する「個別マニュアル群」を整備していくことが望まれる。



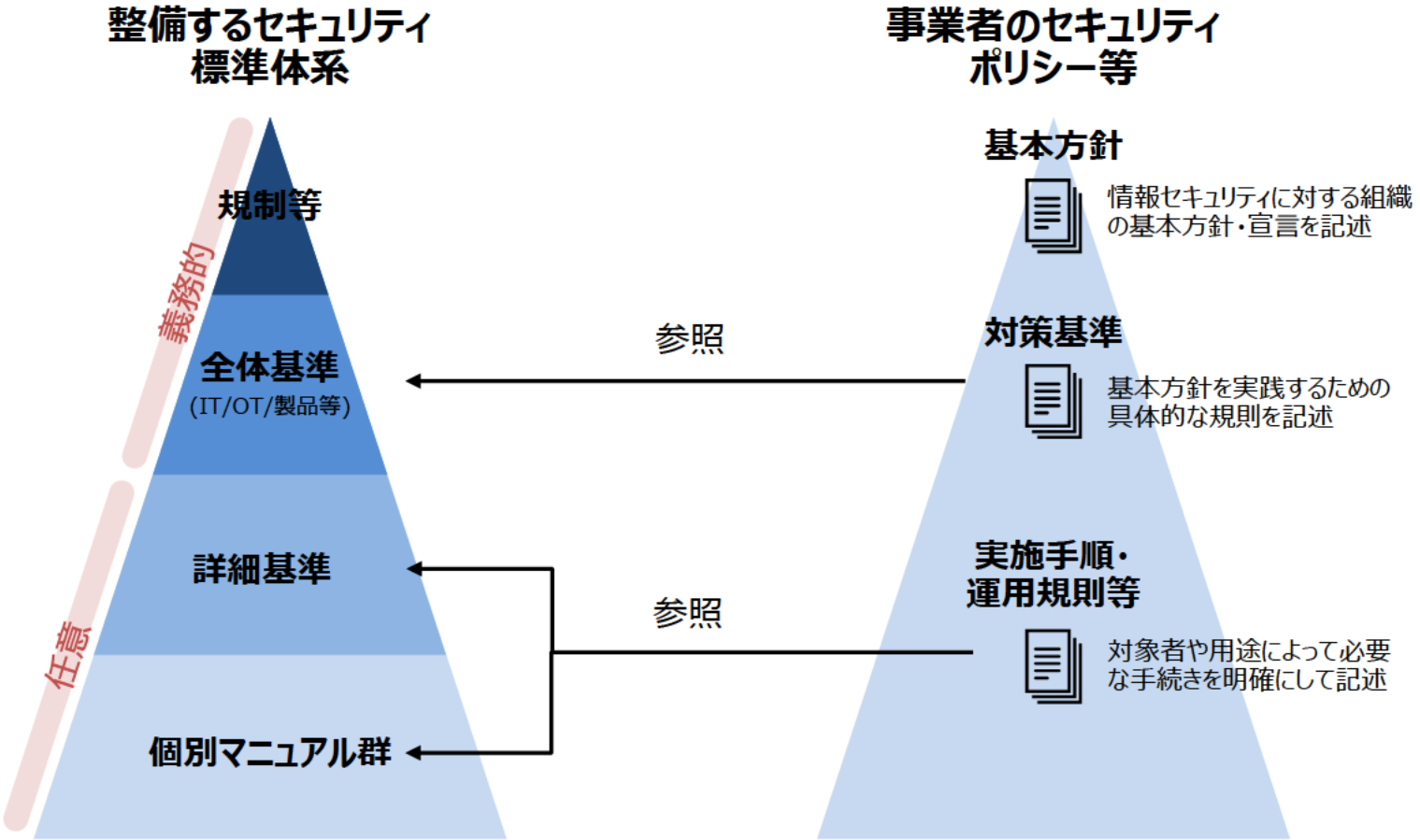
概要	具体例
特定の事業者に対して、一定のセキュリティ対策の実施を強制したり、推奨したりするもの	• サイバーセキュリティ基本法 14条 • 政府機関等のサイバーセキュリティ対策のための統一規範 • 各業法及び施行規則等
規制等の対象となっている事業者が遵守すべきハイレベルな要求事項を規定するもの	• 政府機関等のサイバーセキュリティ対策のための統一基準 • サイバーフィジカルセキュリティ対策フレームワーク(CPSF)
対策基準の遵守事項に対応した基本的な対策事項を例示したもの	• 政府機関等の対策基準策定のためのガイドライン • CPSFに係る分野別ガイドライン(ビル、スマートホーム、自動車、工場等)
対策基準や詳細基準に対応する対策の実装例等について個別具体的に解説したもの	• 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル • 政府機関等における情報システム運用継続計画ガイドライン

© Hitachi, Ltd. 2024. All rights reserved.

4-1. 標準の策定・改定 / セキュリティ標準体系の整備(2/3)

HITACHI
Inspire the Next

- 各事業者が整備する基本方針に基づく対策基準及び、実施手順・運用規則等の策定にあたり、整備するセキュリティ標準体系の文書が参照される。



© Hitachi, Ltd. 2024. All rights reserved.

4-1. 標準の策定・改定 / セキュリティ標準体系の整備(3/3)

HITACHI
Inspire the Next

- サイバーセキュリティ基本法に基礎を有する政府統一基準と重要インフラ関連規定の枠組みを維持しつつ、基本法で規定する範囲外であり庶務6省庁*が自身の所掌事務の範囲で整備するものについてCPSFを頂点とする標準体系となるよう整理をすることが一案。
- 大枠が定まった後に更なる体系の詳細化が必要。

	基本法に基づきNISC及び各省で整備するもの			基本法で規定する範囲外であり、庶務6省庁*が自身の所掌事務の範囲で整備するもの	
規制等	政府機関等 統一規範 (第6条3項)	サイバーセキュリティ基本法 (第14条)	各業法・ 施行規則等	現状特にないが、今後の動向に合わせて適宜設定が必要	
全体基準 (遵守すべき事項の全体を示すもの)	政府機関等 統一基準	重要インフラのサイバーセキュリティに係る安全基準等策定指針	施行規則等で指定された安全基準	サイバーフィジカルセキュリティ対策フレームワーク(CPSF)	
詳細基準 (全体基準を包括的に補足するもの)	政府機関等の対策基準策定のためのガイドライン	業種ごとの安全基準 (14業種)	安全基準遵守のためのガイドライン	分野別ガイドライン (府省庁、重要インフラ以外)	横断的ガイドライン (制御システム、IoT等)
個別マニュアル (特定分野の対策について詳述するもの)	個別マニュアル群 (基本的には特定の業種でなく、SP 800シリーズ等のような様々な分野からの参照が有効となる内容を目指すが、対象となる業種によってあまりに内容の差異が大きい場合には分野別のマニュアルとして整備する。)				

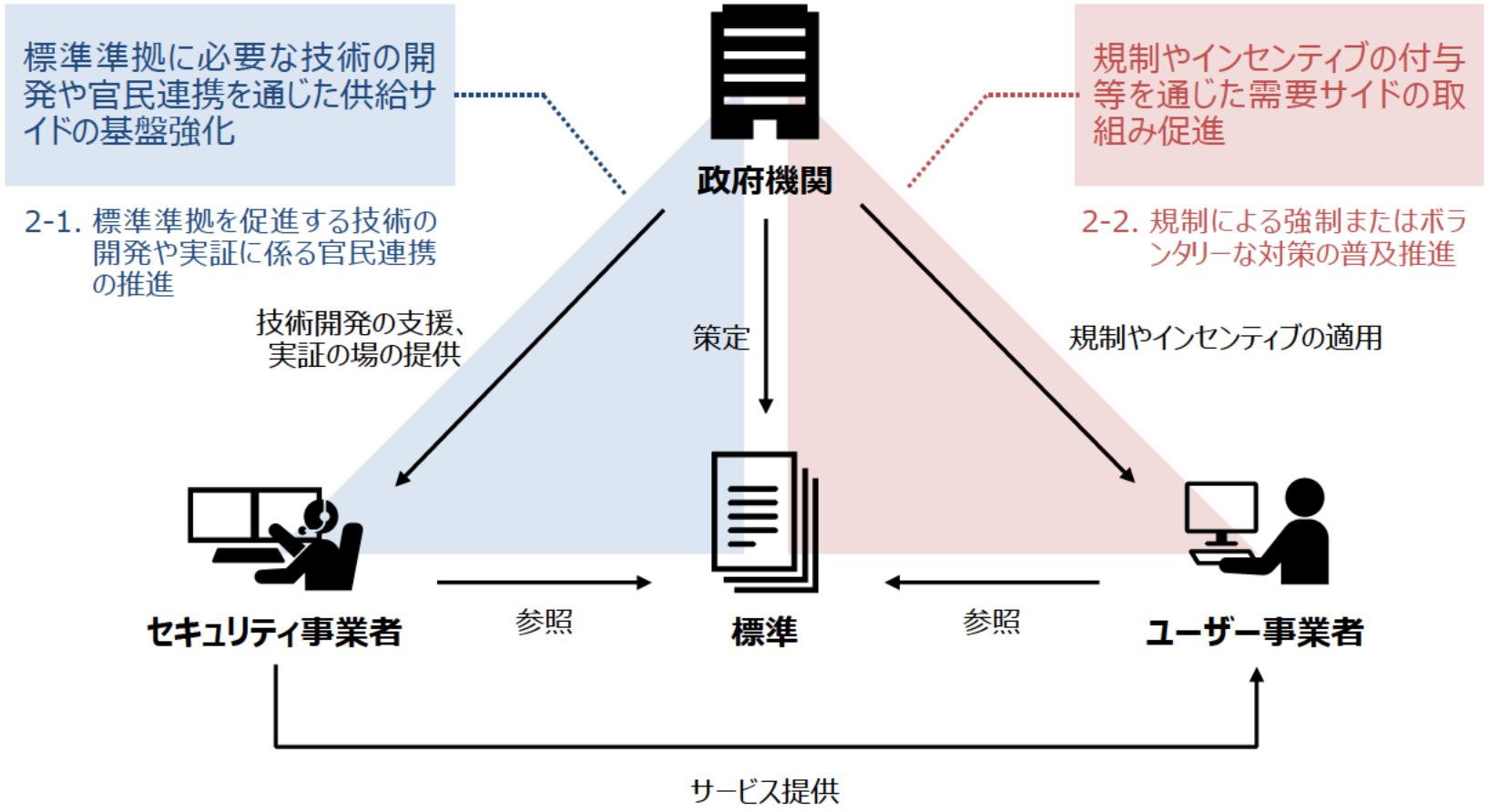
標準策定機関に策定及び維持を委託(一案)

* 庶務6省庁とは、警察庁、総務省、経済産業省、デジタル庁、外務省、防衛省を指す。

© Hitachi, Ltd. 2024. All rights reserved.

4-2. 普及及び産業創出 / 概要

- 供給サイドの基盤強化と需要サイドの取組み促進を並行して実施することで、策定された標準を官民に普及しつつ、標準準拠を支援する技術開発等を通じてデジタル産業基盤の強化を図る。



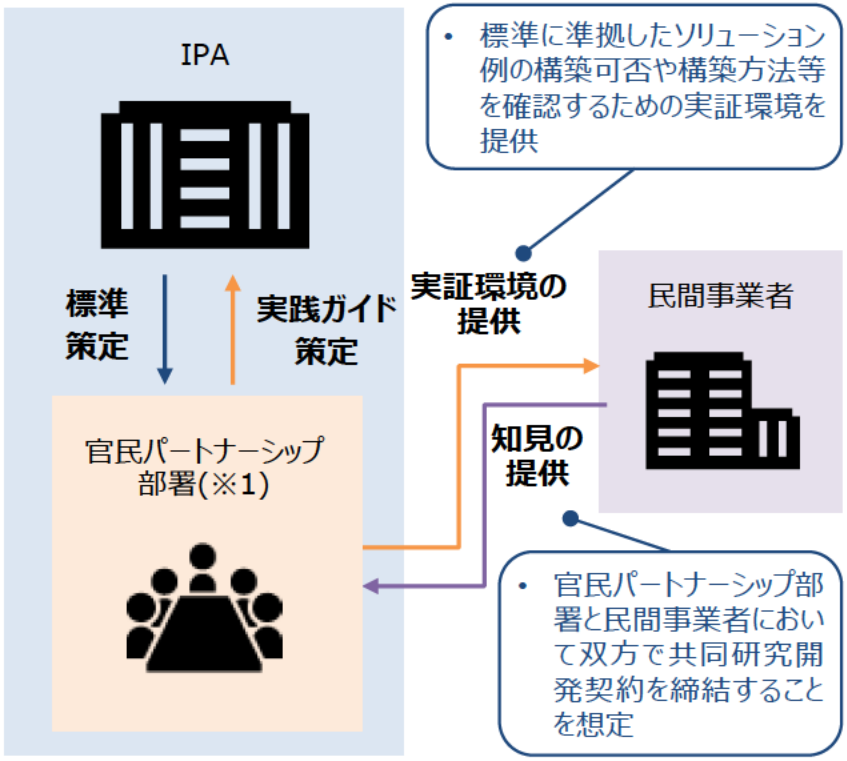
© Hitachi, Ltd. 2024. All rights reserved.

4-2. 普及及び産業創出 /標準準拠を促進する技術開発、官民連携

HITACHI
Inspire the Next

- 標準の社会実装に向けて、IPA等に標準策定部署に加えて、官民パートナーシップ部署を新たに設立し、標準に準拠した実践ガイドを民間事業者と協力して作成する場を整備することも一案。
- 場を整備することによって、民間事業者側で標準に準拠したソリューション(製品)の導入が進み、結果的に民間事業者全体のセキュリティ機能を高めることが可能ではないか。

各団体の関係性



※1:必ずしもIPAの部署である必要はない点に留意いただきたい。

成果物及びその効果

成果物

- **標準に準拠した実践ガイド**
  - ✓ IPAが策定した標準を民間事業者が実装する場合のソリューション例
  - ✓ 上記ソリューション例を構築するための製品のインストール、構成、および統合に関する重要な手順

効果

<民間事業者側の効果>

- [ユーザ側]実践ガイドを参照することによって、標準に準拠したソリューション(製品)を円滑に導入可能。
- [ベンダ側]実践ガイドに自社のソリューション(製品)が掲載されることによって、ユーザに対するソリューション(製品)の訴求力を高めることが可能。

<政府側の効果>

- 民間事業者のソリューションが標準に準拠可能なこと、また、その実装手順を示すことで、民間事業者側での標準の実装が進展。その結果、民間事業者側でのセキュリティ機能が高めることが可能。

© Hitachi, Ltd. 2024. All rights reserved.


Hitachi Social Innovation is
POWERING GOOD

HITACHI
Inspire the Next

別紙４　委託調査に関する最終報告

© Hitachi, Ltd. 2024. All rights reserved.

目次

1. 官民連携センターに係る国内外の動向 …… 2
2. 機微技術保有組織のサイバーセキュリティの確保方策に係る動向 …… 56
3. ITベンダー向けの規制動向 …… 138
4. ITベンダーとユーザー間の紛争に関する判例の収集 …… 188

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

1. 官民連携センターに係る国内外の動向

© Hitachi, Ltd. 2024. All rights reserved.

調査目的及び調査対象(1/2)

HITACHI
Inspire the Next

- 調査項目(1)では、サイバーセキュリティを研究テーマとした官民連携センターを対象として、当該センターが持つ機能や特徴等を調査した。

調査目的

- サイバーセキュリティを対象とした海外の官民連携センターの設置状況及びその内容についての情報収集を通じて、官民連携センターが持つ機能や特徴、機能を果たすための具体的な取組み及びその取組みの結果、民間企業に対するサポートの内容を理解する。

調査対象

分類		調査対象	概要
米国		The National Cybersecurity Center of Excellence (NCCoE)	2012年、メリーランド州に設立。NISTの一部。業界グループ、政府機関、教育機関のメンバからなり、協働してサイバーセキュリティの問題に取り組む。
		Mach37	2013年、バージニア州に設立。バージニア州から資金提供を受け、バージニアイノベーションパートナーシップの一部門として設立。サイバーテクノロジー企業の形成と成長を可能とするとされている。2020年よりベンチャースコープ社によって運用。
欧州	EU	The Cybersecurity Competence Centre	2020年12月に設立について欧州委員会にて合意。国内・越境のサイバーセキュリティオペレーションセンターのキャパシティビルディングの支援やサイバーセキュリティ関連規制への法令順守支援等への活用を想定。
	オランダ	The European Network for Cyber Security	2012年、ハーグに設立。オランダの協同組合法のもと設立され、欧州において安全で重要なエネルギーグリッドやインフラを展開するため、重要インフラの関連企業・機関とセキュリティーの専門家を集める。

© Hitachi, Ltd. 2024. All rights reserved.

調査目的及び調査対象(2/2)

HITACHI
Inspire the Next

調査対象 (続き)

分類		調査対象	概要
欧州	英国	LONDON CYBER INNOVATION CENTRE	2018年、ロンドン(オリンピックセンター跡地)に設立。政府が主導し、新技術を開発する場を企業へ提供。
	ロシア	Skolkovo Innovation Center	2010年にロシアの首都モスクワの郊外のスコルコボにイノベーション拠点を設立。中核を成すテクノパークの面積は10万平米近くに達する。「バイオテクノロジー」「エネルギー」「原子力」「宇宙通信」「IT(情報技術)」の５つの分野でベンチャー企業の育成を目指している。
その他	イスラエル	Cyberspark	2018年、ベエルシェバに設立。国家サイバー局直下の研究開発機関。スタートアップ企業、多国籍企業、大学、ベンチャーキャピタルから構成され、共同研究とスタートアップ支援を目的とする。
	韓国	国家サイバーセキュリティ協力センター	2022年11月に京畿道(キョンギド)城南市(ソンナムシ)板橋(パンギョ)に設立。官民がサイバー脅威の情報や技術を共有し、共同で対応するための拠点として設立された。国家情報院、科学技術情報通信部（部は省に相当）、国防部などの関連機関や、AhnLab(アンラボ)、EST Security(イーストセキュリティ)等のITセキュリティ企業の専門の技術者が共に業務にあたる。

© Hitachi, Ltd. 2024. All rights reserved.

調査項目及び整理の観点等

HITACHI
Inspire the Next

- 個々の調査対象ごとに、基礎情報として一般的な事項を整理した上で、以下を整理した。
  - 当該センターが持つ機能
  - 当該センターが持つ特徴
  - 機能を果たすための具体的な取組み及びその取組みの成果
  - 民間企業に対するサポートの内容

分類	調査項目		整理の観点等
1 一般的な事項	1-1	設立年度	-
	1-2	設立場所(国・地域)	-
	1-3	参加団体(民間企業側や政府側の主な参加団体)	-
	1-4	規模(参加団体数/広さ/予算)	(可能であれば、出資比率も整理予定)
	1-5	設立目的	-
	1-6	ミッション/ビジョン	-
2 詳細情報	2-1	官民連携センターが持つ機能	• 技術の研究開発機能 • ビジネス創出機能 • 人材育成機能
	2-2	官民連携センターが持つ特徴	• 人材面(例:スタートアップ企業とベンチャーキャピタルをマッチングする仕組みがある) • 設備面(例:高額な設備を共同で利用可能) • 金銭面(例:政府からの恒常的な支援がある) • 情報面(例:更なる集積効果を生み出す仕掛けがある)
	2-3	機能を果たすための具体的な取組み及びその取組みの成果	• 取組みの全体像(ソフト面/ハード面) ※うまくいかなかった取組み(及び反省点)を含む • その取組みの成果(例:論文公開数、ビジネスの創出数、人材の増減)
	2-4	民間企業に対するサポートの内容(インセンティブの内容)	• 人材面でのサポート(例:大学機関との共同研究支援) • 金銭面でのサポート(例:費用の一部軽減) • 設備面でのサポート(例:高度な設備の利用支援) • 情報面でのサポート(例:研究開発論文の入手支援)

© Hitachi, Ltd. 2024. All rights reserved.

1. 官民連携センターに係る国内外の動向

1.1 一般的な事項
1.2 詳細情報

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (1/4)

HITACHI
Inspire the Next

分類		調査項目		調査結果
1 米国	The National Cybersecurity Center of Excellence (NCCoE)	1-1	設立年度	2012年
		1-2	設立場所(国・地域)	米国・メリーランド州
		1-3	参加団体	産業界、政府機関、教育機関のメンバが参加。なお、NCCoEには126名が在籍。
		1-4	規模(参加団体数/広さ/予算)	センターを運営するための官民パートナーシップを確立するために1000万ドル(2012年/NIST予算)
		1-5	設立目的	最先端のサイバーセキュリティ技術導入を加速させることを目的とする。
		1-6	ミッション/ビジョン	**ミッション:**安全なテクノロジーの採用を加速する(イノベーターと協力し、ビジネスニーズに対応する標準ベースのサイバーセキュリティ機能を提供する) **ビジョン:**サイバーセキュリティを推進する(技術革新を促し、経済成長を促進する安全なサイバーインフラを提供する。) **目標:**実用的なサイバーセキュリティを提供する/サイバーセキュリティの採用率の向上させる/効果的なイノベーションを加速させる
2	Mach37	1-1	設立年度	2013年(2020年にスタートアップコンサルティング会社のベンチャースコープによって完全に所有および運営)
		1-2	設立場所(国・地域)	米国・バージニア州
		1-3	参加団体	スタートアップ企業
		1-4	規模(参加団体数/広さ/予算)	85のサイバー企業が起業(83%が現在も事業を継続中) ※プログラムへの参加団体数は管見の限り、みつけることができなかった。
		1-5	設立目的	バージニア州からの資金提供を受けて、バージニア州に本拠を置く革新的技術センター(CIT)の一部門として設立。
		1-6	ミッション/ビジョン	**目標:** • ビジネスモデルの仮定に挑戦し、理論を有料の顧客との検証済みのビジネスモデルに変える。 • 業界の専門家とつながる。 • 投資と成長に備える。 • サポートし、あなたの説明責任のパートナーになる。 • 他のセキュリティ組織へのテクノロジーの移行と採用を加速する。 • サイバー世界をより安全な場所にするのを助ける。

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (2/4)

分類		調査項目		調査結果
3 欧州	The Cybersecurity Competence Centre	1-1	設立年度	2021年
		1-2	設立場所(国・地域)	欧州(本部はブカレスト)
		1-3	参加団体	各国の調整センター(1カ国1団体で、政府機関が調整センターの役割を担う)
		1-4	規模(例:参加団体数/広さ/予算)	在籍スタッフ:14名(2023年時点、2024年には40名に増員予定) ブカレスト工科大学内に設置
		1-5	ミッション/ビジョン	<ミッション> サイバーセキュリティ技術コミュニティの能力を強化し、経済と社会をサイバー攻撃から保護し、研究の卓越性を維持し、かかる分野におけるEU産業の競争力を強化する。
4	Plexal Innovation Centre	1-1	設立年度	2017年(2012年ロンドンオリンピックの跡地を活用)
		1-2	設立場所(国・地域)	英国
		1-3	参加団体(民間企業側や政府側の主な参加団体)	参加したスタートアップ企業:72社 支援企業における投資調達額:2億1,000万ポンド(約384億円)
		1-4	規模(例:参加団体数/広さ/予算)	68,000平方フィート(参考:6,317㎡)
		1-5	ミッション/ビジョン	<ビジョン> テクノロジーを社会にとってより良いものにすること。 ・コラボレーションを通じてイノベーションの課題を解決 ・コンサルティング・サービスと最先端のワークスペースを提供し、適切なパートナーを探し出す ・新興の科学技術全般にわたって起業家、新興企業、スケールアップ企業を支援 ・5つのコア・プロダクト(戦略、発見、検証、イノベーション・プログラム、エコシステム)を通じて、クライアントの課題を解決 ・情報・防衛、政府、金融サービス、通信など、さまざまな分野で事業を展開

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (3/4)

HITACHI
Inspire the Next

分類		調査項目		調査結果
5 欧州	The European Network for Cyber Security	1-1	設立年度	2012年
		1-2	設立場所(国・地域)	オランダ
		1-3	参加団体	欧州の大手送電網事業者 (欧州内の配電系統運用者もしくは送電系統運用者であれば参加可能)
		1-4	規模(例:参加団体数/広さ/予算)	参加している大手送電網事業者数:25社(2023年10月時点)
		1-5	ミッション/ビジョン	欧州の重要なエネルギー・グリッドとインフラを安全に配備するために、重要インフラの関係者とセキュリティの専門家を集め、知識の共有を通じて、再生可能エネルギーへの安全な移行を可能にし、サイバー攻撃から社会を守る。
6	Skolkovo Innovation Center	1-1	設立年度	2010年9月(スコルコボについての連邦法が成立)
		1-2	設立場所(国・地域)	ロシア
		1-3	参加団体(民間企業側や政府側の主な参加団体)	スコルコボのプロジェクトに参加しているスタートアップ企業:1,900社(2018年) 特許出願数:約2,000(2018年時点) 大手企業がスコルコボ内に開設した研究所:45(2018年時点)
		1-4	規模(例:参加団体数/広さ/予算)	イノベーションセンター「スコルコボ」の広さ:400万㎡(※1) テクノパークの広さ約10万㎡(※2)
		1-5	ミッション/ビジョン	<目的> 以下の5つの方向性に従った研究、開発及びその成果の商用化を実現すること ①エネルギー技術の開発を含むエネルギー効率化及び省エネルギー ②原子力技術 ③戦略的コンピューター技術及びソフトウェア ④通信、ナビゲーションシステム等の宇宙技術(対応する地上基盤の整備を含む) ⑤設備・薬剤の開発の領域の医療技術

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (4/4)

分類		調査項目		調査結果
7	その他 CyberSpark	1-1	設立年度	2014年
		1-2	設立場所(国・地域)	イスラエル ベエルシェバ
		1-3	参加団体	• イスラエル国家サイバーセキュリティ局 • ベエルシェバ市 • 企業(イスラエル国内のスタートアップ企業/多国籍企業/ベンチャーキャピタル) • ベングリオン大学
		1-4	規模(例:参加団体数/広さ/予算)	• 企業数:40社 • 従業員数:1,200人 ※2017年ののレポート公開時点
		1-5	ミッション/ビジョン	<ミッション・ステートメント> • イスラエルのサイバーエコシステムを活用し、革新性と将来性においてベエル・シェバを世界に例のない「グローバル・サイバー・キャピタル」とする。
8	国家サイバーセキュリティ協力センター	1-1	設立年度	2022年
		1-2	設立場所(国・地域)	韓国　京畿道城南市盆唐区　第2板橋テクノバレー
		1-3	参加団体	• 公的機関(国家情報院、科学技術情報通信部、国防部など9つの機関) • 民間企業(AhnLab、East Security、S2W、Chainalysisなど8社)
		1-4	規模(例:参加団体数/広さ/予算)	• 企業数:8社 • 公的機関、民間企業合計で46名

© Hitachi, Ltd. 2024. All rights reserved.

1. 官民連携センターに係る国内外の動向

1. 一般的な事項
2. 詳細情報

© Hitachi, Ltd. 2024. All rights reserved.

サマリ (1/2)

HITACHI
Inspire the Next

- 官民連携センターの構築、運用において、民間企業の支援や政府側の取組みの推進を行うための取組みに特徴がみられた。

分類	米国	EU・英国	ロシア (※1)
立地・設備面の特徴	• 航空関係であればシミュレーター、送電関係ではOT機器を設置し、企業が共同で研究ができるようテスト施設を設置。[NCCoE] • テーマ(例:安全保障)によってはclassifiedなエリアを設定。[NCCoE]	• 人材の調達や政府との密な連携が行いやすいよう、大学や政府との距離が近い場所に官民連携センターを配置。[Plexal Innovation Centre] • 大学の研究施設をテスト用設備として利用。[Plexal Innovation Centre]	• 行政的な権限が付与されたスコルボ基金(当時大統領が評議会議長を務める)を設けた上で研究を行う特別な管理区域を設定。 • 研究センター(テクノパーク)への人材提供の役割の機能を持つ大学(スコルテック)を設立。
内容面の特徴	• 政策的なテーマと結びついた研究開発テーマを設定。[NCCoE] • 共同研究で策定した文書を政府が公開し、お墨付きを与えることで、結果的にかかる文書が業界標準となる。[NCCoE]	• 民間企業において準備が難しい模擬環境を活用したプログラムを提供。[European Network for Cyber Security]	• 大企業による技術の調達及びスタートアップ企業による売上確保を目的として、大企業とスタートアップ企業のマッチングを実施。
金銭面の特徴	• スタートアップ企業が投資家に対して研究成果に関するプレゼンテーションを行う場を設け、スタートアップと投資家を結びつけるための仕組みを構築。[Mach37]	• 各社が無料で1対1の相談を実施できるようセンター側でファンドと提携。[Plexal Innovation Centre]	• 関係法令により、民間企業に対する税制優遇措置(法人税や固定資産税の減免)や保険料率(社会保険料の減免)に関する優遇措置を実施。
人材面の特徴	• FFRDC(Federally Funded Research and Development Centers)の立場より、高度な知識を有する企業(MITRE)がセンターにおける民間企業の研究を支援。[NCCoE]	• 大学研究機関やコンサルティング企業と協力することによって、かかる機関の専門人材から民間企業に対して、研究等にかかるアドバイスを提供。[Plexal Innovation Centre]	• メンターによる経営サポートに加えて複雑な行政手続き(知的財産登録や通関業務)を代行。 • 外国人労働者に対する労働許可の有効期間を延長。

© Hitachi, Ltd. 2024. All rights reserved.

サマリ (2/2)

- イスラエルにおいては、スタッフの雇用に対して政府から助成金支給がなされており、特徴的な支援内容となっている。また、韓国においては、官民連携で分析したサイバー脅威情報が民間企業や公共機関に対してリアルタイムで共有されている。

分類	イスラエル	韓国
立地・設備面の特徴	• 人材の確保や各種手続き面でメリットがあるため、テック系の人材が多いテルアビブと官公庁が多いエルサレムに近いベエルシェバに設立。 • 施設は産業界の研究機関や大学と隣接した位置に設立。参画企業はかかる団体と日常的にアイディア交換が可能。	• IT系の企業が多くテック系の人材が多いテクノバレーに設立。テクノバレーは官公庁やテック系の大学が立地するソウルから20キロほどの距離に位置する。 • 合同分析室等を設立し、行政機関の職員とITベンダが合同で分析を実施。
内容面の特徴	• CyberSparkにR&Dセンターを設立する際に、サイバー分野での豊富な経験とイスラエルでの深い知識に基づいて、最適なチャネル(例:地元の起業家との合弁事業、多国籍企業との合弁事業の開始)を選別するための情報を提供。	• 合同分析室で分析したサイバー脅威情報は、公共機関を対象とした国家サイバー脅威インテリジェンス(NCTI)や民間企業を対象とした韓国サイバー脅威インテリジェンス (KCTI)を通じて、リアルタイムで共有。
金銭面の特徴	• 政府補助金による広範なインセンティブや多額の部分的資金援助を用意。例えば、現地のスタッフを採用する際、賃金に対して一定の割合で助成金を企業に対して支給。	• 請負事業者との契約条件等は管見の限り、確認できなかった。
人材面の特徴	• サイバー分野におけるプロジェクトマネージャーの採用支援やイスラエルに精通した専門のプロジェクトチームによる支援を実施。	• 常駐しているIT事業者の技術者を中心として、分析作業を実施。

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 設備面で政府機関が支援するメリット

HITACHI
Inspire the Next

- 政府機関が設備面の整備を支援することで、金銭的なメリットに加えて、情報面においてメリットがみられる。
- 特に、テストベッド施設における円滑な組織運営や対外組織との効率的な情報交換等が可能となる。

[問い]
テストベッド施設の設立にあたって、民間企業の取組みに対してなぜ政府機関が支援するのか。民間企業のみで設立・運用する際にみられる具体的な課題と政府機関が支援するメリットは何か。

項目	民間企業のみで設立・運用の際にみられる課題(例)	政府が支援するメリット(例)
金銭面	• テストベッド施設の設立には多額の費用が必要となるため、そもそも民間企業のみではテストベッド施設の設立自体が進まない可能性がある。	• 政府機関が金銭面で支援し、民間企業側の費用負担の問題を解決することによって、テスト施設の設立や安定的な運営を支援することが可能。
非金銭面 (主に情報面)	• テストベッド施設を運用組織では、連携体制の信頼関係の構築が重要となる。一方で、民間企業のみでテストベッド施設を構築した場合、協力が不可欠な大企業の一部が組織内で過大な発言力を持つ可能性や、組織から離脱する可能性が生じ、信頼関係を構築できない場合がある。	• 所有権やリーダーシップを政府機関に委ねることにより、ミッションやビジョンの円滑な調整が可能となるとともに、民間企業内の紛争において、政府機関が直接的または間接的に公認の仲裁人として機能することが可能となり、組織内の信頼構築を促進させることが可能。
	• 民間企業のみで設立した場合、海外のテストベッド施設や公的機関と調整が困難になる場合や、各民間企業が情報交換を行うことで、情報統制ができなくなる場合がある。	• 政府機関が支援することによって、海外のテストベッド施設や公的機関とのコミュニケーションのチャネルを一元化できるため、効率的な情報管理が可能。
	• テストベッド施設にて脆弱性が発見されたとしても、自社の不利益となるため、民間企業が脆弱性を是正しない場合がある。	• 政府機関が支援することによって、政府機関が脆弱性対応が放置されることを防ぐセーフガードの役割を担うことが可能となるため、セキュリティレベルの向上に寄与することが可能。 • ただし、製品に対する信頼が揺らぎうるため、政府は公的CERTとの連携が選択肢と入り得る点に留意。

[参考] ENISA" Good Practices for an EU ICS Testing Coordination Capability"(2013/12/10)
(https://www.enisa.europa.eu/publications/good-practices-for-an-eu-ics-testing-coordination-capability)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 基礎情報(1/2)

HITACHI
Inspire the Next

- NCCoEは、民間企業を含むイノベーターと協力し標準ベースのセキュリティソリューションを提供する。

項目	内容
設立年度	• 2012年
規模 (人員/予算)	• NCCoE在籍メンバーは126名(2023年9月時点) • NCCoEプロジェクトにおける協力企業の累計数は396社(2021年実績) • センターを運営するための官民パートナーシップを確立するために1000万ドル(2012年/NIST予算)
設立目的	• 最先端のサイバーセキュリティ技術の導入を加速させることを目的とする。
ミッション/ビジョン	• **ミッション:**安全なテクノロジーの採用を加速する。(イノベーターと協力し、ビジネスニーズに対応する標準ベースのサイバーセキュリティ機能を提供する) • **ビジョン:**サイバーセキュリティを推進する(技術革新を促し、経済成長を促進する安全なサイバーインフラを提供する) • **目標:**実用的なサイバーセキュリティを提供する/サイバーセキュリティの採用率の向上させる/効果的なイノベーションを加速させる
主要なアウトプット	• NIST SP 1800シリーズ • 業界固有のサイバーセキュリティペーパー　等

NIST SP 1800シリーズ
NCCoEが募集し民間事業者が参画するコンソーシアムにて作成。サイバーセキュリティ・コミュニティに対して、**実用的で使用可能なサイバーセキュリティ・ソリューションを提示**。

<記載内容>
- ソリューションと機能の詳細な例
- 同じ最終結果を得るために複数の製品を使用する実証されたハウツーアプローチ
- あらゆる規模の組織に対する機能の実装に関するモジュール形式のガイダンス
- 組織が容易にソリューションを複製できるように、必要なすべてのコンポーネント、インストール、構成、および統合に関する情報

[参考] NIST Special Publication 1800-series General Information
(https://www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information)
NCCoE"Mission & Vision"
(https://www.nccoe.nist.gov/our-approach/mission-vision)

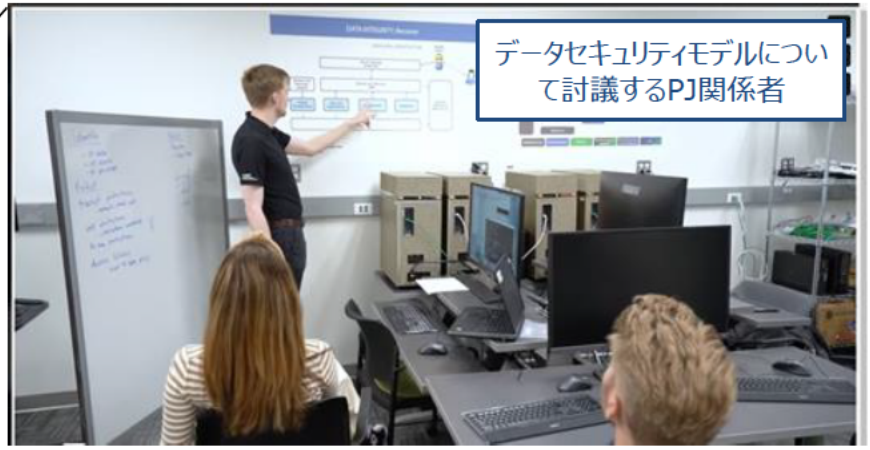
© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 基礎情報(2/2)

HITACHI
Inspire the Next

- NCCoEではセクターごとにラボを設置し、実証環境を構築した上で各種課題に取り組んでいる。

ラボ	内容
データセキュリティラボ	ランサムウェア、データ侵害、その他の脅威に対する、企業におけるシステムの保護に取り組む。
エネルギーセクターラボ	送電網、石油・天然ガスパイプライン、その他のエネルギー・システムを動かすサイバー・フィジカル・システムの保護に取り組む。
ヘルスケアセクターラボ	医療機関のサイバーセキュリティを向上させるために、セキュアな技術の開発に取り組む
製造業ラボ	製造業におけるサイバーセキュリティの喫緊の課題に対処するための実践的なソリューション例の開発に取り組む
モバイルデバイスセキュリティラボ	組織によるモバイルデバイスの配備を改善し、最も差し迫ったサイバーセキュリティの課題に取り組む
・・・	NCCoEには20を超える応用サイバーセキュリティ・ラボがあり、実証環境を構築した上で、エンジニアが協力して、標準、ベストプラクティス、市販の技術を使ったサイバーセキュリティ・ソリューションの実証を行う。





(データセキュリティラボ内の)5Gプロジェクトでは、5Gに係るユースケースを調査した上で、実証環境にてデモンストレーションを行い、実際に機能していることを確認している。



(5Gプロジェクトに参画)
Intel マネージャー

[参考] NCCoE" Virtual Tours: Take a Look Inside the NCCoE"(https://www.nccoe.nist.gov/virtual-tours)
Youtube(https://www.youtube.com/watch?v=EXlQargmFL0)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / プロジェクトのプロセス

- プロジェクトは、3つのプロセス(定義/収集/構築)からなる。
- 実証環境を提供するNCCoEに対して、民間事業者は対象製品の情報と専門知識を提供を行う。

プロジェクトのプロセス

Define 定義

- サイバーセキュリティの喫緊の課題を解決するために、産業界と業務範囲を定義
  - ✓ パブリック・コメントのためにプロジェクトの草案を発表
  - ✓ コメントを審査した上で、サイバーセキュリティの課題をアーキテクチャの草案とともに概説した最終版をウェブサイトに公開

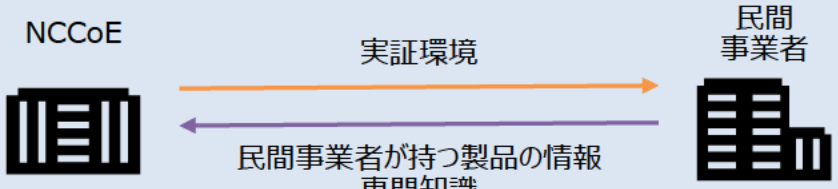
Assemble 収集

- サイバーセキュリティの課題に取り組むために、業界団体(民間事業者)、政府機関、学術機関からなるチームを編成
  - ✓ 連邦官報公告を発表し、協力の機会を告知する。
  - ✓ 協力者候補は、記入済みの関心表明書を提出する。(提出された関心表明書は先着順で受理)
  - ✓ 協力者がコンソーシアムに参加すると、共同研究開発契約に署名し、商業的に入手可能な製品と専門知識を提供。

Build 構築

- サイバーセキュリティの課題に対処するために、実用的で、使用可能で、再現可能な実装を構築
  - ✓ このフェーズでは、リファレンス・アーキテクチャを確定する。
  - ✓ 協力者は、各自の技術をインストールし設定するためのサポートを提供する。
  - ✓ また、相互運用性などの問題に対処するために、構築全体を通じてサポートを提供する。

NCCoEと民間事業者の関係性及び成果物例



【成果物例】
- NISTの標準で明らかになっているコンセプトや原則に則ったアーキテクチャ
- アーキテクチャに製品を当てはめた場合のソリューション例
- 具体的なソリューションの実装事例

[参考] NIST" NATIONAL CYBERSECURITY CENTER OF EXCELLENCE(NCCOE)"
(https://www.nccoe.nist.gov/our-approach/how-we-work)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 機能・成果物

- NCCoEは、市販のテクノロジーに基づく実用的なサイバーセキュリティソリューションを開発している。ただし、NCCoEは、従来の研究開発(R&D)活動を行っていない。
- また、州政府や郡政府とパートナーシップ協定を締結し、人材育成を実施している。

機能	内容	成果物(例)
技術の研究開発	• 企業が日々直面する実際の課題に迅速に対応できるよう、市販のテクノロジーに基づく実用的なサイバーセキュリティソリューションを開発している。具体的には、**プロジェクトごとに民間企業の協力を募り、セキュリティガイダンスを開発している。** • 従来の研究開発(R&D)活動を行っていない。	• セキュリティガイダンス(例:NIST SP1800シリーズ) • 業界固有のサイバーセキュリティペーパー
ビジネス創出機能	(民間事業者のビジネスを直接支援する機能はないが、策定した規格が民間事業者のビジネスに対して間接的に影響を与えている可能性はある。)	
人材育成機能	• NIST、メリーランド州およびメリーランド州のモンゴメリー郡はパートナーシップ協定を締結。(NCCoE設立当初より締結。2023年に再締結。)州内の企業に加えて、州内の公立学校や学術機関との関係を強化することも目的としており、NCCoEは学生のインターンシップなどを通じてサイバーセキュリティ人材育成を図っている。	• 各種プログラム(例:サマーハイスクールインターンプログラム(SHIP))

<ゼロトラストの場合>
2020年に、NISTがSP800-207を公開。2021年に、大統領令にてゼロトラストアーキテクチャ移行計画策定が指示された。これらの動きを受けて、**NCCoEはSP800-207に則り市販の技術を活用してゼロトラストを実現するためのガイドを策定中**

※2023/8/24時点

[出典]NCCoE(https://www.nccoe.nist.gov/our-approach/how-we-work)等

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 企業の参加メリット

HITACHI
Inspire the Next

- NCCoEでは、専門的なオペレーション支援を受けつつ、産官学が密な連携を行い研究開発を実施。
- NCCoEの文書等が実質的な業界標準となっており、企業にとって参加のインセンティブとなっている。

産官学が共同で研究可能な場の設置



モノの観点

- 場所を貸した上で企業ごとに研究スペースを作り、研究、テストを実施。(航空関係ではシミュレーター、送電関係ではOT機器を設置)
- 広大なスペースを確保しており、classifiedなエリアとそれ以外のエリアが存在。上記のエリアではセキュリティクリアランスによって入室を制限。
- 場所選定には立地や通信環境等が重要な要素となるが、主要な政府機関から車で30分程度に位置。

ステークホルダー間での密な連携



ヒトの観点

- 政府間(ホワイトハウス、CISA、関係省庁)の連携が強固であり、NISTの所掌範囲外の分野(例:電力) であってもNCCoEにて研究開発を実施。
- 政府機関(関係省庁)と大手企業(例:シュナイダー)と連携し研究開発を実施。研究開発テーマが政策的なテーマと結びついていることによって、安心して民間企業は企業に参加可能。また、公開された文書がNISTにより権威付けされていることが、民間企業にとって重要。

専門的なオペレーション支援が可能



情報の観点

- オペレーション支援を行っているMITREの存在が大きい。専門的な知見を有している。支援機関については国防権限法等によって、位置づけされている。
- また、CISAのような政府機関もオペレーションを支援。

潤沢な資金が提供されている

- 政府予算として、初期投資及び運用費用に潤沢な資金が計上されている。(ただし、具体的な費用までは不明。)

カネの観点

**NCCoEで作成した文書等が実質的な業界標準となっており、
参加する民間企業にとってはビジネス上で大きなメリットとなっている。**

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 参加費用

HITACHI
Inspire the Next

- NCCoEの取組みの中では、民間企業に対する研究施設の使用料は徴収していない(政府予算からねん出)が、人件費や研究所への機材持ち込み費用は民間企業側が負担することとしている。

ご質問	調査結果(※)
参加企業のコスト(入居費等)はどの程度か。	• 参加企業は時間と能力をボランティア(無償)で提供し、人件費や研究所への持ち込み機材についても民間企業側が負担。 ✓ 米国の企業に対しては基本、部屋やラボの使用代は政府予算からねん出。研究結果が生み出された知的財産は政府やコミュニティに帰属する。NISTから出版する形で知的財産は共同関係者らと共有する。 ✓ ただし、海外系の企業による研究所の使用料はケースバイケース(同志国であれば優遇される可能性)。出身国やニーズ、他の協力企業などで決定。 ✓ 政府からMITREに対して5年間で$2,500万ドルの運用資金が提供された。
参加企業にとってのベネフィットは何か。	• 実際を模した環境にて研究が行われることによって、実践的なガイドを策定することが可能。 • NIST等の政府機関から承認されたガイドを策定することが可能。 • 様々な主体(民間企業、大学、MITRE等)が参画することによって、イノベーションが起こりやすくなるとともに、作成したガイドがデファクトスタンダードとなる。 • 複数の企業と連携を行う仕組みがあるため、一社へのロックインを回避可能。(NISTなどとの関係で、標準とともに成長し、負け組、勝ち組を作らない) • 他の連邦政府機関(例:DHSなど) とのパートナーシップの構築や投資を募ることがが可能。 • 日本企業も含めた海外企業が参加可能。 • ISAC、MITREなどとも関係ができ、一緒に成長が可能。

2016年の社内レポートを参考としているため、必ずしも最新の情報でない点にご留意いただきたい。

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 参画企業 (1/3)

HITACHI
Inspire the Next

- プロジェクトごとに参画している団体に加えて、継続的に支援を行っている企業がみられた。

項目	調査結果
プロジェクトに参加している団体(プロジェクト数/団体数)	• [プロジェクト数] 16分野 31プロジェクト • [団体数(のべ)] 219社 (※1)(※2) ※1 プロジェクトに参画している団体の詳細は次頁以降参照 ※2 団体数については、以下の2点を留意いただきたい。 ✓ 参画団体を非公開としている5つのプロジェクトを含む。 ✓ 「スコープ定義中」、もしくは「協力ベンダ募集中」としているプロジェクトを含む。
継続的に支援を行っている団体(団体数/団体名)(※3)	• [団体数] 39社 • [団体名] AMI/Archer/AWS/BedRock Systems/CISCO/CLOUD FLARE、COMCAST/CYBER ARK/Delinea/Dell Technologies/DigiCert/DRAGOS/Forescout/Fortinet/Global Cyber Alliance/Google Cloud/Hewlett Packard/IBM/ID Dataweb/Intel/JPMorgan Chase & Co/Lookout/Mandiant/Microsoft/MOTOROLA/NextLabs/ORock Technologies/Palo Alto Networks/Seagate Technology/Spherical Analytics /Broadcom/TDI TECHNOLOGIES/Tenable/Thales TCT/Trellix/Venafi/Zimperium/Zscaler ※3 継続的に支援を行っている団体は、連邦技術移転法に基づきNCCoEの「National Cybersecurity Excellence Partnership (NCEP) プログラム」をNCCoEと締結している団体を指す。本プログラムにおいて、参画団体はテスト環境の構築等を目的としてハードウェア、ソフトウェア、専門知識を提供する。また、各団体においてゲスト研究者として指定された社員は直接または遠隔からセンターで作業を行う。

【参加費】
プロジェクト参加にかかる費用(負担額)は発生しない。

[参考] NCCoE(https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments)(https://www.nccoe.nist.gov/get-involved/collaborate-us-technical-contributions))等

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 参画企業 (2/3)

HITACHI
Inspire the Next

- セキュリティ事業者だけでなく、特により実装に近い医療分野(IoT機器)において相対的に多くのユーザ企業(非セキュリティ事業者)を巻き込んでいる。
- セキュリティ関連団体に加えてユーザ企業等の意見を反映することで、ユーザにより活用されやすい研究結果となる可能性。

プロジェクト		セキュリティ関連団体	非セキュリティ団体(省庁、ユーザ企業)	団体数
5G サイバーセキュリティ (5G Cybersecurity)		10	1	11
応用暗号 (Applied Cryptography)	ポスト量子暗号への移行	26	3	29
	TLS 1.3 による可視性の課題への対処	8	2	10
	NIST暗号モジュール検証プログラムの自動化	11	1	12
	TLS サーバー証明書の管理	5	0	5
AI (Artificial Intelligence)	コンテキストにおけるAI/MLバイアスの軽減	(スコープ定義中)		
	人工知能:敵対的機械学習	(非公開)		
サイバーハイジーン(Critical Cybersecurity Hygiene)		8	0	8
宇宙領域のサイバーセキュリティ(ハイブリッド衛星ネットワーク)		(非公開)		
データ分類		9	1	10
データセキュリティ	データの機密性:資産の特定と保護	7	0	7
	データの機密性:データ侵害の検出、対応、および回復	4	0	4
	データの完全性:ランサムウェアやその他の破壊的なイベントに対する資産の特定と保護	6	0	6
	データの完全性:ランサムウェアやその他の破壊的なイベントの検出と対応	7	0	7
	データの完全性:ランサムウェアやその他の破壊的なイベントからの回復	5	0	5

[参考] NCCoE(https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments)(https://www.nccoe.nist.gov/get-involved/collaborate-us-technical-contributions))等

© Hitachi, Ltd. 2024. All rights reserved.

1.2-1. NCCoE / 参画企業 (3/3)

HITACHI
Inspire the Next

プロジェクト		セキュリティ関連団体	非セキュリティ団体 (省庁、ユーザ企業)	団体数
DevSecOps		(協力ベンダ募集中)		
デジタルID		(協力ベンダ募集中)		
ゲノムサイバーセキュリティ		(公開なし)		
IoT	信頼できるIoTデバイスのネットワーク層オンボーディングとライフサイクル管理	9	2	11
	分散型エネルギー資源の確保	9	0	9
	遠隔医療リモート患者モニタリングエコシステムの保護	7	3	10
	IoTデバイスの特性評価	(公開なし)		
	MUD を使用したホーム IoT デバイスのセキュリティ保護	6	3	9
	ワイヤレス輸液ポンプの固定	8	5	13
IPv6		(公開なし)		
モバイル端末セキュリティ Mobile Device Security	モバイル端末セキュリティ:BYOD	4	1	5
	モバイル端末セキュリティ:企業所有物の個人対応	4	1	5
	モバイル端末セキュリティ:クラウドおよびハイブリッド ビルド	4	0	4
サプライチェーンアシュアランス		7	1	8
トラステッドクラウド Trusted Cloud		7	0	7
ゼロトラストアーキテクチャ Zero Trust Architecture		24	0	24
合計				219

[参考] NCCoE(https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments)(https://www.nccoe.nist.gov/get-involved/collaborate-us-technical-contributions))等

© Hitachi, Ltd. 2024. All rights reserved.

[参考] NCCoEのプロジェクトに参画している具体的な団体名 (1/3)

HITACHI
Inspire the Next

- 16分野 31プロジェクトに対して、のべ219団体が参画している。

プロジェクト		参画団体 ※非セキュリティ企業(省庁、ユーザ企業等)は赤字下線
5G サイバーセキュリティ (5G Cybersecurity)		AMI/AT&T/CableLabs/Cisco/Dell/Intel/Keysight Technologies/MiTAC/Nokia/Palo Alto Networks/T-Mobile/
応用暗号 (Applied Cryptography)	ポスト量子暗号への移行	AWS/Cisco/CISA/Cloudflare/Crypto4A Technologies/CryptoNext Security/Dell Technologies/DigiCert/Entrust/HP, Inc. /IBM/Information Security Corporation/InfoSec Global/ISARA Corporation/JPMorgan Chase Bank/Keyfactor/Microsoft/NSA /PQShield/SafeLogic, Inc. /Samsung SDS Co., Ltd. /SandboxAQ/SSH Communications Security Corp/Thales DIS CPL USA, Inc. /Thales Trusted Cyber Technologies/Utimaco/Verizon/VMware, Inc. /wolfSSL/
	TLS 1.3 による可視性の課題への対処	AppViewX/DigiCert/F5/JP Morgan Chase Bank/Mira Security, Inc. /Not For Radio, LLC/ NETSCOUT/Nubeva/Thales Trusted Cyber Technologies/US Bank/
	NIST暗号モジュール検証プログラムの自動化	Acumen Security/AEGISOLVE/Apple/atsec/AWS/Cisco/Cloudflare/Lightship Security/Microsoft/NXP Semiconductors/SUSE/
	TLS サーバー証明書の管理	DigiCert/f5/Symantec (now NortonLifeLock Inc.) /Thales/Venafi/
AI (Artificial Intelligence)	コンテキストにおけるAI/MLバイアスの軽減	(スコープ定義中)
	人工知能:敵対的機械学習	(非公開)
サイバーハイジーン (Critical Cybersecurity Hygiene)		Cisco/Eclypsium/Forescout/IBM/Lookout/Microsoft/Tenable/VMware/
宇宙領域のサイバーセキュリティ (ハイブリッド衛星ネットワーク)		(非公開)
データ分類		Adobe/ActiveNav/GitLab/Google/Janusnet/JPMorgan Chase BANK/Quick Heal/Thales Trusted Cyber Technologies/Trellix/Virtru

[参考] NCCoE(https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments)等

© Hitachi, Ltd. 2024. All rights reserved.

[参考] NCCoEのプロジェクトに参画している具体的な団体名 (2/3)

HITACHI
Inspire the Next

プロジェクト		参画団体 ※非セキュリティ企業(省庁、ユーザ企業等)は赤字下線
データセキュリティ	データの機密性:資産の特定と保護	Avrio Software/Dispel/FireEye/GreenTec/PKWARE/StrongKey/Symantec
	データの機密性:データ侵害の検出、対応、および回復	Cisco/Dispel/FireEye/PKWARE
	データの完全性:ランサムウェアやその他の破壊的なイベントに対する資産の特定と保護	Cisco/GreenTec/CryptoniteNXT/Micro Focus/Semperis/Tripwire/
	データの完全性:ランサムウェアやその他の破壊的なイベントの検出と対応	Cisco/Glasswall Solutions/GreenTec/Micro Focus/Semperis/Symantec/Tripwire
	データの完全性:ランサムウェアやその他の破壊的なイベントからの回復	GreenTec/IBM/Micro Focus/Tripwire/Veeam Software
DevSecOps		(協力ベンダ募集中)
デジタルID		(協力ベンダ募集中)
ゲノムサイバーセキュリティ		(公開無し)
IoT	信頼できるIoTデバイスのネットワーク層オンボーディングとライフサイクル管理	Aruba,/CableLabs/Cisco/Foundries.io/Kudelski IOT/NquiringMinds/NXP Semiconductors/Open Connectivity Foundation (OCF) /Sandelman Software Works/Silicon Labs/WISeKey
	分散型エネルギー資源の確保	Anterix/Cisco/Dots and Bridges/Radiflow/Spherical Analytics/Sumo Logic/TDi Technologies/University of Maryland/Xage Security/
	遠隔医療リモート患者モニタリングエコシステムの保護	Accuhealth/Cisco/Inova/LogRhythm/MedCrypt/MedSec/Onclave Networks/Tenable/University of Mississippi Medical Center/Vivify Health
	IoTデバイスの特性評価	(公開無し)
	MUD を使用したホーム IoT デバイスのセキュリティ保護	Arm/CableLabs/Cisco/CTIA/DigiCert/Forescout/Global Cyber Alliance/MasterPeace Solutions/Molex/Patton/Symantec (now a division of Broadcom)
	ワイヤレス輸液ポンプの固定	B.Braun/Baxter/BD/Cisco/Clearwater/DigiCert/ICU Medical/Intercede/MDISS/PFP Cybersecurity/Ramparts/Symantec/TDI Technologies

© Hitachi, Ltd. 2024. All rights reserved.

[参考] NCCoEのプロジェクトに参画している具体的な団体名 (3/3)

HITACHI
Inspire the Next

プロジェクト		参画団体 ※非セキュリティ企業(省庁、ユーザ企業等)は赤字下線
IPv6		(公開無し)
モバイル端末セキュリティ Mobile Device Security	モバイル端末セキュリティ:BYOD	IBM/Kryptowire (now known as Quokka) /Palo Alto Networks/Qualcomm/Zimperium
	モバイル端末セキュリティ:企業所有物の個人対応	Kryptowire (now known as Quokka) /Lookout/MobileIron/Palo Alto Networks/Qualcomm
	モバイル端末セキュリティ:クラウドおよびハイブリッド ビルド	Intel/Lookout/Microsoft/Symantec
サプライチェーンアシュアランス		Archer/Dell Technologies/Eclypsium/HP, Inc. /Hewlett Packard Enterprise/IBM/Intel/Seagate
トラステッドクラウド Trusted Cloud		Dell Technologies/Gemalto/Hytrust/IBM/Intel/RSA/VMware
ゼロトラストアーキテクチャ Zero Trust Architecture		Appgate/AWS/Broadcom Software/Cisco/DigiCert/F5/Forescout/Google Cloud/IBM/Ivanti/Lookout/Mandiant/Microsoft/Okta/Palo Alto Networks/PC Matic/Ping Identity/Radiant Logic/SailPoint/Tenable/Trellix/VMware/Zimperium/Zscaler/

© Hitachi, Ltd. 2024. All rights reserved.

1.2-2. Mach37 / 機能・成果物

HITACHI
Inspire the Next

- Mach37では、サイバーセキュリティ分野におけるスタートアップ企業の支援に主眼を置いて、シードマネーの提供や製品開発を包括的に支援している。

機能	内容	成果物(例)
技術の研究開発	(ビジネスの創出に主眼を置いている一方で、パートナーとの関係性の中で、新たな技術が開発される可能性がある。)	-
ビジネス創出機能	• 次世代のサイバーセキュリティ製品を提供する企業の発展を支援するため、毎年2回、5～8 社のスタートアップを対象に 90 日間にわたる集中プログラムを提供し、シードマネーの提供や製品開発を包括的にサポートしている。 • 各スタートアップは最大5 万ドルのシード資金を受け、製品アイディアの検証や最初の顧客層につながる関係作り、投資資本の獲得を主に重視することで、持続的なビジネスモデルの構築を目指す。	• 3件のエグジット／買収に成功(※) • 100万ドル＝平均調達額 • 85のサイバー企業が起業し、83%が現在も事業を継続中 • 64%が後続投資を調達
人材育成機能	(ビジネスの創出に主眼を置いている一方で、上記の集中プログラムにおいて、スタートアップ企業の創業者等の教育がなされる。)	-

フォーブスによると、Mach37はMACH37は米国トップのサイバーアクセラレータープログラムとされている。

※2023/8/24調査時点

[出典]Mach37 (https://www.mach37.com/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-2. Mach37 / 特徴

HITACHI
Inspire the Next

- スタートアップ企業支援を目的として、各段階ごとにプログラムが整備されている。

	プレアクセラレータプログラム	サイバーアクセラレータプログラム	成長ステージアクセラレーターププログラム
対象企業/対象者	• 立ち上げ前もしくは立ち上げ直後のスタートアップ企業	• **初期段階のスタートアップ企業**(ビジネスアプローチを学び、投資を求めることでビジネスを次のレベルに引き上げる準備が完了)	• **成長段階にあるスタートアップ企業**
実施内容	• サイバーアクセラレータプログラムから最大の効果が得られるよう以下を含むビジネスの基礎に焦点を当てたプログラムを提供 ✓ **ビジョンの作成:**会社を始めた理由、求める結果、成功の意味をより深く理解する ✓ **価値提案**:製品と市場の適合性を達成し、提供することを提案する価値は、市場の顧客のニーズと要求を満たす ✓ **会社設立:**ビジネスを行うために会社を設立するためのベストプラクティス ✓ **チームの構築:**勝利チームのために人を雇う方法 ✓ **ウェルビーイング:**起業家のウェルビーイングへのオリエンテーション	• 12週間のアクセラレータプログラムを提供 ✓ **アジャイル起業家精神:**ビジネスのスピードで起業家精神とイノベーションの方法を育成 ✓ **エコシステムの橋渡し:**エコシステム、セクター、組織、人々を超えてパートナーをつなぐ ✓ **問題解決:**問題に対する実行可能な解決策の重要なニーズを満たす ✓ **テックディスカバリー:**サイバーセクターにおける水平的な技術とトレンドの特定 ✓ **ウェルビーイング:**創業者、チーム、コミュニティメンバーのウェルビーイングを構築し、より豊かな体験、パートナーシップ、成果を促進	• スタートアップ企業を次のレベルを押し進めるためのプログラムを提供 ✓ **文化の確立** ✓ **リーダーシップと管理スキル** ✓ **ビジネスの運営** ✓ **顧客セットの拡大** ✓ **ソリューションのスケーリング** ✓ **次期ラウンドの資金調達の確保**

[参考]mach37(https://www.mach37.com/pre-accelerator)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-2. Mach37 / サポート内容

HITACHI
Inspire the Next

- 集中プログラム(サイバーアクセラレータプログラム)に参加することによって、投資家に対するプレゼンテーションの機会が認められており、資金を得るチャンスが与えられている。
- 併せて、広範な人的ネットワークから情報を得ることが可能となっている。

機能	サポート内容
金銭面のサポート	• 各企業は集中プログラム(90日間)に参加することで、起業家がサイバーセキュリティのコンセプトを検証し、投資に向けて会社を準備することが可能。 • 3ヶ月の終了時には、**投資家コミュニティに対してプレゼンテーションを行うことが可能。**(年に2回、MACH37は5-8社のセキュリティスタートアップ企業へ投資する) • なお、各90日間の集中プログラムへの参加費用は、5万ドル(※)
情報面のサポート	• 分野の専門家、成功したサイバーセキュリティ起業家、先見の明のある起業家、実務家、成功したセキュリティ起業家、セキュリティ市場に精通した投資家の**広範なネットワークから集中的な指導を受けることが可能**。 • 集中プログラムは、卒業企業が成長し、資金調達や市場シェアを獲得するための競争に打ち勝つスキルを身につけ、市場に参入できるように設計されている。

※2015年時点の参加費用

[出典] (https://securitywa.blogspot.com/2015/05/if-you-are-in-virginia-consider-mach-37.html)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-3. ECCC / センターの基礎情報

HITACHI
Inspire the Next

- 欧州サイバーセキュリティ・コンピテンス・センター(ECCC)は、2021年に欧州のサイバーセキュリティ能力と競争力を高めることを目的として設立された。

項目	内容
設立年度	• 2021年
規模 (人員/予算)	• スタッフ14名(2023年時点、2024年には40名に増員予定) • ブカレスト工科大学内に設置
設立目的	• 欧州のサイバーセキュリティ能力と競争力を高めることを目的としており、各国の調整センター(NCC)のネットワークと協力して、強力なサイバーセキュリティ共同体を構築する。
ミッション/ビジョン	• ミッション このエコシステムは、サイバーセキュリティ技術共同体の能力を強化し、サイバー攻撃から経済と社会を守り、卓越した研究を維持し、この分野におけるEU産業の競争力を強化する。ECCCは、加盟国、産業界、サイバーセキュリティ技術共同体とともに、技術開発と、公共の関心分野および企業、特に中小企業への幅広い展開のための共通アジェンダを策定し、実施する。 • タスク センターと各国の調整センター(NCC)のネットワークは、戦略的な投資決定を行い、技術と産業界のサイバーセキュリティ能力を向上・強化し、EUの戦略的自律性を強化する。センターは、デジタル・ヨーロッパ・プログラム及びホライゾン・ヨーロッパプログラムのサイバーセキュリティ目標を実現する上で重要な役割を果たす。センターはネットワークとともに、革新的なサイバーセキュリティ・ソリューションの展開を支援する。また、共同体内のすべての関係者(特に研究・産業界、公的機関など)間の協力や、専門知識・能力の共有を促進する。
根拠法	• EU労働基本条約(TFEU)173条3項および188条1項

[出典] European Cybersecurity Competence Centre and Network" About us"
(https://cybersecurity-centre.europa.eu/about-us_en)
EURACTIV"" Cybersecurity Competence Centre in Bucharest to provide Europe-wide Cyber Shield (https://www.euractiv.com/section/politics/news/cybersecurity-competence-centre-in-bucharest-to-provide-europe-wide-cyber-shield/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-3. ECCC / 取組み内容 (1/2)

HITACHI
Inspire the Next

- ECCCでは、サイバーセキュリティに係るツールの開発に加えて、先端的な技術(例:量子暗号)の開発を支援している。

戦略的アジェンダ

項目	内容
1.1 サイバーセキュリティ情報とリスク管理のためのプロセスとツール	• サイバーセキュリティインシデントの情報共有、予防、検知、 対応・回復、調査を支援するための技術、サービス、プロセスの開発・導入
	• 組織の脆弱性管理に係る意識向上等を支援 • ENISAと連携して、脆弱性の是正を目指す協調的脆弱性開示のイニシアチブの開発支援
	• ネットワークセキュリティの最適化と、サイバー脅威への対応を目的としたモデリングとシミュレーションのソリューションの開発・実装
	• 中小企業を対象としたサイバーセキュリティツールの確保
1.2 安全で弾力性のあるハードウェアおよびソフトウェアシステム	• 主要エンティティかつ重要エンティティ(※1)のサイバー脅威に対する回復力の向上
	• サイバーセキュリティプロセスのための自動化ツールの開発と採用の支援
	• セキュリティ・プライバシー「バイ・デザイン」の促進
	• IT/OT環境における製品開発及び長期使用におけるサイバーセキュリティ・ソリューションの導入支援
	• ポスト量子暗号の開発、実装、保証(監査の利用)の支援

※1:NIS2にて、主要エンティティ及び重要エンティティが定義されている。

[出典] European Cybersecurity Competence Centre and Network" Strategic Agenda"
(https://cybersecurity-centre.europa.eu/strategic-agenda_en)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-3. ECCC / 取組み内容 (2/2)

HITACHI
Inspire the Next

項目	内容
2.1 サイバーセキュリティ・スキルの開発：教育と職業訓練	ニーズに沿った教育カリキュラムの開発、調整、採用
	共通のツールや容易にアクセスできるプラットフォームの開発
	サイバーセキュリティのキャリアパス開発のための専用キャンペーンの展開
	セキュリティとプライバシーの「バイ・デザイン」アプローチの推進
	サイバー専門家の能力開発の促進
	サイバーセキュリティの脅威、手口、潜在的な影響に係る認識の向上
2.2 サイバーセキュリティ・スキルフレームワークと能力評価	サイバーセキュリティ技能枠組みの採用と実施の確保
	サイバー領域で働く人材の能力評価と認証制度の開発と普及支援
3.1 ポスト量子暗号の標準化と採用の促進	ポスト量子暗号アルゴリズムの開発を主導する専門家組織と専門家の支援
	ポスト量子暗号の採用戦略の策定
3.2 欧州のサイバーセキュリティ認証を支援	産業界に対するサイバーセキュリティ認証制度等の取り込みの奨励・促進
	適合性評価システムの強化
3.3 市場競争力の強化	サイバーセキュリティコミュニティに対する理解の深化
	EUのサイバーセキュリティ技術や製品の導入支援
	小規模なプレーヤーが大規模な組織に即座に販売できるような市場の実現に向けた支援
3.4 コラボレーションと情報共有の促進	高等教育機関や学際的研究機関等と産業界との連携の奨励
	情報 共有・分析センター(ISAC)型の協力イニシアティブの創設と能力構築の推進
	NIS協力グループの当局間でサイバー強靭性を高めるための協力の奨励

© Hitachi, Ltd. 2024. All rights reserved.

1.2-3. ECCC / 財源

- ECCCは、欧州における研究開発プログラム(ホライズンヨーロッパやデジタルヨーロッパプログラム)より提供される財源を使用。
- ECCCは、資金提供されたプロジェクトについて、プロジェクト受益者のためのコミュニケーション、普及、利用、および資金の可視化に関する具体的なガイドラインを作成、更新する。

項目	内容
ホライズンヨーロッパ	• ホライズンヨーロッパプログラムに従い、幅広い活動を実施する。主な重点分野は以下の通り。 ✓ デジタル・バリュー・チェーン全体にわたる技術(セキュアな部品や耐量子暗号からセルフヒーリングソフトウェアやネットワークまで) ✓ 技術、方法、標準、ベストプラクティス(電子ID、脅威の検出、サイバーハイジーン) 等
デジタルヨーロッパプログラム	• デジタルヨーロッパプログラムにおける特定目標3「サイバーセキュリティと信頼」に基づき、以下を実施する。 (a) サイバーセキュリティ機器、ツール、データ基盤の構築と調達の支援 (b) サイバーセキュリティに関する知識、能力、技能の蓄積とベストプラクティスの活用、共有等を支援 (c) 欧州経済全体で最先端のサイバーセキュリティ・ソリューションの幅広い展開の確保 (d) (EU) 2016/1148(25)(※)を遵守できるよう、加盟国および民間部門の能力を強化 (e) 公共及び民間組織が基本レベルのサイバーセキュリティを達成することを支援 (f) サイバーセキュリティのデュアルユースプロジェクト、サービス、コンピテンス及びアプリケーションに関して、民間と防衛の間の協力を強化 ECCCは、プロジェクト受益者のためのコミュニケーション、普及、利用、および資金の可視化に関する具体的なガイドラインを作成、更新する。

※:(EU) 2016/1148はNIS指令を指す。

[出典] European Cybersecurity Competence Centre and Network "Funding opportunities" (https://cybersecurity-centre.europa.eu/funding-opportunities_en)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-4. Plexal Innovation Centre / センターの基礎情報

HITACHI
Inspire the Next

- 欧州最大のイノベーションセンターの1つであるPlexal Innovation Centreは、2012年ロンドンオリンピック跡地に建設された。
- 2017年より約6年間で多数のイノベーションセンタープロジェクトの主導とスタートアップ企業の成長を支援。

項目	内容
設立年度	• 2017年(2012年ロンドンオリンピックの跡地を活用)
位置づけ	• 民間企業
規模(面積)	• 68,000平方フィート(参考:6,317㎡)(※1)
成果	• 2017年以来、Plexalは50を超えるイノベーション・プロジェクトを実施。 • 500を超えるスタートアップの成長ジャーニーを支援。
ビジョン	テクノロジーを社会にとってより良いものにすること。 • 英国政府の使命を受け継ぎ、コラボレーションを通じてイノベーションの課題を解決する。 • オーダーメイドのコンサルティング・サービスと最先端のワークスペースを提供し、エコシステムから適切なパートナーを探し出す。 • 私たちは、サイバーやヘルスケアからAIやML、コネクテッド・プレイスや気候変動技術に至るまで、新興の科学技術全般にわたって起業家、新興企業、スケールアップ企業を支援する。 • 戦略、発見、検証、イノベーション・プログラム、エコシステムという5つのコア・プロダクトを通じて、クライアントの課題を解決する。 • 私たちは、情報・防衛、政府、金融サービス、通信など、さまざまな分野で事業を展開する。
実施事項	• 起業家、新興技術の構築、スケールアップをサポートし、サイバー、ヘルスケア、諜報と防衛、政府、公安、金融サービス、通信などの複数のセクターにわたって事業を展開する。 • 私たちは、公共部門と民間部門の間のギャップを縮め、イノベーション、コラボレーション、知性を解き放ち、ミッションの成功を達成することで、主要な政府部門にプロジェクトを提供する。

欧州最大のイノベーションセンターの1つとされている。

※1:約80m×約80m。
※2:調査時点(2023年10月)

[参考]Plexal" CLOSING THE GAP" (https://www.plexal.com/)
HereEast "Bringing innovators together at Plexal"(https://hereeast.com/whos-here/plexal/)
GRIMSHAW" Plexal Innovation Centre　London, UK"
(https://grimshaw.global/projects/workplace/plexal-innovation-centre/)

© Hitachi, Ltd. 2024. All rights reserved.

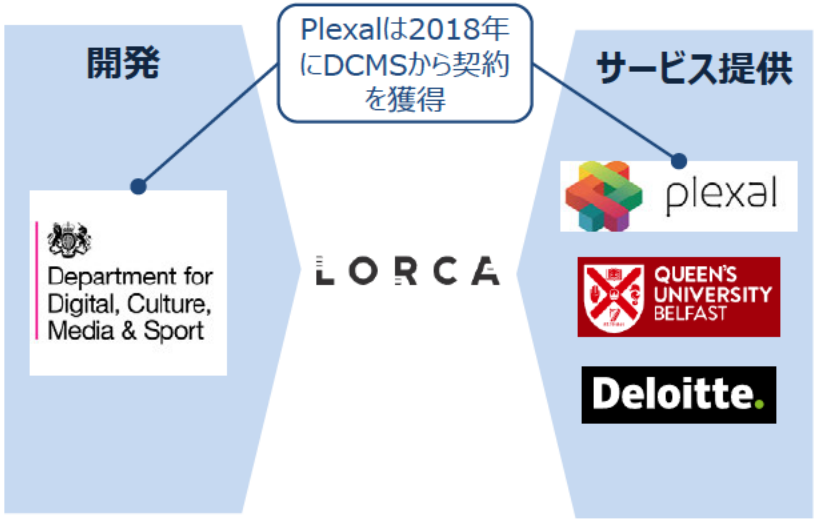
1.2-4. Plexal Innovation Centre / 個別プログラム:LORCA (1/2)

HITACHI Inspire the Next

- Plexalは、クイーンズ大学のセキュア情報技術センター及びデロイトと共同でThe London Office for Rapid Cybersecurity Advancement (LORCA)を運営。デジタル・文化・メディア・スポーツ省(DCMS) が予算的な支援を実施。

仕組み

- 国家サイバーセキュリティ戦略(2016～2021年)及び国家サイバーセキュリティプログラムを通じて、DCMSは、政府および業界全体のパートナーと協力して、サイバーセキュリティセクターとエコシステムの成長を支援するLORCAを2018年に開発。
- Plexalはクイーンズ大学のセキュア情報技術センター、及びデロイトと共同でサービス提供を行っている。



成果

- 過去4年間で、多くのスタートアップアップ企業を支援するとともに、そのスタートアップ企業が多くの投資獲得や収益増加を達成。

種類	成果(2018年～2022年)
支援企業数	• 72 社の成長を促進
雇用	• 865件の雇用を創出
投資額	• 支援企業合計で2億1,000万ポンド(約384億円)の投資を調達
収益額	• 支援企業合計で3,700万ポンド(約67億円)の収益増加

[参考] GOV.UK "Evaluation of the LORCA programme" (https://www.gov.uk/government/publications/evaluation-of-the-lorca-programme/evaluation-of-the-lorca-programme)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-4. Plexal Innovation Centre / 個別プログラム:LORCA (2/2)

HITACHI Inspire the Next

- PlexalにおいてLORCAによって、スタートアップ企業は様々なメリットを享受することが可能。

LORCAのメリット(例)

	メリット	内容
設備面でのメリット	**試験施設へアクセス可能**	• クイーンズ大学のセキュア情報技術センターの試験施設へアクセスが可能 • デロイトのテスト施設へのアクセス可能
	無料特典	• Plexal Innovation Centreとコワーキングスペースの無料デスクスペース、およびメンバーとしてのすべての特典を受けることが可能
情報面でのメリット	**知識面でのサポート**	• クイーンズ大学のセキュア情報技術センターのエンジニアリングサポートと受けることが可能 • サイバーに係る専門知識へアクセス可能
	相談可能	• ビジネス面で相談が可能
人的なメリット	**投資家や業界バイヤとのつながり**	• ショーケースや会員限定イベントを通じて投資家や業界バイヤとつながることが可能
金銭面でのメリット	**プログラム参加に係る費用**	• 参加費は無料

<参考>設備の利用料金
自由席:240ポンド/月(約43,000円) (※1)
固定席:375ポンド/月(約67,000円)
プライベートオフィス:1,350ポンド/月(約244,000円)

[参考] Plexal" NCSC FOR STARTUPS"
(https://www.lorca.co.uk/apply/)

© Hitachi, Ltd. 2024. All rights reserved.

[参考] Plexal Innovation Centre / メンバーベネフィット

HITACHI
Inspire the Next

- Plexal のメンバーとなることによって様々な特典を受けることができるため、企業の参加に係るインセンティブとなり得る。

メンバーベネフィット



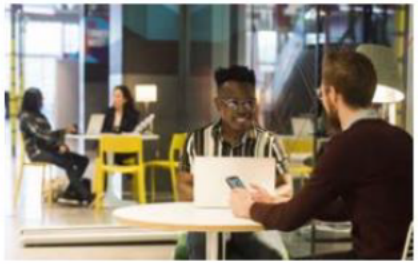
コミュニティイベント

毎週のイベント(パネルディベート、ワークショップ、パーティー)によって、Plexalのメンバーは親睦を深めている。



イノベーションチーム

Plexalのイノベーションチームが産業界や政府向けに提供するプログラムにPlexalのメンバーは参加している。



資金調達に係るアドバイス

ファンドと提携し、Plexalのメンバーに対して無料で1対1の相談を実施している。



メンタリング

Plexalのリーダーシップチームやイノベーションチームと1対1で相談を行うことができる。



世界中のどこでも働ける

Plexalのメンバーは、サンフランシスコやチェルトナム、テキサス州オースティンのワークスペースの5日間無料パスを入手できる。



働きやすいワークスペース

ワークスペースを改修し、様々な障害を持つ人々が利用しやすいように配慮している。

[参考] Plexal" CLOSING THE GAP" (https://www.plexal.com/workspace-stratford/#private-office)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-5. European Network for Cyber Security / センターの基礎情報

HITACHI
Inspire the Next

- European Network for Cyber Security(ENCS)は、2012年、オランダのハーグに設立された。
- オランダの協同組合法のもと設立され、欧州において安全で重要なエネルギーグリッドやインフラを展開するため、重要インフラの関連企業・機関とセキュリティーの専門家を集める。

項目	内容
設立年度	• 2012年設立
位置づけ	• オランダの協同組合法の下、設立 • グリッド オペレーターが所有する非営利団体
参加者	• 応用研究、技術的セキュリティ要件の定義、コンポーネントおよびエンドツーエンドのテスト、教育とトレーニングに取組む専任の研究者とテスト専門家
ミッション	• ENCSは、欧州の重要なエネルギー・グリッドとインフラを安全に配備するために、重要インフラの関係者とセキュリティの専門家を集めている。知識の共有を通じて、再生可能エネルギーへの安全な移行を可能にし、サイバー攻撃から社会を守る。
実施事項	• 学界、政府、企業のネットワークを利用して、サイバーセキュリティプログラムを提供し、各国の配電システムオペレーターおよび規制当局のニーズに特化したアドバイスを提供する。

[参考] European Network for Cyber Security"Home" (https://encs.eu/)
産総研「欧州サイバーセキュリティー機関ENCSと産業技術総合研究所情報技術研究部門がLetter of Intent(確認書)を締結」
(https://www.aist.go.jp/aist_j/news/pr20151015.html)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-5. European Network for Cyber Security / 取組み内容(全体)

HITACHI
Inspire the Next

- European Network for Cyber Securityは組織内の役割に応じて、セキュリティの知識を開発するプログラムを提供。

European Network for Cyber Securityが提供するプログラム

プログラム	内容
セキュリティオペレーションプログラム	• セキュリティ運用とグリッド制御システムの監視に関する知識を開発し、共有する。 • このプログラムは、SOC および CSIRT アナリストとそのマネージャーまたはチーム リーダーを対象とする。 • 例えば、以下のトピックを扱う。 ✓ 運用技術システムを監視するユースケース ✓ 運用技術システムを監視するセンサーと技術 ✓ 脆弱性管理 ✓ 運用技術システムのインシデント対応
セキュリティアーキテクチャプログラム	• 安全なシステムの設計、構築、調達、アップグレードに関する知識を開発し、共有する。 • このプログラムは、セキュリティ アーキテクトや調達チームのセキュリティ スペシャリストなど、メンバーの技術セキュリティ スペシャリストを対象とする。 • 例えば、以下のトピックを扱う。 ✓ ゾーニングとネットワークセグメンテーション ✓ リモートアクセスを含むアクセス制御 ✓ 鍵管理と公開鍵インフラストラクチャ(PKI) ✓ 分散側エネルギーリソース(DER)など外部との安全な接続 ✓ 社内アプリケーション開発のための安全なプロセス
セキュリティポリシープログラム	• セキュリティ リスクとそれに対応する欧州規制の管理に関する専門知識を開発し、共有する。 • このプログラムは、重要なインフラストラクチャを担当するメンバーのセキュリティ担当者を対象とする。 • 例えば、以下のトピックを扱う。 ✓ ISO/IEC 27001 または IEC 62443 などに基づく情報セキュリティ管理システム(ISMS)の実装 ✓ NIS 指令の実装 ✓ サイバーセキュリティに関するネットワークコード ✓ 組織的対策の有効性のモニタリング ✓ セキュリティ意識向上トレーニング

[参考] European Network for Cyber Security" Security programs at ENCS"
(https://encs.eu/security-programs/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-5. European Network for Cyber Security / 取組み内容(個別)

HITACHI
Inspire the Next

- 民間企業において準備が難しい模擬環境を活用したプログラムを提供。

ENCSオペレーションプログラム

項目	内容
対象者	• 運用技術 (OT) システムの脆弱性の発見とインシデントの検出を担当するスタッフを対象
目的	• 参加者は次の方法を学習する ✓ 最大のセキュリティ・リスクに対抗するために、モニタリングのユースケースを選択する方法 ✓ OT領域全体をカバーするために、適切なセンサーとデータセンサーを選択する方法 ✓ 脆弱性と緩和策を特定する方法 ✓ アラートとインシデントの可能性を分析する方法 ✓ OT向けに開発された新しいセキュリティ・センサーの設定と使用
参加費	• 参加者 1 名あたりの費用は 1,650ユーロ (ENCS正会員の場合:約25万円)

プログラムの学習内容

分類	学習内容
1.リスクベースの検出戦略	• OTシステムでのユースケースの適用 • リスクに基づいたユースケースの選択方法 • SCADAシステムへの適用方法
2.脆弱性管理	• 脆弱性管理及びその対応方法 • 個々のホストにおける脆弱性発見方法 • ネットワークアーキテクチャにおける脆弱性発見方法 • 脆弱性に係る優先度の設定方法 • OTシステムにおける修正策等の発見方法
3.ミスユース検知	• OTにおけるIT侵入検知センサーの使用方法 • 不正パケットのアラート分析方法
4.アクセス監視	• 異常なアクセスログの分析方法 • ホワイトリストの設定方法 • ホストや新たな接続に係るアラートの分析方法
5.ログの確認	• 異常な保守作業(バックドアの設置など)のログの分析方法 • SCADAシステムの異常なアクションを検出するためのディープパケットインスペクションの設定と使用方法
6.統合	• 過去事例を対象とした分析 • 攻撃を検知するための実習 • 様々なユースケースにおける情報の関連付け方法

[参考] European Network for Cyber Security" Security programs at ENCS"
(https://encs.eu/security-programs/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / センターの基礎情報

HITACHI
Inspire the Next

- 2010年9月の連邦法が成立によって、エネルギー、原子力、IT、通信・宇宙、バイオ医療の技術研究開発に注力するスコルコボが設立された。
- 開始から約8年間で1900のスタートアップ企業が企業し、2000ものの特許出願がなされており、一定の成果があがっている。

項目	内容
設立年度	• 2010年9月 (スコルコボについての連邦法が成立)
規模 (面積)	• イノベーションセンター「スコルコボ」の広さ:400万㎡(※1) • テクノパークの広さ約10万㎡(※2)
人員/予算	• スコルコボのプロジェクトに参加しているスタートアップ企業:1,900社(2018年) • 特許出願数:約2,000(2018年時点) • 大手企業がスコルコボ内に開設した研究所:45(2018年時点)
設立目的	• 5 つの方向性に従った研究、開発及びその成果の商用化を発展させること ①革新的なエネルギー技術の開発を含むエネルギー効率化及び省エネルギー ②原子力技術 ③戦略的コンピューター技術及びソフトウェア ④通信、ナビゲーションシステム等の宇宙技術(対応する地上基盤の整備を含む) ⑤設備・薬剤の開発の領域の医療技術

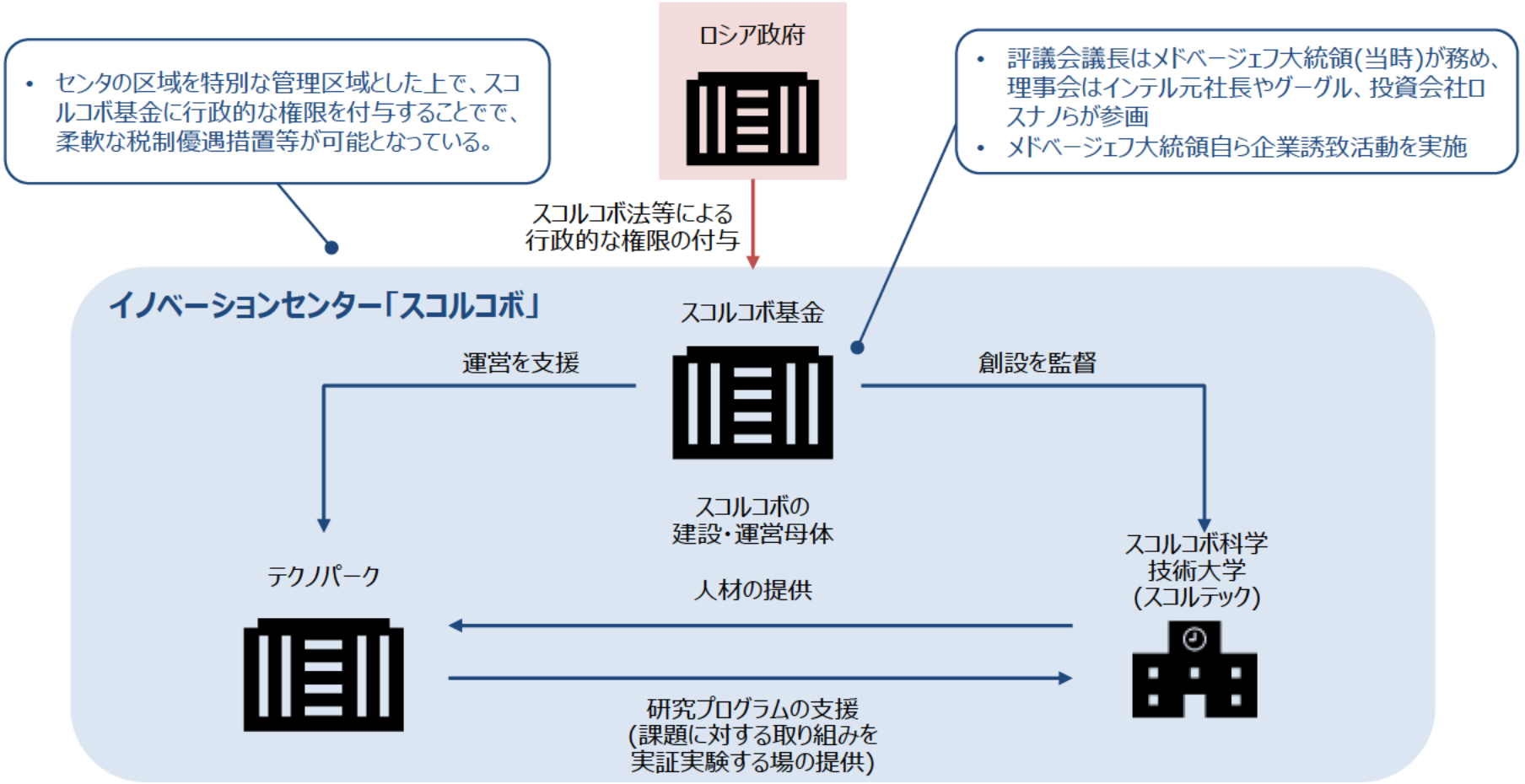
※1:参考400万㎡=2km×2km
※2:参考10万㎡=316m×316m

[参考]朝日新聞デジタル「ロシア版シリコンバレー、スコルコボで進む国家主導型イノベーションの現実」
(https://globe.asahi.com/article/12774440)
堀内賢志「イノベーションセンター「スコルコヴォ」に関する法制」等
(https://dl.ndl.go.jp/view/download/digidepo_3050653_po_02480005.pdf?contentNo=1)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / 団体間の関係性

- スコルコボ法等によって、ロシア政府から行政的な権限を付与されたスコルコボ基金(当時大統領が評議会議長を務める)がスコルコボの建設、運営団体となり、テクノパークやスコルコボ科学技術大学を支援、監督。
- センタの区域を特別な管理区域とすることで、柔軟な税制優遇措置等が可能となっている。



※その他、センター内には公共施設やレジデンスも建設されている

[参考]堀内賢志「イノベーションセンター「スコルコヴォ」に関する法制」等
(https://dl.ndl.go.jp/view/download/digidepo_3050653_po_02480005.pdf?contentNo=1)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / 取組み内容 (1/2)

HITACHI
Inspire the Next

- スコルコボでは、研究開発型、特に新技術を開発し商用化していくタイプのスタートアップを支援。
- スタートアップ企業に対して、各アクセラレータプログラムを提供。

スタートアップ企業へ提供するアクセラレータプログラム(例)

項目	内容
アクセラレーション・プログラム	• アイデアから市場投入まで、プロジェクトを包括的にサポートする自社およびパートナーのプログラム。アクセラレーターの目標は、最高のスタートアップ技術を探し、選択し、開発し、実装を加速することである。このようなプログラムに参加することで、スタートアップ技術プロジェクトのチームは、ビジネスと技術の能力を開発し、ビジネスモデルの開発支援を受け、ベンチャー投資を呼び込むことができる。
企業アクセラレーション	• スコルコボ基金は、パートナーである大企業からの特定の委託を受けて、プロジェクト参加者の企業アクセラレーションを行っている。これにより、若手チームのソリューションを顧客の実際のニーズに近づけることができ、将来的には、得られた開発成果をビジネスに統合することができる。(次頁にて説明)
スコルコボ基金メンターシップ・プログラム	• 企業がメンターの知識や成功経験を無料で活用し、プロジェクトを飛躍させるためのツール。スコルコボ財団は、プロジェクト参加者とメンターコミュニティの仲介役として、それぞれの具体的な要望に応じて最適なメンターを選ぶ。
グローバル市場へのアクセスのための国際プログラム	• プロジェクト参加者は、各国への定期的なビジネス・ミッションへの参加、国際展示会や会議への参加支援、世界有数のテクノロジー・センターと共同で実施される産業別の国際アクセラレーション・プログラムなど、国際市場へのアクセスを支援する幅広いツールを利用することができる。

[出典]skolkvo" Преимущества участника проекта"
(https://sk.ru/project-participant-benefits/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / 取組み内容 (2/2)

HITACHI
Inspire the Next

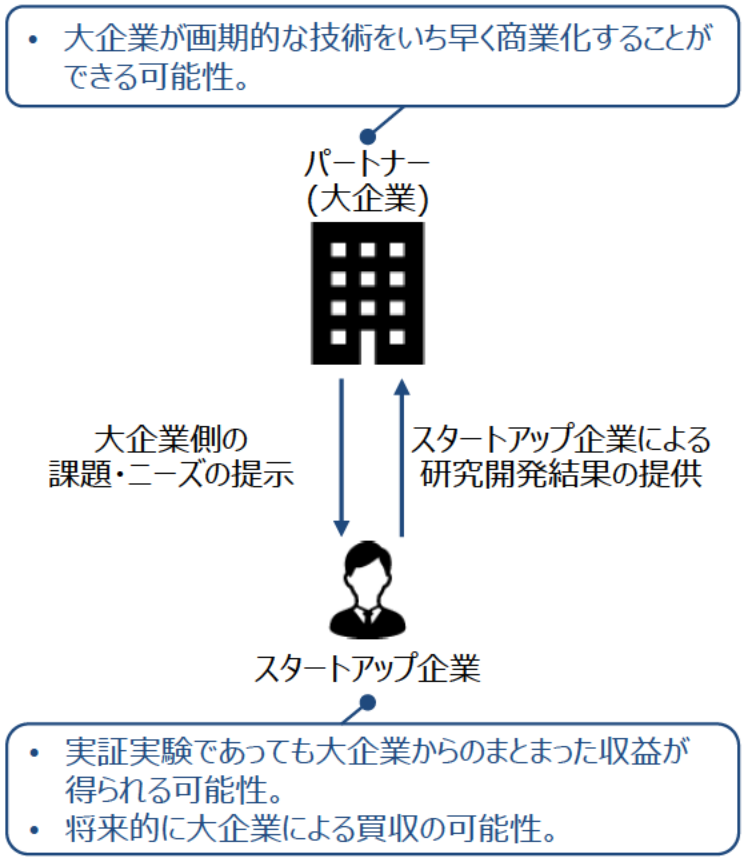
- パートナー(大企業)とスタートアップ企業をスコルコボがマッチングすることにより、大企業では技術の(社内で技術研究開発を行わずに)調達が可能となり、スタートアップ企業では金銭的なメリットを得ることが可能。

企業アクセラレーションプログラムのステップ

フェーズ	内容
準備	• イノベーション課題の分析 • プログラムパートナーのニーズ分析
コンペティション/スカウティング	• 評価基準の作成 • 参加者獲得のためのPRキャンペーン • テーマ別スタートアップの幅広いファネル(※)の形成 • テクノパーク、インキュベーター、研究機関/大学、イノベーションセンターによるチームの発掘と結成
専門家の関与	• 専門家パネルの結成 • 提出されたソリューションの共同詳細分析 • 専門家による評価と最終選考
加速	• **<u>パートナーのニーズへの新興企業ソリューションの適合</u>** • 最終候補者の準備：ビジネス能力、追跡調査 • **<u>パートナーの代表者の関与</u>** • チームの追加審査
ピッチセクション	• ファイナリスト5～10名の準備 • 審査員の編成 • PRサポート • イベント開催 • プロの司会進行

※ファネル:顧客が商品を認知してから購入に至るまでの行動ステップを図式化したもの

大企業とスタートアップ企業のメリット



[参考]skolkvo" Корпоративный акселератор" (https://services.sk.ru/service/223)
日経ビジネス「メドベージェフお墨付きのスコルコボが目指す道」
(https://business.nikkei.com/atcl/report/16/011900003/032100005/?P=3)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / サポート内容 (1/2)

HITACHI
Inspire the Next

- スコルコボのイノベーションセンターに関連する法律として、スコルコボ法及びスコルコボ関係法令改正法が定められており、参画企業に対する税制優遇措置や保険料率に関する優遇措置、外国人の雇用に関する優遇地措置が定められている。

分類		サポート内容
金銭面のサポート	税制優遇措置	• 参画事業者は以下の税が免除される。 ✓ **付加価値税:**資格を取得した日から10年間、付加価値税を免除される権利を持つ。 <参考:付加価値税>ロシアへの商品輸入、ロシア国内における商品の売買、その他の譲渡ならびに役務・サービスの提供には付加価値税が課税され、通常の税率は20%である。 ✓ **組織利潤税** <参考:組織利潤税>日本の法人税に相当し、企業の利潤に課される。通常の税率は20%。 ✓ **組織資産税** <参考:組織資産税>企業の固定資産の額に課される連邦構成主体税であり、税率は 2.2%を超えない範囲で連邦構成主体の法律により規定される。 ✓ **土地税** <参考:土地税>企業及び自然人の所有する土地の額に課される地方自治体税であり、税率は、農地や地方自治体所有の住宅及び住宅公益部門の基盤等の土地については 0.3%を超えない範囲、その他の土地については 1.5%を超えない範囲で地方自治体の法令によって規定される。
	保険料	• 参画事業者は保険料率が一般的な保険料率より安くなる。 ✓ **強制年金保険の保険料率**:14%(2013～2014年度は21.0%) ✓ **年金機器への保険料率:**14%(2013～2014年度は 21.0%) ✓ **社会保険基金への保険料率:**0%(2013～2014年度は2.4%) ✓ **連邦強制医療保険基金への保険料率:**0%(2013～2014 年度は3.7%) ✓ **地域強制医療保険基金への保険料率:**0%(2011年度は1.2%、2013～2014年度0.0%)

[出典]「イノベーションセンター「スコルコヴォ」に関する法制」
(https://dl.ndl.go.jp/view/download/digidepo_3050653_po_02480005.pdf?contentNo=1)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-6. skolkvo / サポート内容 (2/2)

HITACHI
Inspire the Next

分類		サポート内容
金銭面のサポート	手数料の免除	• 事業実施参加主体と業務に関する労働契約又は民法上の契約を結びロシアに入国した外国市民に対する労働許可の交付手数料、入国招聘状の交付手数料、ビザの発給・期間延長の手数料の支払いは免除される。
	助成金	• グラントと呼ばれるスコルコボ基金からの助成金がスタートアップに提供される。資金と引き換えに株式を所持しないため既存株主の持分は希薄化せず、一定の条件を満たせば返済義務がない。
	その他	• その商品や業務、サービスの年売上額が10億ルーブル以下の場合、より簡略な収入・支出の報告を許可
人材面のサポート	企業の外部からの支援	• メンターによる経営サポートに加えて知的財産登録や通関業務の代行を実施。(特にロシアの通関業務は不透明で分かりにくく、また関係者とのつながりなどでも手続きのスムーズさが変わってくるということも多いため、相当な業務負荷の軽減となる。)
	企業内部の雇用支援	• 事業実施のために外国人を雇用する際、通常雇用主が外国人労働者の雇用の際に取得しなければならない雇用許可は必要とされない。 • 通常外国人労働者の雇用には自治体ごとの割当枠が設定されるが、こうした割当枠も同センターで雇用される外国人労働者には存在しないこととなる。 • 外国人労働者に対する労働許可の有効期間は入国から3年間となるが、その後3年以下の期限で延長し続けることが可能。

[出典]「イノベーションセンター「スコルコヴォ」に関する法制」
(https://dl.ndl.go.jp/view/download/digidepo_3050653_po_02480005.pdf?contentNo=1)
日経ビジネス「研究開発型スタートアップへの支援が充実」
(https://business.nikkei.com/atcl/report/16/011900003/020300002/)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-7. CyberSpark / センターの基礎情報

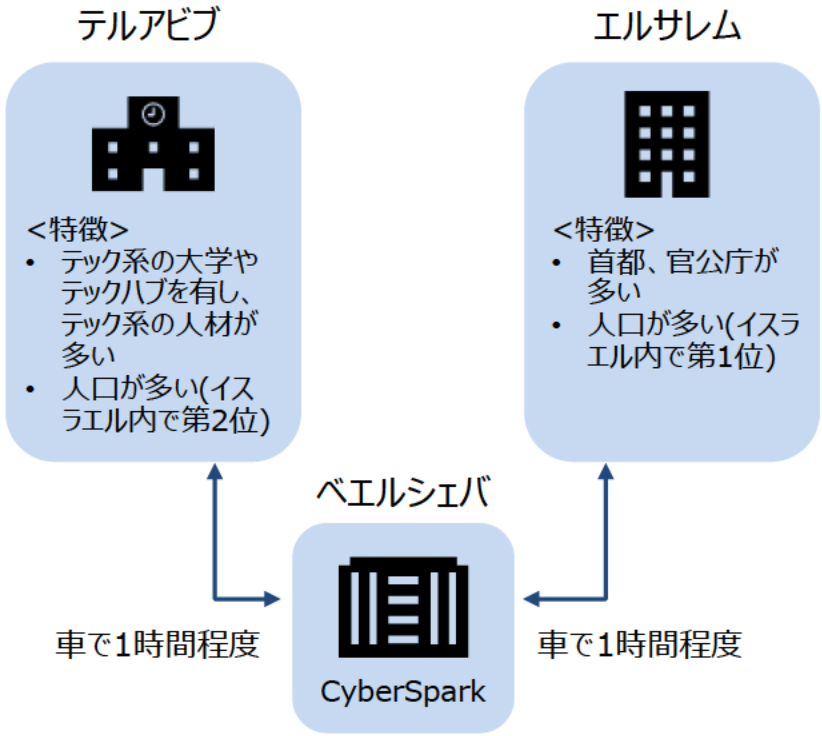
- CyberSparkは、イスラエル南部のベエルシェバにある研究開発特区・機関。
- 同国国家サイバー局の下で運営され、イスラエル国内のスタートアップ企業や多国籍企業、ベンチャーキャピタルが参加。

基本情報

項目	内容
設立年度	• 2014年
場所	• イスラエル ベエルシェバ
構成	• イスラエル国家サイバーセキュリティ局 • ベエルシェバ市 • 企業(イスラエル国内のスタートアップ企業/多国籍企業/ベンチャーキャピタル) • ベングリオン大学
規模(人員/予算)	• 企業数:40社 • 従業員数:1,200人 ※2017年のレポート公開時点
目的	• スタートアップ支援 • 多国籍企業との大学との共同研究
ミッション/ビジョン	<ミッション・ステートメント> • イスラエルのサイバーエコシステムを活用し、革新性と将来性においてベエル・シェバを世界に例のない「グローバル・サイバー・キャピタル」とする。
提供プロジェクト(例)	• Landing-Pad

• **立地**

テック系の人材が多いテルアビブと官公庁が多いエルサレムから車で1時間程度であり、人材の確保や各種手続き面でメリットを有する。



[参考] Yumpu" WHY CYBERSPARK?"
(https://www.yumpu.com/en/document/view/57004628/why-cyberspark)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-7. CyberSpark / Landing-Pad (1/2)

HITACHI
Inspire the Next

- CyberSparkが提供するプロジェクトの1つであるLanding-Padでは、イスラエルに実質的な拠点を持たない外国企業を対象として、外国企業におけるサイバー関連の事業体の設立を支援。

プロジェクトの基礎情報

項目	内容
目的	• イスラエルに実質的な拠点を持たない外国企業を対象として、外国企業におけるサイバー関連の事業体の設立を支援する。
プロジェクトを通じて達成可能な事項	• コラボレーション(デザイン・パートナー、アルファサイト、買収など)のを目的とした地元新興企業の発掘 • 大学研究機関のメンバーとの共同研究提案の構築 • イスラエルにおける起業家との合弁事業の開始 • 多国籍企業との合弁事業の開始 • イスラエルのCERTとからの情報共有 • 革新的なイスラエル企業との共同プロジェクトの開始 • サイバーシンクタンクでのブレインストーミング(例:サイバーセキュリティのトップエキスパートとパートナーチームが実施) • ハッカソンの開催
費用	• 事前に決められた作業明細書に従って、CyberSparkと直接価格交渉を行い、費用を決定。
期間	• 基本的なサービス期間は3-6ヶ月

[参考] CyberSpark "Soft Landing in CyberSpark"
(http://media.wix.com/ugd/9be112_40f13f3f27a841b19f98ba3f1b97a6ab.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-7. CyberSpark / Landing-Pad (2/2)

HITACHI
Inspire the Next

- CyberSparkが提供するLanding-Padにおいては、特にイスラエルでのビジネスを成功させるためのモノ・情報面の支援と人材面の支援が手厚い。

分類	支援内容
モノ・情報の支援策	• **活発な情報交換及び適切な情報管理** ➢ 産業界の研究機関や大学と隣接しているため、参画企業はかかる団体と日常的にアイディア交換が可能。 ➢ 一方で、プロジェクトの期間中、知的財産の登録、共同研究における知的財産の保護、セキュリティ規制を考慮する。 • **適切なチャネル選択のため情報提供** ➢ CyberSparkにR&Dセンターを設立する際には、サイバー分野での豊富な経験とイスラエルでの深い知識に基づいて、最適なチャネル(例:地元の起業家との合弁事業、多国籍企業との合弁事業の開始)を選別するための情報を提供する。
金銭面の支援策	• **財務面からの事業性の評価** ➢ 専門チームが支援を行い、財務面の分析を行うことで、イスラエルでの出資(例:新たな企業の設立)の可否やビジネスの結果得られる利益等の評価を行う。
人材面の支援策	• **サイバー分野におけるプロジェクトマネージャーの採用支援** ➢ イスラエルのサイバー分野におけるネットワークからプロジェクトをリードするマネージャーやディレクターを採用できるよう企業側を支援。また、その際の給与や雇用条件の見積支援を行う。 • **イスラエルに精通したプロジェクトチームの組織** ➢ 主に以下の分野から専門チームを結成し、プロジェクトを支援する。例えば、行政分野においてはまた、現地での手続きや規制への対応の支援を行う。 ◆ サイバー分野(例:技術に精通した研究者) ◆ イスラエル市場(例:中小企業、多国籍企業、プロバイダー) ◆ 行政分野(例:政府、助成金に精通した人材)

[参考] CyberSpark "Soft Landing in CyberSpark"
(http://media.wix.com/ugd/9be112_40f13f3f27a841b19f98ba3f1b97a6ab.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

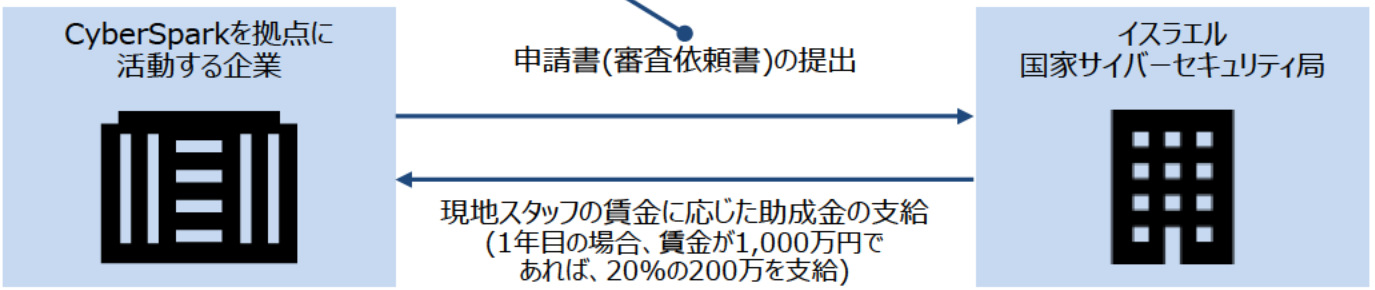
1.2-7. CyberSpark / 政府による補助金

- 以下の資料では、政府補助金による広範なインセンティブや多額の部分的資金援助が用意されている。
- 例えば、現地のサイバーセキュリティ分野のスタッフを採用する際、以下の割合で助成金を企業に対して支給されており、実質的な政府補助金として機能している。

政府補助金の仕組み (※1)

<条件>
- 勤務時間の少なくとも60%が国立サイバー・アリーナで行われる。
- 労働時間の少なくとも80%がサイバー関連活動

※ただし、以下は除く
- 政府または政府予算による他の機関から既に他の手当を受けている従業員
- 国立サイバー・アリーナにおいて、国との契約により直接または下請け業者を通じて雇用される従業員。



年	1年目	2年目	3年目	4年目	5年目	6年目	7年目
賃金に対する政府の助成率	20%	20%	20%	15%	15%	10%	5%

※1　2015年の政府決議に基づき支給

[参考] Yumpu" WHY CYBERSPARK?"
(https://www.yumpu.com/en/document/view/57004628/why-cyberspark)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-8. 国家サイバーセキュリティ協力センター/ センターの基礎情報

- 国家サイバーセキュリティ協力センターは、ソウルから20キロ程度の距離に位置する国家情報院(※)が所管する機関。国家情報院、科学技術情報通信部、国防部に加えて、民間のIT企業も参加。

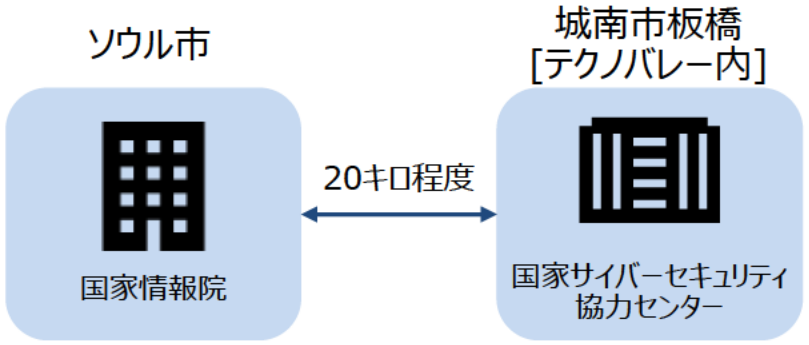
基本情報

項目	内容
設立年度	• 2022年11月 (2020年12月15日に改正された「国家情報院法」に基づき設立)
場所	• 城南市板橋(パンギョ)第2テクノバレー内
構成	• 公的機関 (国家情報院、科学技術情報通信部、国防部など9つの機関) • 民間企業(AhnLab、East Security、S2W、Chainalysisなど8社)
規模 (人員/予算)	• 公的機関、民間企業合計で46名 • 企業数:8社 報道によると参加する機関/企業を40まで増やす計画

※国家情報院は、韓国の大統領直属の情報機関・秘密警察

立地

- ソウルから車で30分程度の城南市板橋(パンギョ)の第2テクノバレー内に設立。
- テクノバレーは、京畿科学技術振興院に設立された板橋テクノバレー支援団が管理運営業務を行うIT研究開発団地であり、韓国版シリコンバレーと呼ばれる。



- 官公庁が多い。
- 国家サイバーセキュリティ協力センターを所管する国家情報院やサイバー国防学科を有する高麗大学が立地。

- 科学技術情報部が運営する情報セキュリティクラスターを有する
- IT系の企業が多くテック系の人材が多い。

[参考] KOREA WAVE「民間の手を借りてサイバー攻撃に対抗…韓国国情院「安保協力センター」」(2022/12/30)
(https://koreawave.jp/%E6%B0%91%E9%96%93%E3%81%AE%E6%89%8B%E3%82%92%E5%80%9F%E3%82%8A%E3%81%A6%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E3%81%AB%E5%AF%BE%E6%8A%97%E9%9F%93%E5%9B%BD%E5%9B%BD%E6%83%85/)
You Tube「국정원 "내년 北 사이버 공격 거세질 것"...민관 합동대응 / YTN」
(https://www.youtube.com/watch?v=NHLy4htwU5A)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-8. 国家サイバーセキュリティ協力センター/ 主な活動内容

HITACHI
Inspire the Next

- 国家サイバーセキュリティ協力センターには以下の3つの活動を実施する。
- 本調査では、「コラボレーション」における脅威インテリジェンスの分析(項番2)について取り扱うものとする。

コミュニケーション (Communication)

1. 顧客が必要とするサイバー脅威情報をいち早く提供し、被害を未然に防ぐ。
2. 国民からのサイバーセキュリティ関連の提案や苦情を国の政策に反映させる。

コラボレーション (Collaboration)

1. 国家的なサイバー脅威を分析し、民間、公的機関、軍の参加を得て迅速に対応することで、被害の拡大を防ぐ。
2. 国内外のITサービスプロバイダーと共同で脅威インテリジェンスを分析し、攻撃パターンと攻撃源を特定する。

共存共栄 (Co-Prosperity)

1. 優れた情報保護製品の官民への導入を支援し、技術および産業の発展を促進する。
2. 最先端のセキュリティ技術に対処する方法を訓練し、サイバー脅威への対応能力を強化する。

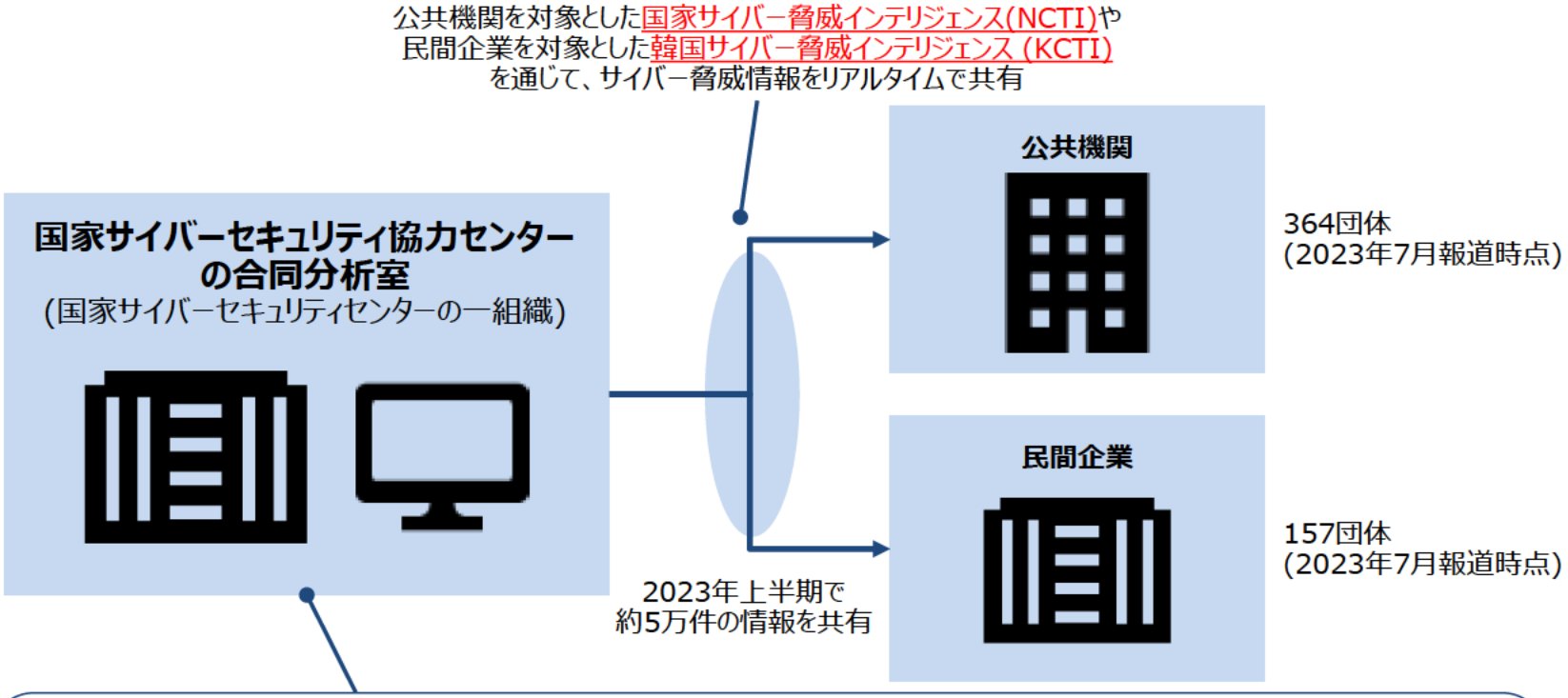
[参考] National Cyber Security Center “2022 Annual Report National Cyber Security Center”
(https://www.ncsc.go.kr:4018/main/PageLink.do#LINK)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-8. 国家サイバーセキュリティ協力センター/ 情報の共有・分析 (1/2)

HITACHI Inspire the Next

- 国家サイバーセキュリティセンターの一組織である国家サイバーセキュリティ協力センターがサイバー脅威の動向や技術を分析した上で、国内のサイバー脅威インテリジェンスを活用し、公共機関や民間企業に対してサイバー脅威情報を共有。



<実施主体>
以下の団体が参加しし、合同分析室(次頁参照)にて分析を実施。
- [公共機関] 国家情報院、科学技術情報通信部、国防部などの関係機関の専門家
- [民間企業] AhnLab、East Security、S2W、ChainalysisなどITセキュリティ企業の技術者

<実施事項(例)>
- ランサムウェアや仮想資産窃盗などのサイバー脅威の動向や技術の共同分析、分析報告書の作成
- マルウェアや侵害指標などの脅威情報の共有

[参考] 보안뉴스"[대한민국 사이버범죄, 우리가 막는다-1] 국가사이버안보협력센터"(2023/7/24)
(https://m.boannews.com/html/detail.html?idx=120426)

© Hitachi, Ltd. 2024. All rights reserved.

1.2-8. 国家サイバーセキュリティ協力センター/ 情報の共有・分析 (2/2)

HITACHI
Inspire the Next

- 国家サイバーセキュリティ協力センターの合同分析室では、常駐しているIT事業者を中心として、サイバー脅威の動向や技術の共同分析等を実施。



[引用] news1 KOREA "[르포]민관 협력의 '심장'…국정원 '국가사이버안보협력센터' 가보니"
(https://www.news1.kr/articles/?4902820)

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 国家情報セキュリティ基本ガイドライン

- 国家情報院が定める「国家情報セキュリティ基本ガイドライン」には、発注機関内で請負事業者が作業を行う場合の作業場所に係るセキュリティについて定めている。
- 請負事業者が作業を行うネットワークは発注機関と分離しなければならず、避けられない場合にはアクセス制御等のセキュリティ対策を講じることを規定している。

項番	規定内容(抜粋)
第27条の2 (発注機関内の作業場所のセキュリティ)	① 各級機関の長は、発注機関内(機関長が賃借した外部事務所を含む)に請負業者の作業場を設置する場合、セキュリティ制御が可能な空間を設けて運営しなければならない。 ② 発注機関内の請負業者の作業場に設置・運営するネットワークは、発注機関のネットワークと分離しなければならない。ただし、請負業者が事業遂行のために発注機関の情報システムの利用が避けられない場合には、必要な情報システムに限って指定された端末からの限定的なアクセスを許可するなど、一定のセキュリティ対策を施行しなければならず、この場合、内部ネットワークの情報システムへのアクセス許可については、国家情報院長と事前に協議しなければならない。 ③ 作業場所内の情報システムは、役務事業の遂行に必要な場合、当該情報化事業担当官のセキュリティ管理の下でインターネットに接続することができる。ただし、発注機関の情報システムアクセス用端末の場合には、インターネット接続を禁止する。

<参考>
国家情報セキュリティ基本ガイドライン:各機関における情報セキュリティ基本業務を規定

[参考] 국가정보보안기본지침(2023.1.31부)
(https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18588&pageIndex=1)

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2. 機微技術保有組織のサイバーセキュリティの確保に関する調査

© Hitachi, Ltd. 2024. All rights reserved.

調査項目及び整理の観点等

HITACHI
Inspire the Next

- 調査対象とする国ごとに、大学を対象にした取組み及び企業を対象にした取組みの双方について、以下を整理した。
  - リスクに対する考え方
  - 対象となる事業、情報の分類等
  - 具体的な要求事項の内容

分類	調査項目	整理の観点等
1 大学を対象にした取組み	1-1 リスクに対する考え方	• 「研究インテグリティ」、「研究セキュリティ」の全体像 • 全体像におけるサイバーセキュリティの位置づけと具体的な脅威認識 • 具体的なインシデント事例
	1-2 対象となる事業、情報の分類等	• 規制対象となっている対象の類型(例：政府資金活用の有無) • 機微技術として扱う情報の類型
	1-3 具体的な要求事項の内容	• 政府機関または資金配分機関から大学・その他の研究機関及び研究者に課せられるセキュリティ要求事項 • 上記要求事項を実施するにあたり指摘されている現状の課題
2 企業を対象にした取組み	2-1 リスクに対する考え方	• 念頭に置くリスクの全体像 • 全体像におけるサイバーセキュリティの位置づけと具体的な脅威認識 • 具体的なインシデント事例
	2-2 対象となる事業、情報の分類等	• 規制対象となっている対象の類型(例：政府資金活用の有無) • 機微技術として扱う情報の類型
	2-3 具体的な要求事項の内容	• 企業及び技術者に課せられるセキュリティ要求事項 • 上記要求事項を実施するにあたり指摘されている現状の課題
3 対応事例	3-1 機微技術等漏洩後の対応事例	• 機微技術漏えい発覚後の一般的な対応の流れ • 事案の概要、対応のタイムライン • 行政機関及び司法機関の対応

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.1 米国の動向

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.1.1 大学・研究機関を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

米国施策の背景

- 世界の科学研究をリードしている米国では、80年代の国家安全保障決定189号(NSDD-189)に代表されるように、可能な範囲で、オープンサイエンス(科学の開放性)原則の優位性を確認してきた。
- 一方で最近では、2018年に表面化した米中貿易摩擦からハイテク技術覇権争いにまで発展した議論の中で、オープンサイエンス原則が悪用され、国家安全保障の脅威になりかねないという問題が提起されており、開放性原則に制限をかける必要性をめぐる議論が、主要な連邦ファンディング機関や研究コミュニティを中心に改めて喚起されつつある。

オープンサイエンスの推進

- 1985年にレーガン政権は**国家安全保障決定189号(NSDD-189)**を発令。
- NSDD-189は「科学・工学における基礎・応用研究」を2種類に区別し、そのうち**「基盤研究」に「最大限の範囲」を与え、「原則的に制限を受けない」ことを宣言**。
  - ✓ 基盤研究(Fundamental Research)
  - ✓ 格付けされた研究(Classified Research)
- NSDD-189は科学研究を制限する法的ルールの基礎となり、現在に至るまで科学研究における「開放性原則」の連邦規制の基礎となっている。

国家安全保障の強化

- オバマ政権は、**大統領令13556号にて管理すべき非格付け情報(CUI)の管理強化を志向**したが、CUIレジストリには学術研究の実施に直接関係する部門やカテゴリーがないとされており、CUI関連規制の適用については明確ではない状況。
- さらに、国際武器取引規則(ITAR)、輸出管理規則(EAR)及び輸出管理改革法(ECRA)等の輸出管理に関する法律を通じて、**「新興技術」と「基盤的技術」に対する輸出規制に着目**し、科学研究への制限が厳しくなるという見通しがある。

[出典] JASON “Fundamental Research Security”
https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

© Hitachi, Ltd. 2024. All rights reserved.

米国施策の全体像

HITACHI
Inspire the Next

- 前頁の動向を受け、研究活動に対する統制(研究セキュリティ・研究インテグリティ)について、2019年から政府外での動きが現れ、2021年以降に大統領府及び連邦議会でのルール形成が盛んに実施されている。

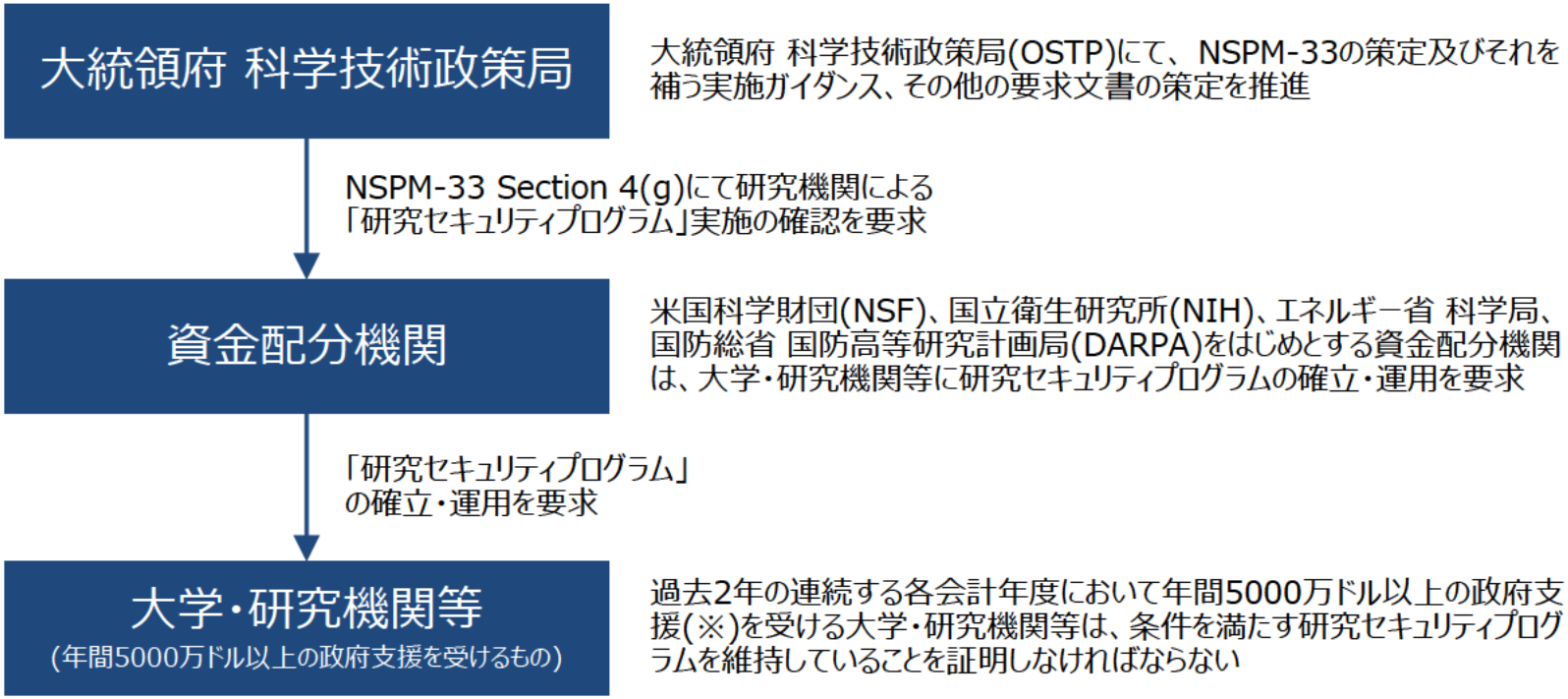
	大統領府等の動き	連邦議会の動き	その他の動き (米国大学協会と公立・ランドグラント大学協会等)
2019年			学内における安全保障上の脅威と外国の不当な影響に関する懸念の増大に対処するための大学によるアクション
2020年			学内における安全保障上の脅威と外国政府の不当な影響に関する懸念に対処するための大学によるアクション
2021年	国家安全保障大統領覚書33号(NSPM-33) ・研究セキュリティ・インテグリティ確保のための連邦省庁等への要求事項を規定	2021年 国防権限法 ・第223条で、すべての連邦研究機関(資金配分機関)が、現在及び未決の支援についての情報開示を、申請する研究者から求めること等を義務付け	大学の研究における外国政府の干渉に関連する対応をガイドする原則と価値観 ・政府の動きに先立って、米国大学協会(AAU)と公立・ランドグラント大学協会(APLU)が研究インテグリティ・研究セキュリティに関する複数の文書を公開
2022年	国家安全保障大統領覚書33号(NSPM-33)実施ガイダンス ・連邦省庁に対してNSPM-33の実施に関する指針を提供するため、より詳細なガイダンスを提示	CHIPS・科学法 ・研究セキュリティ関連規定として、米国科学財団(NSF)に Research Security and Policy Office の設置、助成の申請時にNSFがリスク評価を実施する権限の付与、大学・研究機関がセキュリティリスクを理解し軽減できるよう独立したリスク評価センターを設立すること、等の規定を含む。	米国アカデミー報告書「米国の技術優位を保護する」 ・国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言を実施
2023年	研究セキュリティプログラム標準要求事項(草案) ・NSPM-33 実施ガイダンスの最後の条項である「研究セキュリティプログラム」に関して具体的内容を規定		

[出典] 未来工学研究所, “研究インテグリティ（Research Integrity）に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_3.pdf

© Hitachi, Ltd. 2024. All rights reserved.

研究セキュリティ確保に向けた施策の推進体制(概要)

- サイバーセキュリティに関するものを含む研究セキュリティに関する上位ルールの策定は、主に大統領府 科学技術政策局(OSTP)が担っている。
- 定められたルールに基づき、資金配分機関(NSF、NIH、DARPA等)は、条件を満たす大学・研究機関において「研究セキュリティプログラム」が確立・運用されているかを確認する。



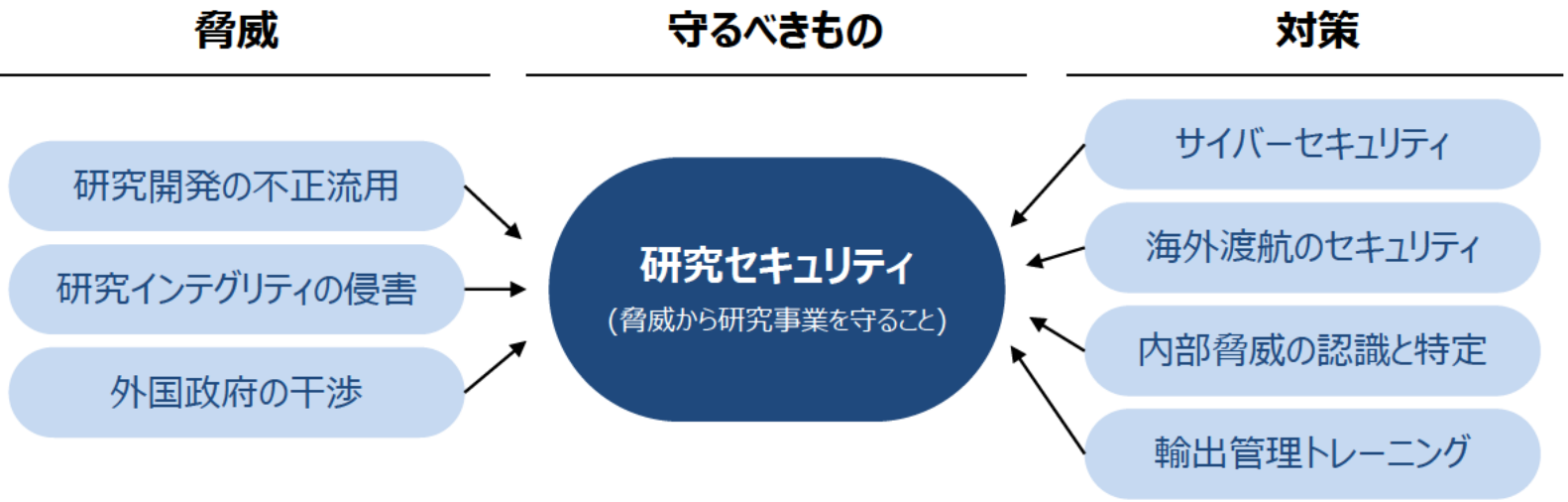
※プロジェクトの全部または一部に米国政府が資金を提供する研究開発プロジェクト、研究開発を実施するために米国政府の設備または施設を使用するプロジェクト、およびプロジェクトの資金源に関係なく米国政府の職員および請負業者の職員が参加する研究開発プロジェクトを含む。

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-1. リスクに対する考え方

HITACHI
Inspire the Next

- 研究セキュリティとは、「国家安全保障や経済安全保障を害する研究開発の不正流用、それに関連する研究インテグリティの侵害、外国政府の干渉から研究事業を守ること」であり、サイバーセキュリティ、海外渡航セキュリティ、内部脅威の認識と特定、および輸出管理トレーニングの要素が対策に含まれる。



文献	記載
GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33)	研究セキュリティ - 国家安全保障や経済安全保障を害する研究開発の不正流用、それに関連する研究インテグリティの侵害、外国政府の干渉から研究事業を守ること Research security – Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.
	機関の研究セキュリティプログラムには、サイバーセキュリティ、海外渡航のセキュリティ、内部脅威の認識と特定、および必要に応じて輸出管理トレーニングの要素を含めるべきである。 Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training.

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-2. 対象となる事業、情報の分類等

HITACHI
Inspire the Next

- NSPM-33に示される研究セキュリティプログラム確立・維持の適用対象は、「過去2会計年度連続で、連邦科学技術支援を年間5,000万ドル以上受けている研究機関」とされている。
- CHIPS・科学法は、研究セキュリティ研修に関する要件を、大学またはその他の研究機関の職員として連邦科学技術資金の受給を申請するすべての者に拡大した。

ルールの適用対象となる主体や条件等	
NSPM-33 (DRAFT Research Security Programs Standard Requirement)	• 過去2会計年度連続で、連邦科学技術支援を年間5,000万ドル以上受けている研究機関 [研究セキュリティプログラムの確立、維持] ※大学のような研究組織で、その構成部分(例えば、学科、附属研究センター、学校)が、合計で年間少なくとも5,000万ドルの連邦科学技術支援を受ける場合に適用される。研究組織が相互に連結された研究組織のネットワーク(例：公立大学システム)の一部である場合、この要件は、個別に年間5,000万ドル以上の連邦科学技術支援を受けているネットワーク内の個々の組織にのみ適用される。 • 機密情報および管理された未分類の情報(CUI)の取扱い [連邦研究機関(資金配分機関)による追加要件の提示]
CHIPS・科学法 (CHIPS & Science Act)	• 研究資金の公募申請の一部として申請書に記載された各対象者 [資金配分機関は、研究セキュリティ訓練の修了(過去1年以内)を認証するという要件を設ける] • 大学・研究機関 [雇用されている各対象者がそのような訓練を修了していることを証明]

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-3. 具体的な要求事項の内容 / サイバーセキュリティの位置づけ

HITACHI
Inspire the Next

- サイバーセキュリティ関連の取組みは、NSPM-33関連文書では「研究セキュリティプログラム」の一部を構成するものと捉えられる。

NSPM-33の重要領域におけるサイバーセキュリティの位置づけ

#	NSPM-33における重要領域	要求事項
1	開示要件と標準化	略
2	永続的なデジタルID	略
3	開示義務違反の結果	略
4	情報共有	略
5	研究セキュリティプログラム (Research Security Programs)	1. 研究セキュリティプログラムの要件 2. どの研究組織が要件の対象となるかの決定 3. 組織横断的なプログラム要件の標準化 4. 要件の最終決定と実施プロセス 5. 研究セキュリティプログラムの内容の開発 **6. 研究セキュリティプログラムのサイバーセキュリティ要素が要求事項の目的に適合していることの確認** 7. 要求事項への適合の認証 8. 研究セキュリティプログラム構築における研究機関の裁量 9. 研究機関がコンプライアンスを確立するまでのスケジュール

[出典] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL “GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT”
https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-3. 具体的な要求事項の内容 / サイバーセキュリティ対策の内容(1/2)

HITACHI
Inspire the Next

- 「研究セキュリティプログラム」におけるサイバーセキュリティ対策として、以下が求められている。
- 今年2月に公開されたDRAFT Research Security Programs Standard Requirementでも同様の事項が規定されているところ、覚書の公開(現状草案の段階)から1年以内の要求適合が求められる。

研究機関に実施を求める対策	• 情報システムの正規の利用者に対して、ソーシャル・エンジニアリングの脅威やサイバー侵害の認識と対応を含め、定期的なサイバーセキュリティに関する意識向上トレーニングを実施する。 • 情報システムへのアクセスを、正規の利用者、正規の利用者の代理として行動するプロセスまたは機器(他の情報システムを含む)に限定する。 • 情報システムへのアクセスを、正規のユーザが実行できるトランザクション及び機能に制限する。 • 外部情報システムへの接続を確認し、その利用を管理・制限する。 • 一般にアクセス可能な情報システムに掲載または処理される非公開情報を管理する。 • 情報システムの利用者、利用者の代理となるプロセスまたは機器を識別する。 • アクセスを許可する前提条件として、利用者、プロセス、または機器の身元を認証(または検証)する。 • 情報システムの外部境界及び重要な内部境界において、組織の通信(組織の情報システムによって送受信される情報)を監視、制御、及び保護する。 • 内部ネットワークから物理的または論理的に分離された、一般にアクセス可能なシステムコンポーネント用のサブネットワークを導入する。 • ランサムウェアやその他のデータインテグリティ攻撃メカニズムから科学データを保護する。 • 情報および情報システムの欠陥を適時に特定し、報告し、修正する。 • 組織の情報システム内の適切な場所で、悪意のあるコードからの保護を提供する。 • 新しいリリースが利用可能になった場合、悪意のあるコード保護メカニズムを更新する。 • 情報システムの定期的なスキャン及び、外部ソースからのファイルがダウンロードまたは実行される際にリアルタイムスキャンを実行する。
機密情報やCUIを取扱う場合の対策	• 機密情報やCUIを含む研究など、場合によっては米国立標準技術研究所(NIST)が提供するような追加のサイバーセキュリティ要件が適用される。

[出典] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL “DRAFT Research Security Programs Standard Requirement”
https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-3. 具体的な要求事項の内容 / サイバーセキュリティ対策の内容(2/2)

HITACHI
Inspire the Next

- DRAFT Research Security Programs Standard Requirementでは、
- 研究セキュリティプログラム確立後の研究機関に対して具体的な要求事項を定めている。

研究セキュリティプログラム確立後の研究機関に対する要求事項

要求事項への対応者	対応場所/相手	要求事項
助成金支援を受けている研究機関	自研究機関のWebサイト	• 研究セキュリティプログラムの確立に関する説明をウェブサイト上に記載 • 研究セキュリティに関する連絡窓口を指定し、ウェブサイトなどに連絡手段を記載
	SAM.gov※	• 条件を満たす研究セキュリティプログラムを維持していることをSAM.gov上で自己証明
	資金配分機関	• 資金配分機関から要請があった場合、30日以内に研究セキュリティプログラムを維持している旨の文書を提出 • 研究セキュリティ違反時、資金配分機関に報告
その他各研究機関内での実施事項		• 研究セキュリティ違反の申し立てに対処するために、明確な対応手順を作成・維持 • 研究セキュリティプログラムが機能していることを確認するため、定期的な自己評価を実施

※System for Award Management : U.S. General Services Administration が運営するウェブサイト

[参考] “DRAFT Research Security Programs Standard Requirement”
https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み

HITACHI
Inspire the Next

- 大統領府及び連邦議会を中心とした取組みに加え、NSFやNIH等の資金配分機関においても個別に研究セキュリティに関する施策が講じられているものの、サイバーセキュリティに係る推進事項は目立っていない。

資金配分機関	研究セキュリティに関する主な取組み
米国科学財団(NSF) ※1	• NSFの職員とNSFが資金を提供する機関及び研究者の両方に対して、NSFの「提案及び採択方針と手順ガイド」(PAPPG)の開示規則の遵守を強調 • すべてのNSF職員が米国市民であること、又は市民権を取得する過程にあることを要求 • NSF職員が外国人人材採用プログラムに参加することを禁止 • NSFの全職員に対して、毎年「科学とセキュリティのトレーニング」を義務付け • 研究セキュリティ分野の研究に特化した新たなプログラムである「研究セキュリティ研究プログラム(Research on Research Security Program)」の推進
国立衛生研究所(NIH) ※2	• 研究申請書における情報開示を通じた助成期間を通じての透明性確保 • 海外からの干渉(foreign interference)についてのコンプライアンスレビュー実施
エネルギー省 科学局 ※3	• DOE及び研究所職員による潜在的な利益相反及び責務相反への対処を中心とした多くの方針変更の実施 • 研究提案時等における情報開示の強化
国防総省 国防高等研究計画局(DARPA) ※4	• 「海外からの影響対策プログラム」(CFIP)を通じた、DARPAの研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を支援することを目的とした適応型リスク管理の推進

※1 Research Security at the National Science Foundation
https://new.nsf.gov/research-security
※2 Requirements for Disclosure of Other Support, Foreign Components and Conflicts of Interest
https://grants.nih.gov/policy/foreign-interference/requirements-for-disclosure
※3 Office of Science Laboratory Policy Science and Security
https://www.energy.gov/science/office-science-laboratory-policy-science-and-security
※4 DARPA website “Universities”
https://www.darpa.mil/work-with-us/for-universities

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み / NSFによる取組み

HITACHI
Inspire the Next

- NSFは、NIH、DoE、DoDと共同で、連邦研究費の受給者にグローバルな研究エコシステムに対するリスクと脅威に関する情報及びこれらのリスクから保護するために必要な知識とツールを提供する、4つのモジュールからなるオンライン研修の開発提案を募集している。
- 本研修は、NSPM-33やCHIPS・科学法の要求事項への対応にも活用され得る。

1 研究セキュリティはなぜ重要なイシューなのか？

この研修では、研究セキュリティの問題と、連邦政府資金による研究のセキュリティが米国政府と国家安全保障にとって重要である理由について説明する。

2 開示ポリシーとはいかなるものであり、どのように利用されるか？

この研修では、連邦資金提供機関の情報開示方針、なぜこの情報が重要なのか、そしてどのように利用されるのかを説明する。

3 連邦政府から資金提供を受けた研究者は、リスク管理・軽減のためにどのような行動を取ることができるか？

この研修では、強固なリーダーシップと監督を発揮し、透明性を促進し、利益相反やコミットメントを防止するための方針を確立・管理し、研究セキュリティに関する研修、支援、情報を提供し、組織の方針を遵守するための効果的な仕組みを確保し、共同研究やデータに関連する潜在的なリスクを評価・管理するプロセスを実施することで、次世代の研究者の育成を含め、組織が研究のスチュワード(受託責任者)としての役割をどのように果たすことができるかを取り上げる。

4 国際連携は推奨されるか？

この研修では、原則に基づいた国際共同研究は成功に不可欠であるが、不適切な外国の影響力は科学技術事業における国際共同研究の脅威であることを強調し、その重要な違いについて議論する。

[出典] Research Security at the National Science Foundation
https://new.nsf.gov/research-security

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み / NSFによる要求事項

HITACHI
Inspire the Next

- NSFは研究機関に対してNSFの共通ガイドラインとプログラム別のガイドラインの遵守を要求している。
- 共通ガイドラインにはサイバーセキュリティに関する記載として、データ管理計画の作成に関する要求事項があり、遵守しなければ、助成金が不許可となる。

要求事項	サイバーセキュリティに関する記載
共通ガイドライン、及びプログラム別ガイドラインの遵守	**共通ガイドライン** 以下の内容が含まれたデータ管理計画書を作成する •データおよびメタデータの形式と内容に使用される既存の標準がない、あるいは不十分であると考えられる場合は、提案されている解決策や改善策とともに文書化する。 •プライバシー、機密性、セキュリティ、知的財産権、その他の権利または要求事項の適切な保護に関する規定を含む、データへのアクセスと共有に関する方針。 •データの再利用、再配布、派生物の作成に関する方針および規定。 •データ、サンプル、その他の研究成果物の保管、およびそれらへのアクセス権の保全に関する計画。

[参考] NSF “Preparing Your Data Management Plan”
https://new.nsf.gov/funding/data-management-plan

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み / NIHによる要求事項

HITACHI
Inspire the Next

- NIHは研究機関に対して助成金ポリシー、助成金プログラムの利用規約と契約条件の遵守を要求している。
- ポリシーでは主に機密データ、情報の取扱いに関する要求をしている。

要求事項	サイバーセキュリティに関する記載
NIH助成金ポリシー	**NIH GRANTS POLICY STATEMENT** **2.3.12 機密データと研究で使用される情報の保護** •ポータブル電子機器に機密情報を保存しない。 •ポータブル電子デバイスを使用する場合、データや情報を暗号化する。 (電子デバイスの例：ラップトップ、CD、ディスク ドライブ、フラッシュドライブ) •パスワード設定等による、個人を特定できる情報へのアクセスを制限する。 •調査データは、受信者のセキュリティが確保されている場合のみ送信する。
利用規約、契約条件の遵守	•合格通知に記載されている助成金プログラムの規約 •文書または添付ファイルに引用されているすべての契約条件 ※上記はいずれも助成金獲得者のみに送付されるもので、 現時点では、記載内容を確認できていない
NSPM-33の遵守	※割愛

[参考]NIH “Award Conditions and Information for NIH Grants”
https://grants.nih.gov/grants/policy/awardconditions.htm

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み / DARPAによる要求事項 (1/2)

- DARPAは研究機関に対してDARPAの利用規約と個別助成金プロジェクト要項の遵守を要求している。
- それぞれの要求事項として、機密情報へのアクセス制限に関する言及やセキュリティマネジメント方法の提示要求がなされている。
- 助成金受領期間中のセキュリティ対策については、採択されて以降の契約で要求されると考える。

要求事項	サイバーセキュリティに関する記載
DARPAの共通利用規約	助成金受領者による機密情報へのアクセスは許可されない。 研究が機密扱いを必要とする場合、または機密データへのアクセス、保管を伴う場合、政府は、助成金受領者からの書面による通知受領後30日以内に、機密分類の必要性、またはそのようなアクセスもしくは保存の必要性について決定を下すものとする。
個別助成金プロジェクトの要項	**IV. 申請および提出情報** セクションⅡ.提案内容の詳細 K.セキュリティマネジメント • 申請者は、セキュリティ管理アーキテクチャおよび/またはアプローチを説明する 対象： CUI(制御された非機密情報)または秘密区分情報に対する情報システム認証、OPSEC、プログラム保護計画、テスト計画、輸送計画、異なる秘密区分の情報を使った作業、承認されていないテスト機器の利用 セクション IV. その他のコスト情報 4. セキュリティ情報 a. プログラム・セキュリティ情報 •申請者は、プログラム固有のセキュリティ要件について対応策を提案書に含める •申請者は、プロポーザルの内容について、秘密区分別の提出要件に従う (秘密区分別の提出方法は次頁に記載)

[参考] DARPA “Contract Management”
https://www.darpa.mil/work-with-us/contract-management

© Hitachi, Ltd. 2024. All rights reserved.

2.1.1-4. 資金配分機関による取組み / DARPAによる要求事項 (2/2)

HITACHI Inspire the Next

- DARPAはプロポーザルに含まれる情報の機密区分別に提出方法を指定している。

秘密区分	プロポーザルの提出方法
CUI(Controlled Unclassified Information)	CUIを含む場合、申請者は、CUIのセキュリティ要件を実行する人、及び情報システムが整備されていることを確認する。 1. CUI プロポーザルのマーキング CUI またはその疑いが含まれる場合、その情報に適切かつ目立つようにCUI マークを付けなければならない。 2. CUI 提出要件 CUI を含む未分類の提出物は、DARPAのBAAウェブサイト(プログラムの公募を行うサイト)を通じて提出する。 CUI情報処理権限を有する情報システムを有しているか、または契約締結前に取得できる必要がある。
未分類情報(Unclassified Submissions)	提案者が機密情報の提出を希望する場合は、電子メールをBAAメールボックスに送信し、プログラムセキュリティオフィスに通知する。
機密情報と非機密情報の両方の提出(Both Classified and Unclassified Submissions)	機密情報と非機密情報の両方を含むプロポーザルの場合、プロポーザルを非機密部分と機密部分に分けて提出する。
機密および秘密情報 (Confidential and Secret Information)	機密および極秘の機密情報は、以下の2つの方法のいずれかを通じて提出することができる。 • DARPA CDRから許可された宅配業者による手渡し。事前にDARPA Classified Document Registry（CDR）に連絡し、到着および引渡しの調整をすること。 • 米国郵政公社(USPS)、書留郵便またはUSPS速達郵便により郵送する。不透明な内カバーと外カバーで封入し、二重に包装する。内側の封筒は密封され、指定された分類と差出人および受取人の住所が明記されなければならない。
極秘情報(Top Secret Information)	極秘情報は、許可された配達業者がDARPA CDRまで手運びしなければならない。移動に先立ち、宅配業者はDARPA CDRに連絡し、到着および配達の調整を行うものとする。
機密扱い情報(Sensitive Compartmented Information)	機密扱い情報である旨、マークし、BAA メールボックスを経由して DARPA プログラムセキュリティオフィスに送るか、DARPA 特別セキュリティ責任者に連絡する。
特別アクセスプログラム情報 (Special Access Program Information)	特別アクセスプログラム情報である旨、マークし、プログラムセキュリティオフィスまたはそのスタッフによって提供される特別に承認された方法で送信されなければならない。

[参考] DARPA “Contract Management”
https://www.darpa.mil/work-with-us/contract-management

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.1.2 企業を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-1. 米国におけるデータ保護法制(全体像)

- CUI等があるが、防衛産業などの一部を除いて一般的に保護規制が課されているわけではない。
- 米国では、価値あるデータは営業秘密に該当する場合には営業秘密によって保護することが基本であり、連邦法によりサポートされる。アメリカの現行法において各法令がパッチワークのような状態であり、重複性もあるが、ロバスト性の高い保護を実現している。

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、営業秘密関連法、その他現行法、契約等によってロバスト性の高い保護を実現している。 一方で、契約関係にない第三者による不正取得等に対する懸念もある。	不正行為法リステイトメント	○		コンピュータ犯罪取締法(刑法第1030条)		○	懲罰的損害賠償	連邦著作権法(インターネット上のコンテンツを対象としたデジタルミレニアム著作権法)	-
	連邦経済スパイ法(EEA)		○						
	統一営業秘密法(UTSA)	○							
	連邦営業秘密保護法(DTSA)	○							

- 営業秘密は、州法におけるコモン・ローにより保護されてきたが、連邦刑事法において営業秘密の保護を強化するため、1996 年に連邦経済スパイ法が制定された。
- 近年まで連邦法としては、刑事的救済のみが取扱われ、民事的救済はもっぱら州法によっていたが、2016 年に連邦営業秘密保護法(DTSA)が制定されたことで連邦レベルでも民事的救済を求めることが可能となった。
- コンピュータ犯罪取締法では、コンピュータに対する不正なアクセス行為と、コンピュータ及びデータへ損害を与える行為を連邦レベルで規制している。

- 懲罰的損害賠償により、実際に生じた損害の金額を超える賠償額が認められる場合がある。
- 1998 年に制定されたデジタルミレニアム著作権法が策定されるも、データ保護手段として著作権は適切ではないとみられている。

[出典] 平成２９年度産業経済研究委託事業 海外におけるデータ保護制度に関する調査研究 調査報告書
https://www.meti.go.jp/policy/economy/chizai/chiteki/keizaisanngyou29.pdf

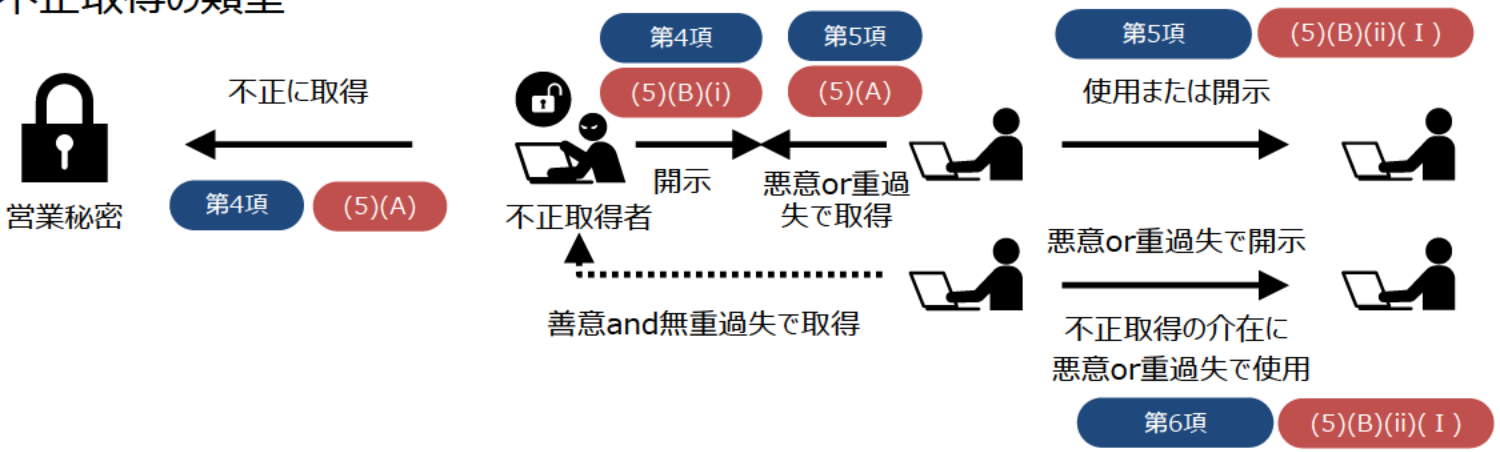
© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-2. 民事事案の違法行為類型(1/2)

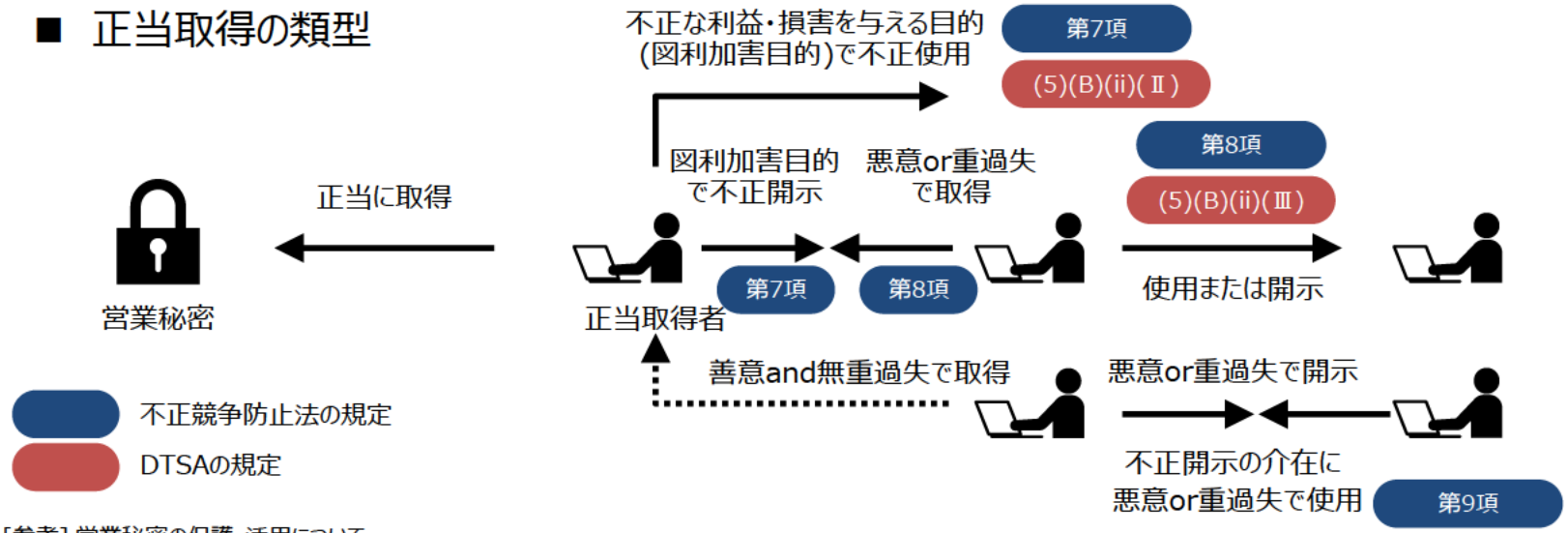
HITACHI
Inspire the Next

- DTSAにおける不正利用の類型と不正競争防止法における不正利用の類型とは、偶然または過誤による営業秘密の開示を受けた場合の規律を除いて、おおむね共通している。

■ 不正取得の類型



■ 正当取得の類型



[参考] 営業秘密の保護・活用について
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706tradesec.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-2. 民事事案の違法行為類型(2/2)

HITACHI
Inspire the Next

- DTSAにおける不正利用の類型と不正競争防止法における不正利用の類型とは、偶然または過誤による営業秘密の開示を受けた場合の規律を除いて、おおむね共通している。
- 一方で、DTSAでは「窃取、贈収賄、虚偽表示」「スパイ行為」に加えて「秘密保持義務違反」を不正な手段の例としている点、秘密保持義務または使用制限義務に違反した使用・開示行為を不正利用として規律している点(不正競争防止法では、「図利加害目的」のものが対象)が双方で異なる。

連邦営業秘密保護法(DTSA)	不正競争防止法
不正な手段により営業秘密を取得する行為 [18 U.S.C §1839(5)(A)] 不正取得者が同意なく営業秘密を使用・開示する行為 [18 U.S.C §1839(5)(B)(i)]	窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為(営業秘密不正取得行為)または当該行為により取得した営業秘密を使用もしくは開示する行為 [2条1項4号]
秘密保持義務または使用制限義務を負っていることを知りながら、または知りうべき理由がありながら同意なく使用・開示する行為 [18 U.S.C §1839(5)(B)(ii)(Ⅱ)]	保有者から示された営業秘密を図利加害目的で使用・開示する行為 [2条1項7号]
偶然または過誤により取得された営業秘密であることを知りながら、または知りうべき理由がありながら自己の地位を実質的に変化させて、同意なく使用・開示する行為 [18 U.S.C §1839(5)(B)(iii)]	
不正取得された営業秘密であることを知りながら、または知りうべき理由がありながら転得する行為 [18 U.S.C §1839(5)(A)] 上記で転得した営業秘密を同意なく使用・開示する行為 [18 U.S.C §1839(5)(B)(ii)(Ⅰ)]	営業秘密不正取得行為が介在したことを知って、もしくは重大な過失により知らないで営業秘密を取得または使用、開示する行為 [2条1項5号]
不正取得された営業秘密であることを知りながら、または知りうべく理由がありながら同意なく使用・開示する行為 [18 U.S.C §1839(5)(B)(ii)(Ⅰ)]	取得後に営業秘密に営業秘密不正取得行為が介在したことを知って、または重大な過失により知らないで当該営業秘密を使用または開示する行為 [2条1項6号]
秘密保持義務または使用制限を負っている者からもたらされた営業秘密であることを知りながら、または知りうべき理由がありながら同意なく使用・開示する行為 [18 U.S.C §1839(5)(B)(ii)(Ⅲ)]	営業秘密不正開示行為であることもしくは営業秘密不正開示行為が介在したことを知って、若しくは重大な過失により知らないで営業秘密を取得または使用、開示する行為 [2条1項8号]
	営業秘密不正開示行為があったこともしくは営業秘密不正開示行為が介在したことを知って、または重大な過失により知らないで営業秘密を使用または開示する行為 [2条1項9号]

[参考] アメリカにおける営業秘密の保護(2)：連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/78741/1/55_01-Yamane.pdf

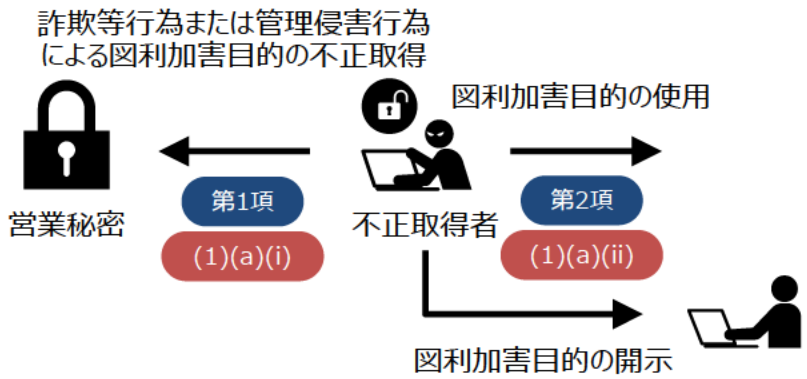
© Hitachi, Ltd. 2024. All rights reserved.

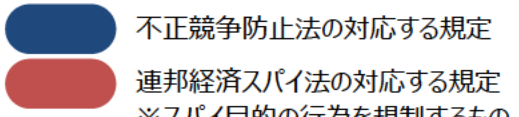
2.1.2-3. 刑事事案の違法行為類型(1/2)

HITACHI
Inspire the Next

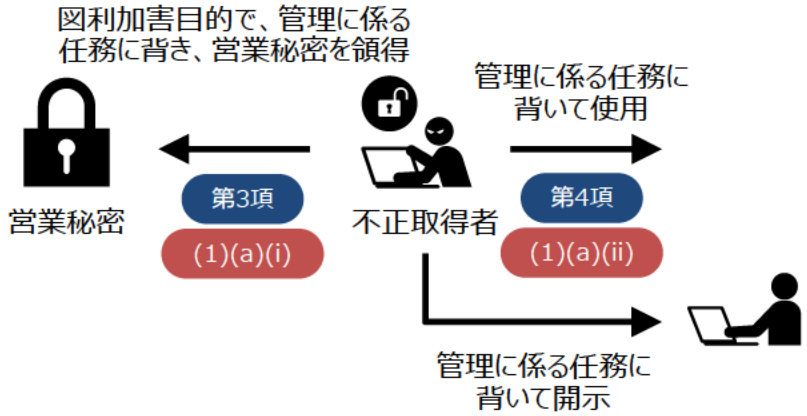
- 違法行為を類型化する際の考え方は異なるが、刑事規制の対象としている行為の範囲は日本と米国で概ね重なってる。

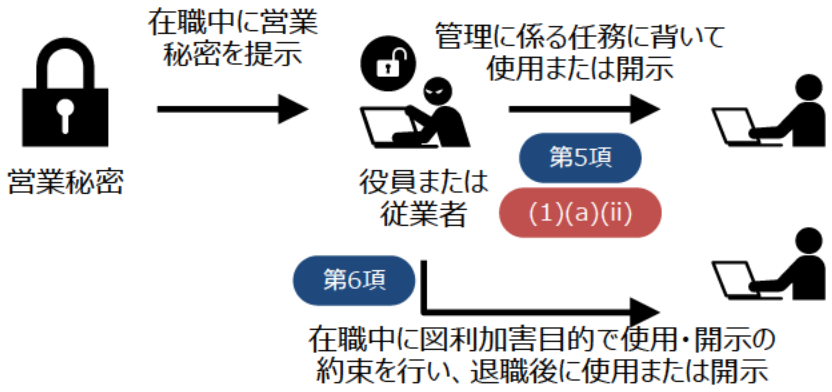
■ 不正な手段による取得





■ 正当に営業秘密が示された者による背信行為





[参考] 営業秘密の保護・活用について
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706tradesec.pdf

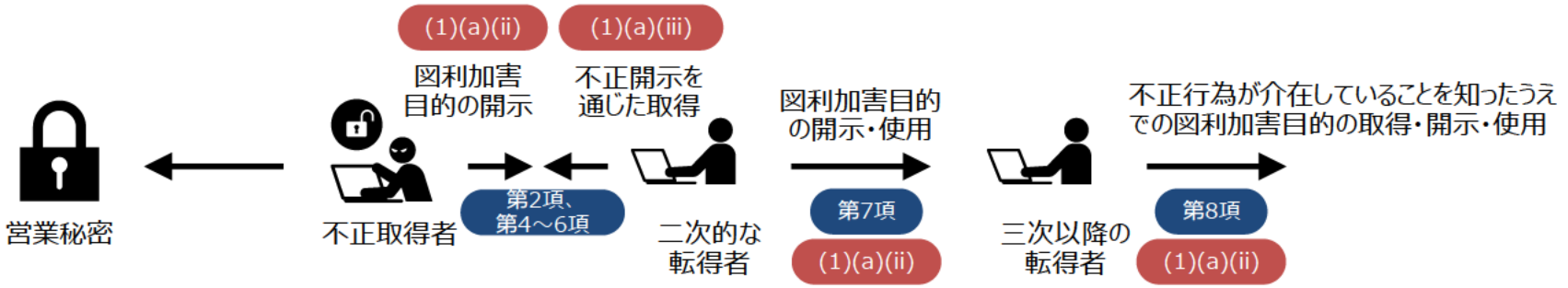
© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-3. 刑事事案の違法行為類型(2/2)

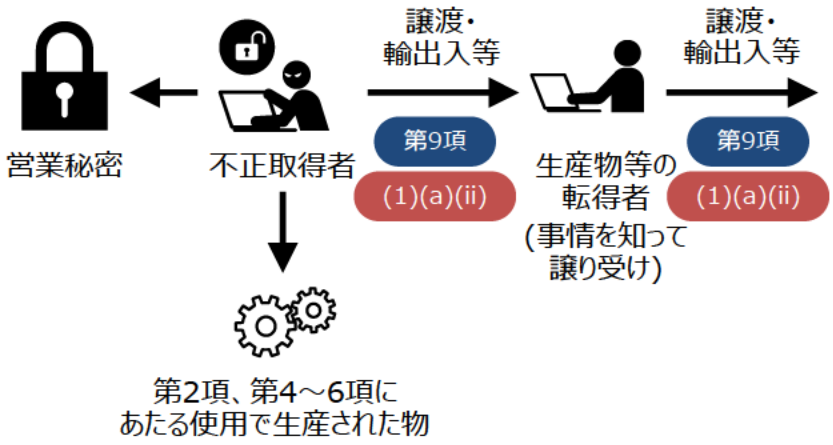
HITACHI
Inspire the Next

- 違法行為を類型化する際の考え方は異なるが、刑事規制の対象としている行為の範囲は日本と米国で概ね重なってる。

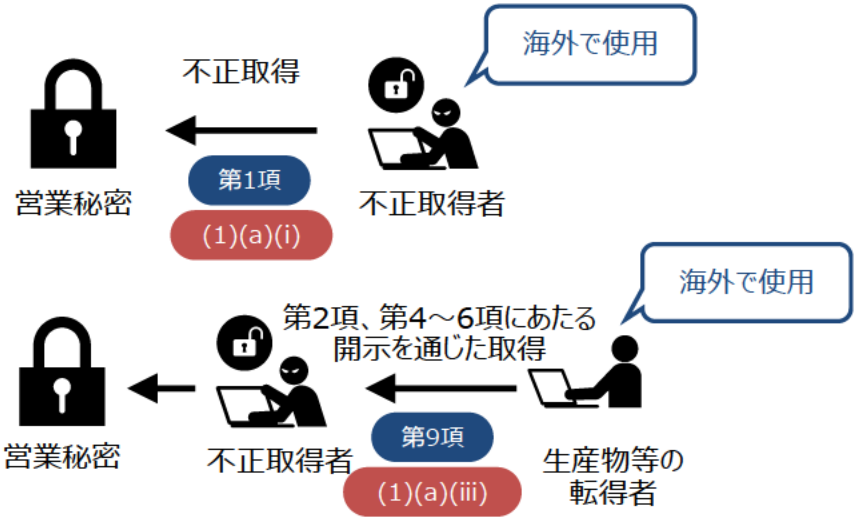
■ 転得者による使用・開示



■ 営業秘密侵害品の譲渡等



■ 海外重罰



[参考] 営業秘密の保護・活用について
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706tradesec.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-4. 刑事事案の罰則規定

HITACHI
Inspire the Next

連邦経済スパイ法(EEA)

(1) スパイ目的(産業スパイ)の営業秘密侵害

a. 外国政府、外国機関または外国の代理人に利益をもたらすことを意図して、または、それを知る者が、故意に以下を行うこと
   i. 盗難または許可のない流用、取得、持ち去りあるいは隠蔽及び、偽りまたは欺瞞による営業秘密の取得
   ii. 許可のない営業秘密のコピー、複製、スケッチ、描画、撮影、ダウンロード、アップロード、変更、破棄、複写、模造、送信、配信、送付、郵送、通信または伝達
   iii. 営業秘密が盗難または許可のない流用、取得、変換されたものであることを知ったうえでの受取り、購入、所持
   iv. (i)から(iii)のいずれかに記載されている違反を犯そうとすること

(2) 非スパイ目的(産業スパイ)の営業秘密侵害

a. 営業秘密を領得する目的で、州間取引または外国取引で使用される、または、使用予定である製品もしくはサービスに関連して、その所有者以外の者の経済的利益に、営業秘密の所有者に不利益を与えることを、意図し、あるいは、知りながら、故意に、前条の行為を犯す場合に、罰金、10 年以下の懲役、又は、その両方を科す。

b. (a)に違反した組織には、500万ドル、又は、営業秘密の研究、デザイン、その他必要となる費用の回避分を含む、盗まれた営業秘密の価値の3倍を超えない額のいずれか高い金額で罰金を科す。

不正競争防止法

第二十一条　罰則

次の各号のいずれかに該当する者は、十年以下の懲役若しくは二千万円以下の罰金に処し、又はこれを併科する。

一 不正の利益を得る目的または営業秘密保有者に損害を加える目的(図利加害目的)で、詐欺等行為又は管理侵害行為(財物の窃取、施設への侵入、不正アクセス行為その他の営業秘密保有者の管理を害する行為)により、営業秘密を取得した者

二 詐欺等行為または管理侵害行為により取得した営業秘密を、図利加害目的で、使用または開示した者

三 営業秘密を営業秘密保有者から示された者であって、図利加害目的で、管理に係る任務に背き、次に掲げる方法で営業秘密を領得した者
   イ 営業秘密記録媒体等または営業秘密が化体された物件の横領
   ロ 営業秘密記録媒体等の記載、記録または営業秘密が化体された物件の複製の作成
   ハ 営業秘密記録媒体等の記載または記録で、消去すべきものを消去せず、かつ、当該記載又は記録を消去したように仮装すること

四 営業秘密を営業秘密保有者から示された者であって、その営業秘密の管理に係る任務に背いて領得した営業秘密を、図利加害目的で、管理に係る任務に背き、使用または開示した者

五 営業秘密を示された役員または従業者であって、図利加害目的で、管理に係る任務に背き、営業秘密を使用しまたは開示した者

六 営業秘密を示された役員または従業者であった者であって、在職中に図利加害目的で、管理に係る任務に背いて営業秘密の開示の申込み、使用もしくは開示について請託を受けて、職を退いた後に営業秘密を使用または開示した者

七 図利加害目的で、二、三の罪に当たる開示によって営業秘密を取得、使用または開示した者

八 図利加害目的で、二または四から七までの罪、第三項第二号の罪に当たる開示が介在したことを知って営業秘密を取得、使用、開示した者

九 図利加害目的で、自己又は他人の二または四号から八、第三項第三号の罪に当たる行為(違法使用行為；技術上の秘密に限る)により生じた物を譲渡、引き渡し、展示、輸出、輸入または電気通信回線を通じた提供を行った者

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-5. 連邦経済スパイ法(EEA)の課題

HITACHI
Inspire the Next

- 経済スパイや営業秘密の窃盗との闘いは連邦法執行機関にとって最優先事項である一方、連邦捜査局や司法省が投入できる資源には限りがあるため、営業秘密の窃盗を阻止するための刑事執行は依然として限定的とされている。

「連邦営業秘密保護法(DTSA)」に関する上院報告書

- 連邦レベルでは、合衆国法律集第 18 編第 1831 条他で法典化される 1996 年経済スパイ法(EEA)が、州際または外国に関連する企業秘密を不正流用することを連邦犯罪としている。しかし、EEA は、営業秘密所有者に連邦裁判所における私的訴権を与えていない。委員会は、**経済スパイや営業秘密の窃盗との闘いは連邦法執行機関にとって最優先事項である一方、連邦捜査局や司法省が投入できる資源には限りがあるため、営業秘密の窃盗を阻止するための刑事執行は依然として限定的な解決策である**ことを学んだ。

上院司法委員会Hatch上院議員による上院本会議指摘

- 最近、営業秘密を専門とする経験豊富な弁護士から聞いた話によると、**通常司法省が訴追を検討するのは、損害賠償額が10万ドルを超える事例だけ**だという。その理由は、営業秘密の捜査と訴追には他の連邦法上の犯罪よりも複雑な資源を集中して投じる必要があるため、極めて専門的で科学的な背景が求められる場合が多い点にある。こうした制約があるため、FBIと司法省はたった一つの問題の捜査や訴追に貴重な資源を費やすことに二の足を踏むのだ。
- したがって、**連邦経済スパイ法制定後の20年間に、連邦検察官が起訴した人物が300人程度に過ぎない**ことも意外ではない。しかも、訴追に至った事例では、多くの場合に被告人が複数であるために、訴追されるのは年間平均で10件程度にとどまっている。

[参考] アメリカにおける営業秘密の保護(1)：連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/73425/1/53_01-Yamane.pdf
DEFEND TRADE SECRETS ACT OF 2016 Report
https://www.congress.gov/114/crpt/srpt220/CRPT-114srpt220.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-6. 営業秘密侵害に係る救済措置等

HITACHI
Inspire the Next

- 米国DTSAには、一方的差押え(民事上の差押え)や懲罰的損害賠償、民事事案におけるDTSA等域外適用等の日本法では必ずしも整備されていない規定が散見される。

	DTSA/EEA	不正競争防止法
一方的差押え	• 不正な手段により営業秘密が不正利用された場合に、裁判所に対して自己の申告のみに基づいて必要な対象財産の差押えを求めることができる。(DTSA(18 U.S.C. §1836(b)(2))にて新たに導入) • 濫用を防ぐため、発令条件や差押え範囲が厳格に規定されている。 • 刑事上の差押えや刑事没収と区別して、民事上の差押え(civil seizure)と呼ばれる。	-
差止	• 営業秘密の侵害に対して裁判所の裁量で差止を付与できる。 • DTSAは裁判所に対して、「現に行われている不正利用」に対する差止めだけでなく、「行われる恐れのある不正利用」を防止するための差止めを発令する権限も認めている。	• 不正競争によって営業上の利益を侵害された/侵害されるおそれがある者は、営業上の利益を侵害する/侵害するおそれがある者に対し、侵害の停止または予防を請求することができる。 • 前項の規定による請求をするに際し、侵害の行為を組成した物の廃棄、侵害の行為に供した設備の除却その他の侵害の停止または予防に必要な行為を請求することができる。
損害賠償	• 営業秘密の不正利用により現実に損害を被ったことを立証すれば、現実の損害について賠償を受けることができる。また、原告が被った現実の被害を上回る利得を被告が不正利用により得ている等、現実の損害の算定では考慮されなかった不当利得を立証すれば、当該不当利得についても賠償を得ることができる。(填補的損害賠償) • 営業秘密の不正利用が故意かつ害意に基づいて行われた場合、より厳しい責任を求める懲罰的損害賠償が認められる場合がある。	• 故意又は過失により不正競争を行って他人の営業上の利益を侵害した者は、生じた損害を賠償する必要がある。
域外適用	• 連邦経済スパイ法では、1837条にて営業秘密の窃取や経済スパイ行為といった犯罪行為が米国外でなされた場合に、米国外で刑事訴追するための手段を提供している。 • 上記規定は、民事事案においても同様に適用される可能性がある。	刑事事案においては、国外において営業秘密に対する侵害行為が発生した場合にも罰則を適用する海外重罰・国外犯処罰規定(第21条第3項・第6項)が整備されている。

[参考] アメリカにおける営業秘密保護(3・完):連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/81694/1/59_02-Yamane.pdf
デジタル化に伴うビジネスの多様化を踏まえた不正競争防止法の在り方（案）
https://www.jpo.go.jp/resources/shingikai/sangyo-kouzou/shousai/chizai_bunkakai/document/18-shiryou/s04.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-7. 営業秘密関連争訟の状況(1/2)

HITACHI
Inspire the Next

- 日米間では訴訟数、秘密保持契約の取扱い、「不正取得」の事例割合等で大きな差異が見られる。

	米国(DTSA)	日本(不正競争防止法)
概況	• 2017年以降、連邦地裁では平均すると年間700件を超えるペースで訴訟が提起されている。	• 2006年から2015年までに94件の訴訟が確認されている。(仮処分や和解の事案は未確認)
営業秘密要件に基づく請求棄却事由	• 訴訟全体の請求棄却率は41%である。 • 非公知性・非容易確認性の欠如が棄却事由の23%を占めるが、合理的な秘密保持措置の欠如は11%を占めるにとどまる。	• 訴訟全体の請求棄却率は87%である。 • 秘密管理性の欠如による棄却が51%を占め、他の要件(非公知性の欠如は米国と同じ23%)と比較して突出して多い。
不正取得に係る争訟等の状況	• 不正利用が肯定された事例のうち、76%が不正取得の事例とされる。 • 不正取得事例のうち、89%のケースでは契約上の秘密保持義務を負っている者が不正取得の行為者として認定されている。 • 無権限の被告が原告のネットワークに不正アクセスして営業秘密を取得したと主張されたケースは全体の9%にとどまる。	• 不正利用が肯定された事例のうち、不正取得の事案は35%にとどまる。 ※「不正の手段」に秘密保持義務違反が含まれるかは、当該違反が窃取等と評価されるかに依存する。
不正使用・開示に係る争訟等の状況	• 訴訟では、被告の不正利用について、秘密保持契約に違反した取得、使用、開示の事実が併せて主張されることが多い。	• 不正利用肯定例の大半(71%)は不正使用・開示の事案となっている。 • 秘密保持義務や使用制限義務に違反した営業秘密の使用・開示行為について「図利加害目的」である点が否定されることは稀である。

[参考] アメリカにおける営業秘密の保護(1)：連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/73425/1/53_01-Yamane.pdf
アメリカにおける営業秘密の保護(2)：連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/78741/1/55_01-Yamane.pdf
The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112679

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-7. 営業秘密関連争訟の状況(2/2)

HITACHI
Inspire the Next

- 日米間では、差止め措置の認容率や損害賠償請求の実施率、域外適用に係る判例の状況等にて差異が見られる。

	米国(DTSA/EEA)	日本(不正競争防止法等)
一方的差押	• DTSAに関する訴訟は1000件以上提起されているが、一方的差押えが申し立てられた事案は約40~50件、認容事例は9件に留まる。 • 上記の原因は発令要件の厳しさによるとされる。	• 一方的差押えに関連するものとして、刑事事件において捜査機関が収集した証拠を民事事件の立証に活用することが議論されることがある。
差止	• 58%の営業秘密保有者が緊急差止め命令または暫定的差止め命令を申し立てた。 • 上記差止めの認容率も高い。 (緊急差止め：58%、暫定的差止め：58%)	• 差止めの請求率は58%だが、そうした事案における認容率は13%にとどまる。 • 特に、技術情報事案の認容率(20%)と比較して営業情報事案における認容率(5%)が低い。
損害賠償	• 損害賠償はトライアルにおいて陪審により審理判断されるが、そもそもトライアルまで進むケースは全体の1割に満たず、陪審審理の結果として損害賠償が認容された事例は3件にとどまる。	• 差止め(55%)よりも損害賠償(87%)を請求する事案が多く、認容率も差止め事案(13%)よりも損害賠償事案(17%)の方が高い。 • 損害賠償が主たる救済として機能している。
域外適用	• 管見の限り、民事事案において1837条に定めのある域外適用規定が否定された裁判事例は存在しない。 • DTSA域外適用の条件として、①窃取者が米国人か米国企業である、②窃取後に何らかの行為が米国内で発生したことが挙げられている。	• 渉外事案が散見される民事上の営業秘密侵害事案に係る国際裁判管轄・不競法の適用範囲について、現行法制を前提とした場合、裁判例等において定見は確立されていない。

[参考] アメリカにおける営業秘密の保護(3・完)：連邦営業秘密防衛法(DTSA)の運用実態と日本の営業秘密訴訟との比較
https://eprints.lib.hokudai.ac.jp/dspace/bitstream/2115/81694/1/59_02-Yamane.pdf
デジタル化に伴うビジネスの多様化を踏まえた不正競争防止法の在り方（案）
https://www.jpo.go.jp/resources/shingikai/sangyo-kouzou/shousai/chizai_bunkakai/document/18-shiryou/s04.pdf

2.1.2-8. 刑事事案に関する争訟等の状況

HITACHI
Inspire the Next

- EEAに基づく起訴数は、特定国からの知財窃取等が特に問題となっている近年でも増えておらず、外国支援のスパイの起訴はさらに少数となっている。
- 一方で、外国からのサイバースパイ活動については依然として様々なものが指摘されている状況。

■ EEAに基づく起訴数

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
1831条 (国家支援型スパイ)	1	2	0	N.A.	15	10	1	2	1	2	2
1832条 (上記以外)	11	11	5				5	9	10	14	6

■ 2023年に報告された中国によるサイバースパイ活動

- 中国国家支援のハッカー集団が、2023年5月から米商務省と米国務省の機密扱いのないマイクロソフトの電子メール・サーバーに侵入し、閣僚に対するハッキングを成功させた。ハッカーはブリンケン長官のアカウントへのアクセスには失敗したものの、ニコラス・バーンズ駐中国大使やダニエル・J・クリテンブリンク東アジア担当国務次官補を含む複数の国務省高官の電子メールアカウントやライモンド商務長官のアカウントへの侵入に成功した。
- マイクロソフトは2023年5月、Volt Typhoonとして知られる中国国家支援のハッキング・グループが、グアムや他地域の重要インフラを標的にしていたと発表した。このキャンペーンは、政府、海事、通信、輸送、製造、情報技術などの分野の重要インフラ組織を標的としていたと報じられている。
- ロイターは2023年5月、中国の支援を受けたハッカーが3年間にわたってケニア政府に対してサイバースパイ活動を行ったと報じた。このハッキングでは、大統領府、ケニアの諜報機関、財務局、外務省を含むケニアの8つの省庁と政府部門が侵害された。
- マンディアントは2023年6月、バラクーダネットワークスの電子メールセキュリティシステムに最近発見された欠陥を大規模に悪用した背後に、中国国家を後ろ盾とするハッカーがいた可能性が高いと報告した。このハッカーは、さまざまな政府機関や民間組織(アジアとヨーロッパの政府関係者、ASEAN外務省、台湾と香港の学術研究者と組織を含む)のメールドメインやユーザーを含むデータを流出させたと報告されている。

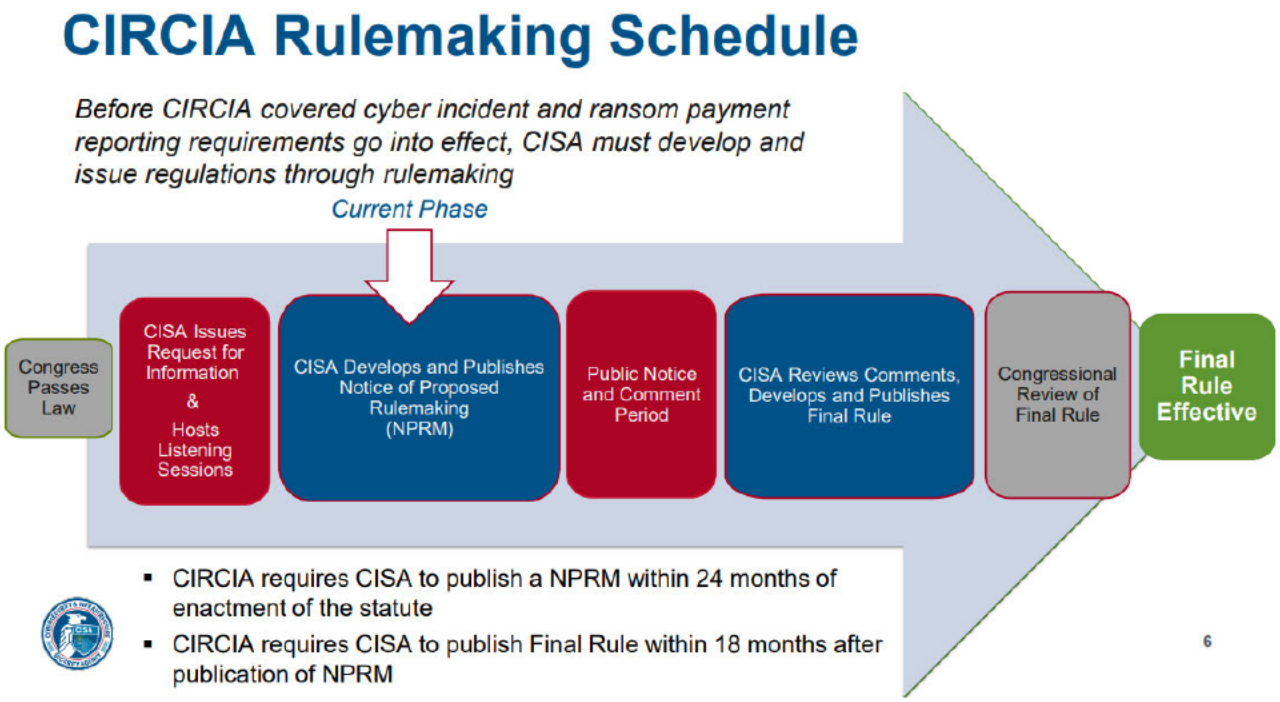
[参考] 諸外国における営業秘密保護制度に関する調査研究報告書
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H25FYshogaikokuchosa.pdf
PRO IP Act Annual Report
https://www.justice.gov/criminal-ccips/page/file/1392186/download
2023 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION
https://www.uscc.gov/sites/default/files/2023-11/2023_Annual_Report_to_Congress.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-9. 重要インフラインシデント報告規制 (1/2)

HITACHI
Inspire the Next

- 2023年8月時点では、CISA(サイバーセキュリティ・インフラセキュリティ庁)にて規制案を策定中である。
- 規制案を策定するにあたり情報提供要請を提出しており、CIRCIAの下で要求される報告書の形式、方法、内容、提出手順 等を含むインシデント報告要件、および規制の実施手順や情報保護方針 等に関する意見を特に募集している。



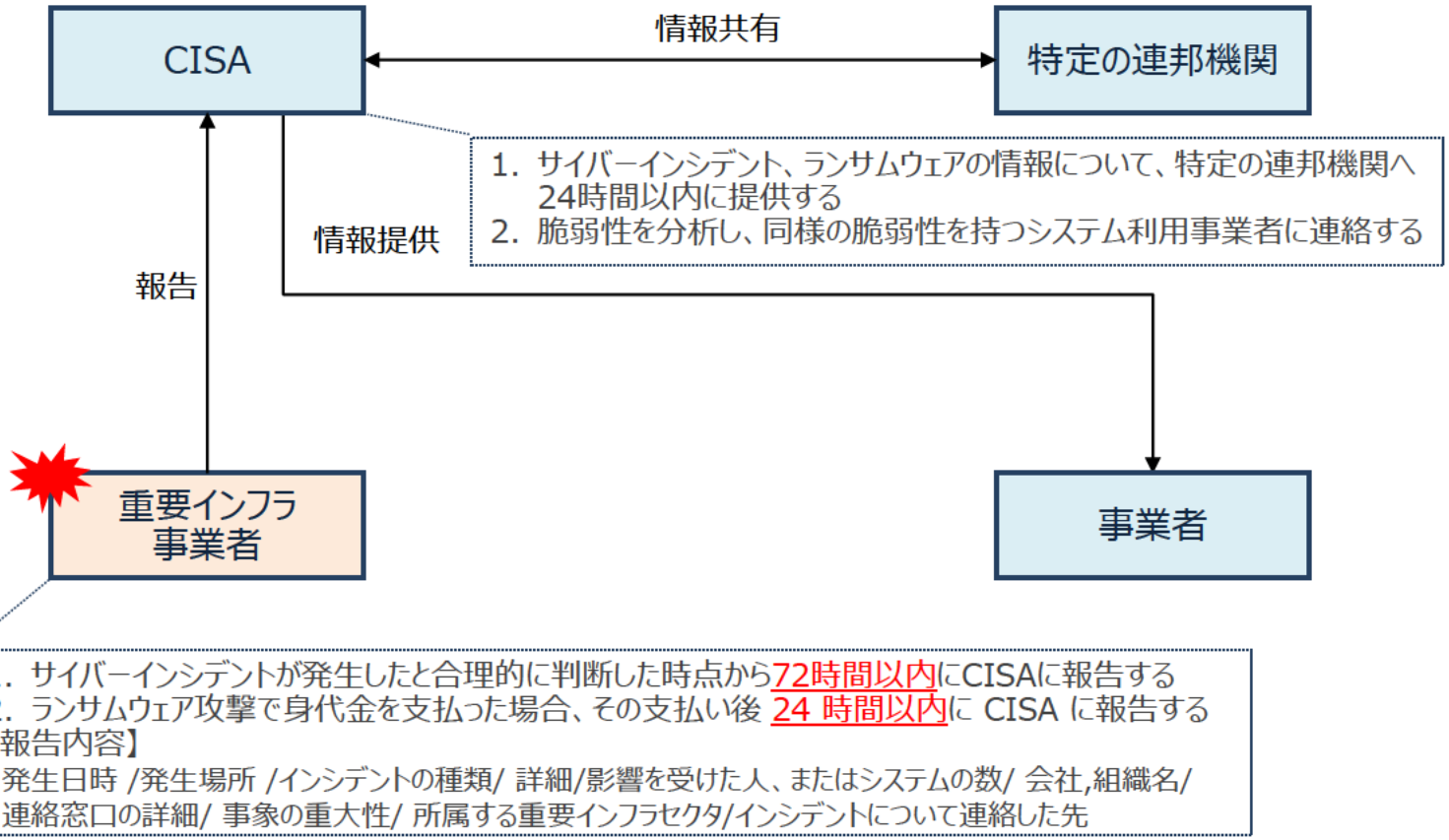
[参考] "CHEMICAL SECURITY SUMMIT August 2023"
https://www.cisa.gov/sites/default/files/2023-09/2023-summit-circia-508.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.2-9. 重要インフラインシデント報告規制 (2/2)

HITACHI
Inspire the Next

- インシデント報告フロー、及び報告内容についてはCISAで策定中であるが、現在公開されている情報では、報告対象はサイバーインシデントとランサムウェア(身代金を支払った場合)の2つがある。
- サイバーインシデントの場合、発生後 72時間以内にCISAへインシデント報告
- ランサムウェアの場合、身代金を支払ってから24時間以内にCISAへインシデント報告



[参考] CISA “CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA) FACT SHEET”
https://www.cisa.gov/sites/default/files/2023-01/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.1.3 機微技術流出後の対応事例

© Hitachi, Ltd. 2024. All rights reserved.

2.1.3-1. サイバー犯罪捜査のプロセス

HITACHI
Inspire the Next

- 米国におけるサイバー犯罪捜査の基本的な手順には、1. 状況の把握、2. 初期調査の実施、3. 可能性ある証拠の特定、4. 機器の保護と令状取得、5. 検察官との結果分析 を含むとされる。

1. 状況の把握
(Assess the Situation)

- 警察はまず、犯罪の具体的な要素と、管轄区域の法律が起訴をサポートしているかどうかを判断しなければならない。(例えば、有罪が証明されるとしても、告訴は維持できるのか。)
- 多くの新しい技術が使用されているため、コモンローや連邦法、州法が犯罪に追いついていないことが非常に多い。
- サイバー犯罪を調査する際には、インターネットのグローバルな性質も考慮すべきである。

2. 初期調査の実施
(Conduct the Initial Investigation)

- 通常の捜査と同様、誰が、何を、どこで、いつ、なぜ、どのように、を問いかける。
  - 容疑者候補は誰か。
  - どのような犯罪が行われたか。
  - 犯行はいつ行われたのか。
  - これらの犯行は米国の司法権下に限定されたものか。
  - 収集すべき証拠は何か。
  - 証拠はどこにあるか。
  - すぐに写真撮影・保存する必要がある証拠はあるか。
  - 裁判手続きのために証拠をどのように保存・維持できるか。

3. 可能性ある証拠の特定
(Identify Possible Evidence)

- デジタル証拠には、多くのファイルタイプやサイズがある。証拠が暗号化されていたり、保護されていたり、その他の方法で隠されている場合もある。
- このような証拠を特定し、収集するために必要なリソース、ツール、または特定の専門知識を有していない場合は、これらの能力を持つ他の機関と提携することを検討すべきである。

4. 機器の保護と令状取得
(Secure Devices and Obtain Court Orders)

- 機器の捜索を行うためには令状を取得しなければならない。特定の機器が複数の犯罪に関連している場合、複数の令状の取得が必要な場合がある。
- 令状には、捜索対象となるすべてのファイル、データ、及び電子機器をできるだけ具体的に明記し、オフサイトで分析を実施する承認を求める必要がある。

5. 検察官との結果分析
(Analyze Results with Prosecutor)

- 検察官と協力して、(既存のコモンローおよび州法・連邦法に基づいて)適切な告発を特定し、告発の前にどのような追加情報や証拠が必要になるかを判断することも重要になる。

[出典] CYBERCRIME INVESTIGATIONS
https://www.iacpcybercenter.org/officers/cyber-crime-investigations/

© Hitachi, Ltd. 2024. All rights reserved.

2.1.3-2. 事例検討 (1/5)

HITACHI
Inspire the Next

- これまで、外国から産業分野の知的財産等を標的としたサイバー活動が多数報告されているところ、司法省(DoJ)による訴追まで至ったケースが複数報告されている。

脅威グループ	概要	司法省の対応
APT1 (別名：Comment Crew, Comment Panda)	2013年2月のレポートでMandiantが初めて明らかにした人民解放軍第61398部隊に関連するサイバー脅威グループであり、少なくとも141の組織から数百テラバイトのデータを盗んでいる。司法省がサイバースパイ行為で外国を刑事告発した初めてのケースとなった。	2014年、司法省がAPT1のハッカー5人を、米国企業に対するサイバースパイ行為で起訴
APT3 (別名：UPS Team, Gothic Panda, TG-0110, Boyusec, Buckeye)	MSSPとして知られる中国のサイバーセキュリティ企業に関連するサイバー脅威グループ。APT3は、航空宇宙、防衛、建設、エンジニアリング、ハイテク、電気通信、運輸分野の組織を標的としている。シマンテックによると、2015年以降、APT3は米国を拠点とする被害者を標的とすることから、香港の政治組織にシフトしている。	2017年、司法省は、金融、エンジニアリング、テクノロジー業界の企業を商業利益のためにハッキングしたとして、ハッカー3人を起訴
APT10 (別名：Menupass Team, Stone Panda, POTASSIUM, Red Apollo, Cicada, CVNX)	中国の国家安全保障上の目標を支援するため、外国政府だけでなく、建設・エンジニアリング、航空宇宙、電気通信企業を標的としてきた MSS に関連するサイバー脅威グループ。APT10は、エンジニアリング、工業製造、小売、エネルギー、製薬、通信、政府産業などの顧客の情報を入手するために、米国やその他の国の多数のMSPを侵害した世界的なサイバースパイキャンペーンである「Operation Cloud Hopper」を実行した。	2018年、司法省は、MSPと45社以上のテクノロジー企業を標的とした10年以上にわたる世界的なコンピュータ侵入キャンペーンに関連して、APT10のメンバー2人を起訴
APT26 (別名：Tur-bine Panda)	MSSの江蘇支部に関連するサイバー脅威グループで、航空宇宙、防衛、エネルギー分野を標的としたサイバースパイキャンペーンを行ってきた。2019年、CrowdStrikeは、同社がTurbine Pandaと呼ぶこのグループが、2010年から2015年にかけて、中国国産旅客機C919の部品を製造する複数の外国企業からIPを窃取していたことを明らかにした。	2018年、司法省は、民間旅客機に使用されるターボファンエンジンに関する情報を含む、機密データ、知的財産、及び機密情報の窃盗を共謀したとして、MSS江蘇支社の諜報部員2名を起訴
APT40 (a.k.a. Kryp-tonite Panda, GAD-OLINIUM, BRONZE MOHAWK, TEMP. Periscope, Levia-than)	MSS海南支社のフロント企業である海南湘敦科技発展有限公司に関連するサイバー脅威アクターで、中国の海軍近代化プログラムを促進する可能性が高い国家主導のスパイ活動を行っている。APT40は、米国、カナダ、欧州、中東、一帯一路構想諸国にわたり、政府、企業、大学を標的として、海洋研究を含む幅広い産業にわたるIPを提供している。APT40はHAFNIUMと関連しているか、重複している可能性がある。	2021年、司法省は、2011年から2018年にかけて実行された感染症研究を含む知財を標的とした世界的なコンピュータ侵入キャンペーンに関連して、APT40のメンバーを起訴

[出典] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION “2022 Annual Report to Congress”
https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf

2.1.3-2. 事例検討 (2/5)

HITACHI
Inspire the Next

- 2006年から2014年にかけて、人民解放軍61398部隊に所属していたとされる中国人5名により引き起こされたとされる大規模な営業秘密漏えい事案を事例として取扱う。
- この事案は、米司法省がハッキング容疑で海外の政府当局者を訴追した初のケースとされている。

項目	概要
事案の概要	• 2006年から2014年にかけて、米国企業(Westinghouse、Solarworld、US steel等)がハッキングされ、中国国営企業(SOE)を含む競合他社にとって有益な営業秘密情報を盗まれるという事案が発生した。 • ペンシルベニア州西部地区(WDPA)の大陪審は、中国のハッカー5名(人民解放軍61398部隊に所属)を、米国の原子力発電、金属、太陽電池製品業界の被害者6社を狙ったコンピューター・ハッキング、経済スパイ、その他の犯罪で起訴した。 • 「これは中国軍のメンバーによる経済スパイの申し立てであり、この種のハッキングで国家的アクターを告訴した初めてのケースである」とエリック・ホルダー米司法長官(当時)は述べている。
行政機関の対応	• 2014年、司法省がAPT1のハッカー5人を、米国企業に対するサイバースパイ行為で起訴 • 公開された事実には表れていないが、米国サイバー当局による情報収集、アトリビューション等が実施されていたと思われる。
司法機関の対応	• 管見の限り、5名の逮捕や裁判結果等の続報は確認できなかった。

[出典] Indictment
https://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.1.3-2. 事例検討 (3/5)

HITACHI
Inspire the Next

- 5名の中国人により、原子力、太陽電池、鉄鋼等に係る合計6社(Westinghouse、SolarWorld、U.S. Steel、ATI、USW、Alcoa)から重要な技術情報の窃取がなされたとされている。

被告	被害者	犯行
Sun Kailiang	Westing house	• 2010年、同社が中国で4基のAP1000発電所を建設し、技術移転を含むその他の建設条件について中国のSOE(SOE-1)と交渉していた際、孫はAP1000発電所の建屋内の配管、配管サポート、配管ルーティングに関する極秘の専有技術および設計仕様を盗んだ。 • さらに、2010年と2011年、同社がSOE-1との他のビジネスベンチャーを模索している間に、孫は、ウェスチングハウスとSOE-1とのビジネス関係を担当する上級意思決定者の機密、非公開、審議用電子メールを盗み見た。
Wen Xinyu	SolarWorld	• 2012年、中国の太陽電池製品メーカーが適正価格を下回る価格で製品を米国市場に「ダンピング」したと商務省が認定したのとほぼ同時期に、Wenと少なくともう1人の身元不明の共謀者は、SolarWorldのキャッシュフロー、製造指標、生産ライン情報、コスト、進行中の貿易訴訟に関する弁護士と依頼人の特権的なやりとりなどに関する情報を含む数千ものファイルを盗んだ。こうした情報は、中国の競合他社がさまざまな角度からSolarWorldの事業運営を攻撃的に狙うことを可能にした。
Wang Dong, Sun Kailiang	U.S. Steel	• 2010年、U.S. Steelは、ある国有企業(SOE-2)を含む中国の鉄鋼会社との貿易訴訟に参加していた。訴訟のひとつで予備的な決定が発表される予定時刻の少し前に、SunはU.S. Steelの従業員(うち何人かは訴訟に関連する部門に所属)にスピアフィッシングメールを送信した。電子メールの中には、U.S. Steelのコンピュータにマルウェアをインストールさせるものもあった。3日後、WangはU.S. Steelのコンピュータのホスト名と説明を盗み出した。Wangはその後、そのリストにある脆弱なサーバーを特定し、悪用する手段を講じた。
Wen Xinyu	ATI	• 2012年、ATIはSOE-2と合弁事業を行い、SOE-2と競合し、SOE-2との貿易紛争に巻き込まれた。同年4月、WenはATIのネットワークにアクセスし、事実上すべてのATI従業員のネットワーク認証情報を盗んだ。

[出典] U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage
https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and

2.1.3-2. 事例検討 (4/5)

HITACHI
Inspire the Next

- 5名の中国人により、原子力、太陽電池、鉄鋼等に係る合計6社(Westinghouse、SolarWorld、U.S. Steel、ATI、USW、Alcoa)から重要な技術情報の窃取がなされたとされている。

被告	被害者	犯行
Wen Xinyu	USW	• 2012年、USWは少なくとも2つの産業で中国の貿易慣行をめぐる紛争に巻き込まれた。USWがこれらの貿易紛争と関連する立法案に関する公式声明を発表した頃、WenはUSWの上級従業員から、USWの戦略に関する機密、非公開、審議情報を含む電子メールを盗み出した。USWのコンピューターは、少なくとも2013年初めまで共謀者のインフラに接続し続けていた。
Sun Kailiang	Alcoa	• Alcoaが2008年2月に中国国有企業(SOE-3)との提携を発表してから約3週間後、SunはAlcoaにスピアフィッシングEメールを送信した。その後、2008年6月頃、正体不明の人物がAlcoaのコンピュータから数千の電子メール・メッセージと添付ファイルを盗み出し、その中にはその取引に関する内部協議も含まれていた。
Huang Zhenyu	-	• Huangは、共謀者が米国企業へのハッキングに使用するドメイン・アカウントを登録・管理することで、ハッキング活動を促進した。さらに、2006年から少なくとも2009年の間、61398部隊はHuangにSOE-2のプログラミング作業を命じ、鉄鋼業界に関する企業「情報」(米国企業に関する情報を含む)を保持するための「秘密」データベースを作成させた。
Gu Chunhui	-	• Guは、アメリカの団体に対するハッキング活動を促進するために使用されたドメイン・アカウントを管理し、また犯行を推進するためにスピアフィッシング・メールのテストも行った。

[出典] U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage
https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and

2.1.3-2. 事例検討 (5/5)

HITACHI
Inspire the Next

- 前節で紹介したコンピュータ犯罪取締法(刑法1030条)や連邦経済スパイ法(1031条)等への違反を根拠として5名の起訴がなされた。

カウント	請求	規定	罰則(最大)
1	コンピューター詐欺と不正利用の共謀	コンピュータ犯罪取締法(刑法1030条) (b)項	10年
2-9	商業的利益や私的な金銭的利益を得る目的によるコンピュータへの無許可のアクセス、情報の入手	コンピュータ犯罪取締法(刑法1030条)(a)(2)(C)、1030(c)(2)(B)(i)-(iii)、2	5年
10-23	保護されたコンピュータに損害を与える目的でのプログラム、情報、コード、またはコマンドの送信	コンピュータ犯罪取締法(刑法1030条)(a)(5)(A), 1030(c)(4)(B), and 2.	10年
24-29	悪質なID窃盗	刑法 1028 条(身分証明書類、認証機能、及び情報に関する詐欺及び関連行為)(a)(1), (b), (c)(4), and 2	2年
30	経済スパイ	連邦経済スパイ法(刑法 1031 条) (a)(2), (a)(4), and 2.	15年
31	営業秘密の窃取	刑法 1032 条(保佐人、管財人、清算人に対する資産の隠匿) (a)(2), (a)(4), and 2.	10年

[出典] U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage
https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and

HITACHI
Inspire the Next

2.2 EUの動向

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.2.1 大学・研究機関を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

EU施策の背景

- 優れた研究の実施のためには国際協力が必須であるが、地政学的リスクが高まる今日の情勢の下では、EUが主導的地位に立ち、多国間主義、開放主義、相互主義を促進することが必要と考えられている。
- こういった中で、EUは外国の干渉から高等教育機関や研究実施機関を守るためのガイドラインの策定に取組んでおり、EU加盟国及び高等教育機関や研究実施機関、研究助成機関等が協力し、2022年１月に「研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書(以下、スタッフ作業文書という)」を公表した。

オープンサイエンスの推進

- 2021～2027 年の間で、EUにおいて産学連携など研究・イノベーションの連携プロジェクトを助成する枠組みであるHorizon Europe Programme(以下、HE Programmeという)を開始している。

外国からの干渉への対策

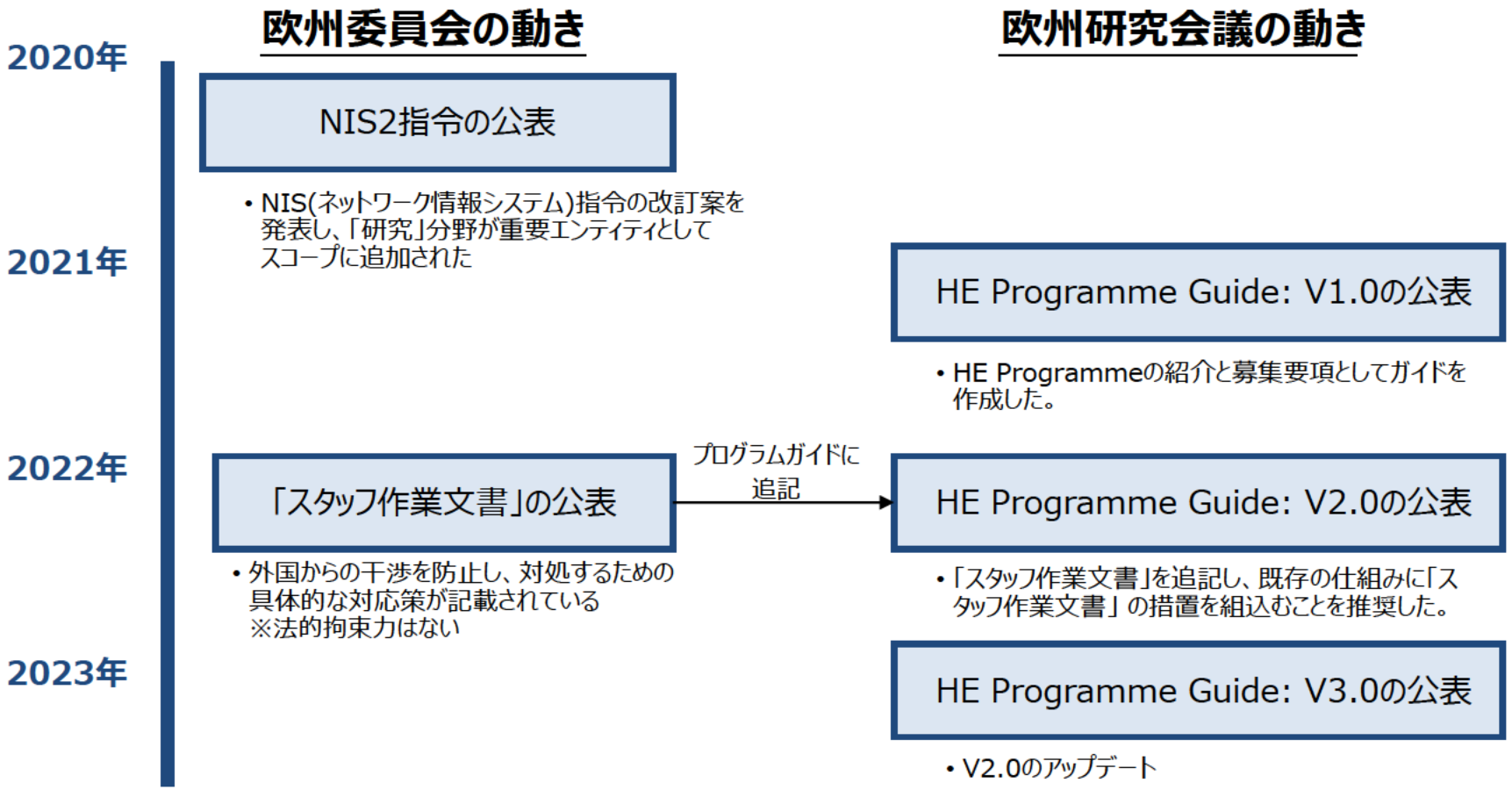
- 欧州委員会は2022年１月に「スタッフ作業文書」を発行した。
- 本文書はEUの主権や利益を脅かす外国の干渉リスクを低減することを目的としている。

[出典] European Commission” Europe's global approach to cooperation in research and innovation: strategic、open、and reciprocal”
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2465
pwc“研究インテグリティ(Research Integrity)に係る調査・分析報告書”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2021.pdf

© Hitachi, Ltd. 2024. All rights reserved.

施策の全体像

- 前頁の動向を受け、欧州委員会は欧州連合国や大学・研究機関、及びHorizon Europe Programme(以下、HE Programmeという)への応募機関に対して、可能な限り「スタッフ作業文書」を既存の仕組みの中に組み込むことを推奨している
- また、「研究」分野をNIS2指令における重要エンティティに指定する等、研究活動を通じて機微な情報を取扱い得る領域のサイバーセキュリティ強化にも取り組んでいる。

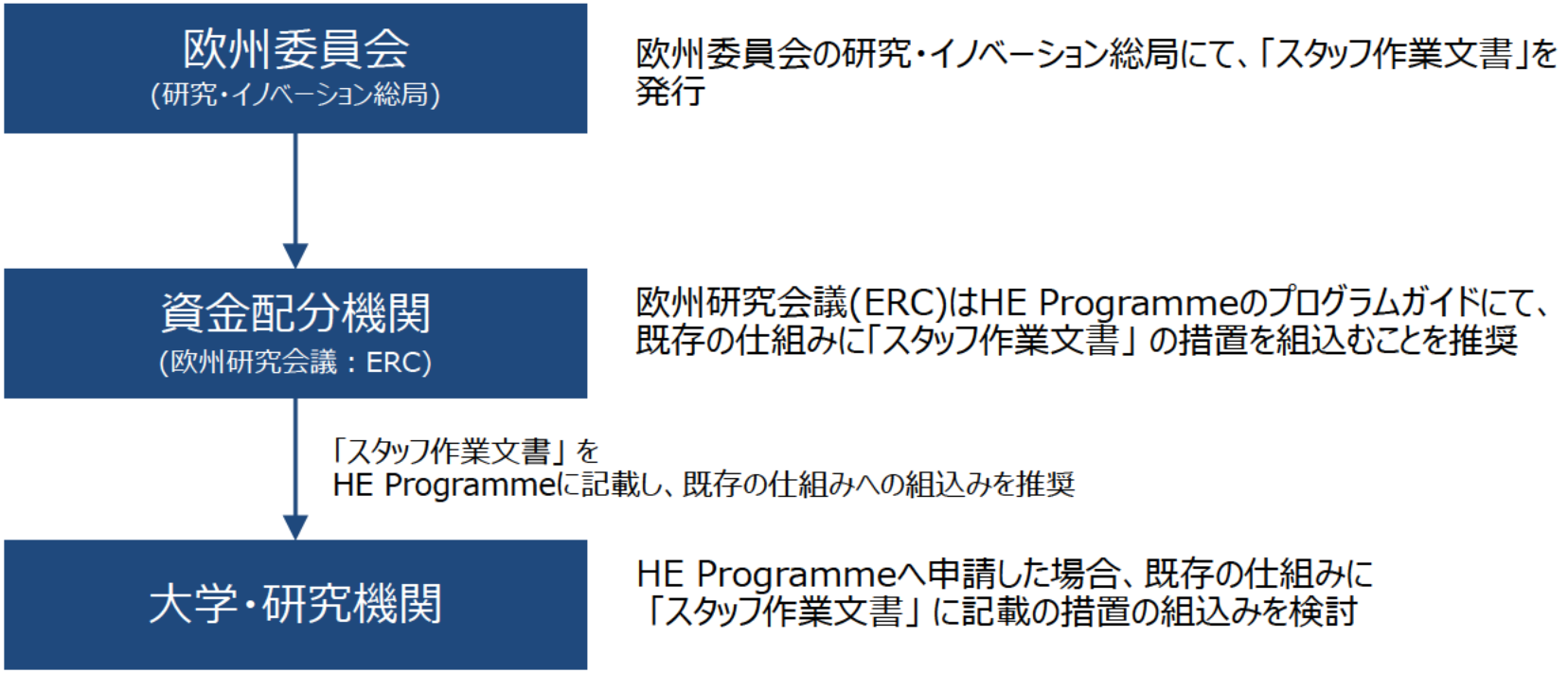


[出典] 未来工学研究所、"研究インテグリティ(Research Integrity)に係る調査・分析"
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022.pdf

© Hitachi, Ltd. 2024. All rights reserved.

研究セキュリティ確保に向けた施策の推進体制(概要)

- 研究セキュリティに関する方針の策定は主に欧州委員会内の研究・イノベーション総局が担っている。
- 資金配分機関である欧州研究会議(ERC)はHE Programmeに申請する機関に対して既存の仕組みに「スタッフ作業文書」の措置を組込むことを推奨している。

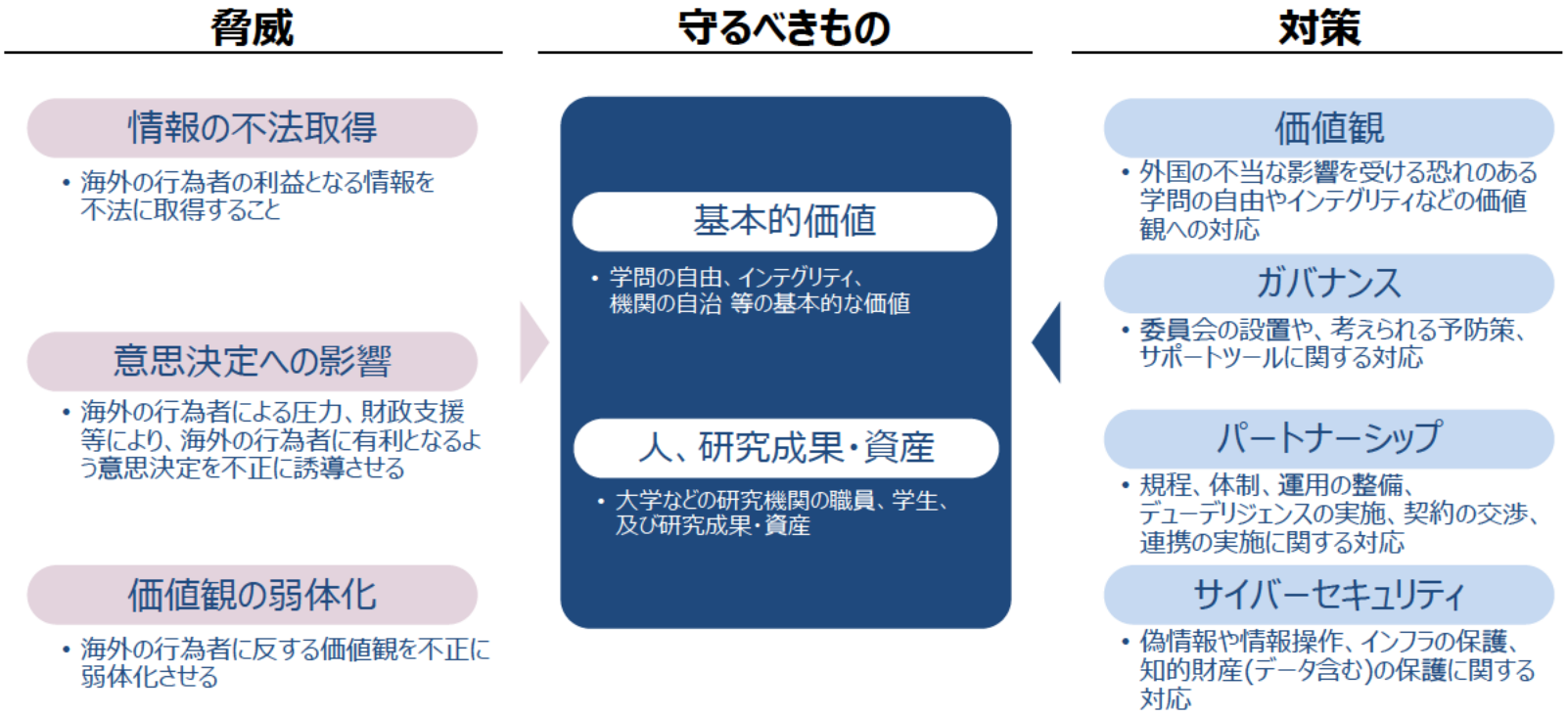


出典：欧州委員会“Horizon Europe (HORIZON) Programme Guide”
programme-guide_horizon_en.pdf (europa.eu)

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-1. リスクに対する考え方

- EUでは、外国による情報の不正取得や意思決定への影響、価値観の弱体化等を脅威として認識しており、そういった干渉から学問の自由、インテグリティ、機関の自治等の基本的価値と職員、学生、研究成果・資産を守るために、価値観、ガバナンス、パートナーシップ、サイバーセキュリティの観点から対応策を検討する必要があるとされている。



[出典] 未来工学研究所、“研究インテグリティ(Research Integrity)に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022.pdf
European Commission、” Tackling R&I foreign interference. Staff Working Document”
file:///D:/Users/70746152/HitachiXPC/Downloads/tackling%20r&i%20foreign%20interference-KI0922004ENN.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-2. 対象となる事業、情報の分類等

- 「スタッフ作業文書」の対象は、欧州連合加盟国や、大学・研究機関となっているが、各組織への推奨レベルのものであり、遵守すべき事業の条件は特に示されていない。
- 一方、2022年にNIS指令の改正案が承認され、研究機関もスコープに含められたため、新たにサイバーセキュリティリスク管理と報告の義務が課されることとなった。

ルールの適用対象となる主体や条件等

文書、指令	対象
「スタッフ作業文書」	対象：欧州連合加盟国や、大学・研究機関 (2022年からはHE Programmeに申請する機関に推奨) ※推奨レベルで、法的な拘束力はなく、かつ適用対象となる条件もない
NIS2指令	対象：研究 (「重要エンティティ」に位置付けられた) ※1: 具体的な対象等は今後国内法で規定される見込み ※2: リスク管理と報告の義務が課せられている(以下、具体的内容) **〈リスク管理(21条)〉** ・リスクマネジメント及び情報セキュリティ対策 ・インシデントハンドリング ・ビジネス継続性 ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ ・サイバーセキュリティリスクマネジメントの効率性評価 ・サイバー衛生の実施及びサイバーセキュリティ教育 ・暗号技術の活用 ・アクセスコントロール等の人的セキュリティ ・多要素認証の活用 **〈報告義務(23条)〉** インシデント通報(24時間以内に早期警告、72時間以内にインシデント通知)

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-3. 具体的な要求事項の内容 / サイバーセキュリティの位置づけ

HITACHI
Inspire the Next

- 「スタッフ作業文書」において、サイバーセキュリティは、海外からの干渉への対応策の４カテゴリの内の１つを構成している。

スタッフ作業文書におけるサイバーセキュリティの位置づけ

#	カテゴリ	要求事項
1	価値観	1. 学問の自由が危険にさらされている国やパートナー機関を特定する 2. 学問の自由とインテグリティに対する外部からの圧力を理解するために脆弱性評価を実施する 3. 機関及び個人レベルでの学問の自由とインテグリティへのコミットメントを強化する 4. 抑圧的な環境下にあるパートナーとの協力を継続する
2	ガバナンス	1. 海外からの干渉に対する行動規範を公表する 2. 海外からの干渉委員会を設置する
3	パートナーシップ	1. リスクマネジメントシステムを導入するための一般的な前提条件を整備する 2. 強固なパートナーシップ合意を策定するための健全な順序を確立する
4	サイバーセキュリティ	1. サイバーセキュリティリスクの認知を向上する 2. 海外からの干渉行為者によるサイバー攻撃を検知し、防御する 3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-3. 具体的な要求事項の内容 / サイバーセキュリティ対策の内容

HITACHI
Inspire the Next

- 前頁のサイバーセキュリティカテゴリでは、具体的に以下の対策が推奨されている。

#	要求事項	具体的な内容
1	サイバーセキュリティリスクの認知を向上する。	1. 機密コンピューティング(confidential computing)を含む、利用可能で実装されているすべてのデータ保護技術に関するトレーニングを開発し、セミナーを開催する。 2. 研究者、学生、事務・支援スタッフに対し、サイバー衛生(cyber hygiene)に関する教育・訓練を行い、リスクを特定し、サイバー攻撃を回避・対処する方法を知ってもらう。 3. サイバー攻撃が疑われる場合に適用するわかりやすいエスカレーションプロセスを開発・伝達し、報告されたインシデントをトリアージするための単一の連絡窓口を周知する。 4. サイバーセキュリティリスクのトップ10 リストの維持と伝達を行う。 5. サイバーセキュリティインシデントを説明するベストプラクティスを掲載したニュースレターを定期的に発行する。
2	海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、防止する。	1. オープンソースインテリジェンス(OSINT)調査を定期的に設定・実行し、異常な行動にフラグを立てるアラート機能を作成する。 2. 研究者、事務・支援スタッフの審査手順を策定する。 3. サイバーセキュリティ認証を受けた機器を調達し、機密コンピューティングを含むデータセットの機密保護ソリューション(confidentiality protection solutions)の開発に投資する。 4. 必要なレベルに応じた物理的なアクセス制御を実施する。 5. オフィス/企業活動クラスターにおいて、OSとインストールされたアプリケーションの集中管理アプローチを開発し、ローカル管理権(LAR)を無効化及び削除する。 6. 重要なサービスやリポジトリにアクセスするための二要素認証を有効にし、既知の悪意あるウェブサイトや侵害するウェブサイトへのアクセスを禁止するブロックリストを維持・実施する。
3	海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う。	1. 教訓を共有し、共有ブラックリスト、評価システム、データベースを更新することにより、状況認識能力を向上させる。 2. 影響を受ける当事者と対応に必要な人物の双方が参加する明確なプロセスを含む、インシデント対応計画を策定する。セキュリティインシデント管理成熟度モデル(SIM3: Security Incident Management Maturity Model)などのインシデント処理モデルから慣行や要素を採用する。 3. フォレンジック準備機能を導入し、対応にかかる時間を短縮する。 4. 違反したスタッフの懲戒処分を行い、その際、デジタル調査の証拠も含める。 5. インシデントに、法執行機関、国家情報・セキュリティ機関、知的財産局、データ保護当局を関与させる。

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-3. 具体的な要求事項の内容 / NIS2指令の概要

HITACHI
Inspire the Next

- NIS2指令では「研究」が重要エンティティに位置付けられたため、研究機関もリスク管理とインシデント等の報告に関する義務が課せられている。

	NIS	NIS2指令
スコープ	ヘルスケア、交通、金融、デジタルインフラ、水道、エネルギー、デジタルサービスプロバイダー	**〈主要エンティティ〉** エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、宇宙 **〈重要エンティティ〉** 郵便・宅配、廃棄物管理、化学品、食品、製造業(医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器)、デジタルプロバイダー、**研究**
要件	• 各者のサイバーセキュリティ対策 • 重大事故が起きた際の当局への通報 等	**〈リスク管理(21条)〉** ・リスクマネジメント及び情報セキュリティ対策 ・インシデントハンドリング ・ビジネス継続性 ・サプライチェーンセキュリティ ・ネットワークやシステムのセキュリティ ・サイバーセキュリティリスクマネジメントの効率性評価 ・サイバー衛生の実施及びサイバーセキュリティ教育 ・暗号技術の活用 ・アクセスコントロール等の人的セキュリティ ・多要素認証の活用 **〈報告義務(23条)〉** インシデント通報(24時間以内に早期警告、72時間以内にインシデント通知) **〈その他〉** サイバーセキュリティ認証制度(EUCC)の活用 等
罰則	罰則額は加盟国の裁量	違反した場合には、売上げの最大２%又は1000万ユーロの罰金

© Hitachi, Ltd. 2024. All rights reserved.

2.2.1-4. 資金配分機関による取組み

HITACHI
Inspire the Next

- 資金配分機関であるERCによる取り組みとしては、これまでにご紹介の通り、HE Programmeのプログラムガイドにて、プログラム申請者に対し 、既存の仕組みに「スタッフ作業文書」の措置を組込むことを推奨している。

資金配分機関	研究セキュリティに関する主な取組み
欧州研究会議(ERC)	• 2022年4月15日に、HE Programmeのプログラムガイドにて、プログラム申請者に対し 、既存の仕組みに「スタッフ作業文書」の措置を組込むことを推奨 • 2023年4月1日に、HE Programmeのガイドラインをバージョンアップ ※研究セキュリティに関する記述に変更はなし

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.2.2 企業を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-1. EUにおけるデータ保護法制の全体像 (1/2)

HITACHI
Inspire the Next

- EUにおいてもデータの保護は契約による保護を基本としており、第三者からの不正取得に対しては営業秘密保護指令やデータベース保護指令により、欧州各国の現行法で対応することとなっている。

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあるという考え	営業秘密保護指令	○		–	–	–	モデル契約開発中	データベース保護指令(著作権と独自の権利による保護)	単一デジタル市場戦略

- 営業秘密は非技術的なものを含めたイノベーションや競争力のために重要であるにもかかわらず、現状において欧州域内における**不統一な保護状況が国を超えた研究開発や知識の流通を阻害している**との認識が示されている。
- 2016 年に採択された営業秘密保護指令は、**営業秘密保護について、共通の定義※を提供**し、営業秘密侵害に該当する行為と、しない行為を明確にしている。
- 評価としては、新たなデジタル経済に対応する意図で策定されたものではなく、自動生成されるデータ・リアルタイムのデータに適用するのにはかい離があるといった批判的なものと、欧州域内でハーモナイズが図られることは望ましい」といった好意的なものがある

※営業秘密の定義：
「当該情報と類似する情報を通常扱う関係者(circles)に属する者にとって、当該情報が集合として又は構成する正確な配列や構造が、一般的に知られておらず又は容易に知ることができないという意味において秘密であること」、「秘密であることによって商業的価値があること」、「当該情報を合法的に管理するものによって、当該情報を秘密とするために合理的な措置を講じていること」

[出典] 平成２９年度産業経済研究委託事業 海外におけるデータ保護制度に関する調査研究 調査報告書
https://www.meti.go.jp/policy/economy/chizai/chiteki/keizaisanngyou29.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-1. EUにおけるデータ保護法制の全体像 (2/2)

HITACHI
Inspire the Next

- データの保護は契約による保護を基本としており、第三者からの不正取得に対して営業秘密保護指令やデータベース保護指令により、欧州各国の現行法で対応することとなっている。

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあるという考え	営業秘密保護指令	○		–	–	–	モデル契約開発中	データベース保護指令(著作権と独自の権利による保護)	単一デジタル市場戦略

- データベース保護指令は、データベースが各国の現行法によって十分に保護されておらず、データベースを提供することに対して負の影響を与えているという認識から採択された。
- 本指令の特徴は、著作権による保護と、独自の権利(sui generis)による保護の両方を定めていることである。
- 1988年頃、著作権による保護については、データベースの創作性を要求していたが、1966年に独自の権利により、経済的資源、時間、努力や労力等を含む「投資」を保護することが定められた。
- 採択後の判例により、多くのデータベースが独自の権利によって保護されないことが示され、早い時期から批判が多く、見直しの必要性が指摘されている。

- データ・オーナーシップという観点で**ビッグデータの取扱いについて論点が提示**されており、欧州においても比較的関心が高まっている
- 欧州委員会はデータベース保護指令による保護の可能性については、自動集積される生データを扱うデータベースの構築について相当の投資がなされている場合にのみ適用されうるとし、営業秘密保護指令は国内法化が進んだとしてもデータが企業にとって知的資本として秘密にされ、「営業秘密」の要件を満たしていなければ保護がされないことから **EU レベルでは既存のルールで直接的に「自動集積される生データ」に適用されるものはない**と指摘している。

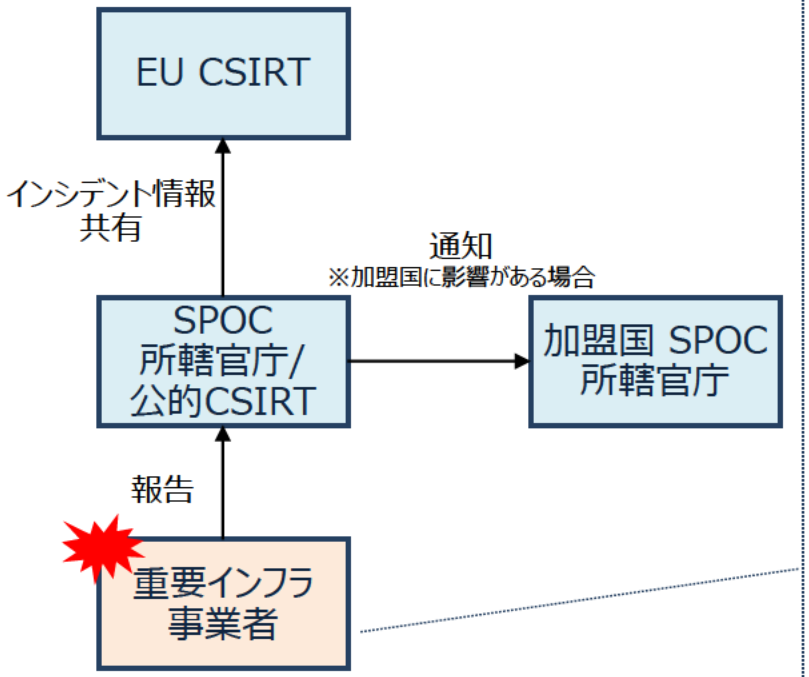
[出典] 平成２９年度産業経済研究委託事業 海外におけるデータ保護制度に関する調査研究 調査報告書
https://www.meti.go.jp/policy/economy/chizai/chiteki/keizaisanngyou29.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 報告フロー

HITACHI
Inspire the Next

- 重大インシデント※発生後、事業者は早期警告、インシデント通知、最終報告(要求に応じて中間報告)を単一連絡窓口(SPOC)に通知する必要がある。



初期報告
重大インシデントの発生を認識してから24時間以内に報告施設へ報告を行う

【報告内容】
1. 重大インシデントが不法行為または悪意によるものである疑いがあるか
2. 国境を越えて影響を及ぼす可能性があるか

インシデント通知
重大インシデントの発生を認識してから72時間以内に報告施設へ報告を行う

【報告内容】
インシデントの性質 /インシデントの影響 /連絡先情報 /運用情報
情報共有 /事後情報共有
※詳細は次頁を参照

最終報告
重大インシデントの発生を認識してから1か月以内に報告施設へ提出する

【報告内容】
所轄官庁が要求するすべての情報

※報告対象となる重大インシデントとは、以下に該当するものである
1.サービスの運営に重大な混乱を引き起こした、または当該事業体に経済的損失を引き起こす可能性がある。
2.重大な物質的または非物質的な損害を通じて自然人または法人に影響を及ぼしている、または影響を与える可能性がある。
("1." より、企業の社外秘情報等、機微情報漏洩も含まれる可能性がある)

[参考] "NIS Cooperation Group"
https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 報告内容 (1/2)

HITACHI
Inspire the Next

- インシデント通知は、インシデント対応リソースを報告にとられないよう、報告内容が具体的に決められている。

報告分類	報告内容
インシデント通知	**インシデントの性質** - インシデントの原因となった脅威または根本原因の種類、一般的なカテゴリー〈別紙 #1〉。 - 脅威の深刻度(スケールを使用するなど)。 - 詳細な原因／脅威の説明（自然災害、ソフトウェアバグ、ランサムウェア攻撃、DDoS攻撃、破壊行為、侵入など）。 **インシデントの影響** - 影響を受けたセクターまたは重要インフラ - 影響を受けた重要サービス - 必須サービスへの影響の説明 - 社会および経済への影響の規模〈別紙 #2〉 - 国内外への地理的広がり - 影響を受けた国民の数〈別紙 #3〉 - 期間〈別紙 #4〉 **連絡先情報** - 影響を受けた組織名 - インシデントに関する連絡先(氏名、役割、連絡先の詳細、連絡可能な時間帯) - インシデントに関与する可能性のあるその他の関係者(サイバーセキュリティ企業など) **運用情報** - インシデントの発生時刻(インシデントの開始またはインシデントの発見) - インシデントの状況(進行中、解決済み、コントロール下) - インシデントの詳細(使用されたマルウェア、内部/外部アクター、既知のキャンペーンとの関係) - インシデント解決までの予想時間 - インシデントを軽減するために取られた、または進行中のアクション - 国の CSIRT に要請したサポート **情報共有** - 脅威の影響を受けた IT 資産(ソフトウェアのバージョン、ハードウェアのモデルなど)。 - 脅威に関する情報(システムやネットワークに侵害や攻撃があった際に残されるデータなど) **事後情報共有** - インシデントを軽減するために取られた措置 - 教訓

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 報告内容 (2/2)

HITACHI
Inspire the Next

- インシデント通知は、インシデント対応リソースを報告にとられないよう、報告内容が具体的に決められている。

#	補足情報	選択肢 / 参考情報
1	**根本原因区分**	・ システム障害（例：ソフトウェアのバグ、ポリシーの欠陥、ハードウェア障害など） ・ 自然災害（例：嵐、地震など） ・ ヒューマンエラー（例：ミス、過失など） ・ 悪意ある行為（例：サイバー攻撃、その他） ・ 第三者の障害（停電、インターネット停止など）
2	**影響の重大度尺度**	・ 非常に大きな影響 ・ 影響大 ・ 軽度の影響 ・ 影響なし
3	**影響を受ける市民またはユーザー**	a)サービスの契約が締結されている自然人および法人の数 b)過去の利用データに基づく影響を受ける利用者の推定
4	**期間**	影響の持続期間、すなわち、影響インシデントが重大である瞬間から重大でなくなる瞬間までの期間

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 罰則執行までの流れ

HITACHI
Inspire the Next

- 主要エンティティに位置付けられる事業者は、所轄官庁から積極的に監視されており、NIS2への違反があった場合に強制措置を命じられる。

罰則適用までの流れ

監査

罰金を課すか否か
金額の検討

執行

主要エンティティは所轄官庁の監査執行権限により監督されている

- 訓練を受けた専門家による抜き打ち検査を含む、立入検査と立入以外の監督
- 独立機関または管轄当局による対象を絞った定期的なセキュリティ監査
- 重大インシデント、本指令の違反を理由とする臨時監査
- 必要に応じてセキュリティスキャンの実施。
- 所轄官庁への情報提出義務の遵守だけでなく、文書化されたサイバーセキュリティポリシーを含むセキュリティリスク管理措置を評価するために必要な情報の要求
- 監督業務を遂行するために必要なデータ、文書および情報へのアクセス要求
- サイバーセキュリティポリシーの実施に関する証拠(資格のある監査人によって実施されたセキュリティ監査の結果およびそれぞれの基礎となる証拠など)の要求

罰金を課すか否か、また金額の算定時に以下を考慮する

※金額の算定基準は個々の違反に対して金額を決定したい場合に使用する

(a) 違反の深刻さと違反した条項の重要性
  (i) 反復的な違反があった場合
  (ii) 重大なインシデントの通知または是正を怠った場合
  (iii) 所轄官庁からの指示に従って不備を是正しなかった場合
  (iv) 違反の発見後に所轄官庁が命じた監査または監視活動を妨害した場合
  (v) サイバーセキュリティのリスク管理措置または報告義務に関連して、虚偽または著しく不正確な情報を提供した場合
(b) 違反の期間
(c) 過去の関連違反
(d) 金銭的または経済的損失、他のサービスへの影響、および影響を受けるユーザー数
(e) 違反が故意または過失か
(f) 物質的または非物質的な損害を防止または軽減するために講じた措置
(g) 承認された行動規範または承認された認証メカニズムの遵守
(h) 所轄官庁に対する協力度合

[参考] “Article 33, Supervisory and enforcement measures in relation to important entities”
https://www.nis-2-directive.com/NIS_2_Directive_Article_33.html

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 罰則執行までの流れ

HITACHI
Inspire the Next

- 重要エンティティに位置付けられる事業者は、インシデントが発生した場合やリスク管理・報告義務への違反疑い、指摘または情報提供がされた場合、必要に応じて事後監督を通じて所轄官庁が措置を講じる。

罰則適用までの流れ



重要エンティティに対する監査はインシデント発生後等に行われる
- 専門家による立入検査と立入以外の事後監督
- 独立機関または所轄官庁による対象を絞ったセキュリティ監査
- 必要に応じてセキュリティスキャンの実施
- 文書化されたサイバーセキュリティポリシーを含む、リスク管理措置を評価するための情報の要求
- 監督業務を遂行するために必要なデータ、文書および情報へのアクセス要求
- サイバーセキュリティポリシーの実施に関する証拠の要求

罰金を課すか否か、また金額の算定時に以下を考慮する
※金額の算定基準は個々の違反に対して金額を決定したい場合に使用する
(a) 違反の深刻さと違反した条項の重要性
  (i) 反復的な違反があった場合
  (ii) 重大なインシデントの通知または是正を怠った場合
  (iii) 所轄官庁からの指示に従って不備を是正しなかった場合
  (iv) 違反の発見後に所轄官庁が命じた監査または監視活動を妨害した場合
  (v) サイバーセキュリティのリスク管理措置または報告義務に関連して、虚偽または著しく不正確な情報を提供した場合
(b) 違反の期間
(c) 過去の関連違反
(d) 金銭的または経済的損失、他のサービスへの影響、および影響を受けるユーザー数
(e) 違反が故意または過失か
(f) 物質的または非物質的な損害を防止または軽減するために講じた措置
(g) 承認された行動規範または承認された認証メカニズムの遵守
(h) 所轄官庁に対する協力度合

[参考] “Article 32, Supervisory and enforcement measures in relation to essential entities”
https://www.nis-2-directive.com/NIS_2_Directive_Article_32.html

© Hitachi, Ltd. 2024. All rights reserved.

2.2.2-2. NIS2指令に基づくインシデント報告 / 罰則適用の考え方

HITACHI
Inspire the Next

- NIS2指令に違反した場合、機関の重要度に応じた罰金額を提示している。
  - 重要エンティティであれば、少なくとも 7,000,000 €、または全世界売上高の1.4%のどちらか高い方
  - 主要エンティティであれば、少なくとも 10,000,000 €、または全世界売上高の2%のどちらか高い方

インシデント報告義務に違反した場合の罰金

#	罰金額	基準
1	少なくとも 7,000,000 € または全世界売上高の1.4% どちらか高い方	**重要エンティティ**が違反した場合
2	少なくとも 10,000,000 € または全世界売上高の2% どちらか高い方	**主要エンティティ**が違反した場合

[参考] “Article 34, General conditions for imposing administrative fines on essential and important entities”
https://www.nis-2-directive.com/NIS_2_Directive_Article_34.html

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.2.3 機微技術流出後の対応事例

© Hitachi, Ltd. 2024. All rights reserved.

2.2.3-1. 事例検討 (1/2)

HITACHI
Inspire the Next

- 機微技術の漏えいが顕在化、または疑われる場合において、欧州理事会による制裁措置(例：関与者の資産凍結、直接・間接の資金提供の禁止)が発動されたケースが複数確認された。

制裁対象	概要	欧州理事会の対応
ロシア連邦軍参謀本部情報総局(GRU)	**ロシアの軍事スパイ組織** 2018年10月に起こったOPCW(化学兵器禁止機関:本部,オランダ ハーグ市)に対するハッキング未遂事件に関与している疑い	**制裁措置の発動** EU加盟国への入国およびトランジットの禁止および全ての資産の凍結が主な内容となる。またEU市民および企業が、制裁対象者に対し直接的・間接的に資金提供を行うことは禁止される (EU理事会が2019年5月に採択した規則2019／796に基づく措置)
Chosun Expo	**北朝鮮のハッキンググループ・APT38のフロント企業** APT38は世界中の銀行から数十億円もの現金を不正に引き出していた	
Huaying Haitai	**中国政府が支援するハッキンググループ・APT10のフロント企業** 世界各国のマネージドサービスプロバイダ(MSP)を標的として、軍事組織を含む多くの企業の知的財産や機密情報を盗み出すハッキング作戦「Operation Cloud Hopper」を展開していた	

[出典] JETRO"サイバー攻撃に対する初の制裁措置を発動(EU)"
https://www.jetro.go.jp/biznews/2020/07/a911e269ccb27f47.html
欧州理事会" Cyber-attacks: Council is now able to impose sanctions(Press release 17 May 2019 11:52)"
https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/

© Hitachi, Ltd. 2024. All rights reserved.

2.2.3-1. 事例検討 (2/2)

HITACHI
Inspire the Next

- EUROPOLが関与した欧州を含む国際規模のサイバー攻撃の事例の内、 Revil / Sodinokibiに関与した犯罪者、及び国際的なハッカー12人の逮捕に貢献している。

脅威グループ ※( )はグループ以外	概要	EUROPOLの対応
Revil / Sodinokibi	**ランサムウェアを利用したサイバー犯罪組織** EUROPOLが参画する「GoldDust作戦※」によりランサムウェアを利用したサイバー犯罪組織「Revil / Sodinokibi」に関与した疑いのある容疑者5人を、ルーマニア、韓国、ポーランド、クウェートで、それぞれ逮捕した。 ※世界17カ国と複数の国際法執行機関が参加する共同捜査	5人の犯罪者を各国で逮捕(共同捜査)
(Emotetの攻撃基盤)	**ウイルスメールをばらまいたり、感染したマシンを操作するための機器 等** 2021年1月27日、EUROPOLは、欧米8カ国の法執行機関・司法当局の協力により、Emotetの攻撃基盤をテイクダウンしたと発表した。	Emotetの攻撃基盤をテイクダウン(共同捜査)
(ハッカー12人)	**71カ国・1800人以上に被害を与えたハッカー** EUROPOLは、2021年10月26日に71カ国・1800人以上に被害を与えたハッカー12人を逮捕した。 ハッカーはブルートフォース攻撃やSQLインジェクション等の配信を通じ、身代金を要求するなどの犯罪を行っていた。また、世界最大のアルミニウム生産企業に仕掛けられたランサムウェア「LockerGoga」や、わずか5カ月で総額27億円を稼いだランサムウェア「NetWalker」も開発していた。	身柄の確保のほか、5台の高級車と5万2000ドル(約600万円)以上の現金、電子機器を押収(共同捜査)

[出典] Europol" Five affiliates to Sodinokibi/REvil unplugged"
https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
Europol" World's most dangerous malware EMOTET disrupted through global action"
https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
Europol"12 targeted for involvement in ransomware attacks against critical infrastructure"
https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.3 英国の動向

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.3.1 大学・研究機関を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

英国施策の背景

- 英国の大学は世界中のパートナーと密接に連携しており、英国の研究の半分以上は国際連携によるものとされる。国際共同研究は英国の科学的発展に対して重要な役割を果たしている。
- 上記認識を踏まえ、2019年、ビジネス・エネルギー・産業戦略省(BEIS)は、英国が長期的な国際研究・イノベーションのパートナーとして選ばれるための目標を策定した。
- 国際的な研究協力が盛んに展開する一方、アカデミアや産業界が行う研究活動を通じた技術流出により、国家安全保障に重大なリスクを与えることが英国政府の安全保障部門により認識されている。

国際連携の推進

- 2019年 BEISは、英国が長期的な国際研究・イノンベーションのパートナーとして選ばれるための目標を掲げた、「UK International Research and Innovation Strategy」を2019 年に発表した。

研究セキュリティの強化

- 2019年から、英国政府の国家安全保障機関である国家インフラ保護センター(CPNI)と国家サイバーセキュリティセンター(NCSC)が、「Trusted Research」というキャンペーンを全国展開している。
- 大学・教育機関向けに、研究インテグリティに関する理解を促すためのガイダンスとして、 Trusted Research Guidance for Academiaを公表した。

[出典] National Protective Security Authority “Trusted Research”
https://www.npsa.gov.uk/trusted-research
未来工学研究所、“研究インテグリティ(Research Integrity)に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_5.pdf

© Hitachi, Ltd. 2024. All rights reserved.

施策の全体像 (1/2)

凡例 イニシアチブやチーム / 文書

HITACHI Inspire the Next

- 前頁の動向を受け、英国政府は国内の大学、研究機関に対して、「Trusted Research」関連ガイダンスへの対応推進を実施している

2019年

CPNI

「Trusted Research」の発足

- 研究・イノベーションセクターの成功を維持・向上させるため、英国の大学・研究機関が、国際共同研究に関して十分な情報を得た上で意思決定を行い、その際に**自国の研究者及び学術的価値を保護できるよう支援することを目的としたイニシアチブ**

「Trusted Research Guidance for Academia」の公開

- 研究者に対して、**セキュリティの観点から研究に係るリスク**について概説し、研究者として**注意すべき事項を記載**

※CPNI:Centre for the Protection of National Infrastructure （国家インフラ保護センター）

2020年

UUK

「Managing risks in Internationalisation : Security related issues」の公開

- **「Trusted Research Guidance for Academia」を補完**

※UUK：Universities UK(英国大学協会)

2021年

UKRI

「Trusted Research and Innovation Principles」の公開

- 国際共同研究のデューディリジェンスに関して、**UKRIのファンディングを受ける機関への要求事項(原則)を定めた文書**

※UKRI：UK Research and Innovation(英国研究・イノベーション機構)

DBT,ECJU

「Export controls applying to academic research」の公開

- **軍事目的に使用される危険性が高い分野**の研究を行っている研究者やポスドク研究者向けの**輸出規制に関するガイドライン**

※ECJU：Export Control Joint Unit (国際通商省輸出管理局)
DBT：Department for International Trade(通商省)

BEIS

「Research Collaboration Advice Team (RCAT)」の発足

- 研究者を敵対行為から守り、**セキュリティ関連の課題について、政府の助言を提供するためのチーム**

2022年

「National Security and Investment Act: guidance for the higher education and research-intensive sectors」の公開

- **大学等の研究機関における NSI 法の適用ルールを提示したガイドライン**

※BEIS：Department for Business,Energy & Industrial Strategy (英国ビジネス・エネルギー・産業戦略省)

CPNI,UUK,UKRI

「Managing risks in international research and innovation: An overview of higher education sector guidance」の公開

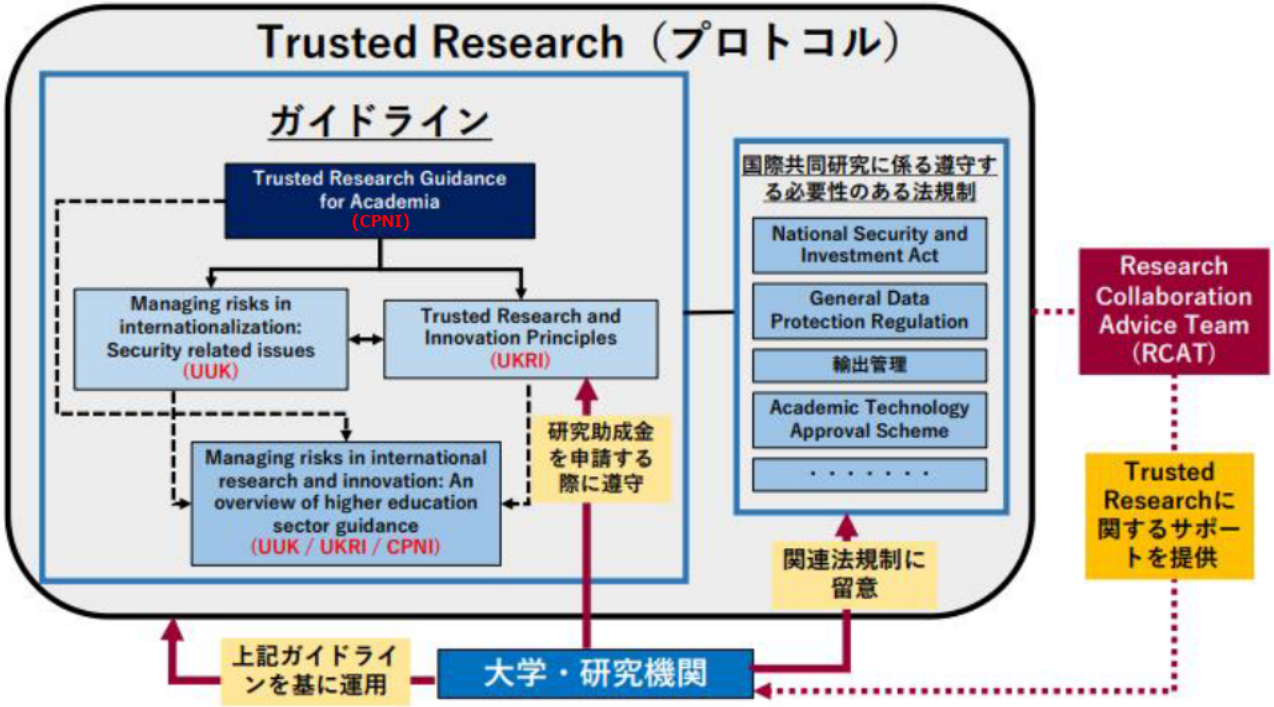
- CPNI、UUK 及び UKRI の **3 機関が作成したガイドラインや主要原則をハイレベルでまとめたガイダンス**

[出典] 未来工学研究所、“研究インテグリティ(Research Integrity)に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_5.pdf

© Hitachi, Ltd. 2024. All rights reserved.

施策の全体像 (2/2)

- CPNIから発表された「Trusted Research Guidance for Academia」を基に、UKRIとUUKにてより具体的なガイドラインを作成している。
- 現時点では、資金配分機関であるUKRIが、助成金を申請する全ての大学・研究機関に対してガイドラインの遵守及び証拠の提出を要求している。
- 上記の通り、ガイドラインが複数存在するため、CPNI、UKRI、UKKはハイレベルでまとめたガイダンスを作成している。



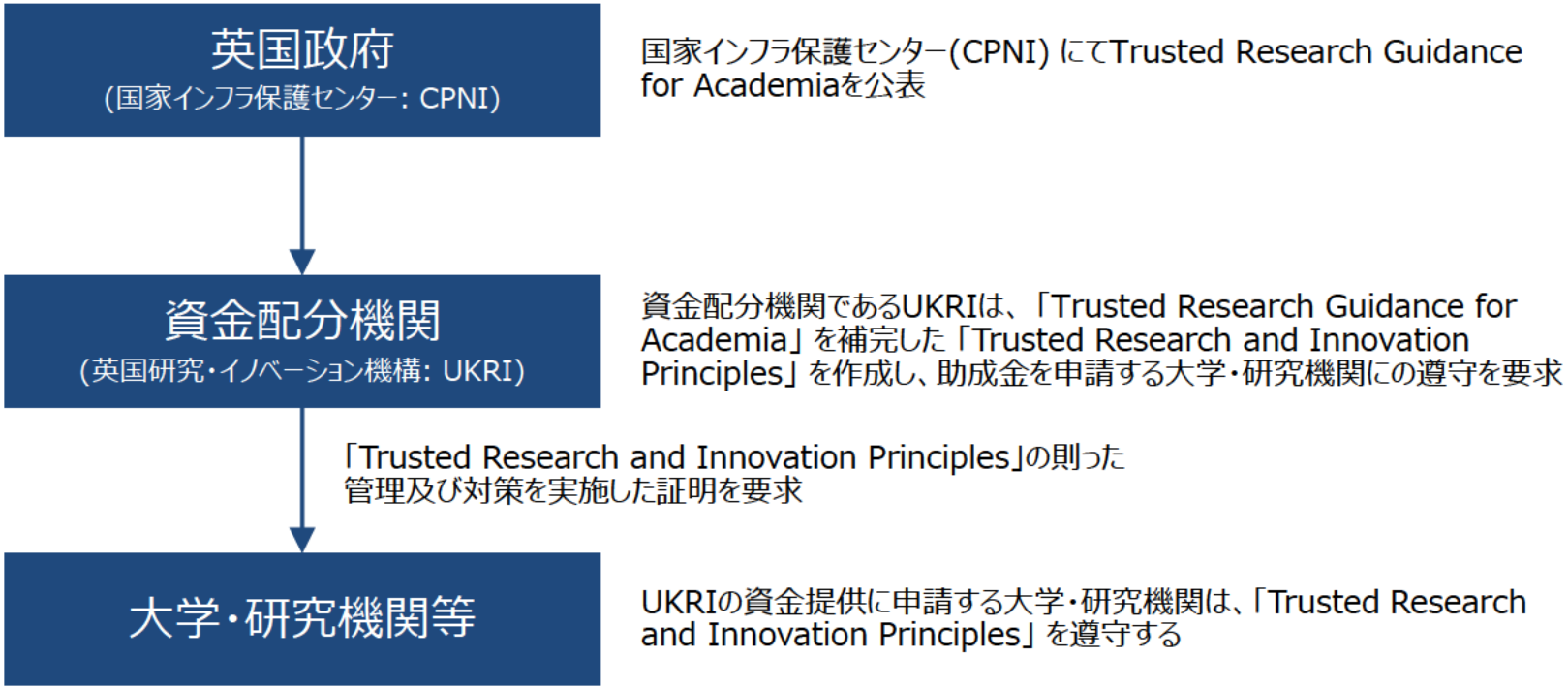
英国における研究インテグリティに関連する政府機関／大学機関／R&D 資金提 供機関、これらの機関が発行するガイドライン、関連する法規制、大学・研究機関等 との相互関係

[出典] 未来工学研究所、“研究インテグリティ(Research Integrity)に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_5.pdf

© Hitachi, Ltd. 2024. All rights reserved.

研究セキュリティ確保に向けた施策の推進体制(概要)

- 研究セキュリティに関する方針はCPNIにて「Trusted Research Guidance for Academia」が公表されている。
- 資金配分機関であるUKRIは、上記のガイドラインを補完した「Trusted Research and Innovation Principles」を公表し、助成金を申請する機関に対しての遵守及び証拠の提出を要求している。

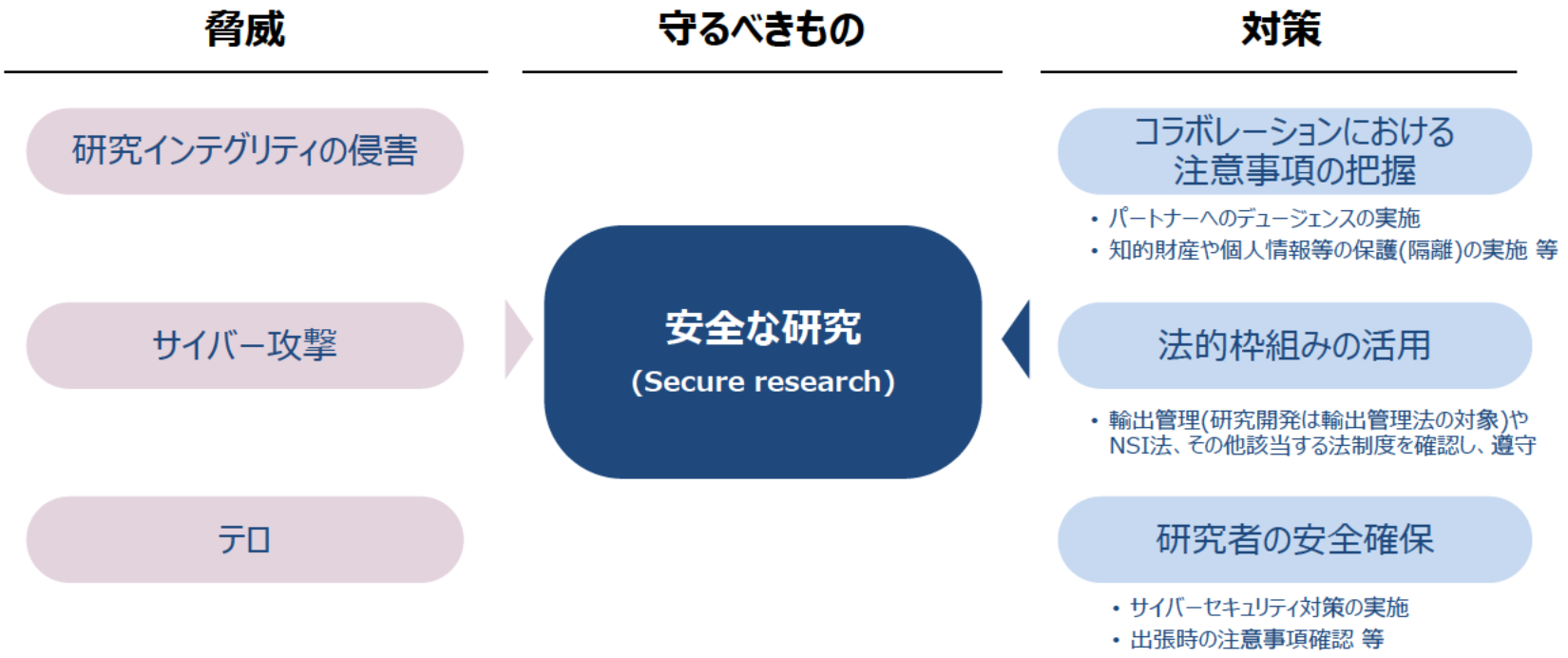


© Hitachi, Ltd. 2024. All rights reserved.

2.3.1-1. リスクに対する考え方

HITACHI
Inspire the Next

- 研究インテグリティの侵害、サイバー攻撃、テロ等が安全な研究に対する脅威と認識されているところ、海外の研究パートナーとコラボレーションする場合の注意事項の把握、法的枠組みの確認・遵守、サイバーセキュリティ対策 等による研究者の安全確保が対策に含まれている。



文献	記載
Trusted Research Guidance for Academia	How to protect your research ・Collaborating with research partners - protecting intellectual property, making informed decisions about international collaboration and managing cyber risks ・Using legal frameworks, understanding contractual expectations, export controls and GDPR ・Helping researchers to stay safe - protecting your personal and research data, working with overseas researchers and attending conferences abroad

© Hitachi, Ltd. 2024. All rights reserved.

2.3.1-2. 対象となる事業、情報の分類等

HITACHI
Inspire the Next

- UUK、UKRI、DBT,ECJU、BEISが公表しているガイドラインは大学等の研究機関を対象にしているがUKRIのみが対象者に遵守を求めており、遵守した証明も提出する必要がある。

ルールの適用対象となる主体や条件等

機関	ガイドライン	対象となる事業
UKRI	「Trusted Research and Innovation Principles」	対象：助成金を申請する大学・研究機関 ※ガイドラインの遵守とその証明を提示する必要がある
CPNI	「Trusted Research Guidance for Academia」	対象：研究者 (特に、STEM 科目、デュアルユース技術、新興技術、商業的に機密性のある研究分野等の研究者)
UUK	「Managing risks in Internationalisation: Security related issues」	対象：UUK に加盟している 139 の大学や研究機構
DBT, ECJU	「Export controls applying to academic research」	対象：軍事目的に使用される危険性が高い分野の研究を行っている研究者やポスドク研究者 (航空宇宙技術/応用化学、生化学、化学工学/応用物理学/バイオテクノロジー/電気および機械工学/計装とセンサー/材料技術/原子力技術/生産およびプロセス技術/電気通信と情報技術)
BEIS	「National Security and Investment Act: guidance for the higher education and research-intensive sectors」	対象：大学等の研究機関
CPNI, UUK, UKRI	「Managing risks in international research and innovation: An overview of higher education sector guidance」	対象：大学等の研究機関

© Hitachi, Ltd. 2024. All rights reserved.

2.3.1-3. 具体的な要求事項の内容 / サイバーセキュリティの位置づけ

HITACHI
Inspire the Next

- 「Managing risks in international research and innovation」において、サイバーセキュリティは「大学の職員とキャンパスの保護」に関する部分で触れられており、「Trusted Research Guidance for Academia」では、サイバーセキュリティは「研究者の安全確保」に関する部分で触れられている。

Managing risks in international research and innovationにおける位置づけ

#	カテゴリ	要求事項
1	大学の評判と価値の保護	略
2	大学の職員とキャンパスの保護	1. 法的枠組み、輸出規制及び GDPR の活用と理解 2. 個人データや研究データの保護と厳重な保管 データへのアクセスの制御と監視を含む、サイバーセキュリティ戦略の策定・実施・見直し 3. プロジェクトや研究活動の性質の考慮
3	教育パートナーシップを理解する	略

Trusted Research Guidance for Academiaにおける位置づけ

#	カテゴリ	要求事項
1	研究パートナーとのコラボレーションで注意すべきこと	1. デューデリジェンス 2. 利益相反 3. 隔離
2	法的枠組みの活用	1. 輸出管理 2. 法律 3. GDPR 4. NSI法
3	研究者の安全確保	1. ビザ 2. 出張時のアドバイス

「研究者の安全確保」カテゴリにて、サイバーセキュリティを適切に実践すれば、研究データの損失や侵害の可能性が低くなる旨、記載有り

© Hitachi, Ltd. 2024. All rights reserved.

2.3.1-3. 具体的な要求事項の内容 / サイバーセキュリティ対策の内容

HITACHI
Inspire the Next

- 「Trusted Research and Innovation Principles」には具体的な対策が記載されているわけではないが、「Trusted Research Guidance for Academia」では、教育機関のポリシーに沿ったサイバーセキュリティに加え、以下のような具体的な対策が推奨されており、参考とすることができる。

#	要求事項	具体的な内容
1	**データの使用、共有**	1. 強力な個別のパスワードを使用してメールを保護する(メールアカウントの保護) 2. 最新のソフトウェアとアプリのアップデートをインストールする 3. 2段階認証をオンにする 4. パスワードマネージャの利用 5. データのバックアップ 6. ランダムな3つの単語を使用した解読困難なパスワードの作成
2	**USBドライブ**	1. USB ドライブのソースがどの程度信頼できるかを考慮する 2. 設定またはシステム環境設定を通じて、デバイスで「自動実行」が無効になっていることを確認する 3. デバイスが USB ドライブ上のデータにアクセスする前に、ウイルス対策ソフトウェアが自動スキャンを実行していることを確認する 4. 情報を共有する必要がある場合は、代替手段 (クラウド ストレージ、電子メール、専用のコラボレーション プラットフォームなど) を検討する
3	**フィッシング攻撃の防止**	1. フィッシング詐欺が電子メールで使用するテクニックを理解する 2. フィッシングメールをクリックした場合、インシデント報告先に迅速な報告を行う (その他、詳細はNCSCのサイトを参照) https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

[出典] NPSA" Trusted Research Guidance for Academia"
https://www.npsa.gov.uk/trusted-research-academia

© Hitachi, Ltd. 2024. All rights reserved.

2.3.1-4. 資金配分機関による取組み

HITACHI
Inspire the Next

- 資金配分機関であるUKRIは「Trusted Research and Innovation Principles」に記載のカテゴリ(パートナーの適正評価、情報・知識共有管理、商用への応用)について遵守することを、助成金申請機関に求めている

#	カテゴリ	要求事項
1	パートナーの適性評価	**財政的及び非財務的な協力パートナーとなりうる組織や個人について適切なデューディリジェンス評価を実施する。** 1. 法的枠組みと提携関係 2. 価値観 3. 利益相反
2	情報・知識共有管理	**組織は機密データや情報へのアクセスが適切に管理されるよう、強固な情報セキュリティ管理策を導入する。** 1. サイバーセキュリティ 2. データの分離 3. データへのアクセス 4. 研究プロジェクト活動と成果
3	商用への応用	**プロジェクトから得られる機密データや知的財産権を含む知的資産が適切に管理されるよう、共同研究契約を締結する。** 1. 知的資産と知的財産権 2. プロジェクトの成果物の公開 3. 輸出管理

[出典] 未来工学研究所、“研究インテグリティ(Research Integrity)に係る調査・分析”
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/ri_report_fy2022_5.pdf

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.3.2 企業を対象にした取組み

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-1. 英国におけるデータ保護法制の全体像

HITACHI
Inspire the Next

- データの保護はコモン・ローでの保護が原則となっており、機密情報が侵害された場合は民事的な救済措置を請求することができる。
- また、機密情報が侵害された際、窃盗や著作権侵害に当たる場合は刑事的措置も可能となる。
- 尚、不正アクセスがなされた場合はコンピュータ不正使用法により刑事罰が執行される。

データ保護に関する考え	法制度によるデータ保護						契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
	営業秘密			不正アクセス					
	制度名称	民事	刑事	制度名称	民事	刑事			
価値あるデータは、営業秘密(機密情報の保持)、競争法、コンピュータ不正使用法 等対応可能な範囲内で保護。	コモン・ロー	○	○	コンピュータ不正使用法(1条、3条)		○		データベース保護指令に基づく国内法	

- 経済的に価値のあるデータの保護は、第一義的にコモン・ローにより「機密情報(confidential information)」が保護され、これが侵害された場合には差止等、民事的な救済措置を請求することができる。
- 機密情報の保護については、刑事的救済措置はないものの、窃盗や著作権侵害にあたるとされる場合には刑事的措置を施すことが可能である。これに加えて、1989 年**競争法によって「商業的にセンシティブな情報(commercially sensitive information)」が保護**され、救済手段として制裁金の支払い等に加え、刑事的訴えが可能な場合もある。
- データへの不正なアクセスが為された場合には、コンピュータ不正使用法により刑事罰が執行される。

[出典] 平成２９年度産業経済研究委託事業 海外におけるデータ保護制度に関する調査研究 調査報告書
https://www.meti.go.jp/policy/economy/chizai/chiteki/keizaisanngyou29.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-2. NIS規則における研究開発機関の扱い

HITACHI
Inspire the Next

- 英国のNIS規則により、経済と社会にとって重要であり、ネット ワーク及び情報システムに大きく依存するエネルギー、運輸、飲料水、医療、デジタルインフラについては、サイバーセキュリティに関するリスク管理、報告義務が課せられている。
- EUのNIS2指令とは異なり、研究機関は対象セクターに含まれていない。

NIS規則

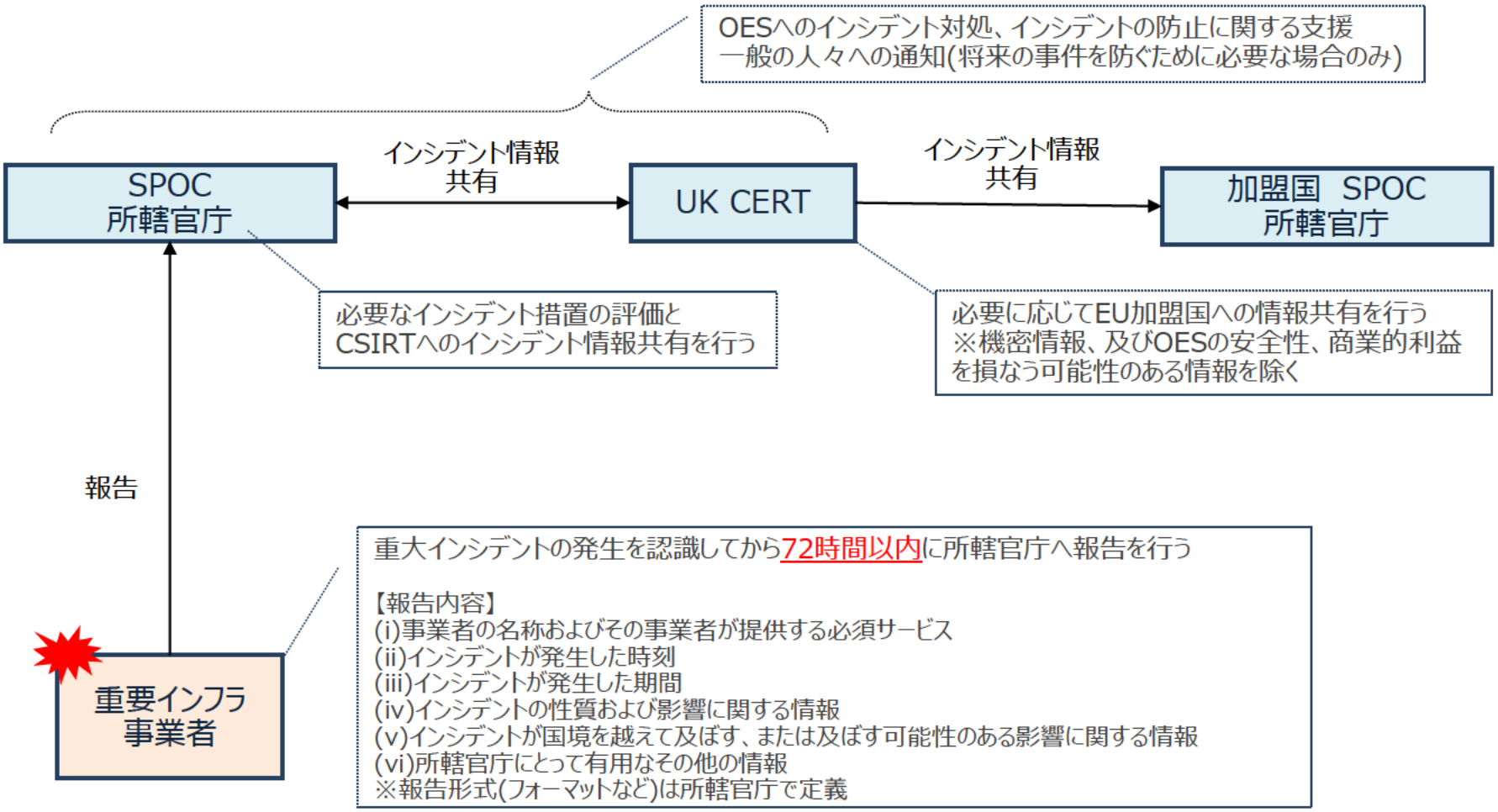
カテゴリ	詳細
スコープ	エネルギー(電力、石油、ガス)、運輸(航空、鉄道、船舶、道路)、飲料水、保険医療、 デジタルインフラ、及び重要デジタルサービスプロバイダー(検索エンジン、クラウドコンピューティングサービス、オンラインマーケットプレイス)
要件	• ネットワークおよび情報システムの セキュリティに及ぶリスクを管理する ために、適切でバランスの取れた技 術的・組織的対策をとること • ネットワークおよび情報システムの セキュリティに影響するインシデント のインパクトを防止し、最小限に抑え るために、適切でバランスの取れた技 術的・組織的対策をとること • それぞれのサービスに重大な影響をもたらしたインシデントについて、関連する所轄官庁に通知すること • NIS規制に基づく検査要件を満たすこと • 情報、執行、罰則の通知に従うこと
罰則	最大1,700万ポンド※の課徴金を課す ※日本円で約30.9億円(1ポンド=181.75円で換算)

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-3. NIS規則に基づくインシデント報告対応 / 報告フロー

HITACHI
Inspire the Next

- インシデント発生後、事業者は72時間以内に単一連絡窓口(SPOC)へインシデント報告を行う必要がある。



[参考] "NIS Cooperation Group"
https://www.ofgem.gov.uk/sites/default/files/2022-04/NIS%20Guidance%20for%20Downstream%20Gas%20and%20Electricity%20Operators%20of%20Essential%20Services%20in%20GB%20v2.0.pdf

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-3. NIS規則に基づくインシデント報告対応 / 重大なインシデントの基準

HITACHI
Inspire the Next

- 所轄官庁(ICO)への報告対象となるインシデントは、「可用性」「完全性、信頼性、または機密性」「危険」「物的損傷」の観点で1つでも該当した場合となる。

パラメータ	閾値
可用性	サービスが 750,000 ユーザ時間※ 以上利用できなかった ※ユーザ時間：英国で60分間に影響を受けるユーザ数
完全性、信頼性、機密性	インシデントにより、以下の完全性、信頼性、機密性が失われた • サービスが保管、または送信するデータ • 事業者が提供するシステム • 事業者が提供するシステムを通じて利用可能な関連システム これが15,000人以上のユーザに影響を与えた
危険	インシデントにより、公共の安全、人命が失われるリスクが生じた
物的損傷	インシデントにより英国の少なくとも1人のユーザに重大な損害が発生し、そのユーザへの損害額は85万ポンドを超えた

[参考] ICO"Enforcement"
https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/?q=DSP

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-3. NIS規則に基づくインシデント報告対応 / 罰則適用の考え方

HITACHI
Inspire the Next

- NIS規則 未遵守の場合、執行通知が出され、措置が取られない場合に基準に応じた罰金が適用される。

NIS規則に関する通知 (遵守状況の確認、違反発見時)

#	通知の種類	説明
1	情報通知 (information notices)	**以下のようなセキュリティ対策状況評価するために合理的に情報が必要な場合** 1.ネットワークと情報システムのセキュリティ 2.実施された検査を含む、セキュリティポリシーの実施
2	執行通知 (enforcement notices)	**以下、NIS規則の要求事項に違反していると判断する合理的な理由がある場合** 1.セキュリティ義務の履行 **2.セキュリティインシデントの通知** 3.通知義務の遵守 4.インシデントについて一般に通知するよう求められた場合、その旨を一般に通知 5.情報通知の遵守 6.検査要件に従う
3	罰則通知 (penalty notices)	**措置を講じなかった場合、またはその措置を講じる必要がない理由について、ICOが説明に満足できない場合** **【通知内容】** 1.罰則を課す理由 2.課す金額通知の日付 3.違約金を支払う期日 4.通知に対する異議申し立ての方法 5.指定された期間内に支払わなかった場合の結果

NIS規則 違反時の罰金

#	罰金額	基準
1	最大 1,000,000 £	情報通知への違反や検査への協力の欠如など、インシデントを引き起こす可能性がないとICOが判断した場合
2	最大 8,500,000 £	重大な規則違反があったとICOが判断した場合 ※重大な規則違反とは、セキュリティ義務の遵守など、 ICOが特定した問題を**是正するための措置を特定の期間内に講じなかった場合を指す**
3	最大 17,000,000 £	重大な規則違反でサービスの提供に重大なリスクまたは重大な影響をもたらした、 または引き起こす可能性があるとICOが判断した場合

[参考] UK GOV"The Network and Information Systems Regulations 2018"
https://www.legislation.gov.uk/uksi/2018/506#commentary-key-a8c9cc8155aaf9922789d00f3cf293d2
ICO"Enforcement"
https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/?q=DSP

© Hitachi, Ltd. 2024. All rights reserved.

2.3.2-3. NIS規則に基づくインシデント報告対応 / 罰金の算定基準

HITACHI
Inspire the Next

- 罰金を課すか否か、またその金額を決定する基準は、規制措置ポリシー(Regulatory Action Policy)で定められており、本ポリシーは他の規則(GDPR 等)も罰則の適用時に参照している。
- 具体的な算定基準としてはインシデントへの故意性、発生時の措置、過去の遵守状況(不履行)が考慮される。

罰金額の算定基準

1. 不履行の性質、重大性、期間
2. 不履行の故意性または関与した過失の程度
3. データ主体が被った損害または苦痛を軽減するために管理者または処理者が講じた措置
4. GDPRおよびDPA第57条、第66条、第103条、第107条に従って管理者または処理者が実施した技術的および組織的措置を考慮した、管理者または処理者の責任の程度
5. 管理者または処理者による関連する過去の不履行
6. 不履行を是正し、不履行がもたらす可能性のある有害なリスクを軽減するための、ICOとの協力の程度
7. 不履行の影響を受ける個人データのカテゴリー
8. 管理者または処理者がICOに不履行を通知したかどうか、および通知した場合はその程度を含め、ICOに知らせた方法
9. 管理者または処理者が過去の施行通知または罰則通知にどの程度従ってきたか
10. 承認された行動規範または認証メカニズムの遵守
11. 事案に適用されるその他の加重要因または軽減要因、不履行の結果（直接的か間接的かを問わず）得られた金銭的利益または回避された損失を含む
12. 罰則が効果的、比例的かつ抑制的であるかどうか

[参考] ICO“Enforcement”
https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/?q=DSP

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

2.3.3 機微技術流出後の対応事例

© Hitachi, Ltd. 2024. All rights reserved.

2.3.3-1. 事例検討

HITACHI
Inspire the Next

- NCA(国家犯罪対策庁)の関与した大規模のサイバー攻撃に関する事例の内、Genesis Market(ダークウェブ)の閉鎖に成功した際、24人をコンピュータ不正使用法と詐欺罪の容疑で拘留している。

脅威グループ	概要	対応
Conti/Trickbot	**ロシアのランサムウェア集団** 11人を摘発し、英米政府が制裁措置を実施した。 本集団はマルウェアとランサムウェアの開発、資金洗浄、詐欺、ログインの詳細情報を窃盗するための悪意あるコードのウェブサイトへの挿入、そして管理業務に携わっていた。 英国の被害者149人から少なくとも2,700万ポンド※を強要した責任があるとNCAに判断されている。 ※日本円で約49億円(1ポンド=181.75円で換算)	渡航禁止と資産凍結(英国政府)
Qakbot(Qbot/Pink Slipbot)	**バンキング型トロイの木馬(銀行口座情報の窃取に特化したトロイの木馬)** 2023年8月、米国司法省が多国籍作戦によりQakbotのテイクダウンを発表した。(NCA関与) QakbotはConti、ProLock、Egregor、REvil、MegaCortex、Black Bastaランサムウェア株の背後にいる犯罪グループによって、銀行の認証情報を含む個人データを被害者から盗むために使用されていました。	約860万ドル相当の違法な仮想通貨利益を押収(米国当局)
Genesis Market	**Qakbotサイバー攻撃によって盗み出した情報を販売する犯罪プラットフォーム** FBIとオランダ警察が中心となって進められ、2023年4月に「Genesis Market」を閉鎖することに成功した(NCAが関与)。 また、英国では34歳と36歳の男性2人を含む24人が逮捕され、コンピュータ不正使用法と詐欺罪の容疑で拘留している。 本プラットフォームでは200万人以上から盗んだ約8,000万件の認証情報とデジタル指紋を保管していた。	コンピュータ不正使用法と詐欺罪の容疑で拘留

[出典] NCA" Russian ransomware group hit with new sanctions"
https://www.nationalcrimeagency.gov.uk/news/russian-ransomware-group-hit-with-new-sanctions
NCA" Notorious criminal marketplace selling victim identities taken down in international operation"
https://www.nationalcrimeagency.gov.uk/news/notorious-criminal-marketplace-selling-victim-identities-taken-down-in-international-operation
NCA" Qakbot: cyber crime service taken out in international operation"
https://www.nationalcrimeagency.gov.uk/news/qakbot-cyber-crime-service-taken-out-in-international-operation

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

3. ITベンダー向けの規制動向

© Hitachi, Ltd. 2024. All rights reserved.

調査目的及び調査対象 (1/2)

- 調査項目(3)では、ITベンダに対する規制を対象として、具体的な要求や過失が発生した場合の行政機関による働きかけの手段等について整理を行った。

調査目的

- 海外におけるITベンダに対する規制の整理を通じて、ITベンダに対する具体的な要求や過失が発生した場合の行政機関による働きかけの手段の有無(及びその内容)等を理解する。

調査対象

- 以下のような特徴を持っている規制を調査対象とした。
  - ✓ 政府からITベンダ等に対して直接的に課される/政府から重要インフラ事業者に課される規制がITベンダ等に間接的に課される
  - ✓ サイバーセキュリティ対策の実施を求める規定が規制全体の一部または全部を構成している
  - ※サプライチェーンにおける特定国製品の排除等を求めるものは今回は対象外とした。

分類	調査対象	概要
米国	アメリカ国防予算経理局 252.204-701条 (DFARS Clause252.204-7012)	2016年公表。米国防総省が契約する者に対し、「NIST SP800-171」相当のサイバーセキュリティの対応を要求。
	行政部門および政府機関の長向けの覚書 (連邦政府機関が調達するソフトウエアに関してセキュリティー要件を定めるガイダンス)	2022年9月公表。「安全なソフトウエア開発フレームワーク(SSDF) と「ソフトウエアサプライチェーン・セキュリティーガイダンス」をベンダ等に順守させることを目的として、OMBが各連邦政府機関に対して公表したガイダンス。
欧州	NIS指令	2022年12月に改正法が官報掲載。2024年10月18日より施行予定。EU域内でサービスを提供する又は活動を行うエンティティを対象にした規制。規制対象には、デジタルインフラ分野において、「クラウドコンピューティングサービスプロバイダー」や「一般に利用可能な電子通信サービスのプロバイダー」が含まれる。(Annex I)
	一般製品安全規則	2023年6月に改正法を施行。(2024年12月適用開始)製造事業者を含む事業者に対して、「安全な製品」のみを域内市場に供給する義務を課す消費者保護規制。安全な製品かを評価する際に、サイバーセキュリティ等の観点も考慮することとされている。

© Hitachi, Ltd. 2024. All rights reserved.

調査目的及び調査対象 (2/2)

HITACHI
Inspire the Next

調査対象 (続き)

分類		調査対象	概要
欧州	EU	EU無線機器指令	2022年2月発行、2024年8月より義務化予定。直接・間接問わずインターネットに接続される無線機器が対象。サイバーセキュリティの要求事項を記載。(第3条3項)
		民間航空機規則 (CRAの対象外)	2018年7月施行。民間航空分野における共通規則。ドローンを含む、航空機に対する必須要件にセキュリティ要素が盛り込まれている。
		自動車の型式承認規則 (CRAの対象外)	2019年11月施行。自動運転車を対象とするシステム、構成部品及び単体技術ユニットの一般的安全性、及び乗員・歩行者の保護に関する型式認証要件を定める。
		機械規則	2023年6月施行。(機械指令から機械規則に変更)機械製品の市場投入または使用開始を可能にするために、機械製品の設計および構造に関する要件を規定。悪意のある第三者の行為から生じるリスクに対処するためのサイバーセキュリティ対策が新たに追加された。(EHSR 1.1.9)
		製造物責任指令案	2022年9月に案を公表。製造物責任指令案は、EU域内で上市されるあらゆる製品に適用され、製造事業者が責任を負うことが明確にされている。製品にはソフトウェアが含まれ、サイバーセキュリティ対応のアップデート等にも製造事業者が責任を負う。
		AI規則案	2023年6月に案を採択。(欧州理事会での年内合意を目指す) AIシステムを対象とした法的枠組み。ハイリスクAIシステムの要件にはサイバーセキュリティに係る要件が含まれる。(例:第15条)
	英国	英国のサイバーレジリエンスを向上させるための法律案	2022年1月に提案内容公表。マネージド・サービス・プロバイダーに出現によってセキュリティ脅威が拡大したため、適切な措置をとることを保証するための包括的な枠組みを提供することを目的とする。
その他	中国	中国サイバーセキュリティ法 ※場合によって中国データ関連三法を調査	2021年6月に改正案が施行。ネットワークサービス事業者に加えて、社内のネットワーク利用者やウェブサイト開設者も対象に含む「ネットワーク運営者」が規制の対象。改正案では、ネットワーク運営でのセキュリティ保護義務違反やネットワーク運営の安全を損なう結果をもたらす行為に対する行政処罰について調整が加えられている。
	日本	PL法	1995年7月施行。製品の欠陥によって人の生命、身体又は財産に被害を被ったことを証明した場合に、被害者は製造業者等に対して損害賠償を求めることができるとする法律。セキュリティ上の欠陥が一般的に考えて予見することができ，かつ回避し得るものならば，民事訴訟を起こして損害賠償を請求できる可能性もある。

© Hitachi, Ltd. 2024. All rights reserved.

調査項目及び整理の観点等

HITACHI
Inspire the Next

- 規制ごとに、基礎情報として一般的な事項を整理した上で、以下を整理した。
  - 規制の類型
  - 具体的な要求
  - 過失が発生した場合の行政機関による働きかけの手段の有無及びその内容

分類	調査項目		整理の観点等
1 一般的な事項	1-1	施行年度	-
	1-2	国・地域	-
	1-3	施行主体	-
	1-4	設立目的	-
2 詳細情報	2-1	規制の類型	• 義務 • 任意
	2-2	具体的な要求	• IT製品上市前の要求 • IT製品上市後の要求
	2-3	過失が発生した場合の行政機関による働きかけの手段の有無及びその内容	• 有無 • (働きかけの手段がある場合)働きかけの内容 ✓金銭的な罰則を伴わない働きかけ(例:行政指導) ✓金銭的な罰則を伴わない働きかけ(例:罰金)

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

3. ITベンダー向けの規制動向

3.1. 一般的な事項

3.2. 詳細情報

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (1/5)

HITACHI
Inspire the Next

分類		調査項目	調査結果
1 米国	アメリカ国防予算経理局252.204-701条	1-1 施行年度	2016年10月21日に最終規則を発行(既存の規則を修正)
		1-2 国・地域	米国
		1-3 施行主体	国防総省(DoD)
		1-4 目的	請負業者に対して、十分な情報セキュリティ保護を実施した情報システムを提供もしくは管理させることを目的とする。
2	行政部門および政府機関の長向けの覚書	1-1 施行年度	2023年6月
		1-2 国・地域	米国
		1-3 施行主体	一般予算管理局(OMB)
		1-4 目的	M-22-18で確立された要件を強化し、安全なソフトウェア開発プラクティスの重要性を再確認し、省庁がソフトウェア製作者から証明書を収集するスケジュールを延長することを目的とする。
3 欧州	NIS指令	1-1 施行年度	2022年12月に改正法が官報掲載。2024年10月18日より施行予定
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	欧州委員会加盟国を対象とする指令であり、市場におけるセキュリティレベルのばらつきを改善するよう法的枠組みを最新化し、急速なデジタル化に合わせて進化するサイバー攻撃の脅威に対応することを目的とする。

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (2/5)

HITACHI
Inspire the Next

分類		調査項目	調査結果
4 欧州	一般製品安全規則	1-1 施行年度	2023年6月に改正法を施行。(2024年12月適用開始)
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	製造事業者、認定代理人、輸入事業者、販売事業者などの事業者に対して「安全な製品」のみを域内市場に供給することを目的とする。なお、安全な製品かを評価する際に、サイバーセキュリティ等の観点も考慮することとされている。
5	EU無線機器指令	1-1 施行年度	2022年2月発行、2024年8月より義務化予定。
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	域内市場の機能向上を視野に入れ、域内全体でサイバーセキュリティの高い共通レベルを達成することを目的としている。
6	民間航空機規則	1-1 施行年度	2018年7月施行
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	欧州における民間航空の安全性を高い水準で均一に確立し、維持することを目的とする。(第1条主題と目的より)

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (3/5)

HITACHI
Inspire the Next

分類		調査項目	調査結果
7 欧州	自動車の型式承認規則	1-1 施行年度	2019年11月施行
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	企業と消費者の利益のために欧州市場の適切な機能を確保し、自動車等における高水準の安全性と健康および環境保護を提供することを目的とする。自動車およびそのトレーラー、ならびに自動車を対象とするシステム、部品および個別の技術ユニットの型式承認、ならびに個々の自動車の承認に関する規則と原則を定める。(前文7より)
8	機械規則	1-1 施行年度	2023年6月施行。(機械指令から機械規則に変更) 機械指令(2006/42/EC)は2027年1月14日に廃止。
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	従来の機械指令の目的は、欧州市場において機械に対する安全衛生要件を調和させ、加盟国間の機械貿易の障害を取り除くこととしている。(前文1より)本規則では、その目的を引き継ぎつつ、適用範囲内の製品を欧州市場で入手できるようにするための枠組み(適用範囲と定義)に関する明確な規則等を新たに規定している。
9	製造物責任指令案	1-1 施行年度	2022年9月に案を公表
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	欠陥製品によって身体的損害や物的損害を被った人々を補償する制度を提供することを目的とする。(覚書1.1 提案の理由と目的)

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (4/5)

HITACHI
Inspire the Next

分類		調査項目	調査結果
10 欧州	AI規則案	1-1 施行年度	2023年6月に案を採択。 (欧州理事会での2023年内の合意を目指す)
		1-2 国・地域	欧州
		1-3 施行主体	欧州委員会
		1-4 目的	主に、以下の目的を有する。(説明文書1.1 本提案の理由及び目的より) – AIのリスク（健康、安全、基本権などへのリスク）に対処する – AIの導入、AIへの投資、AIによるイノベーションを強化する
11	英国のサイバーレジリエンスを向上させるための法律案	1-1 施行年度	2022年1月に提案内容公表 2022年12月にパブリックコメントの結果公表
		1-2 国・地域	英国
		1-3 施行主体	デジタル・文化・メディア・スポーツ省(DCMS)
		1-4 目的	多くの企業にサービスを提供するマネージド・サービス・プロバイダーに出現によって、攻撃の影響が広範囲に広がりやすくなり、新たなセキュリティ脅威が生じた。サービスを確保するために適切な措置をとることを保証するための包括的な枠組みを提供することを目的とする。
12 中国	重要情報インフラセキュリティ保護条例	1-1 施行年度	2021年9月施行
		1-2 国・地域	中国
		1-3 施行主体	国務院
		1-4 目的	「中華人民共和国ネットワークセキュリティ法」に基づき、重要情報インフラのセキュリティを保障し、ネットワークのセキュリティを維持するため、運営者の責任と義務等を具体的に示すことを目的とする。

© Hitachi, Ltd. 2024. All rights reserved.

基礎情報 (5/5)

分類	調査項目	調査結果
13 日本 PL法	1-1 施行年度	1995年7月施行
	1-2 国・地域	日本
	1-3 施行主体	消費者庁
	1-4 目的	製造物の欠陥により人の生命、身体又は財産に係る被害が生じた場合にお ける製造業者等の損害賠償の責任について定めることにより、被害者の保護を図り、もって国民生活の安定向上と国民経済の健全な発展に寄与することを目的とする。

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

3. ITベンダー向けの規制動向

3.1. 一般的な事項
3.2. 詳細情報

© Hitachi, Ltd. 2024. All rights reserved.

サマリ / 適用対象・具体的な要求

- 適用対象外であったソフトウェアが新たに規制の対象に含まれる可能性がある。
- サイバーセキュリティの要素が改正にて新たに追加されている一方で、具体的な要件は他の標準を参照しているルールが見られた。また、リスク管理義務や機器に関連する要件に加えて、ベンダに対して報告義務を課しているルールがみられた。

分類		調査結果
適用対象		• **対象外であったソフトウェア(単体)が対象に新たに含まれる可能性がある**。なお、日本のPL法ではハードウェアを伴わないソフトウェアは対象外となっている。[製造物責任指令案]
具体的な要求	平常時の要求	• サイバーセキュリティの要素が改正にて新たに追加されている。しかし、**要件レベルでの詳細化**はなされておらず、他の標準を参照することとしている。 • 上市前に自明でなかったとしても、**脆弱性に対処するために必要なソフトウェア・セキュリティ・アップデートを提供しなかった場合、製造業者に責任が生じ得る**とするルールが提案されている。成立した場合、非常に大きな影響があるため、注視が必要。[製造物責任指令案]
	異常時(インシデント等の発生時)の要求	• リスク管理義務や関連する要件を定めていることに加えて、重大なインシデントが発生した場合に、**ベンダに対して監督官庁等へ報告義務を課している場合**がある。[NIS指令] • なお、EUサイバーレジリエンス法(注:本調査の対象外)においても、インシデントや脆弱性を発見した場合に、ベンダに対して、例えば以下のような**監督官庁やユーザに対する報告義務(11条)**を課している。 ✓ 積極的に悪用された脆弱性を発見してから24時間以内にENISAに通知する。 ✓ インシデントを認識してから24時間以内にENISAに通知する。 ✓ インシデントの影響を緩和するための是正措置について遅滞なくユーザーに通知する。

© Hitachi, Ltd. 2024. All rights reserved.

サマリ / 働きかけの手段

- 事業者への監督に係る権限ではなく、製品の販売停止等を含む執行の権限や金銭的な罰金を課す権限を監督省庁へ付与することによって、事業者へ要件遵守を強制していると考えられる。

働きかけの手段		調査結果
金銭的な罰則を含まない働きかけ	事業者の監督について	• 訓練を受けた専門家による抜き打ち検査を含む、**立入検査等の権限を監督官庁に認めているルール**みられる。[NIS指令] • 注意喚起を含む、**不遵守に対する状況の改善を要求する権限を監督省庁に認めているルール**が見られる。[EU無線機器指令、民間航空機規則]
	事業者に対する執行について	• **製品の市場投入または市場での入手を禁止、一時停止、または制限する措置を行う権限**が監督官庁に認められている。[一般製品安全規則、EU無線機器指令]
金銭的な罰則を含む働きかけ		• 対象となる事業者の重要度によって、罰金額に差異を設けており、**より重要度が高いと考えられる事業者における違反に対して、より多額の罰金**を課している。[NIS指令] • また、対象となる事業者が同じであったとしても、遵守していない要件によって、罰金額に差を設けている。**重要と考えられる対策要件を遵守しない事業者に対してより高額な罰金を課している**。[AI規則案] • 規定内で金銭的な罰則を設けていなくとも、EU加盟国によって設けられる可能性がある。

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 主要各国における製造物責任法の比較

HITACHI
Inspire the Next

- 日本と米国では対象外となっているソフトウェアが欧州の製造物責任指令案では対象に含まれている。
- 各国・地域ともに製品が市場で投入された時点で予期できなかった瑕疵や欠陥は免責される一方で、欧州ではソフトウェアがアップデートがされてないない場合には免責対象とはならない。

比較項目	欧州	米国	日本	主な差異
対象法制度(成立年度)	製造物責任指令案(2022年9月案公表)	第3次不法行為リステイトメント(1998年公表)	製造物責任法(1995年7月施行)	-
対象製品	• 製品とは、すべての動産を意味し、他の動産または不動物と一体化している場合も含む。 • 製品には、電子、デジタル製造ファイル、ソフトウェアが含まれる。	• 製品とは、使用または消費のために商業的に流通する有形動産を指す。 • 製造物に組み込まれたソフトウェアは対象となる可能性がある。	• 製造又は加工された動産 • 製造物に組み込まれたソフトウェアは対象となる可能性がある。	• 米国と日本において対象外のソフトウェア(単体)が欧州では対象に含まれている。 • 米国、日本では製造物に組み込まれる場合対象となる可能性。
免責事項	• 主に製品が市場に投入された時点等には存在しなかった場合には免責される。 • ただし、安全性を維持するために必要なソフトウェアのアップデートやアップグレードが行われていない場合は除く。	• 販売・供給時点において、製品が、製造上の欠陥を含むか、設計に欠陥が存在するか、または指示・警告が不適切なために欠陥となる場合にはその製品は欠陥製品となる。	• その製造業者等が引き渡したときにおける科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかった場合	• 各国・地域ともに製品が市場で投入された時点で予期できなかった瑕疵や欠陥は免責される。 • ただし、欧州ではソフトウェアがアップデートされていない場合、免責されない。

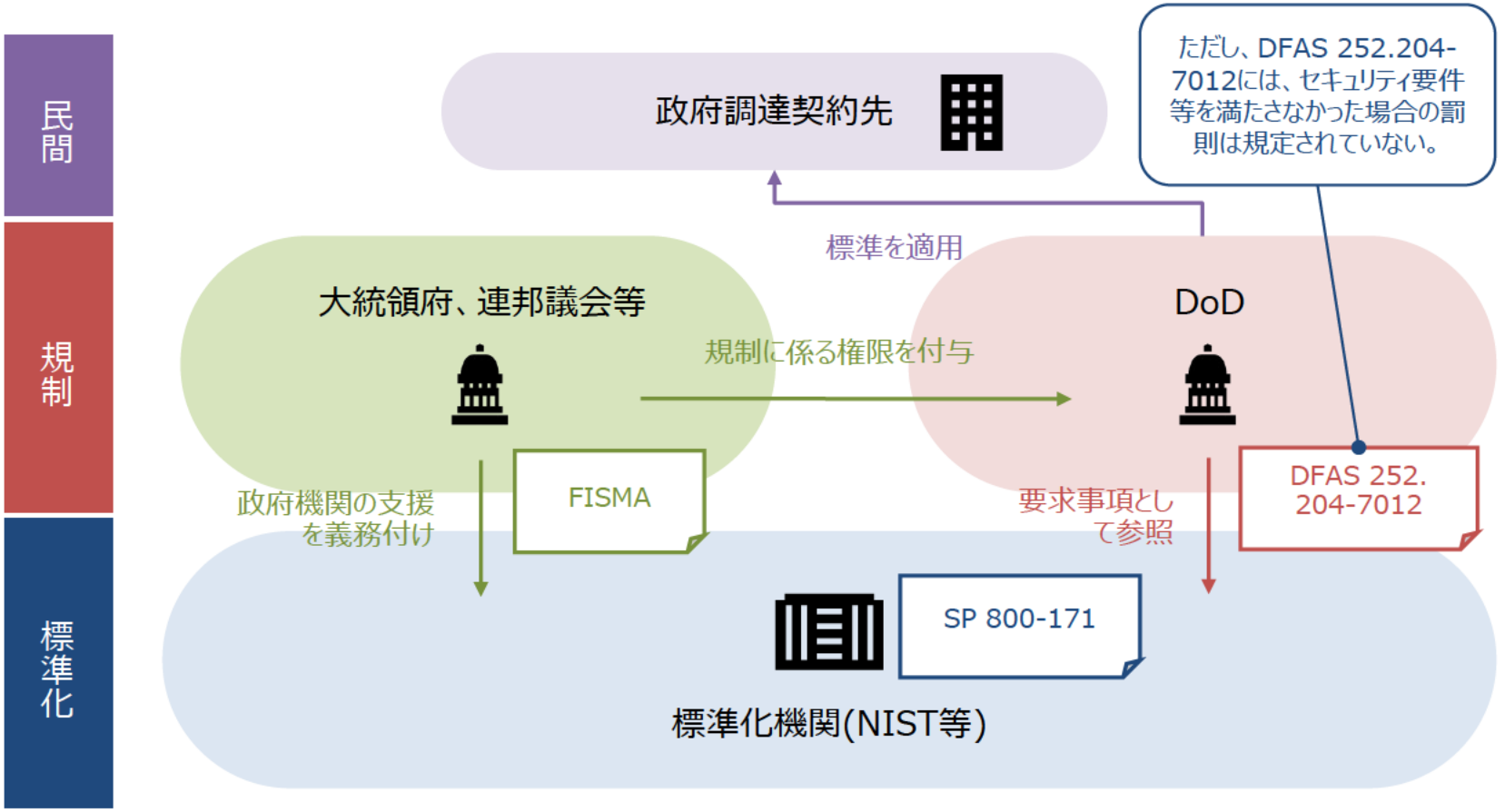
© Hitachi, Ltd. 2024. All rights reserved.

3.2-1. アメリカ国防調達規則(DFARS) / 概要

HITACHI
Inspire the Next

- アメリカ国防総省(以下、DoD)は、NISTが策定したSP 800-171を要求事項として参照したアメリカ国防予算経理局　252.204-7012条(以下、DFARS Clause252.204-7012)の遵守を政府調達契約先に対して義務づけた。

各ステークホルダーと文書の関係性



[参考] DFAS" 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
(https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-1. アメリカ国防調達規則(DFARS) / 具体的な要求 (1/2)

HITACHI
Inspire the Next

- DFAS 252.204-7012では、具体的な要求としてNIST SP 800-171を参照するよう規定されている。

項番	内容
(b)	適切なセキュリティ 請負業者は、対象となるすべての請負業者情報システムに適切なセキュリティを提供するものとする。適切なセキュリティを提供するために、請負業者は、少なくとも次の情報セキュリティ保護を実装するものとする。
(1)	政府に代わって運営されるITサービスまたはシステムの一部である請負業者情報システムには、次のセキュリティ要件が適用される。 (i)クラウドコンピューティングサービスは、DFASの252.239-7010「クラウドコンピューティングサービス」に規定されているセキュリティ要件に従う。 (ii)その他のそのようなITサービスまたはシステム(クラウドコンピューティング以外)は、DFASのその他の箇所で指定されているセキュリティ要件に従う。
(2)	政府に代わって運営されるITサービスまたはシステムの一部ではなく、本項の(b)(1)で指定されたセキュリティ要件の対象とならない請負業者情報システムについては、次のセキュリティ要件が適用される。 (i)本条第(b)項(2)(ii)に定める場合を除き、対象となる請負業者の情報システムは、募集が発行された時点、または契約担当官により許可された時点で有効なNIST SP 800-171のセキュリティ要件に従うものとする。 (ii)(A)請負業者は、2017年12月31日までに、可能な限り速やかに、NIST SP 800-171を実施するものとする。2017年10月1日以前に締結されたすべての契約について、契約者は、契約締結時に実装されていないNIST SP 800-171で指定されたセキュリティ要件について、契約締結後30日以内に、電子メールを介して、国防総省最高情報責任者(CIO)に通知するものとする。 (B)請負業者は、NIST SP 800-171 からの変更要求を契約担当官に書面で提出し、国防総省CIOによる審査を受けるものとする。

[参考] DFAS" 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
(https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-1. アメリカ国防調達規則(DFARS) / 具体的な要求 (2/2)

HITACHI
Inspire the Next

- DFAS 252.204-7012には、前頁に示す要求に加えて72時間以内のサイバーインシデント報告義務を請負事業者に課している。

項番	内容
(c)	サイバーインシデント報告要件
(1)	請負業者は、対象となる請負業者情報システムまたはそこに存在する対象となる防御情報に影響を与えるサイバーインシデント、または運用上重要なサポートとして指定され、契約で特定されている契約の要件を実行する請負業者の能力に影響を与えるサイバーインシデントを発見した場合、請負業者は以下を行うものとする。 (i) 侵害されたコンピューター、サーバー、特定のデータ、およびユーザー アカウントの特定を含むがこれらに限定されない、対象となる防御情報の侵害の証拠についてレビューを実施する。このレビューには、サイバーインシデントの一部であった対象請負業者情報システム、および侵害された対象となる防御情報を特定するためにインシデントの結果としてアクセスされた可能性のある請負業者のネットワーク上の他の情報システムの分析も含まれます、または契約者が運用上重要なサポートを提供する能力に影響を与えるもの。 (ii)サイバーインシデントを国防総省に迅速に報告。(※)
(2)	サイバーインシデントレポート。 サイバーインシデントレポートは、国防総省によって作成された、または国防総省のために作成された情報として扱われ、少なくともhttps://dibnet.dod.milにおいて必要な要素を含めるものとする。
(3)	中程度の保証証明書の要件 この条項に従ってサイバーインシデントを報告するために、請負業者または下請業者は、サイバーインシデントを報告するためのDoD承認の中程度の保証証明書を所有または取得するものとする。DoD 承認の中程度の保証証明書の取得については、「https://public.cyber.mil/eca/」を参照すること。

※:(a)定義において、迅速な報告とは、サイバーインシデントの発見から72時間以内を意味するとされている。

[参考] DFAS" 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
(https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-1. アメリカ国防調達規則(DFARS) / 指摘されている問題点

HITACHI
Inspire the Next

- 米国ミサイル防衛局が、DFAS 252.204-7012への適合について契約企業を調査した結果、全ての要件を満たした企業は存在しなかった。
- Tier1と同等の管理を下請け企業へ要求することが難しかった点や自己申告のため管理レベルは各自の判断に委ねられていただことが指摘されており、かかる問題を踏まえてCMMCの適用が提案された。

NIST800-171がなぜ機能しなかったのか

過大な要求事項と自己申告制が
各企業に都合の良い解釈・判断を許していた

米国防総省監査官によるMDA事前調査レポート

MDA*と契約している7社ほどを抽出して、DFARS 252.204-7012の適合を含む技術情報の保護状況を調べた結果、**全てに合格した事業者はいなかった。**
（2018年3月29日付）

*MDA:Missile Defense Agencyアメリカミサイル防衛局

下請け会社にフローダウン	Tier1と同等の管理は**下請け会社には無理**
契約時に対応状況を提出	自己申告のため、管理レベルは**各自の判断**に委ねれていた

∨

DFASで生じた問題を踏まえて、米国国防総省はNIST SP800-171要件を展開して新しい認証制度の仕組みとしてCMMC(Cybersecurity Maturity Model Certification)適用することを宣言

[参考]株式会社エヴァアビエーション「米国発サイバーセキュリティ対策の新しい評価システムCMMC」
(https://www.jasa.jp/wp-content/uploads/20201112-JasaSeminar_V1.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-2. M-23-16 / 適用対象・各団体の関係性

- OMBは、連邦政府に対して政府情報システムで動作するサードパーティ製コンポネントがNISTガイダンスに準拠することを要求。
- OMBは連邦政府を通じて間接的に民間企業へ規制を課している。

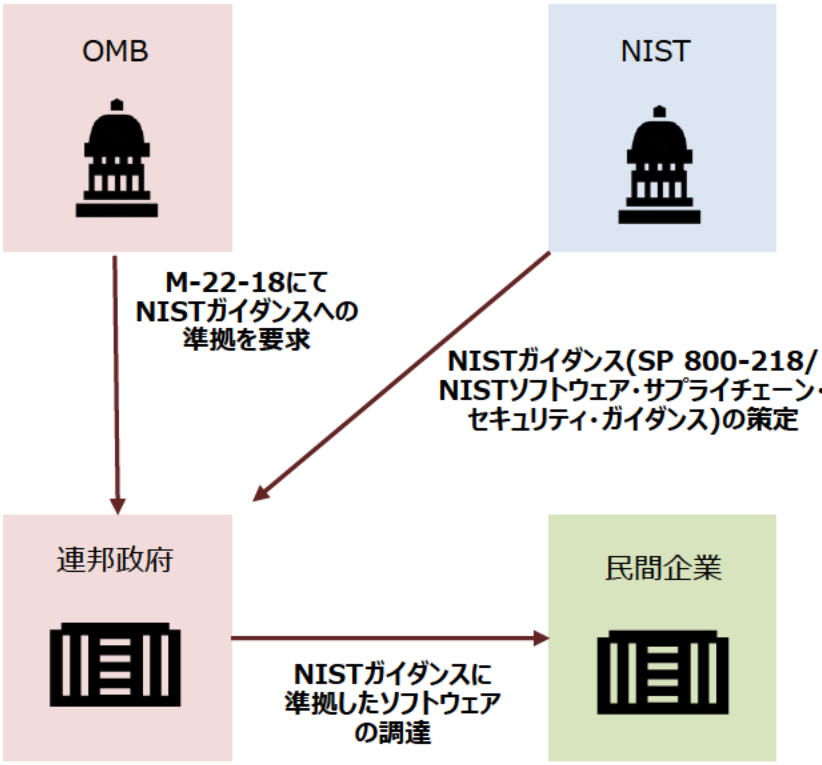
M-23-16の適用対象

項目	概要
適用対象	• (政府が調達する情報システム上で動作する)サードパーティ製コンポネント(※) • 「ソフトウェア」という用語には、ファームウェア、オペレーティング・システム、アプリケーション、およびアプリケーション・サービス(クラウドベースのソフトウェアなど)、ならびにソフトウェアを含む製品が含まれる。
対象者	• 各連邦政府機関

- ただし、本文書の中で、民間企業が連邦政府機関に対して、NISTガイダンスに準拠しなかった場合の罰則については記載されていない。
- ただし、遵守していない企業は政府調達に参加できない可能性があるため、実質的な罰則の役目を果たしている可能性。

※ただし、連邦政府機関が自由に入手できる製品や一般に公開されている製品、省庁が開発したソフトウェアは対象外

各団体の関係性



[参考] OMB"Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices "
(https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-2. M-23-16 / 具体的な要求

HITACHI
Inspire the Next

- 政府機関からの要求に伴い、企業はソフトウェアに係る自己証明書や場合によってはSBOMを公開する必要が生じた。

項目	内容(抜粋)(※)
1. NISTのガイダンスに従い、以下に示す期限までに、各省庁はソフトウェアを使用する前にソフトウェア製作者から自己証明を取得する必要がある。	a. ソフトウェア製造者の自己証明書は、NISTガイダンスで説明されている「適合性宣言書」の役割を果たす。当該政府機関は、当該政府機関が使用する本覚書の要件の対象となるすべてのサードパーティ製ソフトウェア(ソフトウェアの更新や主要なバージョン変更を含む)について、自己証明書を取得しなければならない。 (中略) c. 受理可能な自己証明書には、以下の最低要件が含まれていなければならない。 i. ソフトウェア製作者の名前 ii. ステイトメントがどの製品または製品を指すかの説明 iii. ソフトウェア製作者が、標準的な自己証明書に記載されている安全な開発プラクティスとタスクに従っていることを証明するステイトメント iv. (自己認証は最低限必要なレベルであるが)M-21-30に定義されているように、取得するサービスまたは製品の重要性により、第三者による評価が必要であると、機関はリスクに基づいて判断可能か。
2. 機関は、必要に応じて、安全なソフトウェア開発プラクティスへの適合を実証する成果物をソフトウェア製造者から入手することができる	a. ソフトウェア部品表(SBOM)は、M-21-30に定義されているソフトウェアの重要性に基づき、または政府機関が決定したとおり、募集要件において政府機関が要求する場合がある。要求された場合、ソフトウェア製造者はSBOMを公開し、その公開へのリンクを機関に提供しない限り、SBOMは機関が保持するものとする。 b. SBOMは、米国電気通信情報局の報告書「ソフトウェア部表(SBOM)の最小要素(The Minimum Elements for a Software Bill of Materials」で定義されているデータ形式のいずれかで生成されなければならない。または、Cybersecurity and Infrastructure Security Agency (CISA)によって発行された後継ガイダンスに定義されたデータ形式のいずれかで生成されなければならない。

※M-23-16はM-22-18で確立された要件を強化するものである。上記内容はM-22-18に記載された要件である点に留意いただきたい。

- M-23-16(及びM-22-18)によって、企業はソフトウェアに係る自己証明書や(場合によっては)SBOMを公開する必要が生じた。

[参考] OMB" Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience"
(https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-3. NIS2指令 / 適用対象

- NIS2指令は、EU域内でサービスを提供する又は活動を行う主要エンティティ及び重要エンティティを対象にした規制。本規制は主にユーザが対象となると想定されるが、ITベンダも一部対象の範囲に入る。
- また、対象外となっていたとしても、間接的にITベンダに対して影響を与え得る。

NIS2指令の適用対象

- NIS指令は主にユーザを対象とした規制と考えられる。

分類		内容
46条対象者	主要エンティティ	• エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、**デジタルインフラ、ICTサービスマネジメント**、公的サービス、宇宙
	重要エンティティ	• 郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）、デジタルプロバイダー、研究

ITベンダへの適用状況

- ITベンダも一部対象に入り得る。(パターン1)
- 対象外であっても、間接的にITベンダにも影響を与え得る。(パターン2)

分類			事業者(例)
パターン1	NIS指令の対象	ITベンダ	• クラウド・コンピューティング・サービス・プロバイダー(デジタルインフラ) • マネージド・サービス・プロバイダー(ICTマネジメント)
パターン2	NIS指令の対象外(ただし、間接的に関わり得る)	IT ベンダ	• 受託開発を行うIT事業者(ただし、クラウド等でのオペレーションを行う場合には、パターン1に含まれる)

[参考] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684136497194)等

© Hitachi, Ltd. 2024. All rights reserved.

3.2-3. NIS2指令 / 具体的な要求

HITACHI
Inspire the Next

- 主要及び重要エンティティに対して、リスク管理措置や報告義務に係る要求を定めている。

項目	概要
リスク管理（21条）	2.第1項で言及される措置は、ネットワーク及び情報システム並びにこれらのシステムの物理的環境をインシデントから保護することを目的とするオール・ハザード・アプローチに基づくものとし、**少なくとも次の事項を含むものとする**： (a) リスクマネジメント及び情報セキュリティ対策 (b) インシデントハンドリング (c) ビジネス継続性 (d) サプライチェーンセキュリティ (e) ネットワークやシステムのセキュリティ (f) サイバーセキュリティリスクマネジメントの効率性評価 (g) サイバー衛生の実施及びサイバーセキュリティ教育 (h) 暗号技術の活用 (i) アクセスコントロール等の人的セキュリティ (j) 多要素認証の活用
報告義務（23条）	1. 各加盟国は、必要不可欠かつ重要なエンティティが、第3項（重要なインシデント）にいうサービスの提供に重大な影響を及ぼすインシデントが発生した場合、第4項に従って、**当該エンティティが、過度の遅滞なく、自国のCSIRT又は該当する場合には所轄庁に通知することを確保しなければならない。適切な場合、関係主体は、サービスの提供に悪影響を及ぼす可能性のある重要なインシデントについて、過度の遅滞なく、サービスの受領者に通知しなければならない。**各加盟国は、これらのエンティティが、特に、CSIRTまたは該当する場合、管轄当局がインシデントの国境を越えた影響を判断することを可能にする情報を報告することを確保するものとする。単なる通知行為により、通知主体が責任を負うことはない。 4. 加盟国は、第1項に基づく通知のために、関係主体が CSIRT 又は該当する場合、管轄当局に提出することを保証するものとする： (e) (d)の最終報告書を提出する時点で事故が継続している場合、加盟国は、関係機関がその時点で進捗報告書を提出し、事故の処理から1カ月以内に最終報告書を提出することを確保するものとする。第 1 号の(b)の適用除外として、信託サービス提供者は、信託サービスの提供に影響を及ぼす重大なインシデント について、過度の遅延なく、かつ、いかなる場合においても、重大なインシデントを認識してから **24 時間以内に、CSIRT 又は該当する場合、管轄当局に通知しなければならない**。

- パターン①の事業者は、リスク管理措置を講じることが求められる。
- パターン②は、ユーザ事業者から間接的にリスク管理措置を講じることを求められる可能性がある。

- パターン①の事業者は、報告義務が課せられる。
- パターン③の事業者は、ユーザ事業者の報告に対して協力をする必要が生じる可能性がある。

[参考] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684136497194)等

© Hitachi, Ltd. 2024. All rights reserved.

3.2-3. NIS2指令 / 過失が生じた際の働きかけ (1/2)

HITACHI
Inspire the Next

- 主要エンティティ及び重要エンティティごとに監督上及び執行上の権限を定めており、その権限には差異がみられる。また、定められている罰金も対象ごとに金額が異なる。
- 重要エンティティと比較して、主要エンティティに対して強い働きかけを認めている。

分類		主要エンティティ	重要エンティティ
金銭的罰則を伴わない働きかけ	監督上の権限	(第32条) 2.加盟国は、所管官庁が、主要エンティティに関して監督上の任務を行使する場合、少なくとも当該主体を監督対象とする権限を有することを確保しなければならない (a) 訓練を受けた専門家による抜き打ち検査を含む、立入検査および立入禁止の監督； (b) 独立機関または所轄官庁による、定期的かつ的を絞ったセキュリティ監査； **(c) 重要なインシデントまたは必須事業体による本指令の侵害を理由に正当化される場合を含む、臨時の監査**； (d) 客観的、非差別的、公正かつ透明性のあるリスク評価基準に基づき、必要に応じて関係事業体の協力を得て、セキュリティ・スキャンを実施する； (e) 文書化されたサイバーセキュリティポリシーを含む、当該事業体が採用したサイバーセキュリティリスク管理措置を評価するために必要な情報の要求、および第27条に基づく管轄当局への情報提出義務の遵守； (f) 監督業務の遂行に必要なデータ、文書、情報へのアクセス要求； (g) 有資格の監査人によるセキュリティ監査の結果や、その根拠となる証拠など、サイバーセキュリティポリシーが実施されていることの証拠を求める。	(第33条) 2. 加盟国は、所管官庁が重要エンティティに関して監督上の任務を行使する場合、少なくとも当該事業体を監督対象とする権限を有することを確保しなければならない： (a) 訓練を受けた専門家による立入検査とオフサイトの事後監督； (b) 独立機関または所轄官庁が実施する、対象を絞ったセキュリティ監査； (c) 客観的、非差別的、公正かつ透明性のあるリスク評価基準に基づき、必要に応じて関係事業体の協力を得て、セキュリティ・スキャンを実施する； (d) 文書化されたサイバーセキュリティポリシーを含む、当該事業体が採用したサイバーセキュリティリスク管理措置を事後的に評価するために必要な情報の要求、および第27条に基づく管轄当局への情報提出義務の遵守； (e) 監督業務の遂行に必要なデータ、文書、情報へのアクセス要求； (f) 有資格の監査人によるセキュリティ監査の結果や、その根拠となる証拠など、サイバーセキュリティポリシーが実施されていることの証拠を求める

主要エンティティに対して、臨時の監査が認められている一方で、重要エンティティに対しては認められていない。

[参考] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684136497194)等

© Hitachi, Ltd. 2024. All rights reserved.

3.2-3. NIS2指令 / 過失が生じた際の働きかけ (2/2)

HITACHI
Inspire the Next

分類		主要エンティティ	重要エンティティ
金銭的罰則を伴わない働きかけ	執行上の権限	4. 加盟国は、所管官庁が必須事業体に関する執行権限を行使する際、少なくとも以下の権限を有することを確保しなければならない： (a) 関係団体による本指令の違反について警告を発する (b) インシデントの予防又は是正に必要な措置、当該措置の実施及びその実施に関する報告の期限を含む拘束力のある指示の採択、又は特定された欠陥若しくは本指令の違反の是正を当該事業体に求める命令の採択； (c) 本指令を侵害する行為を中止し、その行為を繰り返さないよう関係団体に命じる； (d) 当該事業体に対し、サイバーセキュリティリスク管理措置が第21条に準拠していること、または第23条に定める報告義務を所定の方法および期間内に履行することを命ずる； (e) 重大なサイバー脅威の影響を受ける可能性のあるサービスを提供または活動を行う自然人または法人に対し、脅威の性質、およびその脅威に対応して自然人または法人が取り得る保護措置または救済措置を通知するよう、関係主体に命じる； (f) セキュリティ監査の結果として提示された勧告を合理的な期限内に実施するよう、関係事業体に命じる **(g) 第21条および第23条を遵守する関係事業体を監督するため、定められた期間、明確な職務を持つ監視役員を指名する；** (h) 本指令の違反の側面を特定の方法で公表するよう関係団体に命じる； (i) 本項の(a)から(h)に掲げる措置に加え、国内法に従い、第34条に基づき、行政上の罰金を科すこと、又は関係機関、裁判所若しくは審判所により科すことを要求すること。	4. 加盟国は、管轄当局が重要な事業体に関して執行権限を行使する場合、少なくとも以下の権限を有することを確保しなければならない： (a) 関係団体による本指令の違反について警告を発する； (b) 特定された不備または本指令の侵害を是正するよう、関係団体に拘束力のある指示または命令を採択する； (c) 本指令を侵害する行為を中止し、その行為を繰り返さないよう関係団体に命じる； (d) 当該事業体に対し、サイバーセキュリティリスク管理措置が第21条に準拠していること、または第23条に定める報告義務を所定の方法および期間内に履行することを命ずる； (e) 重大なサイバー脅威の影響を受ける可能性のあるサービスを提供または活動を行う自然人または法人に対し、脅威の性質、およびその脅威に対応して自然人または法人が取り得る保護措置または救済措置を通知するよう、関係主体に命じる； (f) セキュリティ監査の結果として提示された勧告を合理的な期限内に実施するよう、関係事業体に命じる (g) 本指令の違反の側面を特定の方法で公表するよう関係団体に命じる； (h) 本項の(a)から(g)に掲げる措置に加え、国内法に従い、第34条に基づき、行政上の罰金を科すこと、又は関係機関、裁判所若しくは審判所により科すことを要求すること。
金銭的罰則を伴う働きかけ		4. 加盟国は、主要エンティティが第21条または第23条に違反した場合、本条第2項および第3項に従い、**少なくとも1万ユーロ**、または主要エンティティが属する事業体の前会計年度における**全世界の年間総売上高の少なくとも2%**のいずれか高い方を上限とする行政罰の対象となることを保証する。	5. 加盟国は、重要エンティティが第21条または第23条に違反した場合、本条第2項および第3項に従い、**少なくとも7,000,000ユーロ**または重要エンティティが属する事業体の前会計年度における全世界の年間総売上高**の少なくとも1.4%**のいずれか高い方を上限とする行政罰の対象となることを保証する

主要エンティティに対して監督役員を指名する権限が設けられている一方で、重要エンティティに対しては設けられていない。

主要エンティティの方が課されている罰金が高い。

© Hitachi, Ltd. 2024. All rights reserved.

3.2-4. 一般製品安全規則 / 概要

- 対象製品:EU 市場に出される、消費者のために意図された、あるいは消費者が使用しそうな製品
- 適用対象:製造者、承認代理人、輸入業者、流通業者、運送事業者等

項目		概要
適用製品(※)		• 高水準の消費者保護を与えながら EU内の市場の機能を改善することを目的に、EU 市場に出される、消費者のために意図された、あるいは消費者が使用しそうな製品 • この規則は関係するリスクが当該の製品の安全性を規制する他の EU 法(低電圧指令2014/35/EU や機械指令 2006/42/EC)の同一の目的の条項でカバーされない製品に適用される。
適用対象	製造業者	• 製造業者 (manufacturer) は、製品を製造し、あるいは設計や製造された製品を入手し、その製品をその者の名前や商標のもとで市場に出す任意の自然人や法人を意味する
	承認代理人	• 承認代理人 (authorised representative) は、この規則のもとでの製造業者 (§4.2) の義務に関わる指定された任務に関して製造業者の代理として振る舞うように製造業者からの書面による委任を受けた、EU 内に所在する任意の自然人や法人を意味する。
	輸入業者	• 輸入業者 (importer) は、第三国からの製品を EU市場に出す、EU 内に所在する任意の自然人や法人を意味する
	流通業者	• 流通業者 (distributor) は、製品を市場で入手可能とする、製造業者 (§4.2) と輸入業者 (§4.4) 以外の任意の自然人や法人を意味する。
	運送事業者	• 運送事業者(fulfilment serviceprovider) は、指令 97/67/EC † 13 の第 2 条 (1) 項で規定された郵便サービス、Regulation (EU) 2018/644 の第 2 条 (2) 項で規定された配達サービス、及びその他の任意の郵便サービスや貨物輸送サービスを除く、関係する製品の所有権を持たずに、保管、梱包、宛先の指定と発送のうち少なくとも 2 つのサービスを商業活動として提供する任意の自然人や法人を意味する。
	その他の自然人や法人	この規則のもとで製品の製造や上市に関係する義務を持つ任意のその他の自然人や法人

※除外製品が規定されている

[参考] REGULATION (EU) 2023/988 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2023.135.01.0001.01.ENG)
(株)e・オータマ「一般製品安全規則 Regulation (EU) 2023/988 の概要」(https://www.emc-ohtama.jp/emc/doc/gpsr-eu-2023-988-explained.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-4. 一般製品安全規則 / 具体的な要求

HITACHI
Inspire the Next

- 今回の改正によって、一般製品安全規則において、サイバーセキュリティの観点が新たに盛り込まれた。一方で、具体的なサイバーセキュリティの要件までは盛り込まれてない。

製品の安全性を評価するための側面

項目	概要
製品の安全性を評価するための側面(第6条)	• ここで言う「安全な製品 (safe products)」は、実際の使用期間を含む、通常の、あるいは合理的に予見可能な使用条件において、いかなるリスクも与えない、あるいは製品の使用と釣り合った受容可能かつ消費者の健康と安全の高水準の保護に合致するとみなされる最小限のリスクのみを与える任意の製品を意味する。**製品が安全かどうかの評価では、特に以下の側面を考慮する**: 1. その設計、技術的特徴、構成、梱包、組み立て、また該当する場合は設置、使用、及び保守の指示を含む、製品の特性; 2. その製品が他の製品と共に用いられることが合理的に予見可能な場合、それらの製品との接続を含む、他の製品の影響; 3. 他の製品がその製品と共に用いられることが合理的に予見可能な場合、評価対象の製品の安全性の評価で考慮しなければならない、評価対象の製品の働きを決定し、変更し、あるいは完成させるための組み込まれていない要素の影響を含む、他の製品が評価対象の製品に与えるかも知れない影響; 4. 製品の外観、子供の対象年齢に関するラベリングを含むラベリング、安全な使用と廃棄のための任意の警告や指示、また製品に関する任意のその他の表示や情報; 5. その製品を使用する消費者のカテゴリ ― 特に子供、老人、また障害者のような脆弱な消費者に対するリスク、また安全と健康への性差の影響の評価による; 6. それが消費者によるその製品が設計された目的と異なる形での使用をもたらしそうな場合、その製品の外観、特に: (a) 製品が、食品ではないが、その形態、匂い、色、外観、包装、ラベリング、体積、大きさ、あるいはその他の特徴のために食品に似ており食品と混同されそうな、従って消費者、特に子供が口に入れ、しゃぶり、あるいは飲み込むかも知れない場合; (b) 製品が、子供のために設計されたり意図されたりしたものではないが、子供が使用しそうな、あるいはその設計、包装、あるいは特徴から一般に子供への訴求性が認められる、あるいは子供による使用が意図された物体に似ている場合; **7. その製品の性質上必要な場合、そのような影響が相互接続の喪失の可能性を含む、製品の安全性に影響するかも知れないならば、悪意の第三者を含む外的な影響から製品を保護するために必要な適切なサイバー・セキュリティの特徴;** 8. その製品の性質上必要な場合、製品の進化、学習、及び予測機能。 • より高水準の安全性の達成の可能性やより低いリスクの製品の存在は製品が危険な製品であるとみなす根拠とはならない

今回の改正によって、一般製品安全規則において、サイバーセキュリティの観点が新たに盛り込まれた。一方で、具体的なサイバーセキュリティの要件までは盛り込まれてない。

[参考] REGULATION (EU) 2023/988 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2023.135.01.0001.01.ENG)
(株)e・オータマ「一般製品安全規則 Regulation (EU) 2023/988 の概要」(https://www.emc-ohtama.jp/emc/doc/gpsr-eu-2023-988-explained.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-4. 一般製品安全規則 / 過失が生じた場合の働きかけ

HITACHI
Inspire the Next

- 欧州委員会は、消費者の健康及び安全に重大な危険をもたらす製品等を発見した場合には、その製品をEU市場から排除する権限を持っている。

分類		概要
金銭的罰則を伴わない働きかけ	重大なリスクをもたらす製品に対する連合の行動(第28条)	欧州委員会は、消費者の健康及び安全に重大な危険をもたらす製品又は特定のカテゴリー若しくは製品群を発見した場合には、次の場合には、自らの発意又は加盟国の要請により、状況の重大性及び緊急性に適合した行為を実施することにより、適当な措置をとることができる。 (ア)リスクは、製品、カテゴリー、または製品グループによってもたらされる安全性の問題の性質を考慮して、事件の重大度または緊急度に適合する方法で、関連する製品に適用される特定の連合法によって定められた他の手順の下で対処することはできません。そして (イ)リスクは、消費者の健康と安全、および域内市場の適切な機能の一貫した高レベルの保護を確保するために、**EUレベルで適用可能な適切な措置を採用することによってのみ効果的な方法で排除することができます**。 これらの措置には、高レベルの消費者安全保護を確保するために、**そのような製品の市場投入または市場での入手可能化を禁止、一時停止、または制限する措置**、または該当する場合、**安全要件に関する適合性評価、またはそれらの製品の代表的なサンプルテストなどのマーケティングのための特別な条件を設ける措置**が含まれる場合があります。

消費者の健康及び安全に重大な危険をもたらす製品等を発見した場合には、その製品をEU市場から排除することができる。

[参考] REGULATION (EU) 2023/988 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2023.135.01.0001.01.ENG)
(株)e・オータマ「一般製品安全規則 Regulation (EU) 2023/988 の概要」(https://www.emc-ohtama.jp/emc/doc/gpsr-eu-2023-988-explained.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-5. EU無線機器指令 / 概要

- 対象製品:無線通信等に基づき、電波を意図的に放射、及び/もしくは受信する電気/電子製品
- 適用対象:製造者、承認代理人、輸入業者、流通業者

項目		概要
適用対象(※)		• 無線通信、及び/もしくは 電波の伝搬特性に基づく、物体の位置、速度、及び/もしくはその他の特性の同定、あるいはそれらのパラメータに関連する情報の取得の目的で電波を意図的に放射、及び/もしくは受信する電気/電子製品に適用される。
適用対象	製造業者	• 製造業者とは、機器の生産を行ない、あるいは設計/生産された機器を入手し、自らの名前や商標を付して市場に出す個人や法人のことを意味する。 • なお、市場に出された機器を、指令への適合に影響するかも知れないような形で改造する者も、製造業者とみなされる。
	承認代理人	• 承認代理人とは、EU 域内の個人や法人で、製造業者のために指令に関連する特定の業務を行なうように書面 (委任状) によって委任された者を意味する。
	輸入業者	• 輸入業者は、域外から EU 市場に機器を持ち込む、EU 域内の個人や法人を意味する。
	流通業者	• 流通業者は、サプライ・チェーン内の、製造業者と輸入業者を除く全ての個人や法人を意味する。

※除外製品が規定されている

[参考] (株)e・オータマ無線機器指令 2014/53/EU への適合のためのガイド (第6版)
(https://www.emc-ohtama.jp/emc/doc/radio-equipment-directive-guide-2014.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-5. EU無線機器指令 / 具体的な要求

HITACHI
Inspire the Next

- 今回の改正によって、必須要求にサイバーセキュリティの要素が新たに追加された。

必須要求

項目		概要
第3条(1)		• 無線機器は以下のことを確かとするように構成されていること: 1. Article 3(1)(a) — 低電圧指令 2014/35/EU の安全目標を含む、人と飼育動物の健康と安全の保護、及び財産の保護; 2. Article 3(1)(b) — EMC 指令 2014/30/EU で定められた、適切な水準の電磁両立性
第3条(2)		• 無線機器は、有害な干渉の防止のため、無線スペクトラムを有効に使用し、またその効率的な使用をサポートするように構成されていること
第3条(3)	A	• 無線機器はこの条項の第 4 項で別途規定される Annex Ia の Part I で規定されたカテゴ • リやクラスの無線機器のための充電デバイスを除く周辺機器と協調して動作すること
	B	• 通信網を介して他の無線機器と協調して動作すること
	C	• EU 全域で適切なタイプのインターフェースに接続できること
	D	• **通信網やその機能に害を与えず、また通信網の資源を濫用せず、サービスの受容できない低下を引き起こさないこと**
	E	• **ユーザーや加入者の個人情報やプライバシーの保護を確かとする防護手段を持つこと**
	F	• **詐欺行為の防止のための機能を備えること**
	G	• 緊急サービスへのアクセスのための機能を備えること
	H	• 障害を持つユーザーによる使用を可能とするための機能を備えること
	I	• 無線機器とソフトウェアの組み合わせの適合性が実証されたソフトウェアのみを無線機器にロードできることを確かとするための機能を備えること
第3条(4)		• Annex Ia の Part I で規定されたカテゴリやクラスに該当する無線機器はその Annex で該当するカテゴリやクラスの無線機器に対して設定された充電能力に関する仕様に適合するように構成されていること

今回の改正によって、必須要求にサイバーセキュリティの要素が新たに追加された。

[参考] (株)e・オータマ無線機器指令 2014/53/EU への適合のためのガイド (第6版)
(https://www.emc-ohtama.jp/emc/doc/radio-equipment-directive-guide-2014.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-5. EU無線機器指令 / 過失が生じた場合の働きかけ

- 事業者に対して、規則への不遵守を要求した上で、無線機器の市場展開を制限することが可能。
- なお、罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

分類	項目	概要
金銭的罰則を伴わない働きかけ	第43条 正式な違反	• 1 加盟国が次の各号のいずれかの認定をした場合には、第40条を損なうことなく、**当該事業者に対し、当該不遵守に終止符を打つことを要求**する。 (a)CEマーキングは、規則(EC)No 30/765の第2008条またはこの指令の第20条に違反して貼付されている。 (b)CEマーキングは貼付されていない。 (c)附属書IVに定められた適合性評価手順が適用される通知機関の識別番号が第20条に違反して貼付されているか、または貼付されていない。 (d)EU適合宣言は作成されていない。 (e)EU適合宣言が正しく作成されていない。 (f)技術文書が利用できないか、完全ではない。 (g)第10条(6)または第7条または第12条(3)で言及されている情報が存在しない、虚偽である、または不完全である。 (h)無線機器の使用目的に関する情報、第10条(8)、(9)、および(10)に規定されているEU適合宣言または使用制限は、無線機器に添付されていない。 (i)第15条に定められた経済主体の識別に関する要件が満たされていない。 (j)第5条は遵守されていない。 • 2 1に規定する**不適合が続く場合には、当該加盟国は、対応する無線機器が市場で入手可能であることを制限し若しくは禁止し、又は当該無線機器が市場から撤回若しくはリコールされることを確保するため、あらゆる適当な措置**をとる。
	第46条 罰則	• 加盟国は、この指令に従って採択された国内法の規定の経済事業者による侵害に適用される罰則に関する規則を定め、それらが**執行されることを確保するために必要なすべての措置を講じるものとする。**。このような規則には、**重大な違反に対する刑事罰が含まれる場合がある**。 • 規定された罰則は、効果的で、比例し、説得力のあるものでなければならない。

事業者に対して、規則への不遵守の是正を要求した上で、無線機器の市場展開を制限することが可能。

EU無線機器指令には罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

[参考] (株)e・オータマ無線機器指令 2014/53/EU への適合のためのガイド (第6版)
(https://www.emc-ohtama.jp/emc/doc/radio-equipment-directive-guide-2014.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-6. EU民間航空機規則 / 概要

- 対象製品:主に航空機を遠隔操作するための製品、部品/自然人または法人による、航空機を遠隔操作するための製品、部品および機器の設計および製造
- 適用対象:対象製品の設計、製造、保守、運用に携わる人員や組織

項目		概要
適用対象	第2条(スコープ)	1. 本規定は以下に適用される： (a)(b)に含まれない範囲で、当機関または加盟国の監督下にある**自然人または法人による、航空機を遠隔操作するための製品、部品**および機器の設計および製造； (b)**航空機、ならびにそのエンジン、プロペラ、部品、非搭載機器**、および航空機を遠隔操作するための機器の設計、製造、保守、および運用： (i)ただし、加盟国がシカゴ条約に基づく責任を第三国に移譲し、かつ、当該航空機が第三国の航空機運航者によって運航される場合はこの限りでない； (ii)第三国において登録され、かつ、条約が適用される領域内に設立され、居住し、又は主たる営業所を有する航空機運航者により運航されること；三加盟国でも第三国でも登録されておらず、条約が適用される領域内で、その領域内に設立され、居住し、または主たる事業所を有する航空機運航者により運航される無人航空機； (c)第三国の航空機運航者により、条約が適用される領域内への、領域内での、または領域外への航空機の運航； (d)(e)に掲げる飛行場において使用され、又は使用することを目的とする安全関連飛行場設備の設計、製造、整備及び運用並びにこれらの飛行場における地上取扱業務及びAMSの提供； (e)条約が適用される領域内にある飛行場の設計、維持及び運用(これらの飛行場で使用される安全関連設備を含む (i)公共の用に供されていること； (ii)商業航空輸送に供されるものであること。 (iii)800メートル以上の舗装された計器用滑走路を有するか、またはヘリコプターのみに使用されること (f)環境および土地利用計画に関する連邦法および国内法を害することなく、(e)の飛行場の周辺環境を保護すること (g)単一欧州空（Single European Sky）空域におけるATM/ANSの提供、および、これらのATM/ANSの提供に使用されるシステムおよび構成要素の設計、製造、保守および運用； (h)欧州議会および理事会規則(EC) No 551/2004(32)および加盟国の管轄空域に関する責任を損なうことなく、単一欧州空空域における空域構造の設計。
適用対象	第2条(スコープ)	2. 本規定は、第1項の活動に携わる人員および組織にも適用される。

[参考] REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1139)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-6. EU民間航空機規則 / 具体的な要求

HITACHI
Inspire the Next

- 民間航空機規則では、各対象に対する必須要件の中にセキュリティに係る要件が盛り込まれている。

項目	必須要件
セクション1 耐空性および環境保護	• 附属書Ⅱ[耐空性に関する必須要件]、附属書Ⅲ[製品に関する環境適合性の必須要件]
セクション2 航空機乗務員	• 附属書Ⅳ[航空機乗務員の必須要件]
セクション3 航空機運航	• 附属書Ⅶ[飛行場の必須要件]、附属書Ⅷ[AT/ANおよび航空管制官の必須要件]
セクション4 飛行場	• 附属書Ⅶ[飛行場の必須要件]、附属書Ⅷ[AT/ANおよび航空管制官の必須要件]
セクション5 大気／水蒸気	• 附属書Ⅶ[飛行場の必須要件]、附属書Ⅷ[AT/ANおよび航空管制官の必須要件]
セクション6 航空管制官	• 附属書Ⅷ[AT/ANおよび航空管制官の必須要件]
セクション7 無人航空機	• 附属書Ⅸ[無人航空機の必須要件]、(場合によっては附属書Ⅱ[耐空性に関する必須要件]、附属書Ⅳ[航空機乗務員の必須要件]、附属書Ⅴ[航空業務の必須])
セクション8 第三国の運航会社が域内、域外へ、または域外から使用する航空機	• 無人航空機以外の航空機:附属書Ⅱ[耐空性に関する必須要件]、Ⅳ[航空機乗務員の必須要件]、Ⅴ[航空業務の必須] • 無人航空機の航空機:附属Ⅸ[無人航空機の必須要件](場合によっては附属書Ⅱ[耐空性に関する必須要件]、Ⅳ[航空機乗務員の必須要件]、Ⅴ[航空業務の必須])

セキュリティに関連する記載(例)

1. 製品の完全性**(附属書Ⅱ)**
情報セキュリティ上の脅威からの保護を含む製品の完全性は、航空機の運用期間中、予測されるすべての飛行条件に対して保証されなければならない。すべての要求事項への適合は、評価または分析によって示されなければならず、必要な場合には試験によって裏付けられなければならない。

1.3.5. **情報セキュリティ上の脅威**を含む、航空機の内部および外部の合理的に起こりうる脅威による航空機および乗員への危険を最小限に抑えるための設計上の予防措置を講じなければならない

3.3. システムおよびコンポーネントの設計**(附属書Ⅷ)**
3.3.1. システムおよび構成要素は、適用される安全および**セキュリティ要件を満たすように設計されなければならない**。

1. 無人航空機の設計、製造、保守、運用に必要な要件**(附属書Ⅸ)**
1.3. 運航から生じる**安全、プライバシー、個人情報保護、セキュリティまたは環境に関するリスクを軽減するために必要な場合、**無人航空機は、設計上および既定上、プライバシーおよび個人情報保護の原則を考慮した、対応する特定の特徴および機能を備えていなければならない。・・・

[参考] REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1139)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-6. EU民間航空機規則 / 過失が生じた場合の働きかけ

- 注意喚起を行うとともに、立入調査や監視活動の権限を認めている。一方で、航空免許のはく奪等までは言及されていない。
- 本規則には、罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

分類	項目	概要
金銭的罰則を伴わない働きかけ	第62条 認証、監督、執行	1. 欧州委員会、航空局、および加盟国は、単一の欧州航空安全システムの中で協力し、本規則およびこれに基づいて採択された委任法および実施法の遵守を確保するものとする。 2. 本規則及びこれに基づいて採択された委任法及び実施法の遵守を確保するため、本庁及び各国主管庁は、以下を行うものとする： (a) 第III章に従い、申請書を受理し、審査し、該当する場合には、証明書を発行または更新し、宣誓書を受理する； (b) 証明書の保有者、申告を行った自然人および法人、ならびに本規則の対象となる製品、部品、機器、ATM/ANSシステムおよびATM/ANS構成部品、飛行シミュレーション訓練装置、飛行場に対する監督を行う； (c) **本規則の対象となる法人または自然人による、本規則およびそれに基づいて採択された委任法および実施法に規定された要求事項への違反の可能性を特定するために、必要な調査、検査（立ち入り検査を含む）、監査およびその他の監視活動を実施すること**； (d) 特定された違反行為を排除するため、発行された証明書の修正、制限、一時停止、取り消し、航空機の接地、罰則の賦課など、必要なあらゆる強制措置を講じること； (e) 安全のため、第III章で言及されている活動を禁止、制限、または一定の条件付きとする； (f) 適切な研修を提供することを含め、認証、監督、実施業務に携わるスタッフの適切なレベルの資格を確保すること。(中略) • 本規則の対象となる法人または自然人は、加盟国間の**規則の適用における相違の疑いがある場合、弊庁の注意を喚起することができる。**当該相違が当該者の活動を著しく妨げ、またはその他の実質的な困難につながる場合、弊庁および関係する加盟国の国家主管庁は、当該相違に対処し、必要な場合には速やかに当該相違を解消するために協力しなければならない。このような相違を解消できない場合、弊庁は、この問題を欧州委員会に提示するものとする。
	第131条 罰則	• 加盟国は、この規則およびこれに基づいて採択された委任法および実施法の違反に適用される**罰則に関する規則を定め**、その実施を確保するために必要なすべての措置を講じるものとする。規定される罰則は、効果的、比例的かつ説得力のあるものでなければならない。

立入調査や監視活動の権限を認めている。

民間航空機規則には罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

[参考] REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1139)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-7. EU自動車型式承認規則 / 概要

- 対象製品:車両、及び車両用に設計・製造されたシステム、コンポーネント、個別の技術ユニット
- 適用対象:上記製品の製造事業者

項目		概要
適用対象		• 規則(EU)2018/858の第4条に定義されるカテゴリーM、N、Oの車両、及び車両用に設計・製造されたシステム、コンポーネント、個別の技術ユニット <参考>規則（EU）2018/858の第4条に定義されるカテゴリーM、N、O ✓ カテゴリM:主に旅客とその荷物の運送を目的として設計・製造された自動車 ✓ カテゴリN:主に貨物輸送用に設計・製造された自動車 ✓ カテゴリO:トレーラー
適用対象	製造事業者	(本規則内で明確に定義されていないものの、上記車両やシステム等を製造する事業者と考えられる)

なお、自動車の型式承認規則は、以下の要件を定めるものであり、罰則等の記載はなされていない。
(a) 車両、並びに車両用に設計及び製造されたシステム、構成部品及び個別の技術ユニットの一般的特性及び安全性、並びに車両乗員及び交通弱者の保護及び安全性に関すること
(b) タイヤ空気圧監視システムについて、その安全性や燃費、CO2排出量に関すること
(c) 新しく製造されるタイヤの安全性と環境性能に関すること

[参考] REGULATION (EU) 2018/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0858)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-7. EU自動車型式承認規則 / 具体的な要求

- 自動車の型式承認規則では、セキュリティに係る具体的な要求は記載されていない。一方で、前文には、サイバーセキュリティに関する国連規則等を発行後速やかに適用させるべきとの記載がある。

セキュリティに係る要求の関連記載

項目	記載内容
前文(26)	• 自動車のコネクティビティと自動化は、車載データへの無許可のリモートアクセスや、無線によるソフトウェアの違法改造の可能性を増大させる。**このようなリスクを考慮するため、サイバーセキュリティに関する国連規則またはその他の規制法は、発効後できるだけ速やかに強制的に適用されるべきである。**
前文(27)	• ソフトウェアの変更は、車両の機能を大幅に変更する可能性がある。ソフトウェアの変更に関する調和された規則および技術要件は、型式承認手続きに沿って確立されるべきである。したがって、**ソフトウェア更新プロセスに関する国連規則またはその他の規制法は、発効後できるだけ速やかに強制的に適用されるべきである。**ただし、こうしたセキュリティ対策は、車両の修理・整備に関連する包括的な診断情報および車載データへのアクセスを提供するという自動車メーカーの義務を損なうものであってはならない。

[参考] REGULATION (EU) 2018/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0858)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-8. EU機械規則 / 概要

- 対象製品:機関及び関連製品
- 適用対象:製造事業者、公認代理人、輸入業者、販売事業者

項目		概要
適用対象	機械及び関連製品(※)	• 本規則は、機械および以下の関連製品に適用される。 (a) 交換可能な機器 (b) 安全部品 (c) リフティング・アクセサリー (d) チェーン、ロープ、ウェビング (e) 取り外し可能な機械式変速装置 • この規則は、部分的に完成した機械にも適用される。
適用対象	製造業者	• 「製造業者」とは、自然人または法人を指す。 (a) 本規則の適用範囲内の製品を製造し、またはそれらの製品を設計もしくは製造させ、それらの製品を自己の名称もしくは商標の下で販売する者。 (b) は、本規則の適用範囲内の製品を製造し、その製品を自社で使用するために使用する。
	公認代理人	• 特定業務に関して製造業者からその代理を務めるよう書面による委任を受けた、EU域内に設立された自然人または法人を意味する
	輸入業者	• 第三国からこの規則の適用範囲内の製品を域内市場に出す 、域内に設立された自然人または法人を意味する
	販売事業者	• サプライチェーンの中で、製造業者または輸入業者以外の自然人または法人で、本規則の範囲内の製品を市場で入手できるようにする者をいう
セキュリティに係る要求の関連記載		• 規則（EU）2019/881 に従って採択されたサイバーセキュリティ認証制度に基づき認証され、又は適合性宣言書が発行された機械及び関連製品は、**サイバーセキュリティ認証書又は適合性宣言書又はその一部によってこれらの要求事項がカバーされている限りにおいて、腐敗に対する保護及び制御システムの安全性及び信頼性に関して、附属書Ⅲの 1.1.9 及び 1.2.1 項に規定された本質的な安全衛生要求事項に適合しているものと推定**される。

※除外製品が規定されている

[参考] REGULATION (EU) 2023/1230 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/eli/reg/2023/1230/oj)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-8. EU機械規則 / 罰則

- 事業者に対して、規則への不遵守を要求した上で、機械及び関連製品の市場展開を制限することが可能。
- なお、罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

分類	項目	概要
金銭的罰則を伴わない働きかけ	第45条 本規制の適用範囲内で、リスクをもたらす適合製品	第43条(1)に基づく評価を実施した結果、加盟国は、本規則の適用範囲内の製品が附属書IIIに定める安全衛生に関する必須要件に適合しているにもかかわらず、人及び適切な場合には家畜の健康及び安全、又は財産に対するリスク、並びに該当する場合には環境に対するリスクをもたらすと認める場合には、**関連する経済事業者に対し、以下のすべての適切な措置を講じるよう求めるものとする。当該製品が上市された時点で、もはやそのリスクを示さないことを確実にし、リスクの性質に見合った合理的な期間内に、その製品を撤去し、または回収する**こと。 2. 経済事業者は、本規則の適用範囲内にある、当該経済事業者が域内全域で市販しているすべての製品について、すべての適切な是正措置が取られることを保証しなければならない。
	第46条 正式なコンプライアンス違反	1. 第43条を損なうことなく、加盟国が**機械又は関連製品に関して**所見を行った場合、当該経済事業者に対し、**当該不遵守を解消するよう求めるものとする**： 2. 第43条を損なうことなく、加盟国は、**部分的に完成した機械に関して**所見を行った場合、当該経済事業者に対し、**当該不適合を解消するよう求めるものとする**： 3. 第1項および第2項の不遵守が継続する場合、当該加盟国は、当該規則の適用範囲内の製品が市場で**入手可能となることを制限もしくは禁止し、または当該製品が市場から回収もしくは撤回されることを確保するためのあらゆる適切な措置**を講じるものとする。
	第50条 罰則	1. 加盟国は、経済事業者が本規則に違反した場合に適用される罰則に関する規則を定め、その履行を確保するために必要なあらゆる措置を講じるものとする。規定される罰則は、効果的、比例的、かつ抑制的でなければならず、**重大な違反に対しては刑事罰を含むことができる**。

事業者に対して、規則への不遵守の是正を要求した上で、機械及び関連製品の市場展開を制限することが可能。

機械規則には罰金規定は定められてないないが、加盟国によって設けられる可能性がある点に留意。

[参考] REGULATION (EU) 2023/1230 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
(https://eur-lex.europa.eu/eli/reg/2023/1230/oj)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-9. EU製造物責任指令案 / 概要

- 対象製品:電気、デジタル製造ファイル、ソフトウェアを含む全ての動産を意味する。
- 適用対象:経済事業者(製造者、関連サービスの提供者、代理店、輸入業者、フルフィルメントサービス提供事業者、販売事業者を含む)

項目		概要
適用対象	製品(第2条)	• 発効後12カ月以降に上市または使用開始される製品に適用される。ここで言う製品とは、すべての動産を意味し、他の動産または不動物と一体化している場合も含む。**製品には、電気、デジタル製造ファイル、ソフトウェアが含まれる。(前文12には機器に組み込まれたものに加えて、ソフトウェア単体が含まれる旨が記載されている)**
適用対象	経済事業者(第1条、第6条)	• 経済事業者は、以下を指す。 ✓ 製造者(製品を開発、製造もしくは生産する者、または製品を設計もしくは製造させる者、またはその製品を自己の名称もしくは商標の下で販売する者、または自己使用のために製品を開発、製造もしくは生産する自然人もしくは法人を意味する) ✓ 関連サービスの提供者 ✓ 代理店(特定業務に関して製造業者からその代理を務めるよう書面による委任を受けた、EU域内に設立された自然人または法人を意味する) ✓ 輸入業者(第三国からの製品を域内市場に流通させる 、域内に設立された自然人または法人を意味する) ✓ フルフィルメントサービス提供事業者(商業活動の過程において、以下のサービス(※)のうち少なくとも2つを提供する自然人又は法人を意味する) ※製品の所有権を持たずに、製品の倉庫保管、梱包、宛名書き、発送を行うこと。 ✓ 販売事業者(商業活動の過程において、以下のサービスのうち少なくとも2つを提供する自然人又は法人を意味する)

製造物責任指令案は以下を定めるものであり、罰則等の記載はなされていない。

第1章　一般規定
第2章　欠陥製品責任に関する具体的規定
第3章　責任に関する一般規定
第4章　最終規定

[参考] COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products (https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-9. EU製造物責任指令案 / 具体的な要求

- 欠陥製品の製造者が責任を負う旨を定めている製造物責任指令案では、免責事項が定められている一方で、必要なソフトウェアのアップデートやアップグレードが行われていない場合はその責任は免除されない。

経済事業者の責任

- 製造物責任指令案では、欠陥製品の製造者が責任を負う旨を定めている。

項目	内容
第7条1項	• 加盟国は、**欠陥製品の製造者が、その製品に起因する損害について責任を負うことができるようにしなければならない**。
	• 加盟国は、欠陥部品が製品の欠陥の原因となった場合、**欠陥部品の製造者も同様の損害賠償責任を負うことができるようにしなければならない**。

免責事項

- 製品が市場に投入された時点で瑕疵が存在しなかった場合には、免責される一方で、アップデートが可能なソフトウェアはその限りではない。

項目	内容
第10条1項 [抜粋]	• 第7条の経済事業者は、以下のいずれかを証明する場合、欠陥製品によって生じた損害について責任を負わない。 (c) 損害の原因となった瑕疵が、製品が市場に投入された時点、使用開始された時点、または販売業者に関して市場で入手可能になった時点には存在しなかったか、またはその瑕疵がその時点以降に存在するようになった可能性が高いこと
第10条1項	第1項の(c)の免除により、**経済事業者は、製品の欠陥が以下のいずれかに起因する場合であっても、それが製造者の管理範囲内である限り、責任を免除されない**： (a) 関連サービス； (b)ソフトウェア(アップデートまたはアップグレードを含む) (c) 安全性を維持するために**必要なソフトウェアのアップデートやアップグレードが行われていないこと**。

製造物責任指令改訂の具体的な各目的に関する利害関係者の意見の要約を以下に示す。(抜粋)

- **サイバーセキュリティの脆弱性有する製品は欠陥品とみなされる可能性があるという点については、すべての利害関係者グループの間で幅広いコンセンサスが得られた**。公開協議の回答者の70%は、そのような**脆弱性に対処するために必要なソフトウェア・セキュリティ・アップデートを提供しなかった製造業者に責任を負わせる可能性に賛成した**。

製造物責任指令案の覚書

[参考] COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products (https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-9. 製造物責任指令案 / 罰則

HITACHI
Inspire the Next

- 適切な対応をしないと、AIシステムの市場からの取下げやリコールなどの是正措置を公的な機関から義務付けられる可能性がある。
- また、違反した場合には上記と併せて巨額の制裁金が課され得るが、金額は違反の程度によって異なる。

分類		主要エンティティ
金銭的罰則を伴わない働きかけ	正式な不遵守(68条)	1. EU 加盟国の市場監視機関は、次に掲げるいずれかを発見した場合には、関係する提供者に、関係する不遵守を終わらせるよう要求するものとする。 （a） 適合性マーキングが、第 49 条に違反して付されていること。 （b） 適合性マーキングが付されていないこと。 （c） EU 適合宣言書が作成されていないこと。 （d） EU 適合宣言書が正しく作成されていないこと。 （e） 適合性評価手続に含まれる第三者認証機関の識別番号が付されるべき場合において、付されていないこと。 2. 第 1 項に定める不遵守が持続する場合には、関係する EU 加盟国は、ハイリスク AI システムが市場において利用できるようにされることを**制約し若しくは禁止するために適切な全ての措置を講じ**、又はハイリスク AI システムが市場からリコールされ若しくは取り下げられることを確保するものとする。 適切な対応をしないと、AIシステムの市場からの取下げやリコールなどの是正措置を公的な機関から義務付けられる可能性がある
金銭的罰則を伴う働きかけ	制裁(71条)	• 次の違反の場合には、**3,000万ユーロ**以下の行政上の制裁金に服するものとし、又は違反者が会社である場合には、前会計年度の**世界全体における売上総額の6%以下の金額**のうち、いずれか高い金額の行政上の制裁金に服するものとする。 （a） 第5条に規定する人工知能の実務の禁止の不遵守 （b） 第10条に規定する要件の AI システムによる不遵守 • 第5条及び第10条に規定する要件又は義務を除く本規則に規定する要件又は義務を AI システムが遵守しなかった場合には、**2,000万ユーロ**以下の行政上の制裁金に服するものとし、又は違反者が会社である場合には、前会計年度の**世界全体における売上総額の4%以下の金額**のうち、いずれか高い金額の行政上の制裁金に服するものとする • 要請に対し、不正確な、不完全な又は誤解を招く情報を第三者認証機関及び加盟国所管機関に提供した場合には、**1,000万ユーロ**以下の行政上の制裁金に服するものとし、又は違反者が会社である場合には、前会計年度の**世界全体における売上総額の2%以下の金額**のうち、いずれか高い金額の行政上の制裁金に服するものとする

違反した場合には上記と併せて巨額の制裁金が課され得るが、金額は違反の程度によって異なる。

[参考] 総務省「人工知能に関する調和の取れたルールを定める規則の提案」
(https://www.soumu.go.jp/main_content/000826706.pdf)
総務省「EUのAI規則案の概要」(https://www.soumu.go.jp/main_content/000842190.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-10. EU AI規則案 / 概要

- 対象製品:要件を満たすAIシステム
- 適用対象:AIシステムに係るサービスの提供者、AIシステムの利用者、EU域内で利用されるアウトプットに係るAIシステムの提供者及び利用者

項目		概要
適用対象	AIシステム	• 以下の二つの要件を満たすもの 1. 付属書Iの技法及びアプローチで開発されたソフトウェア ✓ 「ディープラーニングを含む様々な方法を用いた機械学習によるアプローチ」 ✓ 「知識表現、帰納（論理）プログラミングを含む論理ベース及び知識ベースのアプローチ」 ✓ 「統計的アプローチ」など 2. 人間が定めた一定の一連の目的のために、当該ソフトウェアが相互作用する環境に影響を与えるコンテンツ、予測、推奨又は決定などのアウトプットを生成することができるもの
適用対象	AIシステムに係るサービスの提供者	• 設立されたのが EU 域内であるか第三国であるかにかかわらず、EU において **AI システムを市場に置き又はサービスを提供する提供者**
	AIシステムの利用者	• EU 域内に所在する **AI システムの利用者**
	EU域内で利用されるアウトプットに係るAIシステムの提供者及び利用者	• AIシステムが生み出すアウトプットが EU域内で利用される場合における、**第三国に所在する当該システムの提供者及び利用者**

[参考] 総務省「人工知能に関する調和の取れたルールを定める規則の提案」(https://www.soumu.go.jp/main_content/000826706.pdf)
総務省「EUのAI規則案の概要」(https://www.soumu.go.jp/main_content/000842190.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

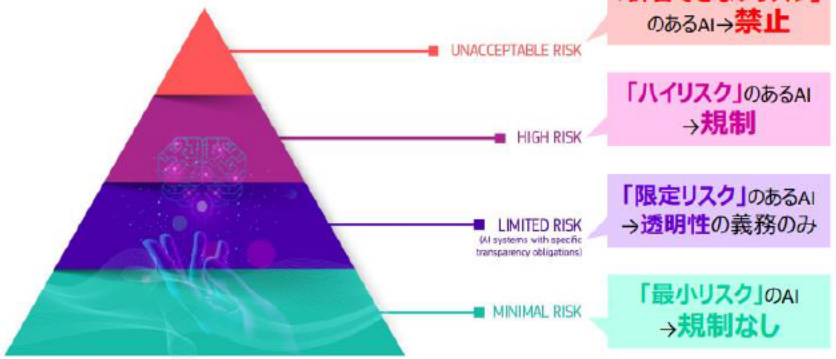
3.2-10. EU AI規則案 / 具体的な要求

HITACHI
Inspire the Next

- AIシステムを以下の４つの分類した上で、各システムに対して規制を課した上で、「ハイリスク」のあるAIに対して、セキュリティに係る要件を課している。

リスクに応じた規制

- AIシステムを以下の４つの分類した上で、各システムに対して規制を実施している。



「ハイリスク」のあるAIに対してセキュリティに係る要求がなされている。

ハイリスクのある規制

- リスクが2番目に高い「ハイリスク」のあるAIに係る規制として、ハイリスクAIシステムの要件と提供者等の義務が課されている。

項目	概要 ※条文にセキュリティの記載があるものに下線
ハイリスクAIシステムの要件（第III編第2章）	• リスクマネジメントシステム • **データとデータガバナンス** • 技術文書の要件 • 記録の保持 • **透明性・情報提供** • 人間による監視 • **正確性、頑健性及びサイバーセキュリティ**
提供者等の義務（第III編第3章）	• 品質管理システム • 適合性評価を受ける義務 • 自動生成ログの維持義務 • 是正措置・情報提供義務 • EU代理人選任義務 など • 販売者、輸入者、利用者 • その他の第三者にも一定の義務あり

[出典] 総務省「人工知能に関する調和の取れたルールを定める規則の提案」(https://www.soumu.go.jp/main_content/000826706.pdf)
総務省「EUのAI規則案の概要」(https://www.soumu.go.jp/main_content/000842190.pdf)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-11. 英国サイバーレジリエンス向上法案 / 提案内容 (1/2)

HITACHI
Inspire the Next

- 英国でも従来効力のあった欧州NIS指令の対象を拡大し、デジタルマネージドサービスのプロバイダに対する義務を課すとともにデジタルサービスプロバイダに対して監督制度を設けることを提案している。

提案内容	提案内容	根拠
1. デジタルサービスプロバイダーの規制の拡大	NIS規則の下で規制されているデジタルサービスの範囲を「マネージドサービス」に拡大し、デジタルマネージドサービスのプロバイダーが他のデジタルサービスプロバイダーと同じ義務を負うこと。	DCMSのサプライチェーン・サイバーセキュリティに関する意見募集(2021年5月)への回答者は、マネージド・サービスへの依存が企業の攻撃対象領域を必然的に拡大することを強調したため。また、回答者は、最も重要なマネージド・サービス・プロバイダーは、英国市場におけるサービスの規模と集中により、英国経済と社会にとってシステミック・リスクとなり得ると指摘している。このようなリスクがあるにもかかわらず、現在、英国市場のマネージド・サービス・プロバイダーに対するサイバーセキュリティに特化した強制的な要件はほとんどない。
2. デジタルサービスプロバイダーの監督体制	政府は、NISの対象となるデジタル・サービス・プロバイダーに対し、2段階の監督制度を設けることを提案している。これには、最も重要なデジタルサービスに対する事前監督体制と、NISで規制される残りのデジタルサービスに対する事後監督体制が含まれる。	最近の著名なサイバー攻撃は、外部プロバイダー、ひいてはそのプロバイダーが提供するデジタルサービスの脆弱性を通じて、英国の組織に脅威がますます及んでいることを示している。デジタル・サービス・プロバイダーが大規模かつ複数のセクターにまたがる組織にサービスを提供している場合、その脆弱性は英国の国家安全保障と経済的繁栄にとってかなりの脅威となるため。

[参考] GOV.UK" Proposal for legislation to improve the UK's cyber resilience"
(https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#annex-a-examples-of-managed-services)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-11. 英国サイバーレジリエンス向上法案 / 提案内容 (2/2)

HITACHI
Inspire the Next

- 監督下に置くための判断要因を設定した上で、積極的な(事前の)監督が新たに提案された。
- 指定されたデジタルサービスプロバイダは情報コミッショナー事務局(ICO)(※1)が要求する場合、セキュリティ対策に関する情報提供を行う義務が生じた。

	積極的な(事前の)監督 (proactive (ex-ante) supervisory	反応的な(事後の)監督 (reactive (ex-post)supervisory
対象	• 英国の回復力にとって重要であり、ICOによって決定されたデジタルサービスプロバイダ。以下の要因によって指定される。 A. マーケットリーチ B. 提供されるサービスの規模 C. 財務および/または収益 D. 市場における集中度 E. 供給する顧客の重要性 F. 顧客のサービスへの依存度 G. 顧客のネットワークへの接続性とアクセスのレベル H. インシデントがサービスに影響を及ぼした場合、国家安全保障にどのような影響を及ぼすか。	• 左記以外のデジタルサービスプロバイダ
要求事項 (※2)	• サイバーセキュリティインシデントが発生する前に、ICOの求めに応じて実施するセキュリティ対策について情報提供を行う。 • サイバーセキュリティインシデントが発生後に、ICOへ報告する。	• サイバーセキュリティインシデントが発生後に、事後的にICOへ報告する。

• NIS指令で定められていなかった、デジタルサービスプロバイダに対する事前の監督が新たに提案された。

※1:1984年に、データ保護法(DPA)およびプライバシーおよび電子通信に関する規則(PECR)に基づく監督機関としてICOが設置された。非政府部門公共機構として政府からは独立の権限を有するが、予算上はDCMSが後援官庁となる。
※2:NIS指令の要求事項は別頁「NIS指令」を参照されたい。

[参考] GOV.UK" Proposal for legislation to improve the UK's cyber resilience"
(https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#annex-a-examples-of-managed-services)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-11. 英国サイバーレジリエンス向上法案 / パブリックコメント結果

- 一部分類や考慮事項について修正指摘があったものの、パブリックコメントにおいて、提案に対して概ね賛成意見が寄せられた。

提案内容	フィードバック
1. デジタルサービスプロバイダーの規制の拡大	• デジタル・サービス・プロバイダーの規制拡大に関する措置については84%の賛成。 • 改善すべき点も指摘された。政府は特徴をさらに絞り込み、対象となる組織の種類をより明確にすべきであるとの指摘があった。政府はこの点を考慮し、特性と事例を修正し、小規模・零細企業に関する位置づけをさらに明確にした。
2. デジタルサービスプロバイダーの監督体制	• デジタル・サービス・プロバイダーの監督制度の改正に関する措置については79%の賛成。 • ある組織が事後的ではなく、積極的な監視の対象とされるべきかどうかを検討する際に考慮すべき要因の一部(すなわち、規模、財務内容、市場への到達度、市場集中度)について、修正が必要であるというものであった。すなわち、可能であれば主に非立法的な手段でこの措置を継続すること、情報コミッショナーからデジタル・サービス・プロバイダーへのさらなるガイダンスが予定されていること、などである。

[参考] GOV.UK" Proposal for legislation to improve the UK's cyber resilience" (https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#annex-a-examples-of-managed-services)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-12. 中国重要情報インフラセキュリティ保護条例 / 概要

HITACHI
Inspire the Next

- 中国における重要インフラセキュリティ保護条例では、重要情報インフラ運営者に加えて、重要情報インフラセキュリティ運営者にシステムを納入するITベンダが間接的に対象となり得る。

概要

項目	内容
制度の目的	• 重要情報インフラのセキュリティを保障し、ネットワークのセキュリティを維持
時期	• 2021年9月施行
対象組織	• 重要情報インフラ運営者 (重要情報インフラとは公共通信と情報サービス、エネルギー、交通、水利、金融、公共サービス、電子行政サービス、国防科学技術工業等の重要な業種と分野のほか、一旦破壊或いは、機能を喪失又は、データが漏れることがあれば、国家安全、国家経済と人民生活、公共利益に深刻な危害を及ぼす可能性のある重要なネットワーク施設、情報システム等)

ITベンダへの適用状況

分類		事業者(例)
パターン1	重要情報インフラセキュリティ保護条例	重要情報インフラ運営者(ユーザ)
パターン2	重要情報インフラセキュリティ保護条例の対象外 (ただし、間接的に関わり得る)	重要情報インフラ運営者にシステムを提供するITベンダ

[参考] 松田健輔事務所" 210730_重要情報インフラセキュリティ保護条例(日本語試訳)"
(https://matsuda.ne.jp/210730_jp_gwy745/)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-12. 中国重要情報インフラセキュリティ保護条例 / 詳細

HITACHI
Inspire the Next

- ユーザに対する責任義務が、実質的にベンダに対する義務となっている可能性がある。具体的にはユーザに納入しているITシステムに係る義務はベンダの実質的な義務になり得る。

運営者責任義務(例)

項目	規定内容	パターン1(ユーザへの影響)	[想定]パターン2(ベンダへの影響)
第十四条	• 運営者は専門的なセキュリティ管理機構を設置し、専門セキュリティ管理機構の責任者と重要職位の人員に対してセキュリティ背景審査を行わなければならない。	• セキュリティ管理機構の設置 • 責任者と重要職位の人員に対してセキュリティ背景審査	• -
第十七条	• 運営者は自らまたはネットワークセキュリティサービス機構に委託して、重要な情報インフラに対して毎年少なくとも一回のネットワークセキュリティ検査とリスク評価を行い、発見されたセキュリティ問題に対して適時に改善し、保護業務部門の要求に従って状況を報告しなければならない。	• 年一回のネットワークセキュリティ検査とリスク評価を実施 • システムに関連する問題についてITベンダへの改善指示、それ以外の問題は適時改善 • 上記改善状況の報告	• ユーザと協力し、セキュリティ検査とリスク評価を実施 • 評価結果を踏まえたシステム更新及びユーザに対する結果の報告
第十八条	• 重要情報インフラに重大なネットワークセキュリティインシデントが発生した場合、または重大なネットワークセキュリティの脅威が発見された場合、運営者は関連規定に基づいて保護業務部門、公安機関に報告しなければならない。	• 関連部局に対するネットワークセキュリティインシデント及びネットワークセキュリティの脅威の報告 • ユーザに対するネットワークセキュリティの常時監視、脆弱性管理等の指示	• ネットワークセキュリティの常時監視、脆弱性管理等の実施 • ユーザに対するネットワークセキュリティインシデント及びネットワークセキュリティの脅威の報告

[参考] 松田健輔事務所" 210730_重要情報インフラセキュリティ保護条例(日本語試訳)"
(https://matsuda.ne.jp/210730_jp_gwy745/)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-13. 製造物責任法 (日本) (1/2)

HITACHI
Inspire the Next

- 日本の製造物責任法において、ソフトウェアは対象に含まれていない。ただし、ソフトウェアを組み込んだ製造物においてはその対象に含まれる場合がある。

項目	概要
適用対象	• この法律では、製造物を「製造又は加工された動産」と定義しています(本法第2条第1項)。人為的な操作や処理が加えられ、引き渡された動産を対象としており、このため、不動産、電気、ソフトウェア、未加工農林畜水産物などは、この法律の対象にはならない。 • 製造物の要件は以下の通り。 ✓ 有体物であること ✓ 動産であること ✓ 製造又は加工された動産であること • なお、ソフトウェア自体は無体物であり、この法律の対象とはならない。ただし、ソフトウェアを組み込んだ製造物についてはこの法律の対象と解される場合がある。ソフトウェアの不具合が原因で、ソフトウェアを組み込んだ製造物による事故が発生した場合、ソフトウェアの不具合がその製造物自体の欠陥と解されることがあり、この場合、その欠陥と損害との間に因果関係が認められるときには、その製造物の製造業者等にこの法律による損害賠償責任が生じる。
対象者	• 製造事業者 なお、販売業者は、基本的にはこの法律の対象とならない。(ただし、販売業者であっても、輸入業者や表示製造業者に当たる場合は、その観点から製造物責任を負う対象となる。
欠陥の定義	• この法律でいう「欠陥」とは、製造物に関する様々な事情を総合的に考慮して、「製造物が通常有すべき安全性を欠いていること」をいう。(本法第2条第2項)。このため、安全性に関わらないような単なる品質上の不具合は、この法律の損害賠償責任の根拠とされる「欠陥」には当たらない。

[参考] 消費者庁「製造物責任(PL)法の逐条解説」
(https://www.caa.go.jp/policies/policy/consumer_safety/other/product_liability_act_annotations/)
消費者庁"製造物責任法の概要Q&A
(https://www.caa.go.jp/policies/policy/consumer_safety/other/pl_qa.html)

© Hitachi, Ltd. 2024. All rights reserved.

3.2-13. 製造物責任法 (日本) (1/2)

HITACHI
Inspire the Next

- 米国のリステイトメントと同様、当該製造物をその製造業者等が引き渡したときにおける科学又は技術に関する知見において、当該製造物にその欠陥があることを認識できなかった場合には、責任が免責されるとしている。

項目	概要
第4条 免責事由	• 前条の場合において、製造業者等は、次の各号に掲げる事項を証明したときには、同条に規定する賠償の責めに任じない。 1. 当該製造物をその製造業者等が引き渡したときにおける科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかったこと。 2. 当該製造物が他の製造物の部品又は原材料として使用された場合において、その欠陥がもっぱら当該他の製造物の製造業者が行った設計に関する指示に従ったことにより生じ、かつ、その欠陥が生じたことにつき過失がないこと。

[参考] 消費者庁「製造物責任(PL)法の逐条解説」
(https://www.caa.go.jp/policies/policy/consumer_safety/other/product_liability_act_annotations/)
消費者庁"製造物責任法の概要Q&A
(https://www.caa.go.jp/policies/policy/consumer_safety/other/pl_qa.html)

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 製造物責任法の比較 / 第3次不法行為リステイトメント (米国)

HITACHI Inspire the Next

- 米国の第 3 次不法行為リステイトメント(Restatement of the law third Tort Products Liability)では、ソフトウェアは対象に含まれていないが、商品に組み込まれた場合対象に含まれる。
- 販売・供給時点で欠陥の定義に該当する場合には、その製品は欠陥製品となるとされている。

項目		概要
適用対象		• 製品:製品とは、使用または消費のために商業的に流通する有形動産を指す。
対象者		• 製造事業者 • 販売事業者
欠陥の定義		• 販売・供給時点において、製品が、製造上の欠陥を含むか、設計に欠陥が存在するか、または指示・警告が不適切なために欠陥となる場合にはその製品は欠陥製品となる。
	製造上の欠陥	• 製品の準備・販売に際し、あらゆる可能な注意が尽くされていたとしても、製品がその意図された設計から逸脱している場合には、その製品の製造上の欠陥を含む
	設計上の欠陥	• 販売者、他の供給者または供給の商業的連鎖における前者による合理的な代替設計を採用していれば、その製品がもたらす被害の予見可能な危険を減少または回避することができた場合で、かつその代替設計を採用しなかったことで製品が合理的に安全なものとならなかった場合には、その製品には設計上の欠陥がある。
	指示・警告上の欠陥	• 販売者、他の供給者または供給の商業的な連鎖における前者による合理的な指示・警告を用意していれば、その製品をもたらす被害の予見可能な危険を減少、回避することができた場合で、かつその指示・警告を用意しなかったことで製品が合理的な安全なものとならなかった場合には、その製品には指示・警告上の欠陥がある。

- 「製品」を「有形のもの」と明確に定義しており、ソフトウェアを含む電子の配列は対象としていない。
- 一方で、2005年の米国統一法典(UCC:Uniform Commercial Code)の改正により、「製品」は「製品に組み込まれたコンピュータ・プログラム」を含むものとして定義されている。

[参考] 小森悠吾"日本・欧米・アジアにおけるPL法の比較検討" (http://aplics.sakura.ne.jp/ronbun/201902.pdf)
"New Decision Directly Addresses the "Is Software a Product" Question"
(https://www.druganddevicelawblog.com/2022/05/new-decision-directly-addresses-the-is-software-a-product-question.htm)

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

4. ITベンダーとユーザー間の紛争に関する判例の収集

© Hitachi, Ltd. 2024. All rights reserved.

調査項目及び整理の観点等

HITACHI
Inspire the Next

- 本調査では、ITベンダーとユーザー間の責任分界について、法令やガイドライン等で一般的に定められる事項及び、判例ごとに個別で判断された事項について調査、整理した。

分類	調査項目		整理の観点等
1 一般的な事項	1-1	ITベンダーとユーザー間での責任分界に係る法、ガイドライン等の規定	• 責任分界に係る既存規定の概要(例：民法上の債務不履行責任、不法行為責任、PL法における製造物責任、等) • ベンダの債務の内容としてのセキュリティ対策
	1-2	ITベンダー側の過失が認められる/認められない場合とその根拠	• 契約書・仕様書に明記した対策の不実装 • 契約書・仕様書に明記のない対策の不実装 - 契約締結時点で脅威が既知の場合 - 契約締結時点で脅威が未知の場合 ・ ITベンダーによる脆弱性の修補責任
	1-3	脆弱性の原因がSIer等の直接の委託先以外の主体(OSSまたはOSS以外のサードパーティ製品開発ベンダー)にあった場合のベンダー責任のあり方	• 脆弱性の原因がOSSにあった場合の責任のあり方 • 脆弱性の原因がOSS以外のサードパーティ製品にあった場合の責任のあり方
	1-4	セキュリティ対策不足が重過失となり得る場合の条件等	• ITベンダ側の重過失が問われ得る際の判断条件 • 代表的な判例
2 判例ごとの検討事項	2-1	事案の概要	• 関係する事業者のプロフィール • 生じた被害及び係争上の争点
	2-2	ITベンダー側の過失が認められた/認められなかった具体例とその根拠	• ITベンダーの過失として認定された事項 • ユーザーの過失として認定された事項 • 上記判断の具体的根拠
	2-3	セキュリティ対策不足が重過失となった具体例とその根拠	• ITベンダーの重過失とされた具体的事項 • 上記判断の具体的根拠
	2-4	賠償の範囲	• 事故対応・調査費用・お詫び関連 • システム改修 • 逸失利益、信用低下
3 その他	3-1	発注者及びITベンダー間の責任分界に係る示唆	• 報告書等で指摘された論点

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

4.1 一般的な事項

© Hitachi, Ltd. 2024. All rights reserved.

4.1-1. 関連する法、契約等の規定 (1/2)

HITACHI
Inspire the Next

- ITベンダーとユーザーそれぞれの責務は、双方で締結する契約(主に、請負または準委任)に記される。
- ユーザーおよびベンダーの責任分界を考える際、ユーザに完成されたものとして引き渡された成果物が契約の内容に適合しているかどうか、事務処理に関して善管注意義務が果たされているかどうかがポイントになる。

	請負契約	準委任契約
概要	請負人が仕事を完成させる約束をし、請負人の仕事の完成に対し、注文者がそれに対して報酬を支払う契約	委託者が受託者に対し、ある事務作業(法律行為以外)自体を委託する契約
受託側(ベンダ企業)の義務	仕事(受託業務)の完成義務を負う。	善良な管理者の注意をもって委任事務を処理する義務を負う(善管注意義務)。 仕事の完成についての義務は負わない。
義務を果たさない場合	ユーザに完成されたものとして引き渡された成果物が契約の内容に適合しない場合、債務不履行責任の特則としての契約不適合責任を負う。	事務処理に関して善管注意義務違反があった場合には、通常の債務不履行責任(例えば不完全な履行を完全なものにすることや損害賠償責任等)を負う。
関連法規	• 請負は、当事者の一方がある仕事を完成することを約し、相手方がその仕事の結果に対してその報酬を支払うことを約することによって、その効力を生ずる。[民法632条] (契約不適合責任に関する条文は以下) • 引き渡された目的物が種類、品質又は数量に関して契約の内容に適合しないものであるときは、買主は、売主に対し、目的物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を請求することができる。[民法第562条] • その他関連する条項：民法第563条～	• 委任は、当事者の一方が法律行為をすることを相手方に委託し、相手方がこれを承諾することによって、その効力を生ずる。[民法643条] • 受任者は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う。[民法644条] • この節の規定は、法律行為でない事務の委託について準用する。[民法656条]

[参考] 情報処理推進機構(IPA) “情報システム・モデル取引・契約書（第二版）”

© Hitachi, Ltd. 2024. All rights reserved.

4.1-1. 関連する法、契約等の規定 (2/2)

HITACHI
Inspire the Next

- ITシステムの開発・運用等においては、企画段階から開発段階、運用段階、保守段階に至るまで、システムライフサイクルの段階に応じた様々な契約が締結され得る。

モデル契約におけるフェーズの分類		契約類型	類型を選択した根拠
企画段階	システム化の方向性	準委任	• ユーザ側の業務要件が具体的に確定しておらず、ユーザ自身にとってもフェーズの開始時点では成果物が具体的に想定できないものであるから、ベンダにとっても成果物の内容を具体的に特定することは通常不可能である。 • そのため、仕事の完成を目的とし予め成果物の内容が具体的に特定できることを前提とする契約類型である請負には馴染みにくく、準委任が適切と考えられる。
	システム化計画	準委任	
	要件定義	準委任	
開発段階	システム設計(システム外部設計)	準委任・請負	• 開発段階は実務上、準委任と請負の両方があり得る。 • 請負に馴染むのは、業務に着手する前の段階でベンダにとって成果物の内容が具体的に特定できる場合であるが、内部設計やソフトウェア設計などのフェーズはこうしたことが可能であり、請負で行うことができる。 • 特に論点となっているのは、システム外部設計・内部設計業務及び当該外部設計の妥当性を検証するシステムテスト業務である。システム外部設計とシステムテスト業務はユーザ側の業務要件に関わる部分が多く、その点では準委任に馴染むが、従来の実務では請負で行われている場合も多い。
	システム方式設計(システム内部設計)	請負	
	ソフトウェア設計	請負	
	プログラミング	請負	
	ソフトウェアテスト	請負	
	システム結合	請負	
	システムテスト	準委任・請負	
	受入・導入支援	準委任	
運用段階	運用テスト	準委任	-
	運用	準委任・請負	
保守段階	保守	準委任・請負	-

[参考] 情報処理推進機構(IPA) “情報システム・モデル取引・契約書（第二版）”

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 関連する法規定(例)

HITACHI
Inspire the Next

- 民法及び製造物責任法において、ITベンダーとユーザー間の責任分界に係る損害賠償請求等に関する規定が設けられている。

法令等	条	条文 ※一部を適宜省略	本件との関連性
民法	第415条	(債務不履行による損害賠償) 債務者がその債務の本旨に従った履行をしないとき又は債務の履行が不能であるときは、債権者は、これによって生じた損害の賠償を請求することができる。ただし、その債務の不履行が契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由によるものであるときは、この限りでない。	開発する情報システムの性質にもよるが、個人データ等を取り扱うウェブシステムについては、個人データ等の流出を防ぐために、必要なセキュリティ対策を施したプログラムの提供が契約上の債務の内容となる。[サイバーセキュリティ関係法令 Q&Aハンドブック Ver1.0]
	第562条	(買主の追完請求権) 引き渡された目的物が種類、品質又は数量に関して契約の内容に適合しないものであるときは、買主は、売主に対し、目的物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を請求することができる。ただし、売主は、買主に不相当な負担を課するものでないときは、買主が請求した方法と異なる方法による履行の追完をすることができる。	開発業務等を請負契約に基づいて実施する際、ITベンダーによる適切なセキュリティ対策の実装がない場合に本条に示す契約不適合責任を問われ得る。
	第644条	(受任者の注意義務) 受任者は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う。	開発業務等を準委任契約に基づいて実施する際、ITベンダーによる適切なセキュリティ対策の実装がない場合に本条に示す善管注意義務違反を問われ得る。
	第709条	(不法行為による損害賠償) 故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。	ITベンダーに故意又は過失があったことなどの要件を証明できる場合、不法行為による損害賠償請求が問われ得る。
製造物責任法	第3条	(製造物責任) 製造業者等は、その製造、加工、輸入(中略)した製造物であって、その引き渡したものの欠陥により他人の生命、身体又は財産を侵害したときは、これによって生じた損害を賠償する責めに任ずる。ただし、その損害が当該製造物についてのみ生じたときは、この限りでない。	ソフトウェアは無体物のため、ソフトウェアのライセンス契約では同法の問題は生じない。他方、ソフトウェアがチップのファームウェア等に書き込まれて一体化している場合にはこの限りではない。

[参考] 情報処理推進機構(IPA) “情報システムの脆弱性情報の取扱いにおける法律面の調査 報告書改訂版”
内閣官房内閣サイバーセキュリティセンター(NISC) “サイバーセキュリティ関係法令 Q&Aハンドブック Ver1.0”

© Hitachi, Ltd. 2024. All rights reserved.

4.1-2. 開発ベンダー側の過失認定とその根拠

- システム等の納入後にセキュリティインシデントが起きた際、対策を施すことが仕様書等に明示されていたにもかかわらず対応していなかった場合に開発ベンダが責任を負うことについては争いがない。
- また、契約締結当時あるいは納品時において未知の脅威が将来発生して攻撃を受けたというような場合に開発契約上の責任を負わないことについても争いがない。
- 契約締結当時で既知の脅威に十分な対応を取っておらず、かつ仕様書にも記載がなかった場合のベンダ責任については必ずしも明確ではない。

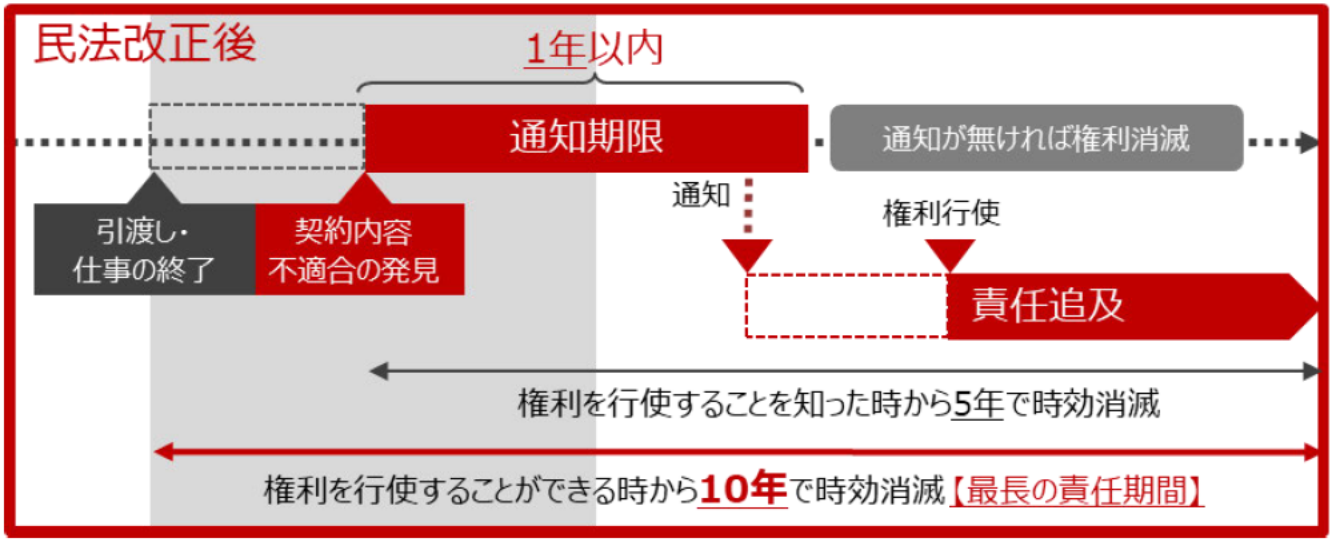
契約書・システム仕様への記載	契約締結時における脅威・脆弱性の存在：既知	契約締結時における脅威・脆弱性の存在：未知
記載あり	• セキュリティ要件の不実装等が「システム仕様書との不一致」に該当し、「契約不適合」に含まれる。 • 契約不適合が発見された場合には、ベンダはその修正等の追完義務を負う。 [IPA, 情報システム・モデル取引・契約書]	• 新たに判明する欠点、脆弱性について、これらすべてを責任の対象とするのは開発者等にとって酷であり、妥当ではない。 • トラブルを未然に防止すべく、新たに判明する欠点、脆弱性に関しては瑕疵担保責任の対象外であることを契約上明記しておくべき。 [IPA, 脆弱性情報の取扱いにおける法律面の調査 報告書]
記載なし	• 業務委託契約書や発注仕様に記述されていない場合でも、開発当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示に合意されていたとされ、特段の事情もなく既知の脆弱性についてセキュリティ対策を講じなかった場合、発注者に生じた損害の賠償義務を負う。 [NISC, 関係法令Q&Aハンドブック Q41]	• ソフトウェアの納入後においても、納入物を使い続けると契約の目的を達することができない重大なセキュリティ上のリスクが顕在化することをベンダが知った場合には、ユーザに対する情報提供が行われることが望ましいが、ベンダの責務はセキュリティ仕様に適合したソフトウェアの納入に限られるため、納入後も期限なく情報提供が求められるものではない。 [IPA,情報システム・モデル取引・契約書]

© Hitachi, Ltd. 2024. All rights reserved.

4.1-2. ITベンダー側の過失認定とその根拠 / 脆弱性の修補責任(1/2)

HITACHI Inspire the Next

- 2020年施行の改正民法では、買主が目的物に契約内容と異なる点があることを発見した際、売主に対して、契約不適合責任として、追完、代金減額、契約解除等の対応を売主に請求することができる。
- 権利行使にあたり、買主は売主に対して契約不適合の発見から1年以内にその旨を通知する必要がある。



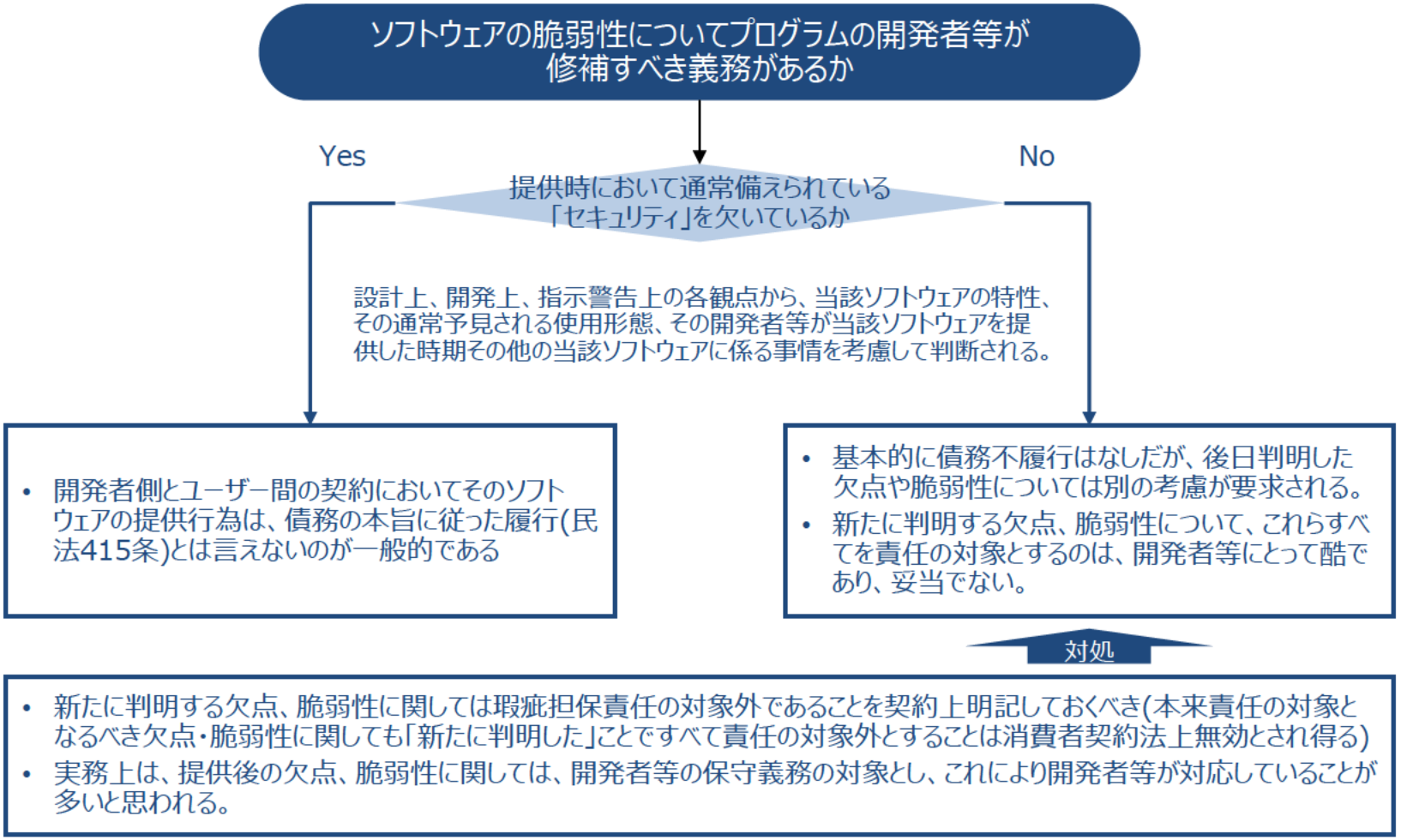
契約不適合責任に係る買主の権利	
追完請求権(562条)	引き渡された目的物が契約の内容に適合しないものであるときは、買主は、目的物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を請求することができる。
代金減額請求権(563条)	買主が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、買主は、その不適合の程度に応じて代金の減額を請求することができる。
催告による解除(541条)	当事者の一方がその債務を履行しない場合において、相手方が相当の期間を定めてその履行の催告をし、その期間内に履行がないときは、相手方は、契約の解除をすることができる。
債務不履行による損害賠償(415条)	債務者がその債務の本旨に従った履行をしないとき又は債務の履行が不能であるときは、債権者は、これによって生じた損害の賠償を請求することができる。

© Hitachi, Ltd. 2024. All rights reserved.

4.1-2. ITベンダー側の過失認定とその根拠 / 脆弱性の修補責任(2/2)

HITACHI Inspire the Next

- ソフトウェアが提供時において通常備えられている「セキュリティ」を欠いている場合、開発ベンダ―による脆弱性の修補責任が生じ得る。
- 後日判明した欠点や脆弱性すべてを責任の対象とするのは、開発者等にとって酷であり、妥当でない。



[参考] 情報処理推進機構(IPA) “情報システム等の脆弱性情報の取扱いにおける法律面の調査報告書 改訂版

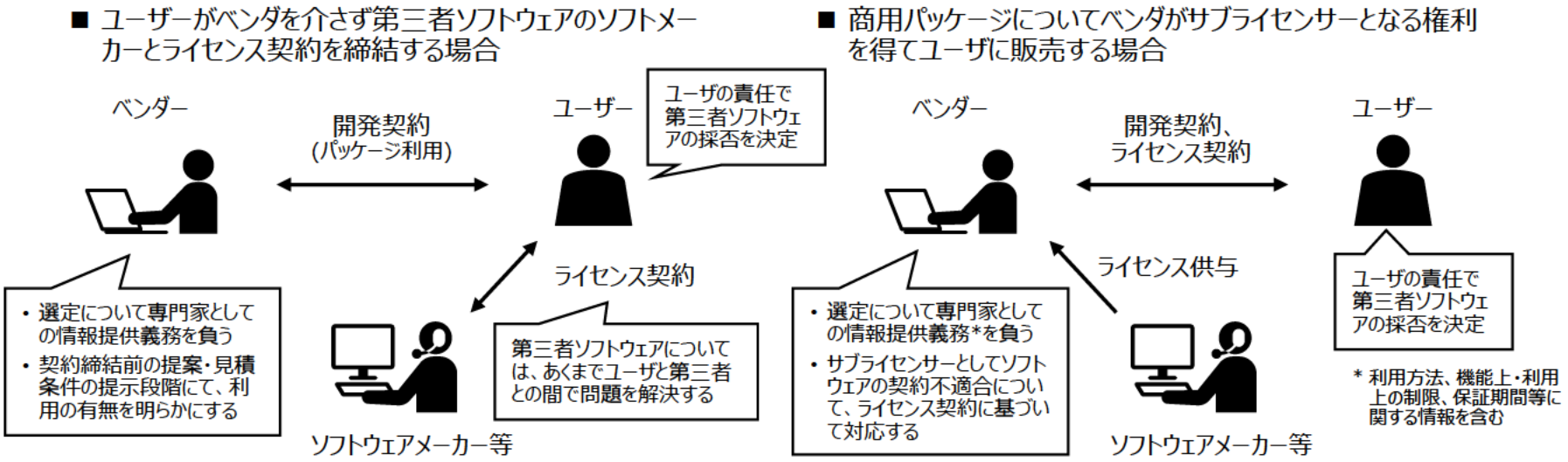
© Hitachi, Ltd. 2024. All rights reserved.

4.1-3. 脆弱性の原因がOSS等にあった場合のベンダ責任のあり方

HITACHI
Inspire the Next

- 第三者ソフトウェアやFOSSの採否は基本的にユーザーの責任で決定されるが、ベンダーも当該ソフトウェアの選定について専門家としての情報提供義務(利用方法、機能上・利用上の制限、保証期間等)を負う。
- FOSS について提供者が脆弱性情報を提供しているにもかかわらず、これを安易に放置していた場合には、過失が有るとして、ベンダーが債務不履行責任を負う可能性も否定できない。

第三者ソフトウェア及びFOSS*をベンダーが主体で選定する場合のベンダー責任



第三者ソフトウェア及びFOSSをユーザが主体で選定する場合のベンダー責任

- ユーザと第三者ソフトウェアのメーカーとの間でライセンス契約を締結し、原則としてベンダは責任を負わない。
- FOSSについても、ユーザーの費用と責任において、第三者との間で保守、障害対応支援契約の締結等、必要な措置を講じる。
- 但し、情報システムの専門家であるベンダが、情報提供時に第三者ソフトウェアが本件ソフトウェアの契約不適合や他者の知的財産権侵害について悪意重過失でこれを告げなかった場合には、免責されない。

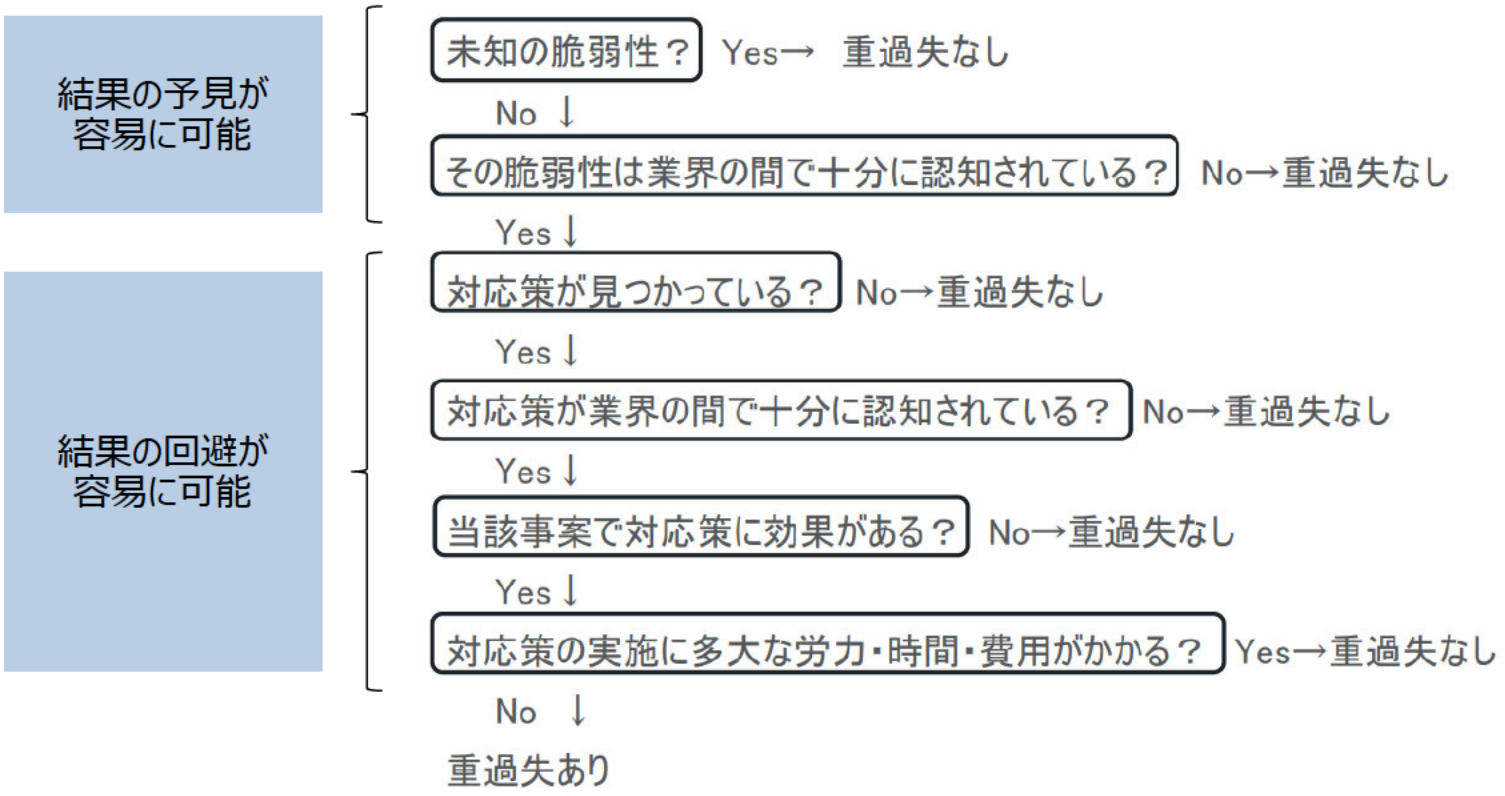
* FOSS：Free and Open Source Softwareの略称。「オープンソース」「オープンソースソフトウェア」「フリーソフトウェア」などとも言う。

[参考] 情報処理推進機構(IPA) “情報システム・モデル取引・契約書（第二版）”

© Hitachi, Ltd. 2024. All rights reserved.

4.1-4. セキュリティ対策不足が重過失となり得る場合の条件等

- セキュリティ攻撃への対策を講じなかった場合の結果が容易に予見可能であり、対策そのものに多大な労力や費用がかかるものではないような場合、対策を怠ったベンダの債務不履行責任は、重大な過失(重過失)があったものとされることがある。
- 重過失が認められる場合、重い賠償義務を負ったり、システム開発契約において合意していた損害賠償額の上限に関する規定などの免責条項の有効性について制限を受ける場合がある。



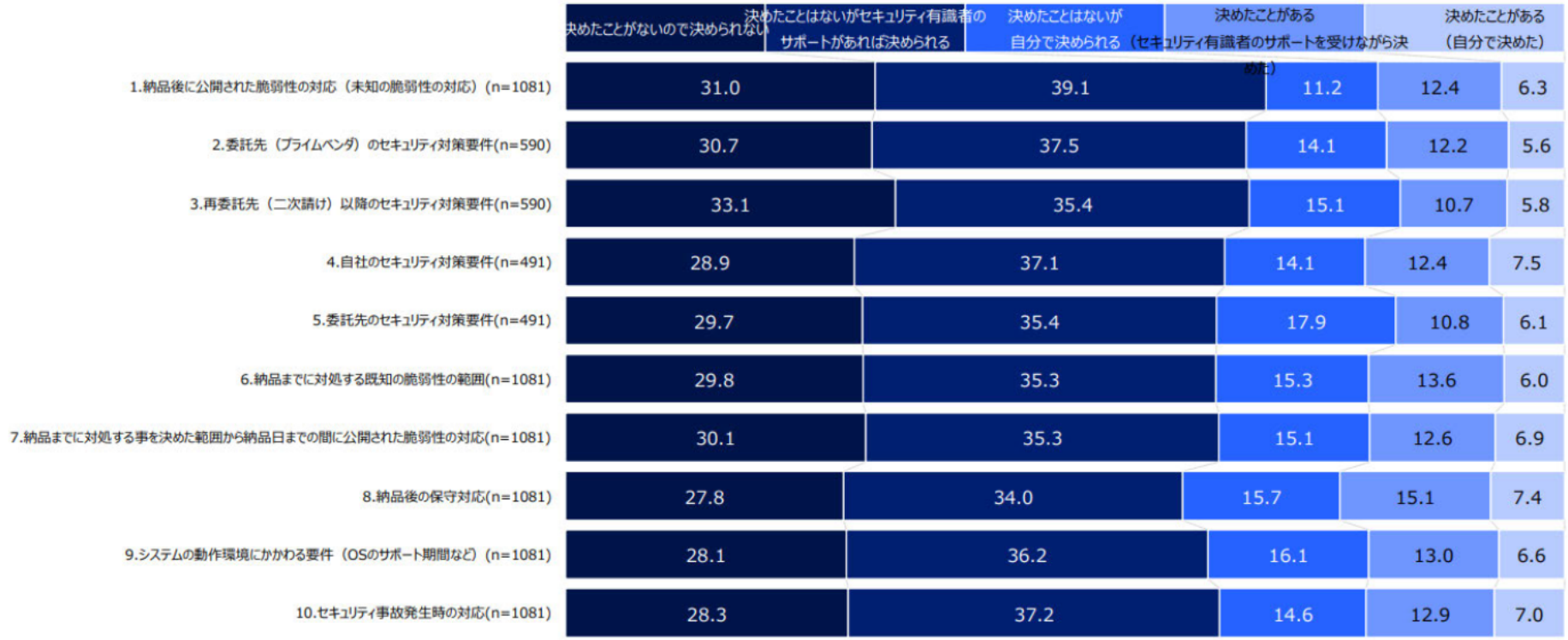
[参考] 武田勝弘, “システムベンダのセキュリティ対策義務～東京地裁平成26年1月23日判決（平23（ワ)32060号）を素材として～”

© Hitachi, Ltd. 2024. All rights reserved.

4.1-5. 企業における対策状況

- IPAが2020年に実施した調査によれば、約8割の契約実務者には契約関連文書におけるセキュリティ要件の内容決定の経験がなく、3割程度がセキュリティ有識者のサポートがあっても決定は困難と回答。
- 契約の中にセキュリティ要件を盛り組む文化は未だ必ずしも一般化していないと推測できる。

■ あなた(契約実務担当者)は、契約関連文書のひな型の作成や見直しを行う際のセキュリティ要件の内容を決めることができますか。



[参考] 情報処理推進機構(IPA), “ITシステム・サービスの業務委託契約書見直しに関する実態調査報告”
https://www.ipa.go.jp/archive/security/reports/economics/scrm2020.html

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

4.2 判例ごとの検討事項

© Hitachi, Ltd. 2024. All rights reserved.

調査対象の判例一覧

HITACHI
Inspire the Next

- セキュリティインシデント発生による損害に係るユーザー企業とITベンダーとの責任分界について争ったものとして、国内判例5件、国外(米国)判例3件を調査対象とする。

分類	調査対象	概要
国内	東京地判平26.1.23判時2221号71頁	クレジットカード情報漏えい事故に対する保守事業者の責任が問われた事例
	東京地判平30.10.26 判例集未登載	SQLインジェクション対策をしていなかったことについて開発会社の責任が問われた事例
	東京地判平30.3.29(平28ワ13202)	ネットショップ運営者が、決済サービス提供者に対して立替払金の返還を求めたのに対し、セキュリティ対策が不備であるとして拒絶した事案
	東京地判平31.1.25(平29ワ22870)	不正にビットコインに交換されて出コインされたという事案における取引所運営者の責任が問題となった事例
	東京地判令元.12.20(平29ワ6203)	クレジットカード情報漏えい事故に関し，その原因の一つと考えられる脆弱性対応が運用保守業務に含まれていたか否かが争われた事例
国外	Traveler`s Casual and surety Company of America v. Ignition Studios	Traveler`s Casual and surety Company of AmericaとIgnition Studios社との係争。Traveler`s側は、ウェブサイトがホスティングされているサーバーのインターネット・セキュリティがIgnition社の過失により甘いため、不正アクセスを許したと主張した。
	Solarwinds Corp	2021年、Solarwinds社とその幹部がサイバーリスクの監視を怠ったために受託者義務に違反し、その結果最近で最大規模の情報漏洩が発生したとして株主はSolarwinds社を提訴した。
	Blackbaud	クラウド・サービス・プロバイダーのBlackbaud社は、非営利団体の会員に関するデータが流出したサイバー攻撃を防止する義務を怠ったとして、2020年に集団訴訟を起こされた。

© Hitachi, Ltd. 2024. All rights reserved.

国内判例の調査結果サマリ

HITACHI
Inspire the Next

- 今回対象とした5件の国内判例においては、2件でベンダー等の過失が認められ、残りの3件ではそれが認められなかった。

名称	ベンダー等の過失	根拠の概要
東京地判 平26.1.23	過失あり	• ユーザーと開発ベンダーとの間で当時の技術水準に沿った対策を施したプログラムを提供することが黙示的に合意されていたと認められる。 • SQLインジェクション対策の不備が、適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行にあたるとされた。
東京地判 平30.10.26	過失あり	• 開発ベンダーには、契約締結当時でも業界で十分に周知されていたSQLインジェクションに対する対策を講ずべき注意義務があったのにこれを怠っていた点で、過失による不法行為の成立を認め、同社の使用者責任を認定した。
東京地判 平30.3.29	過失なし	• ユーザー企業は、サービス事業者において3Dセキュアによる本人認証システムの実装が義務だと主張したが、同社において決済を運営すること自体による利益は決済額の0.6パーセント余りにとどまり、一定の配慮がなされていた点も認定したことから、ユーザー企業の主張を取り下げた。
東京地判 平31.1.25	過失なし	• ユーザーから「異常取引の検知義務違反」及び「二段階認証」の実装が利用者財産の保護に必要であったという主張があったところ、当時の技術水準等を勘案するに、いずれについても積極的に推奨する義務を負っていたとは認められなかった。
東京地判 令元.12.20	過失なし	• 「本件サイトの運用、保守管理」及び「EC-Cubeカスタマイズ」とある注文書の記載の内容に鑑みて、運用ベンダーの債務には、インシデントの原因となったOpenSSLの脆弱性対応は含まれていないとした。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-1. 東京地判平26.1.23(平23ワ32060) / 事案の概要

HITACHI
Inspire the Next

- クレジットカード情報漏えい事故に対する保守事業者の責任が問われた事例
- 争点2~4及び当該争点に対する裁判所の判断について、次頁以降で詳述する。

項目	概要
当事者	• 原告(X社)：インテリア商材の卸小売、通信販売等を行う株式会社 • 被告(Y社)：情報処理システムの企画、保守受託及び顧客へのサポート業務、ホームページの制作、業務システムの開発、ネットショップの運営等を行う株式会社
事案の概要	• X社は、2009年2月4日、Y社にX社のウェブサイトにおける商品のウェブ受注システムの導入を委託した。Y社は本件システムを完成させて納入し、X社は2009年4月15日、サイトの稼働を開始した。 • 本件ウェブサイトでは、当初、顧客のクレジットカード情報を保存していなかったが、2010年1月にY社はX社の依頼を受けて本件システムを変更し、顧客のクレジットカード情報(カード会社名、カード番号、有効期限、名義人、支払回数及びセキュリティコード)が本件システムのデータベースに保存される仕組みとなった。ただし、クレジットカード情報は暗号化されていなかった。X社とY社との間には，本件ウェブサイトの保守に関する契約が締結されていた。 • 2011年4月、本件システムのサーバに不正アクセスがあり、顧客のクレジットカード情報を含む個人情報が流出した。セキュリティ会社の調査によると、SQLインジェク ション攻撃により、当時サーバ内に保有されていたクレジットカード情報6975件全件が漏えいした可能性があるということであった。 • X社は、Y社に対し適切なセキュリティ対策を執っていなかったなどと主張し、委託契約の債務不履行に基づき損害賠償金約1.1億円を請求した。被告は、これに対し、債務不履行の有無や損害の額を争うとともに、「契約金額の範囲内において」支払うという損害賠償責任制限規定の適用を主張した。
係争上の争点 (次頁以降で詳述)	1. 本件流出の原因及び程度 2. Y社の債務不履行責任の有無 3. X社の過失と因果関係の断絶 4. 損害 5. 損害賠償責任制限の合意の成否等
判旨	• X社の請求の一部である2200万円余りの損害賠償及び遅延損害金について認容した。

[参考] 東京地方裁判所判決／平成２３年（ワ）第３２０６０号
https://www.softic.or.jp/semi/2014/5_141113/op.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-1. 東京地判平26.1.23(平23ワ32060) / 争点への裁判所見解

HITACHI Inspire the Next

- SQLインジェクション対策の不備が、適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行にあたるとして、Y社の過失を認めた。

2 Y社の債務不履行責任の有無

- X社は、Y社に以下の５つの債務不履行責任があると主張した。
  1. 適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行
  2. ネットワークやサーバーのセキュリティ対策を講ずべき債務の不履行
  3. カード情報を保存せず，保存する場合には暗号化すべき債務の不履行
  4. サーバー、データベース及び管理機能へのログインID及びパスワードを管理すべき債務の不履行
  5. 被告によるセキュリティ対策の程度についての説明義務違反
- 裁判所は、X社主張の５つの債務不履行のうち、SQLインジェクション攻撃が原因だったこと(争点1)に照らして、１、３、５の有無について検討した。

X社主張の責任	責任	判断の根拠
適切なセキュリティ対策が採られたアプリケーションを提供すべき債務の不履行	あり	• Y社は、2009年当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められる。 • 2006年経産省及びIPAから対策実施について注意喚起があり、IPAは具体的なSQLインジェクション対策を書面により公表していた一方、Y社はいずれの対策も取っていなかった。
カード情報を保存せず，保存する場合には暗号化すべき債務の不履行	なし	• 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」等では、左記対策を「望ましい」と指摘するにすぎない。 • 暗号化の設定内容等は暗号化の程度によって異なり、それによってY社の作業量や代金も増減すると考えられることに照らすと、契約で特別に合意していなくとも、当然に、Y社が左記対策の実施に係る債務を負っていたとは認められない。
被告によるセキュリティ対策の程度についての説明義務違反	なし	• Y社がX社に対してセキュリティ対策等の説明をすべき信義則上の義務を負うと主張した。 • Y社が説明すべき具体的内容としては、①SQLインジェクション対策を講じていないこと、②本件システムのセキュリティ対策が脆弱であること、③Y社とA社との間のレンタルサーバー契約において最低のセキュリティレベルの内容としていたこと、④金種指定詳細化の際にクレジットカード情報を暗号化せずに保存する設定としたことを指摘したが、①～④のそれぞれについてY社による説明義務違反は認められなかった。

© Hitachi, Ltd. 2024. All rights reserved.

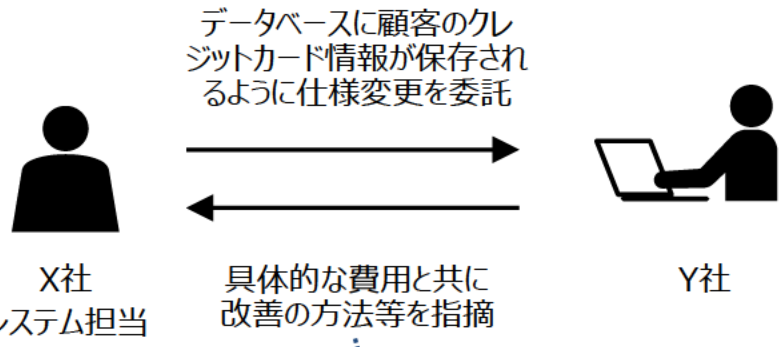
4.2-1. 東京地判平26.1.23(平23ワ32060) / 争点への裁判所見解

HITACHI Inspire the Next

- Y社からは過失相殺の主張はなかったが、X社の過失(Y社からの提案があったにも関わらず、データベースに顧客クレジットカ ード情報が保存される仕様を放置)を考慮し、3割の過失相殺をするのが相当とされた。

3 X社の過失と因果関係の断絶(特に、X社の過失について)

- Y社からは過失相殺の主張はなかったが、顧客のクレジットカード情報のデータがデータベースにあり、セキュリティ上はクレジットカード情報を保持しない方が良いことをX社のシステム担当者が認識しながら、Y社から本件システム改修の提案を受けていたにもかかわらず何ら対策を講じずにこれを放置したことが、本件流出によるクレジットカード情報の漏洩の一因となったことは明らか。
- X社に損害が認められるとしても、上記X社の過失を考慮し、3割の過失相殺をするのが相当とされた。



Y社からの回答後も、データベースに顧客のクレジットカ ード情報が保存される仕様を放置

- カード会社が管理するウェブサイトの画面上でクレジットカード情報を入力する方式でカード会社名の情報を取得することができ、改修の費用は20万円程度
- 現状はデータベースにクレジットカード情報のデータはあるが、データベースを直接見る手法を用いなければカード番号は見られない
- セキュリティ上はクレジットカード情報を保持しない方が良く、その方が一般的

© Hitachi, Ltd. 2024. All rights reserved.

4.2-1. 東京地判平26.1.23(平23ワ32060) / 争点への裁判所見解

HITACHI Inspire the Next

- 「本件ウェブ受注システム委託契約に関連して支払った代金」、「顧客への謝罪関係費用」、「顧客からの問い合わせ対応費用」、「調査費用」、「売上損失」等についてX社の損害を認め、Y社の支払いを指示。

4 損害

- 東京地裁は、「本件ウェブ受注システム委託契約に関連して支払った代金」、「顧客への謝罪関係費用」、「顧客からの問い合わせ対応費用」、「調査費用」、「売上損失」等についてX社の損害を認め、Y社の支払いを指示した。
- 前頁で示したように、X社側の過失が認められた側面もあるため、合計約3230万円の損害から、 3割を過失相殺し、Xが請求できる金額は約2260万円となった。

項目		概要
ア	本件ウェブ受注システム委託契約に関連して支払った代金	• X社は、開発代金合計約2070万円全額が損害だと主張したが、裁判所は、サービスによって利益を享受していたのであるから、全額が損害となるものではなく、保守サービス料として前払いしていた費用のうち、期間按分した約27万円を相当因果関係ある損害と認めた。
イ	顧客への謝罪関係費用	• X社が顧客全員に対して送付したQUOカードとその包装代金、郵送代、作業費などの合計約1860万円を損害であると認めた(1件あたり約1000円)。
ウ	顧客からの問い合わせ対応費用	• 顧客からの問い合わせのために設置したコールセンターの外注費用として支払われた合計約490万円が損害であると認めた。
エ	調査費用	• X社が調査を依頼したB社、L社の調査費用の合計約390万円が損害であると認めた。
オ	売上損失	• X社は4か月間にわたってクレジットカード決済機能が利用できなかったとして、約6000万円の売上損失を主張していたが、裁判所は民訴法248条を適用して400万円の限度で相当因果関係が損害だと認めた。
カ	その他	事故対策会議出席交通費その他の事故対策費用として約50万円の損害が認められた。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-1. 東京地判平26.1.23(平23ワ32060) / 重過失の有無等

HITACHI
Inspire the Next

- 本判例においては、求められる水準の注意義務が満たされていなかったとして、ITベンダー(Y社)の重過失を認め、賠償額の制限規定の適用を棄却した。

項目	本判例における概要
論点	• X社とY社の間で締結された基本契約29条2項(賠償額の制限に関する規定)は、Y社に故意又は重過失がある場合には適用されないと解するのが相当であるが、本件事案において、Y社に重過失が認められるか。※争点⑤(2)の記載に相当
重過失の有無に関する要旨 (原文を一部加工)	• Y社は情報処理システムの企画、ホームページの制作、業務システムの開発等を行う会社として、プログラムに関する専門的知見を活用した事業を展開し、その事業の一環として本件ウェブアプリケーションを提供しており、X社もその専門的知見を信頼して本件システム発注契約を締結したと推認でき、Y社に求められる注意義務の程度は比較的高度なものと認められる • SQLインジェクション対策がされていなければ、第三者がSQLインジェクション攻撃を行うことで本件データベースから個人情報が流出する事態が生じ得ることは被告において予見が可能であり、かつ、経済産業省及びIPAが、ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ、バインド機構の使用又はSQL文を構成する全ての 変数に対するエスケープ処理を行うこと等のSQLインジェクション対策をするように注意喚起をしていたことからすれば、その事態が生じ得ることを予見することは容易であったといえる。 • また、バインド機構の使用又はエスケープ処理を行うことで、本件流出という結果が回避できたところ、本件ウェブアプリケーションの全体にバインド機構の使用又はエスケープ処理を行うことに多大な労力や費用がかかることをうかがわせる証拠はなく、本件流出という結果を回避することは容易であったといえる。そうすると，被告には重過失が認められるというべきである。
判断結果	• 本件基本契約29条2項(賠償額の制限規定)の適用はないとし、相当因果関係ある損害について賠償責任を認めた(ただし、過失相殺により3割減額)。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-2. 東京地判平30.10.26(平29ワ40110) / 事案の概要

HITACHI
Inspire the Next

- SQLインジェクション対策不備の責任が問われた事案であり、開発ベンダY社の過失を認め、X社の請求の一部である約95万円が損害として認定された。

項目	概要
当事者	• 原告(X社)：車・バイクの一括査定システムをY社に委託 • 被告(Y社)：情報処理システムの企画、保守受託及びサポート業務を行う事業者であり、X社の提供する車・バイクの一括査定システム(本件システム)の開発を受託
事案の概要	• X社は、Y社に対し、X社の提供する車・バイクの一括査定システム(本件システム)の開発を約320万円で委託し、2012年9月に納品を受けた。 • その後X社は、2016年12月に、IPAから中国のサイトに本件システムの脆弱性に関する情報が掲載されているという指摘を受けて、Y社に対しその調査と報告を依頼した。 • その結果、本件システムには、SQLインジェクション対策が不十分という脆弱性が判明したことから、X社はY社に対し、その脆弱性はY社の被用者の故意過失によって生じたものであるから使用者であるY社には使用者責任があると主張して、民法715条1項所定の損害賠償請求権に基づき、緊急対策費用47万5200円、詳細な調査、抜本的な修正費用640万円、サーバー移転費用35万6400円、セキュリティ対策のための本件システム停止期間の売上減200万円の合計923万1600円の損害賠償金の支払を求めた。
係争上の争点 (次頁以降で詳述)	1. Y社の使用者責任の成否 2. X社の損害の発生及び額
判旨	• X社の請求の一部である約95万円が損害として認定された。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-2. 東京地判平30.10.26(平29ワ40110) / 争点への裁判所見解

HITACHI Inspire the Next

- 裁判所は、Y社にはSQLインジェクションに対する対策を講ずべき注意義務があったのにこれを怠っていた点で、過失による不法行為の成立を認め、Y社の使用者責任を認定した。(2-1の判例とも整合)

1 Y社の使用者責任の成否

- 裁判所は、前提事実として前記事案の概要に加え、おおよそ以下の事実を認定した。
- 裁判所は、SQLインジェクションに対する対策を講ずべき注意義務があったのに、これを怠っていた点で、Y社の使用者責任(不法行為)を認定した。

裁判所の解釈	認定された事実
遅くともX社がY社に本件システムの制作を発注した平成24年当時までには、既にSQLインジェクションによる不正アクセス等のセキュリティ上のリスクの存在が広く知られ、その対策としてエスケープ処理の実施という具体的な方法もシステム開発の業界内では周知されていた。	2007年に公表されたOWASPの提供する脆弱性の資料では、SQLインジェクションの欠陥は2位に挙げられていた。
	2008年には、IPAが作成した「SQLインジェクション対策について」等で注意喚起されるとともに、エスケープ処理等が示されていた。
	X社がY社に対して本件システムの開発を発注する際に交わされた「確認書」には、本件システムの制作に当たってはセキュリティを十分に確保し、インターネット上の様々な環境においてもエラーや投稿情報漏れをなくし、個人情報の流出に対して十分な対策を備えるよう努めることが定められ、その主な仕様を定めた仕様書にも、セキュリティに関して気を付ける点として「SQLインジェクション」が既知の脆弱性の一つとして明記されていた。
	2016年のX社からの指摘を受けたY社の調査により、SQLインジェクション対策の不足があり、謝罪とともに修正と対策を申し入れた。
	X社は、第三者たるP社に対して調査を依頼した結果、SQLインジェクション対策不備を含む14カ所の脆弱性が発見され、対策を講じた(ただし、P社から提案された詳細なセキュリティ診断や本件システムのリニューアルは実施しなかった)。
	X社は、サーバー管理会社からもすべてのファイルの削除等の勧告を受けたが、個人情報の漏えいが確認されなかったこともあり、本件システムの使用は継続していたが、匿名アカウントによる攻撃を受けた事実はあった。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-2. 東京地判平30.10.26(平29ワ40110) / 争点への裁判所見解

HITACHI Inspire the Next

- 本件では、X社において情報漏えい等の具体的な被害は必ずしも確認されなかったものの、X社の請求の一部である約95万円が損害として認定された。

2 X社の損害の発生及び額

- 裁判所は、脆弱性発覚後にP社へ委託した調査と対策の費用、サーバー管理会社から推奨された施策に係る実際に支出されていない費用、P社による対策のために2日間本件システムを停止させたことによる逸失利益を損害として認め、これらの合計である約95万円が損害として認定した。

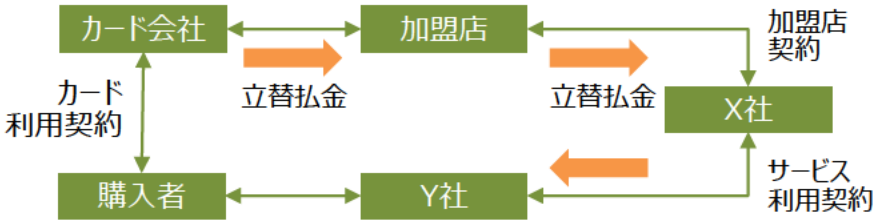
項目	損害認定	概要
委託した調査と対策の費用	○	• P社に委託した調査と対策費用の合計約47万円は、相当因果関係ある損害だと認定した。
P社が提案した抜本的なリニューアル費用	×	• P社が提案した抜本的なリニューアル費用(約640万円)は、元の開発代金を大幅に上回るものであり、P社の対応作業も相当なものであって、抜本的修正をも行う必要はなかったとして損害とは認めなかった。
サーバー上の全ファイルの削除及び再構築を実施すること又はこれに代替する措置を講ずる費用	○	• 本件システムのサーバー管理会社から推奨された、サーバー上の全ファイルの削除及び再構築を実施すること又はこれに代替する措置を講ずることに特段の反証のない本件においては、X社の主張するサーバーの移転は上記の代替措置として適切なものであり、これに要する費用(35万6400円)もサーバー内の全ファイルの削除及び再構築に要する費用よりも低額であると考えられるから、実際に支出されていない費用についても損害の一部とした。
逸失利益	○	• P社による対策のために2日間本件システムを停止させたことについて、X社の決算書から1日あたりの平均売上総利益の2日分(約12万円)を相当因果関係ある損害だとした。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-3. 東京地判平30.3.29(平28ワ13202) / 事案の概要

HITACHI
Inspire the Next

- カードの不正利用によってチャージバックされたネットショップ運営者が、決済サービス提供者に対して立替払金の返還を求めたのに対し、セキュリティ対策が不備であるとして拒絶した事案

項目	概要
当事者	• X社：決済手段を含めたネットショップ開設サービスを提供 • Y社：X社のサービスを利用し、ネットショップを開設
事案の概要	• X社は、決済手段を含めたネットショップ開設サービスを提供しており、Y社はその会員としてネットショップを開設していた。 • 決済のルートは下記の図のようにカード会社から加盟店、X社を経由してY社に支払われるようになっていた。それぞれの契約において、一定の問題が生じた場合には立替払金を立替元に返金しなければならない旨の規定があった。  • Y社は、平成27年7月から9月頃までの間に合計55件のドローン関連製品を複数の顧客に販売したところ、後日クレジットカード名義人から身に覚えがないといったクレームが入ったため、カード会社から加盟店を経由してX社に対して立替払金の返金を求め、X社はこれに応じた。 • X社の担当者は、当時からY社に対し、上記の過程で、Y社の取引の中には不正利用の疑いがあるため契約解除や配送停止をするよう注意するとともにチャージバックとなる可能性を指摘していた。同年9月7日にY社からX社に差し入れられた誓約書には、物品購入契約が「解除、取消し、無効等の理由により効力を失った」「実体がない又は金額相違などの疑義が生じた」場合には、立替払金を返金しなければならない旨が記載されていた。 • Y社が返金に応じなかったため、XはYに対し立替払金の返還を求めた。 • なお、決済時のセキュリティ手段としては、セキュリティコードの入力はあるもの3Dセキュア等を利用した本人認証の仕組みまでは採用されていなかった。
係争上の争点	1．Y社の返金義務の有無
判旨	• Y社の反論を退け、X社の請求を認容した

© Hitachi, Ltd. 2024. All rights reserved.

4.2-3. 東京地判平30.3.29(平28ワ13202) / 争点への裁判所見解

HITACHI Inspire the Next

- 裁判所は、X社には安全な決済を提供する責任があることを示唆しつつも、Y社の反論を退け、X社の請求を認容した。

1 Y社の返金義務の有無

- Y社は、X社が安全な決済手段を提供する義務を負っており、具体的には3Dセキュアによる本人認証システムを採用するなどして不正利用を防止する義務を負っていたのにこれを怠っており、そのようなＸ社が返金を求めることは信義則に反すると主張していた。
- 裁判所は、X社には安全な決済を提供する責任があることを示唆しつつも、Y社の反論を退け、X社の請求を認容した。

裁判所の解釈	判決文(抜粋)
Ｘ社には安全な決済の提供責任がある	X社は、決済の提供者として会員が決済に伴うリスクに徒らに晒されないように配慮すべき立場にあるから、決済がクレジットカードの不正利用に係るリスクとの関係で致命的な欠陥を有するにもかかわらず、X社がそれを殊更に放置しているような特段の事情がある場合には、そのリスクを一方的に会員に転嫁することが信義則違反と評価される余地はあるといえる。
X社には安全な決済に関する具体的内容の裁量がある	もっとも、会員には退会の自由も保障されている以上、その具体的な配慮の仕方については運営者であるX社に一定の裁量が認められているというべきである。
X社においても一定の対策がなされている	そのような観点からすると、X社としては、決済において、クレジットカードの不正利用に対する一般的な対策の一つであるカード利用者をしてセキュリティコードの入力をさせるシステムを整備した上で、クレジットカードの不正利用の疑いがある取引について情報を入手し次第、これをY社に伝えて、契約解除及び商品発送の取りやめを慫慂したり、カード会社による返金請求(チャージバック)がされた場合でも、これに対する反証のための資料の収集・提出について被告を促したりしており、Y社が無用な損失を被らないように一定の配慮をしていることが認められる。
X社が決済から得られる対価は少額であり、Y社主張の対策は必須だったとは言えない	しかし、X社がY社に対して決済手段を提供することの対価として得る手数料とX社がb社決済を利用できることの対価としてb社に支払う手数料との間にはほとんど差がなく、X社において決済を運営すること自体による利益は決済額の0.6パーセント余りにとどまることも考慮すると、X社において、上記で述べたような配慮をしているのであれば、Y社の主張するような水準の措置まで講じていなかったとしても、X社の権利行使を法的に制限するような特段の事情があるとはいえないというべきである。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-4. 東京地判平31.1.25(平29ワ22870) / 事案の概要

HITACHI
Inspire the Next

- 不正にビットコインに交換されて出コインされたという事案における取引所運営者の責任が問題となった事例。
- 争点2~3及び当該争点に対する裁判所の判断について、次頁以降で詳述する。

項目	概要
当事者	• X：仮想通貨売買・取引所運営事業者Y社にアカウントを開設していた個人 • Y社：仮想通貨売買・取引所運営事業者
事案の概要	• 本件は、仮想通貨売買・取引所運営事業者Y社にアカウントを開設していたX(個人)が、何者かにXの預託金約4500万円がビットコインに交換され、すべてXの了知しないビットコインアドレスに送付されたことについて、Yに対し、[1]消費寄託契約に基づく預託金の支払い、[2]不正取引防止等の義務に違反したという債務不履行に基づく損害賠償、[3]不法行為に基づく損害賠償として、約4500万円の支払いを求めたという事案である。 • XとY社は、平成28年8月5日にY社が提供する仮想通貨売買・取引所サービスの利用契約(本件契約)を締結した。 • Xのアカウントには、平成29年2月10日時点で、4545万4702円、0.00472013BTCが残高として記録されていた。その後、同月22日午前6時14分から同日午前7時21分ころまでの間にXの預託金がビットコインに次々と交換され(本件交換)、さらに出コイン(本件引出し)が行われ、残高は61円、0BTCになった(本件交換と本件引出しを合わせて「本件取引」)。 • 本件取引は、Y社が提供するAPIを利用して行われており、本件引出しの送信元IPアドレスは、Yが提供している「プレイグラウンド」と呼ばれるテスト画面のものであった。 • なお、Y社は、平成30年6月22日に不正アクセスによる仮想通貨の不正流出の未然防止などの内部管理体制において問題が認められたとして、関東財務局から資金決済法63条の16に基づいて業務改善命令を受けたが、本件取引との関係は明らかになっていない。
係争上の争点	1. 本件契約の性質 2. 債務不履行及び不法行為の成否 3. 免責規定の適用可否
判旨	• システム構築義務違反は認められなかったことから、Xの請求はすべて棄却された。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-4. 東京地判平31.1.25(平29ワ22870) / 争点への裁判所見解

HITACHI Inspire the Next

- XからY社に対して、一定の対策の実装が利用者財産の保護に必要であったという主張があったところ、当時の技術水準等を勘案するに、いずれについてもかかる対策の義務があるとは認められなかった。

2 債務不履行及び不法行為の成否

- XからY社に対して、「異常取引の検知義務違反」及び「二段階認証」の実装が利用者財産の保護に必要であったという主張があったところ、当時の技術水準等を勘案するに、いずれについてもかかる対策の義務があるとは認められなかった。

解釈	判決文(抜粋)
Y社に利用者保護のための セキュリティ対策義務は存在	Y社のビットコインの取引の仕組みからすると、Y社は、本件交換及び本件引出し当時、信義則上、利用者財産の保護のために十分なセキュリティを構築する義務を負っていたと解される
当時の技術水準からして、 異常取引の検知義務違反は 認められない	APIは、もともと通常のログイン取引に比して、複雑な取引条件を設定したり、大量又は自動的な取引をすることを希望するユーザー向けに設置されているサービスであり、Xの取引においても、短時間に多額の出金措置を講じたり、本件口座においてビットコインの売買をしたりするなどしていることからしても、API利用者には、ビットコインの取引に関し、多様なニーズがあることがうかがわれる。 そして、そのようなAPI利用者の取引のうち、どのような取引をもって異常なものと判断することには困難を伴うと考えられ、また、Y社として本件交換及び本件引出しがされた当時の技術水準からして、API利用者の通常の取引と比較して、異常な取引がされた場合に、そのような取引を注視させる措置を講ずることが技術的に可能であったとも認められない。
Y社において二段階認証を通常 設定とし積極的に推奨する義務 を負っていたとは認められない	Y社のCTOを務めるBの陳述書によれば、当時の仮装通貨業界では二段階認証を一般的に採用している会社はない旨の記載があり、Bも証人尋問において同旨の証言をするところ、Bの証言の信用性を左右するに足りる的確な証拠はなく、その信用性は否定し難い上に、APIが通常のログイン取引と異なり、API利用者の多様なニーズに対応する必要があり、二段階認証を通常の設定とすることが、複雑な取引条件を設定することや、大量又は自動的な取引を行うことを希望するユーザーにとって障害となる可能性も否定できないことからしても、本件交換及び本件引出しの当時、Y社において、API利用時に当然に二段階認証を通常設定とし、積極的に推奨する義務を負っていたとまでは認められない。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-4. 東京地判平31.1.25(平29ワ22870) / 争点への裁判所見解

HITACHI Inspire the Next

- APIキー及びAPIシークレットの管理や、当該ユーザーID及びパスワードの管理が不十分であったなど、特段の事情がある場合には、契約上の免責規定は適用されないとされた。

3 免責規定の適用可否

- APIキー及びAPIシークレットの管理や、当該ユーザーID及びパスワードの管理が不十分であったなど、特段の事情がある場合には、契約上の免責規定は適用されないとされた。

解釈	判決文(抜粋)
本件契約を構成する規約には、左記のような免責規定があった	(ア) 5条2項 パスワード又はユーザーIDの管理不十分、使用上の過誤、第三者の使用等による損害の責任は登録ユーザーが負うものとし、当社は一切の責任を負いません。 (イ) 13条1項1文 当社は、ビットコインの販売・買取、その他関連サービス並びにビットコインの価値、機能、使用先及び用途につき如何なる保証及び如何なる責任(瑕疵担保責任を含みます。)を負うものではありません。 (ウ) 14条2項 当社は、本サービスに関連して登録ユーザーが被った損害について、一切賠償の責任を負いません。なお、消費者契約法の適用その他の理由により、本項その他当社の損害賠償責任を免責する規定にかかわらず当社が登録ユーザーに対して損害賠償義務を負う場合においても、当社の賠償責任は、損害の事由が生じた時点から遡って過去１ヶ月の期間に登録ユーザーから現実に受領した本サービスの利用料金の総額を上限とします。
APIキー及びAPIシークレットの管理や、当該ユーザーID及びパスワードの管理が不十分であったなど、特段の事情がある場合には、免責規定は適用されない	通常のウェブサイト上からユーザー自身のAPIキー及びAPIシークレットを入力して、Y社のウェブサイトにあるユーザーのアカウント内の情報を呼び出して、ビットコインの取引が行われた場合や、通常のウェブサイト上からユーザー自身のユーザーID及びパスワードを入力して、Y社のウェブサイトにあるユーザーのアカウントにアクセスして、ビットコインの取引が行われた場合であっても、Y社において、当該APIキー及びAPIシークレットの管理や、当該ユーザーID及びパスワードの管理が不十分であったなど、上記義務に違反していると認められる特段の事情がある場合には、本件免責規定は適用されないと解される(最高裁平成5年7月19日第二小法廷判決・集民169号255頁、判タ842号117頁参照)。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-5. 東京地判令元.12.20(平29ワ6203) / 事案の概要

HITACHI
Inspire the Next

- クレジットカード情報漏えい事故に関し、その原因の一つと考えられる脆弱性対応が運用保守業務に含まれていたか否かが争われた事例。

項目	概要
当事者	• X社：通販サイト(本件サイト)を運営する事業者 • Y社：X社から本件サイトの運用業務を受託していた事業者
事案の概要	• X社は、同社の運営する通販サイト(本件サイト)を第三者に開発委託し運用していたが、その後、2013年1月ころまでに、Y社に対し、本件サイトの運用業務を月額20万円で委託した(本件契約)。本件サイトはEC-CUBE(※)で作られていた。なお、X社からY社への業務委託に関し、契約書は作成されておらず、注文書には「本件サイトの運用、保守管理」「EC-CUBEカスタマイズ」としか記載されていない。 ※株式会社イーシーキューブが提供している、ECサイト構築パッケージ • 2014年4月には、OpenSSLの脆弱性(いわゆる「Heartbleed」脆弱性)があることが公表されたが、本件サイトではOpenSSLが用いられていた。 • 2015年5月ころ、X社は、決済代行会社から本件サイトからXの顧客情報(クレジットカード情報を含む)が漏えいしている懸念があるとの連絡を受け(本件情報漏えい)、X社はクレジットカード決済機能を停止した。 • X社は、Y社に対し、本件契約に基づくYの債務にはOpenSSLの脆弱性対応も含まれるところ、これを怠り、それによって本件サイトから本件情報漏えいが生じたとして、本件情報漏えいに伴ってXに生じた損害(ユーザへのお詫びクオカード代、調査費用、逸失利益等の合計約1.6億円)の賠償を求めた。
係争上の争点	1. 本件契約における委託業務にOpenSSLの脆弱性対応が含まれていたか。
判旨	• Yの債務にはOpenSSLの脆弱性対応は含まれていないとした。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-5. 東京地判令元.12.20(平29ワ6203) / 争点への裁判所見解

HITACHI
Inspire the Next

- 「本件サイトの運用、保守管理」及び「EC-Cubeカスタマイズ」とある注文書の記載の内容に鑑みて、Y社の債務にはOpenSSLの脆弱性対応は含まれていないとした。

1 本件契約における委託業務にOpenSSLの脆弱性対応が含まれていたか

- 「本件サイトの運用、保守管理」及び「EC-Cubeカスタマイズ」とある注文書の記載の内容に鑑みて、Y社の債務にはOpenSSLの脆弱性対応は含まれていないとした。

解釈	判決文(抜粋)
当然にOpenSSLに関するセキュリティ対策業務の委託を受けたこととなると解することはできない	本件契約における当事者の合意内容をうかがわせる本件注文書(甲4)に委託される業務として記載された「本件サイトの運用、保守管理」との記載は、本件サイトが直ちに本件システム全体を意味するとまではいえない以上は、少なくともその文言上、これに本件システム全体を対象とする業務が含まれることが直ちに読み取れるとまでいうことはできず、 また、同じく本件注文書に委託される業務として記載された「EC-Cubeカスタマイズ」との記載についても、EC-Cubeはインターネット上の通販サイト用のソフトウェアの一つである一方、OpenSSLはインターネット上の暗号化通信に用いられるオープンソースソフトウェアであり、両者は全く性質の異なるソフトウェアであることから、このような記載に係る業務にOpenSSLに関するセキュリティ対策業務が含まれている旨を直ちに読み取ることも困難であって、EC-CubeにおいてOpenSSLを経由した通信がされるからといって、EC-Cubeのカスタマイズ業務の委託を受けた者が、当然にOpenSSLに関するセキュリティ対策業務の委託を受けたこととなると解することはできない。
	かえって、(略)本件注文書のファイル名や業務の件名として、SEO施策(すなわち検索エンジンによる検索結果の改善に向けた業務)と記載されていたことからみて、本件契約による委託の主な目的が、X社の公式サイトである本件サイトの顧客誘引力をいかにして高め、売上げの向上を図るかというマーケティング施策にあったことがうかがわれる。

© Hitachi, Ltd. 2024. All rights reserved.

海外判例の調査結果サマリ

HITACHI
Inspire the Next

- 今回対象とした3件の米国判例においては、2件でベンダー等の過失が認められ、残りの1件では結果が不明だったもののそれが認められなかった可能性もある。

名称	ベンダー等の過失	判断根拠の概要
Traveler`s Casual	主張取り下げ(和解条件不明)により、詳細は不明	[原告主張] • 被告は顧客金融機関に対し、ウェブサイトの保守・サービス業務を遂行する上で、専門家としての注意義務を負っていたにもかかわらず、同義務に違反し、機関へ損害を与えた。 [被告主張] • 原告主張は、当事者が契約に基づく請求に不法行為法を用いて経済的損害を回復することを禁止している経済的損失法理に違反しており無効。
Solarwinds	過失あり	• Solarwinds社がインシデント前後に公表していたセキュリティステートメントの内容は、虚偽を含み、誤解を招くものであり、かつ重要な事実を省いていた。 • 上記は、米国証券取引所法及び関連規則の条項に違反する。
Blackbaud	過失あり	• Blackbaud社において、顧客や個人の機微なデータは適切に保護されておらず、契約または州データ保護法により定められた対策を実装していたとは言えない状況であった。 • 上記インシデントに係るBlackbaud社から顧客または個人への情報開示は適切になされておらず、米国証券取引所法及び関連規則の条項に違反する。

© Hitachi, Ltd. 2024. All rights reserved.

4.2-6. Traveler`s Casual / 事案の概要

HITACHI
Inspire the Next

- 2012年にAlpine銀行において発生したサイバーインシデントに関連して、攻撃対象となったウェブサイトの設計、保守にかかわるIgnition Studioに注意義務違反があるとして民事訴訟が提起された。

項目	概要
当事者	• Travelers Casualty and Surety Company of America：本事案の原告。ウェブサイトの設計とサービスを被告に委託したAlpine銀行(Travelersの保険サービスを利用)の代理として訴訟を提起。 • Ignition Studio：本事案の被告。ウェブサイトの設計業者・サービス事業者としてAlpine銀行にサービスを提供。
事案の概要	• Travelersの被保険者であるAlpine銀行は、同行顧客の極めて機微な情報を保護するために専門的能力を発揮することを期待して、ウェブサイトの設計とサービスを被告に委託。 • 訴状によれば、ウェブサイトがホスティングされるサーバのセキュリティが被告の過失により脆弱なものとなり、外部の攻撃者がAlpine銀行のシステムに不正アクセスする原因をつくった。また、被告の過失により、Alpine銀行はデータ侵害通知義務遵守に多額の資金を費やさなければならなかった。 • Alpine銀行はこれらの損失についてTravelersに保険金を請求し、同社はこれを支払った。訴状によれば、被告は、Alpine銀行の譲受人および代位者であるTravelersに対し、15万4711ドルを超える損失に関する責任を負うとされている。
係争上の争点	1. 被告はAlpine銀行に対して専門家としてどのような注意義務を負っていたか。 2. 被告が銀行のウェブサイトの保守・管理業務に従事する企業に適用される注意基準の範囲内でウェブサイトの保守・管理業務を行うことは、当事者間の合意の暗黙の条件であったと言えるか。 3. 被告により注意義務は十分に履行されたと言えるか。
判旨	• 2015年1月のTravelers側の訴えの後、同年4月に両当事者は「本訴訟を全面的に却下し、各当事者が自己の費用、経費及び弁護士費用を負担する」ことを合意したことが報道されている。具体的な和解条件は不明。 https://www.databreaches.net/travelers-ignition-studio-agree-to-dismiss-lawsuit-over-alpine-bank-data-breach/

[参考] JURY TRIAL DEMANDED
https://s3.amazonaws.com/cdn.orrick.com/files/Travelers-Complaint.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-6. Traveler`s Casual / 双方の主張

HITACHI
Inspire the Next

- 原告側は被告の注意義務違反を指摘しつつ、被告側はイリノイ州法における「経済的損失法理」による主張の無効性を主張していたところ、本訴訟は最終的に双方合意のもと取り下げられた。

	原告側の主張	被告側の主張
訴因① 業務上の過失	• 被告は、専門的な訓練及び知識を持つ専門家によって実行されるべきウェブサイトの保守・サービスに従事していた。 • アルパイン銀行は、専門的なウェブサイトの保守・管理業務に従事するために被告を採用した。 • 被告は同行に対し、ウェブサイトの保守・サービス業務を遂行する上で、専門家としての注意義務を負っていた。 • 被告は同行に対して負っていた注意義務に違反し、損害を与えた。	• イリノイ州法では、左記請求は確立された経済的損失法理(well-established economic loss doctrine)により禁止されており、棄却されるべき。 • 経済的損失法理は、当事者が契約に基づく請求に対して不法行為法を用いて経済的損害を回復することを禁止している。 • 原告の主張する損害は、「個人情報への不正アクセスについて銀行顧客に通知し、個人情報保護法で義務付けられているその他の措置を講じるために支出した資金」であり、経済的損害に該当する。
訴因② 契約違反	• 被告は、ウェブサイトの保守及びサービス」業務を行うことを申し出、同行は被告の申し出を受け入れた。 • 被告が同行のウェブサイトの保守・管理業務に従事する企業に適用される注意基準の範囲内で業務を行うことは、当事者間の合意の暗黙の条件であった。 • 被告は、同行との契約に違反し、注意基準の範囲内にない標準以下の保守・サービス業務を行った。 • 被告の契約違反により、同行は損害を被った。	• 原告訴状における訴因①と②は、同じ基礎事実を採用し、組み込んでいる。 • 訴因①と②を比較すると、②は①を「過失」ではなく「契約違反」という見出しで再表明したものであることがわかる。 • 訴因①に関連する申し立てを裁判所が却下する場合、請求の重複性から、訴因②の却下が正当化される。

[参考] JURY TRIAL DEMANDED
https://s3.amazonaws.com/cdn.orrick.com/files/Travelers-Complaint.pdf
MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS
http://ia804701.us.archive.org/20/items/gov.uscourts.ilnd.305690/gov.uscourts.ilnd.305690.21.0.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-7. Solarwinds / 事案の概要

HITACHI
Inspire the Next

- 2020年に発生した非常に大規模なサイバーインシデントに起因して、Solarwinds社を相手取り、同社の株主が集団訴訟(Class Action)を提起した。

項目	概要
当事者	• 株主：本訴訟の原告。2018年10月18日から2020年12月17日の期間(クラス期間)に被告企業の普通株式を購入またはその他の方法で取得し、それによって損害を被ったすべての人を指す。 • Solarwinds社：本訴訟の被告。テキサス州オースティンに本社を置き、情報技術ネットワークの監視に使用されるソフトウェア製品を提供する企業である。同社の主力製品はOrion Platformであり、自社のネットワークを監視するために政府機関やフォーチュン500企業により広く使用されていた。
事案の概要	• Solarwindsを標的としたサイバー攻撃被害(詳細は割愛)を受け、2021年1月・2月、連邦証券法違反を主張する集団訴訟がテキサス州西部連邦地方裁判所に提起された。原告が提起した主張は以下の通り。 - クラス期間に、セキュリティ管理及び顧客のセキュリティを優先するというコミットメントに関して、被告が多数の誤解を招く発言を行った。 - 被告は表向きのサイバーセキュリティ保護措置を採用しておらず、保護措置に脆弱性があった結果、被告とその顧客は特にサイバー攻撃を受けやすかった。 - 被告によるこれらの虚偽の説明および不作為により、期間中に被告の株式が人為的につり上げられた価格で取引され、2020年12月の一連の情報開示の結果、会社の株価が下落した。
係争上の争点	1. Solarwindsにはセキュリティステートメントで示したサイバーセキュリティ保護が欠如していたか 2. 同社セキュリティステートメントの内容は、虚偽を含み、誤解を招くもので、重要な事実を省いていたか
判旨	• 2022年11月、和解金2600万ドルにて当事者間で合意し、当該和解案は2023年7月に裁判所により承認された。

[参考] Consolidated Class Action Settlement
https://www.solarwindssecuritieslitigation.com/Content/Documents/Consolidated%20Complaint.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-7. Solarwinds / 訴状の概要

HITACHI
Inspire the Next

- 原告はSolarwindsによるセキュリティ対策の欠如や重大な虚偽及び誤解を招く情報公開を指摘。
- 下記の原告側の主張に対して、被告のSolarwinds側は現在も否認を続けている。

原告側の主張

詐欺の概要	当時、投資家は知らなかったが、Solarwindsの社内セキュリティは荒廃しており、同社はホームページ上で公表するセキュリティステートメントを守っていなかった。	同社の幹部は、サイバーセキュリティ管理の不備について認識していた。
		同社が改善を拒否したことで、グローバル・サイバーセキュリティ・ストラテジストが抗議し、辞任した。
		同社は、内部のアップデートサーバーにアクセスするパスワードがインターネットに公開されていることを数年前から認識していた。
		同社にはセキュリティステートメントで記載されたサイバーセキュリティ保護が欠如していた。
	顧客や投資家は、同社がサイバーセキュリティの維持ができていないという点を後から知った。	
	SolarWindsは、クラス期間中に十分なセキュリティ対策が欠如していたことを認めざるを得ない。	
	米証券取引委員会(SEC)、司法省、州検事総長が同社への調査を開始したが、同社は依然として役員報酬を支払っている。	
被告の重大な虚偽及び誤解を招く記述	被告セキュリティステートメントにおける重大な虚偽および誤解を招く記述	セキュリティステートメントには、同社のサイバーセキュリティに関する表明が含まれていたが、これらの表明は虚偽を含み、誤解を招くもので、重要な事実を省いていた。
	同社ウェブサイトにおける被告の重大な虚偽及び誤解を招く記述	同社の他の声明も虚偽で誤解を招くものであり、重要な事実を省略していた。同社は「セキュリティを最優先」とせず、サイバーセキュリティの不備な慣行を維持していた。
	クラス期間を通じて被告が行った重大な虚偽および誤解を招く記述と不作為の継続	同社の重大な虚偽及び不作為により、株価が人為的につり上げられ、隠蔽されたリスクが現実化することにより、株価が下落することは予見可能であった。

[参考] CONSOLIDATED COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS
https://solarwindssecuritieslitigation.com/Content/Documents/Consolidated%20Complaint.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-7. Solarwinds / 争点へのSEC見解

HITACHI
Inspire the Next

- 本事案では、Solarwinds社は、米国証券取引所法及び関連規則への違反という主張がなされた。

本事案にて根拠とされた米国証券取引所法及び関連規則における条文		
1	Section 10(b) 操作的及び 欺瞞的手段	以下に示すいかなる者も、直接または間接を問わず、州際通商、郵便、または全国証券取引所のいかなる手段または設備を用いても、違法とする。 (a) (1) 公共の利益または投資家保護のために必要または適切であるとして委員会が定める規則および規制に反して、政府証券以外の証券の空売りを行うこと、または売買に関連してストップロス注文を使用すること。 (2) (1)は、証券先物商品には適用されない。 (b)国営証券取引所に登録されている有価証券、登録されていない有価証券、または有価証券スワップ契約の売買に関連して、公益または投資家保護のために必要または適切であるとして委員会が定める規則及び規制(＃2参照)に反して、操作的または欺瞞的な装置または仕掛けを使用または用いること。
2	17 CFR § 240.10b-5 操作的及び 欺瞞的手段の採用	以下に示すいかなる者も、直接または間接を問わず、州際通商、郵便、全国証券取引所のいかなる手段または設備を用いても、違法とする。 (a)詐欺の手段、計画、策略を用いること (b)重要な事実について虚偽の陳述をすること、またはその陳述を行った状況に照らして、その陳述を誤解を招かないようにするために必要な重要な事実の陳述を省略すること (c)個人を欺く、または欺くことになるような行為、慣行、商習慣を行うこと
3	Section 20(a) 連帯責任、 誠実の抗弁	(a)連帯責任、誠実の抗弁 本章の規定またはそれに基づく規則もしくは規制の下で責任を負う者を直接的または間接的に支配する者(本事案ではSolarwindsの取締役を指す)はすべて、当該支配者が責任を負う者に対して、当該支配者と連帯して、また当該支配者と同程度に責任を負うものとする。

[参考] Securities Exchange Act of 1934
https://www.law.cornell.edu/wex/securities_exchange_act_of_1934#:~:text=Section%2010%20%28b%29%20%28codified%20in%2015%20U.S.C.%20%C2%A7,of%20any%20%22device%2C%20scheme%2C%20or%20artifice%20to%20defraud.%22

© Hitachi, Ltd. 2024. All rights reserved.

4.2-8. Blackbaud / 事案の概要

HITACHI
Inspire the Next

- 2020年に発生した大規模なランサムウェア感染・情報漏えい事案に起因して、クラウドサービス事業者であるBlackbaud社を相手取り、情報漏えいの被害者が以下を一例とする多数の集団訴訟(Class Action)を提起した。

項目	概要
当事者	• 情報漏えい被害者：本訴訟の原告。2020年2月から5月にかけて、Blackbaud社におけるデータ漏えい事件で個人情報が漏えいしたすべての人物が含まれる。 • Blackbaud社：本訴訟の被告。慈善団体、学校、医療機関などの非営利団体向けのソフトウェア・ソリューションの大手プロバイダーで、クラウドサービス提供者(CSP)として寄付者のエンゲージメントと寄付者データの管理に特化したソリューションを提供している。
事案の概要	• 2020年5月、Blackbaud社にて管理する1万3000人以上(同社の顧客の約4分の1にあたる)に関する100万以上のファイルが不正にアクセスされ、流出したことが判明した。 • 2020年7月16日、Blackbaud社は本件をウェブサイトで公表し、影響を受けた顧客に通知した。投稿と通知の中では、攻撃者が寄付者の銀行口座情報や社会保障番号にアクセスした事実はないとしたが、数日以内に、同社スタッフはそれらが誤りであることを認識した。 • インシデントの発生後、23件のクラスアクション(2020年11月時点)が提起されるとともに、米国証券取引員会(SEC)からの行政処分が検討された。
係争上の争点	1. Blackbaud社において顧客や個人の機微なデータは適切に保護されていたか。 2. 上記インシデントに係るBlackbaud社から顧客または個人への情報開示は適切になされていたか。 3. データ侵害の対象となった個人へと適切に救済措置を講じたか。
判旨	• 多数のクラスアクションへの対応を統合したカルフォルニア州以外の49州と結んだ和解では、4900万5000ドルの和解金の支払い及び後述する対策の実施が課された。 • SECとの和解では、300万ドルの和解金が課された。

[参考] Class Action Complaint
https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/blackbaud-class-action-lawsuit-12aug2020.pdf
Blackbaud To Pay States, DC $49.5M For Data Breach Claims
https://www.law360.com/colorado/articles/1729697/blackbaud-to-pay-states-dc-49-5m-for-data-breach-claims

4.2-8. Blackbaud / 事案の概要

HITACHI
Inspire the Next

- クラスアクションにて原告から提起された訴因の例は以下の通り。

訴因		原告の主張
1	過失	• クラス構成員の個人情報を適切に保護しなかった場合に損害が発生することが予見可能だったにもかかわらず、被告は個人情報を保護する合理的な措置を講じなかった。被告が犯した過失行為及び不作為には、以下が含まれる。 a. クラス構成員の個人情報を保護するための適切なセキュリティ対策を採用、実施、及び維持しなかった b. ネットワークおよびシステムのセキュリティを適切に監視しなかった c. 自社の電子メールシステムに合理的なセキュリティ保護措置を維持する計画があることを定期的に確認しなかった d. クラス構成員の個人情報への不正アクセスを許可した e. クラス構成員の個人情報が漏洩したことを適時に検出しなかった f. ランサムウェア攻撃についてクラス構成員に適時に通知しなかった
2	私事への不当な侵入/プライバシーの侵害	• 被告は、クラス構成員の個人情報を安全に保管することを怠り、当該情報を不正な主体に開示し、利用されたことによって、意図的にクラス構成員のプライバシーを侵害した。
3	明示的契約違反	• 被告は、被告が収集した個人情報を保護する契約上の義務に実質的に違反した。 • 被告は、関連するプライバシーポリシーに記載された条件を含む、明示的な契約の条件に重大な違反をした。 • クラス構成員は、少なくとも、支払ったデータ・セキュリティ保護を伴うサービスの価値と、提供されたサービスの価値の差額に相当する額の損害を被った。
4	黙示的契約違反	• クラス構成員は、被告及び被告の顧客に個人情報を提供する際、被告が情報を合理的に保護することに同意する暗黙の契約を被告と締結した。 • このような黙示の契約を結ぶにあたり、クラス構成員は、被告のデータ・セキュリティ慣行が関連法規に準拠し、業界標準に合致していると合理的に期待した。 • 被告はクラス構成員の個人情報の保護および保護を怠ったため、黙示の契約に違反した。
5	行為自体で成立する過失	• 被告は、クラス構成員の個人情報を保護するための公正で合理的、または適切なデータ・セキュリティ慣行を提供せず、連邦取引委員会法及びグラム・リーチ・ブライリー法に基づくクラス構成員に対する義務に違反した。 • 被告が適用される法規制を遵守しなかったことは、それ自体が過失となる。
6	州データ侵害法違反	• 被告は、クラス構成員の個人情報を含むデータを所有、ライセンス供与、及び管理している。 • 上記の被告の行為は、サウスカロライナ州のデータ侵害法に違反した。

[参考] Class Action Complaint
https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/blackbaud-class-action-lawsuit-12aug2020.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-8. Blackbaud / 争点への裁判所見解

HITACHI
Inspire the Next

- Blackbaud社とカルフォルニア州以外の49州との間でなされた和解には、同社の過失に関する詳細な説明は含まれていなかったものの、実施を求める事項から同社の当時の状況についてある程度推測できる。

項目	実施を求める事項(例)
A. 法令遵守	• 消費者保護法、データ漏洩通知法、HIPAA(医療保険の相互運用性と説明責任に関する法令)プライバシー/セキュリティ規則の遵守 • Blackbaud社の顧客または消費者に対する誤解を招くような虚偽説明の不実施
B. インシデント対応計画	• 書面によるインシデント対応計画の実施、維持 • セキュリティインシデント準備態勢の評価を目的とした年2回以上の演習実施
C. 違反への対応と通知	• 法執行機関及び影響を受ける顧客への通知及び調整や規制当局への通知に関する方針及び手順を含む計画を実施し、維持 • 計画の評価を目的とした年2回以上の演習実施
D. 情報セキュリティプログラム	• 既存の情報セキュリティプログラム及び関連する保護措置の見直し、維持、更新 • NIST SP 800-53 AC-6に準拠した最小権限アクセス、例えばSP 800-207に準拠したゼロトラストアーキテクチャのような適切なアクセス制御の実施 • 法令遵守に関連したガバナンスプロセスの実施に責任を負う責任者(Chief Privacy Officer, Chief Information Security Officer)の設置
E. トレーニング要件	• 必要とされるトレーニングを従業員全員に提供
F. 個人情報及び医療情報の保護措置と管理	• 個人情報を含むバックアップが必要最小限の範囲で保存されるガバナンスプロセスの維持、遵守 • 個人情報及び医療情報を不正アクセスから保護するガバナンスプロセスの維持、定期的な見直し
G. 特定の技術的保護措置と管理	• ネットワークセグメンテーションプロトコル及び関連ポリシーの維持、定期的な見直し • NISTサイバーセキュリティフレームワークに準拠したリスク評価プログラムの実施 • すべての同社製品へ侵入テストを少なくとも年1回実施、社内ネットワークの脆弱性スキャンを毎週実施 • 社内ネットワーク上の監視、ロギング、及び運用の一元化 • 社内ネットワーク及び同社管理デバイス全体にわたるEDRソリューション導入、利用
H. 評価及び報告要件	• 情報セキュリティプログラムの第三者評価実施

[参考] SETTLEMENT AGREEMENT
https://ncdoj.gov/wp-content/uploads/2023/10/FINAL-Blackbaud-Settlement-Agreement-NC-executed.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.2-8. Blackbaud / 争点へのSEC見解

HITACHI
Inspire the Next

- 2020年のランサムウェア攻撃の影響を完全に開示しなかったとして、証券取引委員会(SEC)から提起された告発に対し、300万ドルを支払って和解することに合意した。

1 2020年5月14日に発生したサイバーセキュリティインシデントへの対応

- 2020年5月14日、Blackbaud社は、システムへの不正アクセスを検知し、情報漏えい及びランサムウェア感染を確認した。
- 2020年7月16日、同社はウェブサイト上で初めてインシデントを発表したが、「サイバー犯罪者は……銀行口座情報や社会保障番号にアクセスしなかった」と述べた。
- 一方で、同社は、7月末までに攻撃者が暗号化されていない多数の顧客の寄付者の銀行口座情報と社会保障番号にアクセスしたことを認識したが、この情報を持つ担当者は、情報開示を担当する管理職にこのことを伝えておらず、同社にはそれを保証するように設計されたポリシーや手順もなかった。

➡ **連邦証券取引所法 規則 13a-15(a)に違反**

2 2020年8月4日に提出したForm 10-Q (四半期決算開示様式)

- 2020年8月4日、同社は2020年第2会計四半期のForm 10-Qを提出したが、同文書では、攻撃者が寄付者の機密データを削除したことについて、特に寄付者の社会保障番号と銀行口座番号の流出について言及していない。
- この声明では、その時点で担当者がデータ流出について認識していたにもかかわらず、多くの顧客が暗号化されていない銀行口座と社会保障番号が流出したという重要な事実が省かれている。

➡ **連邦証券取引所法 第17条(a)(2)及び(3)、同法 第13条(a)、規則 12b-20、13a-13に違反**

3 2020年9月29日に提出したForm 8-K (臨時報告書情報)

- 2020年9月29日、同社は本事案に関するForm 8-Kを提出し、「サイバー犯罪者は、銀行口座情報、社会保障番号、ユーザー名および／またはパスワードを意図した暗号化されていないフィールドにアクセスした可能性がある」と初めて認めた。

Blackbaud社は、証券取引法第21条F(g)(3)に従い、300万ドルの民事金銭処罰を証券取引委員会(SEC)に支払う。

[参考] SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors
https://www.sec.gov/news/press-release/2023-48

© Hitachi, Ltd. 2024. All rights reserved.

[参考] 米国証券取引所法及び関連規則の参考条文

HITACHI
Inspire the Next

- 本事案では、Blackbaud社は、米国証券取引所法及び関連規則への違反という主張がなされた。

本事案にて根拠とされた米国証券取引所法及び関連規則における条文

1	第17条(a)(2)(3) ※15 U.S. Code § 77q 不正な州間取引	(a)詐欺または欺瞞を目的とした州際通商の利用 証券または証券ベーススワップ契約の募集または販売において、州際通商における輸送、通信手段、または郵便を使用して、直接的または間接的に以下のことを行う者は違法とする。 (2) 重要な事実に関する虚偽の陳述、または陳述された状況に照らして誤解を避けるために必要な重要な事実の記載漏れにより、金銭または財産を取得すること (3) 購入者に対する詐欺または欺瞞として機能する、または機能する可能性のある取引、慣行、または事業過程に従事すること
2	第13条(a) ※15 U.S. Code § 78m 定期及び不定期の報告	(a)証券の発行者による報告、内容 証券の発行者は、投資家を適切に保護し、証券の公正な取引を確保するために必要または適切であるとして委員会が定める規則および規制に従って、委員会に以下を提出しなければならない。 (1) 第78l条に従って提出された申請書または登録届出書に記載または添付が義務付けられている情報及び書類を合理的に最新に保つために、委員会が要求する情報および書類 (2) 独立した公認会計士が委員会の規則及び規則で義務付けられている場合はその証明を受けた年次報告書及び委員会が定める四半期報告書
3	§ 240.12b-20 追加情報	陳述書または報告書に明示的に記載が義務付けられている情報に加え、必要な記述がある場合には、それらが作成された状況に照らして誤解を招かないようにするために必要な重要情報を追加しなければならない。
4	§ 240.13a-13 Form 10-Qによる四半期報告書	(a) 本節の(b)及び(c)に規定されている場合を除き、第12条に従って登録された証券を有し、第13条に従って年次報告書を提出する必要があり、かつ、当該報告書を様式10-Kにより提出した、または提出する予定であるすべての発行体は、発行体の各会計年度の最初の3四半期ごとに、その一般教示A.1に指定された期間内に、様式10-Qによる四半期報告書を提出しなければならない。
5	§ 240.13a-15 管理及び手続	(a) 資産担保証券発行体、フォームN-5で登録された中小企業投資会社、または1940年投資会社法に定義されるユニット型投資信託は、開示統制と手続を維持しなければならず、発行体が前会計年度について同法第13条(a)項もしくは第15条(d)項に従って年次報告書を提出する必要があった場合、または前会計年度について委員会に年次報告書を提出していた場合は、財務報告に係る内部統制を維持しなければならない。

[参考] Securities Exchange Act of 1934
https://www.law.cornell.edu/wex/securities_exchange_act_of_1934#:~:text=Section%2010%20%28b%29%20%28codified%20in%2015%20U.S.C.%20%C2%A7,of%20any%20%22device%2C%20scheme%2C%20or%20artifice%20to%20defraud.%22

HITACHI
Inspire the Next

4.3 その他

© Hitachi, Ltd. 2024. All rights reserved.

4.3-1. 発注者及びITベンダー間の責任分界に係る示唆

HITACHI
Inspire the Next

- 今回調査を実施した範囲では、大阪急性期・総合医療センター報告書における「法的な視点」による提言が、発注者及びITベンダー間の責任分界の改善を図るうえで示唆的であった。

1 契約書におけるあいまいな表現を具体的な表現に変えるべき

- 法令からみると、保守契約においては、いわゆる善管注意義務に違反したか、債務不履行があったか、不法行為の要件である「過失」があったかなどが責任の所在を決める基準だが、これらはいずれも抽象的な基準で具体的には適用するのは難しい場合が多い。
- 本事案においても、単に「ガイドラインに従う」と記載するだけで、個々の当事者がどこまでのことを行うべきであったかが判然としていない点があったところ、以下のような点について誰が責任を負うかについて具体的に記載をしていれば事故が防げた可能性があるので、今後の契約における改善が望まれる。

  1. セキュリティ設定、2. 強固なパスワードの設定、3. ロックアウトの設定、4. 管理者権限をもつものを最小限にする、
  5. サプライチェーンも含めた（外部接続）監視、監督、6. 安全なリモート接続の設定、監査、7. OS、アプリケーションのバージョン管理

2 契約後の変化に対応できるための規定を入れるべき

- 契約書締結時点にはなかったセキュリティのリスクが契約締結後に発生し、その点における手当のなさから事故につながった可能性がある。そこで、契約後の変化に対応することについての取り決めを行う必要がある。例えば以下のようなことを記載すべき。

  1. インシデント予防のためのアドバイス、情報提供、情報には以下のようなことを入れることが考えられる
     (1) 政府機関（省庁、NISC）、JPCERT コーディネーションセンター、IPA が注意喚起したセキュリティリスク
     (2) 国内 ISAC、セキュリティ関連団体が注意喚起したセキュリティリスク
     (3) OS、アプリケーションソフトのバージョンアップ情報
  2. インシデント発生時のベンダーの協力体制

3 契約を遵守するための体制

- 本事案においても、契約書に書いていることを遵守しているかのチェックが徹底していなかった。その結果リスクにつながる契約の不遵守を見落とし、あるいは、不遵守に気が付いても一方の当事者は相手に遵守を求めることを行っていなかった可能性がある。
- 今後の契約書には、契約書の遵守を確保するための規定が必要であることが望ましい。例えば、定期的に第三者による監査を行うことについての規定が考えられる。その結果、リスクの早期発見、対処につながると思われる。

[参考] 地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 調査報告書
https://www.gh.opho.jp/pdf/report_v01.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.3-2. 日医総研報告書における主張の実現可能性等に係る検討(1/2)

HITACHI Inspire the Next

- システムベンダーに対し、「信義則」違反を理由に一定の責任を問える可能性を完全に否定することは困難と思われるが、結果として「結局誰も適切な対応を行わない」状況を助長する可能性もあり得る。

箇所	報告書の主張	主張の妥当性・実現可能性等
4-1	保守契約に、システムベンダーの情報提供義務が明記されていることは少なく、保守契約上の善管注意義務違反を理由にシステムベンダーの責任を問えるケースは、実態としては極めて少ない。	• 日医総研の他の検討*にもあるように、保守契約にシステムベンダーの情報提供義務が明記されていることが少ない点は妥当と言える。 *医療機関へのサイバー攻撃の事例研究：民間病院・診療所の被害事例に学ぶ (https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136-1.pdf) • 契約上ベンダーの責務として明記されている場合で実施がない場合に契約不履行となる点は争いがないが、契約に記載がない場合は基本的には責任を負わない。 • 他方、東京地判平26.1.23(平23ワ32060) のように、当時の技術水準に沿ったセキュリティ対策を施すことが黙示的に合意されているとみなされたケースも存在しており、契約上明記のない全てのケースでベンダーが責任を負わないと言い切ることも困難と考えられる。
4-2	医療機関と医療情報システムの保守契約を結び Fortinet製VPN装置を設置したシステムベンダーから、医療機関に対し当該装置の脆弱性に関する情報提供がなされないまま、当該装置の脆弱性を突いたサイバー事故が発生した場合には、医療機関から保守契約の当事者であるシステムベンダーに対し、「信義則」違反を理由に一定の責任を問える可能性がある。 特定類型のサイバー事故で患者等の個人情報漏洩が発生し、医療機関が患者等に対し損害賠償責任を負ったことにより医療機関に発生した損害についても、考え方は上記同様である。	• 既に攻撃手法が知られて実際に被害も発生しているような顕在化率が極めて高い状況下における信義則違反の成立を完全に否定することは困難だが、以下について検証を行う必要がある。 - 規模の大小があるところ、あらゆる医療機関が対象となるか。 - 医療機関等とシステムベンダーとの間でいかなる内容を有する契約がある場合に情報提供義務が課され得るか。 - システムベンダーはセキュリティに関する専門業者と言えるか。 - 仮に情報提供義務が成立するとして、どのような情報が義務的な提供対象となるか。 • 一方で、契約に明記せずにベンダー側の責任を問うという状況は、大阪急性期・総合医療センターで指摘される「契約の規定があいまいで、セキュリティ対策について、誰が何を行うべきかが曖昧になり、お互いに相手がやってくれると期待し、結局誰も適切な対応を行わない」状況を助長する可能性もあり得る。

[参考] サイバー事故に関し システムベンダーが負う責任：医療DXを推進するために
https://www.jmari.med.or.jp/result/other/post-3766/

© Hitachi, Ltd. 2024. All rights reserved.

4.3-2. 日医総研報告書における主張の実現可能性等に係る検討(2/2)

HITACHI Inspire the Next

- 「５．今後の課題と提言」で示される提案についても、主張の妥当性・実現可能性等について以下のように一定の検討を行った。

箇所	報告書の主張	主張の妥当性・実現可能性等
5	装置のセキュリティ上の脆弱性が指摘されているFortinet製VPN装置(CVE-2018-13379)が設置されている全ての医療機関に対し、個別に注意喚起することで、事故の回避を図ることが急務	• 有効な取組みと考えられるが、未端の機関までどのように情報を行きわたらせるかは課題と思われる。また、情報提供を受けても、医療機関側で事故の回避に必要な対応がなされるかは未知数。
	行政には、システムベンダー側に対しても、システムベンダー自身の責任として適正に対処するよう指導することを期待	• 行政からの指導以前に、適正に対処すべきシステムベンダーの責任が何かという整理が必要。
	医療機関に発生する保守契約料金増額相当の資金面での支援(診療報酬上の加算等)を、行政が積極的に行うべき	• 運用費用は継続的に支出されるため、一時的な補助金ではなく、診療報酬上の加算等のより持続性のある取組みが必要。 • 一方で、診療報酬への加算とするのが適切か、診療報酬に加算するとして広範なセキュリティ対策のどこまでを支援対象とするかについては議論が残ると思われる。
	システムベンダーからのサイバーセキュリティ対策関連サービスの提供を保守契約上に明記した際の費用負担を行政による支援(診療報酬上の加算等)で行うべき	
	システムベンダーの「経済産業省ガイドラインの遵守」を明記した保守契約を標準形とする取組から着手し、従来型契約に追加されるサービスを「当リスクにかかる情報提供」に限ることで料金の増額を抑える一方で、将来に亘り毎年発生し続ける費用であることを鑑み、当該増額相当を公的支援の対象とすることも一案	• 「経済産業省ガイドラインの遵守」を明記した保守契約が従来の標準形ではない場合がある可能性もあり、その場合は「経済産業省ガイドラインの遵守」により生じる追加項目を「当リスクにかかる情報提供」には限定できず、ベンダーとしてはユーザーである医療機関等に負担を求めるしかない。 • 公的支援の対象となり得るかという点については上記参照
	システムベンダーにおいてもサイバーセキュリティ問題の意識が高まる中で、保守契約上に不可抗力条項を採用したいとの申し入れを医療機関が受ける可能性があるが、同条項があると、システムベンダーの信義則違反の判定結果に影響を及ぼす可能性があると考えられるので、医療機関としては慎重な対応が必要である。	• 同条項がなければ高度な攻撃を受けた際であってもシステムベンダー側が免責を得ることは事実上困難であり、ベンダー側には採用の動機が強くなる。 • ベンダー側で十分なセキュリティ対策を実施してない場合には免責条項は無効となる。

[参考] サイバー事故に関し システムベンダーが負う責任：医療DXを推進するために
https://www.jmari.med.or.jp/result/other/post-3766/

© Hitachi, Ltd. 2024. All rights reserved.

4.3-3. 提起された論点に対する見解の比較分析(1/2)

HITACHI
Inspire the Next

- 医療機関等とベンダーとの責任分界について、日医総研報告書にて契約に明記されていない場合であってもベンダー側に情報提供義務を課す類の主張がなされる一方で、大阪急性期・総合医療センター 調査報告書では契約中に該当する事項を含めて明記して責任分界の明確化を図るという論調であった。

日医総研報告書	大阪急性期・総合医療センター 調査報告書
医療機関等とベンダーとの責任分界について	
• システム保守契約において、当リスクにかかるシステムベンダーの情報提供義務が明記されていないとしても、医療機関とシステムベンダーのセキュリティに関する専門性の格差を鑑み、既に攻撃手法が知られて実際に被害も発生しているような顕在化率が極めて高い状況下では、システムベンダーは医療機関等に対し、委託契約又は信義誠実の原則(信義則)に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務を負うと考える。 • このような特殊事情が認められない環境下でのサイバー事故について、医療機関とシステムベンダーとの責任関係の判断基準は今後の研究課題である。	• 今回の最大の課題は、医療機関としてセキュリティの重要性を再認識し、医療機関とベンダーの責任分界点を明確にすることである。 • 契約書に誰が何をやるべきかが網羅的に書いてあれば、事故が起こる前に、責任を負うべき当事者が何をやらなければならないかに気付くため、事故が起こるリスクを低減できる。 • 本事案においても契約書締結時点にはなかったセキュリティのリスクが契約締結後に発生し、その点における手当のなさから事故につながった可能性がある。そこで、契約後の変化に対応することについての取り決めを行う必要がある。
追加対応費用の有無について	
• システムベンダーとしては応分の保守契約料金の増額を医療機関に対して求めることが予想される。 • システムベンダーの「経済産業省ガイドラインの遵守」を明記した保守契約を標準形とする取組から着手し、従来型契約に追加されるサービスを「当リスクにかかる情報提供」に限ることで料金の増額を抑える	• 特に関連する記載なし

[参考] サイバー事故に関し システムベンダーが負う責任：医療DXを推進するために
https://www.jmari.med.or.jp/result/other/post-3766/
大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 調査報告書
https://www.gh.opho.jp/pdf/report_v01.pdf

© Hitachi, Ltd. 2024. All rights reserved.

4.3-3. 提起された論点に対する見解の比較分析(2/2)

HITACHI
Inspire the Next

- 対応費用の負担主体について、日医総研報告書では診療報酬加算等の国による負担が望ましいとする一方、大阪急性期・総合医療センター 調査報告書ではその可能性も認めつつ慎重な議論が必要という見解が示されていた。

日医総研報告書	大阪急性期・総合医療センター 調査報告書
対応費用の負担主体について	
• 対策に要する費用負担の問題が原因で、両者の円滑な関係構築を阻害するような事態は、絶対に避けなければならない。ついては、上記費用負担を行政による支援(診療報酬上の加算等)で行うべき。 • まずはシステムベンダーの「経済産業省ガイドラインの遵守」を明記した保守契約を標準形とする取組から着手し、従来型契約に追加されるサービスを「当リスクにかかる情報提供」に限ることで料金の増額を抑える一方で、将来に亘り毎年発生し続ける費用であることを鑑み、当該増額相当を公的支援の対象とすることも一案と考える。	• 需要と供給によって価格設定ができるような事業のやり方は医療機関ではできない。これは医療安全および安定した医療を継続的に提供するために、法律によって定められた公定価格である「診療報酬」でしか、基本的に医療機関は収益を上げられないからである。 • この診療報酬改定を行ってでも医療機関のセキュリティ強化に資源を割くことはできるかもしれないが、診療報酬を改定するということは、国民の負担が増えることであり、国民的な議論に発展することを忘れてはならない。 • サイバー攻撃による大規模システム障害は「災害」と同様に捉え、DMAT 同様の初動チームの編成、緊急財政出動、各種要件の緩和、また、そもそもこのような災害が起きないために、基盤となるセキュリティ対策費用の診療報酬以外の手段での供給も必要である。
その他のセキュリティ向上等を目的とした解決策の提案について	
• 特に関連する記載なし	• 医療機関においても各自でセキュリティを検討し、例えば、ファイアウォールを個別に設定したり、管理させたりするのではなく、包括的な枠組みと体制が必要である。国や自治体レベルでセキュリティ機能を集約したり、医療サービスにおける共通プラットフォームを確立したりするなどの検討を、厚生労働省に限らず、国全体で国民の命を守るための医療機関のセキュリティ体制の検討が必要である。

[参考] サイバー事故に関し システムベンダーが負う責任：医療DXを推進するために
https://www.jmari.med.or.jp/result/other/post-3766/
大阪急性期・総合医療センター 情報セキュリティインシデント調査委員会 調査報告書
https://www.gh.opho.jp/pdf/report_v01.pdf

© Hitachi, Ltd. 2024. All rights reserved.


Hitachi Social Innovation is
POWERING GOOD