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

令和 5 年 3 月 31 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 5

1.3　実施スケジュール 10

1.4　実施体制 10

1.5　本調査報告書の構成 11

2　サイバー空間におけるつながりの信頼性及び 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についての調査 12

2.1 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についての調査 12

2.2 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についての調査 13

3　CPSF 等に基づく国際規格(TS 等を含む)の推進 16

3.1　本事業項目の目的 16

3.2　本事業項目の実施内容 16

3.3　本事業項目の実施結果 16

4　ガイドライン等の普及・啓発の推進 32

4.1 本事業項目の目的 32

4.2 本事業の実施内容 32

4.3 本事業項目の実施結果 32

エクゼクティブサマリー

・ 経済産業省では、これまでサプライチェーンのサイバーセキュリティ強化に向けて、「Society5.0」における新たな形のサプライチェーンに求められるセキュリティ対策の全体像を整理した「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)を策定した。また、分野別のサイバーセキュリティガイドラインの作成や「IoT セキュリティ・セーフティ・フレームワーク」(IoT-SSF)、「データによる価値創造を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク」(DMF)などを策定してきた。

・ 「Society5.0」における産業社会では、様々なモノやサービスがつながる中で、信頼できる主体が生成・加工したとは必ずしもいえないデータによる産業活動が想定されるため、サイバー空間におけるデータの信頼性確保は重要な課題となる。また、サイバー空間とフィジカル空間の境界で交換される情報が正確に転換すること、つまり境界上における“転写”機能を担う IoT 機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえ、IoT 機器等に求められるセキュリティ対策やリスクアセスメントの考え方等についても更なる検討が必要である。さらに、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みでは十分ではなく、諸外国との連携を強化し、我が国の取組みを積極的に国際標準に提案するなど、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みを進めていく必要がある。

・ 本事業では、研究会及び各 WG 等の議論を踏まえ、各国政府の取組みやその他国内外のセキュリティ等に関する文献等を調査し、サイバー空間におけるつながりの信頼性及び 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した。また、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・啓発活動を推進した。

・ 本事業項目(1)「サイバー空間におけるつながりの信頼性及び 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についての調査」では、IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取組み等や IoT 機器等のセキュリティ対策等について、日本、米国、欧州、中国の公開情報等を調査し整理した。また、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標準化団体、業界団体及び外国政府の取組み等やデータのセキュリティ対策等について、日本、米国、欧州、中国、インド、シンガポール、ベトナムの公開情報等を調査し整理した。

・ 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みが進められており、米国では、民間事業者における自発的な取組み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み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みが進むものの、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 Frow 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。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。

・ 本事業項目(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又は政府関連機関、業界団体、標準化団体等によるルール形成の取り組み状況等の調査や、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。

・ 本事業項目(3)「ガイドライン等の普及・啓発の推進」においては、IoT-SSF と DMF の改善に向けた課題の整理や事例の蓄積を目的として、適用実証を実施し、「IoT-SSF 適用実証報告書」と「DMF 適用実証報告書」を作成した。また、適用実証の結果と対応する TF の委員から得た意見を反映し、「IoT-SSF 適用手順書」と「DMF 適用手順書」を作成した。

・ IoT-SSF の第 3 軸の第 3 の観点「機器・システムの運用・管理を行う者の能力に関する確認要求」及び第 4 の観点「その他、社会的なサポート等の仕組みの要求」を更に具体化する目的で、適用実証に参画した団体や関連サービス提供事業者、民間・公共団体に対して IoT-SSF の第 3 軸(第 3 の観点及び第 4 の観点)の具体化に関するヒアリング調査を行った。今後、IoT セキュリティの技術者確保やサイバー関連のリスクを補償範囲とする保険の普及に係る議論を踏まええつつ、IoT セキュリティ人材のモデル化や重大なサイバーインシデントによる被害を受けた事業者に対する一時的な金銭的支援に関する枠組みの構築について検討を行うことが望まれる。

・ IoT-SSF の適用が有効性を検証するため、過去に発生したインシデント事例を対象として IoT-SSF の有効性を検証した。事前の IoT-SSF によるリスクアセスメントの実施は有効に機能することを確認した。

・ 製造業及びその関連産業における CPSF 等に基づくガイドライン等の認知・普及状況のアンケート調査を実施し、アンケート回答者のうち一定の条件に基づいて抽出されたものを対象にヒアリング調査を実施した。CPSF/IoT-SSF/DMF の認知率・利用率は、サイバーセキュリティ経営ガイドラインや ISMS のそれよりも低かった。効率性等の観点から外部団体(業界団体、IT 事業者)からの情報提供のメリットを指摘する事業者が大企業、中小企業の双方で見られた。ガイドライン等の普及にあたっては、業界団体や IT 関連事業者、取引先からの情報提供が一定の役割を有しているところ、それらの団体との協調が念頭に置かれるべきである。係るチャネルを利用したガイドライン等の普及の優先度が高いのではないかと考えられる。

1 本事業の概要

1.1 目的

我が国では、AI や IoT、ビッグデータなど、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「Society5.0」の実現を目指している。「Society5.0」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新たな攻撃の機会ともなっていくおそれがある。

サイバー攻撃の起点は急激に拡大し、攻撃の手法も高度化しており、サイバー攻撃の脅威は、あらゆる産業活動に潜むようになっている。このような状況においては、各企業における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みでは十分ではなく、諸外国との連携を強化し、我が国の取組みを積極的に国際標準に提案するなど、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みを進めていく必要がある。

このような背景を踏まえ、経済産業省では、平成 29 年 12 月に、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会」(以下、「研究会」という。)を立ち上げた。そして、同研究会の下に専門的な議論を行う 3 つのワーキンググループ(以下、「WG」という。)を設置し、「制度・技術・標準化」、「経営・人材・国際」及び「サイバーセキュリティビジネス化」のテーマ毎に議論を進めてきている。

特に、サプライチェーンのサイバーセキュリティ強化に向けては、「制度・技術・標準化」WG にて、「Society5.0」における新たな形のサプライチェーンに求められるセキュリティ対策の全体像を整理した「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。)を平成 31 年 4 月に策定した。CPSF では、「Society5.0」における産業社会を 3 つの層(企業間のつながり(第 1 層)、フィジカル空間とサイバー空間のつながり(第 2 層)、サイバー空間におけるつながり(第 3 層))に整理し、セキュリティ確保のための信頼性の基点の明確化を行った。加えて、CPSF の考え方を産業活動に実装するために、産業活動の実態に応じて、必要な対策要件や対策水準について検討を行う産業分野別のサブワーキンググループ(ビルサブワーキンググループやスマートホームサブワーキンググループ等。以下、まとめて「産業分野別 SWG」という。)に加えて、産業分野共通の課題を検討する分野横断 SWG、タスクフォース(以下、「TF」という。)等を立ち上げ、分野別のサイバーセキュリティガイドラインの作成や「IoT セキュリティ・セーフティ・フレームワーク」(以下、「IoT-SSF」という。)、「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」、「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。)などを策定してきた。

「Society5.0」における産業社会では、様々なモノやサービスがつながる中で、信頼できる主体が生成・加工したとは必ずしもいえないデータによる産業活動が想定されるため、サイバー空間におけるデータの信頼性確保は重要な課題となる。CPSF では、第 3 層の信頼性の基点をデータとした上で、データの信頼性を確保するための対策要件及び対策例を提示しているが、実際の産業活動への実装に向けて、産業活動におけるデータの区分やデータ利活用の実態を踏まえた上で、より具体的な対策要件やデータの完全性や真正性を確認する仕組みとしてどのような手法やルールが効果的か、その実効性や国際的な動向も踏まえた上で更なる検討が必要である。また、CPSF では、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の中で、サイバー空間とフィジカル空間の境界で交換される情報が正確に転換すること、つまり境界上における“転写”という役割に焦点を当て、第 2 層の信頼性の基点を転写機能とした上で、転写機能の信頼性を確保するための対策要件及び対策例を提示しているが、転写機能を担う IoT 機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえ、IoT 機器等に求められるセキュリティ対策やリスクアセスメントの考え方等について更なる検討が必要である。

サプライチェーンのサイバーセキュリティ強化に向けては、各国に取組みがある。例えば、欧州では、令

和 2 年 12 月、欧州委員会が、域内の重要インフラ事業者等のサイバーセキュリティ対策について規定する「ネットワークおよび情報システム指令」の改定案を公表し、ICT サプライチェーンにおけるセキュリティへの対応を明記するなど、規制が強化されている。また、米国では、令和 3 年 5 月に署名された大統領令に基づき、政府調達のソフトウェアサプライチェーンセキュリティの対策強化に向け、Software Bill of Materials(以下、「SBOM」という。)の提供を含む基準作りが進められているほか、令和 3 年 12 月には国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁が SBOM に関するイベントを開催し、今後の課題検討を推進していくことを発表する等など、SBOM に係る取組みが加速化している。このような状況下で、日本が国際的なサイバーセキュリティ対策のルールメイキングに主導的な役割を担えるようになるためにも、日本からサイバーセキュリティ対策の枠組みを提案することが重要である。

本事業では、研究会及び各 WG 等の議論を踏まえ、各国政府の取組みやその他国内外のセキュリティ等に関する文献等を調査し、サイバー空間におけるつながりの信頼性及び 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の検討及び CPSF 等に基づく国際規格(TS 等を含む。)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表 1-1 に示す。

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	サイバー空間におけるつながりの信頼性及び 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についての調査	【事業内容】 本事業では、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するために求められる外国政府の取組みやその他国内外のデータのセキュリティ対策やIoT機器等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、4⑥に示すTF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及びIoT機器やシステム等のセキュリティ確保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やIoT機器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、普及状況など) ●データやIoT機器等の差異や区分(カテゴリ)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 ●データやIoT機器等の信頼性を確認するための技術的又は制度的枠組	IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取り組み等や IoT 機器等のセキュリティ対策等について、日本、米国、欧州、中国の公開情報等を 11 件調査し、本調査報告書にまとめた。 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標準化団体、業界団体及び外国政府の取り組み等やデータのセキュリティ対策等について、日本、米国、欧州、中国、インド、シンガポール、ベトナムの公開情報等を 21 件調査し、本調査報告書にまとめた。

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		また、上記調査の結果及び4.⑥に示すTFでの議論の内容について、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するための具体的なセキュリティ対策要件等を今後策定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。 なお、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が、例えば、以下に示す論点を含むこととする。 ＜調査報告書における論点の例＞ ●データやIoT機器等の区分(カテゴリ)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やIoT機器等の信頼性の確認方法 ●データマネジメントの考え方 【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などを目的として、必要に応じてデータやIoT機器等のセキュリティに精通した有識者(国外の有識者を含む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。 ・調査の際は、CPSFの関係項目や国際動向とのハーモナイゼーションを常に考慮しながら、データ やIoT機器等の区分(カテゴリ)及びそれらに応じたセキュリティ対策例や信頼性の確認方法や、データマネジメントの考え方等について整理を行うこと。	
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み状況や、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＞	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ドラフト文書の作成、提案及びPWI(予備業務項目)としてのプロジェクト推進、その

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		●CPSF等に基づく国際規格(TS等を含む。)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・関係者の巻き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(TS等を含む。)策定に向けたドラフト文書の作成、およ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 【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等により実施する。調査結果の妥当性確認などを目的として、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。ヒアリング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。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(ISO Meetings等。対面での会議を2回程度、その他複数回の電話会議等を想定。)に参加して日本の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うこと。 ・ 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、英語での意見交換の場合の議事概要は日本語に翻訳する。 ・ CPSF等に基づく国際規格(TS等を含む)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。	他必要に応じて国内外の関係者との意見交換を行った。 　また、国際標準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、政策文書等について、日本、米欧、シンガポールなどが提案している8件を調査した。
3	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、4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	IoT-SSFとDMFの改善に向けた課題の整理や事例の蓄積を目的として、適用実証を実施し、「IoT-SSF適用実証報告書」と「DMF適用実証報告書」を作成した。また、適用実証の結果と対応するTFの委員から得た意見を反映し、「IoT-SSF適

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		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	用手順書」と「DMF適用手順書」を作成した。 IoT-SSFの第3軸の第3の観点及び第4の観点を更に具体化する目的で、適用実証に参画した団体や関連サービス提供事業者、民間・公共団体に対してIoT-SSFの第3軸(第3の観点及び第4の観点)の具体化に関するヒアリング調査を行った。 IoT-SSFの適用が有効性を検証するため、過去に発生したインシデント事例を対象としてIoT-SSFの有効性を検証した。 製造業及びその関連産業におけるCPSF等に基づくガイドライン等の認知・普及状況のアンケート調査とヒアリング調査を実施した。
4	研究会、各WG、分野横断ＳWG及びTFの運営	【事業内容】 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(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3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り組みを議論する。研究会の構成員(10名程度)は、産学を代表する有識者とし、担当者が指定する。令和4年度中に2回程度開催する。 ②WG1(制度・技術・標準化) 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。令和4年度中に2回程度開催する。 ③WG2(経営・人材・国際)	研究会、WG及び2つのTF(『第2層：フィジカル空間とサイバー空間のつながり』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(第2層TF)、『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(第3層TF)、について、構成員との日程調整、開催案内(出欠確認)、資料準備等といった事務的な業務を全て行った。また、第2層TF及び第3層TFにおいて、資料の作成及び経済産業

Ｎｏ	事業項目	仕様書の内容	具体的な実施内容
		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。令和4年度中に2回程度開催する。 ④WG3(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。令和4年度中に2回程度開催する。 ⑤分野横断SWG WG1の下に設置し、産業分野に共通する課題について議論する。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。令和4年度中に2回程度開催する。 ⑥特定課題の検討TF 2つの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及び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を議論する。各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。令和4年度中に各TF2回程度開催する。 なお、産業分野別SWGの運営は、他の委託事業や他府省庁、民間団体等において実施されているため、本事業の対象外とする。 【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3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、経済産業省担当者の指示に基づき行う。なお、実施に係る経費については事業費に計上する。 ・4⑥のTFのうち、1の調査に基づく議論を行うTFにおいて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り組みの海外発信の観点に基づき、経済産業省担当者が指示する資料について英訳を行う。	省担当者への報告を行った。

1.3 実施スケジュール

本事業の実施スケジュールを図 1-1 に示す。「サイバー空間におけるつながりの信頼性及び 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」「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、検討 TF における検討や助言を踏まえて検討を推進した。

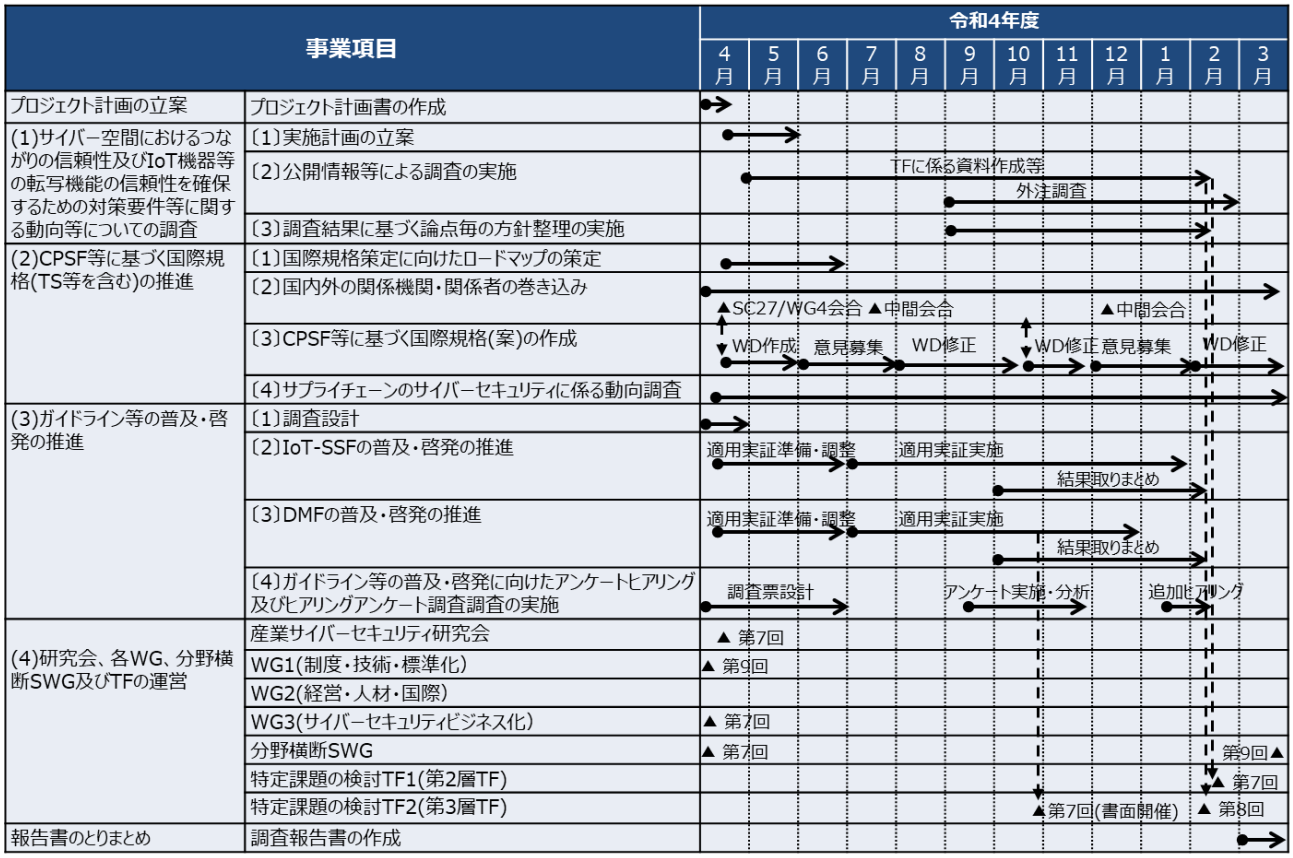


図 1-1 本事業の実施スケジュール

1.4 実施体制

本事業は、プロジェクトオーナーである経済産業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)、事業項目(3)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を踏まえながら推進した。本事業の実施体制を図 1-2 に示す。

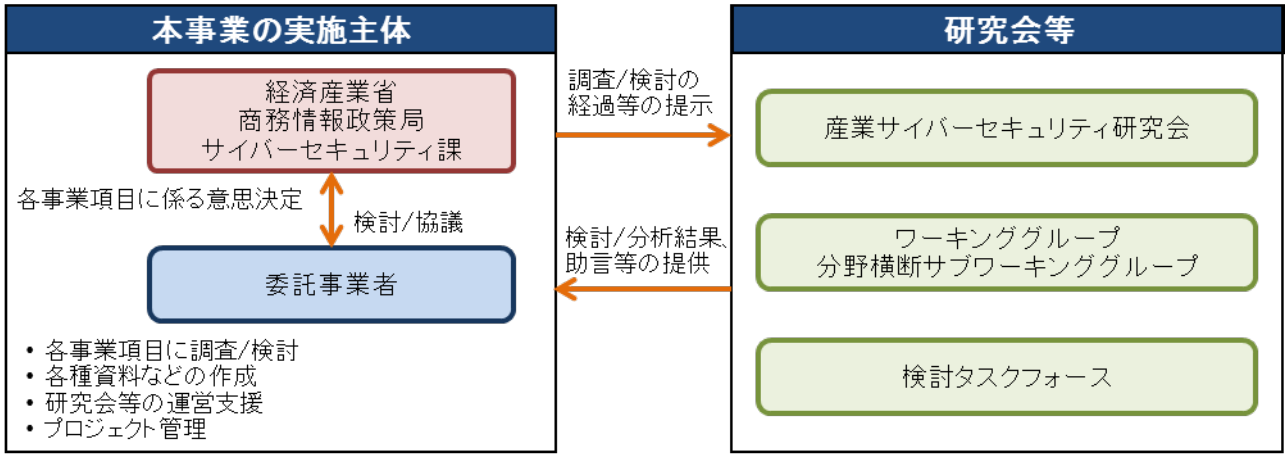


図 1-2 本事業の実施体制

1.5 本調査報告書の構成

本調査報告書では、「サイバー空間におけるつながりの信頼性及び 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、「サイバー空間におけるつながりの信頼性及び 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についての調査」の目的、実施内容、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、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、実施結果を報告する。

2　サイバー空間におけるつながりの信頼性及び 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についての調査

2.1 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についての調査

2.1.1 本事業項目の目的

本事業項目では、IoT 機器等の転写機能の信頼性を確保するため、転写機能を担う IoT 機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえて、IoT 機器等に求められるリスクアセスメントの考え方やセキュリティ対策等について整理することを目的とした。

2.1.2 本事業項目の実施内容

上記目的を達成するため、IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び各国政府の取り組み等や IoT 機器等のセキュリティ対策、及びそれらの信頼性の確認手法等について、公開情報等を調査し整理した。

2.1.3 本事業項目の実施結果

（１） 公開情報等の調査

本事業の調査対象を表 2-1 に示す。詳細な調査結果は別紙 1 を参照されたい。

表 2-1 調査対象一覧

No	国	文書名
1	日本	電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン
2		セキュリティ知識分野(SecBoK)人材スキルマップ 2021 年版
3	米国	国家サイバーセキュリティの向上に関する大統領令(Executive Order on Improving the Nation's Cybersecurity)
4		消費者向け IoT 製品のサイバーセキュリティ・ラベルの推奨規準(Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products)
5	欧州	サイバーセキュリティ認証 EUCC スキーム候補(EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0)
6		ETSI TS 103 701 ベースライン要求事項の適合性評価(ETSI TS 103 701 Conformance Assessment of Baseline Requirements)
7		欧州サイバーレジリエンス法(Proposal for a REGULATION on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020)
8		機械製品規則(Proposal for a REGULATION on machinery products)
9		無線機器指令(COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021)
10		BSI カイトマーク(BSI Internet of Things Testing, verification and certification solutions for a smarter, more secure world （BSI Kitemark))
11	中国	サイバーセキュリティ審査弁法(网络安全审查办法)

調査結果を地域(欧州、米国、日本及びその他地域)ごとにまとめると以下のようになった。

- 日本では、下記の米欧の動きを受け、米国と同様に民間事業者における自発的な取組み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。2022 年 11 月に産業サイバーセキュリティ研究会のワーキンググループ 3 において「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」が立ち上げられ、IoT 機器・システムに対するセキュリティ適合性評価制度構築に向けて、適用性評価制度の位置づけや対象範囲、適合性評価基準、適合性評価スキームについて検討されている。

- 米国では、規制による IoT 機器・システムのセキュリティ確保ではなく、民間事業者における自発的な取組みの促進を中心とした検討が進められている。2021 年 5 月に署名された「Executive Order on Improving the Nation's Cybersecurity」に基づき、2022 年 2 月に「Recommended Criteria for Cybersecurity Labeling of Consumer Software」、2022 年 9 月に「NISTIR 8425 Profile of the IoT Core Baseline for Consumer IoT Products」が公開された。これらの文書の公開によって、消費者向け IoT 製品のサイバーセキュリティ・ラベリングにおける推奨基準や求められるサイバーセキュリティ能力に係る基準が示された。

- 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みが進められている。2019 年 6 月に施行されたサイバーセキュリティ法に基づき、2021 年 5 月に「EUCC Candidate Scheme V1.1.1」が公表され、機器を対象とした認証制度の具体化が進んでいる。また、分野ごとの垂直的(Vertical)なルールとして 2021 年 4 月には「機械製品規則案」、同年 6 月には「一般製品安全規則案」、2023 年 1 月には「無線機器指令の委任法」が公表され、既存の NLF 関連指令/規則にサイバーセキュリティの要素を盛り込む検討がなされている。また、2022 年 9 月には、分野に跨る水平的(Horizontal)なルールとして「欧州サイバーレジリエンス法案」が公表され、デジタル要素を含む製品のセキュリティ必須要件や製造業者への義務、係る規定に関する罰則等が提案されている。

- 日本以外のアジア地域では、中国において、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。中国サイバーセキュリティ法(35 条)やデータセキュリティ法(24 条)に基づき、2022 年 2 月に「サイバーセキュリティ審査弁法」が施行され、政府が実施する審査に係る申請手続が規定された。また、シンガポールにおいて、欧州各国(ドイツ、フィンランド)と相互認証を得ることでより国際ハーモナイゼーションも考慮しつつ、民間事業者における自発的な取組みの促進によるセキュリティ確保を目的とした仕組み作りが進められており、2020 年 10 月に「Cybersecurity Labelling Scheme」が開始された。

- 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みが進むものの、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。今後、国際間のルールにおける相互運用性の向上や相互認証の構築による事業者の負担を減らす取組みが期待される。

2.2 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についての調査

2.2.1 本事業項目の目的

本事業項目では、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、産業活動におけるデータの区分やデータ利活用の実態を踏まえた上で、より具体的な対策要件やデータの完全性や真正性を確認する仕組みとしてどのような手法やルールが効果的か、その実効性や国際的な動向も踏まえた上

で更なる検討が必要となっているため、データマネジメントにおけるモデルの具体化にあたり、必要となる情報を整理することを目的とした。

2.2.2 本事業項目の実施内容

上記目的を達成するため、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標準化団体、業界団体及び各国政府の取り組み等や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について、公開情報等を調査し整理した。

2.2.3 本事業項目の実施結果

（1） 公開情報等の調査

本事業の調査対象を表 2-2 に示す。詳細な調査結果は別紙 2 を参照されたい。

表 2-2 調査対象一覧

No	国	文書名
1	日本	包括的データ戦略
2		プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0
3	米国	2021 年データ保護法案（Data Protection Act of 2021）
4		SP 800-47 Rev. 1 情報交換のセキュリティ管理 (SP 800-47 Rev. 1 Managing the Security of Information Exchanges)
5	欧州	欧州データ戦略（A European strategy for data）
6		欧州委員会におけるデータガバナンス・データ政策（Data governance and data policies at the European Commission）
7		データガバナンス法（Data Governance Act）
8		データ法案（Proposal for a Regulation on harmonised rules on fair access to and use of data(Data Act)）
9		欧州健康データスペース規則案（Proposal for a Regulation on the European Health Data Space）
10	中国	サイバーセキュリティ法（网络安全法）
11		データセキュリティ法（数据安全法）
12		個人情報保護法（个人信息保护法）
13		GB/T 22240-2020 情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド（Information security technology - Classification guide for classified protection of cybersecurity）
14		データ域外移転安全評価弁法（数据出境安全评估办法）
15		データ越境安全評価申告ガイドライン 第 1 版（数据出境安全评估申报指南）
16		個人情報越境取扱活動安全認証規範（个人信息跨境处理活动安全认证规范）
17		個人情報越境標準契約規定 意見募集稿（个人信息出境标准合同规定）
18	インド	個人データ保護法（Personal Data Protection Bill）
19		非個人データガバナンスフレームワーク（Non-Personal Data Governance Framework）
20	シンガポール	2012 年個人情報保護法（Personal Data Protection Act 2012）
21	ベトナム	個人情報保護に関する政令（Draft Decree on Personal Data Protection）

調査結果を地域(欧州、米国、日本及びその他地域)ごとにまとめると以下のようになった。

・ 日本では、2019 年 6 月の G20 大阪サミットにて提唱された Data Free Frow with Trust(DFFT)というコンセプトのもと、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。データ活用を更に促進させることを目的として、デジタル庁より 2021 年 6 月に「包括的データ戦略」が公表された。また、2023 年 5 月に予定されている G7 会合に向けて、経済産業省にて「データの越境移転に関する研究会」が立ち上げられ、データの越境移転に係る相互運用可能な枠組みについて検討が進められている。加えて、同省より 2022 年 4 月に「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」が公表されており、DFFT も含めたデータの相互流通促進に向けた活用が期待されている。

・ 米国では、欧州ほどルール策定の動きが活発とは言えないものの、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。連邦法レベルでは 2021 年 6 月に「Data Protection Act of 2021」のドラフトが公表され、州法レベルでは 2022 年 7 月に「California Consumer Privacy Act」がカリフォルニア州で施行された。また、２国間・多国間の議論としては、2020 年 7 月に EU 司法裁判所のシュレムスⅡ判決により欧州と米国間の「プライバシー・シールド」が無効になったことを受け、2022 年 3 月に欧州米国データプライバシー枠組み(DPF)が原則合意された。(2022 年 12 月、欧州委員会は DPF の GDPR 上の十分性を認める決定案を発表している。)

・ 欧州では、米国及び中国のメガプラットフォーマー対策も念頭に置きながら、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いる。2018 年 5 月に General Data Protection Regulation(GDPR)が施行され、個人データの保護に関するルールが EEA 内で統一された。また、欧州委員会より 2020 年 2 月に「欧州データ戦略」が公表された後、データ関連法案(「データガバナンス法」、「デジタル市場法」、「デジタルサービス法」、「データ法」)が続々と公表され、EEA 域内のデータ保護とデータ共有に係る仕組みの検討が加速している。また、より実装に近い取組みとして、2020 年 6 月に「GAIA-X」、2021 年 3 月に「Catena-X」の設立が発表され、個人データのみならず産業データも含めた形で技術的なルールの策定とそれに対応した基盤構築の取組みが進められている。

・ 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。中国では、2021 年 9 月に「データセキュリティ法」や 2022 年 9 月に「データ域外移転安全評価弁法」が施行された。データの越境移転に係る具体的な手続きを規定するガイドライン(「データ越境安全評価申告ガイドライン(第 1 版)」、「個人情報越境取扱活動安全認証規範」、「個人情報越境標準契約規定(意見募集稿)」)が 2022 年に公表されている。また、インドでは 2019 年 12 月に「THE PERSONAL DATA PROTECTION BILL,2019」が施行され、国境を越えたデータを行う事業者に対して説明責任が課された。タイでは、2022 年 6 月に「個人情報保護法」が施行され、事業者に越境移転に関する規制が課された。

・ 連邦法の検討が引き続き続いている米国を例外として、GDPR に代表される個人データ保護規制の動きがある程度一巡しているところ、中国等における一部の産業データを対象とした規制の立法化の影響もあり、データの越境移転に関する問題が多くの場面で顕在化している。加えて、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。それらの動きがグローバルにビジネスを推進する事業者にとっての重大な障壁にならないよう、ルールと技術の両面に関して国際的な相互運用性を確保する取組みが官民連携して進められることが期待される。

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

上記目的を達成するため、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) 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・関係者の巻き込みや必要な資料の作成等の実施
(3) 国際規格ドラフト文書の作成及び(2)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に係る動向調査

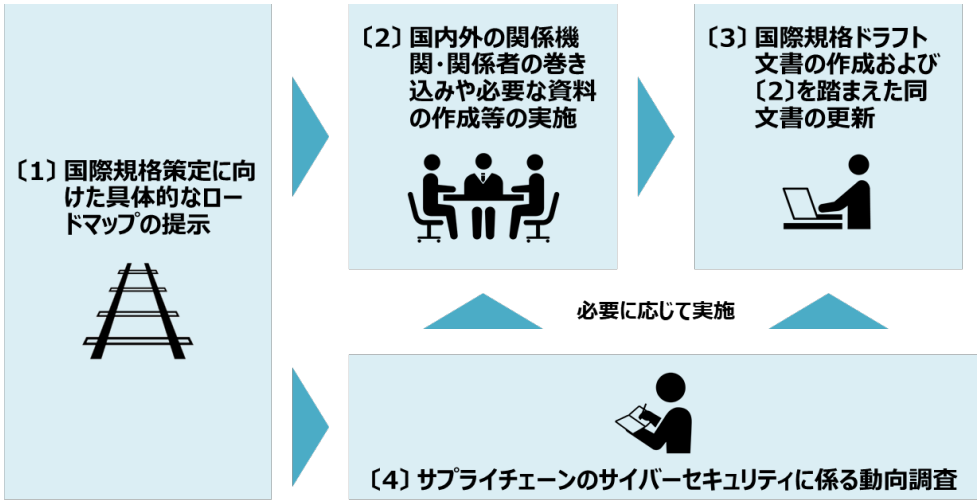


図 3-1　本事業項目の実施プロセス(概要)

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

一般に国際規格は、ISO(国際標準化機構)や IEC(国際電気標準会議)等の機関が規定した標準的なプロセスに則り策定される。当該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)によって異なるため、具体的な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

国際規格の開発及び保守等を実施している代表的な国際標準化機関として、以下が挙げられる。

- ISO(国際標準化機構)
- IEC(国際電気標準会議)
- ISO/IEC JTC 1(ISO/IEC 第一合同技術委員会)
- ITU(国際電気通信連合)

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/SC 27 にて規格化のプロジェクトを立ち上げている。図 3-2 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。

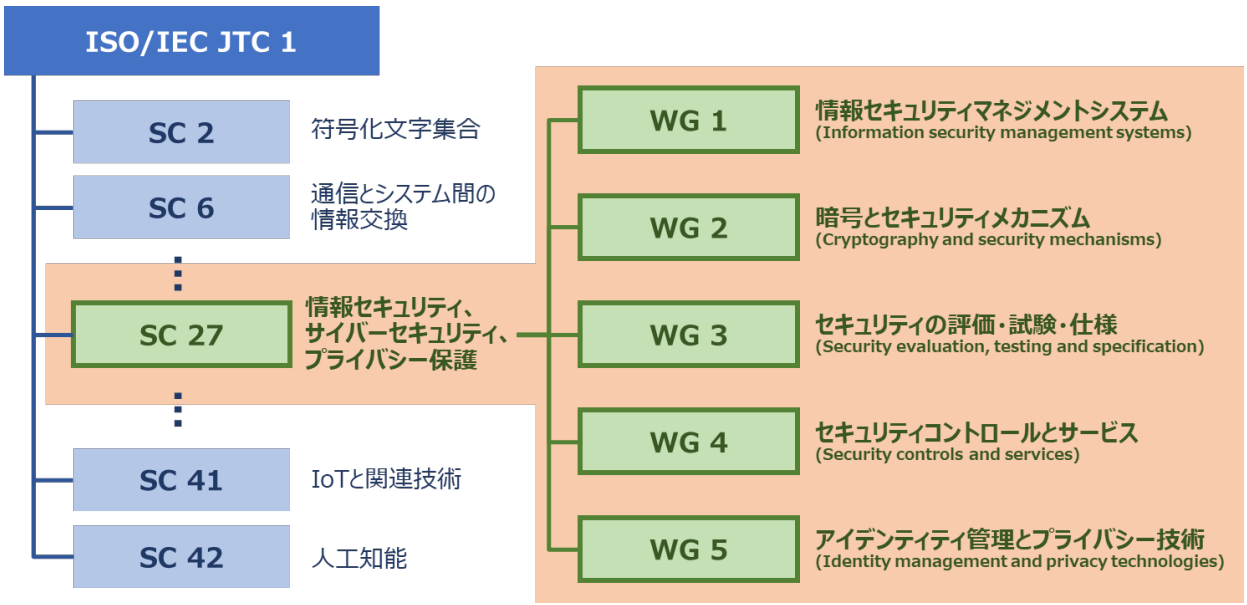


図 3-2 JTC 1/SC 27 の構成

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 systems)という IoT(Internet of Things)とも関連した概念を取扱うのにより適していると考えられる。

■　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 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。

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」では、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 の過半数による承認を通じて新プロジェクトを登録する。

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。

表 3-1 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通り作成した。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、2023 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. 2023 年 3 月時点までの経過

CPSF 等に基づく国際規格策定に向けては、「予備段階」の検討を経て、2022 年 12 月 2 日から 3 月 5 日までの期間で「提案段階」にあたる投票を行った。承認条件が、棄権票を除く 2/3 以上の賛成及び、5 か国以上からの積極的な貢献の表明となる中、賛成 19 票、反対 2 票、棄権 29 票、賛成票を投じた国の中で積極的な貢献の表明を行ったのが 2 か国(日本、ベルギー)となり、賛成多数となったものの結果は否決となった。

上記の投票結果を受け、4 月 7 日に実施された SC 27/WG 会合では、投票結果をレビューするとともに、改めて PWI の提案を行った。その後、PWI として 2 度の意見募集を経て、2023 年 2 月 1 日に実施された中間会合(Interim meeting)にて、本案件を「提案段階」に進め、2 か月の投票にかけることが決議された。期間中の会合の実施状況や議論の内容等については、「国内外の関係機関・関係者の巻き込み」を参照されたい。

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、「提案段階」において案件が可決された後に「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。

上述の通り、本案件は「提案段階」に進むこととなっており、投票(2 か月)を SC 27 の定期会合(米国での現地開催とリモート開催のハイブリッド形式)が開催される 4 月下旬以降に設定することが予定されている。投票の結果、案件が可決された場合、7 月から 8 月を目途に中間会合を設定し、「作成段階」の議論を開始する。そこで策定される作業原案(Working Draft)の改善を 1 年程度実施し、2024 年以降に投票を行い、承認段階へ移行することを仮定すると、図 3-3 に示す形で国際規格(案)の策定が進んでいくものと想定している。

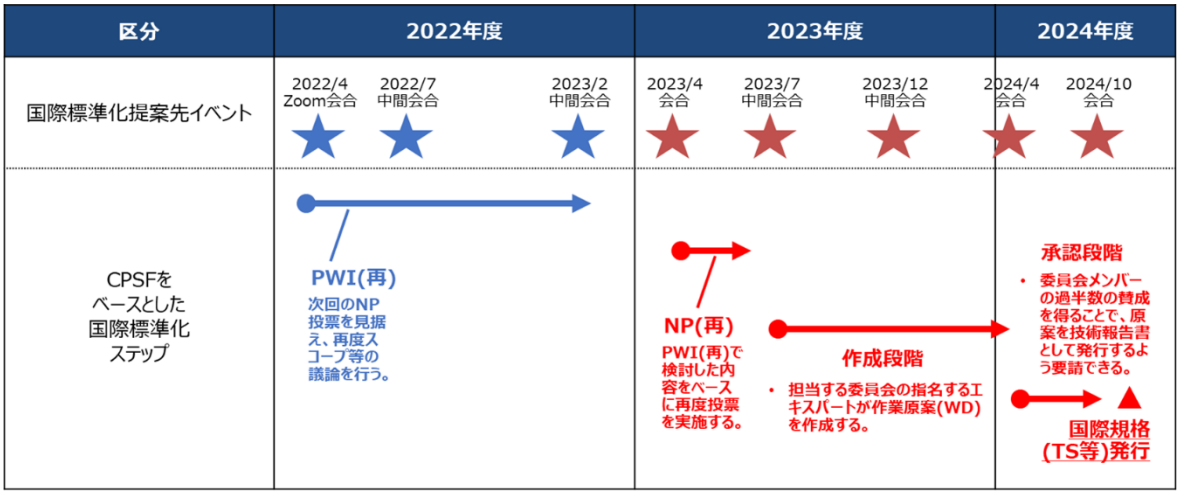


図 3-3 CPSF 等に基づく国際規格策定に向けたロードマップ

3.3.2 国内外の関係機関・関係者の巻き込み

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(案)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き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 3-4 にて示すように、(1) JTC 1/SC 27/WG 4、(2)その他という 2 つの観点から整理した。

図 3-4 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、2022 年 3 月の NWIP 投票否決を受け、4 月の WG 会合において PWI としての再提案を行った。再提案の実施にあたり、エディタからは以下の見直し方針を提示し、参加者からの賛同を得た。

- 本プロジェクト(ISO/IEC 5689)の検討を SC27/WG4 で継続すること
- より実用的な内容にフォーカスするため、タイトルを "Security frameworks and use cases for cyber-physical systems" へ変更すること
- エディタやエキスパートの所見に基づき、適用範囲(Scope)を更新すること
- より多くのエキスパートの理解を得るため、内容を見直すべき。改訂内容には、Clause 8 (ユースケース)の新設等がある。

上記会合での決議を受け、エディタでは改めてドラフト文書の修正を行い、修正稿に基づいて 1 か月の意見募集(CfC: Call for Contribution)を行った。同意見募集では、フランス、米国、中国、日本の 4 か国からコメントの提出があり、特にフランスによる CPS の概念モデルとして新たなものを提案する意見が議論の焦点となった。それらのコメントへの対応に関してエキスパート間の合意を得るため、7 月 27 日に中間会合を実施した。中間会合後、ドラフトの 5 章にあたる CPS の基本的な理解等について更なる検討を行うため、ドラフトの改定及び意見募集が行われることとなった。

改訂版のドラフトに基づいて、2 度目の意見募集は 12 月 6 日から翌年の 1 月 20 日までの期間で実施され、ドイツ、中国、日本の 3 か国からコメントを得た。中国と日本のコメントは比較的エディトリアルなものである一方、ドイツからのコメントは前回のフランスからのものと同様、CPS のモデルに関する概念的なものであった。こちらの結果を踏まえて実施された 2023 年 2 月 1 日の中間会合では、それらのコメントへの対応及び今後のプロジェクトの進め方について議論がなされた。会合における決議事項は以下の通り。

- 本プロジェクトは、PWI から NWIP に進める。
- 今日の議論を踏まえて、エディタは最終的な DoC と会議報告書を作成すべきである。
- 投票用のドラフト文書と NWIP 文書が今後の投票に向けて作成されるべきである。
- リエゾンオフィサーを通じて、次回のドラフト文書は SC 41 と共有されるべきである。SC 41/ahG 30 からのフィードバックが期待される。

会合後、今後の進め方について WG 4 コンビーナ(議長)と相談した結果、NWIP 投票は 4 月に開催される WG 4 の定期会合後に実施する運びとなった。エディタは、それまでにドラフト文書等の準備をしておく必要がある。なお、ドラフト文書の最新版は、2 月の中間会合を踏まえて作成されている準備ドラフ

ト(Preliminary draft)の草案であり、その概要については次節にて述べる。

(2) その他

(1)で述べた議論の状況に加え、ISO/IEC エキスパートや経済産業省担当者等の関係者と協議のうえ、ISO/IEC 国際会議以外の個別の場での働きかけの企画及び支援も行った。特に、前回の NWIP 投票が「5 か国以上からの積極的な貢献の表明」の未達で否決されたことを踏まえ、4 月以降の投票実施の前後で複数の国の政府機関または標準化関係者(エキスパート)に対して計画的な働きかけを行っていくことが望まれる。

表 3-2 NWIP 投票に向けた働きかけの方針

国	前回の投票結果	目指す状況
ドイツ	賛成	賛成＋積極貢献
フランス	棄権	賛成＋積極貢献
スイス	賛成	賛成＋積極貢献
韓国	賛成	賛成＋積極貢献
中国	棄権	賛成＋積極貢献
アメリカ	棄権	賛成 (可能であれば賛成＋積極貢献)
イギリス	棄権	賛成 (可能であれば賛成＋積極貢献)
ASEAN 諸国(全般)	-	-
マレーシア	棄権	賛成
シンガポール	棄権	賛成

3.3.3 CPSF 等に基づく国際規格(ドラフト文書)の作成

これまでに述べたように、2022 年 4 月に再始動した本事業項目に係る標準策定プロジェクトは、JTC 1/SC 27/WG 4 を中心に JTC 1/SC 41 やその他の関連する委員会と議論をしつつ、現在 NWIP 投票前の準備フェーズにある。本節では、2023 年 3 月現在の最新版の文書である、2 月に実施された中間会合後に修正を施した版について概要等を記載する。

当該ドラフト文書では、以下のように章節を設けて内容を記載している。

序文 [Introduction]
1 適用範囲 [Scope]
2 引用規格 [Normative references]
3 用語及び定義 [Terms and definitions]
4 略語 [Abbreviated terms]
5 サイバー・フィジカル・システム(CPS)の概念モデル及び一般的性質 [Conceptual cyber-physical systems (CPS) and its general features]
5.1 CPS 概念モデル [Conceptual cyber-physical systems (CPS)]
5.2 CPS の一般的性質 [General features of cyber-physical systems (CPS)]
5.3 CPS と関連する概念、文書との関係 [The relationship of CPS to other related concepts and documents]
5.3.1 一般 [General]
5.3.2 IoT との関係 [The relationship to “IoT” (ISO/IEC 30141, ISO/IEC 27400/27402/27403)]
5.3.3 デジタルツインとの関係 [The relationship to “digital twin”]
5.3.4 クラウドサービスとの関係 [The relationship to “cloud service”]

5.3.5 エッジコンピューティングとの関係 [The relationship to “edge computing” (ISO/IEC TR 23188)]
5.3.6 産業インターネット・プラットフォームとの関係 [The relationship to “Industrial internet platform (IIP)” (ISO/IEC 24392)]
5.3.7 マルチソースデータ処理との関係 [The relationship to “Multi-Source Data Processing” (PWI 7709)]

6 CPS におけるセキュリティ及びその他の懸念[Security concerns and other concerns in cyber-physical systems]
6.1 一般 [General]
6.2 CPS におけるセキュリティに関する懸念 [Security concerns in CPS]
6.3 CPS におけるプライバシーに関する懸念 [Privacy concerns in CPS]
6.4 CPS におけるセーフティに関する懸念 [Safety concerns in CPS]
6.5 CPS におけるレジリエンスに関する懸念 [Resilience concerns in CPS]

7 CPS 概念モデルに基づくセキュリティ・フレームワーク [Security frameworks based on the conceptual model of cyber-physical systems]
7.1 概要 [Overview]
7.2 CPS 概念モデルに基づくセキュリティ・フレームワーク – CPSF [Security framework based on the conceptual model of CPS – CPSF]
7.2.1 イントロダクション [Introduction]
7.2.2 CPSF 3 層モデル [CPSF Three-tier model]
7.2.3 6 つの構成要素 [Cyber-physical actors (Six elements)]
7.2.4 3 層モデルと 6 つの構成要素による CPSF 記述 [CPSF description with three-tier model and six elements]
7.2.5 セキュリティ・プライバシーに関する懸念 [Key features and security/privacy considerations]
7.3 CPS 概念モデルに基づく OT/IT フレームワーク [OT/IT framework based on the conceptual model of CPS]
7.3.1 イントロダクション [Introduction]
7.3.2 変数と関数 [Variables and Functions]
7.3.3 運用技術(OT) [Operation Technology]
7.3.4 制御技術(CT) [Control Technology]
7.3.5 情報技術(IT) [Information Technology]
7.3.6 機械学習 [Machine Learning Technology]
7.3.7 セキュリティ・プライバシーに関する懸念 [Security/privacy considerations]

8 ユースケース [Use cases]
8.1 CPSF のユースケース [Use case of CPSF (7.2)]
8.1.1 ユースケース①：スマートホーム [Use case of smart home system]
8.1.2 ユースケース②：建物管理システム [Use case of building management system]
8.1.3 ユースケース③：サプライチェーンにおける情報共有 [Use case of an information sharing system among stakeholders in supply chain]
8.2 OT/IT framework のユースケース [Use case of OT/IT framework (7.3)]

Annex A 特定のユースケースを対象にしたフレームワークの利用方法 [How to utilize the framework for specific business cases for 7.2 (CPSF) (informative)]

まず、5 章にて CPS の概念モデルと一般的な性質を導入し、IoT やデジタルツイン、エッジコンピューティング等の関連概念との差異を示すことを通じて基礎を確立している。ここでは現在、CPSF の 3 層構造モデルをベースにしたモデルが議論されている。本ドラフトでは、CPS は、「デジタル、アナログ、物理、人の各構成要素が相互に作用し、物理と論理を統合して機能するように設計されたシステム」(system with digital, analogue, physical, and human components interacting with each other engineered to function through integrated physics and logic)と定義されている。他の概念との差異については、SC 41 と SC 27/WG 4 の間で設置されたアドホック・グループにおいて今後も検討がなされる。

次に 6 章では、5 章で定義した CPS においていかなる懸念が生じ得るのかを整理している。係る整理は、セキュリティだけでなく、セーフティ、プライバシー、レジリエンス等、広義の「信頼性」(trustworthiness)を構成する観点を踏まえて実施されている。懸念の整理にあたっては、ISO/IEC 30147:2021[1] や ISO/IEC 27400:2022[2] 等の既存の国際規格を参照しつつ網羅的な検討がなされている。本章で示される懸念は、後にセキュリティ・フレームワークを導入する際の基礎となるものとなる。

7 章では、5 章及び 6 章の内容を踏まえ、組織が自らのセキュリティ課題を解決しようとする際に「参照」として機能するものとして、セキュリティ・フレームワークを提示している。提示するフレームワークについては、各国・各機関からインプットを得つつ内容の検討を行っているが、日本からは CPSF にて提示されている「三層構造モデル」、「6 つの構成要素」を提案している。加えて、ドイツ(DIN)からの提案に基づき、OT/IT フレームワークも掲載しており、合計で 2 種類が提示されている。これまでの議論では、5 章の CPS の概念的な理解が主な議論の対象となっているが、今後はこちらの内容も含めた検討が進められていくものと考えられる。

CPS やそのセキュリティ・フレームワークのような抽象度の高い概念に関して共通の理解を醸成するためには、8 章にあるように、ユースケースを記述し、共有することが有用なことから、本検討においてもビル分野、スマートホーム分野等に関してそれらを拡張したユースケースの提案を行っている。こちらの内容は、以前は Annex A にあったものを、再提案の経緯から 8 章に移植したものである。

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標準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。

表 3-3 調査対象文献一覧

No.			対象文献	発行/審議団体
1	ISMS 及びサイバーセキュリティ関連標準の動向	1-1	ISO/IEC 27001:2022	ISO/IEC JTC 1
		1-2	ISO/IEC 27002:2022	ISO/IEC JTC 1
2	IoT セキュリティ関連標準の動向			ISO/IEC JTC 1
3	サプライチェーンセキュリティ関連標準の動向			ISO/IEC JTC 1
4	ITU-T における検討動向			ITU-T SG 17

(1) ISMS 及びサイバーセキュリティ関連標準の動向 [3]

情報セキュリティ、サイバーセキュリティ、プライバシーに関する国際標準を策定・維持する ISO/IEC JTC 1/SC 27/WG 1 では、国内外で広く活用されている ISO/IEC 27001 や同規格で要求されているセキュリティ管理策を補足する ISO/IEC 27002、それらを補足する個別領域のガイドライン等の策定及びメンテナンスを実施している。

(1)では、中でも昨今の大きな動きである ISO/IEC 27001・27002 の改定及び、サイバーセキュリ

ティ関連規格の開発状況について詳述する。なお、ISO/IEC 27001・27002 の改定に伴い、表 3-4 に示すように既存の ISMS 関連規格群(ISMS ファミリ規格)の見直しが行われているが、それら個別の状況については紙幅の関係で詳細を割愛する。

表 3-4 今後策定または改定が予定される ISMS ファミリ規格

No.	規格名称		概要
1	ISO/IEC 27003:2017	Information security management systems — Guidance	ISO/IEC 27001:2022 Clause 4～１０についての説明と指針
2	ISO/IEC 27004:2016	Information security management — Monitoring, measurement, analysis and evaluation	ISO/IEC 27001:2022 Sub-clause 9.1 (監視、測定、分析及び評価)の要求事項についての説明と指針
3	ISO/IEC 27005:2022	Guidance on managing information security risks	情報セキュリティリスクマネジメントの説明と指針 ISO/IEC 27001:2022 と同時に出版
4	ISO/IEC TS 27008:2019	Guidelines for the assessment of information security controls	情報セキュリティ管理策の実施に関する評価の指針
5	ISO/IEC PWI 27028	Guidance on ISO/IEC 27002 attributes	ISO/IEC 27002 属性の活用指針
6	ISO/IEC CD TR 27029	additional document for ISO/IEC 27002 and ISO and IEC standards	ISO/IEC 27002 の管理策を引用している ISO または IEC の文書一覧
7	ISO/IEC 27011:2016	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	通信事業者向けの情報セキュリティ管理策 現在、DIS の段階
8	ISO/IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	クラウドサービスカスタマ、クラウドサービスプロバイダ向けの情報セキュリティ管理策とガイダンス 現在、WD の段階
9	ISO/IEC 27019:2017	Information security controls for the energy utility industry	エネルギー産業における情報セキュリティ管理策とガイダンス 現在、CD の段階

上記のような従来から議論されている情報セキュリティ関連標準に加えて、JTC 1/SC 27 では、2016 年頃よりサイバーセキュリティに関する体系的な標準化活動が行われるようになっており、表 3-5 に示すように既に複数の規格が策定されている。

表 3-5 サイバーセキュリティ関連規格

No.	規格名称		概要
1	ISO/IEC TS 27100:2020	Cybersecurity — Overview and concepts	サイバーセキュリティの概要及び概念
2	ISO/IEC 27102:2019	Information security management — Guidelines for cyber-insurance	情報セキュリティリスクマネジメントにおけるサイバー保険の活用
3	ISO/IEC TR 27103:2018	Cybersecurity and ISO and IEC Standards	サイバーセキュリティフレームワークと ISO/IEC 27001、27002 その他の文書との対応関係 ISO/IEC 27001 の改定に合わせ、改定を準備中
4	ISO/IEC TS 27110:2021	Cybersecurity framework development guidelines	サイバーセキュリティフレームワーク開発指針
5	ISO/IEC 27032:2012	Guidelines for cybersecurity	改訂中であり、現在、CD の段階

(1-1) ISO/IEC 27001:2022 情報セキュリティ、サイバーセキュリティ、プライバシー保護 - 情報セキュリティマネジメントシステム – 要求事項 [Information security, cybersecurity and privacy protection – Information security management systems – Requirements]

ISO/IEC 27001 は、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用する情報セキュリティマネジメントシステムの要求事項を規定した国際規格であり、ISMS 適合性評価制度における認証基準として国内でも安定して活用されてきた。2013 年の改定版がしばらくの間最新版として参照されてきたが、出版後 3 年目となる 2016 年に、SC 27 にて改定要否を検討したところ、以下の決定がなされた [3]。

- ISO/IEC 27001:2013 の本文は改定の必要がない。
- 先行して ISO/IEC 27002:2013 を改定することによって、附属書 A の差し替えが必要になる。差し替えの時期や方法については後に検討する。

2 点目に関連して、2022 年に ISO/IEC 27002:2022 が出版されたところ、その管理策を ISO/IEC 27001 附属書 A に反映することをもって、ISO/IEC 27001 の改定が進められることとなった。以降では、2022 年版における附属書 A 以外の改定事項及び、規格改定による既存の ISMS 認証取得組織への影響について述べる。ISO/IEC 27002:2022 における改訂事項については、(1-2) を別途参照されたい。

■ 2022 年版における主な改定事項

2022 年版への改定においては、管理策を示した附属書 A の変更が中心であり、本文及び要求事項の追加・変更は少なかった。附属書 A 以外の改定ポイントは、主に次の 2 点である。

- 最新の MSS 共通テキストの反映
  最終ドラフト(FDIS)の段階で、以下の文書(＊)を参照し、最新の MSS 共通の構造とテキストを反映することを決定した。
  * ISO/IEC Directives, Part 1 —Consolidated ISO Supplement— Procedure for the technical work— Procedures for specific to ISO: 2022, Annex SL

・ ISO/IEC 27001 に固有の形式的な変更
他標準(ISO/IEC 27002、ISO 31000)の改定に合わせ、参照している箇条等の記載を修正した。

■ 既存の ISMS 認証取得組織への影響

ISO/IEC 27001:2022 の発行に伴い、ISMS 認証を取得済みの組織は、改訂版への対応(移行)が必要となっている[4]。一般社団法人情報マネジメントシステム認定センター(ISMS-AC)のリリースによれば、ISO/IEC 27001:2013 から ISO/IEC 27001:2022 への認証移行期限や、現行版による新規の認証審査(初回認証審査)の期限は以下の通りとされている。

【認証の移行期限】
2025 年 10 月 31 日 (2022 年 10 月 31 日から 3 年間)
※ 期間内に改訂版への移行を行わない場合、現行版の ISMS 認証は失効となる。

【現行版による初回認証審査の期限】
2023 年 10 月 31 日 (2022 年 10 月 31 日から 1 年間)

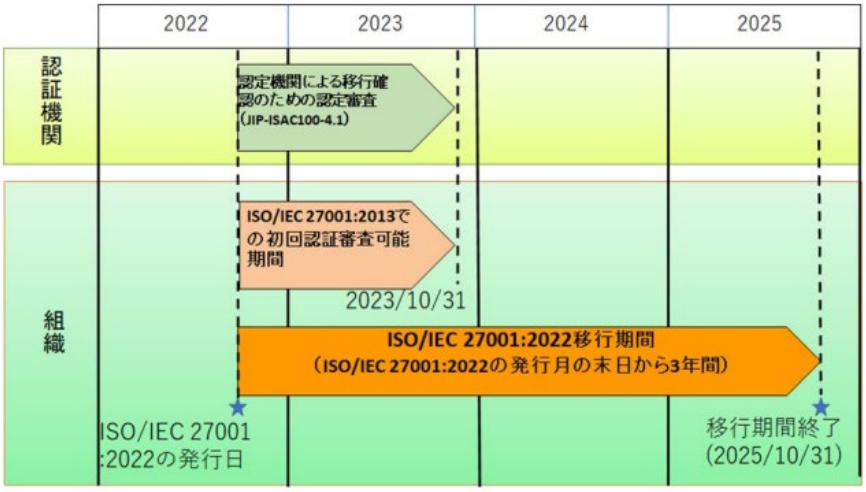


図 3-5. 新基準対応への移行期限と移行期間[4]

(1-2) ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ、プライバシー保護- 情報セキュリティ管理策 [Information security, cybersecurity and privacy protection — Information security controls]

ISO/IEC 27002 は、情報セキュリティマネジメントシステム(ISMS)に関する要求事項を規定する ISO/IEC 27001 の附属書 A にて示されたセキュリティ管理策の実施方法を具体的に記載したガイドラインとして位置づけられる。同規格は、2013 年に出版されたものがこれまで活用されていたが、ISO/IEC JTC /SC 27/WG 1 における審議を経て、2022 年 2 月に最新版が公開されている。
最新版では、主に以下 3 つのポイントについて改定がなされている[5]。

① 章構成の見直し
従来は、ISO/IEC 27001:2013 Annex A の構成にならって 14 に分かれていた章構成を、「組織的管理策」(5 章)、「人的管理策」(6 章)、「物理的管理策」(7 章)、「技術的管理策」(8 章)の 4 つに再編している。

② 管理策の再編
前回改定時からの環境変化等を勘案し、11 の新規管理策を追加し、24 の管理策を統合、

58 の既存管理策を更新した結果、管理策数は 2013 年版の 114 個から 93 個となった。
新規管理策の概要は以下の通り。

表 3-6 2022 年版における新規管理策

ID	管理策	概要
5.7	脅威インテリジェンス	脅威インテリジェンス(脅威の防止や検知に利用できる情報)の収集・分析を実施し、組織のリスク管理プロセスに組込む。
5.23	クラウドサービスの利用における情報セキュリティ	クラウドサービスの普及に対応するため、クラウドサービスを利用するプロセスを確立する。
5.30	事業継続のための ICT の備え	災害やサイバー攻撃等の有事の際にも事業継続を可能にするため、ICT の継続について、計画・実施・維持・試験を実施する。
7.4	物理的セキュリティの監視	守衛や監視カメラ等により組織の敷地を物理的に監視する。
8.9	構成管理	ハードウェア、ソフトウェア、サービス(クラウドを含む)、ネットワーク等の構成管理のため、標準テンプレートの使用や監視等を行う。
8.10	情報の削除	機器・装置の廃棄段階における情報漏えいを防止するため、削除手法の選択、削除記録(削除証明書)の取得等を行う。
8.11	データマスキング	アクセス制御方針や法的要求事項を考慮し、データマスキングを利用する。
8.12	データ漏えい防止	情報漏えいの技術的な監視を強化するため、利用者によるデータ利用状況の監視や漏えいの検知(例：情報が信頼できない外部サービスにアップロードされた)を行う。
8.16	監視活動	技術的な監視を強化するため、システムへのアクセスや利用者による異常な行動の監視を行う。
8.23	ウェブフィルタリング	不正なサイトへのアクセスを防止するため、IP アドレスやドメインのブロック等を通じて、不法な情報やマルウェアを含むサイト、フィッシングサイトへのアクセスを防ぐ。
8.28	セキュアコーディング	開発段階からのセキュリティを強化するため、セキュリティに配慮したコーディング原則をソフトウェア開発に適用する。

③ 管理策に対する属性の設定
各管理策を様々な観点から見ることができるようにするため、管理策ごとに管理策タイプ(予防/検知/是正)、情報セキュリティプロパティ(機密性/完全性/可用性)、サイバーセキュリティコンセプト(識別/防御/検知/対応/復旧)等の「属性」(attribute)を設定している。

(2) IoT セキュリティ関連標準の動向

ISO/IEC 等の国際標準化団体では、技術トレンドの変化に応じて、従来からある ISMS 等の領域に留まらない新たな領域に対応したセキュリティ規格の策定等を行っている。特に、SC 27/WG 4 では、従来から開発対象としてきた ISMS を技術的に補足する規格に加え、IoT やビッグデータ等の比較的新しい領域におけるセキュリティ規格を活発に実施するようになっている。

なお、本事業において日本から提案している PWI 5689 についても、これら IoT セキュリティ関連標準のひとつとして位置づけることが可能と考えられる。

表 3-7 JTC 1/SC 27 にて策定中の IoT セキュリティ関連標準

No.	規格名称		概要
1	ISO/IEC 27400:2022	Cybersecurity — IoT security and privacy — Guidelines	IoT のセキュリティ及びプライバシーに関する基本文書であり、IoT システムにおけるリスク源や管理策を提示 2022 年 6 月出版
2	ISO/IEC DIS 27402	Cybersecurity — IoT security and privacy — Device baseline requirements	IoT 機器の基礎的な要求事項 現在、DIS の段階
3	ISO/IEC DIS 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	ISO/IEC 27400 を前提として、居住環境における事業者向けの指針を提示 現在、DIS の段階
4	ISO/IEC WD 27404	Cybersecurity — IoT security and privacy — Universal cybersecurity labelling framework for consumer IoT	消費者用 IoT 機器のセキュリティ・プライバシー評価基準とラベリング 現在、WD の段階

(3) サプライチェーンセキュリティ関連標準の動向

SC 27/WG 4 では、ISO/IEC 27001:2013 附属書 A における「供給者関係」をより詳細化する目的で、ISO/IEC 27036 シリーズとしてサプライチェーンセキュリティに関する規格開発を実施してきた。昨今、当該テーマが社会的に注目を集める中、同規格群の参照価値は高まりつつあると考えられる。

表 3-8 ISO/IEC 27036 シリーズ規格の概要

No.	規格名称		概要
1	ISO/IEC 27036-1:2021	Cybersecurity — Supplier relationships — Part 1: Overview and concepts	ISO/IEC 27036 のイントロダクションであり、組織が供給者関係において情報及び情報システムを保護することを目的としたガイダンスの概要を提供する。
2	ISO/IEC 27036-2:2022	Cybersecurity — Supplier relationships — Part 2: Requirements	供給者と取得者の関係を定義、実施、運用、監視、レビュー、維持及び改善するための基本的な情報セキュリティ要件を規定する。
3	ISO/IEC FDIS 27036-3	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	ハードウェア・ソフトウェア製品及びサービスの取得者及び供給者に対し、情報セキュリティ確保に係るガイダンスを提供する。
4	ISO/IEC 27036-4:2016	Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services	クラウドサービスの利用者と提供者に対して、サービスの使用に関連する情報セキュリティリスクを可視化し、リスクを効果的に管理するためのガイダンスを提供する。

(4) ITU-T における検討動向

これまで記載してきた ISO/IEC JTC 1/SC 27 以外にも、ITU-T SG 17 においてセキュリティ関連の標準策定等がなされている。現在、SG 17 では、5 つの作業部会(WP: Working Party)が設置されており、それぞれが課題(Question)の検討を行っている。以下では、CPSF の内容に関連している WP 2 における IoT 関連の検討(Q6)、WP 4 におけるデータ流通・利活用に係る検討(Q8)について取組みの概要をまとめる。

表 3-9 ITU-T SG 17 (Security)の構造 [6]

WP 1/Security strategy and coordination	
Q1	セキュリティ標準化戦略と協調 Security standardization strategy and coordination
Q15	Security for/by emerging technologies including quantum-based security
WP 2/5G, IoT and ITS security	
Q2	セキュリティ・アーキテクチャとネットワークセキュリティ Security architecture and network security
Q6	通信サービス及び IoT のセキュリティ Security for telecommunication services and Internet of Things (IoT)
Q13	ITS のセキュリティ Intelligent transport system (ITS) security
WP 3/Cybersecurity and management	
Q3	通信の ISMS とセキュリティサービス Telecommunication information security management and security services
Q4	サイバーセキュリティとスパム対策 Cybersecurity and countering spam
WP 4/Service and application security	
Q7	セキュアなアプリケーションサービス Secure application services
Q8	クラウドコンピューティングとビッグデータインフラのセキュリティ Cloud computing and big data infrastructure security
Q14	分散台帳技術(DLT)のセキュリティ Distributed ledger technology (DLT) security
WP 5/ Fundamental security technologies	
Q10	アイデンティティ管理、テレバイオメトリクスのアーキテクチャとメカニズム Identity management and telebiometrics architecture and mechanisms
Q11	セキュアなアプリケーションを支える汎用技術(ディレクトリ、PKI、形式言語、オブジェクト識別子等) Generic technologies (such as Directory, PKI, formal languages, object identifiers) to support secure applications

■ WP 2 における IoT 関連の検討(Q6)[7,8]

通信業界では、モバイル技術を利用した通信サービスの分野が急成長している。特に IoT やスマートシティ(M2M、RFID、NFC、センサーネットワーク等)、ホームネットワーク、産業制御システム(スマート工場)、スマートグリッド、eSIM、スマートフォン、IPTV ネットワーク等、アプリケーションレベルの技術における異種デバイス間のドメイン固有の通信サービスやネットワークのセキュリティは、業界、ネットワーク事業者、サービスプロバイダーがさらに発展する上で重要とされている。IoT 環境特有の特性(例えば、小型モバイル機器の限られた計算能力とメモリサイズ、長いライフサイクル、カスタマイズされたオペレーティングシステム

とソフトウェア等)により、セキュリティと個人識別情報(PII)保護は、特に注意と研究に値する難しい課題となっている。

本課題に関連した検討項目としては、以下が例示されている。

a. モバイル通信において、通信サービスや IoT のセキュリティ面はどのように識別・定義されるべきか？
b. 通信サービスや IoT の背後にある脅威をどのように特定し、対処すべきか？
c. 通信サービスや IoT を支えるセキュリティ技術とは何か？
d. 通信サービスや IoT におけるセキュアな相互接続はどのように維持・管理されるべきか？
e. 通信サービスや IoT のために、AI/ML ベースの技術を用いたセキュリティ技術をどのように研究・開発すべきか？
f. 新しい通信サービスや IoT、特に新しいデジタルコンテンツ保護サービスに必要なセキュリティ技術、仕組み、プロトコルは何か？
g. 通信サービスや IoT(例：スマートシティ、スマートグリッド、スマートファクトリ)のためのグローバルセキュリティソリューションとは何か？
h. 通信サービスや IoT を安全に利用するためのベストプラクティスやガイドラインは何か？
i. 電気通信/ICT または他の産業において、気候変動への影響(例：エネルギー節約、温室効果ガス排出の削減、監視システムの導入)を直接的または間接的に削減するため、レビュー中の既存の勧告または開発中の新しい勧告に対してどのような強化を採用すべきか？
j. セキュアな通信サービスや IoT に必要な PII 保護・管理の仕組みとは何か？

本課題に係る作業項目(Working item)として、「中」(Medium)以上の優先度が割り当てられているものは以下の通り。

- IoT システムにおけるブロードキャスト認証方式 (Broadcast authentication scheme for IoT system) [優先度：中]
- クロスドメインセキュア通信に用いられる ID ベース暗号システムに関するガイドライン (Guidelines for identity based cryptosystems used for cross-domain secure communications) [優先度：中]
- モバイル端末の安全性を評価するセキュリティ機能 (Security features to assess mobile terminal security) [優先度：中]
- 携帯端末の完全性保護に関するセキュリティガイドライン (Security guidelines for mobile terminal integrity protection) [優先度：中]
- IoT 機器のセキュリティリスク分析フレームワーク (Security risk analysis framework for IoT devices) [優先度：中]
- IoT (Internet of Things) システムのセキュリティ管理策 (Security Controls for Internet of Things (IoT) systems) [優先度：高]
- IoT 機器・ゲートウェイの技術実装ガイドライン (Technical implementation guidelines for IoT devices and gateway) [優先度：中]

■ WP 4 におけるデータ流通・利活用に係るクラウドセキュリティ関連の検討(Q8)[9,10]

近年広く普及しているクラウドへの移行は、安全な従来の社内 IT システムから、安全でない「クラウド interworking 化」されたオープンインフラへの移行を意味するため、セキュリティの徹底的な見直しが必要となる。また、クラウド環境における豊富なリソースの柔軟な利用を通じて、オンプレミス環境では実現できない新しいセキュリティサービスも可能になる場合がある。

一方で、ビッグデータは、大量のデータを処理するために使用される技術、ツールのセット、データと考えられている。多くの場合、データの収集、保存、分析、管理、可視化といったビッグデータの中核となるプロ

セスは、クラウドコンピューティングを基盤として実現される。
本課題に関連した検討項目としては、以下が例示されている。

a. クラウドコンピューティング、エッジコンピューティング、協調のセキュリティ等、クラウドコンピューティングエコシステム全体のセキュリティを向上させるために、サービスプロバイダー、サービスユーザ、サービスパートナーなどの主要アクター、その他の主要業界関係者のために、どのような新規勧告や他のタイプの文書を作成すべきか？
b. 参照アーキテクチャに沿ったセキュリティ・アーキテクチャとセキュリティ組織のために、どのような新たな勧告を作成すべきか？
c. 異なるアクター間の信頼を確立するための保証メカニズム、監査技術、及び関連するリスク評価について、どのような新たな勧告を作成すべきか？
d. ビッグデータプラットフォーム及びインフラストラクチャーのセキュリティソリューション、ベストプラクティス又はガイドラインについて、どのような新たな推奨事項を開発すべきか？
e. 他の課題、研究会、SDO との努力の重複を最小限にするために、どのような協力が必要であるか？
f. 通信/ICT システムを保護するために、どのようにサービスとしてのセキュリティを開発すべきか？

本課題に係る作業項目(Working item)として、「中」(Medium)以上の優先度が割り当てられているものは以下の通り。

- 分散クラウド向けセキュリティガイドライン (Security guidelines for distributed cloud) [優先度：高][11]
- ビッグデータインフラにおける機械学習を利用したデータセキュリティ向けガイドライン (Guidelines for data security using machine learning in big data infrastructure) [優先度：中]
- エッジクラウドのセキュリティ・アーキテクチャ (Security architecture of edge cloud) [優先度：中]
- クラウドサービスプロバイダが提供する演算方式やリソース選定を選定するためのセキュリティガイドライン (Security guidelines for selecting computing methods and resources from Cloud Service Providers) [優先度：中]
- クラウドサービス向けのセキュリティオーケストレーション、自動化及び対応フレームワーク (Framework of security orchestration, automation and response for cloud computing) [優先度：中]
- 低遅延・高信頼な適用シナリオ下におけるクラウドベースプラットフォームのセキュリティ要求事項 (Security requirements of cloud-based platform under low latency and high reliability application scenarios) [優先度：高]

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、様々な産業界における認知・普及の拡大に向けた課題の調査や対策の検討等を通じて、CPSF やこれに連なるガイドラインやユースケース等の普及・啓発を行うことを目的とした。

4.2 本事業の実施内容

上記目的を達成するため、以下の(1)～(3)を実施内容として整理した上で、第 2 層 TF の枠組みの中で IoT-SSF の普及・啓発の推進と第 3 層 TF の枠組みの中で DMF の普及・啓発の推進を行った。また CPSF や IoT-SSF、DMF 等の普及・啓発に向けて、課題や対策の洗い出しを行う目的でヒアリング調査及びアンケート調査を行った。

＜本事業項目の実施内容＞
(1) IoT-SSF の普及・啓発の推進
(2) DMF の普及・啓発の推進
(3) ガイドライン等の普及・啓発に向けたアンケート及びヒアリング調査

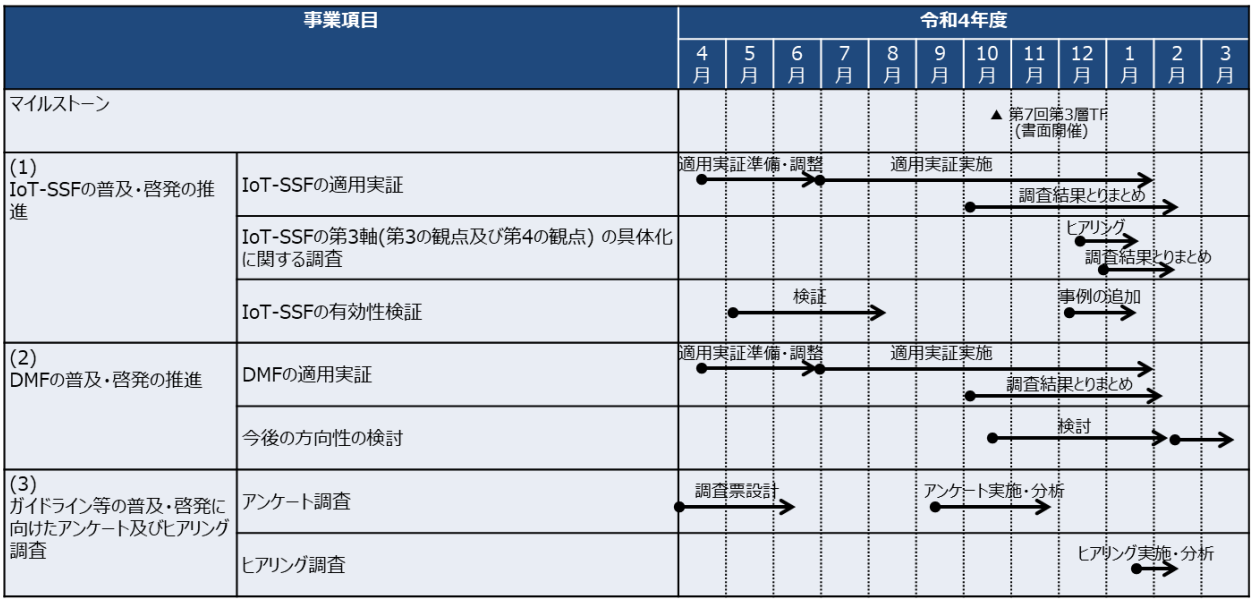


図 4-1 本事業項目の実施スケジュール

4.3 本事業項目の実施結果

4.3.1 IoT-SSF の普及・啓発の推進

IoT-SSF の普及・啓発を推進するにあたって、本事業では以下の 3 項目を実施した。また、第 7 回第 2 層 TF で A～C の結果を説明し、委員よりご意見を頂戴した。

A. IoT-SSF の適用実証
B. IoT-SSF の第 3 軸(第 3 の観点及び第 4 の観点)の具体化に関する調査
C. IoT-SSF の有効性検証

A. IoT-SSF の適用実証

IoT-SSF の事例の蓄積と今後の改善に向けた課題の整理を目的として、IoT-SSF の適用実証を行った。適用実証を開始する当たり、IoT-SSF 適用手順(案)を作成し、第 2 層 TF 委員や関連する事業者を対象として説明会を実施した。参加に同意された事業者から順次適用実証を開始した。結果として、2022 年 7 月から 2023 年 1 月の期間で以下の 5 社、1 団体に参画いただき、4 件の適用実証を行った [12]。

実施した適用実証は以下のとおりである。

① スマートホームサービスにおける窓シャッター連携
② 家庭用エアコン操作
③ ボイラーの遠隔監視
④ 設備保全業務支援サービス

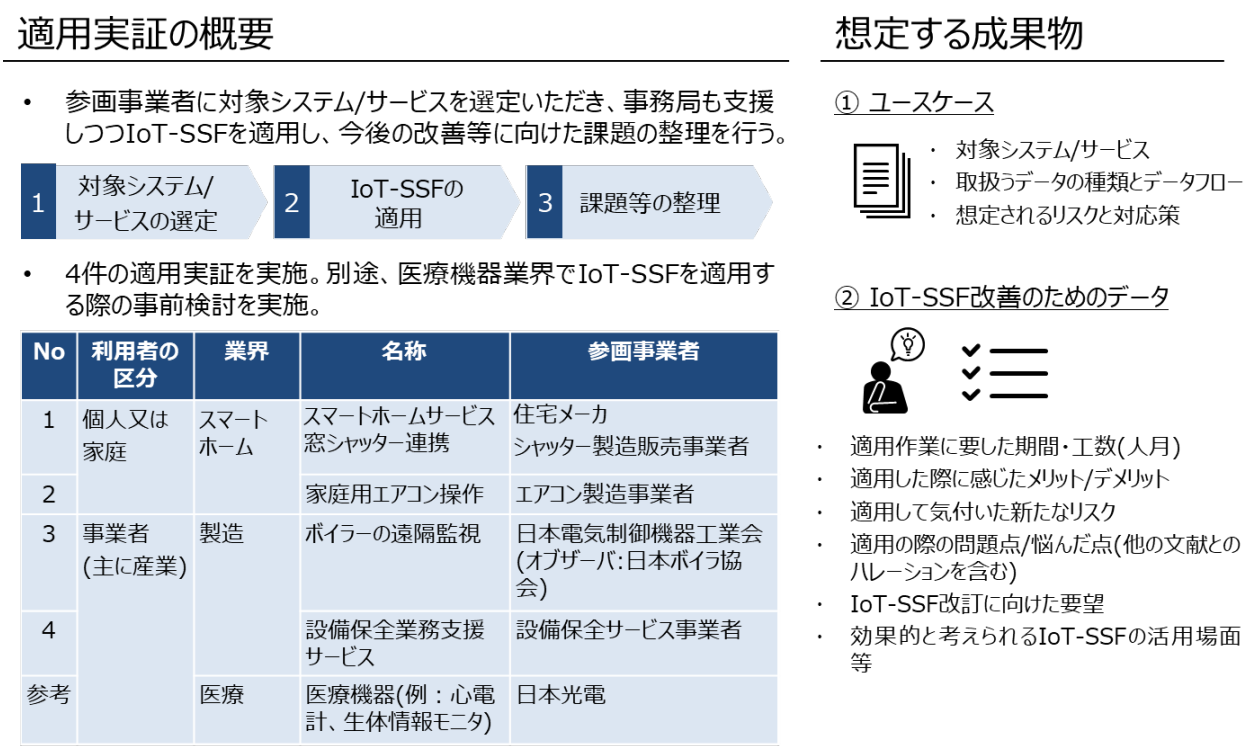


図 4-2 IoT-SSF の適用実証の概要

① ユースケースの概要

(ア) スマートホームサービスにおける窓シャッター連携

- 住宅メーカ及び、シャッター製造販売事業者が、住宅メーカが提供している住宅に居住する住まい手向けに提供しているスマートホームサービス及び、スマートホームサービスと連携する窓シャッターを対象に IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめた。
- 住宅メーカ及びシャッター製造販売事業者は、リスクを低減するため、対象機器・システムに関するリスクアセスメントを行い、リスクに対してはステークホルダー間で対策内容を調整した。

(イ) 家庭用エアコン操作

- エアコン製造事業者が、住まい手向けに提供しているエアコンを対象に IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめた。回線契約やインターネットサービスプロバイダ契約、ルータ購入等のインターネット環境も住まい手が準備するものとする。

・ エアコン製造事業者は、対象機器・システムに関するリスクアセスメントを行い、残存するリスクに対してはステークホルダーに対して対応を依頼することで、リスクを低減することとした。

(ウ) ボイラーの遠隔監視

・ 架空のアセットオーナにおける自社プラントのボイラーを対象に、IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめた。
・ 遠隔監視を行うことで新たに生じ得るリスクやそのリスクへの対応策に焦点を当てることとし、制御システムにおいて一般的に想定され得るリスクやその対応策のうち、ボイラーの遠隔操作とは必ずしもかかわりがないものについては取り扱わないこととした。

(エ) 設備保全業務支援サービス

・ 製造事業者向けにメンテナンスやサポートを行う事業者が工場を持つユーザ事業者へ提供する設備保全業務支援サービスシステム等を対象に IoT-SSF に基づくリスクアセスメント及びリスク対応を行った結果をまとめた。
・ 設備保全サービス事業者は、新たにサービスを提供するにあたって、リスクを低減するため、サービスを受ける事業者をユーザ事業者として設定してリスクアセスメントを行い、リスクに対してはステークホルダー間で対策内容を調整した。

② IoT-SSF 改善のために取得したデータの分析

各適用実証では、IoT-SSF 改善のため各事業者に対して以下の項目をヒアリングした。ここでは、その分析結果を示す。

・ 適用作業に要した期間・工数(人月)
・ 適用した際に感じたメリット/デメリット
・ 適用して気付いた新たなリスク
・ 適用の際の問題点/悩んだ点
・ IoT-SSF 改訂に向けた要望

(ア)適用作業に要した期間・工数(人月)

各ユースケース作成にかかった作業工数を集計した。表 4-1 に各ユースケース作成にかかった作業工数をステップごとに示す。

適用実証の範囲は事業者ごとに異なり、作業工数はあくまでも本適用実証にかかったものである点に留意いただきたい。ユースケースの作成方法の指示やユースケース作成にあたって生じた疑義への対応は事務局で適宜行った。

作業工数に係る分析にあたって、ユースケースごとに参加事業者の IoT-SSF への理解度、対象としたサービス、それまでのリスクアセスメント等の実施状況が異なる。

・ 「スマートホームサービス窓シャッター連携」及び「家庭用エアコン遠隔操作」、「設備保全業務支援サービス」は、既に社内プロセスにおけるリスクアセスメントを実施済みで、運用段階にある IoT 関連サービスを対象としている。
・ 「ボイラーの遠隔監視」は架空の IoT 関連サービスを対象としている。
・ 「スマートホームサービス窓シャッター連携」及び「家庭用エアコン遠隔操作」、「設備保全業務支援サービス」は、各事業者の IoT 関連サービスの企画・運用に関連する部門が作成した。
・ 「ボイラーの遠隔監視」は第 2 層 TF 委員が参画した上で、ユースケースを作成した。
・ 「家庭用エアコン遠隔操作」及び「設備保全業務支援サービス」は、適用実証に要する期間の制限から、想定される脅威や脅威の対象となる機器を絞った上で IoT-SSF を適用した。

表 4-1　適用作業に要した期間・工数(人月)

#	利用者の区分	業界	名称	参画事業者	作業工数			
					事前準備	リスクアセスメント	リスク対応	合計
1	個人又は家庭	スマートホーム	**スマートホームサービス窓シャッター連携**	住宅メーカ シャッター製造販売事業者	**2.0人日** (住宅メーカ:0.7人日/シャッター製造販売事業者:1.3人日)	**7.8人日** (住宅メーカ:5.9人日/シャッター製造販売事業者:1.9人日)	**8.2人日** (住宅メーカ:6.1人日/シャッター製造販売事業者:2.1人日)	**18.0人日**
2			**家庭用エアコン遠隔操作**	エアコン製造事業者	**1.2人日**	**1.2人日**	**0.8人日**	**3.2人日**
3	事業者(主に産業)	製造	**ボイラーの遠隔監視**	日本電気制御機器工業会 オブザーバ：日本ボイラ協会	**1.75人日**	**2.0人日**	**3.25人日**	**7.0人日**
4			**設備保全業務支援サービス**	設備保全サービス事業者	**2.2人日**	**1.1人日**	**2.3人日**	**5.6人日**

作業工数の分析結果を以下に示す。

- 単一の事業者によって作成されたユースケースに比べて、複数の事業者によって作成されたユースケース(「スマートホームサービス窓シャッター連携」)では、他に比較して作業工数を要している。IoT関連サービスの所掌範囲の違いより、事業間でリスクの大きさやリスク対策への認識に差異が生じ、事業間でのすり合わせに時間を要したことで作業工数を要したと考えられる。

- 事前準備に比べて、リスクアセスメントやリスク対応に作業工数を要している場合が多い。リスクアセスメントやリスク対応は、既存の情報整理作業が中心となる事前準備に比べて、リスクの特定や係るリスクへの対応策の立案等の検討すべき事項が多いことから作業に時間を要したと考えられる。

- 他のユースケースと比較して、特徴が見られた箇所は以下の通り。
  - 「スマートホーム窓シャッター連携」のリスクアセスメント、リスク対応に作業工数を要している。住宅メーカ及びシャッター製造販売事業者は既に CCDS の認証を取得しており、IoT-SSF で示した対策要件(例)との対応関係の整理に時間を要した可能性があると考えられる。
  - 「家庭用エアコン遠隔操作」のリスク対応に要した作業工数は少ない。脅威の対象となる機器をクラウドサービスに絞って適用したため、機器ごとの脅威の整理に係る作業工数が少なくなった可能性があると考えられる。
  - 「設備保全業務支援サービス」のリスクアセスメントに要した作業工数は少ない。ユースケース集「2-3-6 金属製造現場の温度センサ等による製造設備の状態監視」に示すシステム構成やデータフロー図の大部分を参考にすることができたため、想定されるセキュリティインシデントやその結果を特定する際の作業の工数を減らすことが可能となったと考えられる。

- 今回の適用実証では、ユースケースを作成する作業者の力量も一定程度あったと考えられる。また、一部スコープを狭めた上で IoT-SSF を適用したユースケースも見られた。今回の適用実証では扱わなかった以下の場合には更に作業工数を要する可能性がある。
  - 運用段階ではなく、企画運用段階にある IoT 関連サービスを対象とする場合

- リスクアセスメントを未実施の IoT 関連サービスを対象とする場合
- ユースケースを作成する作業者が、対象となる IoT 関連サービス並びに IoT-SSF を含むリスクアセスメントに係る知識を持っていない場合
- 想定される脅威や脅威の対象となる機器を絞らずにリスクアセスメントを行う場合

(イ)適用した際に感じたメリット/デメリット・適用して気付いた新たなリスク・適用の際の問題点/悩んだ点・IoT-SSF 改訂に向けた要望

IoT-SSF 適用に際して参画事業者が感じたメリット/デメリットや今後に向けた要望をヒアリングした。いただいた主な意見は、以下のとおりである。

表 4-2 適用実証にて寄せられた主な意見

No.	分類	主なご意見
1	適用した際に感じたメリット/適用して気付いた新たなリスク	サービスに係るステークホルダー間で共通認識を持ちつつ、リスク等を洗い出すことが可能。
2		今までのリスクアセスメント手法で気付くことができなかったリスクに気付くことが可能。
3		製品安全分野における既存の規定に関連するステークホルダーと協力して、リスクアセスメントを実施した上で、対象とするシステムへの対策を検討することができる点にメリットを感じた。製品安全の分野の技術者とセキュリティの分野の技術者で認識の差異が生じている点に対して認識をすり合わせることが可能。
4	適用の際の問題点/悩んだ点	システム構成図やデータフロー図を作成する際の記載粒度で悩んだ。
5		どこまでの粒度で情報を整理すれば IoT-SSF の適用したことになるのか判断できない。
6		IoT-SSF の適用に大きな工数が必要となる。
7		類似事例がない場合、セキュリティの知識を持たない企業では IoT-SSF の適用が難しい。
8		他のリスクアセスメントにて採用している考え方と一部異なる部分があり、判断に悩んだ。
9	IoT-SSF 等の改訂に向けた要望	安全分野(けがの分野)との関係性の整理及び係る記載を IoT-SSF に追加いただきたい。
10		IoT-SSF における第 3 軸の記載を充実化していただきたい。
11		適用主体やとりまとめを行う主体に関する記載を IoT-SSF の適用手順書に追加いただきたい。
12		ステークホルダー関連図やシステム構成図、データフロー図の記載粒度を IoT-SSF の適用手順書に明確化いただきたい。
13		作業手順や各手順の関係性を説明する図を IoT-SSF の適用手順書に追加いただきたい。
14		ユースケースを作成する際に、PowerPoint 版だけではなく Excel 版のワークシートも作成いただきたい。

ヒアイリングで得た意見をまとめると以下のようであった。

- ステークホルダー間で共通の認識を持ちつつ脅威を整理可能、製品安全分野の技術者と認識をすり合わせつつリスクアセスメントが可能など、IoT-SSF の目的を達成している意見が多かった。

・　一方で、記載粒度や、適用主体やとりまとめを行う主体に関する記載などの追記が必要との意見があった。これらに関しては、適用手順書(案)の修正が必要である。

B. IoT-SSF の第 3 軸(第 3 の観点及び第 4 の観点) の具体化に関する調査

第 3 軸の第 3 の観点「機器・システムの運用・管理を行う者の能力に関する確認要求」及び第 4 の観点「その他、社会的なサポート等の仕組みの要求」を更に具体化する目的で、適用実証に参画した団体や関連サービス提供事業者、民間・公共団体に対して 2022 年 12 月～2023 年 1 月の期間でヒアリング調査を行った。

第 3 の観点のヒアリング調査では、「IoT 機器・システムの運用・管理を行う者に求められるセキュリティ能力」及び「求められるセキュリティ能力の習得方法/確認方法」についてヒアリング調査を行った。

第 4 の観点のヒアリング調査では、「金銭的なサポート」と「モノ・情報面でのサポート」についてヒアリング調査を行った。

	第3の観点	第4の観点
目的	● 「第3の観点:機器・システムの運用・管理を行う者の能力に関する確認要求」の具体化を見据え、「機器・システムの運用・管理を行う者」に求められる能力と今後の検討内容を明らかにする。	● 「第4の観点:その他、社会的なサポート等の仕組みの要求」の具体化を見据え、事業者にとって有効と考えられる「社会的なサポート」や今後の検討内容について明らかにする。
ヒアリング対象	● 適用実証参画団体 ● 関連サービス提供事業者 ● 民間団体 **合計　7団体**	● 適用実証参画団体 ● 関連サービス提供事業者 ● 民間・公共団体 **合計　7団体**
ヒアリング内容	● 「機器・システムを運用・管理する者」に関するセキュリティ能力のあるべき姿と現状について ● 「機器・システムを運用・管理する者」に関するセーフティ能力のあるべき姿と現状について　等	● 既存の社会的なサポートの活用状況について ● 既存の社会的なサポートの改善点について ● 新たなサポートの可能性について　等
スケジュール	● 12月中旬～1月上旬	● 12月中旬～1月上旬

図 4-3 ヒアリング調査の概要

第 3 の観点に関するヒアリング調査結果と第 4 の観点に関するヒアリング調査結果を以下に示す。

表 4-3 ヒアリング調査結果

No.	分類		ヒアリング結果
1	IoT 機器・システムの運用・管理を行う者に求められるセキュリティ能力	質問への回答	IoT セキュリティにはセキュリティとセーフティを理解する技術者が必要となる。(民間・公共団体)
2			全てのセキュリティ能力を 1 人が備えている必要はなく、事業部として能力を備えていればよい。業務によって求められる能力を整理することが重要である。(適用実証参画事業者)
3			事業部門(OT 部門)の技術者には、安全確保の能力が必要となる。機器・システムで不具合が発生した場合、後からセキュリティインシデントの発生に気付く場合が多く、発生した当初は判断ができない。その上で、素早く適切にエスカレーションをする能力が求められる。(関連サービス提供事業者)
4		問題意識	業務ごとに求められる能力が異なるが、その定義が難しい。(適用実証参画事業者)

No.	分類		ヒアリング結果
5			IoT セキュリティにはセキュリティとセーフティを理解する技術者が必要となるがその数は非常に少ない。(民間・公共団体)
6	求められるセキュリティ能力の習得方法/確認方法	質問への回答	組織としてセキュリティ能力を得るためには、製品開発や保守のセキュリティを扱う各事業部と本社の情報システム部門での情報連携が重要となる。 (民間・公共団体)
7			継続的にセキュリティに関する情報を得る必要があるが、業界団体を通じて情報を取得することができている。(適用実証参画事業者)
8		問題意識	セキュリティとセーフティを理解する技術者が不足している。したがって、現場作業者よりまずはその監督者へ係る知識を身に付けさせることが効果的である。(民間・公共団体)
9			組織内の人材の能力は確認可能であるが、組織外の人材においては確認が難しい。(適用実証参画事業者)
10			求められるセキュリティリテラシーも専門的＆高度であるため、人材が不足している。(適用実証参画事業者)

表 4-4 ヒアリング調査結果

No.	分類		ヒアリング結果
1	金銭的なサポート	質問への回答	リスク移転の方法としてサイバー保険は有効である。一方で、一般的に言われるサイバー保険は主に IT セキュリティ領域を対象としており、物理的な被害については火災保険等の従来型保険で補償対象としている。理由としてリスクの大きさを測ることが難しい点や IoT 機器・システムにおける被害が現時点で少ない点が挙げられる。(関連サービス提供事業者)
2			リスクが業界ごとに異なるため、保険が成立するかを分野別に検討する必要がある。(民間・公共団体)
3			企業に対して加入を促すメッセージを伝えることができることから、サイバー保険を、業界団体を経由して募集することは有効と考えられる。(民間・公共団体)
4			サイバーセキュリティお助け隊サービスにおける簡易保険において、補償範囲の拡大を検討している。(民間・公共団体)
5		問題意識	保険業界では、既存の財物保険や賠償責任保険等における潜在的なサイバー関連の損失リスクであるサイレントサイバーリスクについて議論がなされている段階である。係るリスクは既存の保険(例:火災保険)で対処することとなるが、免責事項に含まれている。免責事項を復活されることも考えられるが、保険料を設定することが難しい。(関連サービス提供事業者)
6	モノ・情報面でのサポート	質問への回答	IoT 機器の認証取得を促す製品に対する取組みがなされるとよい。製品が認証を取得することによって消費者の安心感を醸成できる。(適用実証参画事業者)
7			業界団体や関連団体からセキュリティに関する情報(例:セキュリティ対策や脆弱性情報)について継続的に入手することは有効である。また、他社事例を知りたい。(適用実証参画事業者)

No.	分類		ヒアリング結果
8		問題意識	新たに求める社会的なサポートは、「ネットワークの見える化」及び「問題のある通信への自動的な遮断等の対応」である。ルータ等への不審な大量のパケット受信によって住まい手はサービスを利用不可になる場合がある。瑕疵ではないものの、メーカ側で対応をする必要があり、不要なコストとなっている。(適用実証参画事業者)
9			企業の枠組みを超えた支援があるとよい必要と感じる。例えば業界ごとの対応も一定程度有効であると考えられる。(適用実証参画事業者)

ヒアリング等で共有いただいた問題意識に対する取組み・アプローチ方法(案)を整理すると以下のようになった。

- 第 3 の観点の具体化としては、例えば各従業員に対して全てのセキュリティ能力を備えさせるのではなく、求められるセキュリティ能力を特定した上で組織(例:事業部単位)として備えさせるための仕組みを検討することも有効と考えられる。
- 第 4 の観点の具体化としては、対象となる業界や業種を絞った上で、サイバー保険の提供方法に関して業界団体による検討を行うことが有効と考えられる。
- 一方で、以下に示す課題が指摘された。
  - セキュリティとセーフティを理解する技術者の不足(第 3 の観点)
  - 既存保険におけるサイバー関連の補償範囲の曖昧さ(第 4 の観点)
  - サイバー関連の損害発生時における責任分界点の不明確さ(第 4 の観点)
- 今後、IoT セキュリティの技術者確保やサイバー関連のリスクを補償範囲とする保険の普及に係る議論を踏まええつつ、IoT セキュリティ人材のモデル化(第 3 の観点)や重大なサイバーインシデントによる被害を受けた事業者に対する一時的な金銭的支援に関する枠組みの構築(第 4 の観点)について検討を行うことが望まれる。

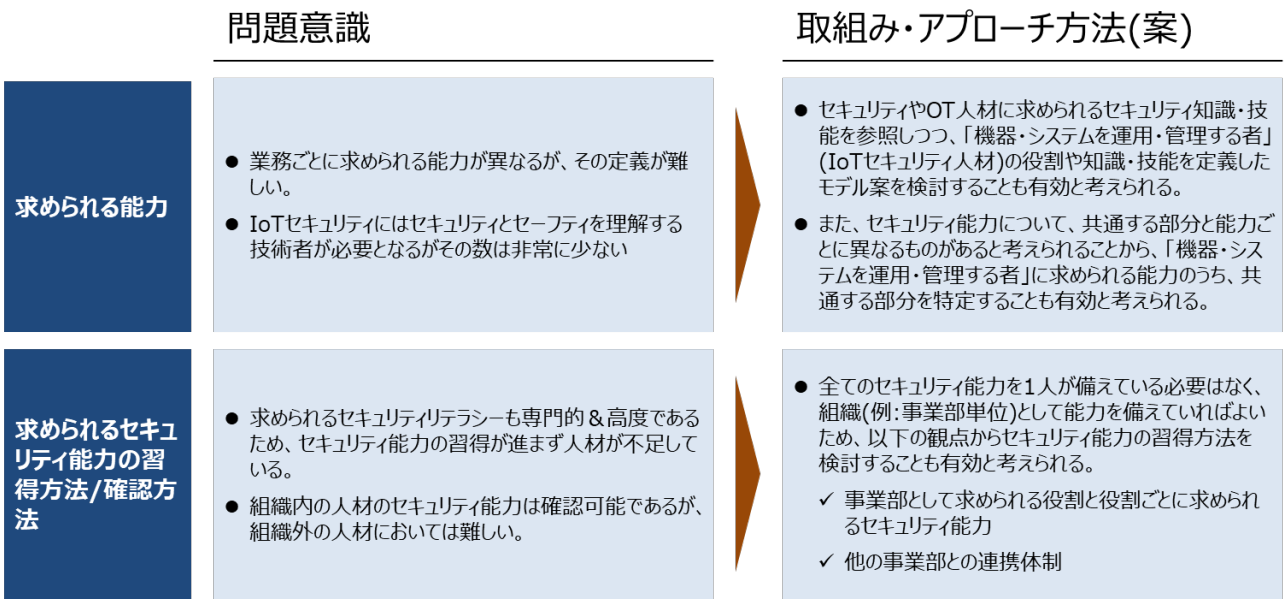


図 4-4 第 3 の観点における問題意識及び取組み・アプローチ方法(案)

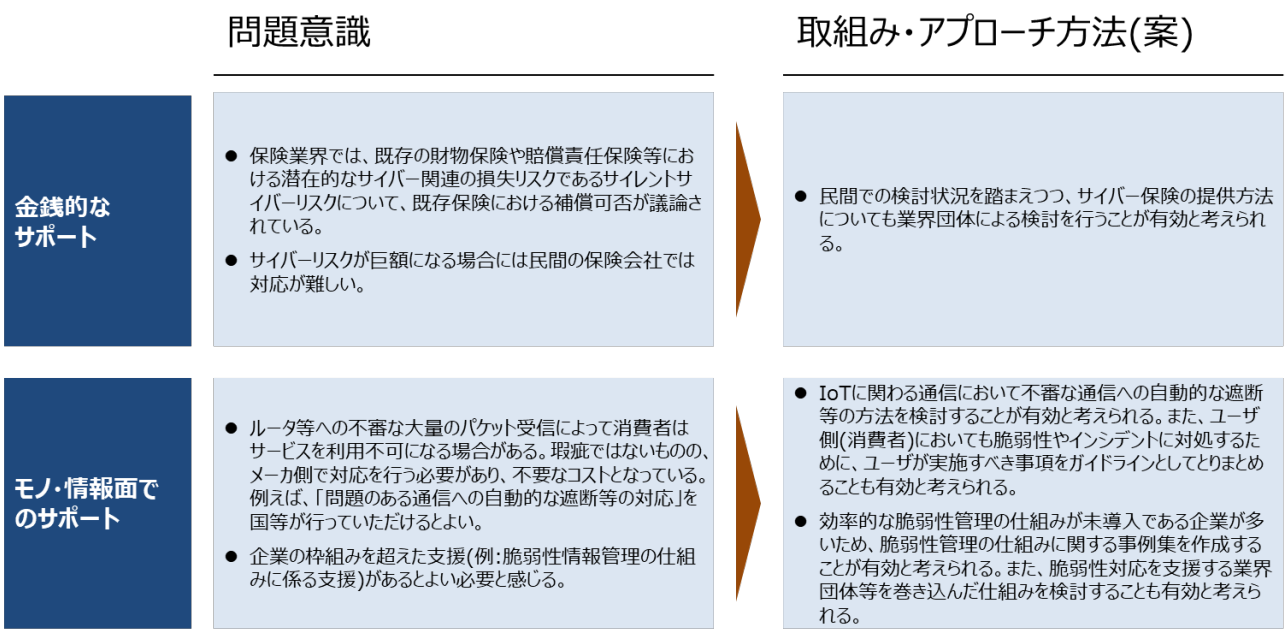


図 4-5 第 4 の観点における問題意識及び取組み・アプローチ方法(案)

C. IoT-SSF の有効性検証

IoT-SSF の適用が有効と考えられるケース、有効と言えないケースをそれぞれ整理し、より利便性の高い内容とするために必要な修正等を具体化する目的で、過去に発生したインシデント事例を対象として IoT-SSF の有効性を検証した。

過去に発生したインシデント事例のうち、有効性検証の対象とした事例を以下に示す。

① 安全計装への HATMAN による攻撃
② 米国水道施設への不正アクセス事案
③ マルウェア「Mirai」感染機器による大規模 DDoS 攻撃
④ 産業用ロボットに対する攻撃の検証
⑤ 製鉄所を模したローカル 5G 実証環境への攻撃検証
⑥ 脆弱性を悪用したスマートスピーカー乗っ取り
⑦ スマートロックの脆弱性悪用

対象とした事例に対して以下に示す検証項目の有効性の検証を行った。

- 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性
IoT-SSF による方法かを問わず、事前に対象システムにおいてリスクアセスメントを通じた脅威シナリオの特定、緩和策の実施がなされていた場合に、インシデント等を未然に防ぐことができていたか、あるいは被害を最小限に抑えることができていたかを評価する。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
リスクアセスメントにおいて IoT-SSF の第 1 軸及び第 2 軸を用いた評価を行った場合に、他の方法(例:被害の大きさとその起こりやすさによる評価、リスクシナリオごとのリスク値評価)と比較して、インシデント等の未然防止あるいは被害の最小化に対する寄与が認められるかを評価する。特に、IoT-SSF の第 1 軸及び第 2 軸を用いた場合に、そうでない場合と比較して対象インシデント・被害に結びつく脅威に相対的に重要な評価がなされるかという点が評価され得る。

- 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価

対象インシデントに対して政府機関又は他のセキュリティ関連組織が推奨する施策が、IoT-SSF の第 3 軸の 4 つの観点に包括され得るかを評価する。

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
対象インシデントへの有効な緩和策のうち、IoT-SSF において特徴ある観点となっている第 3 の観点(運用者等に対する確認要求)、第 4 の観点(その他、社会的なサポート等)に含まれ得る施策が特定され得るかを評価する。

以下では、各事例の概要を示すとともに検証結果を示す。

① 安全計装への HATMAN による攻撃

<事例の概要>

HATMAN は、中東の企業で使用されていた Schneider Electric 社製の安全計装システム(SIS)コントローラや関連製品に対してサイバー攻撃を行うために開発・使用されたとされる。結果的に SIS のフェールセーフ機能が作動し、操業が一時停止する事態となった。

<検証結果>

● 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性
アセスメント時に当該脅威を適切に識別している場合、後のリスク評価、リスク対応の段階において適切に影響度が評価された上で保護措置が講じられることが一般的と考えられるため、リスクアセスメントを事前に実施しておくことが有効に機能したと考えられる。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
業務端末を侵入口とするシナリオや SIS を対象とするシナリオが複数想定されるところ、機器・システムごとに 1 つの評価値のみを付与する方法は、値の異なる他のリスクを見落とす可能性を生じさせ得る。したがって、有効であった可能性もあるが、リスクの見落としが生じないかという点で注意が必要と考えられる。

● 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
ICS-CERT から提案された以下の 3 つの緩和策は第 1 の観点及び第 2 の観点に包括されているため、第 3 軸が示す 4 つの観点は有効に機能する。
  - SIS コントローラを正常な機能に必要なネットワークにのみ接続する。
  - 必要な場合のみ、SIS コントローラをプログラム可能なキー設定に切り替える。
  - SIS エンジニアリング端末をより上位のネットワークに接続しない、外部記憶媒体を使ってプログラムを転送しない、端末のアップデートのベストプラクティスを遵守する。

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
第 3 の観点に関連して、攻撃に利用されたメンテナンス端末やコントローラの適切な管理・運用が情報処理推進機構(IPA)において有効とされているところ、機器・システムの運用・管理を行う者においても通信状況の監視や端末の設定状況の把握等に資する能力があれば、事象の早期検知・防止が図れた可能性がある。したがって、第 3 の観点に基づく対策(例:OT 環境の人材育成、機器・システムの運用管理)が有効であった可能性がある。

② 米国水道施設への不正アクセス事案

<事例の概要>

2021 年 2 月、米国フロリダ州オールズマー市の水道施設(浄水場)がサイバー攻撃を受け、飲用水に含まれる水酸化ナトリウムの濃度の設定値が 100ppm から 1 万 1100ppm に引き上げられた。施設内の端末はトラブル対応時に施設外より接続できるよう、リモートアクセスソフト

TeamViewer を使ってインターネット経由でアクセス可能となっており、ファイアウォール等による防護もなかった。最終的には、職員がすぐに気づいたために実害は生じなかった。

＜検証結果＞

- 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性
本事案の発端になったリモートアクセスソフトの導入等において、最低限のリスクアセスメントが実施され、通信経路の保護や強固な認証の導入等がなされていれば、事象発生の可能性を大きく低減することができていたと考えられる。アセスメントが適切に実施されていれば容易に想定され得るシナリオであるため、有効に機能すると考えられる。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
本事案におけるリモートアクセス機能の悪用は、必ずしも高度な攻撃能力を要求するものではなく、起こりやすさの評価において優先的な課題として認識されてしかるべきものだった。また、対象のシステムでは影響度や起こりやすさの異なる多数のリスクシナリオが想定されるところ、それらを単一の評価結果にまとめることは重要なリスク項目の見落としにもつながり得る。したがって、「起こりやすさ」が対策優先度の評価にポジティブな影響をもたらし得る事案であり、第 1 軸、第 2 軸に基づく機器・システム単位の評価による効用は限定的と考えられる。

- 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
WaterISAC により示された以下の推奨策は、概ね第 1 の観点及び第 2 の観点に含まれるものであり、第 3 軸に示される観点の包括性を否定するものとはなっていない。したがって、第 1 の観点及び第 2 の観点で主要な対策を包括できている点で、有効に機能したと考えられる。
  - リモートアクセスが必要な場合は、安全に構成された VPN を使用する。
  - ホワイトリストやジオ・ブロッキングなどの方法でトラフィックをフィルタリングし、許可されていない人や場所からのアクセスを防ぐ。
  - トラフィックを暗号化する、等。

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
本事案の主要な原因のひとつとして、設備の運用・管理を担当する者のセキュリティに関する能力の低さが挙げられることから、第 3 の観点としてこうした重要システムの運用・管理に従事する者が満たすべき最低限の能力について検討される余地が議論され得る。したがって、第 3 の観点が明確化され、適切な施策が講じられるならば、有効に機能すると考えられる。

③ マルウェア「Mirai」感染機器による大規模 DDoS 攻撃

＜事例の概要＞

セキュリティ設定・対策が不十分なままネットワークに接続された多数の IoT 機器を踏み台として、DNS サービス提供会社 Dyn 等に DDoS 攻撃が行われ、同社のサービスを利用する Twitter 等のサービスが一時利用不能となる等、第三者に多大な被害を与えた。

＜検証結果＞

- 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性
従前では、大量の IoT 機器をボットネット化し、DDoS 攻撃の踏み台とされるリスクについて、製造者や利用者に十分に認識されていなかった可能性があり、基本的なセキュリティ対応に不足が見られたことから、製造者側でのリスクアセスメントが有効となり得る。一方で、どの程度の被害が生じるかは事前には未知であり、本件事象にあるような攻撃はそれほど重要な影響と評価されなかった可能性がある。したがって、機器製造者による事前のリスクアセスメントが有用に機能し得るが、評価の実施が相対的に困難と考えられる。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
上記で述べた通り、脅威を識別した上で、開発時等に大規模 DDoS 攻撃の正確な規模感を製造者等が知り得ることは困難であり、その程度によって対策の水準を振り分けることも同様に困難な側面がある。また、攻撃による被害の経済的影響の度合い、回復困難性の度合いは、DDoS 攻撃の標的となるシステム等の性質に依存することから、いずれも製造者等による事前の評価は困難と言える。したがって、被害の程度を事前に想定することが相対的に困難であり、第 1 軸、第 2 軸による効用は限定的と考えられる。

● 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
以下に示す対策は、概ね第 1 の観点または第 2 の観点に位置づけられるものと言える。したがって、第 1 の観点及び第 2 の観点で主要な対策を包括できている点で、有効に機能したと言える。
  - 不要な管理機能の無効化[IoT 機器の製造者・開発者がとるべき対策]
  - 初期認証情報の変更の周知徹底[IoT 機器の製造者・開発者がとるべき対策]
  - 説明書を熟読し、指示に従い使用する。[IoT 機器の利用者がとるべき対策]
  - 常時動作不要な管理機能が搭載されていた場合は、説明書等の指示に従って無効化する。[IoT 機器の利用者がとるべき対策]

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
第 3 の観点を、高度なスキル等を有しているとは想定しがたい IoT 機器の利用者(一般消費者)に求めることは現実的とは言えない。ただし、係る能力ギャップを埋め合わせるような取組みを喚起し得る点で、対策に具体性が伴うならば有用に機能し得ると考えられる。

④ 産業用ロボットに対する攻撃の検証

＜事例の概要＞

トレンドマイクロ社は、ミラノ工科大学と共同で産業用ロボットのセキュリティに関する調査を実施し、これらの産業用ロボットへの不正アクセスの可能性について検証した。検証に用いた産業用ロボットは、最新の機能を備え、業界の基準を満たした一般的なものとされている。検証では、5 つのシナリオを検討し、遠隔からの攻撃により元々プログラムされているコードを変更することなく、ロボットの動作を改変することに成功している。

＜検証結果＞

● 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性
アセスメント時に当該脅威を適切に識別している場合、後のリスク評価、リスク対応の段階において適切に影響度が評価された上で保護措置が講じられることが一般的と考えられるため、リスクアセスメントを事前に実施しておくことが有効に機能したと考えられる。一方で、未知の脅威を事前に想定できるかという点については対応の限界がある。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
攻撃を通じてロボットの不正挙動がもたらされることが想定されるが、機器を利用する環境により生じ得る影響の内容やのその度合いの評価結果は変動するため、本ケースの情報だけで被害の程度を事前に想定することが相対的に困難と考えられる。また、本来同システムでは、ここで紹介されるものを含む多数のシナリオが特定され得ることから、網羅的かつ効率的な対応を実施しようとすれば、リスクごとの評価が必要になると考えられ、有効に機能しない可能性があると考えられる。

● 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
以下に示すトレンドマイクロ社及びミラノ工科大学によって推奨された対策は、第 1 の観点及び

第 2 の観点で主要な対策に含まれるものであるため、有効に機能したと考えられる。
- 人が作動させる安全機能(例:緊急停止ボタン)の実装
- 攻撃検知機能の実装(短期的な対策)
- システムの要塞化(短中期的な対策)
- 構成要素間の相互接続の要塞化(中期的な対策)
- セキュアソフトウェア開発ライフサイクルの確立 (長期的な対策) 等

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
産業用ロボットの運用・管理には、製造事業者の現場部門のほか、開発・運用委託先、製造元のロボット製造事業者の保守部門等が関係し得ると考えられるが、製造事業者の各運用・管理者が実施すべき具体的な対策が明確化されるならば、有効に機能すると考えられる。

⑤ 製鉄所を模したローカル 5G 実証環境への攻撃検証
<事例の概要>
トレンドマイクロ社は 2021 年 6 月から製鉄所を模した「仮想製鉄所」を用意し、セキュリティリスクを洗い出す実証実験を実施することで、コアネットワーク内の攻撃者が通信を傍受/改ざんし製造システムに影響を与えるというシナリオを検証した。

<検証結果>
● 第 1 軸/第 2 軸の有効性
・ リスクアセスメントを事前に実施しておくことの有用性
アセスメント時に当該脅威を適切に識別している場合、後のリスク評価、リスク対応の段階において適切に影響度が評価された上で保護措置が講じられることが一般的と考えられるため、リスクアセスメントを事前に実施しておくことが有効に機能したと考えられる。一方で、未知の脅威を事前に想定できるかという点については対応の限界があると考えられる。
・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
「起こりやすさ」という観点では、本シナリオは現状として攻撃の実施に高い技能を要するものと考えられるが、対応判断の際により発生しやすい(が被害は軽度な)事象との比較考量がしにくい点に課題がある。また、本件では同一の機器・システムを対象にした複数のシナリオが提案されているところ、機器・システム単位でのリスク評価はそれらを双方含んだ単体の評価対象となることから、シナリオ間で想定される被害の程度が異なる場合は、より軽度なシナリオへの対処が看過され得る点にリスクがある。したがって、より発生しやすい(が被害は軽度な)リスクシナリオがある場合や、提案されている複数のシナリオで生じ得る被害の程度が異なる場合に、有効に機能しない可能性がある。
● 第 3 軸の有効性
・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
以下に示す推奨されている対策は、第 1 の観点及び第 2 の観点で主要な対策に含まれるものであるため、有効に機能したと考えられる。
- VLAN や SDN の使用による、適切なネットワークの分離
- EDR、XDR による、ローカル 5G ネットワーク内の状態監視・攻撃検知
- サーバ、ルータ、基地局への適時のパッチ適用 等

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
参照元の報告書では EDR/XDR 等の利用による侵入検知・早期のインシデント対応や平時のパッチ適用等の運用時中の施策が提案されているところ、報告書では明確には言及されていないが、第 3 の観点からは係る施策の実施に必要な(主に製鉄事業者の内部でセキュリティ監視や設備の保守管理等を担当する)「機器・システムの運用・管理を行う者」の能力が議論され得る。したがって、特に機器・システムの運用・管理を行う者に関してより具体的な対策が明確化さ

れるならば、有効に機能する。

⑥　脆弱性を悪用したスマートスピーカー乗っ取り

＜事例の概要＞

2017 年 9 月、IoT セキュリティ企業の armis は、Android、iOS、Linux、Windows などの主要な OS に存在する脆弱性である「BlueBorne」を発表した。同脆弱性を悪用されると、第三者により Bluetooth の有効範囲内から任意のコードが実行され、デバイスを不正に操作されたり、情報を窃取されたりするといった被害が発生しうる。

＜検証結果＞

- 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性

アセスメント時に当該脅威を適切に識別している場合、後のリスク評価、リスク対応の段階において適切に影響度が評価された上で保護措置が講じられることが一般的と考えられるため、リスクアセスメントを事前に実施しておくことが有効に機能したと考えられる。一方で、未知の脅威を事前に想定できるかという点については対応の限界があると考えられる。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性

機器を利用する環境により生じ得る影響の内容やその度合いの評価結果は変動するため、本ケースで与えられた条件だけで「経済的影響の度合い」や「回復困難性の度合い」を評価することは難しい。したがって、複数のリスクシナリオが想定されることに加え、本ケースの情報だけで被害の程度を事前に想定することが相対的に困難であり、第 1 軸、第 2 軸による効用は限定的と考えられる。

- 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価

以下に示す推奨されている対策は、第 1 の観点及び第 2 の観点で主要な対策に含まれるものであるため、有効に機能したと考えられる。

  - OS を最新の状態にする。
  - Bluetooth を無効にする。

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価

本ケースでは主たる「機器・システムの運用・管理を行う者」はユーザ(住まい手を含む)となるが、「OS を最新の状態にする」及び「Bluetooth を無効にする」の実施にあたって一定の役割が求められるところ、「第 3 の観点」または「第 4 の観点」として、係る能力ギャップを埋め合わせるような取組みを喚起し得る。したがって、ユーザが実施すべき具体的な対策が明確化されるならば、有効に機能する。

⑦　スマートロックの脆弱性悪用

＜事例の概要＞

フィンランドのセキュリティ会社 F-Secure は、2019 年、KeyWe 社が開発・販売するスマートロックサービスの脆弱性悪用を通じて、第三者がスマホアプリとスマートロック間の BLE(Bluetooth Low Energy)通信を傍受して鍵を取得し、ドアの解錠／施錠などが可能になる点を報告した。

＜検証結果＞

- 第 1 軸/第 2 軸の有効性

・ リスクアセスメントを事前に実施しておくことの有用性

アセスメント時に当該脅威を適切に識別している場合、後のリスク評価、リスク対応の段階において適切に影響度が評価された上で保護措置が講じられることが一般的と考えられるため、リス

クアセスメントを事前に実施しておくことが有効に機能したと考えられる。一方で、未知の脅威を事前に想定できるかという点については対応の限界があると考えられる。

・ リスクアセスメントを IoT-SSF の提示する軸や方法で実施することの有用性
傍受用デバイスのチップやハードウェアは安価に入手・製作可能とされており、「起こりやすさ」に関連して、高度なスキルを要するものかを判断することが対処の優先度を変化させ得る。
スマートロックやそれを含むスマートホームシステムを狙ったリスクシナリオが多数想定されるところ、機器・システム単位で一つのリスク値を割り当てることでその値に該当しないリスクシナリオが対応上見落とされる可能性がある。したがって、本ケースの「起こりやすさ」(実施容易性)や、スマートホームにおけるリスクシナリオの多様性を考慮すると、有効に機能しない可能性があると考えられる。

● 第 3 軸の有効性

・ 第 3 軸が示す 4 つの観点が有効な対策を「括る」枠組みとして有効に機能することの評価
以下に示す推奨されている対策は、第 1 の観点及び第 2 の観点で主要な対策に含まれるものであるため、有効に機能したと考えられる。
  - 設計段階での安全な暗号鍵生成・交換メカニズムの採用
  - より安全なバージョンへのファームウェアのアップデート
  - 上記の実施が困難な場合、スマホアプリでの解錠／施錠をあきらめて旧来の物理鍵に戻す

・ 4 つの観点を考慮することで、既存の枠組みでは抽出できなかった対策を特定することができるかの評価
本ケースでは主たる「機器・システムの運用・管理を行う者」は住まい手となるが、高度なスキル等を有しているとは想定しがたい一方で、「より安全なバージョンへのファームウェアのアップデート」等の実施にあたって一定の役割が求められるところ、「第 3 の観点」または「第 4 の観点」として、係る能力ギャップを埋め合わせるような取組みを喚起し得る。したがって、住まい手が実施すべき具体的な対策が明確化されるならば、有効に機能する。

IoT-SSF の有効性検証結果のまとめを以下に示す。

・ IoT-SSF の有効性検証では、基本的に、事前の IoT-SSF によるリスクアセスメントの実施は有効に機能することが確認された。また、IoT-SSF の第 1 軸・第 2 軸の利用は、事業リスクを複数の観点で評価し、適切なリスクレベルを割り当てる際に有益であったことも確認された。一方で、例えば、以下に示す点についても指摘されたため、脆弱性対応に資する体制構築・運営や対処の優先度決定のための精度向上ための判断基準の設定等、IoT セキュリティを確保するための各種取組みを行いつつ IoT-SSF を適用することが望ましいと考えられる。
  - 評価時点では未知の脅威・脆弱性を含めて対処することは困難であり、その点については、事前のアセスメントに加えて、サービス等の運用時にあっても別途迅速な脆弱性対応に資する体制構築・運営等が必要である点に留意が必要となる。
  - 評価に際して(ユーザに用途等が委ねられており)機器・システムの稼働する環境を事前に明確化する必要がある点や、機器の踏み台化のように最終的な被害がどの程度生じるかが事前にはわからない場合に正確な評価の実施に限界がある点に留意が必要となる。
  - IoT-SSF はリスク値の算定にあたり、基本的に「起こりやすさ」を考慮しないモデルとなっているが、脅威や脆弱性の悪用に高度なスキルを要するものかを判断することで、仮想的に「起こりやすさ」を算定することが対処の優先度決定の精度を向上させ得る。

D.第 2 層 TF で頂戴したご意見とまとめ

本事業期間中、令和 5 年 2 月に第 7 回第 2 層 TF が開催され [13]、A. IoT-SSF の適用実証、B. IoT-SSF の第 3 軸(第 3 の観点及び第 4 の観点)の具体化に関する調査、C. IoT-SSF の有効性検証について説明し、各委員からコメントを頂戴した。表 4-5 に第 2 層 TF にて頂戴した主な意見

を示す。

表 4-5 第 2 層 TF にて頂戴した主なご意見

No.	分類	主なご意見
1	A. IoT-SSF の適用実証	IoT-SSF は基本的に事業リスクを見るものと位置づけるのがよいと思われる。
2		対策の洗い出しには有効であるが、「起こりやすさ」を考慮していないため、最終的な対策の絞り込みには限界がある。対策の優先順位決定にはプラスアルファのシステムが必要である。
3		適用実証は産業機器向けの事例として分かりやすく、産業機器向けに IoT-SSF が使えることを示していると思う。
4	B IoT-SSF の第 3 軸(第 3 の観点及び第 4 の観点)の具体化に関する調査	第 3 の観点では、主に人材の話について書かれているが、人材に加えて、機械と組織の 3 点についての認定や認証も重要と思う。
5		第 4 の観点では色々な損害が起きたときに、起きた災害が誰の責任かを明確にすることは非常に難しいと思うが、その線引きが必要ではないかと感じた。
6	C IoT セキュリティ・セーフティ・フレームワークの有効性検証	様々な観点があり、整理が必要だが、具体的な事例の検討をしていく中で、IoT-SSF が有用と示すことができていてよい。
7		本当に機器のリスクが無くなったのか、あるいは機器に対して攻撃できないのかということを検討する必要があるが、未知のインシデントが起きるかは誰も予見ができない以上、議論がまとまらないのではないかと思う。
8	その他	IoT-SSF のプロモーションも併せて考えないといけない。セキュリティ対策は重要と認識しているが、IoT-SSF の内容を関係部門の幹部が理解しないと採用されにくくなるので、IoT-SSF の内容を分かりやすくまとめた資料を用意していただけるとよい。

- 4 件の IoT-SSF の適用実証を行うことで、事例の蓄積を行うとともに IoT-SSF 及び IoT-SSF の適用手順書の改善点を明確化することができた。今後、既に公開している「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」や、本事業で作成した IoT-SSF 適用手順書や適用実証報告書を用いて、普及啓発活動を推進することが有効と考えられる。

- IoT-SSF の第 3 軸に関するヒアリングを実施することで、セキュリティとセーフティを理解する技術者の不足や既存保険におけるサイバー関連の補償範囲の曖昧さ、サイバー関連の損害発生時における責任分界点の不明確さなど第 3 の観点や第 4 の観点をより具体化するための課題があることがわかった。今後、IoT セキュリティの技術者確保やサイバー関連のリスクを補償範囲とする保険の普及に係る議論を踏まええつつ、IoT セキュリティ人材のモデル化や重大なサイバーインシデントによる被害を受けた事業者に対する一時的な金銭的支援に関する枠組みの構築について検討を行うことが望まれる。

- IoT-SSF の有効性検証では、基本的に、事前の IoT-SSF によるリスクアセスメントの実施は有効に機能することが確認された。また、IoT-SSF の第 1 軸・第 2 軸の利用は、事業リスクを複数の観点で評価し、適切なリスクレベルを割り当てる際に有益であったことも確認された。一方で、脆弱性対応に資する体制構築・運営や対処の優先度決定のための精度向上ための判断基準の設定等、IoT セキュリティを確保するための各種取組みを行いつつ IoT-SSF を適用することが望ましいと考えられる。

4.3.2 DMF の普及・啓発の推進

A.DMF の適用実証

DMF の普及・啓発を推進するにあたって、本事業では DMF の適用実証を実施した。また、2023 年 2 月 8 日に開催した第 8 回第 3 層 TF で内容を報告し、委員よりご意見を頂戴した。

DMF の事例の蓄積と今後の改善に向けた課題の整理を目的として、DMF の適用実証を行った。適用実証を開始する当たり、DMF 適用手順(案)を作成し、第 3 層 TF 委員や関連する事業者を対象として説明会を実施した。2022 年 7 月から 2022 年 12 月の期間で以下の 6 つの事業者より参加いただき、6 件の適用実証を行った [14]。

① 車両データ活用基盤の利用による製品開発・改善の推進等 [株式会社デンソー]
② ヒューマンファクターと人工知能を用いた次世代建物制御システム [株式会社竹中工務店]
③ 製造装置の稼働データ等を活用した予防保全・製品向上 [三菱電機株式会社]
④ IoS-OP(Internet of Ships Open Platform)による船舶運航データの流通 [株式会社シップ・データセンター]
⑤ 人起点のデータ取得によるワークプレイスの空間価値の継続的アップデート [パナソニック株式会社]
⑥ ネットワークインフラシステムのリプレースを対象とした設計構築における関係者間での情報共有 [富士通株式会社]

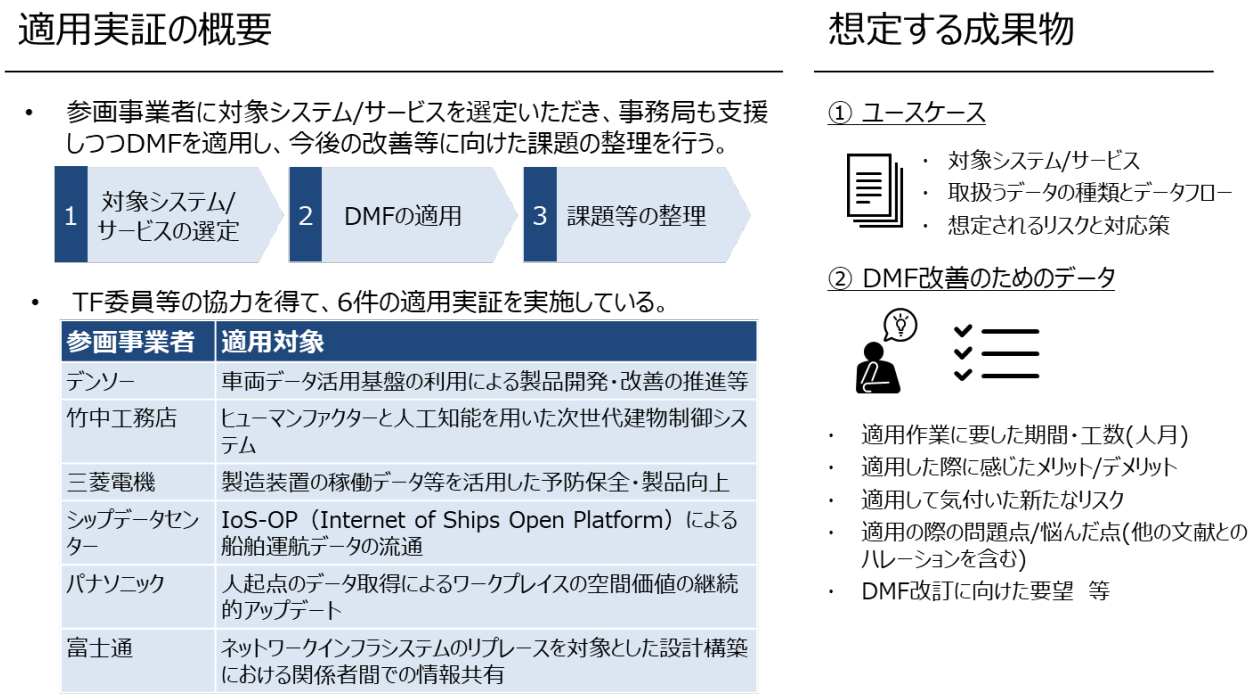


図 4-7 DMF 適用実証の実施概要

① ユースケースの概要

(ア) 車両データ活用基盤の利用による製品開発・改善の推進等

・ 株式会社デンソー(以下、「デンソー」という。)の協力を得つつ、車両から取得したデータを蓄積・分析することを通じて製品開発・改善等に活用する車両データ活用基盤に係る試みをフレームワークの適用対象として取り上げた。
・ デンソーは、自社、グループ会社及び、顧客の運送会社で利用されている社用車にデータ取得装置等を設置し、当該車両の位置情報、車両制御情報等を収集し、外部クラウドインフラ上に構築した「車両データ活用基盤」に蓄積している。収集データについては、今後ドライブレコーダ

による「カメラ画像」や、周辺物体データを含む「センサデータ」を追加することを検討している。
- 車両データ活用基盤に蓄積したデータに対して、デンソーの技術者が可視化ツールや機械学習ツールを適宜用いて、走行経路、操作挙動、走行画像等の分析を行い、自社の製品開発・改善の目的で利用する。データ活用基盤の利用範囲としては、現行の国内のデンソー社員に加えて、欧州拠点の社員及びグループ会社員を追加し、デンソーグループ外部である第三者に対して「データ活用レポート」を提供することも検討している。
- システムの開発・運用・保守は、現在、日本の担当者が実施しているが、今後は海外の事業者へ業務委託することも想定している。

(イ)ヒューマンファクターと人工知能を用いた次世代建物制御システム
- スマートビルを対象とした DMF のユースケースとして、IoT データや AI を活用した次世代建物制御システムを対象として取り上げた。
- 株式会社竹中工務店(以下、「竹中工務店」という。) は、ビルオーナーが管理する建物で稼動する建物設備システム群(例:照明システム、空調システム)や IoT センサ・システム群を通じて、ゲートウェイにてプロトコル変換を行いつつ、自社の運用するデータプラットフォーム“ビルコミ”(以下、「ビルデータ PF」という。)へビル設備の稼働データ(BA データ)や IoT データを共有する。
- 上記データは、BIM データを加工して作成された建物設備や IoT などが抽象化されたデータ表現である「建物メタデータ」と紐づけられ、テレメトリデータとしてビルの快適性向上や制御の高度化を目的として利用される。
- ビルデータ PF に蓄積されたテレメトリデータは外部の AI サービスプロバイダーに提供され、機械学習エンジン(強化学習)による設備制御最適化を実現する。

(ウ) 製造装置の稼働データ等を活用した予防保全・製品向上
- エンジニアリングチェーンとサプライチェーンの連携の一例として、以下に示す仮想的なユースケース「製造装置の稼働データ等を活用した予防保全・製品向上」に、フレームワークを適用した。
- A 社は、日本に拠点を有し製造装置等を製造・販売する事業者であり、フランス(EU 構成国の一例)に所在する多数のユーザ事業者の工場に現地のシステムインテグレータ経由で装置を納め、装置等の運用開始後も振動、温度、動きの情報等の運用データを収集、自社のデータ分析基盤にて異常トレンドの分析等を実施する。
- A 社は、自社の製造装置の故障や異常を検知した場合、あるいは定期的に、現地の保守会社(B 社)や故障や異常が検知された部品のサプライヤ(係る事業者は多数想定されるが、簡便化のため単に「C 社」とする)に対して、必要かつ適切な範囲で異常の通知や稼働情報の提供を行う。
  上記の保守目的でのデータ利用に加えて、A 社は、異常トレンドを示した機器の製造番号やその動作履歴を日本に拠点を有する自社設計部門へと提供し、製品設計の改善等を目的として利用している。

(エ) IoS-OP(Internet of Ships Open Platform)による船舶運航データの流通
- マルチステークホルダー環境におけるリスクの洗い出しや対策の導出を行い、関係各社に展開することで、よりよいデータ管理の実践を進めることを目的として、IoS-OP を対象に DMF を適用した。
- IoS-OP は船舶の運航データを、データ提供者の利益を損なわずに、ステークホルダー間での共有や、造船所やメーカ等への利用権販売、各種サービスへの提供を可能とすべく、海事業界内で合意されたルールと、データセンターで構成された共通基盤である。
- 船主等の PU(Platform User)が船上データ収集装置により収集したデータを船上サーバ等に蓄積し、項目の標準化等を行った上で海事業界内にて合意されたルールと、データセンターで構成された共通基盤(ShipDC)に共有される。

・ 係るデータは、遠隔メンテナンスサポートや性能解析レポート、状態監視等のサービスを提供する SP(Solution Provider)に提供され、船主、船舶管理会社等の SU(Solution User)に向けたサービスに利用される。

(オ) 人起点のデータ取得によるワークプレイスの空間価値の継続的アップデート

・ ニューノーマル時代のワークプレイス創造を目指す取組みの一例として、パナソニック株式会社(以下、「パナソニック」という。) では以下を概要とするワークプレイス向けソリューションを DMF の適用対象として取り上げた。
・ パナソニックは、顧客会社オフィス(主に商業ビルに入居するテナント)に設置された機器から、空間の CO_2濃度や湿度などの環境データ、機器の稼働状況などの設備データを取得、クラウド上で解析を行い、サイネージやスマートフォンでの可視化や、照明・空調・熱交換気、音響機器等の設備運用へのフィードバックを行う。また、バイタルや位置情報、会話量などのヒトデータを取得・解析することで、人起点の空間最適化を行うとともに、効率的な施設管理・運営やそのために必要なコンサルティングレポートの作成等を行う。
・ 顧客会社に提供するコンサルティングレポートの作成は基本的にソリューション提供会社であるパナソニックが実施するが、分析内容が高度である場合などは、適宜外部のコンサルティング会社に委託する。

(カ) ネットワークインフラシステムのリプレースを対象とした設計構築における関係者間での情報共有

・ 富士通株式会社が提供するクラウドサービスである「Fujitsu NIST 対応トラステッドコネクトサービス」を DMF の適用対象として取り上げた。ネットワークインフラシステムのリプレース事業での設計構築における関係者間の情報共有の際に係るサービスを活用した。
・ 「Fujitsu NIST 対応トラステッドコネクトサービス」は、公共機関および民間企業が保有する重要情報を保護し、組織内・組織間で安心・安全に情報共有、コラボレーションを実現する。「Fujitsu NIST 対応トラステッドコネクトサービス」は、重要情報を保護するためのサイバーセキュリティ対策基準である NIST SP800-171 に準拠しており顧客のサイバーセキュリティ強化を安全かつ経済的に実現している。

② DMF 改善のためのデータ

適用実証では、ユースケースの作成に加えて、DMF 改善のため参加事業者に対して以下の項目をヒアリングした。いただいた主なご意見を表 4-6 に示す。

・ 適用した際に感じたメリット/デメリット
・ 適用して気付いた新たなリスク
・ 適用の際の問題点/悩んだ点
・ IoT-SSF 改訂に向けた要望

表 4-6　DMF 改善のためのデータとして適用実証にて寄せられた主なご意見

No.	分類	主なご意見
1	適用した際に感じたメリット/適用して気付いた新たなリスク	DMF は法律や契約、その他の制約に係るリスクの洗い出しや対策の抜け漏れ防止に有用
2	適用の際の問題点/悩んだ点(他の文献とのハレーションを含む)	セキュリティリスク分析の実施には、DMF で求める情報だけでは不足があり、別途実装レベルの情報を補った上でのアセスメントの実施が必要
3		CPSF における三層構造とのリンクが不明確
4		法制度等に係るリスクの特定や対策の検討には、別途法令等の調査や知見の積み上げが必要

No.	分類	主なご意見
5		ケースによっては、データフローは多種多様でゼロからの整理には困難が伴う
6		データの「価値」算定に利用者による恣意的な評価が入り込み得る
7		カテゴリ等の抜け漏れない設定の判断が困難
8		リスク洗い出し結果の網羅性判断が困難
9	DMF 等の改訂に向けた要望	法令からリスクを洗い出し対策を抽出したが、対策のチェックリストがあると対応がしやすい。開発時はサイバーセキュリティの技術的な観点で対応することが多いが、今回のように法的な観点を開発時に考慮するためにチェックリストがあると良い
10		脅威例データベース、対策例データベースなどが整備されると、リスクおよび対策の致命的な抜け漏れ防止になり、本 DMF の有効性が高まるのではないかと思います。
11		リスク洗い出しの表作成の際、参考資料の例がもっとあると参考になる。
12		DMF 利用シーンのイメージが完全には把握出来ておらず、理想的な適用ユースケースを示して欲しい。
13		記載すべき事項のメッシュ感を知るために、ユースケースがたくさんあった方がイメージしやすい。
14		UML 図の様に属性などもデータフローの中に表せると良いと感じた。
15		手順書の適用手順 (概要)には、対象とするデータ利活用プロセスの特定が無いが、適用手順 (詳細)にはあるので、手順の概要と詳細の項目を合わせるべきだと思います。
16		解説には、「リスクの洗い出し」を行った後の検討手順について、もう少し詳しい説明があると使いやすい。

B. 今後の方向性に関する整理

適用実証の結果等も踏まえ、DMF に係る活動の今後の進め方に関する基本的な考え方を整理した。

まず、第 3 層に係る検討の目的が「信頼ある企業間データ流通・利活用の促進」であることを改めて確認した。次に、係る目的を達成するため、第 3 層 TF だけでなく、データ利活用の信頼性を確保するために必要な検討を実施する他の検討体(ルール策定者)との連携も視野に、以下のように今後実施すべき事項(例)の整理を行った。

1. 適用実証にて頂戴したご意見等を踏まえた DMF のさらなる改善
   今回の適用実証で明らかになった課題や事業者から頂戴した意見を参照しつつ、DMF 及び適用手順書の継続的な改善を行う。

2. 分野横断的に適用可能なより具体的な成果の作成とその普及啓発
   DMF よりもより具体的かつ容易に利用可能な成果として、ガイドラインやチェックリスト等を作成し、分野横断的に様々な事業者へと普及啓発する。

3. 他のルール策定者等と連携した分野等を絞った具体的成果の作成

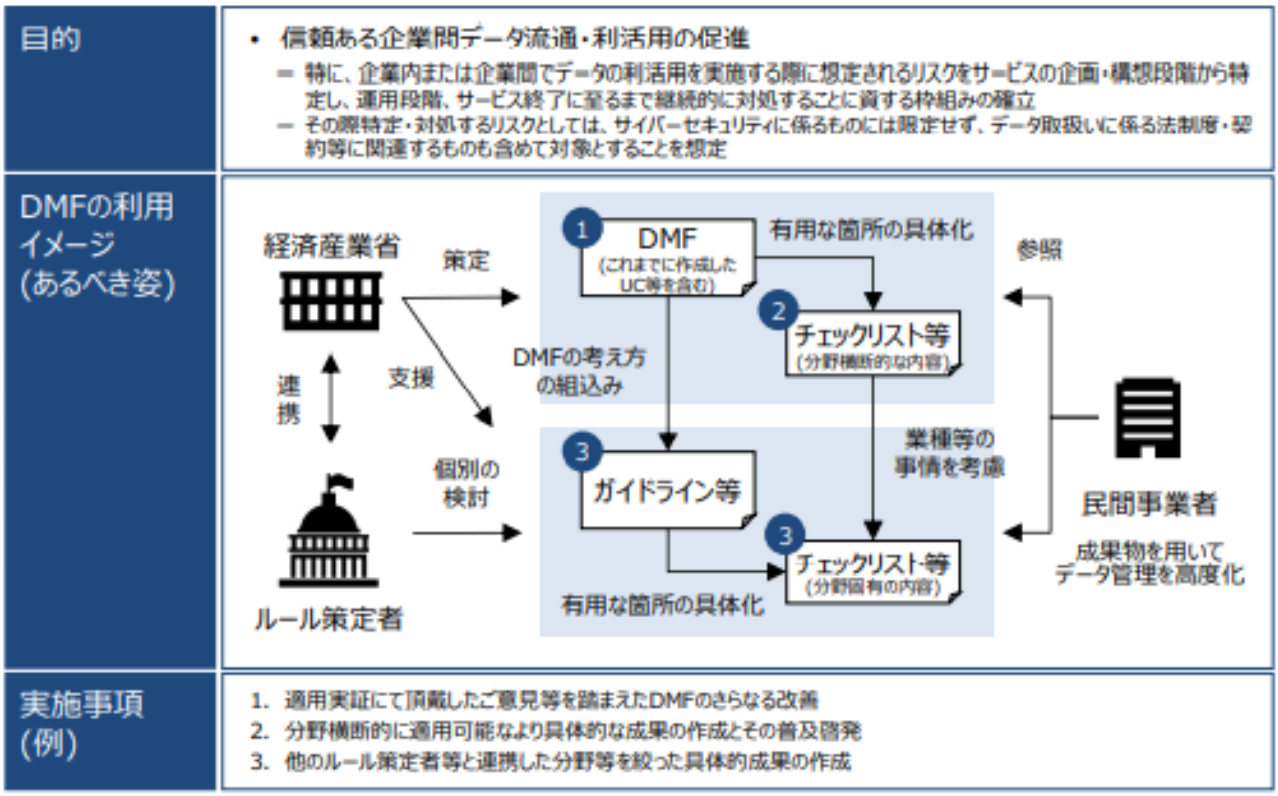
経済産業省サイバーセキュリティ課内外の他のルール策定者と連携し、より具体的な分野を対象として、DMF の考え方を盛り込んだガイドラインやチェックリスト等の策定を行う。

特に上記 3. については、まずはサイバーセキュリティ課内で検討するスマートファクトリ分野対象に、

工場 SWG を「ルール策定者」として将来像も見据えた適切なデータ取扱いに資するルールの明確化を推進していくことを予定している。工場分野及びその後の他分野との連携の手順としては、以下を想定する。

1. スマートファクトリ関連の検討推進
   1-1. DMF 及び TF からの期待事項を共有
   1-2. 分野の将来像(例：スマート工場)に対して DMF 等を当てはめつつ、データ取扱いに係るリスク等の検討事項を整理
   1-3. 連携して既存ルール等とのギャップ分析等を実施し、分野横断的な事項の検討または分野ごとの検討を推進
2. 成果の横展開検討
3. 連携して既存ルール等とのギャップ分析等を実施し、分野ごとの検討を推進

図 4-8 DMF に係る活動の今後の進め方に関する基本的な考え方



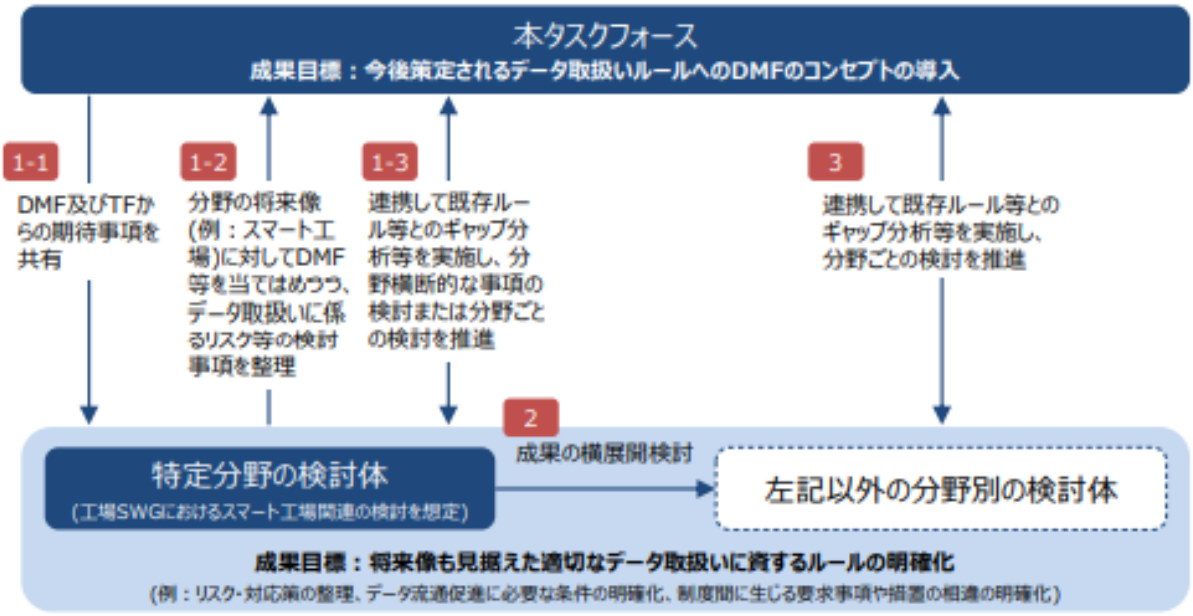


図 4-9 ルール策定者との連携の流れ(想定)

C. 第 3 層 TF で頂戴したご意見とまとめ

A. DMF の適用実証及び B. 今後の方向性に関する整理で整理した内容について、2023 年 2 月 8 日に開催した第 8 回第 3 層 TF[15] で報告を行い、以下のように委員からのご意見を頂戴した。

- キャッシュレス化 PJ、FinTech 関係はスタートアップが多く含まれる一方で、業界団体が未発達で、ルールを決めてもそれを広がりにくいという点が課題になっている。ペイメントの分野でも加盟店の裏側に重要なサービスプロバイダーがいたりするものの、どのくらいの規模でどのような事業をされているかが見えない。そこへどのように対処するかという点が一つポイントと理解。
- デジタル田園国家都市構想の中で、アナログプロセスをデジタル化しようという活動をしている。セキュリティはベースのインプットとなるため、その点での連携が重要と思う。当方が座長のため、つなぐことは可能。
- クラウド事業者内で何をしているかがあまり見えない。クラウドの中でどのような処理をしているかが DMF で可視化されるとよいと思う。SaaS 系のクラウド等はヒアリング対応してくれるのではと認識。
- 事業者向けのインセンティブとして、優良事業者として紹介される等あればよいのではないか。ただ、日本だけではあまり意味なく、世界的に認められるものになれば進むのではないか。
- 意思決定層に訴求力のあるツールになるため、啓蒙活動は課題と認識。社内セキュリティ対応では、IPA のセキュリティサイトなどはよく見る。そこと連携して情報システム部門から見えるようにしてはどうかと思った。
- 他の手法との組み合わせについて、具体的な対策はあった上で、具体な成果としては、そのマッピング、例えば統制目標とのマッピングができると対策も標準化できる。
- データの表現がブルーで書いてあるが、高次データの高次さの度合いで取扱いが変わってくる。取扱いの違いがわかるように命名や分類がなされているとよいかと思った。
- 個人データや統計データの仕分け、どちらに該当するかで対策が大きく変わる。一方で、分けすぎると使いにくくなる側面もある。日本の個人情報と PII の差異もあるように思われる。データについて最小の分類があった方がよいのでは。個人的には、個人データ、仮名加工データ、匿名加工データ、統計データくらいではないか。

今後の連携分野としては、ペイメント業界、行政機関(デジ田を含む)、医療業界、クラウド、政府内

の他 PJ(データスペース、ハイブリッドクラウド、蓄電池規制対応)等が挙げられた。
普及に向けた課題・施策としては、適用のインセンティブの明確化、認知向上のための取組みの必要性、他ガイドライン類との関係性明確化等に関するご意見を多く頂戴した。

4.3.3 ガイドライン等の普及・啓発に向けたアンケート及びヒアリング調査

本項目では、CPSF に基づくガイドライン等の普及・啓発について、様々な産業界での普及・拡大を進めることを目的として、主に製造業及びその関連産業における CPSF やこれに連なるガイドライン等の認知・普及状況の調査、今後の認知・普及の拡大に向けた課題の整理等を実施した。具体的には、実際の認知・普及状況や関連する定量的な基礎情報の収集を目的として、製造事業者を中心にアンケート調査を実施した後、更なる分析の具体化を目的として、アンケート回答者のうち一定の条件に基づいて抽出されたものを対象にヒアリング調査を実施した。

A. アンケート調査
(1) 実施概要
2022 年 9 月下旬から 10 月末までの期間で、アンケート調査を以下の要領で実施した。[16]

表 4-7 アンケート調査の実施概要

項目	概要
調査対象	業界団体より案内を受けた製造事業者及びその関連産業に属する事業者
調査方法	WEB アンケート
調査期間	2022 年 9 月 21 日～11 月 1 日
有効回答数	397 社
設問内容	• 企業におけるサイバーセキュリティに係るガイドライン等の普及・啓発の推進状況 – サイバーセキュリティに関する情報収集の状況、利用している手段 – サイバーセキュリティガイドラインの認知状況と認知のきっかけ – サイバーセキュリティガイドラインの利用状況と利用のきっかけ – サイバーセキュリティガイドライン活用における課題　等

なお、本調査は別委託事業にて検討されている工場におけるセキュリティ対策状況等の調査と併せて実施された。当該別調査の設問は、上記「設問内容」から省略している。

(2) 調査結果 (サマリ)

本調査の設計にあたって、経済産業省担当者と協議のうえ以下の仮説を設定し、設問への落とし込みを行った。

仮説①： 他の文書と比較して、CPSF 等の存在が認知されていないのではないか[17]
仮説②： 他の文書と比較して、CPSF 等の利用が進んでいないのではないか
仮説③： 認知拡大に向けては、事業者がよく活用している情報収集方法を活用するのが有効なのではないか
仮説④： 利用拡大に向けては、既存ガイドラインで普及しているものの活用理由を参考にできるのではないか

それぞれの仮説に対する調査結果の概要は以下の通りである。

＜仮説①に対する調査結果の概要＞
・ CPSF/IoT-SSF/DMF の認知率は、それぞれ 21.8%/12.9%/6.1%となっており、サイバー

セキュリティ経営ガイドライン(46.3%)や ISO/IEC 27001(55.4%)よりも低かった。
- 全般的に従業員数・売上の大きい事業者の方がガイドラインをよく認知しているが、CPSF 等と経営ガイドライン、ISO/IEC 27001(ISMS)、NIST Cybersecurity Framework(NIST CSF)との間には認知率に隔たりがある。
- 事業者がセキュリティに関する情報収集を実施していたとしても、経営ガイドライン、ISMS、NIST CSF と比較して、CPSF 等の認知まで行き着かない事業者の割合が大きい。
- 認知のきっかけは、「インターネット上での情報収集」が最も多く、「社外の IT 関連事業者」、「業界団体」、「政府関係機関」が次いでいる。傾向にはガイドライン間で大きな差異は見られない。

＜仮説②に対する調査結果の概要＞
- CPSF/IoT-SSF/DMF の利用率は、8.6%/4.3%/1.8%となっており、経営ガイドライン(26.3%)や ISMS(31.4%)よりも低かった。
- 認知率の高いサイバーセキュリティ経営ガイドライン、ISMS、NIST CSF は、CPSF 等と比較して、知っていれば利用する者の比率も高い。
- 規模の小さい事業者では全般的に利用率は低調であり、いわゆる大企業との格差が大きい。
- 自社社員からの要請、次いで業界団体、IT 関連事業者からの推奨、取引先からの要望が利用のきっかけとして多くの事業者から利用のきっかけとして報告されている点は一貫性がある。

＜仮説③に対する調査結果の概要＞
- 従業員規模・売上規模が大きくなるほど、セキュリティ情報収集に熱心な傾向がある。全体を通じて、情報収集をまったく実施していない事業者は少ない。
- インターネットや社外の IT 関連事業者、業界団体が主要な情報収集チャネルである点は全体で共通しているが、規模の小さい事業者ではそれら以外のチャネルの利用状況が相対的に低い。
- 従業員規模を問わず、「DX 推進を条件とした税制支援措置等の実施」や「一定のセキュリティ対策の実施等を条件とした税制支援措置等の実施」といった金銭的支援策は、「十分になされていない」という評価が多くなされている。
- DX 推進関連支援策よりも、セキュリティ関連支援策は「十分になされていない」という評価が少ない傾向にある。「最新のセキュリティ動向等に関する情報提供」や「ガイドライン等によるセキュリティ対策の明確化」が少なく、「セキュリティガイドライン等の周知、講習等」は多く選択されている。

＜仮説④に対する調査結果の概要＞
- ISMS 及び NIST CSF は外部へのアピール目的で利用される傾向が他と比較して強いものの、自社社員からの要請、次いで業界団体の呼びかけ、IT 関連事業者からの推奨、取引先からの要望が利用のきっかけとして多くの事業者から利用のきっかけとして報告されている点は一貫性がある。
- 簡便な評価ツール、専門家の派遣、読みやすい文書(100 人未満を除く)は基本的にどの事業規模であっても同程度要望されているが、対象を絞ったより詳細なガイドラインの公開は、事業規模の大きい事業者を中心に要望されている。
- ガイドライン利用の課題としては、人材不足が最も多く回答されており、不明確な進め方や手順、予算の制約が次いで多く選択されている。ガイドライン利用の課題として選択されている項目は、文書間で大きな差異はない。

(3) 調査結果（設問ごとの集計、クロス分析等）

前述の通り、本調査では、大企業・中小企業の双方を含む 397 社の製造関連事業者からの回答を得た。

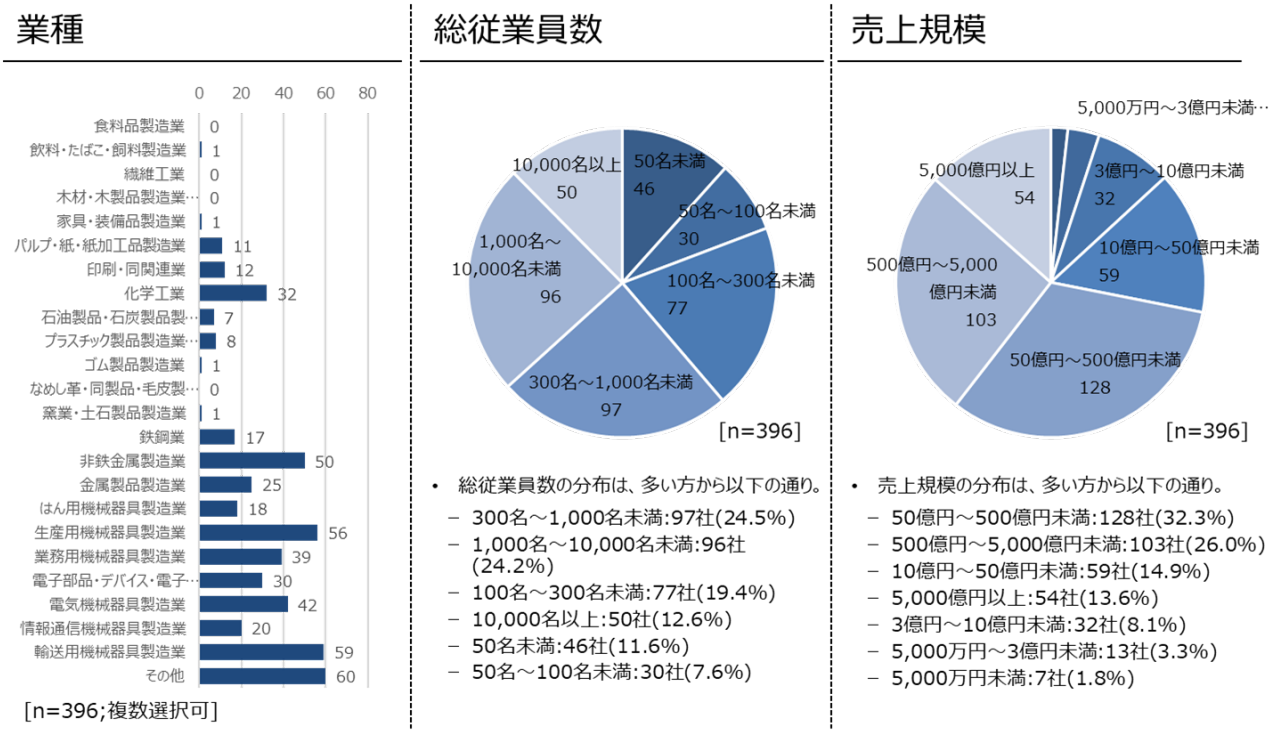


図 4-10 回答者の基礎データ

① ガイドラインの認知・利用状況

CPSF の認知率/利用率は 21.7%/8.6%、IoT-SSF は 13.1%/4.3%、DMF は 6.1%/1.8%となっており、経営ガイドラインや ISO/IEC 27001、NIST Cybersecurity Framework 等の水準を下回った。

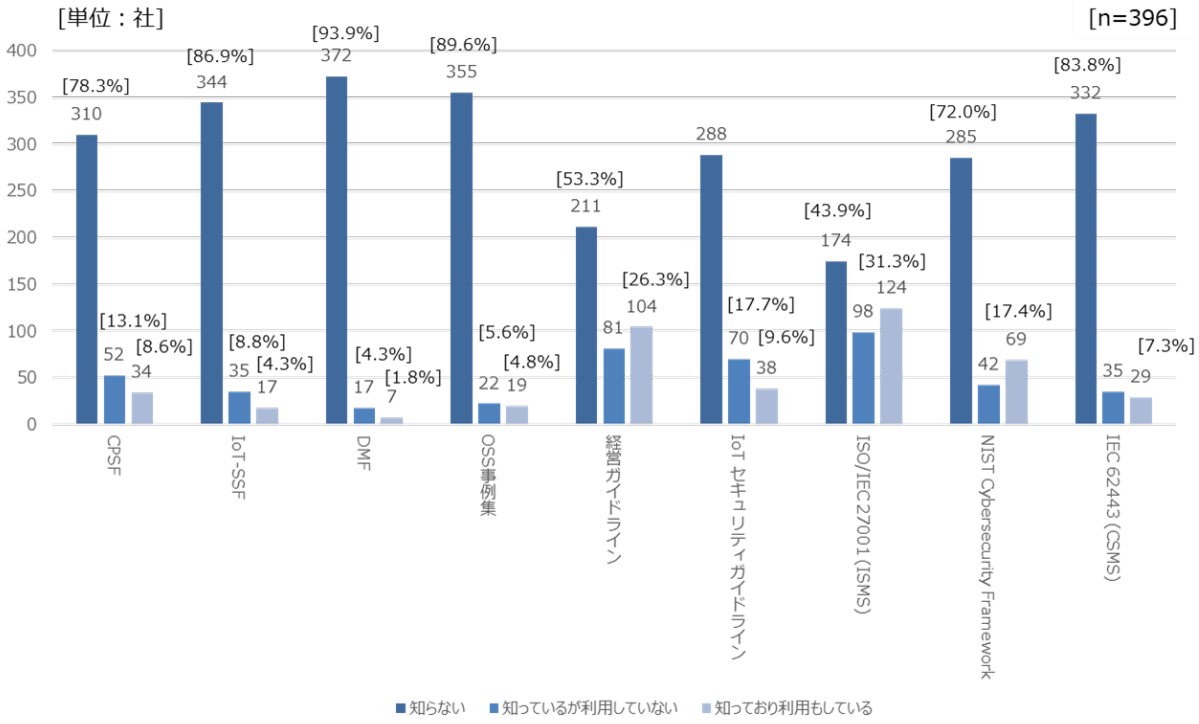


図 4-11 ガイドラインの認知・利用状況

全般的に従業員数の多い事業者や売上規模の大きい事業者の方がガイドラインをよく認知しているが、CPSF/IoT-SSF/DMF は経営ガイドライン、ISMS、NIST Cybersecurity Framework よりも認知率が劣っていた。

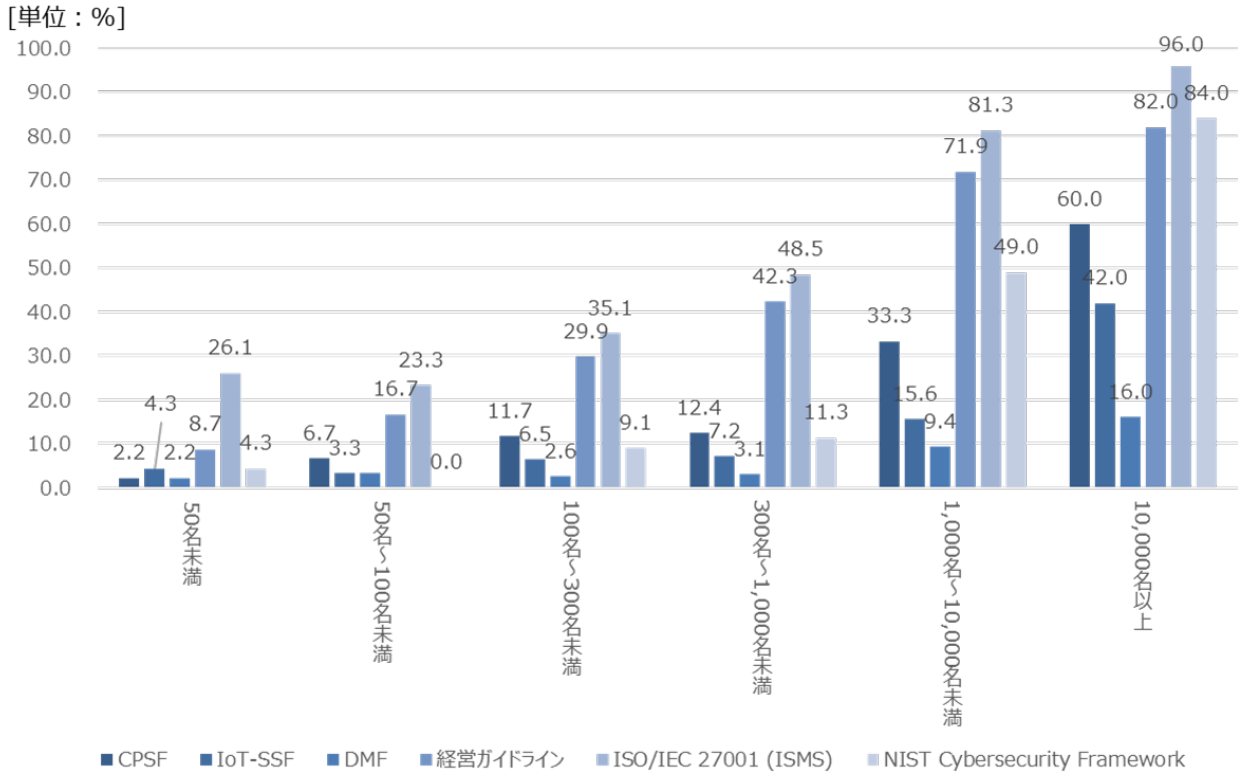


図 4-12 事業規模ごとのガイドラインの認知・利用状況

② ガイドライン認知・利用のきっかけ

ガイドライン認知のきっかけは、「インターネット上での情報収集」が最も多く、「社外の IT 関連事業者」、「業界団体」、「政府関係機関」からの情報提供が次いでいる。傾向にはガイドライン間で大きな差異は見られなかった。

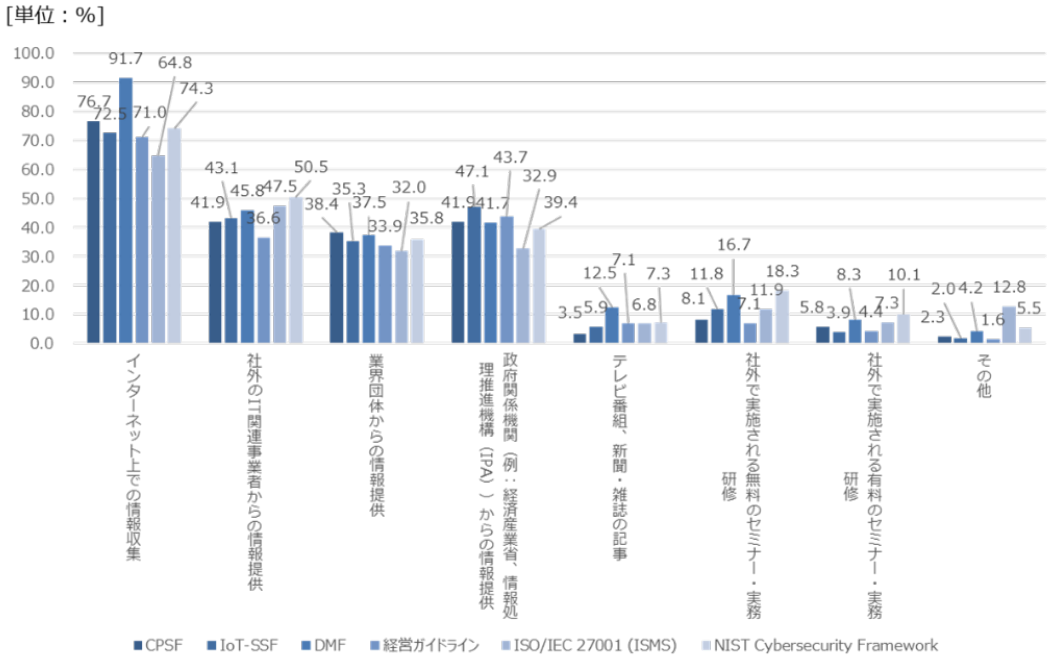


図 4-13 ガイドライン認知のきっかけ

また、利用のきっかけとしては、ISO/IEC 27001 及び NIST Cybersecurity Framework は外部へのアピール目的で利用される傾向が他と比較して強いものの、自社社員からの要請、次いで業界団体の呼びかけ、IT 関連事業者からの推奨、取引先からの要望が利用のきっかけとして多くの事業者から報告されている点は一貫性がある。

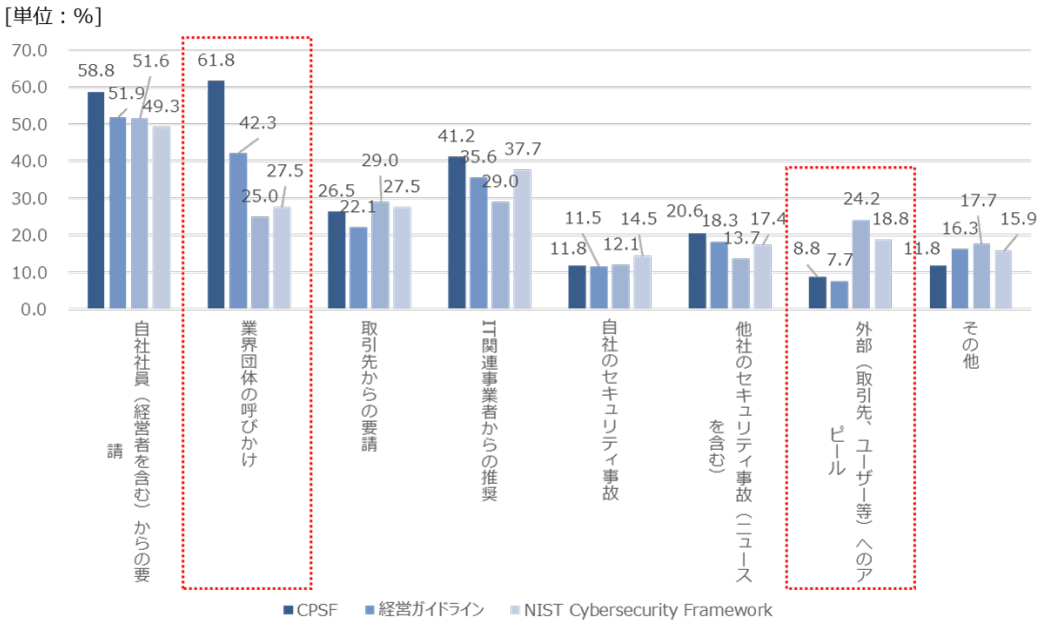


図 4-14 ガイドライン利用のきっかけ

③ ガイドライン利用の課題等

ガイドライン等の利用における課題としては、人材不足が最も多く選択されており、不明確な進め方や手順、予算の制約が次いで多い。ガイドライン利用の課題として選択されている項目は、文書間で大きな差異はない。

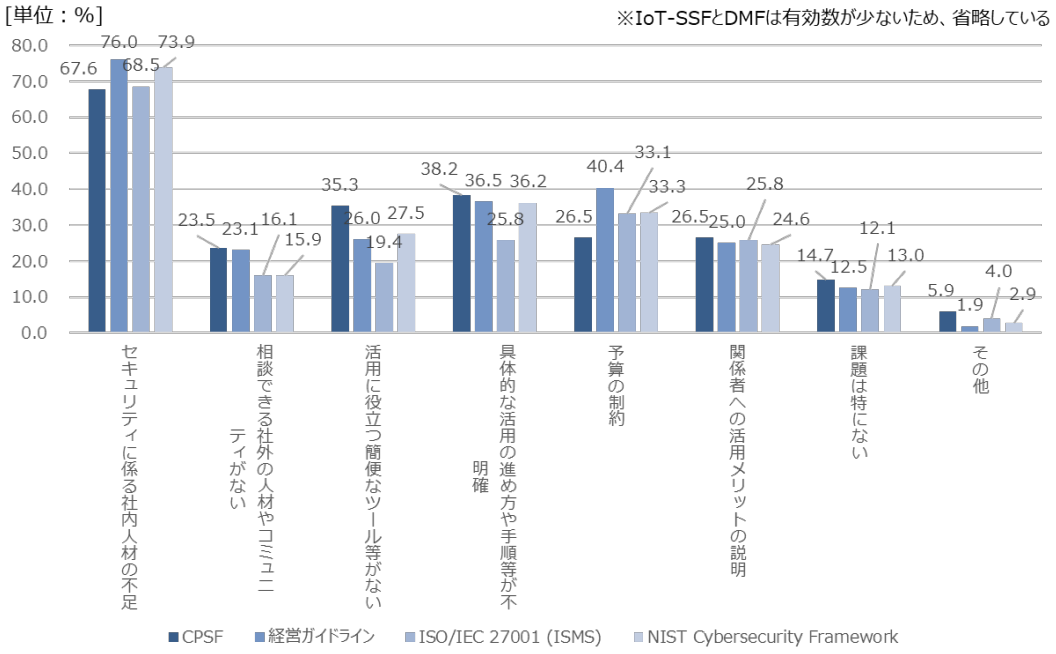


図 4-15 ガイドライン利用における課題

どのガイドラインも活用していないと回答した事業者は、人材不足に加え、何から始めればよいかわからない点、どの文書を見ればわからない点を多く回答した。

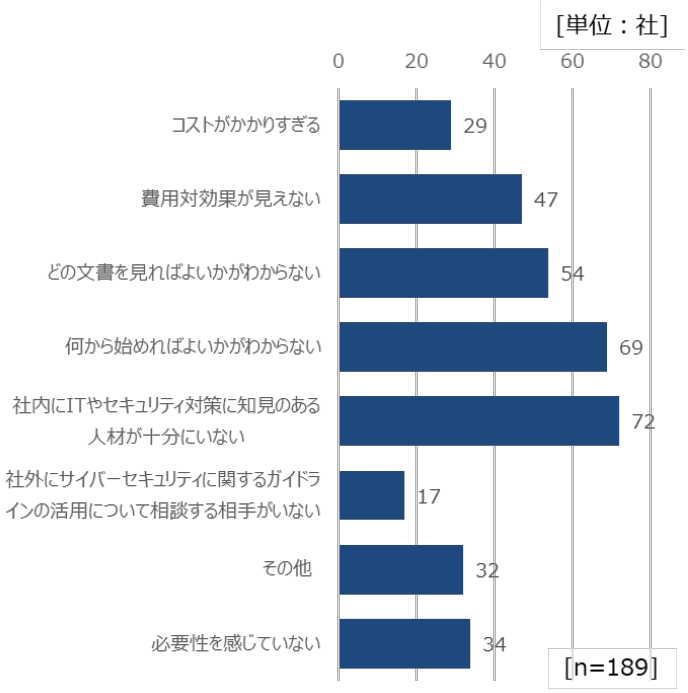


図 4-16 ガイドラインを活用しない理由

④ セキュリティ情報収集の実施状況

セキュリティ情報収集の分布は、多い方から、常時情報を収集している:177 社(44.7%)、機会があれば情報を収集している:108 社(27.3%)、定期的に情報を収集している:104 社(26.3%)、まったく実施していない:7 社(1.8%)であった。

また、セキュリティ情報収集手段の分布は、多い方から、インターネット上での情報収集:316 社(81.4%)、社外の IT 関連事業者からの情報提供:293 社(75.5%)、業界団体からの情報提供:208 社(53.6%)、政府関係機関(例：経済産業省、情報処理推進機構(IPA))からの情報提供:199 社(51.3%)、社外で実施される無料のセミナー・実務研修:141 社(36.3%)、テレビ番組、新聞・雑誌の記事:128 社(33.0%)、社外で実施される有料のセミナー・実務研修:71 社(18.3%)、その他:32 社(8.2%)だった。

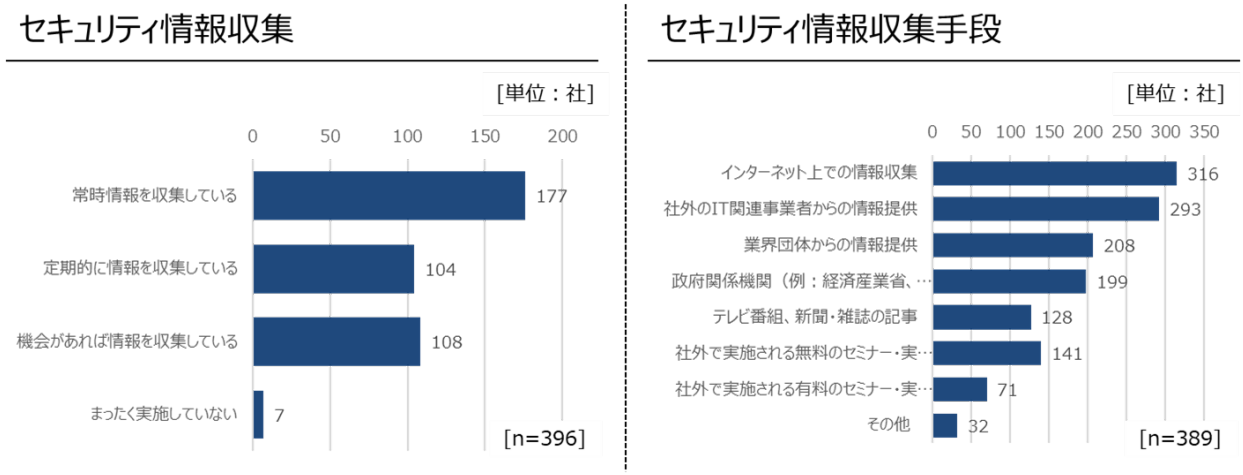


図 4-17 セキュリティ情報収集の実施状況

また、情報収集の実施状況ごとのガイドライン認知状況についても分析を行った。CPSF/IoT-SSF/DMF は、比較的認知率の高いサイバーセキュリティ経営ガイドライン、ISO/IEC 27001 よりも、常時/定期的/機会があれば情報収集を実施している事業者からの認知率が低かった。(日々の情報収集の中で、ガイドライン情報まで行き着いていない事業者が相対的に多い。)

表 4-8 ガイドラインの認知状況と情報収集状況との関係

ガイドライン	認知状況	常時収集している	定期的に収集している	機会があれば収集している	まったく実施していない
CPSF	知らない	**28.0 %**	**22.7 %**	**25.8 %**	1.8 %
	知っている	16.7 %	3.5 %	1.5 %	0.0 %
IoT-SSF	知らない	**34.6 %**	**24.0 %**	**26.8 %**	1.8 %
	知っている	10.1 %	2.3 %	0.5 %	0.0 %
DMF	知らない	**39.9 %**	**25.0 %**	**27.3 %**	1.8 %
	知っている	4.8 %	1.3 %	0.0 %	0.0 %
サイバーセキュリティ経営ガイドライン	知らない	17.2 %	13.6 %	21.2 %	1.8 %
	知っている	**27.5 %**	**12.6 %**	**6.1 %**	0.0 %
ISO/IEC 27001	知らない	14.1 %	11.9 %	17.4 %	1.3 %
	知っている	**30.6 %**	**14.4 %**	**9.8 %**	0.5 %
NIST Cybersecurity Framework	知らない	24.5 %	22.7 %	23.5 %	1.8 %
	知っている	20.2 %	3.5 %	3.8 %	0.0 %

B. ヒアリング調査

(1) 実施概要

A. で示したアンケート調査の結果を踏まえ、ガイドラインの更なる普及にあたって生じる課題を更に具体化するため、大企業と中小企業の双方を含む 8 社を対象に、2023 年 1 月～2023 年 2 月の期間でヒアリング調査を行った。

	中小企業	大企業
目的	● ガイドラインの更なる普及にあたって生じる課題を具体化するため、アンケート調査結果を踏まえて対象団体を選定した上で、セキュリティの情報収集やガイドラインの利用の実態を可視化する。	
ヒアリング対象	● Aアンケート調査にて回答いただいた団体のうち、一定の条件に適合した**3社**	● Aアンケート調査にて回答いただいた団体のうち、一定の条件に適合した**5社**
ヒアリング内容	● セキュリティ情報収集について ✓ 情報収集の実施有無や頻度 ✓ 情報収集ソース 等 ● ガイドラインの利用について ✓ 参照しているガイドライン ✓ ガイドラインに基づく対策を推進する上での課題 等	● セキュリティ情報収集について ✓ 情報収集の実施有無や頻度 ✓ 情報収集ソース 等 ● ガイドラインの利用について ✓ サイバーセキュリティ経営ガイドライン、ISO/IEC 27001、NIST CSF等を利用したきっかけ ✓ ガイドラインに基づく対策を推進する上での課題 等
スケジュール	● 1月下旬	● 1月中旬～2月上旬

図 4-18 ヒアリング調査の実施概要

(2) 調査結果 (サマリ)

ヒアリング調査結果のサマリは以下の通り。

① インターネットでの情報収集の状況

・ 中小企業を含め、各社共通して情報収集の取組みを強化している点が確認された。主な参照先としては、内閣サイバーセキュリティセンター(政府動向)、JPCERT/CC・IPA・製品ベンダー(脆弱性等のセキュリティ技術情報)、経済産業省(ガイドライン)等が挙げられた。

・ 回答者の中には、効率性等の観点から情報収集の多くを外部の事業者からの情報提供に依拠する事業者も見られた。

・ 大企業でも、特にガイドライン・規制等の動向については、スクリーニング済みの情報が得られるということで、効率性の観点から、他社・団体からの収集を主としている事業者が見られた。

② 外部団体等を介した情報収集の状況

・ 今回対象とした中小企業では、社内体制が整っていない、有用性が必ずしも認められていない等の理由で、業界団体からの情報提供を必ずしも活用し切れていなかった。

・ 大企業では、業界団体からスクリーニング済みの業種別の情報を、IT 関連事業者等から製品・ソリューション関連情報を得ているという意見があった。その際、業界団体からの情報は自社の業務に直結して考えやすいという点で有益という見解があった。

③ ガイドライン利用の判断要因

・ 対象事業者の多くにおいて、対象ガイドライン等の内容が事業者の既存の方針、方向性(ISMS 等をベースにした内規定・ポリシー、各社のセキュリティ戦略)と適合しているかを重要な判断指針としていた。

・ また、内容の実務性が認められるか、当該ガイドライン等の認知度及び他社の活用状況も考慮しているという意見があった。

④ 利用しているガイドラインとその理由
・ 既存のガイドラインやフレームワークの利用は、基準を一から考案するのではなく、それらを参考に自社に適したかたちで検討を行うことができる点で有益と指摘された。
・ 対象事業者、特に大企業においては、ISMS や NIST CSF をスタンダードとして理解し、社内のセキュリティ方針、システム導入・運用を定める指針にしているケースが多くみられた。
・ 製品セキュリティについても NIST CSF をベースとした対策に辿り着きつつあるという意見があった。

⑤ 利用しているガイドラインとその理由
・ 中小企業と大企業で共通して、対策推進に係る人材の不足が課題と指摘された。
・ 特に中小企業では、一般従業員のリテラシー向上が社内施策を進めていく上で肝要という意見が複数から挙げられた。
・ 大企業では、企業規模の大きさを反映してか、事業部門等とのコミュニケーション、対応の優先順位付けが課題という意見があった。
・ その他、ガイドライン等で求められる対策の水準(対応が義務か任意か、どのレベルの対処で準拠していると言えるか、等)の明確化が現状十分でない場合があるという指摘があった。

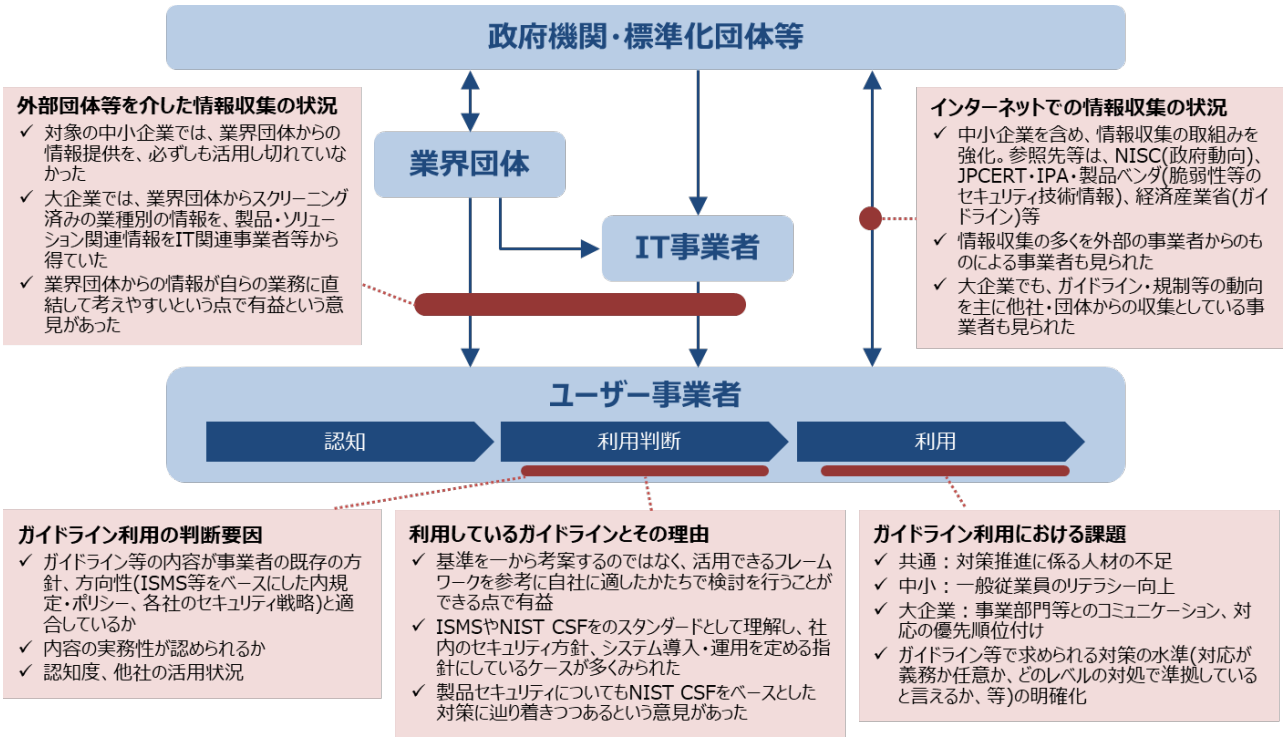


図 4-19 ヒアリング調査の結果サマリ

(3) 調査結果 (設問ごとの回答)

設問ごとに事業者から寄せられた回答の一覧は以下の通り。

[サイバーセキュリティに係る情報収集の全般的な実施状況]
● 総評
近年の情勢変化を踏まえて、中小企業、大企業ともに情報収集の取組みを強化している。関心は社内の情報システムが中心だが、自動車や医療機器等の業界では、製品セキュリティへの

関心が高まっていることが観察された。

● 中小企業向けのヒアリング結果

・ 数年前の基幹システムリプレイスから熱心に情報収集を行うようになり、いくつかのガイドライン等を認知するようになった。現在は、情報収集の手段としては、IT 関連事業者からの情報の比重が大きくなっている。
・ 基本的に情報収集は不定期での実施となっている。実施のきっかけになるのはテレビや新聞等のメディア報道で、報道の内容に対して会社として十分な対策状況であるか等の確認を行う。
・ 能動的にはセキュリティ関係の書籍、Web ニュース記事等、受動的には業界団体等や弊社で導入している機器のベンダー等から、セキュリティ関係のセミナー等の案内も利用している。能動的にとった情報が比重としては多く、外部から提供される情報は読み飛ばしてしまうことが多い。

● 大企業向けのヒアリング結果

＜収集している情報の種類＞

・ 収集している情報としては、規格・規制動向、脆弱性情報、インシデント等の情報が含まれる。
・ 国内外のインシデントやルール形成の動向、日々更新される製品の脆弱性情報等を含め、全般的に情報を収集している。
・ 業界での要求に対応するにはルール面での情報収集も昨今重要になっている。特に、フレームワークとしては NIST CSF、経産省・サイバーセキュリティガイドライン経営ガイドライン等を参照している。業界に特化した対応としては、ISO/SAE 21434、NIST SP 800-171、WP29 関連動向は個別で情報収集を行っている。

＜実施体制・実施頻度＞

・ 担当者が日次で情報を確認している。ここで重要度が高いと思われるものについて自分たちでも深掘りする。
・ 体制としては、製品セキュリティは製品部門で、社内セキュリティ施策は社内セキュリティ担当で実施している。

＜能動的な収集＞

・ 日次でウェブブラウジングでの情報収集。担当者が該当サイトを確認し、内容をチェック。
・ 情報セキュリティポータルサイトを定期的確認
・ IPA から発信される脆弱性情報

＜受動的な収集＞

・ 日次でネットワーク保守ベンダーからのレポート。J-CSIP セキュリティ情報　等の受信
・ 基本的には、自らが各種一次情報に積極的にアクセスすることはほとんどなく、IPA、JPCERT、日本 CSIRT 協議会などからののメルマガを通じて情報収集を実施している。セキュリティベンダー(Mandiant 等)からも月 1 程度の頻度で情報提供がある。製品部門(医療機器)では、脆弱性情報を監視するため、収集、関係者への配信等を実施している。法規制等については、外部からの情報取得が中心であり、IMDRF ガイドライン等への対応を実施しているところ。
・ JPCERT、MCERT、各ベンダーからの情報提供を受けている。ここには、規制・ルール動向等を含む全般的な情報が含まれる。

[インターネット上での情報収集の実施状況]

● 総評

・ 中小企業では、近年の動静を踏まえ取組みを強化している声が多く、参照先等は大企業と大きな違いはない。一方で、リソース等の兼ね合いから情報収集の多くを外部の事業者からのものによる事業者も見られた。
・ 大企業では、自社の情報システムや製品に係る脆弱性情報の日常的な収集等を、各社共通に実施している一方で、ガイドライン・規制等の動向については必ずしも定点観測的で能動的な収集によらず受動的な収集としている事業者も見られた。

● 中小企業向けのヒアリング結果

＜情報収集の問題意識や実施状況等＞

・ 危機感を持ち始めた初期は政府機関 HP を中心に自身で情報を集めていたが、対策を検討するうちに IT 事業者からの情報が中心になっていった。業者からは自社に必要なレベルも含めた具体的なアドバイスがいただけるため、大変重宝している。そのような背景もあり、最近は自主的な情報収集をあまり実施していない。
・ 定期的に決まったサイト等を見る運用にはなっていないが、メディア報道されるような大きな事故が発生した際には、それをきかっけにして様々なサイトを見るようにしている。
・ 昨今はサプライチェーンが攻撃される傾向があると認識している。同業者や取引先で大きなセキュリティインシデントが生じたこともあり、自社でもそのようなことがないよう意識をしてチェックしている。

＜参照している情報源＞

・ 例えば、NISC や IPA、経産省、JPCERT、JC3、警視庁のサイバーポリシー関係のサイトなどを参照している。
・ IPA：中小ガイドライン、チェックツール、動画コンテンツ等、Security NEXT：世間で生じているインシデントの状況等、JVN iPedia：脆弱性情報、JNSA：体制構築、対応手順の参考等

● 大企業向けのヒアリング結果

＜情報収集の問題意識や実施状況等＞

・ 全般的に、明確な目的があって情報を探さない限り、ほとんどは受動的な収集になっている。
・ 規格動向は、業界団体等を介したある程度受動的な収集でもよいが、いつ出るかわからない脆弱性情報は能動的に収集しなければ自社製品等への影響評価ができない。
・ 社内対応としては、定常業務としてのセキュリティ運用に係る Windows アップデートへの対応等については随時情報収集を実施している。
・ 製品側(医療機器)でも、脆弱性対応のため、JVN、CVSS は定期的に参照している。
・ 日常的に収集している IPA の脆弱性情報は各システム担当者に提供し、重要度が高いものについては対処いただく。
・ GDPR や中国 CS 法等の法制度動向については、外部団体に加え、各地域の担当者から情報が入り、社内で対応を協議する。

＜参照している情報源＞

・ NISC：日本政府の動向、JPCERT/CC：脆弱性情報、セキュリティの技術的情報、IPA(＋経済産業省)：脆弱性情報、ガイドライン
・ JPCERT、警視庁、日本サイバー犯罪対策センター、フィッシング対策協議会、日本マイクロソフト等のサイトを担当者が確認している。

[業界団体、IT 事業者等を介した情報収集の実施状況]

● 総評

・ 今回対象とした中小企業においては、業界団体からの情報提供について、必ずしも受領できていない、または受領しているが活用できていないという意見があり、IT 関連事業者等からの情報提供の方が優勢であった。
・ 大企業においては、各企業が属する業界団体を中心にスクリーニング済みの業種別の情報を、製品関連情報・ソリューション情報を IT 関連事業者等から得ている。
・ 上記の差異は、情報処理に係る組織体制、ヒト、知見等の社内リソースの差に(少なくとも部分的には)起因していると想定している。

● 中小企業向けのヒアリング結果

＜業界団体からの情報提供の状況＞

・ 業界団体からはあまり有益な情報を得られていないと感じる。提供される情報の内容と当社の

実態が合っていない場合がある。
・ 業界団体からの情報提供については、自社向けにもなされているのではないかと推測するが、窓口となっている方からも回ってこない状況となっており、社内セキュリティ施策を担当する回答者には届いていない。取得の流れとしては、業界団体の窓口が品証部門となっているため、そこからの転送または依頼になる。

＜IT 関連事業者等からの情報提供の状況＞
・ IT 関連事業者の情報は読みやすく配慮されており、当社の背景を理解した情報提供をしてくれるため、有益に思われる。
・ IT ベンダーとのセキュリティに関する会話は増えてきた。民間のセキュリティベンダーは自社製品を念頭に情報提供をしてくるが、買い手として鵜呑みにはできない部分もあると考えている。
・ 脆弱性情報、新製品の情報、セミナー等の情報の案内をいただいている。様々な情報が含まれるため、同種の内容が複数箇所から配信された場合等、情報収集に活用している。

● 大企業向けのヒアリング結果

＜全般的な状況＞
・ 規格・規制動向については業界団体や IT 関連事業者からの情報提供が主である。
・ 外部団体からの情報は量が多く、捌き切れていないのが実情。

＜業界団体からの情報提供の状況＞
・ 医療機器であれば、日本医療機器産業連合会(医機連)からサイバーセキュリティに関する種々の情報が入ってくる。
・ 業種ごとの情報取得のためには、自工会や規格団体からの情報が重要な位置づけとなっている。
・ 業種別 ISAC から、NISC 重要インフラ情報、業界特有の攻撃情報の提供を受けている。
・ CSIRT 協議会から、CSIRT 関連の動向の提供を受けている。

＜IT 関連事業者等からの情報提供の状況＞
・ IT 関連事業者からは動向、製品紹介、ソリューション情報の提供を受けている。
・ 保守ベンダーから、導入機器・ソフトウェアの脆弱性情報の提供を受けている。脆弱性情報を元にアップデートの実施や回避策の実施をしている。

[利用ガイドラインと利用理由]

● 総評
・ 中小企業のエントリーポイントには、それぞれの根拠とともに様々なものが使われている。
・ 大企業では、ISMS やサイバーセキュリティ経営ガイドラインへの対応とともに、NIST CSF のデファクト化が進んでいることが伺える。

● 中小企業向けのヒアリング結果

＜利用ガイドラインとその理由＞
・ メインとしては、経産省ガイドライン(サイバーセキュリティ経営ガイドライン)をベースに、自社の事情を取り込んで策定している。情報セキュリティに関して、ハードルの高い ISO/IEC の準拠を目指すというより、まずは最低限の取組みを進めるところからと考えている。経営層への説明の際に同ガイドラインを参照し、対策の実施は経営層の責任という点を強調して予算確保等をしている。
・ ベースとして利用しているのは、ISO/IEC 27001 であり、認証も取得している。対応前は社内のルールが曖昧で、性善説に基づく運用であったが、対応にあたり様々なルールを策定した。
・ 社内情報システムへの対応は、IPA から配信される「中小企業の情報セキュリティガイドライン」を参考にしている。自身の所掌が IT システムのため上記ガイドが中心だが、医療現場や製品については必ずしも把握していない。感覚としては、医療現場、製造現場は、古い OS や不用意なネットワーク接続等の脆弱な部分が残っている。

● 大企業向けのヒアリング結果

＜ISO/IEC 27001、NIST CSF、サイバーセキュリティ経営ガイドライン等の用途及び活用理由＞

・ 規程、ガイドライン、リスクアセスメント作成
・ セキュリティに関わるシステム設計、運用などの業務に参考としている。
・ 経営ガイドラインについては、内容が非常にわかりやすく、経営層から担当者まで意識すべきことが網羅されている。また、プロモーションもよくなされていると思われる。
・ 会社としては取引先からの要求や業界全体としての動向もあり、ISMS への準拠を基本としている。取引先からのチェックは NIST 文書が使われているため、その対応が主たる動機となる。
・ NIST CSF はサイバーセキュリティのデファクトスタンダードとして理解し、ISO やサイバーセキュリティ経営ガイドラインの事項も踏まえて、社内のセキュリティ方針、システム導入・運用を定める指針にしているため。
・ 取引先からの要望や業界内でのコンセンサスへの対応が主である。社内 IT システムだけでなく、製品セキュリティについても NIST CSF をベースとした対策に辿り着きつつある。
・ NIST CSF については、コンサル会社の提案に基づき昨年度の対策見直しの際に利用した。主な理由としては、実質的にグローバルスタンダードとなっている点、(ISO と比較して)防御の観点だけでなく事後対応まで網羅したものとなっている点が挙げられる。

[ガイドライン利用判断にて重視する観点]

● 総評

・ 大企業では既に ISMS 等をベースに業界慣習や外部環境も考慮した上で社内規定・ポリシーが整備、運用されているところ、新たに発出されるガイドライン等の内容が事業者の既存の方針、方向性と適合しているかという点が重要との意見が多くの事業者から寄せられた。
・ また、各省庁から多数の文書が公開されているところ、内容の実務性が利用意向を左右する側面が指摘されている。

● 大企業向けのヒアリング結果

＜社内方針等との整合＞

・ 内容が弊社の方針、方向性とあっているか。
・ 当社の属する業界と取り巻く環境について、内容がマッチングする際に利用してる。
・ 自社で既存の規定等に基づき業務を行っている中で、特に運用上の課題等がなければ他のガイドライン等を参照する動機は薄い。特別に課題意識が生じた際には、適宜参照することもある。
・ 事業者としては、様々な文書に対応したくはない。新しいものへの対応を求める場合は、ISO/IEC 27001 や NIST CSF のようなスタンダードになっているものとのマッピングが欲しい。こちら側で整合を確認し、既存の対策で対応できているという状況にしたい。

＜内容の実務性＞

・ 現状は、経済産業省、総務省、NISC 等から発行されている文書が多く、すべてを参照するのは難しいという状況。また、内容が実務的に地に足がついていない場合もあり、その場合は利用意向が弱くなる。

＜その他＞

・ セキュリティ要求は比較的収斂した内容になる傾向があるが、データの越境移転については自国保護の観点が入り、個別の要求事項が盛り込まれる流れがあることから特に厄介と捉えている。

[情報源ごとの重要度]

● 総評

・ 業界固有の情報については業界団体が重要なコミュニケーションチャネルとみなされている。
・ その他、利用しているガイドライン等を発行する標準化団体・政府機関(所管省庁等)も主要な情報源とされている。

● 大企業向けのヒアリング結果

＜業界団体からの情報の有用性＞

・ OT 領域は業界によって特徴があるため、一般的な内容よりも、所属する業界団体からの情報が自らの業務に直結して考えやすい、という点で有益。
・ 社会情勢・周辺環境・取引先からの要求を勘案してガイドラインを利用している。業界団体をまず見るが、背景情報の整理に政府機関や国際団体(国連 WP29 等)の情報も参照している。
・ 高圧ガス保安法上の認定を得るにあたりセキュリティ認証が要件に追加された件を例とすると、認定を受けることはビジネスインパクトが大きく、当社としてはほぼ必須対応になる。業界団体のガイドは、規制上の要求事項との結びつきもあることから、優先度は高い。
・ 長期的な施策に必要な情報は価値が高い。評価の観点としては、当社にとって脅威と感じられるかが重要。

＜政府機関及び標準化団体からの情報の有用性＞

・ 政府機関から法政令などで通知・要請があれば強制力が伴うため有効である。
・ 製品セキュリティについては業界団体からの情報、社内 IT ではグローバル標準(ISO/IEC、NIST)に係る情報が、優先度が高い。社内の状況を踏まえ、ISO/IEC 27001 や NIST CSF の動向はウォッチしている。業界内では共通言語が NIST CSF になっている。政府についても防衛省系は SP 800-171 ベースのルールとなっており、NIST による発信の影響力が強い。
・ 自社のセキュリティ対策方針と合致している度合いの高い情報は、対応の優先度が高くなる。例えば、当社では、ISMS をベースとして NIST CSF 及び SP 800-171 も採用しているところ、自社でアセスメントを実施し、不足部分は積極的に対策をする。ISO/IEC 27001 や NIST CSF、SP 800-171 等の改訂動向等は必然的に有用性が高くなる。

[ガイドライン利用における課題]

● 総評

・ 人材面の課題は規模の大小を問わず指摘されている。中小企業では、一般従業員のリテラシーを課題視する傾向がある。
・ 大企業では、事業部門等とのコミュニケーションや対応の優先順位付け、ガイドライン等で求められる対策の水準(対応が義務か任意か、どのレベルの対処で準拠していると言えるか、等)の明確化等、ガイドラインの利用に係るより具体的な課題が挙げられている。

● 中小企業向けのヒアリング結果

＜従業員のセキュリティ意識＞

・ これまで社員 PC にはアプリインストール等の観点で特段規制をかけていなかったが、今後必要な規制をかけていくにあたり社員からの理解が得られるか、取組みが浸透させられるかが課題になると考えている。
・ ISMS 認証取得に向けた対応時に課題となったのは、社員のリテラシーの低さである。自社内の弱点を悪用され、外部から攻撃を受け得ることに対して感度が低かった。これまで具体的に被害を受けた経験がないこともあり、世間で起きていることにも感度が低かった。また、これまで自由にできていてたことがセキュリティ対策の導入によりできなくなることや、そのような施策が利益を生まない(むしろお金がかかる)ことへの抵抗があったように思われる。
・ 従業員のセキュリティ意識の向上とセキュリティ関係のリソース確保が課題と考えている。ヒト・モノ・カネのすべてが足りないが、最も必要なのはカネである。金額面や内容面などに関して経営陣の説得が課題と認識している。

● 大企業向けのヒアリング結果

＜人材面や費用面の課題＞

・ 社内人材の不足、コスト

＜ガイドラインが求める対策水準・推進スケジュール等の不明瞭さ＞
・ 文書によっては、要求のレベル感が読みにくい場合がある。最低限実施すべきことと、推奨事項との差異がわかるようになるとありがたい。
・ ガイドラインの解釈が自社と取引先でぶれる懸念があり、ガイドラインが求めるサイバーセキュリティ対策のレベルが不明瞭(例：IoT、OT セキュリティ対応)。IPA の情報セキュリティ対策ベンチマークも活用しているが、自社チェックとなっており、共通の第三者による審査等でないため厳密さに欠く。
・ 業界団体等によって対策推進のタイムスケジュールを引いているもの(例：自工会)とそうでないものがあり、とくに後者について対応に苦慮している。政府から出るものを含めて、事業者としていつまでに何をすべきなのか、情報発信の際にスケジュール感を明記していただけるとありがたい。
＜社内他部門とのコミュニケーション＞
・ ビジネスの邪魔にならないよう、セキュリティ対応に係る工数を現実的なレベルに落とさねばならない点が課題。対策は、儀式化しないよう業務に落とさねばならない(特に現場)。対応に優先度を付けて、ステークホルダーを説得しつつ、対応を進める点に配慮している。限られた工数の中で納得感を生みながら対応を進めることが課題である。
＜その他＞
・ 過去の社内規定改訂の際は、ベースとする ISO/IEC 27001 の改定内容が多岐にわたったため、チェック個所が多く、手間がかかった。

[政府への期待事項]
● 総評
・ 企業規模を問わず、補助金や税制優遇等の金銭的支援を要望する点は共通している。
・ 中小企業からは、周知・講習会にて、従業員向けのライトな内容、担当者向けには参考事例、費用の紹介等を求める声があった。
・ 大企業からは、チェックシート等への対応が繁忙であり、負担軽減を可能にする取組みを求めるという意見が複数挙がった。

● 中小企業向けのヒアリング結果
＜周知・講習会に期待する事項＞
・ 周知・講習会では、事例紹介として、自社と同じような環境にある会社(事業規模など、共通点が多いところ)の取組みがあれば参考になる。ガイドラインの内容の説明だけでなく、実際の適用の説明があると腹落ち感がある。また、対策実施の費用感の参考があるとありがたい。
・ 講習会を実施する際に、参加をより強く要請してほしい。また、案内時の宛先として個社名を出して案内を発出してほしい。当社にはガバナンス専門の部署がないが、専門外の方も対象範囲であり参加できるという周知にしてほしい。既存の講習会等にはそのような者が参加しづらいと感じる。
・ ウェビナーによる従業員向けの内容で時間は 10 分程度のものがありがたい。セキュリティ、機密情報の取扱関係でセキュリティに必ずしも興味がない層へ向けたコンテンツを想定する。また、ランサムウェア関係の実態等がガイドラインとして配信されることを希望する。
＜その他、政府に期待する事項＞
・ 税制優遇のような金銭支援策、そのための基準が明確になると社内の説得がしやすくなりありがたい。
・ 金銭面でセキュリティ対策に対する補助金は強化してほしい。自社でも対策実施の結果、かなりのカネがかかった。それらに対する補助がもっと幅広くなれば、様々な事業者が対応しやすくなると思う。
・ リスクアセスメント、セキュリティコンサルタントに対する補助金等の支援制度があれば可視化できていないリスクを認識することが可能になると考える。リスクアセスメントの実施は当社には高価で実施が難しい。

● 大企業向けのヒアリング結果

＜金銭的支援策等＞

・ 資金補助、税制優遇
・ 実施者がメリットを享受できる仕組み、ルール作り

＜より踏み込んだ脆弱性情報の開示＞

・ 脆弱性に関する情報の発信はなされているが、実務対応上有用となる脆弱性のメカニズムや仕組みの解析結果の開示などがあまりなされていない。インテリジェンス情報については、政府等からもう一歩進めた情報開示が必要と考える。

＜サプライチェーンセキュリティ対応の効率化・負担軽減＞

・ 製品の輸出入に関し、日本国内のガイドライン準拠が、他国においても基準をみたすとする多国間の取り決めをしてほしい。
・ 各国各企業からのサイバーセキュリティアンケート(要求)の授受が発生し、個別の要求事項も含まれることから、対応が煩忙である(各社セキュリティポリシーが異なるため、個別対応になる点は理解しているが)。自工会ガイドは国内が対象のため、海外から注文があった際に課題がある。
・ ユーザ団体の部会等に参加すると、本業に支障が出るレベルでチェックシート(への対応)に溺れているという意見が多く出る。昨今、サプライチェーンセキュリティ強化の流れの中で、当社からチェックを求めることも、他社から求められることも出てきており、内容が異なっている場合がある。工数を削減しつつ効果的に機能する施策をいただければありがたい。

C. まとめ

(1) 結果の要点

アンケート調査及び後続のヒアリング調査を通じて、概ね以下のような知見を得ることができた。

＜CPSF 等の認知・利用状況＞

・ CPSF/IoT-SSF/DMF の認知率・利用率は、サイバーセキュリティ経営ガイドラインや ISMS のそれよりも低かった。
・ 対象事業者、特に大企業においては、ISMS や NIST CSF をスタンダードとして理解し、社内のセキュリティ方針、システム導入・運用を定める指針にしているケースが多くみられた。
・ 全般的に従業員数・売上の大きい事業者の方がガイドラインをよく認知または利用していた。
・ 事業者がセキュリティに関する情報収集を実施していたとしても、経営ガイドライン、ISMS、NIST CSF と比較して、CPSF 等の認知まで行き着かない事業者の割合が大きかった。
・ ガイドライン認知のきっかけは、「インターネット」が最も多く、「社外の IT 関連事業者」、「業界団体」、「政府関係機関」が次いだ。全般的な傾向にはガイドライン間で大きな差異はなかった。

＜セキュリティに関する情報収集の状況＞

・ 従業員規模・売上規模が大きくなるほど、セキュリティ情報収集に熱心な傾向があった。全体を通じて、情報収集をまったく実施していない事業者は少なかった。
・ インターネット上の主な参照先としては、内閣サイバーセキュリティセンター(政府動向)、JPCERT/CC・IPA・製品ベンダー(脆弱性等のセキュリティ技術情報)、経済産業省(ガイドライン)等が挙げられた。
・ 効率性等の観点から外部団体(業界団体、IT 事業者)からの情報提供のメリットを指摘する事業者が大企業、中小企業の双方で見られた。特にガイドライン・規制等の動向については、スクリーニング済みの情報が得られるということで、係る手段の有用性を強調する意見があった。
・ 業界団体からの情報は自社の業務に直結して考えやすいという点で有益という見解があった。

＜ガイドライン等利用の判断要因＞

・ ガイドライン等の採否に際して、対象ガイドライン等の内容が事業者の既存の方針や方向性と適合しているか、内容の実務性が認められるか、当該ガイドライン等の認知度及び他社の活用

状況等が採否の判断指針とされていた。

＜ガイドライン等利用における課題＞

・ ガイドライン利用の課題としては、人材不足が最も多く回答されており、不明確な進め方や手順、予算の制約が次いで多く選択されていた。

(2) 今後の方向性に関する提言

(1)までに明らかとなったように、CPSF 等の認知率・利用率は、他の既存ガイドライン等と比較して低かった。まず、認知率については事業者によるセキュリティ情報収集活動の実施レベルにより、仮説をいくつかに分類することが可能と考える。なお、情報収集をまったく実施していない事業者はかなり少数だったことから、以下では検討をスキップしている。

a. インターネット上の公開情報を中心に収集している事業者(主に中小企業)の認知をどのように向上させるか。

a-1. 現状 CPSF に関連したガイドライン等の情報が掲載された経済産業省ページに事業者が行きついていない場合、より参照される頻度が高い、あるいは幅広い事業者から参照されているサイト(例：IPA 情報セキュリティ Web サイト)に情報を掲載することが有効ではないか。

a-2. CPSF に関連したガイドライン等の情報が掲載されたページに事業者が行きついているにもかかわらずガイドライン等が認知されていない場合、当該 Web サイトの構造や内容に改善が必要なのではないか。

b. 定常的に複数のチャネルを活用して情報収集を実施している事業者(主に大企業)の認知をどのように向上させるか。

b-1. 現状実施している政府機関サイトを通じた普及に加え、業界団体と協議のうえ、当該団体を通じた情報提供、その他のサポートの実施が有効ではないか。

b-2. b-1 を検討する際、対象の団体の業界におけるプレゼンス(業界内で参画している企業の割合や影響力、IT またはサイバーセキュリティに関する活動実績)を十分考慮することが必要ではないか。

b-3. b-1 を検討する際、対象の団体が情報提供やサポートの実施に関与するインセンティブの整理が必要ではないか。

また、今回認知率や利用率等の調査対象としたガイドライン等に加え、分野別 SWG で策定されるガイドライン群についても、今後の認知・利用の拡大を図るにあたって、同様の観点からの検討が必要になることも考えられる。その際、基礎データとして、今回 CPSF 等を対象に実施したような認知状況・利用状況、セキュリティ対策推進上の課題等の調査が実施されることも考え得る。

次に、利用率の向上を企図するにあたって、課題となっている事項や必要な施策について検討したところ、(1)で示した結果から、以下のような検討課題があるのではないかと想定される。

a. 業種横断、あるいは業種ごとのセキュリティ施策推進方針の特定

政府機関からガイドライン等の普及を包括的に実施しようとする際、業種横断的な適用範囲を持つものと業種を絞ったものの双方を考慮し、普及するガイドライン(群)とそれらの位置づけ、適用のロードマップ等を明確にしておくことが想定される。その際、事業者にとって、多数のガイドライン等に対応することはリソースの観点から困難が想定されることから、対象ガイドライン等の内容が事業者の既存の方針や方向性と適合しているか等も考慮のうえ、自身が参照し準拠すべき法令やガイドライン等が無駄なく明確にされていることが望ましい。

＜施策例＞

a-1. 対象(例：業種)ごとの準拠を推奨する法令またはガイドライン等の整理
a-2. 業界団体等と十分に協議のうえ、上記適用に向けたロードマップ等の策定
a-3. 対象範囲において既に重複した適用範囲を持つ複数のガイドライン等が存在する場合、それら複数ガイドライン等の内容面での調整やその他の相互運用性向上に向けた施策等

b. ガイドライン等の策定・普及促進における業界団体との連携、役割分担

ガイドライン等の普及にあたっては、それらを発行する政府機関からの情報を直接取得することに加え、業界団体や IT 関連事業者、取引先からの情報提供が一定の役割を有しているところ、それらの団体との協調が念頭に置かれるべきである。特に、業界団体は、大企業を中心に情報提供主体としての役割、有用性を評価されており、政府機関としても係るチャネルを利用したガイドライン等の普及の優先度が高いのではないかと考えられる。政府機関としても、多数存在する様々な業種の事業者それぞれに情報を届け、その実施を支援するための施策を単独で実施することは困難であることから、役割分担等を検討するメリットは大きい。

＜施策例＞

b-1. 既に分野別のガイドライン等を策定している場合、普及の受け皿となり得る業界団体の選定
b-2. 上記で特定された団体との目標・具体的な普及施策の協議、共有
b-3. (業種別の成果を策定する場合)ガイドライン等の策定段階における団体からのコミット確保
b-4. 意図された形式による政府側、業界団体側双方からの普及施策の実施

<参考文献>

1 “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)
2 ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines, (https://www.iso.org/standard/44373.html)
3 山下真 (国立研究開発法人 情報通信研究機構), “ISO/IEC 27001 改定内容と関連規格の動向” , 2022 年 12 月 16 日 (https://www.jnsa.org/seminar/2022/isms2022/kouen1.pdf)
4 一般社団法人情報マネジメントシステム認定センター(ISMS-AC), “ISMS 適合性評価制度 ISO/IEC 27001:2022 への対応について”, 2022 年 10 月 25 日 (https://isms.jp/topics/news/20221025.html?mm221125)
5 土屋直子 (NTT テクノクロス株式会社), ISO/IEC 27002 改定の解説, 2022 年 12 月 16 日 (https://www.jnsa.org/seminar/2022/isms2022/kouen2.pdf)
6 SG17 - Study Group Structure (Study Period 2022-2024) (https://www.itu.int/net4/ITU-T/lists/sgstructure.aspx?Group=17&Period=17)
7 Question 6/17 (Study Period 2022-2024) (https://www.itu.int/net4/ITU-T/lists/q-text.aspx?Group=17&Period=17&QNo=6&Lang=en)
8 ITU-T work programme (https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=6)
9 Question 8/17 (Study Period 2022-2024) (https://www.itu.int/net4/ITU-T/lists/q-text.aspx?Group=17&Period=17&QNo=8&Lang=en)
10 ITU-T work programme (https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=8)
11 ITU-T X.1644 として内容が確定している。(https://www.itu.int/md/T22-SG17-R-0021)
12 IoT セキュリティ・セーフティ・フレームワーク Version 1.0 適用実証報告書
13 経済産業省, “第 7 回『第 2 層：フィジカル空間とサイバー空間のつながり』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” , 2023 年 2 月 17 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/007.html)
14 DMF 適用実証報告書
15 経済産業省, “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” , 2023 年 2 月 8 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/008.html)
16 回答の回収時期の関係で、実際に分析に使用したサンプル数は 396 社となっている。
17 ここで、「CPSF 等」とは、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)、IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)、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(DMF)の 3 種の文書を指している。

<商標又は登録商標>

別紙1 公開情報等の調査 IoT関連文献

調査文献一覧

項番	国・地域	文献等の名称	URL	作成機関	作成時期	文書種別	調査項目
1	日本	電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン	https://www.meti.go.jp/product_safety/consumer/system/iot.html	経済産業省	2021年	ガイドライン	2
2	日本	情報セキュリティ知識項目 SecBoK 2021概要	https://www.jnsa.org/result/skillmap/data/01_SecBoK2021-gaiyo.pdf	JNSA	2021年	ガイドライン	2、3
3	米国	国家サイバーセキュリティの向上に関する大統領令 Executive Order on Improving the Nation's Cybersecurity	https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/	大統領府 (ホワイトハウス)	2021年	政策	1
4	米国	Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products	https://csrc.nist.gov/pubs/cswp/24/criteria-for-cybersecurity-labeling-for-consumer-i/final	NIST	2022年	ガイドライン	2、3
5	欧州	EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0	https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1	ENISA	2021年	ガイドライン	2,4,5
6	欧州	ETSI TS 103 701 Conformance Assessment of Baseline Requirements	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf	ETSI	2021年	ガイドライン	2,5

調査文献一覧

項番	国・地域	文献等の名称	URL	作成機関	作成時期	文書種別	調査項目
7	欧州	Proposal for a REGULATION on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020	https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act	EU	2022年	政策	1,2,4,5
8	欧州	Proposal for a REGULATION on machinery products	https://ec.europa.eu/docsroom/documents/45508	EU	2021年	政策	1,2,5
9	欧州	COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.007.01.0006.01.ENG&toc=OJ:L:2022:007:TOC	EU	2022年	政策	1,2,5
10	欧州	BSI Internet of Things Testing, verification and certification solutions for a smarter, more secure world（BSI Kitemark）	https://www.bsigroup.com/globalassets/localfiles/en-in/resources/bsi-solutions.pdf	英国	2020年	IoT機器認証制度 ※制度概要/要件/評価方法等	5
11	中国	サイバーセキュリティ審査弁法	http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm	国家インターネット情報弁公室　他	2022年改正	政策	1

調査項目

- 「調査文献一覧表」の最右列「調査項目」に記載されている番号は下表の番号にそれぞれ対応

調査項目（IoT機器関連）	
1	文献に記述されている、ステークホルダー間でのIoT機器やシステム等のセキュリティ確保に向けた具体的な手段、方針、方向性、あるいはその方針を促進する規則・ルールなど (文献の狙い)
2	既に国内外で作成されているIoT機器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、書誌的情報（国・地域、適用分野、策定者、対象者、遵守義務、普及状況など）
3	IoT-SSFの更なる具体化に向けて参考となり得る取組み
4	IoT機器等の差異や区分（カテゴリ）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
5	IoT機器等の信頼性を確認するための技術的又は制度的枠組 (例:各種認証制度)

電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン

1	概要	家電製品等がインターネット環境で使われることで想定されるリスクについて、誤操作のみならず、通信遮断やサイバー攻撃を含めた場合であっても、安全が確実に確保されるよう対策を取ることを推進する方向性にある。

2	書誌的情報	名称	電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン		
		主旨	近年、インターネットが広く普及し、スマートフォンやパソコンに限らず、家電製品やガス製品がインターネットに接続され、新たなサービスと連携し、使用者に新たな便益を提供することが想定されている。一方、家電製品やガス製品がインターネット環境で使われる状況下においても、製品安全が確実に確保されるよう対策を取ることが必要である。こうした観点から、新たに電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドラインが制定された。		
		文献タイプ	ガイドライン		
		国・地域	日本	適用分野	スマートフォンやパソコンに限らず、家電製品、ガス製品など。 通信機能を含む機能全体の仕様を機器の製造事業者等が決めるものに限っている。
		策定者	経済産業省	対象者	通信機能を含む機能全体の仕様を機器の製造事業者等。
		順守義務	本ガイドラインは、電気用品、ガス用品等製品のIoT化等による安全確保の在り方を関係業界団体に周知し、必要な対策を求めるものである。		
		普及状況	本ガイドラインは、令和3年4月28日から適用する。		
		策定年	2021年	ページ数	14

3	IoT-SSFに参考となる取組	通信遮断やサイバー攻撃を含めた新たなリスク(間接的な被害等によるリスク及び遠隔操作によるリスク)に対応するため、スリーステップメソッドの考え方を拡大した。ガイドラインでは、安全確保のためのリスク低減対策(間接被害等に対するリスク低減対策や遠隔操作に対するリスク低減対策)の概略を示している。

電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン

4	IoT機器の区分・水準・対策	例えば、アイロン、ミシン、ヘアケア用機器、ほとんどの調理用機器など「遠隔操作に不向き」であり、周辺に危害を及ぼすリスクがあるため、基本的に遠隔操作を行わない機器として整理する。今後、こうした機器の遠隔操作の是非を検討する場合には、「遠隔操作して良い機器である」と、誤ったメッセージを消費者に伝えることのないよう、丁寧な検討が必要である、と述べている。

5	技術的・制度的枠組	記載なし。

関連URL	Safety aspects — Guidelines for their inclusion in standards(ガイドライン) standardshttps://www.iso.org/standard/53940.html IEC 60335-1(家電品等の安全に関する国際標準) http://106.38.59.21:8080/userfiles/fedac97ffde8414e898733b759249bc0/files/teckSolution/2020/04/IEC_60335-1_2001%2BA1_2004(E)(1).pdf 解釈別表第八に係わる遠隔操作(遠隔操作に関する規定等) https://www.eam-rc.jp/pdf/result/remote_control_BP8_report20191118.pdf 解釈別表第四に係わる遠隔操作(遠隔操作に関する規定等) https://www.eam-rc.jp/pdf/result/remote_control_BP4_report20191118.pdf

IoT機器関連文献 #1：主な調査項目

電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン

2. 概要

インターネットが広く普及し、スマートフォンやパソコンに限らず、家電製品やガス製品がインターネットに接続され、新たなサービスと連携し、使用者に新たな便益を提供することが想定されている。
一方、家電製品やガス製品がインターネット環境で使われる状況下においても、製品安全が確実に確保されるよう対策を取ることが必要である。
こうした観点から、新たに電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドラインが制定された。
例えば、スマートスピーカーによる音声アシスタント機能を通じ家電製品が遠隔操作されるなど、製品安全4法(消費生活用製品安全法、電気用品安全法、液化石油ガスの保安の確保及び取引の適正化に関する法律、ガス事業法)の対象製品も新たなサービスと連携し、使用者に新たな便益が提供されていくことが想定される。
一方で、一般家庭にあるこれら製品の脆弱性へのサイバー攻撃も懸念されており、通信基盤やサービス基盤が不正にアクセスされることが想定される。
こうした中、家電製品等がインターネット環境で使われることで想定されるリスクについて、誤操作のみならず、通信遮断やサイバー攻撃を含めた場合であっても、安全が確実に確保されるよう対策を取ることが必要である。
このような観点から、「IoT化等が考えられる電気用品等機器に係る製品安全確保の在り方に関する検討会」を開催し、電気用品、ガス用品等製品のIoT化等による安全確保の在り方をとりまとめた。

IoT機器関連文献 #2：概要

情報セキュリティ知識項目　SecBoK 2021概要

1	概要	JNSA教育部会では、独立行政法人情報処理推進機構(IPA)からの委託事業の実施を契機として、情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理した「情報セキュリティスキルマップ」の作成に2003年度から取り組んでいる。2007年からは名称を「セキュリティ知識分野 SecBoK(Security Body of Knowledge)」と改め、2016年以降は定期的に改定を行っている。 SecBoK 2021は、セキュリティ専門人材以外の人間も容易に利用できるように改定され、セキュリティ人材不足対応への貢献が見込まれている。

2	書誌的情報	名称	情報セキュリティ知識項目　SecBoK 2021概要		
		主旨	SecBokは、セキュリティ人材育成の参考資料として活用されているガイドブックである。SecBoK 2021は、セキュリティ専門人材だけではなく、「プラス・セキュリティ人材」やジョブチェンジ、組織異動する人間等も容易に利用できるように「使いやすい形」に改定されている。		
		文献タイプ	ガイドライン		
		国・地域	日本(グローバル標準との連携で、海外での利用も推進する予定である。)	適用分野	情報セキュリティ関連業務に携わる人材が身につけるべき知識とスキル。
		策定者	JNSA(日本ネットワークセキュリティ協会)	対象者	セキュリティ専門人材、プラス・セキュリティ人材、ジョブチェンジ及び組織異動する人間等。
		順守義務	SecBok 2021は、ディクショナリー的な位置付けとして多くの人間に利用されることを目的としている。		
		普及状況	SecBok 2021は、2021年5月17日に公開されている。		
		策定年	2021年	ページ数	15

3	IoT-SSFに参考となる取組	言及なし。 備考：SecBoK2021本体の資料(SecBoK2021_V1.0)が示す「NIST SP800-181スキル項目」のうち、「IoT-SSFの取組に関連する可能性がある項目」は幾つか存在する。

4	IoT機器の区分・水準・対策	記載なし。
5	技術的・制度的枠組	情報系大学のカリキュラム標準である「情報セキュリティ(J17-CyberSecurity*)」と連携している。 *J17-CyberSecurity: 情報処理学会では2007年度にカリキュラム標準J07を策定し公表した。これは、世界標準である米国ACM/IEEE-CSのCC2001-CC2005を土台として、日本の情報専門教育の状況に対応した見直しを行って、コンピュータ科学(J07-CS)/情報システム(J07-IS)/ソフトウェアエンジニアリング(J07-SE)/コンピュータエンジニアリング(J07-CE)/インフォメーションテクノロジ(J07-IT)の５分野に一般情報教育(J07-GE)を加えた６カリキュラム標準からなるものとした。J07の策定から10年が経過し、技術の内容が大きく変化したこともあり、全面的な見直しを行い、J17として公表することとした。J17は、従来からの６カリキュラム標準に加えて、世の動きに合わせて情報セキュリティ、データサイエンスという発展中の対象領域についても、別立てに側面別カリキュラム標準をおく方針を立てている。ただし、現時点では、サイバーセキュリティに対する側面別カリキュラム標準J17-CyberSecurityの素案だけを提示する段階にある。 https://www.ipsj.or.jp/annai/committee/education/j07/curriculum_j17.html
関連URL		NIST SP800-181rev.1(サイバーセキュリティのための労働力フレームワーク) https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final J17-CyberSecurity(情報処理学会のカリキュラム標準) https://www.ipsj.or.jp/annai/committee/education/j07/curriculum_j17.html ACM/IEEE-CSのCC2001-CC2005(コンピューティング カリキュラム) https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf

概要

JNSAは、SecBoK(Security Body of Knowledge)は、「ディクショナリー的な位置付けとして多くの人々に利用してもらうこと」が目的であることを再確認した。
そこで、セキュリティ専門人材だけではなく、近年その必要性と人材不足が叫ばれている「プラス・セキュリティ人材」への対応を実現した。
またジョブチェンジ及び組織異動(事業部門→セキュリティ/IT、セキュリティ/IT→事業部門)する人間も容易に利用できるように改定した。
SecBok2021は、Job description(ジョブディスクリプション)の考え方を広め、人材エコシステムの推進に貢献するように作成されている。
セキュリティ人材の可視化が様々な方面で進んでいるが、可視化の際のスキル項目として利用してもらい、セキュリティ人材不足対応に貢献することが見込まれている。
SecBok2021は日本国内のみではなく、グローバル標準との連携で、海外での利用も推進する予定である。

IoT-SSFに参考となる取組

「IoT-SSFに関連する可能性がある項目」の例：
- 日本国のサイバーセキュリティに関わる刑法、民法及び自社における人事、コンプライアンス、セキュリティポリシーなど各種規程に関する知識
- サイバー防衛活動についての関連法、法的権限、制限及び規制に関する知識
- 重要なインフラストラクチャのサイバーセキュリティに関連する法律、ポリシー、手続き又はガバナンスに関する知識
- サイバーセキュリティ上の標的とエクスプロイトを管理する適用法令、法律、規則、ポリシーに関する知識
- サイバー法とそのサイバーセキュリティ計画への影響に関する知識
- サイバー法及び法的考察並びにそのサイバーセキュリティ計画への影響に関する知識
- プライバシー影響評価に関する知識
- 暗号及びその他のセキュリティ技術に関連する輸入/輸出規制に関する知識
- ネットワーク及び関連標準のためのサービス管理の概念に関する知識(例：ITILの現行バージョン)
- 政府のサイバーセキュリティ人材フレームワーク、仕事上のロール、関連するタスク、知識、スキル、能力に関する知識
- サイバーセキュリティに関連する海外へのディスクロージャーポリシーと輸出入規制に関する知識
- 個人識別情報(PII)データセキュリティ基準に関する知識
- PCI(Payment Card Industry)データセキュリティ基準に関する知識
- 個人健康情報(PHI)データセキュリティ基準に関する知識

・備考　後述のSecBoK2021本体の資料(SecBoK2021_V1.0)では、「SecBoKの16の役割(ロール)」(例：POC、リサーチャー、キュレーター等)と「NISTSP800-181スキル項目」の約1,150のスキル項目とのマッピングを表示している。

国家サイバーセキュリティの向上に関する大統領令 Executive Order on Improving the Nation's Cybersecurity

1	概要	米国は、公共部門、民間部門、そして最終的には米国民の安全とプライバシーを脅かす、持続的でますます巧妙化する悪意のあるサイバー キャンペーンに直面している。悪意のあるサイバー アクターから国を守るには、連邦政府が民間部門と提携する必要がある。

2	書誌的情報	名称	国家サイバーセキュリティの向上に関する大統領令 Executive Order on Improving the Nation's Cybersecurity		
		主旨	国家サイバーセキュリティの向上については、サイバーインシデントの防止、検出、評価、及び修復が最優先事項であり、国家及び経済の安全保障にとって不可欠である。連邦政府は、アメリカの生活様式を支える重要な制度を守るために、連邦政府が民間部門と提携し、多額の投資を行う必要がある。		
		文献タイプ	政策		
		国・地域	米国	適用分野	情報技術(IT)と運用技術(OT)を含めたサイバーセキュリティ確保が必要な分野
		策定者	大統領府	対象者	連邦政府、及びクラウドサービスプロバイダー等の民間部門
		順守義務	憲法及びアメリカ合衆国の法律によって大統領に与えられた権限により、発せられた命令である。		
		普及状況	命令内容によって「・・日以内に・・・をするものとする」というような形で実行期限が定められている。		
		策定年	2021年	ページ数	ページ表記無し(A4換算約20ページ)

3	IoT-SSFに参考となる取組	「民間部門は、絶え間なく変化する脅威環境に適応し、製品が安全に構築及び運用されることを保証し、連邦政府と提携してより安全なサイバースペースを促進する必要がある」と述べている。 クラウド テクノロジへの移行では、「実行可能な限りゼロトラストアーキテクチャを採用する必要がある」と述べている。(ゼロトラストの考え方は、IoTシステムのセキュリティ課題の解決策として注目されている。) 「エンドポイントの検出と対応(EDR)イニシアチブを展開して、連邦政府のインフラストラクチャ内でのサイバーセキュリティ インシデントのプロアクティブな検出、積極的なサイバーハンティング、封じ込めと修復、及びインシデント対応をサポートするものとする」と述べている。

IoT機器関連文献 #3：概要

国家サイバーセキュリティの向上に関する大統領令 Executive Order on Improving the Nation's Cybersecurity

4	IoT機器の区分・水準・対策	-

5	技術的・制度的枠組	命令の日付から90日以内に、OMB長官は、CISA長官を通じて行動する国土安全保障長官、及びFedRAMP* を通じて行動する一般サービス管理者と協議して、連邦クラウドセキュリティを開発するものとする。 *Federal Risk and Authorization Management Program(FedRAMP) FedRAMPはクラウドサービスオファリングのセキュリティ認証に対する標準化されたアプローチを提供している。 エンドポイントの検出と対応(EDR)イニシアチブを展開して、連邦政府のインフラストラクチャ内でのサイバーセキュリティインシデントのプロアクティブな検出、積極的なサイバー ハンティング、封じ込めと修復、及びインシデント対応をサポートするものとする。

関連URL	Federal Risk and Authorization Management Program(FedRAMP)(クラウド サービス オファリングのセキュリティ認証に対する標準化されたアプローチ説明) https://www.fedramp.gov/ Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT)Products(IoT製品のサイバーセキュリティ ラベル付けの推奨基準) https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final

IoT機器関連文献 #3：主な調査項目

国家サイバーセキュリティの向上に関する大統領令 Executive Order on Improving the Nation's Cybersecurity

狙い

1.サイバーインシデントの防止、検出、評価、及び修復が最優先事項であり、国家及び経済の安全保障にとって不可欠である。
2.この命令の日付から60日以内に、行政管理予算局(OMB)の局長は、協議の上、連邦調達規則(FAR)及び国防連邦調達規則補足の契約要件及びIT及びOTサービスプロバイダーとの契約に関する文言を確認し、その要件及び文言の更新を推奨するものとする。
3.この命令の日付から60日以内に、各機関の長はゼロトラストアーキテクチャを実装するための計画を作成する。
また、90日以内に、OMB長官は、国土安全保障長官、及びFedRAMPを通じて行動する一般サービス管理者と協議して、連邦クラウドセキュリティを開発するものとする。
4.連邦政府は、ソフトウェアサプライチェーンのセキュリティと完全性を迅速に改善するための措置を講じる必要がある。
この命令により、商務長官は、NISTの局長を通じて行動し、連邦政府、民間部門、学界、及びその他の適切な関係者と、既存の標準、ツールを特定又は開発するための様々な行動(消費者ラベリングプログラム等)を行うこととする。
5.国土安全保障長官は、司法長官と協議の上、サイバー安全審査委員会を設立するものとする。
6.この命令の日付から120日以内に、国土安全保障長官は、サイバーセキュリティの脆弱性及びインシデント対応活動の計画と実施に使用される運用手順の標準セット(プレイブック)を作成するものとする。
7.連邦政府は、そのネットワーク上のサイバーセキュリティの脆弱性とインシデントの早期発見を最大化するために、すべての適切なリソースと権限を採用する。
FCEB機関は、エンドポイントの検出と対応(EDR)イニシアチブを展開して、連邦政府のインフラストラクチャ内でのサイバーセキュリティインシデントのプロアクティブな検出、積極的なサイバーハンティング、封じ込めと修復、及びインシデント対応をサポートするものとする。
この命令の日から30日以内に、国土安全保障長官は、ホストレベルの可視性、属性をサポートするためのEDRイニシアチブを実施するためのオプションに関する勧告をOMB局長に提供するものとする。
8.政府機関とそのITサービスプロバイダーが収集、維持するデータが、FCEB情報システムでのサイバーインシデントに対処するために必要な場合は、要求に応じて国土安全保障長官とFBIに提供することが不可欠である。
9.この命令の日付から60日以内に、国防長官は、国家情報長官及びCNSSと調整し、APNSAと協議して、国家管理者を通じて行動し、国家安全保障システム要件を採用するものとする。要件は、国家安全保障覚書(NSM)で成文化されるものとする。

IoT機器関連文献 #4：概要

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products

1	概要	2021年5月12日に発行された大統領令(EO)14028、「国家サイバーセキュリティの向上に関する大統領令(Executive Order on Improving the Nation's Cybersecurity)」は、IoT 製品のサイバーセキュリティラベル付けの取り組みの基準を開発するよう国立標準技術研究所(NIST)に指示した。 具体的には、NISTは、「消費者ラベリングプログラムのIoTサイバーセキュリティ基準を特定し、そのような消費者ラベリングプログラムが、類似の既存の政府プログラムと連携して運用できるか、又はモデル化できるかどうかを検討する」ように指示された。

2	書誌的情報	名称	Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT)Products(消費者向けIoT製品のサイバーセキュリティ ラベル付けの推奨基準)		
		主旨	IoT製品のサイバーセキュリティ ラベル付けの取り組みの推奨基準について説明している。		
		文献タイプ	ガイドライン		
		国・地域	米国	適用分野	コンシューマーIoT製品
		策定者	National Institute of Standards and Technology	対象者	コンシューマーIoT製品ラベル付けプログラムを作成するスキーム所有者
		順守義務	このドキュメントでは、コンシューマーIoT製品のラベリングプログラムの開発に関する考慮事項と推奨事項について説明している。		
		普及状況	現在の普及状況については不明。(大統領令(EO)14028の日付(2021年5月12日)から270日以内に、消費者ラベリングプログラムのIoTサイバーセキュリティ基準を特定し、そのような消費者ラベリングプログラムが運用できるか、又はモデル化できるかどうかを検討する」とされている。)		
		策定年	2022年	ページ数	24

3	IoT-SSFに参考となる取組	IoT-SSFは、サイバー空間とフィジカル空間の境界は、センサやアクチュエータなどから構成される、いわゆるIoTのシステムによって成立している、と述べている。本ガイドラインは、消費者向けIoT製品の範囲内で、消費者向けIoT製品ラベリングプログラムの一環としてIoT製品とIoT製品開発者に期待されるサイバーセキュリティを定義するために、ベースライン製品基準を推奨している。

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products

4	IoT機器の区分・水準・対策	ネットワークへの接続において、IoT製品は、NISTが特定した「ベースライン製品基準」に対する共通のニーズを持っている。この共通のベースラインの後、上位層を定義するための単一の基準はない。革新的な新しいタイプと新しいリスクを伴うIoT製品の用途が引き続き出現するため、特定されたベースラインを超える基準が出てくる場合がある。
5	技術的・制度的枠組	
関連URL		NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers(IoT デバイス メーカー向けの基本的なサイバーセキュリティ活動) https://csrc.nist.gov/publications/detail/nistir/8259/final NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline(デバイスのサイバーセキュリティ機能のコア ベースライン) https://csrc.nist.gov/publications/detail/nistir/8259a/final NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline(IoT の非技術的なサポート機能のコア ベースライン) https://csrc.nist.gov/publications/detail/nistir/8259b/final ANSI / CTA-2088(デバイス及びデバイス システムのベースライン サイバーセキュリティ基準) https://shop.cta.tech/products/https-cdn-cta-tech-cta-media-media-shop-standards-2020-ansi-cta-2088-a-final-pdf

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products

概要

1.このドキュメントでは、消費者向けモノのインターネット(IoT)製品のサイバーセキュリティラベル付けの取り組みの推奨基準について説明する。

2.ベースライン製品基準
- 消費者向けIoT製品の購入と保守について、消費者が「情報に基づいた意思決定」を行えるようにするためのサイバーセキュリティラベリングプログラムに関して以下のような「推奨されるベースライン製品基準」が設定されている。

  ➢資産の識別:IoT製品は一意に識別可能である。
  ➢製品構成:IoT製品の構成は変更可能である。
  ➢データ保護:IoT製品とそのコンポーネントは、保存及び送信されるデータを、不正アクセス、開示、及び変更から保護する。
  ➢インターフェイスアクセス制御:論理アクセスを、許可された個人、サービス、及びIoT製品コンポーネントのみに制限する。
  ➢ソフトウェアの更新:安全で構成可能なメカニズムを使用してのみ、承認された個人、サービス、その他のIoT製品コンポーネントによって更新できる。
  ➢サイバーセキュリティ状態認識:IoT製品は、サイバーセキュリティインシデントの検出をサポートする。
  ➢文書化:IoT製品開発者は、IoT製品とその製品コンポーネントのサイバーセキュリティに関連する情報を作成、収集、及び保存する。
  ➢情報とクエリの受信:IoT製品開発者はサイバーセキュリティに関連する情報に関する顧客などからのクエリに応答する能力をもつ。
  ➢情報の普及:IoT製品開発者は、サイバーセキュリティに関連する情報を普及させる。
  ➢製品の教育と認識:IoT製品開発者は、IoT製品エコシステムの顧客やその他のユーザーの認識を高め、教育する。

- ネットワークへの接続において、IoT製品は、上記のベースライン基準に対する共通のニーズを持っている。
  この共通のベースラインの後、上位層を定義するための単一の基準はない。
  革新的な新しいタイプと新しいリスクを伴うIoT製品の用途が引き続き出現するため、特定されたベースラインを超える基準が出てくる場合がある。

3.ラベル付けに関する考慮事項
- ラベリングアプローチは、提案されたIoT製品のサイバーセキュリティラベルの技術基準に適している必要がある。
- ラベリングアプローチは、サイバーセキュリティの専門知識を必要とせずに、さまざまな消費者が使用できる必要がある。
- IoTサイバーセキュリティラベルにバイナリラベルを採用することを推奨している。
- ラベルは、購入時と場所(店内又はオンライン)、及び購入後に消費者が利用できる必要がある。
- バイナリラベルの採用は、強力な消費者教育キャンペーンを伴う必要がある。

IoT機器関連文献 #4：主要な調査項目

Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products

IoT-SSFに参考となる取組

IoT-SSFではサイバー空間とフィジカル空間の境界を第2層と呼んでおり、その境界において情報が正確に変換されること、つまり転写機能の正確性を確保することを、第2層における信頼性の基点としている。
IoT-SSFでは、サイバー空間とフィジカル空間の境界は、例えば前記の転写機能を担うセンサやアクチュエータなどから構成される、いわゆるIoTのシステムによって成立している、と述べている。
https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf

本ガイドラインでNISTは、消費者向けIoT製品ラベリングプログラムの一環としてIoT製品とIoT製品開発者に期待されるサイバーセキュリティを定義するために、次のベースライン製品基準を推奨している。

- 資産の識別:IoT製品は一意に識別可能であり、IoT製品のすべてのコンポーネントを目録化する。
- 製品構成:IoT製品の構成は変更可能であり、セキュリティで保護された既定の設定を復元する機能があり、すべての変更は許可された個人、サービス、及びその他のIoT製品コンポーネントのみが実行できる。
- データ保護:IoT製品とそのコンポーネントは、(すべてのIoT製品コンポーネントにわたって)保存及び送信されるデータ(IoT製品コンポーネント間及びIoT製品外部の両方)を、不正アクセス、開示、及び変更から保護する。
- インターフェイスアクセス制御:IoT製品とそのコンポーネントは、ローカルインターフェイスとネットワークインターフェイス、及びそれらのインターフェイスで使用されるプロトコルとサービスへの論理アクセスを、許可された個人、サービス、及びIoT製品コンポーネントのみに制限する。
- ソフトウェアの更新:すべてのIoT製品コンポーネントのソフトウェアは、各IoT製品コンポーネントに応じて、安全で構成可能なメカニズムを使用してのみ、承認された個人、サービス、及びその他のIoT製品コンポーネントによって更新できる。
- サイバーセキュリティ状態認識:IoT製品は、IoT製品コンポーネントとそれらが保存及び送信するデータに影響を与える、又は影響を受けるサイバーセキュリティインシデントの検出をサポートする。
- 文書化:IoT製品開発者は、顧客が購入する前に、製品の開発とその後のライフサイクルを通じて、IoT製品とその製品コンポーネントのサイバーセキュリティに関連する情報を作成、収集、及び保存する。
- 情報とクエリの受信:IoT製品開発者はサイバーセキュリティに関連する情報を受け取り、サイバーセキュリティに関連する情報に関する顧客などからのクエリに応答する能力をもつ。
- 情報の普及:IoT製品開発者は、サイバーセキュリティに関連する情報をブロードキャスト(一般など)及び配布(顧客やIoT製品エコシステムの他の人々など)する。
- 製品の教育と認識:IoT製品開発者は、IoT製品とその製品コンポーネントに関連するサイバーセキュリティ関連情報(考慮事項、機能など)について、IoT製品エコシステムの顧客やその他のユーザーの認識を高め、教育する。

IoT機器関連文献 #5：概要

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0

1	概要	ENISAは、サイバーセキュリティ法(CSA)に基づく欧州委員会からの要請を受けて、SOG-IS MRA(上級職員グループ情報システムセキュリティ相互承認契約)の下で運用されている既存のサイバーセキュリティ認証スキームの後継として機能するEUサイバーセキュリティ認証スキームの準備をするために、アドホックワーキンググループを設立した。ENISAは、2019年11月に発足し、業界を代表する20名の選抜メンバー(開発者、評価者など)と、認定機関及びEU加盟国からの約12名の参加者で構成された。そして、ICT製品の認証のためのCommon Criteria(CC：ISO/IEC15408)と、評価方法(ISO/IEC 18045)に基づいた「EUCCサイバーセキュリティ認証スキーム候補」がENISAによって作成された。

2	書誌的情報	名称	EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0		
		主旨	セキュリティ専用のICT製品(ファイアウォール、暗号化デバイス、ゲートウェイ、電子署名デバイス、パスポートなどの識別手段など)だけでなく、セキュリティ機能を組み込んだICT製品(ルーター、スマートフォン、バンキングカード、医療機器など)のセキュリティレベルを強化するためのサイバーセキュリティ認証スキームの「候補」である。		
		文献タイプ	ガイドライン		
		国・地域	EU全域	適用分野	ICT製品の認証
		策定者	European Union Agency for Cybersecurity(ENISA)	対象者	ICT製品のメーカー又はプロバイダー。 ICTサービス/ICTプロセスのプロバイダー。 ICT製品の規制作成者。 ICT製品に関する規制の遵守やセキュリティ証拠の取得を希望するエンドユーザー。
		順守義務	サイバーセキュリティ認証スキームの「候補」としての文書である。		
		普及状況	サイバーセキュリティ認証スキームの「候補」としての文書である。		
		策定年	2021年	ページ数	286

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0

3	IoT-SSFに参考となる取組	記載なし。
4	IoT機器の区分・水準・対策	スマートカード及び類似のデバイスに関連する「技術ドメインに適用する方法に関する開発者向けの要件」等を提供している。
5	技術的・制度的枠組	EUCCサイバーセキュリティ認証スキーム候補は、CC(Common Criteria：コモンクライテリア)、及び対応する標準(ISO/IEC15408及びISO/IEC18045)に基づいて、ICT製品のサイバーセキュリティの認証を調査する。 EUCCサイバーセキュリティ認証スキーム候補は、CSAの第51条、第52条、及び第54条の要件が満たされることを規定している。
関連URL		ISO / IEC 18045(情報技術規格) https://www.iso.org/standard/72889.html Common Criteria (認証スキーム) https://www.ipa.go.jp/security/jisec/about_cc.html https://www.commoncriteriaportal.org/cc/ Cybersecurity Act - REGULATION(EU) 2019/881(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=DE REGULATION(EC) No 765/2008 (規制) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF

EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.0

概要

・ENISAは、サイバーセキュリティ法(CSA)に基づく欧州委員会からの要請を受けて、SOG-ISMRA(上級職員グループ情報システムセキュリティ相互承認契約)の下で運用されている既存のサイバーセキュリティ認証スキームの後継として機能する「EUCCサイバーセキュリティ認証スキーム候補」を作成した。
EUCCスキームは、セキュリティ専用のICT製品(ファイアウォール、暗号化デバイス、ゲートウェイ、電子署名デバイス、パスポートなどの識別手段など)だけでなく、セキュリティ機能を組み込んだICT製品(ルーター、スマートフォン、バンキングカード、医療機器など)のセキュリティレベルを強化する。
EUCCスキームは、以下の事項を示す。

- 評価基準
- 保証レベル
- 適合性の自己評価
- CAB(適合性評価機関)
- 評価基準と方法
- 認証に必要な情報
- マークとラベル
- コンプライアンス監視規程
- 証明書の発行、維持、継続、更新の条件
- 違反に関するルール
- CAB(Conformity Assessment Body：適合性評価機関)による記録の保持
- 国内又は国際的なスキーム
- 証明書に含める情報
- 情報の利用可能期間
- サイバーセキュリティ証明書の最大有効期間
- 証明書の開示方針
- 第三国との認証スキームの相互承認

IoT機器の区分・水準・対策

附属書ではスマートカード及び類似のデバイスに関連する「技術ドメインに適用する方法に関する開発者向けの要件」等を提供している。
(機器の区分による要求水準は含まれていないものとみられる。)

ANNEX 4 (p. 150):スマート カード及び類似のデバイスのセキュリティ アーキテクチャ要件 (ADV_ARC)
ADV_ARCファミリの保証要件をスマートカード及び同様のデバイスに関連する技術ドメインに適用する方法に関する開発者向けの要件を提供している。
これは、ADV_ARC ファミリを満たすために開発者ドキュメントが提供する情報の種類を定義する。
これは、セキュリティ集積回路の開発者と、ハードウェア プラットフォームと組み込みソフトウェアで構成される複合製品の開発者の両方に適用される。
評価者に必須のタスクを定義するものではないが、評価者の活動のガイドラインとして役立つ場合がある。

ANNEX 5 (p.155): 「OPEN」スマートカード製品の認定
「オープン」スマートカード製品の認証目的この附属書は、「オープン」スマート カード製品の認証手順を特定して、変更されたアーキテクチャが、この製品に対して既に発行されている証明書の認証済みセキュリティ機能の有効性に影響を与えないことを保証することを目的としている。

技術的・制度的枠組み

・EUCCサイバーセキュリティ認証スキーム候補は、CC (Common Criteria：コモンクライテリア)、及び対応する標準(ISO/IEC 15408及びISO/IEC 18045)に基づいて、ICT製品のサイバーセキュリティの認証を調査する。

ISO/IEC 15408：
情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格であり、Part 1から5までの５つの文書から構成される。CC (Common Criteria) とISO/IEC 15408は、どちらも同じものを意味する。
https://www.ipa.go.jp/security/jisec/about_cc.html

ISO/IEC 18045：
ISO/IEC 18045:2022は、上記ISO/IEC 15408の関連文書で、ISO/IEC 15408で定義された基準と評価証拠を使用して、ISO/IEC 15408評価を実施するために評価者が実行する最小限のアクションを定義する。
https://www.iso.org/standard/72889.html

・EUCCサイバーセキュリティ認証スキーム候補は、CSAの第51条、第52条、及び第54条の要件が満たされることを規定している。

CSAの第51条ーCSAの第51条は、例えば以下のような内容を含んでいる：
欧州のサイバーセキュリティ認証スキームは、該当する場合、少なくとも次のセキュリティ目標を達成するように設計されるものとする。
- ICT製品、ICTサービス、又はICTプロセスのライフサイクル全体を通じて、保存、送信、又はその他の方法で処理されたデータを、偶発的又は不正な保存、処理、アクセス、開示、不正な破壊、変更、等から保護する。

- CSAの第52条ーCSAの第52条は、例えば以下のような内容を含んでいる：
- 欧州のサイバーセキュリティ認証スキームの保証レベル
- 欧州のサイバーセキュリティ認証スキームは、ICT製品、ICTサービス、及びICTプロセスに対して、「基本」、「実質的」又は「高」の1つ又は複数の保証レベルを指定する場合がある。

- CSAの第54条ーCSAの第54条は、例えば以下のような内容を含んでいる：
- 欧州のサイバーセキュリティ認証スキームには、少なくとも次の要素が含まれる必要がある。
- 対象となるICT製品、ICTサービス、及びICTプロセスのタイプ又はカテゴリー、認証スキームの主題と範囲、評価方法、保証レベルがスキームの対象ユーザーのニーズにどのように対応しているかについての明確な説明。

ETSI TS 103 701 Conformance Assessment of Baseline Requirements

1	概要	家庭内でインターネットに接続するデバイスが増えるにつれて、 IoTのサイバーセキュリティに対する懸念が高まっており、サイバー脅威に耐えられるように設計する必要が増している。そこで、インターネットに接続された消費者向けデバイスのセキュリティにおいて広く検討されている優れた実践を、一連のハイレベルな結果重視の規定にまとめたものが「ETSI ETSI EN 303 645」である。本文書はIoT機器がTS 103 645 [1]/ EN 303 645[2] に適合しているかどうかを判定するときに役立つガイダンスとして作成された。

2	書誌的情報	名称	ETSI TS 103 701 Conformance Assessment of Baseline Requirements		
		主旨	ETSI TS 103 645 [1]/ETSI EN 303 645 [2]は、IoT製品の規定を明示している。本文書はIoT機器がTS 103 645 [1]/ EN 303 645[2] に適合しているかどうかを判定するときに役立つガイダンスである。		
		文献タイプ	ガイドライン		
		国・地域	EU	適用分野	消費者向けIoT製品の適合性評価
		策定者	ETSI	対象者	IoT製品のサプライヤーや実装者、ユーザー組織、独立したテスト組織等。
		順守義務	IoT機器がTS 103 645 [1]/ EN 303 645[2] に適合しているかどうかを判定するときに役立つ文書として作成された		
		普及状況	IoT機器がTS 103 645 [1]/ EN 303 645[2] に適合しているかどうかを判定するときに役立つ文書として広く活用されているものとみられる。		
		策定年	2021年	ページ数	135

3	IoT-SSFに参考となる取組	記載なし。

4	IoT機器の区分・水準・対策	記載なし。

ETSI TS 103 701 Conformance Assessment of Baseline Requirements

5	技術的・制度的枠組	本文書は「消費者用IoT機器のサイバーセキュリティについての欧州規格」である「TS 103 645 [1]/ EN 303 645[2] 」に適合しているかどうかを判定するときに役立つガイダンスとして作成されている。ETSI EN 303 645は、消費者向けIoTの13のサイバーセキュリティ分野を次のように示している： 1. ユニバーサル デフォルト パスワードを使わない 2. 脆弱性のレポートを管理する手段を実装する 3. ソフトウェアを最新の状態に保つ 4. 機密性の高いセキュリティ パラメータを安全に保存する 5. 安全に通信する 6. 露出する攻撃面を最小限に抑える 7. ソフトウェアの整合性を確保する 8. 個人データの安全を確保する 9. 「停止」に対するシステムの回復力を高めるシステム 10.テレメトリ データの調査 11.ユーザーが個人データを簡単に削除できるようにする 12.デバイスの設置とメンテナンスを容易にする 13.入力データの検証

関連URL	ETSI TS 103 645(V2.1.2)(2020-06) (技術規格) https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf ETSI EN 303 645 V2.1.1 (2020-06) (技術規格) https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf NIST Cryptographic Algorithm Validation Program (CAVP). (暗号アルゴリズム検証プログラム) https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program Mozilla®, Security/Server Side TLS. (TLS を使用するサーバーの推奨構成) https://wiki.mozilla.org/Security/Server_Side_TLS Overview of cryptographic key length recommendations. (暗号化関数について) https://www.keylength.com/

IoT機器関連文献 #6：主な調査項目

ETSI TS 103 701 Conformance Assessment of Baseline Requirements

概要

ETSI TS 103 645 [1]/ETSI EN 303 645 [2]は、IoT製品の規定を明示している。
本文書はIoT機器がTS 103 645 [1]/ EN 303 645[2] に適合しているかどうかを判定するときに役立つガイダンスを提供する。

- 本文書は、消費者向けIoT製品の「サプライヤー又は実装者」、「ユーザー組織」、「独立したテスト組織」を、支援することを目的としている。
  認証又は適合宣言スキームの定義は、このドキュメントの範囲外である。

- 本文書の適用には、[1]ETSI TS 103 645(V2.1.2)(2020-06)及び[2]ETSI EN 303 645(V2.1.1)(2020-06) の文献が必要である。

4.1概要とドキュメント構造

条項4.2	適合性評価手順に関連する役割とオブジェクトについて説明している。
条項4.3	評価手順について説明している。
条項4.4	実装適合ステートメント(ICS)のETSI TS 103 645 [1]/ETSI EN 303 645 [2]の規定への「消費者向けIoTデバイスの適合性」を宣言する方法について説明する。
条項4.5	IXIT(テスト用エクストラ情報)プロフォーマを使用して、テスト用実装エクストラ情報(IXIT)で対応するセキュリティ対策を宣言する方法を説明している。
条項4.6	テストケース、テストグループに判定を割り当てる方法の詳細と、最後に全体的な判定を割り当てる方法について説明する。
条項4.7	規定への適合性を判断するためにテストグループを実行する代わりに、外部の証拠を使用する方法を説明している。
条項4.8	本文書で提供される内容に加えて、評価スキームが通常対処するさまざまな側面を強調している。
第5項	TSO(テストシナリオ)が含まれており、各TSOはETSI TS 103 645 [1]/ETSI EN 303 645 [2]の一連の規定に対処し、単一の規定の評価を説明する一連のテストグループで構成されている。

IoT機器関連文献 #6：主な調査項目

ETSI TS 103 701 Conformance Assessment of Baseline Requirements

技術的・制度的枠組み

- 本文書は「消費者用IoT機器のサイバーセキュリティについての欧州規格」である「TS 103 645 [1]/ EN 303 645[2] 」に適合しているかどうかを判定するときに役立つガイダンスとして作成されている。ETSI EN 303 645は、消費者向け IoT の 13 のサイバーセキュリティ分野を次のように説明している。

1.ユニバーサルデフォルトパスワードを使わない	工場出荷時のデフォルト以外の状態である場合、すべての消費者向けIoTデバイスのパスワードは、デバイスごとに一意であるか、ユーザーが定義する必要がある。
2.脆弱性のレポートを管理する手段を実装する	製造業者は、脆弱性開示ポリシーを公開するものとする。
3.ソフトウェアを最新の状態に保つ	セキュリティ更新プログラムをタイムリーに開発して展開することは、メーカーが顧客を保護するために実行できる最も重要なアクションの1つである。 すべてのソフトウェアを最新の状態に保ち、適切に維持することを推奨する。
4.機密性の高いセキュリティパラメータを安全に保存する	ストレージ内の機密性の高いセキュリティ パラメータは、デバイスによって安全に保存する必要がある。
5. 安全に通信する	消費者向け IoT デバイスは、暗号化のベスト プラクティスを使用して安全に通信する必要がある。
6.露出する攻撃面を最小限に抑える	最小権限の原則(The principle of least privilege:PoLP)は優れたセキュリティ エンジニアリングの礎石であり、他のアプリケーション分野と同様に IoTにも適用できる。 例えば「未使用のネットワーク及び論理インターフェースはすべて無効にする」等のような対策が重要である。
7.ソフトウェアの整合性を確保する	消費者向けIoTデバイスは、セキュア ブート メカニズムを使用してソフトウェアを検証する必要がある。

IoT機器関連文献 #6：主な調査項目

ETSI TS 103 701 Conformance Assessment of Baseline Requirements

技術的・制度的枠組み

8.個人データの安全を確保する	デバイスとサービスの間を移動する個人データの機密性は、暗号化のベストプラクティスを使用して保護する必要がある。
9.「停止」に対するシステムの回復力を高めるシステム	個人の安全に関連する機能を含め、消費者の生活のあらゆる面で、「IoTサービスが稼働し続けられるようにすること」が必要である。 重要なのは、停止がユーザーへの影響の原因とならないようにし、一定レベルの回復力を提供する製品とサービスを設計することである。
10.テレメトリデータの調査	消費者向けIoTデバイスやサービスからテレメトリデータ(使用状況や測定データなど)を収集する場合は、セキュリティの異常を調べる必要がある。 (例：セキュリティの異常は、デバイスの通常の動作からの逸脱によって表われることがある。 例えばログイン試行の失敗の異常な増加など。)
11.ユーザーが個人データを簡単に削除できるようにする	ユーザーデータを簡単な方法でデバイスから消去できる機能をユーザーに提供する必要がある。 (ユーザーデータとは、個人データ、ユーザー構成、及びユーザーパスワードやキーなどの暗号化マテリアルを含む、IoTデバイスに保存されるすべての個人データを意味する。)
12.デバイスの設置とメンテナンスを容易にする	消費者向けIoTのインストールとメンテナンスは、容易にするべきであり、使いやすさに関するセキュリティのベストプラクティスに従う必要がある。
13.入力データの検証	消費者向けIoTデバイスソフトウェアは、「ユーザーインターフェイスを介した入力データ」や「アプリケーションプログラミングインターフェイス(API)を介して転送されたデータを検証する必要がある。

IoT機器関連文献 #7：概要

Proposal for a REGULATION on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

1	概要	ハードウェア及びソフトウェア製品は、サイバー攻撃にますますさらされており、2021年までに世界のサイバー犯罪の年間コストは5.5兆ユーロと推定されている。現在のEUの法的枠組みは、サイバーセキュリティ攻撃がこれらの製品の脆弱性をますます標的にし、多大な社会的及び経済的コストを引き起こしているとしても、サイバーセキュリティに十分に対処していない。 この規則の提案は、「デジタル要素を備えた製品のセキュリティ特性の信頼性を強化する」、「企業と消費者がデジタル要素を備えた製品を安全に使用できるようにする」等の目標を達成するために作成された。この規則は、その全体が拘束力を持ち、すべてのEU加盟国に直接適用できるものとする。

2	書誌的情報	名称	Proposal for a REGULATION on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020		
		主旨	この規則提案は、「デジタル要素を備えた製品」を安全に使用できるように「一貫性のあるサイバーセキュリティフレームワークを確保する」等の目標を達成するために作成された。		
		文献タイプ	政策		
		国・地域	EU全域	適用分野	「デジタル要素を備えた製品」に関するサイバーセキュリティ規制
		策定者	EU	対象者	EU加盟国の「デジタル要素を備えた製品」の製造者、輸入者等、販売者及び管轄機関
		順守義務	この規則は、その全体が拘束力を持ち、すべてのEU加盟国に直接適用できるものとする。		
		普及状況	欧州連合の官報に掲載された日から20日目に施行される。すべてこの規則の発効日から24か月後から適用される。ただし、第11条は、この規則の効力発生日から12か月後から適用される。		
		策定年	2022年	ページ数	84

3	IoT-SSFに参考となる取組	本規則で「デジタル要素を備えたクリティカルな製品」と見なされるものの多くは「サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスク」と直接的又は間接的に関連しているものと考えられる。本規則では「デジタル要素を備えたクリティカルな製品」のサイバーセキュリティ リスクのレベルを判断する際に次項(IoT機器の区分・水準・対策)で記される基準が考慮されなければならない、としている。
4	IoT機器の区分・水準・対策	「デジタル要素を備えたクリティカルな製品」のサイバーセキュリティ リスクのレベルを判断する際に、以下のような基準が考慮されなければならない： 「デジタル要素を備えた製品」が以下の属性の少なくとも1つを持っているかどうか確認する。 ➢ 昇格された特権又は管理特権で実行するように設計されている。 ➢ ネットワーク又はコンピューティング リソースに直接又は特権的にアクセスできる。 ➢ データ又は運用技術へのアクセスを制御するように設計されている。 ➢ 信頼に不可欠な機能、特にネットワーク制御、エンドポイントセキュリティ、ネットワーク保護などのセキュリティ機能を実行している。
5	技術的・制度的枠組	Cyber Resilience Act(サイバー レジリエンス法)は、ネットワーク及び情報システムのセキュリティに関する「NIS指令」等、既存のEUの法的枠組みを補完するものである。
関連URL		Regulation (EC)No 765/2008, Article 30 General principles of the CE marking(規制) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF Regulation (EU)2019/1020, REGULATIONS on market surveillance and compliance of products(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1020 NIS Directive(指令) https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

狙い・概要

• ハードウェア及びソフトウェア製品は、サイバー攻撃にますますさらされており、2021年までに世界のサイバー犯罪の年間コストは5.5兆ユーロと推定されている。
このような製品は、以下の2つの大きな問題に苦しんでいる。
(1)脆弱性とそれに対処するためのセキュリティ更新プログラムの提供が不十分で一貫性がなく、サイバーセキュリティのレベルが低い。
(2)ユーザーによる情報の理解とアクセスが不十分であり、適切なサイバーセキュリティ特性を備えた製品を選択したり、安全な方法で使用したりできない。

• コネクテッド環境では、1つの製品におけるサイバーセキュリティインシデントが組織全体又はサプライチェーン全体に影響を及ぼし、多くの場合、数分以内に市場の境界を越えて伝播する。これは、経済的及び社会的活動の深刻な混乱につながったり、生命を脅かすことさえある。
現在のEUの法的枠組みは、サイバーセキュリティ攻撃がこれらの製品の脆弱性をますます標的にし、多大な社会的及び経済的コストを引き起こしているとしても、非組み込みソフトウェアのサイバーセキュリティに対処していない。

市場の適切な機能を確保することを目的として以下の2つの主要な目的が特定された

(1)デジタル要素を備えた安全な製品を開発するための条件を作成し、メーカーが製品のライフサイクルを通じてセキュリティを確実に確保できるようにすること。
(2)ユーザーが製品を選択して使用する際にサイバーセキュリティを考慮できる条件を作成するというデジタルエレメント。

以下の4つの具体的な目標が設定された

(i)メーカーが設計及び開発段階からライフサイクル全体を通じてデジタル要素を備えた製品のセキュリティを向上させることを保証する。
(ii)一貫性のあるサイバーセキュリティフレームワークを確保し、ハードウェア及びソフトウェア生産者のコンプライアンスを促進する。
(iii)「デジタル要素を含む製品」のセキュリティ特性の信頼性を強化する。
(iv)企業と消費者が「デジタル要素を備えた製品」を安全に使用できるようにする。

この規則提案は、上記の目標のために作成された。
この規則は、その全体が拘束力を持ち、すべてのEU加盟国に直接適用できるものとする。

IoT機器の区分・水準・対策

附属書IIIに記載されているカテゴリーに属する「デジタル要素を備えた製品」は、デジタル要素を備えたクリティカルな製品*と見なされるものとする。

*デジタル要素を備えたクリティカルな製品（製品例）：
- ➢スタンドアロン及び組み込みブラウザー
- ➢パスワードマネージャー
- ➢悪意のあるソフトウェアを検索、削除、又は隔離するソフトウェア
- ➢バーチャル プライベート ネットワーク (VPN) の機能を備えたデジタル要素を備えた製品
- ➢ネットワーク管理システム
- ➢ネットワーク構成管理ツール
- ➢ネットワーク トラフィック監視システム
- ➢セキュリティ情報及びイベント管理(SIEM)システム
- ➢ブート マネージャーを含む更新/パッチ管理
- ➢アプリケーション構成管理システム
- ➢リモート アクセス/共有ソフトウェア
- ➢モバイル デバイス管理ソフトウェア
- ➢物理ネットワーク インターフェイス
- ➢プログラマブル ロジック コントローラ(PLC)、分散型制御システム(DCS)、工作機械(CNC)
- ➢サーバー、デスクトップ、及びモバイル デバイス用のオペレーティングシステム
- ➢産業用のファイアウォール、侵入検知及び/又は防止システム
- ➢汎用マイクロプロセッサ
- ➢インターネットへの接続を目的としたルーター、モデム、及びスイッチ
- ➢スマートカード、スマートカードリーダー、トークン

「デジタル要素を備えたクリティカルな製品」のサイバーセキュリティ リスクのレベルを判断する際に、以下のような基準が考慮されなければならない：
「デジタル要素を備えた製品」が以下の属性の少なくとも1つを持っているかどうか確認する。
- ➢昇格された特権又は管理特権で実行するように設計されている。
- ➢ネットワーク又はコンピューティング リソースに直接又は特権的にアクセスできる。
- ➢データ又は運用技術へのアクセスを制御するように設計されている。
- ➢信頼に不可欠な機能、特にネットワーク制御、エンドポイントセキュリティ、ネットワーク保護などのセキュリティ機能を実行している。

技術的・制度的枠組み

本規則Cyber Resilience Act(サイバーレジリエンス法)は、ネットワーク及び情報システムのセキュリティに関する「NIS指令*」等、既存のEUの法的枠組みを補完するものである。
https://www.european-cyber-resilience-act.com/

*NIS指令
NIS指令(EU 2016/1148)は、初の「EU全体のサイバーセキュリティ法」であり、その目標は、EU全体のサイバーセキュリティを強化することであった。
NIS指令は2016年に採択され、その後、EU指令としてすべてのEU加盟国が採用し始めた。
ENISA は、加盟国と協力グループの任務を次のように支援する：
- ➢NIS指令の実施に関する加盟国の優良事例を特定する。
- ➢しきい値、テンプレート、及びツールを開発することにより、サイバーセキュリティ インシデントに関するEU全体の報告プロセスをサポートする。
- ➢共通のアプローチと手順に同意する。
- ➢加盟国が一般的なサイバーセキュリティの問題に対処するのを支援する。

欧州委員会は、2020年12月にNIS2の提案を発表した。
NIS2の主な目的は、より多くのセクターを含め、より高いレベルのネットワークを作成することである。

ENISAは、その権限と作業プログラムの一部として、NIS指令の実施を引き続きサポートする方針である。
https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Proposal for a REGULATION on machinery products

1	概要	MD(Machinery Directive 2006/42/EC:機械指令)は、機械を市場に投入するための規制の枠組みを確立した。しかしその後、欧州委員会の評価で、「MDを改善、簡素化、及び市場のニーズに適合させる必要性」を特定した。(例えば「MDは、新興技術に起因する新たなリスクを十分にカバーしていない」等の問題があるため、MDを改定することの必要性が浮き彫りになった。)本文書で提案された規則は、発効から30か月後に適用され、MDは廃止され、本規則に置き換えられる。

2	書誌的情報	名称	Proposal for a REGULATION on machinery products		
		主旨	本文書の規則は、機械製品の市場投入又は機械製品のサービス提供を可能にするための機械製品の設計及び構築の要件を定め、EUにおける機械製品の自由な移動に関する規則を確立する。本文書で提案された規則は、MD(Machinery Directive 2006/42/EC:機械指令)の問題点を改定するものである。本文書発効から30か月後に適用され、MDは廃止され、本規則に置き換えられる。		
		文献タイプ	政策(提案)		
		国・地域	EU	適用分野	機械製品の設計及び構築の要件。
		策定者	欧州委員会(EC)	対象者	機械製品製造者、輸入者及び管轄官庁、機関等。
		順守義務	本文書が適用された場合、MDは廃止され、機械を市場に投入するための規制の枠組みは、本規則に置き換えられる。		
		普及状況	本文書で提案された規則は、発効から30か月後に適用され、MDは廃止され、本規則に置き換えられる。		
		策定年	2021年	ページ数	54

3	IoT-SSFに参考となる取組	記載なし。

Proposal for a REGULATION on machinery products

4	IoT機器の区分・水準・対策	記載なし。

5	技術的・制度的枠組	この提案は、Decision No 768/2008/EC(製品のマーケティングのための共通の枠組みに関する2008年7月9日の欧州議会及び理事会の決定の規定)に準拠している 。 この提案はサイバーセキュリティに関する欧州連合の方針と一致しており、Regulation(EU)2019/881に準拠した将来のサイバーセキュリティスキームとリンクしている。

関連URL	DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (機械に関する 指令) EUR-Lex - 32006L0042 - EN - EUR-Lex (europa.eu) Commission Report on safety and liability implications of AI, the Internet of Things and Robotics(AI、IoT、ロボティクスの安全性と責任に関する委員会報告書) Commission Report on safety and liability implications of AI, the Internet of Things and Robotics (europa.eu) Decision No 768/2008/EC(製品のマーケティングのための共通の枠組みに関する欧州議会及び理事会の決定) https://op.europa.eu/en/publication-detail/-/publication/493403fe-dd8d-4178-9297-1b324d5b140a/language-en Regulation (EU) 2019/881(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG

IoT機器関連文献 #8：主な調査項目

Proposal for a REGULATION on machinery products

狙い・概要

MD(Machinery Directive 2006/42/EC:機械指令)は、機械を市場に投入するための規制の枠組みを確立した。
MDの一般的な目的は、「国内市場内での機械の自由な移動を確保すること」と「ユーザーその他に対して高レベルの保護を確保すること」であった。

その後、欧州委員会の規制適合性プログラムである「REFIT評価」で、利害関係者は、「MDを改善、簡素化、及び市場のニーズに適合させる必要性」を特定した。
(例えば「MDは、新興技術に起因する新たなリスクを十分にカバーしていない」等の問題があるため、MDを改定することの必要性が浮き彫りになった。)

欧州議会の一部の議員は、「MDを改訂すること」を支持した。
実際、欧州委員会は2020年2月に「人工知能、モノのインターネット、ロボット工学の安全性と責任への影響に関する報告書(Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics)」を伴う人工知能に関する白書を発表した。
新技術の影響とそれらがEUの安全法にもたらす課題の分析を行ったこの報告書は、現在の製品安全法には、特に機械直接法などに対処する必要のある多くのギャップが含まれていると結論付けた。

本文書で提案された規則は、発効から30か月後に適用され、MD(Machinery Directive, Directive 2006/42/EC)は廃止され、本規則に置き換えられる。

IoT機器関連文献 #8：主な調査項目

Proposal for a REGULATION on machinery products

技術的・制度的枠組み

機械製品に関する規制は、Decision No 768/2008/EC*(製品のマーケティングのための共通の枠組みに関する2008年7月9日の欧州議会及び理事会の決定の規定)に準拠している。

*Decision No 768/2008/EC
Decision No 768/2008/ECは、EUと欧州経済領域(EEA)で製品を販売するための条件を調和させる際に、従わなければならない共通の原則と手順を定めており、以下を説明している：

- 製品の「製造者」、「上市」、「リコール」、「撤回」などの関連用語の明確な定義。
- 製品チェーンに沿って、製造業者、輸入業者、及び流通業者に明確な責任分担が設定されていること。
- 製造業者は、製品が関連する法律に準拠していることを確認し、適切な適合性評価手順に従う必要があること。
  コンプライアンスが実証されたら、製品にCEマークを付ける必要があること。
- 輸入業者は、製造業者が適切な適合性評価手順に準拠していること。
  及び製品に必要な文書とCEマーキングが添付されていることを確認する必要があること。
- ディストリビューターは、十分な注意を払って行動し、製品に必要な文書とCEマークが付いていることを確認する必要があること。
- モジュールと呼ばれる、さまざまな適合性評価手順の共通セットが提供されること。
  立法者は、製品がもたらす可能性のあるリスクに応じて、最も適切なものを選択する必要があること。
- EU法に基づいて適合性評価を実施する通知機関を指定及び監督するための統一規則が定められていること。

他の政策との一貫性：
この提案はサイバーセキュリティに関する欧州連合の方針と一致しており、Regulation(EU)2019/881に準拠した将来のサイバーセキュリティスキームとリンクしている。

COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021

1	概要	無線機器指令 Directive 2014/53/EU は、無線技術を使用する製品の法的枠組みを定めている。 本規則REGULATION (EU) 2022/30 は、「Directive 2014/53/EU」の第3条3の(d)(e)(f)の補完を行う目的で作成された。

2	書誌的情報	名称	COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021		
		主旨	無線機器を市場に出すための規制の枠組みを定めた無線機器指令Directive 2014/53/EU に対して、サイバーセキュリティ面などの補完を行う内容となっている。		
		文献タイプ	政策		
		国・地域	EU全域	適用分野	インターネットに接続された無線機器
		策定者	EU	対象者	無線機器メーカー、輸入者、販売者等
		順守義務	この規則は全体として拘束力があり、すべてのEU加盟国に直接適用されるものとする。		
		普及状況	この規則は、欧州連合の官報に掲載された日から20日目に施行される。 この規則は2024年8月1日から適用される。		
		策定年	2021年	ページ数	5

3	IoT-SSFに参考となる取組	• この規則は、「無線機器指令Directive 2014/53/EU」の補完を行う内容となっている。「無線機器指令Directive 2014/53/EU」では「無線機器の必須要件*」について示しているが、これらはすべてIoT-SSFの取組内容に関連していると考えられる。 *必須要件 • 無線機器がネットワークやその機能に害を与えたり、ネットワーク リソースを悪用したりせず、それによって許容できないほどのサービスの低下を引き起こさないこと。 • 無線機器に、ユーザーと加入者の個人データとプライバシーが確実に保護されるように保護手段が組み込まれていること。 • 無線機器が、詐欺からの保護を保証する特定の機能をサポートしていること。

COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021

4	IoT機器の区分・水準・対策	無線機器を市場に出すための規制の枠組みを定めた無線機器指令「Directive 2014/53/EU」では、「特定のカテゴリ又はクラス内の無線機器は、次の必須要件に適合するように構築されている必要がある」と述べている： ➢ 無線機器がネットワークやその機能に害を与えたり、ネットワーク リソースを悪用したりせず、それによって許容できないほどのサービスの低下を引き起こさないこと。 ➢ 無線機器に、ユーザーと加入者の個人データとプライバシーが確実に保護されるように保護手段が組み込まれていること。 ➢ 無線機器が、詐欺からの保護を保証する特定の機能をサポートしていること。 本規則では、無線機器が個人データ又はトラフィック データと位置データを処理できる場合、以下の例外を除いた「すべてのインターネット接続された無線機器」が上記の「必須要件」を満たすことが必要となる。 ➢ Regulation (EU)2017/745(医療機器に関する規則)の対象となる無線機器。 ➢ Regulation (EU)2017/746(体外診断用医療機器に関する 規則)の対象となる無線機器。 ➢ Regulation (EU) 2018/1139(民間航空の分野における規則)の対象となる無線機器。 ➢ Regulation (EU)2019/2144(車両用システム等に関する規則)の対象となる無線機器。 ➢ Directive (EU)2019/520(電子道路通行料システム等に関する規則)の対象となる無線機器。

5	技術的・制度的枠組	無線機器を市場に出すための規制の枠組みを定めた無線機器指令「Directive 2014/53/EU」は、EU立法パッケージ (新しい立法の枠組み (the New Legislative Framework：NLF) の一部である。 https://www.etsi.org/technologies/radio/ この規則は、「無線機器指令Directive 2014/53/EU」の第3条「必須要件」の補完を行う内容となっている。

関連URL	Directive 2014/53/EU Article 3(3)(d)(e)(f) (指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053 Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0048 REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745 REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical…(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency(規制) https://www.easa.europa.eu/en/document-library/regulations/regulation-eu-20181139 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems…(規制) https://eur-lex.europa.eu/eli/reg/2019/2144/oj Directive (EU) 2019/520 of the European Parliament and of the Council of 19 March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union(指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0520

狙い・概要

無線機器指令Directive2014/53/EUは、無線技術を使用する製品の法的枠組みを定めている。
本規則REGULATION(EU)2022/30は、「Directive2014/53/EU」の第3条3の(d)(e)(f)の補完を行う目的で作成された。
「無線機器指令Directive2014/53/EU」では「無線機器の必須要件」について以下のように示している。
第3条必須要件
3.特定のカテゴリ又はクラス内の無線機器は、次の必須要件に適合するように構築されている必要がある。
(d)無線機器がネットワークやその機能に害を与えたり、ネットワークリソースを悪用したりせず、それによって許容できないほどのサービスの低下を引き起こさないこと。
(e)無線機器に、ユーザーと加入者の個人データとプライバシーが確実に保護されるように保護手段が組み込まれていること。
(f)無線機器が、詐欺からの保護を保証する特定の機能をサポートしていること。

本規則REGULATION(EU)2022/30では、上記の「無線機器指令Directive2014/53/EU」の第3条3の(d)(e)(f)について以下のように補完記述している。
Directive2014/53/EUの第3条(3)の(d)に定められた必須要件は、直接通信するか他の機器を介して通信するかにかかわらず、インターネットを介して通信できるすべての無線機器(「インターネットに接続された無線機器」)に適用されるものとする。

Directive2014/53/EUの第3条(3)の(e)に定められた必須要件は、無線機器が個人データ又はトラフィックデータと位置データを処理できる場合、「そのようなすべての無線機器」に適用されるものとする。

Directive2014/53/EUの第3条(3)の(f)に定められた必須要件は、「インターネットに接続された無線機器」によって「所有者又はユーザーが金銭、金銭的価値、又は仮想通貨を転送できるようになる場合」、その「インターネットに接続された無線機器」に適用されるものとする。

- 特例として、上記の必須要件は、次の連合法のいずれかが適用される無線機器には適用されないものとする。
- Regulation(EU)2017/745(医療機器に関する2017年4月5日の欧州議会及び理事会の規則)
- Regulation(EU)2017/746(体外診断用医療機器に関する2017年4月5日の欧州議会及び理事会の規則)
- Regulation(EU)2018/1139(民間航空の分野における共通規則及び欧州連合航空安全機関の設立)
- Regulation(EU)2019/2144(「一般的な安全性」と「車両乗員及び脆弱な道路利用者の保護」に関する、「自動車とトレーラー、及びそのような車両用のシステムやコンポーネント、個別の技術ユニット」の型式承認要件に関する規則)
- Directive(EU)2019/520(電子道路通行料システムの相互運用性と、EUでの道路料金未払に関する国境を越えた情報交換の促進)

IoT機器関連文献 #9：主な調査項目

COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021

技術的・制度的枠組み

無線機器を市場に出すための規制の枠組みを定めた無線機器指令「Directive2014/53/EU」は、EU立法パッケージ
(新しい立法の枠組み(the New Legislative Framework：NLF)の一部である。
https://www.etsi.org/technologies/radio/

この規則は、「無線機器指令Directive2014/53/EU」の第3条3のポイント(d)(e)(f)の補完を行う内容となっている。
「無線機器指令Directive2014/53/EU」では以下のように示している。
第3条必須要件
3.特定のカテゴリ又はクラス内の無線機器は、次の必須要件に適合するように構築されている必要がある。
(d)無線機器がネットワークやその機能に害を与えたり、ネットワークリソースを悪用したりせず、それによって許容できないほどのサービスの低下を引き起こさないこと。
(e)無線機器に、ユーザーと加入者の個人データとプライバシーが確実に保護されるように保護手段が組み込まれていること。
(f)無線機器が、詐欺からの保護を保証する特定の機能をサポートしていること。

IoT機器関連文献 #10：概要

BSI Internet of Things Testing, verification and certification solutions for a smarter, more secure world（BSI Kitemark)

1	概要		IoTデバイスの数は2017年の90億台から、2025年までに640億台以上になると予測されている。接続されたデバイスは外部の脅威に対して脆弱である、という認識の高まりにより、IoTに対する消費者の信頼が失われ、このテクノロジーに対するビジネスの信頼が低下している。BSIでは、品質、安全性、信頼性に裏打ちされた試験と認証を提供することに重点を置いており、グローバル組織として、専用の最先端のIoTラボで、専門家が幅広いIoT製品の迅速かつ効果的なテストを提供し、IoT製品にBSI 認証(Kitemark)を発行している。		
2	書誌的情報	名称	BSI Internet of Things Testing, verification and certification solutions for a smarter, more secure world（BSI Kitemark)		
		主旨	本文書は、BSIで行っているIoT製品のテスト～BSI 認証(カイトマーク認証)発行に関して説明している。		
		文献タイプ	IoT機器認証制度		
		国・地域	グローバルベース	適用分野	IoTデバイスのテスト、認証等。
		策定者	英国	対象者	IoTデバイスの製造者
		順守義務	必須ではないが、BSIは、「BSIカイトマーク認証は、以下のことに役立つ」と述べている： ・ブランドの構築と保護　・顧客基盤と顧客満足度の向上　・製品のプレミアム価格　・競争優位性の獲得		
		普及状況	不明。		
		策定年	2020年	ページ数	8
3	IoT-SSFに参考となる取組		BSIのIoTテストの基礎は、OWASPのセキュリティリスクのトップ10リストに対処することに基づいており、トップ10の多くはIoT-SSFの取組に関連しているとみられる。以下はOWASPのセキュリティリスクのトップ10である。 1.脆弱なパスワード、推測可能なパスワード等　2.安全でないネットワークサービス/プロトコル 3.安全でないアクセスインターフェイス　4.安全でないコンポーネントや古いコンポーネントの使用 5.安全な更新メカニズムの欠如　6.不十分なプライバシー保護 7.安全でないデータ転送と保存　8.物理的硬化の欠如 9.不十分なセキュリティ会議　10.デバイス管理の欠如		

4	IoT機器の区分・水準・対策	記載なし。
5	技術的・制度的枠組	OWASP(IoT)トップ10プロジェクトとBSIコアIoTテスト： 世界中のセキュリティ専門家が評価するOWASP(Open Web Application Security Project)IoTトップ10は、IoTデバイスにとって最も重要なセキュリティリスクを表している。これは、開発者、メーカー、消費者がIoTに関連するセキュリティの問題をよりよく理解するのに役立ち、あらゆるコンテキストのユーザーがIoTテクノロジーを構築、展開、又は評価する際に、より良いセキュリティの決定を下すことにおいて有用である。BSIのIoTテストの基礎は、IoTデバイスに対する最も重要なセキュリティリスクに関する幅広いコンセンサスを表すため、この国際的に認められたOWASPのリストに対処することに基づいている。 品質管理システム(ISO 9001など)： BSIのIoT認証では、品質管理システム(ISO 9001など)が実施されていることを実証する。
関連URL		OWASP® Foundation(組織紹介) https://owasp.org/ ISO 9001(認証規格) https://www.jqa.jp/service_list/management/service/iso9001/

技術的・制度的枠組み

OWASP(IoT)トップ10プロジェクトとBSIコアIoTテスト

世界中のセキュリティ専門家が評価するOWASP(Open Web Application Security Project)IoTトップ10は、IoTデバイスにとって最も重要なセキュリティリスクを表している。
これは、開発者、メーカー、消費者がIoTに関連するセキュリティの問題をよりよく理解するのに役立ち、あらゆるコンテキストのユーザーがIoTテクノロジーを構築、展開、又は評価する際に、より良いセキュリティの決定を下すことにおいて有用である。
BSIのIoTテストの基礎は、IoTデバイスに対する最も重要なセキュリティリスクに関する幅広いコンセンサスを表すため、この国際的に認められたOWASPのリストに対処することに基づいている。

OWASPの最も重要なWebアプリケーションのセキュリティリスクのトップ10は次のとおりである。
1.脆弱なパスワード、推測可能なパスワード、又はハードコードされたパスワード
2.安全でないネットワークサービス/プロトコル
3.安全でないアクセスインターフェイス
4.安全でないコンポーネントや古いコンポーネントの使用
5.安全な更新メカニズムの欠如
6.不十分なプライバシー保護
7.安全でないデータ転送と保存
8.物理的硬化の欠如
9.不十分なセキュリティ会議
10.デバイス管理の欠如

品質管理システム(ISO9001など)

BSIのIoT認証では、品質管理システム(ISO9001など)が実施されていることを実証する。

サイバーセキュリティ審査弁法(网络安全审查办法)

1	概要	「ネットワークセキュリティ審査弁法」は、中国のネットワークセキュリティ審査に関する具体的な要件を明確化・精緻化し、重要情報インフラの運営者が審査を申告する際のガイドラインを提供する。 基幹システム機器のオンライン操作やサービスの調達に際して、厳格なセキュリティの敷居を設定した。 ネットワークセキュリティ製品・サービスのセキュリティリスクを事前判定する仕組みを構築し、脅威の特定とリスク解決の観点からセキュリティゲートの前進を促し、サプライチェーンのセキュリティリスク管理を強化し、ネットワークセキュリティの保護レベルを向上させた。

2	書誌的情報	名称	サイバーセキュリティ審査弁法		
		主旨	サイバーセキュリティの見直しの主な内容は、サイバーリスクの特定と予防であり、これは国家安全保障の見直しの重要な部分である。		
		文献タイプ	政策		
		国・地域	中国	適用分野	重要情報インフラ事業者又は 重要情報インフラ事業者がネットワーク製品・サービスを調達している事業者
		策定者	国家インターネット情報室	対象者	第1：重要な情報インフラの運営者 第2：ネットワークプラットフォームの運営者
		順守義務	重要情報インフラ事業者がネットワーク製品・サービスを調達し、ネットワークプラットフォーム事業者が国家安全保障に影響する、又は影響する可能性のある情報処理活動を行う場合、本措置に基づきサイバーセキュリティレビューを実施するものとする。		
		普及状況	-		
		策定年	2021年11月16日	ページ数	4

サイバーセキュリティ審査弁法(网络安全审查办法)

3	IoT-SSFに参考となる取組	コアネットワーク機器、重要な通信製品、高性能コンピュータ及びサーバ、大容量記憶装置、大規模データベース及びアプリケーションソフトウェア、ネットワークセキュリティ機器、クラウドコンピューティングサービス、その他ネットワーク製品及びサービスの調達案件で、 重要情報インフラセキュリティ、ネットワークセキュリティ、データセキュリティに大きな影響を与えるものなど、ネットワークセキュリティの審査に申告した調達活動については、その審査が行われる。
4	IoT機器の区分・水準・対策	本施策の第5条及び第7条によると、現在、サイバーセキュリティの見直しを積極的に宣言する義務を負う対象者は2種類ある。 (1)ネットワーク製品・サービスの調達が国家安全保障に影響を与える、又は与える可能性のある重要情報インフラ事業者(CIIO)。 (2)海外で公開され、100万人以上のユーザーの個人情報を保有するオンラインプラットフォームの運営者。
5	技術的・制度的枠組	サイバーセキュリティ審査では、重要情報インフラ事業者がネットワーク製品やサービスを調達することによってもたらされる可能性のある国家安全保障上のリスクを評価することに重点を置いている。 例えば、製品やサービスの利用によってもたらされる重要情報インフラへの不正支配、妨害、損害、重要データの盗難、漏洩、破壊のリスク。 製品やサービスの供給の途絶によって引き起こされる重要情報インフラの事業継続への危険、製品・サービスセキュリティ、開放性、透明性、供給源の多様性、供給経路の信頼性及び政治・外交・貿易上の要因による供給停止のリスク。 製品及びサービス提供者の中国の法律、行政法規及び部門規則の遵守、その他重要情報インフラのセキュリティ及び国家安全保障を脅かす可能性のある要因。
関連URL		http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666430.htm （政策）

サイバーセキュリティ審査弁法(网络安全审查办法)

狙い

- サイバーセキュリティ審査は、サイバーセキュリティ分野における重要な法制度である。
  2020年6月1日に方針が施行されて以来、重要情報インフラ事業者の調達活動の見直しや、一部の重要製品等の見直しを開始するなど、重要情報インフラのサプライチェーンのセキュリティを守り、国家の安全を維持するために重要な役割を担っている。

- 2021年9月1日にデータセキュリティ法が施行され、国がデータセキュリティの審査体制を構築することが明確に規定された。
  これに伴い、ネットワークセキュリティ審査弁法も改正され、ネットワークプラットフォーム事業者が行うデータ処理活動が国家安全に影響を与える、又は影響を与える可能性がある場合もネットワークセキュリティ審査の範囲に含める。
  こうしたものに対して、ネットワークセキュリティとデータセキュリティをさらに保護し、国家安全を維持することを主目的として、100万人以上のユーザーの個人情報を保有するネットワークプラットフォーム事業者に対して、海外上場のネットワークセキュリティ審査申告を明示的に要求している。

- サイバーセキュリティ審査の目的は、もともとネットワーク製品やサービスの見直しであり、非国産のネットワークセキュリティ機器やサービスを禁止・排除することではない。
  また、製品やサービスの安全性は相対的なものであり、その安全性は、使用対象、使用目的、使用方法、その製品やサービスの製品供給チャネルの信頼性などの要素に大きく依存する。
  改訂された「サイバーセキュリティ審査弁法」では、具体的なビジネスシーンと連動して審査を行うことで、サイバーセキュリティ審査室が検証・テストを行う際の方向性を明確にしている。

別紙2 公開情報等の調査 データ関連文献

調査文献一覧

項番	国・地域	文献等の名称	URL	作成機関	作成時期	文書種別	調査項目
1	日本	包括的データ戦略	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf	デジタル庁	2021年	政策	1
2	日本	プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/20220304_policies_data_strategy_outline_01.pdf	デジタル庁	2022年	ガイドライン	2,3,4
3	米国	Data Protection Act of 2021	https://www.jetro.go.jp/ext_images/_Reports/01/7f744522a1ddc8eb/20210021.pdf	連邦議会	未成立	法令	1
	米国		https://www.congress.gov/bill/117th-congress/senate-bill/2134/text?r=15				
4	米国	SP 800-47 Rev. 1 Managing the Security of Information Exchanges	https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final	NIST	2021年	ガイドライン	2, 5
5	欧州	A European strategy for data	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN	欧州委員会 (EC)	2020年	政策	1

調査文献一覧

項番	国・地域	文献等の名称	URL	作成機関	作成時期	文書種別	調査項目
6	欧州	Data governance and data policies at the European Commission	https://ec.europa.eu/info/sites/default/files/summary-data-governance-data-policies_en.pdf	欧州委員会(EC)	2020年	政策	1
7	欧州	Data Governance Act	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868&from=EN	欧州委員会(EC)	2022年	法令	1
8	欧州	Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068&from=EN	欧州委員会(EC)	2022年	法令	1
9	欧州	Proposal for a Regulation on the European Health Data Space	https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en	欧州委員会(EC)	2022年	法令	1,3,5
10	中国	サイバーセキュリティ法	https://gkml.samr.gov.cn/nsjg/bgt/202106/t20210608_330399.html	中国政府	2017年	法令	1,2,4
11	中国	データセキュリティ法	http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml	中国政府	2021年	法令	1,2,4
12	中国	個人情報保護法	http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml	中国政府	2021年	法令	1,2,4
13	中国	GB/T 22240-2020 情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド	https://sec.njust.edu.cn/6e/5a/c8144a224858/page.htm	中国政府	2020年	ガイドライン	2,4
14	中国	データ域外移転安全評価弁法	http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm	中国政府	2022年	法令	1,2,4

調査文献一覧

項番	国・地域	文献等の名称	URL	作成機関	作成時期	文書種別	調査項目
15	中国	データ越境安全評価申告ガイドライン(第 1 版)	https://www.tc260.org.cn/upload/2022-09-01/1661994372338082993.pdf	中国政府	2022年	ガイドライン	2,4
16	中国	個人情報越境取扱活動安全認証規範	https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf	中国政府	2022年	ガイドライン	2,4
17	中国	個人情報越境標準契約規定(意見募集稿)	http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm	中国政府	2022年	ガイドライン	2,4
18	インド	THE PERSONAL DATA PROTECTION BILL, 2019	https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf	電子情報技術省	2019年	法令	1,2,4
19	インド	Non-Personal Data Governance Framework	https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf	電子情報技術省	2020年	ガイドライン	1,2,4
20	シンガポール	Personal Data Protection Act 2012	https://sso.agc.gov.sg/Act/PDPA2012?ViewType=Pdf&_=20221206160704	シンガポール政府	2013年	法令	1,2,4
21	ベトナム	個人データの保護に関する政令草案 (DỰ THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)	https://vietnam-business-law.info/blog/2021/8/30/draft-new-decree-on-personal-data-protection-in-vietnam https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Du-thao-Nghi-dinh-quy-dinh-ve-bao-ve-du-lieu-ca-nhan-465185.aspx	公安省	2021年	法令	1,2,4

調査項目

- 「調査文献一覧表」の最右列「調査項目」に記載されている番号は下表の番号にそれぞれ対応

調査項目（データ関連）	
1	文献に記述されている、ステークホルダー間でのデータの流通や利活用の方法・方針・方向性、あるいはその方法を促進する規則・ルールなど (文献の狙い)
2	既に国内外で策定されているデータ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、書誌的情報（国・地域、適用分野、策定者、対象者、遵守義務、普及状況など）
3	文献で挙げられているデータ流通基盤等 (例：DATA-EX、GAIA-X) における信頼性に係るコンセプト及びセキュリティ要件等
4	データの差異や区分（カテゴリ）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
5	データの信頼性を確認するための技術的又は制度的枠組 (例：GAIA-X、IDSAにおける枠組等)

データ関連文献 #1：概要

包括的データ戦略

1	概要		サイバー空間の膨張に伴い、プライバシーの侵害、セキュリティ、データ保護の確保、競争上の課題、さらにはフェイクニュースなど民主主義の根本等に関わる様々な負の側面も顕在化し、国家監視型社会に対する懸念も強まっている。このような背景のもと、世界トップレベルのデジタル国家を目指し、それにふさわしいデジタル基盤を構築するため包括的なデータ戦略を策定することとする。		
2	書誌的情報	名称	包括的データ戦略		
		主旨	我が国では、これまで幾多の関連戦略の策定にもかかわらず、日本社会全体でのデータに係るリテラシーの低さ、プライバシーに関する強い懸念等から、データの整備、データの利活用環境の整備、実際のデータの利活用は十分に進んでこなかった。本戦略は、令和２年10 月よりデータ戦略タスクフォースが抽出した課題に対する具体的対応とその実装に向けた方策を定めるものである。		
		文献タイプ	政策		
		国・地域	日本	適用分野	サイバーセキュリティに関与する分野全般
		策定者	デジタル庁	対象者	国民や行政機関、企業、アカデミア等
		順守義務	データ戦略推進のための行動指針である。		
		普及状況	記載なし。		
		策定年	2021年	ページ数	57
3	データ流通における信頼性のコンセプト・セキュリティ要件		フィジカル空間をサイバー空間につなぐにはフィジカル空間をサイバー空間に変換する層が必要となる。両者の関連を確保するため様々なレベルのトラストを確保することが鍵であり、トラストには、以下が考えられる。 ■サイバー空間におけるデータの真正性や完全性からなるデータそのものの信頼性 ■データの属性を含めた信頼性　■データの提供先の信頼性 まずはこれらトラスト基盤を構築することが必要である。将来的には、Trusted Web 推進協議会が提示したトラステッド・ウェブ構想に示されたように、データの出し手やデータの受け手を検証し、やりとりする相手やそのデータに係るトラストを高める仕組みが求められる。		

包括的データ戦略

4	セキュリティ区分・水準・対策	-
5	技術的・制度的枠組	• これまで我が国では、国民生活や産業社会活動にとって重要な農業、防災、自動運転、インフラ、スマートシティなど幅広い分野を対象に、内閣府SIP事業や各府省庁プロジェクト等を活用し、分野ごとのプラットフォーム構築を官民連携で検討してきた。 今後は、これらの取組を踏まえ、①プラットフォーム検討の共通手順、②データ連携に必要な共通ルール(データ流通を促進・阻害要因を払拭するためのルールを含む)、③データ流通を容易にするツール開発、④DATA-EX による分野間連携と外部組織との連携について、検討する必要がある。 • プラットフォーム構築にあたっては、分野間データ連携に必要なツールとそれを提供するプラットフォームであるDATA-EX の成果やサービスを効率的に活用していくこととする。 • 個別分野におけるプラットフォームについては、分野間連携を念頭に構築するものとする。 その際、既存の政府内等のプラットフォームの推進を進めるとともに喫緊に対応すべき健康・医療・介護、教育、防災、農業、インフラ、スマートシティなどを重点的に取り組むべき分野として取り上げることとする。
関連URL		Trusted Web ホワイトペーパ/Trusted Web推進協議会(白書) https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb2.pdf DATA-EX(データ連携に係る既存の取り組み紹介) https://data-society-alliance.org/data-ex/ eIDAS(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910

包括的データ戦略

狙い

背景

• 世界トップレベルのデジタル国家を目指し、それにふさわしいデジタル基盤を構築するため包括的なデータ戦略を策定することとする。
我が国では、社会全体でのデータに係るリテラシーの低さ、プライバシーに関する強い懸念等から、データの利活用は十分に進んでこなかった。
そこで、令和2年10月よりデータ戦略タスクフォースで課題の頭出しを行った。本戦略は、抽出された課題に対する具体的対応とその実装に向けた方策を定めるものである。

日本全体が参照すべきアーキテクチャ

• 本戦略のビジョンを実現するためには、データに関わる我が国の全てのプレイヤーが我が国全体のデータ構造＝「アーキテクチャ」を共有し、それぞれの取組の社会全体での位置付けを明確化、連携の在り方を模索するとともに、無駄な重複の排除、欠落部分の補完を行っていく必要がある。
• 本戦略の策定、実践は常にこのアーキテクチャを踏まえて行うものとする。

トラスト

• サイバー空間とフィジカル空間が高度に融合したSociety5.0の実現にあたり、フィジカル空間をサイバー空間につなぐことが必要であり、そのためにはフィジカル空間をサイバー空間に変換する層が必要となる。両者の関連を確保するため様々なレベルの信頼性(トラスト)を確保することが鍵である。

プラットフォーム構築

• これまでは、農業、防災、自動運転、インフラ、スマートシティなど幅広い分野を対象に、分野ごとのプラットフォーム構築を官民連携で検討してきた。
今後は、これらの取組を踏まえ、①プラットフォーム検討の共通手順、②データ連携に必要な共通ルール(データ流通を促進・阻害要因を払拭するためのルールを含む)、③データ流通を容易にするツール開発、④DATA-EXによる分野間連携と外部組織との連携について、検討する必要がある。
個別分野におけるプラットフォームについては、分野間連携を念頭に構築するものとする。
その際、既存の政府内等のプラットフォームの推進を進めるとともに喫緊に対応すべき健康・医療・介護、教育、防災、農業、インフラ、スマートシティなどを重点的に取り組むべき分野として取り上げることとする。

データ関連文献 #1：主な調査項目

包括的データ戦略

狙い

データ取引市場とPDS・情報銀行

- 欧州ではGAIA-Xが、データ流通に関わるルールと連携基盤を一体的に整備・拡大している。
  日本では、特にデータ取引市場の取組は十分な規模と認知を得られていない。デジタル庁が関係府省庁と協力して、データ取引市場の実装を検討する。

ベース・レジストリ整備の推進

- スマートシティ等の新しいサービスの創出を図るためには、マイナンバーや地理空間情報50など社会全体の基盤となるデータを整備・活用することが必要である。
  そこで、まずはベース・レジストリを、「公的機関等で登録・公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データであり、正確性や最新性が確保された社会の基盤となるデータベース」と定義し、その整備を推進することとする。

データ関連文献 #2：概要

プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0

1	概要	広く多様なデータを活用して新たな価値を創出するためには、「データ連携」とそれを「利活用したサービスを提供」するプラットフォーム(PF)の構築が鍵であり、PF の構築は包括的データ戦略において重要政策として取り上げられている。重点的に取り組むべき分野として、健康・医療・介護分野、教育分野、防災分野、農業分野、インフラ分野及びスマートシティ分野を指定し、関係省庁はデジタル庁と協力して令和 7 年までに PF の実装を目指すこととしている。本文書はPFにデータ取扱いルールを実装するに際して踏まえるべき視点と検討の手順をまとめている。

2	書誌的情報	名称	プラットフォームにおけるデータ取扱いルールの実装ガイダンスver1.0		
		主旨	本文書は、PF を介してのデータ流通を推進するに当たっての「課題」に対応し、価値創出プロセスの関与者を始めとするステークホルダーの懸念・不安を払拭するための「データ取扱いルールの実装」を行うためのガイダンスである。		
		文献タイプ	ガイドライン		
		国・地域	日本	適用分野	PFに関するデータ取扱いルール実装。
		策定者	デジタル庁	対象者	PFの運営者と関係省庁、デジタル庁の担当者、DATA-EXの運営者、及びこれらのPF上でデータ取引を行うPFの参加者。
		順守義務	本文書は、PFにデータ取扱いルールを実装する際に必要な視点と検討の手順をまとめたガイダンスである。		
		普及状況	記載なし。		
		策定年	2022年	ページ数	47

3	データ流通における信頼性のコンセプト・セキュリティ要件	本ガイダンスは、「健康・医療・介護分野、教育分野、防災分野、農業分野、インフラ分野及びスマートシティ分野」に関連する関係省庁とデジタル庁が協力して構築する PF、及び分野間データ連携を目指す PF である DATA-EX を対象としている。読者としてはこれらの PF の運営者のほか、関係省庁及びデジタル庁の PF 担当者を想定している。また、当該 PF 上でデータ取引を行う PF の参加者も読者として想定をしている。

プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0

4	セキュリティ区分・水準・対策	「ノンパーソナルデータ」と「パーソナルデータ」のコントローラビリティ確保について、以下のように示している。 ■ノンパーソナルデータのコントローラビリティ確保 取引されるデータのタイプによって、被観測者やデータ提供者、データ利用者が抱く懸念・不安の内容が異なるので、これに応じて検討する。 ■パーソナルデータのコントローラビリティ確保 「ノンパーソナルデータのコントローラビリティ確保」に加えてさらに、プライバシー尊重の観点から本人(被観測者)の自身のパーソナルデータに対するコントローラビリティを確保する必要がある。
5	技術的・制度的枠組	■本ガイダンスでは、経済産業省に設置されたSociety 5.0 における新たなガバナンスモデル検討会によって提唱されたガバナンスモデルを採用する。(Society5.0 を実現するためには、ルール形成・モニタリング・エンフォースメントのガバナンスの各プロセスにおいて、サイバー空間及びフィジカル空間のアーキテクチャを設計・運用している企業や、これらを利用するコミュニティ・個人による、ガバナンスへの積極的な関与を確保することが肝要だと提言されている。) ■パーソナルデータに対する本人(被観測者)のコントローラビリティについては、個人情報保護法に加え OECD のプライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告(OECD Council Recommendation)の 8 原則にのっとった検討が必要である。 ■総務省と経済産業省が公表した「DX時代におけるプライバシーガバナンスガイドブック ver1.2」には、企業がプライバシーに関わる問題について能動的に取り組み、信頼の獲得につながるプライバシーガバナンスを構築するために、まず取り組むべきことがまとめられており、参考になる。
関連URL		GOVERNANCE INNOVATION: Society5.0 の実現に向けた法とアーキテクチャのリ・デザイン(ガバナンスモデルに関する説明) https://www.meti.go.jp/press/2020/07/20200713001/20200713001-1.pdf データ社会推進協議会(DSA)(組織紹介) https://data-society-alliance.org/ 総務省、経済産業省、「DX 時代における企業のプライバシーガバナンスガイドブック ver1.2(ガイドライン)」 https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf OECD Council Recommendation - Guidelines on the protection of Privacy and Transborder Flows of Personal Data(ガイドライン) https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0

概要

- 社会のデジタル化に伴い「データ」は智恵・価値・競争力の源泉となり、国民の豊かな生活と活動しやすい事業環境の実現を助ける。
  さらには、地球規模の課題から安全保障に至るまで「データの存在／活用」が決定的に重要となっている。
  広く多様なデータを活用して新たな価値を創出するためには、「データ連携」とそれを「利活用したサービスを提供」する基盤となる「プラットフォーム(PF)」の構築が鍵となる。
  重点的に取り組むべき分野として、健康・医療・介護分野、教育分野、防災分野、農業分野、インフラ分野及びスマートシティ分野を指定し、関係省庁はデジタル庁と協力して令和7年(2025年)までにPFの実装を目指すこととしている。
- PFを介してデータ流通を促進し新たな価値の創出へとつなげるためには、「データ流通を推進するに当たっての課題」に対応し、価値創出プロセスの関与者を始めとするステークホルダーの懸念・不安を払拭するためのデータ取扱いルールの実装が必要となる。
- 本文書は、PFにデータ取扱いルールを実装するに際して踏まえるべき視点と検討の手順をまとめたガイダンスである。
- 本ガイダンスは、「健康・医療・介護分野、教育分野、防災分野、農業分野、インフラ分野及びスマートシティ分野」に関連する関係省庁とデジタル庁が協力して構築するPF、及び分野間データ連携を目指すPFであるDATA-EXを対象としている。
  したがって、読者としてはこれらのPFの運営者のほか、関係省庁及びデジタル庁のPF担当者を想定している。
  また、当該PF上でデータ取引を行うPFの参加者も読者として想定をしている。そして、本ガイダンスではこれらの想定読者が、自ら構築又は参加しようとしているPFについて、以下の2点を可能にすることを狙いとしている：
  ➢ステークホルダーの懸念・不安(＝リスク)を特定し、これを払拭するためのデータ取扱いルールをPFに実装できるようになる。
  ➢環境変化に応じて新たに顕在化するリスクを適切に評価し、ルールを更新できるようになる。

データ流通における信頼性のコンセプト・セキュリティ要件

- 本ガイダンスは、「健康・医療・介護分野、教育分野、防災分野、農業分野、インフラ分野及びスマートシティ分野」に関連する関係省庁とデジタル庁が協力して構築するPF、及び分野間データ連携を目指すPFであるDATA-EXを対象としている。
  したがって、読者としてはこれらのPFの運営者のほか、関係省庁及びデジタル庁のPF担当者を想定している。
  また、当該PF上でデータ取引を行うPFの参加者も読者として想定をしている。
- 本ガイダンスでは、これらの想定読者が自ら構築又は参加しようとしているPFについて、以下の2点を可能にすることを狙いとしている。
  ➢ステークホルダーの懸念・不安(＝リスク)を特定し、これを払拭するためのデータ取扱いルールをPFに実装できるようになる。
  ➢環境変化に応じて新たに顕在化するリスクを適切に評価し、ルールを更新できるようになる。

データ関連文献 #2：主な調査項目

プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0

セキュリティ区分・水準・対策

・「ノンパーソナルデータ」と「パーソナルデータ」のコントローラビリティ確保*について、以下のように示している。

*コントローラビリティ確保:
コントローラビリティとは、明示された目的及びデータ取扱い方針の範囲内でデータが利用されるよう、又は明示された目的及びデータ取扱い方針の範囲外でデータが利用されないよう、当該データの被観測者やデータ提供者が当該データの取扱いに直接的又は間接的に関与可能なことである。

ノンパーソナルデータのコントローラビリティ確保

・ノンパーソナルデータについて必要とされるコントローラビリティの確保レベルは、取引されるデータのタイプによって、被観測者やデータ提供者、データ利用者が抱く懸念・不安の内容が異なるので、これに応じて検討する。
＜取引されるデータのタイプ＞
①開示可能なデータ：有償・無償にかかわらず、不特定の相手へ提供可能。目的外利用も可能。
②条件付きで提供可能なデータ：被観測者やデータ提供者及び存在する場合には上流関与者が同意した相手に、同意した利用目的の範囲でのみ第三者提供可能。
③原則秘匿のデータ：営業上の秘密や技術ノウハウ等、秘匿管理すべきデータ。
提供せざるを得ないデータ利用者にのみ必要最小限の利用目的に限り原則直接提供され、第三者提供は原則不可。

パーソナルデータのコントローラビリティ確保

・パーソナルデータを取り扱う際には「ノンパーソナルデータのコントローラビリティ確保」に加えてさらに、プライバシー尊重の観点から本人(被観測者)の自身のパーソナルデータに対するコントローラビリティを確保する必要がある。
・そのため、個人情報保護法の規定を確認の上、これを遵守するために必要な措置を講ずることはもちろんのこと、本人(被観測者)のプライバシー侵害に対する懸念・不安への対応も必要となる。

データ関連文献 #3：概要

Data Protection Act of 2021

1	方針		「データ保護エージェンシー(以下エージェンシー) 」という独立したエージェンシーが設立され、リスクの高いデータ慣行及び個人データの収集、処理、及び共有を規制するものとする。		
2	書誌的情報	名称	Data Protection Act of 2021		
		主旨	エージェンシーは、連邦プライバシー法に基づいた「連邦取引委員会の権限」(規則の規定、ガイドラインの発行、法律により義務付けられた調査の実施や報告書発行等)のすべての権限及び義務を有するものとする。		
		文献タイプ	法案		
		国・地域	米国	適用分野	個人データを収集、管理する分野全般
		策定者	連邦議会	対象者	行政、大規模な個人データを扱うデータアグリゲーター及び周辺の企業、個人等。
		順守義務	法案の段階にある。		
		普及状況	法案の段階にある。		
		策定年	(例) 2021年	ページ数	90
3	データ流通における信頼性のコンセプト・セキュリティ要件		記載なし。		
4	セキュリティ区分・水準・対策		記載なし。		
5	技術的・制度的枠組		記載なし。		
関連URL			Protecting Consumer Privacy and Security(組織紹介) https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security		

データ関連文献 #3：主な調査項目

Data Protection Act of 2021

狙い

データ保護エージェンシーの設立

「データ保護エージェンシー(以下エージェンシー)」という独立したエージェンシーが設立され、リスクの高いデータ慣行及び個人データの収集、処理、及び共有を規制するものとする。
局長は大統領が指名するものとする。
局長は、すべての執行及び管理機能に関して、エージェンシーの一般的な権限を確立する権限を与えられる。

- エージェンシーは、消費者金融保護局、連邦通信委員会、連邦取引委員会、商務省、及びその他の連邦エージェンシー及び州の規制当局と調整し、必要に応じて、個人データの規制上の取り扱いを促進するものとする。
- エージェンシーは、年間総収入が25,000,000ドルを超えるデータアグリゲーター、又は毎年50,000以上の個人、世帯、又はデバイスのデータを単独又は組み合わせて収集、使用、又は共有しているデータアグリゲーターから料金を徴収することができる。
- エージェンシーは、個人情報の処理を通じて、個人のプライバシーを保護し、プライバシー侵害を防止及び是正し、保護された階級に基づく差別を防止、是正し、及び軽減するよう努めなければならない。
- エージェンシーは、「プライバシー又はデータ保護に関連するすべての連邦法、行政命令、規制、及びポリシーを実施するためのすべての連邦省庁及びエージェンシーの取り組みにリーダーシップと調整を提供する」等の機能をもつ。
- エージェンシーは、本法及び連邦プライバシー法の条項を管理、施行、及び実施するために、本法に基づいてその権限を行使する権限を与えられている。
- 局長は、エージェンシーが本法及びその他の連邦プライバシー法の目的、及び目的を管理、及び実行できるようにするために必要又は適切な規則を規定し、命令及びガイダンスを発行することができる。
- エージェンシーは、大規模なデータ収集者に対して定期的に報告を要求し、調査を実施することができる。
  エージェンシーは、共同調査及び情報の要求をしたり、証人の出席と証言等のために召喚状を発行することができる。
- エージェンシーは、連邦プライバシー法に基づいた「連邦取引委員会の権限」(規則の規定、ガイドラインの発行、法により義務付けられた調査の実施や報告書発行等)すべての権限及び義務を有するものとする。

データ関連文献 #4：概要

SP 800-47 Rev. 1 Managing the Security of Information Exchanges

1	概要	交換前、交換中、及び交換後に交換又はアクセスされる情報の保護の管理に焦点を当て、情報交換の識別、交換された情報を保護するための考慮事項、及び情報交換に関連するリスクの管理を支援するために必要な契約に関するガイダンスを提供している。

2	書誌的情報	名称	SP 800-47 Rev. 1　Managing the Security of Information Exchanges		
		主旨	本ガイドラインでは、異なる組織 (内部又は外部) によって所有及び運用されているシステム間、又は承認の境界を越えるシステム間での情報交換とアクセスを計画、確立、保守、及び中止するためのガイダンスを提供する。		
		文献タイプ	ガイドライン		
		国・地域	米国	適用分野	企業、団体における情報交換 (共有)。(内部又は外部との情報交換/共有) 。
		策定者	NIST	対象者	システム間の情報交換とアクセスの計画、承認、確立、保守等を担当する、権限のある職員、システム所有者、情報所有者、プログラム管理者、セキュリティ担当者、システムアーキテクト、システム管理者、及びネットワーク管理者等。
		順守義務	この刊行物は、情報交換(共有)に関するガイダンス、保護に関する考慮事項を提供しており、組織は、情報交換に関する特定の組織のニーズと要件を満たすようにガイダンスを調整することが期待されている。		
		普及状況	不明。		
		策定年	2021年	ページ数	49

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。

データ関連文献 #4：概要

SP 800-47 Rev. 1 Managing the Security of Information Exchanges

4	セキュリティ区分・水準・対策	記載なし。
5	技術的・制度的枠組	各組織は、それぞれのシステムと情報のセキュリティを確保し、情報交換のフェーズ全体で組織間の定期的なコミュニケーションを含む、情報交換に適切に調整されたアプローチを適用する責任がある。したがって、組織は、適切な管理及び技術スタッフ、ビジネス所有者、システム所有者、情報所有者、システムセキュリティ担当者、システム管理者、ネットワーク管理者、及びシステムセキュリティ アーキテクトを含む参加組織の代表者で構成される共同計画チームの設立を検討する。
関連URL		CIRCULAR NO. A-130TO (SUBJECT: Managing Information as a Strategic Resource)(通達) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

データ関連文献 #4：主な調査項目

SP 800-47 Rev. 1 Managing the Security of Information Exchanges

概要

- 本ガイドラインでは、異なる組織(内部又は外部)によって所有及び運用されているシステム間、又は承認の境界を越えるシステム間での情報交換とアクセスを計画、確立、保守、及び中止するためのガイダンスを提供する。
- ガイダンスは、情報交換の安全な管理のために行政管理予算局(OMB)の通達A-130で指定された要件と一致している。
- このガイダンスでは、情報交換管理の次の4つのフェーズを扱う。

1. 情報交換の計画	参加組織は、関連するすべての技術的、セキュリティ及び管理上の問題を調査し、情報の管理と使用、及び情報の交換方法を管理するための適切な合意を作成する。
2. 情報交換の確立	組織は、適切なセキュリティ制御の実装又は構成、適切な契約の作成と署名など、情報交換を確立するための計画を策定及び実行する。
3. 交換及び 関連する契約の維持	組織は、情報交換が確立された後も情報交換のセキュリティを積極的に維持し、合意された頻度で契約を確認して再検討するなど、関連する契約の条件が満たされ、関連性が維持されるようにする。
4. 情報交換の中止	情報交換は一時的なものである場合もあれば、ある時点で組織が情報交換を中止する必要がある場合もある。 交換が一時的なものであれ、期間的なものであれ、情報交換の締結は、相手方のシステムを混乱させない方法で行われる。 ただし、インシデントやその他の緊急事態に対応して、組織は情報交換を即座に中止することを決定する場合がある。

データ関連文献 #4：主な調査項目

SP 800-47 Rev. 1 Managing the Security of Information Exchanges

技術的・制度的枠組み

各組織は、それぞれのシステムと情報のセキュリティを確保し、情報交換のフェーズ全体で組織間の定期的なコミュニケーションを含む、情報交換に適切に調整されたアプローチを適用する責任がある。
したがって、組織は、適切な管理及び技術スタッフ、ビジネス所有者、システム所有者、情報所有者、システムセキュリティ担当者、システム管理者、ネットワーク管理者、及びシステムセキュリティ アーキテクトを含む参加組織の代表者で構成される共同計画チームの設立を検討する。

共同計画チームは、既存のワーキンググループの一部になることも、計画された情報交換のために特別に作成することもできる。
共同計画チームは、交換された情報を管理するために必要な合意を決定し、文書化する。機密保持契約と組み合わせた相互接続セキュリティ契約*など、複数の種類の契約が必要になる場合がある。

*相互接続セキュリティ契約
相互接続セキュリティ契約 (ISA) は、2 つ以上のシステム間の相互接続を確立、運用、及び維持するための技術要件とセキュリティ要件を指定するドキュメントである。
ISA はシステムを接続するための要件を文書化する。交換される情報と、情報を処理、保存、又は送信するシステムを保護するために必要な保護要件と制御について説明する。通常、相互接続のトポロジ図を含める。

共同計画チームは、各組織の承認担当者又はその他のリスク管理担当者に提案された契約を提出し、情報交換の承認を求める。
受領後、承認担当者又はリスク管理担当者は、提案された契約及びその他の関連する文書又は活動を確認し、レビューに基づいて、承認担当者又はリスク管理担当者は次のいずれかを決定する。
•情報交換を承認する
•情報交換を拒否する

データ関連文献 #5：概要

A European strategy for data

1	概要	欧州委員会は2014年以降、データセキュリティについて、既に多くの措置を講じている。EUは一般データ保護規則(GDPR)により、デジタルトラストのための強固なフレームワークを作成した。GDPRの今後のレビューは、この点でさらに有用な要素を提供する可能性がある。データ経済の発展を促進した他のイニシアチブは、非個人データの自由な流通に関する規則(FFD)、サイバーセキュリティ法(CSA)、及びオープンデータ指令である 。この文書は、EUが世界で最も魅力的で、最も安全で、最もダイナミックなデータアジャイル経済になることを可能にするという野心を持つ欧州のデータ戦略を提案し、この目標を達成するための政策措置を列挙している。

2	書誌的情報	名称	A European strategy for data		
		主旨	欧州における今後5年間のデータ経済を可能にするための戦略について概説している。この戦略に基づいて、欧州委員会は、欧州社会の基盤である基本的価値を尊重しながら、EUをデータアジャイル経済の最前線にとどめるために取ることができる具体的な措置に関して包括的な協議を開始する。		
		文献タイプ	政策		
		国・地域	EU	適用分野	EU全域に関するデータ経済分野全般
		策定者	欧州委員会(EC)	対象者	EU全域に関するデータ経済についての戦略として、EU全域の国家、国民に通知している。
		順守義務	本文書は、欧州のデータ戦略を提案し、目標を達成するための政策措置を列挙している。		
		普及状況	不明。		
		策定年	2020年	ページ数	34

3	データ流通における信頼性のコンセプト・セキュリティ要件	欧州は加盟国、企業、市民の「サイバーセキュリティの脅威と攻撃への取組」を支援するための包括的なフレームワーク「EUサイバーセキュリティ認証フレームワーク」を有している。 本文献では「データへのアクセスと利用のための分野横断的なガバナンスの枠組みを作成すること」の重要性を指摘している。

A European strategy for data

4	セキュリティ区分・水準・対策	記載なし。
5	技術的・制度的枠組	サイバーセキュリティの分野では、欧州は加盟国、企業、市民の「サイバーセキュリティの脅威と攻撃への取組」を支援するための包括的なフレームワークを開発しており、そのフレームワークに基づいて構築されるデータとサービスを保護するためのメカニズムの開発と改善を継続する。データを利用した製品やサービスの安全で広範な使用は、最高のサイバーセキュリティ基準に依存する。EUサイバーセキュリティ認証フレームワーク*とEUサイバーセキュリティ庁(ENISA)**は 、その取り組みに向けて重要な役割を果たすことが期待されている。 *EUサイバーセキュリティ認証フレームワーク(The EU cybersecurity certification framework): 現在、EUにはICT製品のさまざまなセキュリティ認証スキームが存在するが、EU全体で有効なサイバーセキュリティ証明書の共通の枠組みがなければ、加盟国間の断片化と障壁のリスクが高まる。認証フレームワークは、包括的な一連の規則、技術要件、基準、及び手順として、EU全体の認証スキームを提供する。 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework **EUサイバーセキュリティ庁(ENISA) The European Union Agency for Cybersecurity EUのサイバー政策に貢献し、サイバーセキュリティ認証スキームを使用してICT製品、サービス、及びプロセスの信頼性を高め、加盟国及びEU機関と協力し、欧州が明日のサイバー課題に備えるのを支援する。 https://www.enisa.europa.eu/
関連URL		REGULATION (EU) 2016/679 General Data Protection Regulation (GDPR) (規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 REGULATION (EU) 2018/1807 free flow of non-personal data (FFD) (規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807 REGULATION (EU) 2019/881 Cybersecurity Act (CSA) (規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881 Directive (EU) 2019/1024 Open Data Directive(指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024 The EU cybersecurity certification framework(認証フレームワーク) https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework The European Union Agency for Cybersecurity(組織紹介) https://www.enisa.europa.eu/

A European strategy for data

狙い

- 欧州は、生産性の向上や競争の激しい市場だけでなく、健康と福祉、環境、透明性のあるガバナンス、便利な公共サービスの改善など、データをより良く使用することのメリットを享受することを目指している。
- このホワイトペーパーでは、今後5年間のデータ経済を可能にするための戦略について概説している。
- この戦略に基づいて、欧州委員会は、欧州社会の基盤である基本的価値を尊重しながら、EUをデータアジャイル経済の最前線にとどめるために取ることができる具体的な措置に関して包括的な協議を開始する。

データ量の増加と技術の変化

- 世界で生成されるデータの量は急速に増加しており、2018年の33ゼタバイトから2025年には175ゼタバイトになると予想されている。データの新しい波は、EUがこの分野で世界のリーダーになるための大きな機会を表している。

EUの可能性

- EUは、データアジャイル経済で成功する可能性を秘めている。
- EUは技術、ノウハウ、そして高度なスキルを持つ労働力を持っている。
- しかし、中国や米国などの競合他社はすでに急速に革新している。欧州の可能性を実現するためには、高いプライバシー、セキュリティ、安全性、倫理基準を維持しながら、データの流れと幅広い使用のバランスを取りながら、欧州の方法を見つける必要がある。

問題点―以下のような面における問題が、EUにおけるデータ経済向上の可能性を妨げている

- データの可用性 ・データガバナンス ・データインフラストラクチャとテクノロジー ・スキルとデータリテラシー ・サイバーセキュリティ

戦略―以下のような戦略が重視される

- データへのアクセスと利用のための分野横断的なガバナンスの枠組みを作成する。
- データへの投資と、データのホスティング、処理、使用、相互運用性のための欧州の能力とインフラストラクチャの強化
- コンピテンシー(個人のエンパワーメント：個人データに関する個人の権限の増大)、スキルへの投資、中小企業への投資)
- 欧州共通のデータ空間(戦略的経済部門と公益領域における欧州共通のデータスペースの開発)

オープンでありながら積極的な国際的アプローチ

- 今日の欧州企業は、EUの国境を越えた環境で事業を行っているため、国際的なデータフローは競争力に不可欠である。
- EUは、単一市場の規制環境の強みを基盤として、データに関する国際協力を主導・支援し、グローバルスタンダードを形成し、EU法を完全に遵守して経済・技術開発が繁栄できる環境を作り出すことに強い関心を持っている。
- 欧州委員会は、国際的なデータ流通の更なる促進に関して、EUの戦略的利益を分析する能力を引き続き改善する。

Data governance and data policies at the European Commission

1	概要	データガバナンスとデータポリシーは、欧州委員会が規制及び法的要件(特にデータと文書の管理、データとドキュメントへのアクセス、データ保護、知的所有権、情報セキュリティに関連する要件)に対応するのに役立ち、関連するリスクを軽減する。データガバナンスとデータポリシーにより、欧州委員会はデータ駆動型の組織に変革する。

2	書誌的情報	名称	Data governance and data policies at the European Commission		
		主旨	文書の目的は、データガバナンスとデータポリシーにより、欧州委員会がデータ駆動型の組織に変革する方法を示すことである。		
		文献タイプ	政策		
		国・地域	EU	適用分野	欧州委員会におけるデータ取り扱い分野
		策定者	欧州委員会(EC)	対象者	欧州委員会の組織
		順守義務	欧州委員会はデータガバナンスとデータポリシーにより、データ駆動型の組織に変革する。		
		普及状況	記載なし。		
		策定年	2020年	ページ数	20

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。 データ保護に関しては、Regulation (EU) 2018/1725の法的要件及び運用上の義務に準拠する必要がある、と述べている。情報セキュリティに関しては、欧州委員会の情報セキュリティチームが提供する原則と実施ガイドラインを参照する旨述べている。

4	セキュリティ区分・水準・対策	記載なし。

Data governance and data policies at the European Commission

5	技術的・制度的枠組	記載なし。

関連URL	Regulation (EU) 2018/1725(規制) https://edps.europa.eu/data-protection/our-work/publications/legislation/regulation-eu-20181725_en EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725(ガイドライン) https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf

データ関連文献 #6：主な調査項目

Data governance and data policies at the European Commission

狙い

- データガバナンスとデータポリシーにより、欧州委員会はデータ駆動型の組織に変革する方向にある。
- データガバナンスには、「データ資産*の管理と使用に関する戦略、ポリシー、及び共有された意思決定の定義、実装、監視」が含まれる。
  これは、確立されたデータ関連の役割を持つ欧州委員会のスタッフによって実行される。
  データガバナンスには以下の3つのレベルがある。
  - ➢長期ビジョンを定義し、方向性を示し、進捗状況を監督し、戦略的決定を下す。
  - ➢管理職は、組織レベル及びローカルレベルでのデータポリシーの策定と実装に責任を持つ。
  - ➢運用:データポリシーが実際に実装され、データに関する決定が行われる。

- データポリシーは、欧州委員会のデータ資産*を管理できる指針となる枠組みを形成する一連の広範で高レベルな原則である。
- 具体的には、データポリシー次の項目を含む：データ管理/データ資産の作成/収集/取得
- データ品質：管理する必要があるデータ品質には次が含まれる：正確性/完全性/一貫性/一意性/整合性/適時性/出所/データ収集方法
- データ保護に関しては、Regulation(EU)2018/1725等、情報セキュリティに関しては、委員会の情報セキュリティチームが提供する原則と実施ガイドラインを参照するものとする。

*データ資産:「欧州委員会によって作成されたり」、「加盟国又はその他の利害関係者から収集されたり」、「第三者から取得された」データのコレクション、データセット、又は情報である。

データガバナンスとデータポリシーを実装する方法

- 実装には、組織レベルとローカルレベルの両方での行動と投資が必要である。
- 欧州委員会のデータガバナンスとデータポリシーは次のとおりである。
  - ➢組み込み:既存のビジネスプロセスへのシームレスな統合と、可能な限りの簡素化に焦点を当てる。
  - ➢持続可能:終了日が事前に決定されたプロジェクトと見なすべきではなく、継続的な改善プロセスである。
  - ➢測定可能:進捗状況を測定し、事前に計画を立てることができることが、継続的な改善に不可欠である。
  - ➢説明責任と責任:すべての利害関係者に自分自身の役割と責任、及び他者の役割と責任を明確にし、これらと一致する行動を奨励する。
  - ➢透明性重視:欧州委員会は、他のEU機関や加盟国の行政機関、及び第三者が、特に政策立案に使用されるデータ資産にアクセスして再利用できるようにするように努める必要がある。
  - ➢原則ベース:データガバナンスとデータポリシーは、詳細プロセスを指定するのではなく、原則を定めてガイダンスを提供することを重視する必要がある。
  - ➢欧州委員会全体かつ包括的:データガバナンスとデータポリシーはローカルで実装できるが、効果を上げるには組織全体で調整を行う必要がある。

データ関連文献 #7：概要

Data Governance Act

1	概要	データ経済は、事業、特に零細・中小企業と新興企業が繁栄し、データアクセスの中立性とデータポータビリティ、相互運用性を確保できるように構築する必要がある。 本文書は、EU全体でのデータ共有メカニズムを強化することにより、データの可用性を促進することを目的としている。 この規則は「データの再利用に関する条件」、「データ仲介サービス」や「利他的な目的で利用可能なデータを収集及び処理する事業体」に関するフレームワークを示している。この規則は、その全体が拘束力を持ち、すべての加盟国に直接適用されるものとする。

2	書誌的情報	名称	Data Governance Act		
		主旨	この規則は以下を定めている。 (a)EU内で、公共部門の機関が保有する特定のカテゴリーのデータを再利用するための条件 。 (b)データ仲介サービスの提供のための通知及び監督の枠組み 。 (c)利他的な目的で利用可能なデータを収集及び処理する事業体の自発的な登録のためのフレームワーク。 (d)欧州データイノベーション委員会の設立のための枠組み。 この規則は、公的機関にデータの再利用を許可する義務を課すものではなく、公的機関を連合法又は国内法に基づく守秘義務から解放するものでもない。個人データの保護に関するEU法及び国内法は、この規則に関連して処理されるすべての個人データに適用されるものとする		
		文献タイプ	法令		
		国・地域	EU全域	適用分野	個人データの取り扱い。
		策定者	欧州委員会(EC)	対象者	加盟国の官公庁、公共部門、及びデータを収集及び処理を行う事業体。
		順守義務	この規則は、その全体が拘束力を持ち、すべての加盟国に直接適用されるものとする。		
		普及状況	本文献では次のように記されている： 「この規則は、欧州連合の官報に掲載された日から20日後に発効するものとする。2023年9月24日から適用される。」		
		策定年	2022年	ページ数	44

Data Governance Act

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。
4	セキュリティ区分・水準・対策	記載なし。
5	技術的・制度的枠組	政策アナリストのFrancesco Vogelezang氏は、Data Governance Actと、GDPR(General Data Protection Regulation：EU一般データ保護規則)の差異について以下のように述べている： GDPRは、「個人データは、処理される目的に関連して必要なものに限定されなければならない (「データの最小化」)」ことを明確にしている。GDPRは、個人データが処理される際の個人データの保護に重点を置いており、データ主体の立場を適切に保護するために「インフォームド コンセントに基づいて、正当な目的を達成するために必要な範囲でのみデータの処理を追求できる、最小限のアプローチ (「個人データが少ないほど良い」) をとっている。一方、Data Governance Actは、データの共有と再利用を促進するよう努めている。 https://openfuture.eu/blog/four-questions-for-the-european-strategy-for-data/
関連URL		European Data Innovation Board(組織紹介) https://digitalhealtheurope.eu/glossary/european-data-innovation-board/ European Data Protection Board(組織紹介) https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinion-data-governance-act-dga_en General Data Protection Regulation(GDPR)(規制) https://gdpr-info.eu/

Data Governance Act

狙い

Ⅰ章

- この規則は以下を定めている。
  - ➢EU内で、公共部門の機関が保有する特定のカテゴリーのデータを再利用するための条件。
  - ➢データ仲介サービスの提供のための通知及び監督の枠組み。
  - ➢利他的な目的でデータを収集及び処理する事業体の自発的な登録のためのフレームワーク。
  - ➢欧州データイノベーション委員会の設立のための枠組み。

Ⅱ章

- 以下の理由で保護されている公的機関が保有するデータに適用される。
  - ➢ビジネス、職業、及び会社の秘密を含む商業上の機密性
  - ➢統計的 機密性
  - ➢第三者の知的財産権の保護
  - ➢個人データが指令(EU)2019/1024の範囲外である場合の個人データの保護
- 上記のデータカテゴリーについて、以下が述べられている
  - ➢独占手配の禁止
  - ➢再利用の条件
  - ➢手数料
  - ➢管轄機関
  - ➢単一の情報ポイント：加盟国は、新しい機関を設立するか、既存の機関又は構造を単一の情報提供場所として指定する
  - ➢要求又は再利用の手順

Ⅲ章

- データ仲介サービスの義務等が述べられている。
  - ➢データ仲介サービスの届出
  - ➢データ仲介サービス提供者による通知
  - ➢データ仲介サービスの提供条件
  - ➢データ仲介サービスの所管官庁
  - ➢コンプライアンスの監視

データ関連文献 #7：主な調査項目

Data Governance Act

狙い

Ⅳ章　データ利他主義のための国家的取り決め

- 加盟国は、データ利他主義を促進するために、組織的又は技術的取り決め、あるいはその両方を実施している場合がある。
  そのために、加盟国はデータ利他主義のための国家政策を確立することができる。

Ⅴ章

- データ仲介サービスの所轄官庁及びデータ利他主義組織登録の所轄官庁は、データ仲介サービス提供者やデータ利他主義組織とは法的に区別され、機能的に独立していなければならない。

Ⅵ章　欧州データイノベーション理事会(the European Data Innovation Board)

- 欧州委員会は、データ仲介サービスの所管官庁の代表者、すべての加盟国のデータ利他主義組織の登録に関する所管官庁、ENISA、中小企業特使のネットワークによって任命された代表者で構成される専門家グループとして「欧州データイノベーション理事会」を設立するものとする。

Ⅶ章

- 欧州連合に保持されている「非個人データの国際的な転送、又はそれらのデータへの政府によるアクセス」がEUや加盟国の法律に抵触する場合は、そのような「国際的な転送や政府によるアクセス」を防止するため、公共部門機関やデータを再利用する権利が付与された自然人又は法人、データ仲介サービス プロバイダー、及びデータ利他主義組織は、契約上の取り決めを含め、すべての合理的な技術的、法的、及び組織的措置を講じるものとする。

Ⅷ章

- 委任された行為を採択する権限は、本条に定める条件に従って欧州委員会に付与される。
  欧州委員会は、委員会(committee)が補佐する。

Ⅸ章

- 加盟国は、非個人データの第三国への移転に関する義務の違反に適用される罰則等、様々な規則を定めるものとする。
- この規則は、欧州連合の官報に掲載された日から20日目に施行される。
- 2023年9月24日から適用される。
- この規則は、その全体が拘束力を持ち、すべての加盟国に直接適用されるものとする。

データ関連文献 #8：概要

Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)

1	概要	データはデジタル経済の中核的な要素であり、不可欠なリソースである。データへのアクセスと使用を規制することは、デジタル時代によってもたらされる機会をつかむための基本的な前提条件である。2021年3月、欧州議会決議は、すべてのセクターでデータのより大きく公平な流れを可能にするためのデータ法を提示するよう委員会に促した。このような流れに関連して、欧州委員会は、「データからの価値配分の公平性を確保し、データへのアクセスと使用を促進すること」を目的として、このデータ法を提案した。

2	書誌的情報	名称	Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)		
		主旨	この提案は、すべてのセクターにわたるEU企業が、「データに関して個人に力を与え」、企業や公共部門の機関に、「主要な政策的及び社会的課題に取り組むためのメカニズムを適切に装備する」という政策目標を達成するのに役立つ。		
		文献タイプ	法令		
		国・地域	EU全域	適用分野	データからの価値配分の公平性を確保した「データへのアクセスと使用」。
		策定者	欧州委員会(EC)	対象者	データ流通に関与する企業や公共機関。
		順守義務	第31条：各EU加盟国は、この規則の適用及び施行に責任を負う権限のある当局を1つ以上指定する。 第33条：各EU加盟国は、この規則の違反に適用される罰則に関する規則を定め、それらが実施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。		
		普及状況	➢ この規則は、欧州連合の官報に掲載された日から20日目に施行される。 ➢ この規則の発効日から12か月後から適用されるものとする。		
		策定年	2022年	ページ数	63

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。

Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)

4	セキュリティ区分・水準・対策	個人データの保護に対する基本的権利は、特にRegulation(EU)2016/679及びRegulation (EU)2018/1725の下で保護されている。また、Directive2002/58/ECは、端末機器に保存及び端末機器からのアクセスを行う個人データ及び非個人データに条件を提供するなど、私生活と通信の機密性をさらに保護している。本提案は、データ保護とプライバシーに関するEU法、特にRegulation(EU)2016/679及びDirective2002/58/ECを補完し、害を及ぼすものではない。 本提案は、個人データの処理に関するGDPRの規則と一致している。
5	技術的・制度的枠組	本提案の国際的なデータ処理と保存、及びデータ転送は、GDPR、世界貿易機関(WTO)のサービス貿易に関する一般協定(GATS:General Agreement on Trade in Services)に準拠している。 本提案は、個人データの処理に関するGDPRの規則」と一致している。 本提案は、データ保護とプライバシーに関するEU法、特にRegulation(EU)2016/679及びDirecyive2002/58/ECを補完する。
関連URL		GDPR(General Data Protection) (規制) https://gdpr-info.eu/ GATS(General Agreement on Trade in Services) (協定) https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm Directive(EU)2019/770(指令) https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770 Directive2002/58/EC(指令) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 Regulation(EU)2016/679(指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)

狙い

- データはデジタル経済の中核的な要素であり、不可欠なリソースである。
  人間と機械によって生成されるデータの量は、近年指数関数的に増加している。
  ただし、ほとんどのデータは使用されていないか、その価値が比較的少数の大企業の手に集中しており、データ主導のイノベーションの可能性を完全に実現することはできていない。
  したがって、データの再利用の機会を提供し、欧州の規則に準拠し、欧州の価値観を完全に尊重して、欧州のデータ経済の発展に対する障壁を取り除くことが重要である。
  誰もがこれらの機会から利益を得られるように、デジタル・デバイドを減らすことが必須となっている。
  非個人的な産業データの新しい波とモノのインターネットに接続された製品の急増に合わせて、データからの価値の分配におけるバランスを確保することは、ヨーロッパで持続可能なデータ経済を後押しする大きな可能性につながる、ということである。
- データへのアクセスと使用を規制することは、デジタル時代によってもたらされる機会をつかむための基本的な前提条件である。
  欧州委員会のウルスラ・フォン・デア・ライエン委員長は、2019-2024年委員会の政治的ガイドラインの中で、欧州は「高いプライバシー、セキュリティ、安全性、及び倫理基準を維持しながら、データの流れと使用のバランスをとる」と表明した。
- 2021年3月25日、欧州理事会は「社会と経済の利益のために、データとデジタル技術の可能性をより有効に活用することの重要性」を繰り返し表明した。
  また、同日、欧州議会決議は、business-to-business、business-to-government、government-to-business、government-to-governmentなど、すべてのセクターでデータのより大きく公平な流れを可能にするためのデータ法を提示するよう委員会に促した。
- このような流れに関連して、欧州委員会は、「データからの価値配分の公平性を確保し、データへのアクセスと使用を促進すること」を目的として、このデータ法を提案した。
  この提案は、すべてのセクターにわたるEU企業が、「データに関して個人に力を与え」、企業や公共部門の機関に、「主要な政策的及び社会的課題に取り組むためのメカニズムを適切に装備する」という政策目標を達成するのに役立つ。

Proposal for a Regulation on the European Health Data Space

1	概要	今日、自然人は、国内及び国境を越えた電子健康データへのアクセスと送信を含む、電子健康データに対する権利を行使することが困難になっている。 欧州のデータ戦略では、ドメインに特化した欧州共通のデータスペースの設立を提唱している。本文書では「欧州共通データスペース」としてEuropean Health Data Space(EHDS)の設立を提案している。 EHDSは、欧州委員会の健康分野での優先事項の一つである「電子健康データへのアクセスと共有」のための欧州保健連合(European Health Union)を構築する上で不可欠な要素である。

2	書誌的情報	名称	Proposal for a REGULATION on the European Health Data Space		
		主旨	本文書では「欧州共通データスペース」としてEuropean Health Data Space(EHDS)の設立を提案している。EHDSは以下のことを目的としている： ➢ 自然人が自分の電子健康データを容易に管理できる共通の空間を作り出す。 ➢ 研究者やイノベータ、政策立案者が、この電子的な健康データを利用することを可能にする。 ➢ 研究者やイノベータ、政策立案者が、プライバシーを保護した上で、信頼できる安全な方法でこの電子健康データを利用することを可能にする。 ➢ 電子健康記録、ゲノミクスデータ、患者登録など、さまざまな電子健康データへのより良いアクセスを促進する。		
		文献タイプ	法令		
		国・地域	EU全域	適用分野	電子健康データへのアクセスと共有。
		策定者	欧州委員会(EC)	対象者	電子健康データに関わる公共部門、機関、団体及び製造業者、販売者等。
		順守義務	加盟国は、この規則の違反に適用される罰則に関する規則を定め、それらが実施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。(第69条)		
		普及状況	第72条 ➢ この規則は、欧州連合の官報に掲載された日から20日目に施行される。 ➢ この制度は、効力発生後12ヶ月から適用する。		
		策定年	2022年	ページ数	121

Proposal for a Regulation on the European Health Data Space

3	データ流通における信頼性のコンセプト・セキュリティ要件	50条　安全な処理環境 健康データアクセス機関は、技術的及び組織的な対策、セキュリティ及び相互運用性の要件を備えた安全な処理環境を通じてのみ、電子健康データへのアクセスを提供するものとする。(例えば、「安全な処理環境へのアクセスを、それぞれのデータ許可に記載されている権限のある者に制限する」等のセキュリティ対策を講じるものとする。

4	セキュリティ区分・水準・対策	以下のカテゴリの1つに該当する自然人の電子データに基づいて、健康データアクセス機関によって利用可能にされた非個人的な電子データは、機密性が高いと見なされる。 ➢ ヒトの遺伝学的、ゲノム的及びプロテオミクス的データ ➢ 個人が生成した電子健康データ(医療機器、ウェルネスアプリケーション、その他のデジタルヘルスアプリケーションを含む)。 ➢ 特定疾病の医療台帳の電子健康データ ➢ 臨床試験からの電子健康データ ➢ 医療機器及び医薬品及び医療機器の登録簿からの電子健康データ ➢ バイオバンク及び専用データベースからの電子健康データ 上記のデータカテゴリに対する保護措置は、匿名化技術に依存する。

5	技術的・制度的枠組	EHDSは、GDPR、医療機器に関するRegulation(EU)2017/745(医療機器規則)、体外診断用医療機器に関するRegulation(EU)2017/746(体外診断規則)、人工知能法案(Artificial Intelligence Act)、データガバナンス法案(Data Governance Act)、データ法案(Data Act)、ネットワークと情報システムのセキュリティに関する指令(NIS指令)DIRECTIVE(EU)2016/1148、CBHC指令(Directive 2011/24/EU)、Regulation(EU)2018/1725(EUデータ保護規則)といった法制度を基盤にしたものである。 また、欧州保健緊急事態準備対応機関(HERA)、欧州のがん対策計画、EUがんミッション、及び欧州医薬品戦略の作業を支援する位置づけとなっている。

データ関連文献 #9：概要

Proposal for a Regulation on the European Health Data Space

関連URL	DIRECTIVE(EU)2016/1148(NIS Directive) (指令) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN Directive2011/24/EU(the application of patients' rights in cross-border healthcare: CBHC)(指令) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0024 Regulation(EU)No 910/2014(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG ANNEXES to theREGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILon the European Health Data Space(規制) https://health.ec.europa.eu/system/files/2022-05/com_2022-197_annex_en.pdf Regulation(EU)2016/679(規制) https://eur-lex.europa.eu/eli/reg/2016/679/oj COM/2020/767 final(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN Artificial Intelligence Act(法律) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN Regulation(EU)2017/745(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745 Regulation(EU)2017/746(規制) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746 Data Governance Act(法律) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN

データ関連文献 #9：主な調査項目

Proposal for a Regulation on the European Health Data Space

狙い

- GDPR(General Data Protection Regulation:一般データ保護規則)の規定によって、健康データを含むデータに対する自然人の保護が保護されている。
  それにもかかわらず、今日、自然人は、国内及び国境を越えた電子健康データへのアクセスと送信を含む、電子健康データに対する権利を行使することが困難になっている。
  これは、加盟国によるGDPRの解釈の不均一が、法的不確実性を生み出し、その結果、電子健康データの二次利用に障壁が生じているわけである。
  その障壁によって、研究者、イノベーター、規制当局、政策立案者が必要な電子健康データへのアクセスがしにくいため、自然人が革新的な治療法の恩恵を受けることができず、政策立案者が健康危機に効果的に対応できない特定の状況を作り出している。
- 欧州のデータ戦略では、ドメインに特化した欧州共通のデータスペースの設立を提唱している。
  本文書では「欧州共通データスペース」として European Health Data Space(EHDS)の設立を提案している。
  EHDSは、このような分野別欧州共通データスペースの最初の提案である。
  EHDSは、欧州委員会の健康分野での優先事項の一つである「電子健康データへのアクセスと共有」のための欧州保健連合(European Health Union)を構築する上で不可欠な要素である。
- EHDSは以下のことを目的としている。
  ➢自然人が自分の電子健康データを容易に管理できる共通の空間を作り出す。
  ➢研究者やイノベータ、政策立案者が、この電子的な健康データを利用することを可能にする。
  ➢研究者やイノベータ、政策立案者が、プライバシーを保護した上で、信頼できる安全な方法でこの電子健康データを利用することを可能にする。
  ➢電子健康記録、ゲノミクスデータ、患者登録など、さまざまな種類の電子健康データへのより良いアクセスを促進する。
- EHDSは、GDPR、医療機器に関するRegulation(EU)2017/745(医療機器規則)、体外診断用医療機器に関するRegulation(EU)2017/746(体外診断規則)、人工知能法案(Artificial Intelligence Act)、データガバナンス法案(Data Governance Act)、データ法案(Data Act)、ネットワークと情報システムのセキュリティに関する指令(NIS指令)DIRECTIVE(EU)2016/1148、CBHC指令(Directive2011/24/EU)といった法制度を基盤にしたものである。
  また、Regulation規則(EU)2018/1725(EUデータ保護規則)にも完全に準拠している。
- 欧州保健連合の文脈では、EHDSは、欧州保健緊急事態準備対応機関(HERA)、欧州のがん対策計画、EUがんミッション、及び欧州医薬品戦略の作業を支援する。
  また、EHDSの提案は、医療機器規則及び提案されたArtificail Intelligence Actを通じてソフトウェアに課せられた要件にも基づいている。
- この提案は、ヨーロッパをデジタル時代に適合させ、人々のために機能する将来を見据えた経済を構築するという委員会の優先事項と一致している。

データ関連文献 #9：主な調査項目

Proposal for a Regulation on the European Health Data Space

データ流通における信頼性のコンセプト・セキュリティ要件

50条安全な処理環境

- 健康データアクセス機関は、技術的及び組織的な対策、セキュリティ及び相互運用性の要件を備えた安全な処理環境を通じてのみ、電子健康データへのアクセスを提供するものとする。
- 特に、以下のセキュリティ対策を講じるものとする。
  (a)安全な処理環境へのアクセスを、それぞれのデータ許可に記載されている権限のある者に制限すること。
  (b) 安全な処理環境でホストされている電子健康データの不正読み取り、コピー、変更又は除去の危険を、最先端の技術的手段により最小限に抑えること。
  (c)電子健康データの入力及び安全な処理環境でホストされている電子健康データの検査、変更又は削除を、限られた数の許可された識別可能な個人に制限すること。
  (d) データ利用者が、個人及び固有のユーザーID及び機密アクセスモードのみを使用して、データ許可の対象となる電子健康データにのみアクセスできるようにすること。
  (e)安全な処理環境におけるすべての処理操作を検証及び監査するために、必要な期間、安全な処理環境へのアクセスの識別可能なログを保持すること。
  (f)潜在的な安全保障上の脅威を軽減するために、第50条を遵守を確保し、この条に規定する保安措置を監視すること。

技術的・制度的枠組

- EHDSは、GDPR、医療機器に関するRegulation(EU)2017/745(医療機器規則)、体外診断用医療機器に関するRegulation(EU)2017/746(体外診断規則)、データガバナンス法案(Data Governance Act)、データ法案(Data Act)、ネットワークと情報システムのセキュリティに関する指令(NIS指令)DIRECTIVE (EU)2016/1148、CBHC指令(Directive 2011/24/EU)といった法制度を基盤にしたものである。
- EHDSでアクセスされる電子データのかなりの量がEUの自然人に関する個人の健康データであることを考慮して、この提案はGDPRだけでなく、規則(EU)2018/1725(EUデータ保護規則)にも完全に準拠して設計されている。
- 欧州保健連合の文脈では、EHDSは、欧州保健緊急事態準備対応機関(HERA)、欧州のがん対策計画、EUがんミッション、及び欧州医薬品戦略の作業を支援する位置づけとなっている。
  EHDSは、革新的な医薬品やワクチン、医療機器や体外診断薬の開発を支援する法的及び技術的環境を構築する。
  これは、健康上の緊急事態を予防、検出、及び迅速に対応するのに役立つ。
- EHDSの提案は、医療機器規則及び提案されたArtificial Intelligence Actを通じてソフトウェアに課せられた要件にも基づいている。
  医療機器ソフトウェアはすでに医療機器規則の下で認定されている必要があり、AIベースの医療機器やその他のAIシステムもA技術I要件に準拠する必要がある。

データ関連文献 #10：概要

サイバーセキュリティ法(网络安全法)

1	概要	2017年に導入されたサイバーセキュリティ法では、ネットワーク運用セキュリティとネットワーク情報セキュリティの観点から、管理対象であるデータの管理要件が定められている。管理範囲は、個人情報及び重要情報インフラのデータの収集と保存に重点を置いている。

2	書誌的情報	名称	サイバーセキュリティ法		
		主旨	これは、サイバー空間の安全管理に関する問題を総合的に規制する中国初の基本法である。サイバー空間における法治の建設における重要な布石であり、インターネットを法に従って統治し、サイバーリスクを解決するための法的な重しであり、インターネットを法治の軌道に乗せて健全に運営するための重要な保証である。		
		文献タイプ	法令		
		国・地域	中国	適用分野	中国におけるサイバーセキュリティ分野の基本法
		策定者	2016年11月7日全国人民代表大会常務委員会発行、2017年6月1日より適用。	対象者	規制について：本法は、中華人民共和国の領域内におけるネットワークの構築、運用、保守及び使用、並びにネットワークセキュリティの監督及び管理に適用される。
		順守義務	インターネットを利用する個人及び組織は、これを遵守しなければならない。		
		普及状況	普及。《サイバーセキュリティ法》「サイバーセキュリティ啓発週間」などの活動により、この5年間でサイバーセキュリティに対する意識が徐々に人々の心に浸透してきた。		
		策定年	2016年11月7日採択、2017年6月1日発効	ページ数	7

データ関連文献 #10：概要

サイバーセキュリティ法(网络安全法)

3	データ流通における信頼性のコンセプト・セキュリティ要件	サイバーセキュリティ法では、中国のサイバーセキュリティの基本法として、重要情報インフラ保護システム、ネットワークセキュリティレベル保護システム、個人情報保護システム，ネットワーク情報コンテンツ管理システム、ネットワーク製品及びサービス管理システム、ネットワークセキュリティ事故緊急対応システムなど、サイバーセキュリティシステムの最も基本的な枠組みを定めている。
4	セキュリティ区分・水準・対策	国は、ネットワークセキュリティレベルの保護システムを導入している。ネットワーク事業者は、データの可用性と機密性を保護する手段として、重要なデータをバックアップし、暗号化することが求められている。
5	技術的・制度的枠組	中国のサイバーセキュリティの基本法として、重要情報インフラ保護システム、ネットワークセキュリティレベル保護システム、個人情報保護システム，ネットワーク情報コンテンツ管理システム、ネットワーク製品及びサービス管理システム、ネットワークセキュリティ事故緊急対応システムなど、サイバーセキュリティシステムの最も基本的な枠組みを定めている。
関連URL		http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm（中華人民共和国サイバーセキュリティ法） http://mk.36hjob.com/Mo/Article/Detail/QQKIC（サイバーセキュリティ法（草案）） http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm（国家インターネット情報弁公室とその他の部門は、中華人民共和国サイバーセキュリティに関する法律の改正に関する決定案を作成） https://mp.weixin.qq.com/s?__biz=MzI2MTMzMDY0Ng==&mid=2247484123&idx=3&sn=30b1662120b41a90a3556f156f02e0fa&chksm=ea5d4162dd2ac874aeb962b51faf1d5295cce3872c9ca4883087c0a3e6ae6c56349630d5e456&scene=27（サイバーセキュリティ法が成立）

データ関連文献 #10：主な調査項目

サイバーセキュリティ法(网络安全法)

狙い

- サイバーセキュリティ法第37条は、中国の国境を越えたデータフロー管理体制の形成における重要な根幹であり、重要かつ顕著な役割を担っている。
- サイバーセキュリティ法第37条は、中国における国境を越えたデータの流れを管理するためのトップレベルの体制を初めて確立し、個人情報や重要情報インフラの重要データが遵守すべき基本条件として、原則現地保存、業務上の必要性、真に必要なもの、セキュリティ評価という4つの条件を明記した。
- サイバーセキュリティ法は、中国における越境的データフローの管理構築において先駆的な役割を果たし、この分野における従来の法規範を統一し、その後の個人情報保護法やデータセキュリティ法が越境的データフローを包括的に規制するための強固な制度基盤を築いた。
- サイバーセキュリティ法第37条は、重要情報インフラにおける国境を越えたデータの流れを管理するための制度を定めている。
- その内容は、「重要情報インフラの運用者が、中華人民共和国内で業務上収集・生成した個人情報及び重要データは、領域内で保管すること」というもの。
- 業務上の必要から国外で提供する必要がある場合、国務院インターネット情報部門が国務院の関連部門と共同で策定した措置に基づき、法律又は行政法規に別途規定がある場合はその規定に基づき、セキュリティ評価を行うものとする。
- 第37条は、文字通りの意味から、規制対象が重要情報インフラ事業者が中国国内で業務上収集・生成する個人情報及び重要データであること、重要情報インフラ事業者が中国国内で業務上収集・生成する個人情報及び重要データは原則として中国国内に保管し、中国国外へのデータ提供は特例であること、越境条件の観点から、重要情報インフラ事業者が中国国内で業務上収集・生成する個人情報及び重要データの越境は「業務の必要性」「国外データ提供」という3要件を満たしていなければならないという意味を主に含む。
- 越境に関する条件として、重要情報インフラ事業者が中国国内で業務上収集・生成した個人情報及び重要データの越境は、「業務上の必要性」「中国国外への提供が必要」「セキュリティ評価のため」の3要素を満たす必要がある。
- したがって、現地保存の原則、ビジネス上の必要性、国外で提供する真の必要性、セキュリティ評価が、サイバーセキュリティ法第37条に基づく国境を越えたデータの流れを管理する体制の中核的要素を形成している。

データ関連文献 #10：主な調査項目

サイバーセキュリティ法(网络安全法)

概要

- サイバーセキュリティ法　重要な情報インフラの保護に重点を置いたネットワーク運用セキュリティの強化
- サイバーセキュリティ法第3章では、その3分の1近くを割いて、ネットワーク運用のセキュリティ規制、特に重要な情報インフラの運用セキュリティの保護に重点を置いている。
- 重要情報インフラとは、破損や障害、データ漏洩が発生した場合、国の安全や国民生活、公共の利益を著しく損なう可能性のあるシステムや施設のことである。
- ネットワークセキュリティは、ネットワーク運用のセキュリティが中心であり、重要な情報インフラのセキュリティは、国家安全保障や社会公共性に密接に関わる最重要事項である。
- このため、《サイバーセキュリティ法》は重要情報インフラの鍵保護をネットワークセキュリティ階層に基づいて実施することを重視し、重要情報インフラの運用者がより多くのセキュリティ保護義務を負うことを明確にし、国家安全保障審査や重要データのローカル保存義務などの法的措置と組み合わせて、重要情報インフラの運用セキュリティを確保する。

安全性の分類、水準と対策

- 活動分野：事業部門　国有企業　メディア　金融電子商取引　ゲーム SNS 等
- 国は、ネットワークセキュリティレベルの保護システムを導入している。
  この条文にあるネットワークセキュリティレベル保護システムは、公安部が長年運用してきた情報システムセキュリティレベル保護システムである。
  ネットワークセキュリティ法の導入により、平等保護の実施要件も強化され、これを怠ると犯罪となる。
  1.安全管理：ネットワーク事業者は、企業内のネットワーク・セキュリティに対する責任を明確にし、健全な規則と運用手順によって、ネットワーク・セキュリティのための制度的な保護措置を提供する必要がある。
  2.技術的側面：ネットワーク事業者は、サイバー攻撃に対処し、サイバーセキュリティのリスクを低減するために、事前の予防、事後の対応、事後のフォローアップなど様々な技術的手段を採用する必要がある。なお、ウェブログの保存期間は6ヶ月以上と規定されている。
  3.データセキュリティ面：ネットワーク事業者は、データの可用性と機密性を保護する方法として、重要なデータをバックアップし、暗号化する必要がある。

データ関連文献 #11：概要

データセキュリティ法(数据安全法)

1	概要	データセキュリティ法では、データ管理者と運用者のデータ保護責任を明確にし、データ保護の作業方向を規定。情報セキュリティ業界全体にプラスの影響をもたらし、データ管理者と運用者のデータセキュリティ構築における盲点を全面的に排除する。データセキュリティの構築が法律に基づき、データセキュリティ事故による損失が法律で罰せられることができ、経済社会の情報化の健全な発展を促進し、国民と組織の合法的権益を保護するのに大きな価値を持つものである。

2	書誌的情報	名称	データセキュリティ法		
		主旨	同法は、国家安全保障全体構想の立法目的を反映し、データセキュリティ分野の未解決問題に焦点を当て、データ管理の分類と等級を定め、データセキュリティのリスク評価、監視と早期警戒、緊急対応、データセキュリティ審査などの基本システムを確立し、関連主体のデータセキュリティ保護義務を明確化した、中国初のデータセキュリティ分野の基本立法である。		
		文献タイプ	法令		
		国・地域	中国	適用分野	本法は、中華人民共和国の領域内における情報処理活動の実施及びその安全監督に適用されるものとする。
		策定者	2021年6月10日、中華人民共和国第13期全国人民代表大会常務委員会第29回総会で採択された。	対象者	データ処理活動を行うすべての事業者は、特定の種類の対象者に限定されず、サイバーセキュリティ法の対象となるネットワーク事業者(ネットワーク所有者、管理者、サービス提供者)よりも広い範囲に及ぶ。データ処理活動には、データの収集、収集、保管、使用、処理、伝送、提供及び開示が含まれる。 データを処理する可能性のあるすべての政府、企業、組織は、データセキュリティ法の適用範囲に含まれる。
		順守義務	重要データの取扱者は遵守する義務を負う。		
		普及状況	社会啓発活動の実施		
		策定年	2021年6月10日、第13期全国人民代表大会常務委員会第29回会議で「データセキュリティ法」を採択。2021年9月1日から施行。	ページ数	4

データセキュリティ法(数据安全法)

3	データ流通における信頼性のコンセプト・セキュリティ要件	中華人民共和国 データセキュリティ法第11条では、国境を越えたデータの流れは安全と自由の原則に従うべきであると定め、第25条、第26条、第31条、第36条、第46条では、国境を越えたデータの流れに関する規則をさらに改善している。
4	セキュリティ区分・水準・対策	データセキュリティ法でのデータの分類と等級付けは、規制当局の視点に立ち、データの種類によって異なる規制措置や法的要件を課す、すなわち「国がデータの分類と等級付けのシステムを確立する」ものである。
5	技術的・制度的枠組	データセキュリティ法では詳細な制度的・技術的要件を定めておらず、その実施については国や業界の標準に依存している。データセキュリティ保護の枠組みは、これまで発表されたさまざまな国家規格や業界規格を総合的に分析して導き出されたものである。
関連URL		http://www.gov.cn/xinwen/2021-06/11/content_5616919.htm（データセキュリティ法） https://nic.wxc.edu.cn/2020/1022/c5362a130021/page.htm（中華人民共和国データセキュリティ法(草案)） http://www.npc.gov.cn/npc/c30834/202106/7b4f64b447ac49a9841853de113c118d.shtm 中華人民共和国データセキュリティ法の改正（第三次審査案） http://www.npc.gov.cn/npc/c30834/202106/a2292e20dfa743febe23b01fa6aa330b.shtmlデータセキュリティ法の改正（第二次審査案） http://www.cac.gov.cn/2023-01/14/c_1675346873856103.htm（産業情報化部など16部門によるデータセキュリティ産業の発展促進に関するガイダンス）

データセキュリティ法(数据安全法)

狙い

- データセキュリティ法は、個人情報データの収集、保存、使用、提供の一連の流れ及びプロセスを規制している。
- データ要素市場は活況を呈しており、データセキュリティの管理体制の構築は、セキュリティと開発との関係を調整する必要がある。
- 一方では、データセキュリティの主体責任に対する認識を強化し、データ流通・取引関連主体のデータセキュリティ能力を標準化し、データセキュリティ関連主体のセキュリティに対する主体責任を厳格に規定し、データの収集・集約、加工、流通・取引、各リンクの共有・利用において、参加主体が法律に基づいて相応の責任を負担しなければならない。
- 「参入緩やか、管理厳格」の原則を堅持し、標準化された市場セキュリティ監督と秩序規制を基礎に、データ共有と開放を推進し、データ流通効率の向上を図り、データ供給、流通、応用の全過程の統合セキュリティ保護を強化し、確認できるデータソース、定義できる使用範囲、追跡できる流通過程を構築し、秩序ある発展のためのデータ取引市場システムを構築しなければならない。

概要

- データセキュリティ法第2条は、本法が中華人民共和国の領域内の情報処理活動及びその安全監督に適用されることを規定している。
- データ安全法は、中国国内で行われるデータ処理活動に明確に適用されるだけでなく、データ安全法に必要な域外適用も与えている。
- つまり、中華人民共和国外で行われ、国家安全、公共の利益又は中華人民共和国の国民、若しくは組織の合法的権益を害するデータ処理活動に対しても、中国は法に従って法的責任を追及することになる。
- データセキュリティ法に必要な域外適用を与えることは、データ競争の文脈で国内法を通じてデータセキュリティの管轄権を拡大する現在の国際的傾向に合致し、国際データ競争におけるデータ活動に対する中国の管理と言論を強化することに資するものである。

安全性の分類、水準と対策

- 国家データ分類及び保護システム
- データセキュリティ法第21条は、「国は、データの分類及び等級別保護制度を確立し、経済及び社会の発展におけるデータの重要性並びにデータが改ざん、破壊、漏えい又は不正アクセス若しくは不正使用された場合に国家の安全、公共の利益又は個人及び組織の正当な権利及び利益に及ぼす被害の程度に応じてデータの分類及び等級別保護を実施する」と定めている。国家データ安全調整機構は関連部門を調整し、重要データカタログを作成し、重要データの保護を強化する。
- データセキュリティ法では、特に、国の安全、国民経済の生命線、国民の生活、重要な公益に関わるデータは、国家基幹データとして分類され、より厳格な管理体制のもとで取り扱われることになる。
- データセキュリティ法のデータ分類と等級付けは、データの保護と活用のバランスを決定する重要な基礎として国家レベルで提案されており、政府データ、企業データ、産業データ、個人データの保護のための法的基盤を構築している。

個人情報保護法(个人信息保护法)

1	概要		個人情報保護法の公布により、国境を越えた個人情報の流れについて、各業界の立法要件から法的枠組み・制度の確立まで、より包括的かつ体系的に規制され、国境を越えたデータの流れの評価方法、規制手段についても欧州連合と遜色ないものとなった。 データセキュリティ法とサイバーセキュリティ法は全体の枠組みの一貫性を保っている。		
2	書誌的情報	名称	中華人民共和国個人情報保護法		
		主旨	個人情報の権利保護、処理者の開示制限、違法な侵害や公共の利益の侵害の禁止、国家安全保障の確保を価値観として、個人情報の権利と利益を保護し、個人情報の処理を規制し、個人情報の合理的な利用を促進するもの。		
		文献タイプ	法令		
		国・地域	中国	適用分野	個人情報の権益を保護し、個人情報取扱行為を規制し、法律に従って個人情報の秩序と自由な流れを保護し、個人情報の合理的な利用を促進するために制定された法律である。
		策定者	第十三期全国人民代表大会常務委員会第十三回会議で採決された中華人民共和国個人情報保護法	対象者	内：本法は、中華人民共和国の領域内における組織及び個人の自然人の個人情報の取り扱いに関する活動に適用される。 外：本法は、中華人民共和国外において、以下のいずれかの状況下で中華人民共和国内の自然人の個人情報を取り扱う活動にも適用される。 領域内の自然人に対する製品又はサービスの提供を目的とするもの 領域内の自然人の行動の分析及び評価
		順守義務	第9条と第27条の規定によって、データ処理業者であれ、個人データの処理者であれ、必要なデータセキュリティ保護措置を履行することが法的義務となっている。		
		普及状況	普及率　50%以上		
		策定年	2021年8月20日の第13期全国人民代表大会常務委員会第30回会議で議決され、2021年11月1日に施行される。	ページ数	7

個人情報保護法(个人信息保护法)

3	データ流通における信頼性のコンセプト・セキュリティ要件	重要情報インフラ事業者、及び国家インターネット情報機構の定める量まで個人情報を取り扱う個人情報処理事業者は、中華人民共和国の領域内で収集及び発生した個人情報を領域内で保存しなければならない。個人情報処理業者は、中華人民共和国の管轄当局の許可なく、中華人民共和国の領域内に保管されている個人情報を外国の司法機関又は法執行機関に提供してはならないものとする。
4	セキュリティ区分・水準・対策	個人情報の処理者は、その個人情報の処理行為について責任を負い、処理された個人情報の安全性を確保するために必要な措置を講じなければならないものとする。
5	技術的・制度的枠組	其中GB/T 35273：2017 情報セキュリティ技術：個人情報保護方針
関連URL		http://www.gov.cn/xinwen/2021-08/20/content_5632486.htm（個人情報保護法） http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml《中華人民共和国個人情報保護法(草案)》 https://www.66law.cn/laws/1663924.aspx（個人情報保護法（第二次審査案）に対する意見募集について） http://www.xzcca.gov.cn/gzdt_74/dtyw/202010/t20201023_179947.html（個人情報保護法(草案)と解説書）

データ関連文献 #12：主な調査項目

個人情報保護法(个人信息保护法)

狙い

- 個人情報保護法は、個人情報の権利保護と安全性という客観的な要件を満たし、国際貿易や経済取引における実際のニーズに対応するため、個人情報の国境を越えた流れについて明確かつ体系的なルールを定めている。
- まず、本法は、中国国内の自然人に対する製品・サービスの提供、中国国内の自然人の行動の分析・評価等を目的として中国国外の自然人の個人情報を取り扱う活動に適用されることが明らかであり、上記の状況に該当する海外の個人情報取扱事業者は、中国国内に専門機関の設置や個人情報保護に関する事項を担当する代表者を指定することが求められている。
- 第二に、中国が締結又は加入した国際条約・協定に基づき、国のインターネット情報部門が組織する安全性評価、専門機関の認定、標準契約の締結などを通じて、個人情報を海外に提供する方法を明確にすることである。
- 第三に、個人データの処理者に対し、国外における受領者の処理活動が本法に定める保護基準を満たすよう、必要な措置を講じることを求めている。
- 第四に、国境を越えて個人情報を提供する際の「通知と同意」についての要件を厳格化し、個人の情報提供の権利と意思決定の権利を効果的に保護する。
- 第五に、国家の主権、安全及び発展の利益を保護するために、個人情報の国境を越えた提供の安全性評価、国外の司法又は法執行機関への個人情報の提供、個人情報の国境を越えた提供を制限する措置、外国による差別的措置に対する対策について規定している。

安全性の分類、水準と対策

- 個人情報を取り扱う者は、個人情報保護に関する第一の責任者である。したがって、個人情報保護法では、個人情報の処理者は、その個人情報の処理行為について責任を負い、処理する個人情報の安全性を保護するために必要な措置を講じなければならないことが強調されている。

- 個人情報保護法では、コンプライアンス管理及び個人情報の安全保護に関する個人情報取扱事業者の義務を明確にするため、特別章を設け、個人情報取扱事業者に対して、規定に基づく内部管理体制及び業務手順の策定、適切な安全・技術措置、個人情報取扱事業者の監督責任者の指名、個人情報取扱事業者のコンプライアンス監査の定期実施、敏感な個人情報の取扱い、自動意思決定のための個人利用、個人情報の提供・開示などリスクの高い取扱事業者の事前影響評価、個人情報漏洩の届出義務・救済などの義務履行を義務づけている。

データ関連文献 #13：概要

GB/T 22240-2020 情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド

(信息安全技术 网络安全等级保护定级指南)

1	概要		-		
2	書誌的情報	名称	GB/T 22240-2020 ネットワークセキュリティレベル保護分類ガイド		
		主旨	ネットワーク事業者が国家機密を含まない対象物の分類を実施するための根拠となる、分類プロセスが明確化された。		
		文献タイプ	ガイドライン		
		国・地域	中国	適用分野	国家機密を伴わないものについては、採点方法と採点プロセスが定められている。
		策定者	国家市場監督管理局、国家標準化委員会	対象者	本書は、新聞業界の統合メディア/ホールメディアシステム、ニュース収集・編集・配信システム、クラウドコンピューティングプラットフォーム、ビッグデータプラットフォームなどの非国家機密関連クラス保護対象物の分類を指導するのに適している。
		順守義務	これには、企業、機関、代理店などの法人、及び法人格を持たない社会団体などの組織が含まれるが、これらに限定されるものではなく、遵守する必要がある。		
		普及状況	-		
		策定年	2020年4月28日、国家市場監督管理局と国家標準化管理局がGB/T 22240-2020情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイドを発表。2020年11月1日に正式実施される予定。	ページ数	13
3	データ流通における信頼性のコンセプト・セキュリティ要件		-		

GB/T 22240-2020 情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド

(信息安全技术 网络安全等级保护定级指南)

4	セキュリティ区分・水準・対策	情報セキュリティ技術ネットワークセキュリティレベル保護実施ガイドでは、国家ネットワークセキュリティレベル保護管理規範と技術標準に基づき、そのレベル保護対象のセキュリティ保護レベルを決定する責任があり、主管部門がある場合、その主管部門に報告し、審査と承認を受ける必要がある。決定したセキュリティ保護レベルに応じて、公安当局に申請手続きを行う。 国家ネットワークセキュリティレベル保護管理規範と技術標準に従い、レベル保護対象のセキュリティ保護の計画及び設計を実施する。
5	技術的・制度的枠組	ネットワークセキュリティレベルの保護システム、重要情報インフラのセキュリティ保護システムに関する要求事項が設定されている。 この保護は、レベル3以上の重要な情報インフラとネットワークに重点を置いている。
関連URL		https://www.sohu.com/a/395098338_653604（情報セキュリティ技術 ネットワークセキュリティレベルの保護分類ガイド） http://credit.shaanxi.gov.cn/316/10231627.html（中華人民共和国個人情報保護法（草案）） https://www.ciobok.com/3384.html（情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド」は推奨基準である） https://www.wangan.com/docs/4319（セキュリティ保護レベル） https://m.thepaper.cn/baijiahao_15295531（GB/T 25058-2019 情報セキュリティ技術 ネットワークセキュリティレベル保護実装ガイド）

GB/T 22240-2020 情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイド

(信息安全技术 网络安全等级保护定级指南)

概要

- ネットワークセキュリティレベルの保護は、国家ネットワークセキュリティ保護の基本システム、基本戦略、基本方法である。
- 中華人民共和国ネットワークセキュリティ法第21条は、ネットワーク運営者はネットワークセキュリティレベル保護システムの要求に従い、関連するセキュリティ保護義務を履行しなければならないと規定している。
  階層型保護システムの所定の5つの基本動作を実行するための第一歩として、情報システムをどのように等級付けするかを理解することが重要である。
- 2020年4月28日、国家市場監督管理局と国家標準委員会はGB/T 22240-2020情報セキュリティ技術 ネットワークセキュリティレベル保護分類ガイドを発行し、国家機密を含まない対象物の等級付け方法と等級付けプロセスを規定。その後のセキュリティ構築と是正、等級付け評価のための良好な基礎を築いた。

安全性の分類、水準と対策

採点対象

- ネットワークセキュリティの分類対象は、主に情報システム(OAシステム、クラウドコンピューティング基盤・システム、Internet of Things、産業制御システム、モバイル相互接続技術を用いたシステムなど)、通信ネットワーク設備(主に電気通信ネットワーク、ラジオ・テレビ送信ネットワーク、産業・単位などのプライベート通信ネットワークなど)、データリソースなどである。
- 協調：データリソースは、独立した分類対象として作ることができる。
  セキュリティ責任の主体が同じ場合、ビッグデータとビッグデータプラットフォーム/システムは、全体として等級付けすることが適切であり、セキュリティ責任の主体が異なる場合、ビッグデータは独立して等級付けされるべきである。
  ビッグデータプラットフォーム/システムは、大量の市民の個人情報を含み、市民に公共サービスを提供しており、原則としてそのセキュリティ保護レベルは3段階以上である。
  例えば、データは複数のプラットフォームで分散し、それぞれのプラットフォームは独立した責任者を持ち、以下のような場合は、管理・使用という、セキュリティ責任の主体が異なる状況であり、データリソースは、集中データ処理プラットフォームを別の分類対象として扱う必要がある。

採点要素

- セキュリティ保護レベルの定義によれば、「保護対象が国家安全保障、経済建設、社会生活において重要であり、かつ、ひとたび損傷、機能喪失、データの改ざん、漏えい、紛失、破壊等が発生すれば、国家安全保障、社会秩序、公共の利益、国民・法人・その他の組織の正当な権利・利益を侵害する程度」を考慮して分類する必要がある。
  そこで、本規格では、保護対象の等級付けのための要素として、「侵害される対象」と「その対象に対する侵害の程度」の2つを規定している。
- 分類の対象が損なわれたときに侵害される対象には、国家の安全、社会秩序、公共の利益、市民、法人、その他の組織の正当な権利と利益が含まれる。
- 対象物の侵害の程度を、一般的な侵害、重大な侵害、特に重大な侵害の3段階に分けている。

データ域外移転安全評価弁法(数据出境安全评估办法)

1	概要		データ越境活動を規制し、個人情報の権益を保護し、国家の安全及び社会公共の利益を守り、国境を越えたデータの安全かつ自由な流れを促進するため、「中華人民共和国サイバーセキュリティ法」「中華人民共和国データセキュリティ法」「中華人民共和国個人情報保護法」などの法律・法規に従って策定された措置である。		
2	書誌的情報	名称	データ域外移転安全評価弁法		
		主旨	データ越境セキュリティ評価の目的は、データ越境のセキュリティリスクの防止に基づき、秩序ある合法的な方法でデータの自由な流通を確保すること。		
		文献タイプ	政策		
		国・地域	中国	適用分野	データ越境セキュリティ評価書が適用される状況を説明する。
		策定者	国家インターネット情報室	対象者	本措置は、データ処理者が中華人民共和国において業務上収集・生成した重要データ及び個人情報を外国に提供する際の安全性評価に適用される。
		順守義務	中華人民共和国において業務上収集・生成された重要なデータ及び個人情報を外国に提供するデータ処理業者のセキュリティ評価は、本措置の対象となる。		
		普及状況	-		
		策定年	2022年5月19日、国家インターネット情報室2022年第10回会議で採択、公布され、2022年9月1日から施行されるものとする。	ページ数	4

データ域外移転安全評価弁法(数据出境安全评估办法)

3	データ流通における信頼性のコンセプト・セキュリティ要件	データ処理者の基本情報、データ越境に関わる業務及び情報システム、越境されるデータ、データ処理者のデータセキュリティ及び保護能力、国外の受信者の状況、データセキュリティ保護の責任と義務について同意した法律文書など、越境活動の全体的な状況。
4	セキュリティ区分・水準・対策	データ処理業者は、海外の受領者と締結した法的文書において、データセキュリティ保護の責任と義務について明確に同意し、データ越境セキュリティ評価の有効期間中に出国するデータのセキュリティに影響を与える状況が発生した場合、評価を再宣言する必要がある。
5	技術的・制度的枠組	本措置の適用範囲により、重要データ及び特定の越境条件を満たす個人情報は、データ越境セキュリティ評価の対象となるため、セキュリティ評価が適用される個人情報取扱業者のデータ越境状況は、セキュリティ評価を申告する必要がある。 本措置の適用範囲外の個人情報取扱業者は、個人情報保護認証又は国家サイバー情報部門が策定する標準契約の締結により、個人情報の越境提供の条件を満たすことが可能である。
関連URL		http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm（データ越境のセキュリティ評価手法） https://baijiahao.baidu.com/s?id=1688564674361052770&wfr=spider&for=pc（サイバーセキュリティ規格） https://view.inews.qq.com/k/20211108A0BRS000?web_channel=wap&openApp=false（データ越境のセキュリティ評価手法(意見募集稿)） http://www.lifanglaw.com/plus/view.php?aid=1668《データ越境セキュリティ評価ガイド(草案）》 http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm《データ越境のセキュリティ評価手法(意見募集稿)》

データ関連文献 #14：主な調査項目

データ域外移転安全評価弁法(数据出境安全评估办法)

狙い

- 国家インターネット情報室は、2022年9月1日から施行される「データ域外移転安全評価弁法」(以下、「弁法」)を発表した。
- 国家インターネット情報室の担当者は、本措置の導入は、サイバーセキュリティ法、データセキュリティ法、個人情報保護法の規定を実施し、データ越境活動を規制し、個人情報の権益を保護し、国家の安全と社会公共利益を守り、国境を越えたデータの安全かつ自由な流れを促進し、安全とともに発展を確保し、発展とともに安全を推進することを目的としていると述べた。
- データ越境安全評価に関する具体的な規定を明確にすることは、デジタル経済の健全な発展を促進し、データ越境安全リスクを防止・解決し、国家安全保障と社会公共の利益を保護し、個人情報の権益を保護するために必要なことである。
- 本方針は、データ越境安全評価の範囲、条件及び手順を規定し、データ越境安全評価の作業に関する具体的なガイドラインを提供するものである。

概要

- 本弁法は、中華人民共和国において業務上収集・生成された重要データ及び個人情報を外国に提供するデータ処理業者のセキュリティ評価が本弁法の適用を受けることを明確にしている。
- データ越境のセキュリティ評価は、事前評価と継続的な監督を組み合わせ、リスク自己評価とセキュリティ評価を組み合わせるという原則に従うことを提案する。

安全性の分類、レベル及び対策

- 同措置は、データ越境セキュリティ評価の具体的な要求事項を定めており、データ処理者はデータ越境セキュリティ評価を宣言する前にデータ越境リスクの自己評価を行うべきであると規定し、主要な評価項目を明記している。
- データ処理業者は、海外の受領者と締結した法的文書において、データセキュリティ保護の責任と義務について明確に合意し、データ越境セキュリティ評価の有効期間中に出国するデータのセキュリティに影響を与える状況が生じた場合には、評価を再宣言することが規定されている。
- さらに、データ越境のセキュリティ評価手順、監督管理体制、法的責任、コンプライアンス是正の要件も明確化されている。
- この措置の第14条では、セキュリティ評価結果の有効期限を2年間と定めており、制度上も比較的有利な設定となっている。
- これは、データ処理者が2年以内に特定の海外受信者のデータ越境移転を申告できることを意味し、企業が継続的にデータ越境ビジネスを行い、グローバルデジタル経済の発展を促進することを大いに促進するものである。

データ関連文献 #15：概要

データ越境安全評価申告ガイドライン(第1版)(数据出境安全评估申报指南(第一版))

1	概要	申告のガイドラインは、「適用範囲」「申告方法・プロセス」「申告資料」の3つの具体的な項目について、評価指標の関連要求事項を説明・拡張したものである。	

2	書誌的情報	名称	データ越境安全評価申告ガイドライン(第1版)		
		主旨	国家インターネット情報室は、データ処理者がデータ越境セキュリティ評価を標準的かつ秩序立てて申告することを指導、支援するため、「データ越境安全評価申告ガイドライン(第1版)」を作成し、データ越境セキュリティ評価の申告方法、申告プロセス、申告資料に関する具体的な要求事項を説明した。		
		文献タイプ	ガイドライン		
		国・地域	中国	適用分野	(1) データ処理者が領域内の業務の過程で収集し生成したデータを領域外に転送し、保存すること。 (2) データ処理者が収集し生成したデータは領域内に保存され、領域外の機関、組織又は個人が照会、検索、ダウンロード又はエクスポートすることができる。 (3) その他、国家インターネット情報局の定めるデータ越境行為。
		策定者	国家インターネット情報室	対象者	データ処理者が業務上データを国外に提供する必要があり、データ越境セキュリティ評価に適用される状況を満たす場合、データ処理者はデータ越境セキュリティ評価措置の規定に従って、報告ガイドラインに従って申告する必要がある。
		順守義務	データ処理業者、対象者		
		普及状況	-		
		策定年	2022年8月31日夜、「データ越境安全評価申告ガイドライン(第1版)」を発行	ページ数	17

データ越境安全評価申告ガイドライン(第1版)(数据出境安全评估申报指南(第一版))

3	データ流通における信頼性のコンセプト・セキュリティ要件	企業が海外で提供しようとするデータに、他の特別な法律又は部門別規則によって明示的に領域内に保存することが要求されているデータが含まれる場合、そのデータは関連する要件に従って領域内に保存されなければならず、法律や規則で別途規定されていない限り、海外で提供してはならない。
4	セキュリティ区分・水準・対策	ガイドラインの第1条は、適用されるデータ越境セキュリティ評価の範囲について、評価措置の第2条（第4条と合わせて）を再確認するものである。 その中で、送信データに重要なデータが含まれる場合には、セキュリティ評価が必須であること、送信データに個人情報が含まれる場合には、セキュリティ評価が一定の前提条件を満たす必要があることを明確にしている。
5	技術的・制度的枠組	-
関連URL		http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm（データ越境セキュリティ評価宣言に関するガイダンス（第1版）） http://www.iprdaily.cn/news_32309.html（解説） https://jg-static.eeo.com.cn/article/info?id=521f049cebc34ab8ab0d9e4904e96d2a（国家インターネット情報局作成） https://mp.weixin.qq.com/s?__biz=MzI0NjA5MDM4Mw==&mid=2648797035&idx=1&sn=a0aeb13197942a9bd05d0949ed8923ff&chksm=f151508bc626d99d52d5f1316a794bf01d4c0612dda8ea0a5e9bc57b484d60a3bc43bbc54563&scene=27（国家インターネット情報局、ガイドラインを発行） https://www.waitang.com/report/303347.html（GB 情報セキュリティ技術 データ越境セキュリティ評価ガイド（草案））

データ越境安全評価申告ガイドライン(第1版)(数据出境安全评估申报指南(第一版))

概要

- 今回の申告ガイドラインは、「データの越境移転」の定義を明確にしたものである。
- 申告ガイドラインによれば、「データの越境」には、「データ処理者が領域内の業務の過程で収集・生成したデータを外国に移転・保管すること」だけでなく、「データ処理者が収集・生成したデータを外国に移転・保管すること」も含まれる。
- また、データ処理者が収集し生成したデータが領域内に保存され、領域外の機関、組織又は個人がアクセス、検索、ダウンロード又はエクスポートできる状況も含まれる。
- つまり、「データの越境」は、実務上よくある国外のサーバーにデータが保存されている状況だけを対象とするのではなく、国内の業務過程で収集・生成されたデータが、「アクセス、検索、ダウンロード、エクスポート」によって「国外の機関、組織、個人」がアクセスすることができるようになったのである。
- 国内の業務で収集・生成されたデータは、「国外の機関、組織、個人」が「検索、取得、ダウンロード、輸出」の手段でアクセス又は処理することができ、これも「データの輸出」とみなされる。

安全性の分類、レベル及び対策

- データ処理者が業務上データを国外に提供する必要があり、データ越境セキュリティ評価に適用される状況を満たす場合、データ処理者はデータ越境セキュリティ評価措置の規定、申告ガイドラインに申告する必要がある。
- データ処理業者が中国国外でデータを提供する場合、以下の状況に該当する場合は、所在地の省インターネット情報局を通じて国家インターネット情報局にデータ越境セキュリティ評価を申告しなければならない。

（一）重要なデータを国外で提供するデータ処理業者。
（二）100万人以上の個人情報を取り扱う重要情報インフラ事業者及び情報処理事業者による個人情報の国外への提供。
（三）前年1月1日以降に累計で10万人分の個人情報又は1万人分の機微な個人情報を提供したデータ処理者による国外での個人情報の提供。
（四）その他、国家インターネット情報室が指定した、データ越境のセキュリティ評価の申告を必要とする状況。

個人情報越境取扱活動安全認証規範(个人信息跨境处理活动安全认证规范)

1	概要		個人情報の安全な認証のための実施基準(個人情報の安全な認証のための実施規範 越境処理活動)(以下、認証コード)の導入と実施は、越境データ分野における立法と規制の加速を反映している。		
2	書誌的情報	名称	個人情報越境取扱活動安全認証規範		
		主旨	個人情報取扱事業者が行う個人情報の越境処理行為について、認証機関が認証を行うための根拠を提供し、個人情報取扱事業者が個人情報の越境処理行為を規制するための参考とするため。		
		文献タイプ	ガイドライン		
		国・地域	中国	適用分野	個人情報保護認証の実施
		策定者	情報セキュリティ標準化国内技術委員会事務局	対象者	国境を越えた個人情報取扱活動において、認証機関が個人情報保護を認証する際の基準となり、また、個人情報取扱事業者が国境を越えた個人情報取扱活動を規制する際の参考となるもの。
		順守義務	個人情報の処理活動に携わる組織又は個人は遵守する義務を負う。		
		普及状況	-		
		策定年	2022年12月16日、国家情報安全標準化技術委員会は、「サイバーセキュリティ標準に関する実施要領-個人情報の越境処理活動に関するセキュリティ認証仕様 V2.0」の正式版を公開した。	ページ数	14
3	データ流通における信頼性のコンセプト・セキュリティ要件		-		

個人情報越境取扱活動安全認証規範(个人信息跨境处理活动安全认证规范)

4	セキュリティ区分・水準・対策	-
5	技術的・制度的枠組	認証仕様書の「概要」には、「個人情報保護認証を申請する個人情報処理者は、GB/T 35273「情報セキュリティ技術個人情報セキュリティ仕様」の要求事項を遵守しなければならず、国境を越えた処理活動を行う個人情報処理者は、本実施ガイドラインの要求事項をも遵守しなければならない」と明記されている。
関連URL		https://www.tc260.org.cn/front/postDetail.html?id=20221216161852（サイバーセキュリティ標準実施要領 - 個人情報の安全な認証のための仕様書 国境を越えた処理活動 V2.0） http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm（個人情報保護認証実施規程） https://www.cap.edu.cn/wlaq/info/1003/1461.htm（個人情報の越境処理活動に関する安全性認証仕様書 V2.0 (意見募集稿)） https://mp.weixin.qq.com/s?__biz=MzI5Nzc5MTI3MQ==&mid=2247519735&idx=1&sn=22373ede12c936d2ccfdd184eaa1e31d&chksm=ecad77bfdbdafea97ca8932cc0d60bede5c1ac0e61c0003bd4f6fc72319100d8acc115bf4fde&scene=27（個人情報の安全な認証に関する仕様書 国境を処理活動編 V2.0）

データ関連文献 #16：主な調査項目

個人情報越境取扱活動安全認証規範(个人信息跨境处理活动安全认证规范)

概要

- 個人情報越境処理活動安全認証仕様：越境処理活動を行う個人情報処理者は、GB/T 35273「情報セキュリティ技術個人情報安全仕様」及び本書の要求事項に基づき、個人情報保護認証を申請することが明記されている。
- 基本原則、国境を越えた個人情報処理活動における個人情報処理者及び海外受取人の個人情報保護、個人情報主体の権利利益の保護、認証機関が国境を越えた個人情報処理活動の認証を実施するための基礎、個人情報処理者が国境を越えた個人情報処理活動を規制するための参考事項が含まれている。

データ関連文献 #17：概要

個人情報越境標準契約規定(意見募集稿)(个人信息出境标准合同规定(征求意见稿))

1	概要		個人情報の越境活動を規制し、個人情報の権益を保護し、国境を越えた個人情報の安全かつ自由な流通を促進するため、国家インターネット情報局はこのほど「個人情報の出国に関する標準契約条項(意見募集稿)」(以下「意見募集稿」という)を策定した。		
2	書誌的情報	名称	個人情報越境標準契約規定(意見募集稿)		
		主旨	今回の協議案では、個人保護法上の標準契約、データ越境評価方法に言及されたデータ越境契約の内容、利用シーン、情報出口における個人情報保護影響評価の主要要素をさらに精緻化し、データ越境を実際に実施する際のルールを定めている。		
		文献タイプ	ガイドライン		
		国・地域	中国	適用分野	個人データの国外提供
		策定者	国家インターネット情報室	対象者	個人情報取扱事業者、標準契約が適用される場合
		順守義務	個人情報の取り扱い者は遵守する義務を負う。		
		普及状況	-		
		策定年	2022年6月30日、国家インターネット情報局は「個人情報の越境に関する標準契約規定(意見募集稿)」を発表した。	ページ数	19
3	データ流通における信頼性のコンセプト・セキュリティ要件		データ越境セキュリティ評価対策(意見募集稿)」(2021年10月29日OGCIO公表)の第6条によると、セキュリティ評価の申告には、海外の受信者との契約案を提示することが求められている。		

個人情報越境標準契約規定(意見募集稿)(个人信息出境标准合同规定(征求意见稿))

4	セキュリティ区分・水準・対策	標準契約条項の第4条(評価措置の第4条と合わせて読む)によれば、処理者から外国への個人情報の移転で、セキュリティ評価の「基準値」を満たさないものは、標準契約条項に従って処理することができる。 つまり、「大量・高リスク」の個人情報の出国にはセキュリティ評価が必要であり、「少量・低リスク」の個人情報の出国には標準的な契約を選択することができる。 個人情報の処理者は、以下の状況も満たす場合、標準的な契約を締結することにより、個人情報を国外で提供することができる。
5	技術的・制度的枠組	データが国外に出る前に個人情報保護影響評価を実施する
関連URL		http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm（個人情報の越境に関する標準的な契約条項(意見募集稿)） http://www.ipforefront.com/m_article_show.asp?id=2166（個人情報の越境に関する標準的な契約条項（試案）についての簡単な解説） http://www.hackdig.com/07/hack-710544.htm（要点解説）

個人情報越境標準契約規定(意見募集稿)(个人信息出境标准合同规定(征求意见稿))

概要

- 2022年6月30日、国家インターネット情報室は「個人情報越境標準契約規定(意見募集稿)」（以下「規定」）を正式に発表し、附属の「個人情報越境標準契約」（以下「標準契約」）を発表した。
- 先に公開された「データ域外移転安全評価弁法(意見募集稿) 」、「サイバーセキュリティ基準に関する実施要領-個人情報の越境処理活動に関する安全性認定仕様」と合わせて、個人情報保護法で規定されている3つの個人情報の越境条件について、比較的明確な実施要領が定められている。
- 個人情報越境安全評価の厳しい適用条件や高い閾値に比べ、個人情報出口標準契約の重要性は、より幅広いビジネスシーンに適用することができる。
- 同規則は13条で構成され、個人情報の輸出に関する標準契約書の適用範囲、適用条件、手続き、主な内容を明確にしている。
- 今後、標準契約書が正式に作成されれば、個人情報保護法における個人情報の国際的な流通に関する企業の義務を履行するための重要なツールとなることが予想される。

安全性の分類、レベル及び対策

- 個人情報の処理者は、以下の状況も満たす場合、標準的な契約を締結することにより、個人情報を国外で提供することができる。
  1.標準契約書が適用されうる状況。
  （一）非重要情報インフラ事業者。
  （二）100万人未満の個人情報を取り扱うもの。
  （三）前年の1月1日からの国外への個人情報の提供の累計が10万人に達しない場合。
  （四）機微な個人情報の国外への提供の累計が、前年の1月1日以降、1万人に達していない場合。
  標準契約は、これら4つの条件がすべて満たされた場合にのみ適用される。

THE PERSONAL DATA PROTECTION BILL, 2019

1	概要	プライバシーの権利は基本的権利であり、情報的プライバシーの本質的側面として個人情報を保護することが必要である。デジタル経済の成長により、個人間の重要なコミュニケーション手段としてのデータの利用が拡大している。個人の情報的プライバシーを尊重し、デジタルガバナンスを通じて、進歩、革新を確保し、自由で公正なデジタル経済を育む集団文化を創造することが必要である。この法令は「個人情報に関する個人のプライバシー保護」等、個人データの保護について規定している。

2	書誌的情報	名称	THE PERSONAL DATA PROTECTION BILL, 2019		
		主旨	この法令は、「個人情報に関する個人のプライバシー保護」、「個人情報の流れと利用方法の特定」、「個人情報を処理する個人と団体の間の信頼関係の構築」、「個人情報が処理される個人の権利の保護」、「組織的及び技術的措置の枠組みを作成すること」、「個人情報を処理する団体を設立すること」等を規定している。		
		文献タイプ	法令		
		国・地域	インド	適用分野	個人データの流通。
		策定者	電子情報技術省	対象者	個人データの流通に関与する公共機関、サービス企業等。
		順守義務	順守義務があり、「10章　罰則と補償」にて、違反等の場合の措置が規定されている。		
		普及状況	記載なし。(2023年1月現在効力があるものとみられるが、詳細不明。)		
		策定年	2019年	ページ数	52

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。(データ主体は、「不正確又は誤解を招く個人データ」があった場合、修正を要求する権利を有するものとする。5章「18」。)

4	セキュリティ区分・水準・対策	「データ主体に重大な危害を及ぼすリスクがあるかどうか等」を考慮して、「センシティブな個人データ」というようなカテゴリー設定をして通知するものとする。また、すべてのデータ受託者は、子供の権利を保護し、子供の最善の利益になるような方法で、子供の個人データを処理するものとする。

THE PERSONAL DATA PROTECTION BILL, 2019

5	技術的・制度的枠組	すべてのデータ受託者は、以下を含む「プライバシー バイ デザイン* ポリシー」を作成するものとする。(6章「22」) *プライバシー バイ デザイン: エンジニアリング プロセス全体を通じてプライバシーを考慮するコンセプト。

関連URL	THE INFORMATION TECHNOLOGY ACT, 2000(情報技術法) https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf Privacy by Design(プライバシー バイ デザインに関する説明) https://journalsofindia.com/privacy-by-design/

データ関連文献 #18：主な調査項目

THE PERSONAL DATA PROTECTION BILL, 2019

狙い

・プライバシーの権利は基本的権利であり、情報的プライバシーの本質的側面として個人情報を保護することが必要である。
デジタル経済の成長により、個人間の重要なコミュニケーション手段としてのデータの利用が拡大している。
個人の情報的プライバシーを尊重し、デジタルガバナンスを通じて進歩、革新を確保し、自由で公正なデジタル経済を育む集団文化を創造することが必要である。

概要

・この法令は以下を規定している。
➢個人情報に関する個人のプライバシー保護。
➢個人情報の流れと利用方法の特定。
➢個人情報を処理する個人と団体の間の信頼関係の構築。
➢個人情報が処理される個人の権利の保護。
➢組織的及び技術的措置の枠組みを作成すること。
➢個人情報を処理する団体を設立すること。
➢データ処理における組織的・技術的措置の枠組みを構築すること。
➢国境を越えた移転、個人データを処理する事業者の説明責任。
➢無許可で有害な処理に対する救済措置。
➢上記の目的及びそれに関連する事項のためにインドデータ保護局を設置すること。

セキュリティ区分・水準・対策

「センシティブな個人データ」のカテゴリー分け

・中央政府は、当局及び関係部門の規制当局と協議の上、「データ主体に重大な危害を及ぼすリスクがあるかどうか等」を考慮して、「センシティブな個人データ」というようなカテゴリー設定をして通知するものとする。

「子供の個人データ」

・すべてのデータ受託者は、子供の権利を保護し、子供の最善の利益になるような方法で、子供の個人データを処理するものとする。
データ受託者は、子供の個人データを処理する前に、規則で指定されている方法で、子供の年齢を確認し、親又は保護者の同意を得る必要がある。

データ関連文献 #19：概要

Non-Personal Data Governance Framework

1	概要	世界中で、政府は個人データに関連するオープンデータイニシアチブと規制を提案している(インドの個人データ保護法案2019(PDP法案)等)。しかし、非個人データに対する特定の規制が存在しなかったため、電子情報技術省は、「インドにおける非個人データに対する権利」を確立するために、国家レベルの規制を提案した。

2	書誌的情報	名称	Non-Personal Data Governance Framework		
		主旨	電子情報技術省の専門家委員会は、インドで収集及び作成された非個人データに対する権利を確立するために、インドで単一の国家レベルの規制を提案した。		
		文献タイプ	法令		
		国・地域	インド	適用分野	非個人データの取り扱い。
		策定者	電子情報技術省	対象者	非個人データを取り扱う公共団体、民間団体。
		順守義務	本規制の目標の1つに「非個人データに対するインドとそのコミュニティの権利を確立するための強制的な枠組みを作成すること」が掲げられている。		
		普及状況	記載なし。		
		策定年	2020年	ページ数	62

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。

4	セキュリティ区分・水準・対策	高価値なデータセット(High-value Datasets：HVD)の非個人データ共有について、委員会は、「ガイドライン/保護手段 」を示している。(例：非個人データ の共有は、特定の目的のためにのみ提案される、等)

Non-Personal Data Governance Framework

5	技術的・制度的枠組	NPDAは、個人データ保護機関(DPA)、CCI(Competition Commission of India's)などの他の機関と調和する必要がある。

関連URL	Personal Data Protection Bill 2019(法案) http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf GDPR(規制) https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html CCI(Competition Commission of India's)(組織紹介) https://www.mca.gov.in/content/mca/global/en/about-us/affiliated-offices/cci.html.html#:~:text=The%20Competition%20Commission%20of%20India,and%20enforcement%20of%20the%20Act.

Non-Personal Data Governance Framework

狙い

- 世界はデータで溢れている。データは、社会的価値や公共的価値とは別に、経済的価値と富を生み出す。
  データは、コアテクノロジービジネス、世界中のすべての経済セクター、及びさまざまな社会及び行政問題への取り組みにおいて、ますます中心的な存在になっている。
- データ経済の重要性と価値創出能力が増しており、世界中の政府は、データのあらゆる側面を可能にし、規制する必要性を認識している。
  世界中で、政府は個人データに関連するオープンデータイニシアチブと規制を提案している(インドの個人データ保護法案2019(PDP法案)や欧州連合の一般データ保護規則(GDPR)など)。
- しかし、非個人データに対する特定の規制が存在しなかったため、従来、そのようなデータは、知的財産権(著作権及び企業秘密を含む)に関連する法律、又はその他のアクセス権及び管理権(契約法を含む)によって管理されてきた。
- そこで電子情報技術省の専門家委員会は、インドで収集及び作成された非個人データに対する権利を確立するために、インドで単一の国家レベルの規制を提案している。

概要

- データ経済の重要性と価値創出能力が増しており、世界中の政府は、データのあらゆる側面を可能にし、規制する必要性を認識している。
  世界中で、政府は個人データに関連するオープンデータイニシアチブと規制を提案している(インドの個人データ保護法案2019(PDP法案)や欧州連合の一般データ保護規則(GDPR)など)。
  •しかし、非個人データに対する特定の規制が存在しなかったため、従来、そのようなデータは、知的財産権(著作権及び企業秘密を含む)に関連する法律、又はその他のアクセス権及び管理権(契約法を含む)によって管理されてきた。そこで委員会は、インドで収集及び作成された非個人データに対する権利を確立するために、インドで単一の国家レベルの規制を提案している。

データ関連文献 #19：主な調査項目

Non-Personal Data Governance Framework

セキュリティ区分・水準・対策

- 委員会は、高価値なデータセット(High-value Datasets: HVD)を次のように定義する。
  - ➢HVDとは、コミュニティ全体にとって有益なデータセットであり、以下のような公共財として共有されるものである。
  - ➢政策立案、公共サービスや市民参加の向上に役立つもの。
  - ➢質の高い新規雇用の創出に役立つもの。
  - ➢新規事業(スタートアップや中小企業)の創出に役立つもの。
  - ➢研究・教育に貢献する。
  - ➢新たなイノベーション、新たな付加価値サービス／アプリケーションの創出に寄与する。
  - ➢以下のような幅広い社会的・経済的目標の達成に貢献する。
  - ➢貧困の緩和、金融インクルージョン、農業開発、技能開発、医療、都市計画、環境計画、エネルギー、ダイバーシティ＆インクルージョン、その他

- 委員会は、データ受託者(data trustees)を、「インドにおけるHVDの作成、保守、データ共有を担当する、政府機関又は非営利の民間組織のいずれかの組織」と定義している。データ受託者は、非個人データの取り扱いに関して、関係するコミュニティに対する「注意義務」を負う。

- HVDの非個人データ共有に関する「ガイドライン/保護手段」として以下が挙げられる。
  - ➢非個人データ の共有は、特定の目的のためにのみ提案される。
  - ➢このようなデータ共有は、より大きな公共財に利益をもたらすべきものである。
  - ➢データ要求は、一般的又は広範であるべきではなく、「具体的で、定義された目的」をターゲットにする必要がある。
  - ➢委員会は、データ受託者が公共の利益のためにHVDを公的及び私的組織と共有することを勧告する。
  - ➢HVDのためにデータを共有する場合、データの処理(匿名化、集約、データ共有)のために一定の合理的な費用をデータ管理者に支払うことができる。
  - ➢データがインドのHVDの一部でない場合、公的又は個人データ管理者に直接そのようなデータを要求することは、委員会の勧告の範囲外である。
  - ➢公共財の目的以外では、民間団体から民間団体への強制的なデータ共有は、委員会の勧告の範囲では考慮されない。

データ関連文献 #20：概要

Personal Data Protection Act 2012

1	概要	「個人データ保護を促進及び実施すること」を目的とした、Personal Data Protection Act(個人データ保護法)を管理及び施行するためPersonal Data Protection Commission(個人データ保護委員会)が設立された。委員会は、データ保護関連の問題でシンガポール政府を国際的に代表しており、各セクターの規制当局と協力して、それぞれの分野でのコンプライアンスを監督している。

2	書誌的情報	名称	Personal Data Protection Act 2012		
		主旨	この法律の目的は、組織による個人データの収集、使用、及び開示を管理することにある。		
		文献タイプ	法令		
		国・地域	シンガポール	適用分野	個人データの取り扱い。
		策定者	シンガポール政府	対象者	個人データを取り扱う組織全般。
		順守義務	有罪判決を受けた場合、罰金、懲役、又はその両方に処せられる。		
		普及状況	主なデータ保護規則は2014年7月2日に発効した。DNCレジストリの規定は2014年1月2日に発効した。		
		策定年	2013年	ページ数	120

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。 ➢ 個人は、組織が所有又は組織の管理下にある個人データの誤り又は脱落の修正を組織に要求することができる。 ➢ 組織は、個人データが次の場合、組織によって、又は組織に代わって収集された個人データが正確かつ完全であることを保証するために合理的な努力を払わなければならない 。 (a)個人データが「その個人に影響を与える決定」を下すために組織によって使用される可能性がある場合。 (b)組織によって別の組織に開示される可能性がある場合。

Personal Data Protection Act 2012

4	セキュリティ区分・水準・対策	記載なし。
5	技術的・制度的枠組	個人データ保護法(PDPA)は、シンガポールにおける個人データ保護の基準となるものであり、銀行法や保険法などのセクター固有の立法及び規制の枠組みを補完する。 https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act
関連URL		PERSONAL DATA PROTECTION COMMISSION(PDPC) (組織紹介) https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

Personal Data Protection Act 2012

狙い

- 2013年1月、「企業と消費者の間の信頼環境を育み、活気あるシンガポール経済に貢献するために、個人データ保護を促進及び実施すること」を目的とした、Personal Data Protection Act(個人データ保護法)を管理及び施行するためPersonal Data Protection Commission(個人データ保護委員会)が設立された。
- 委員会は個人データ保護に関する問題でシンガポールの主な権限を持ち、データ保護関連の問題でシンガポール政府を国際的に代表しており、各セクターの規制当局と協力して、それぞれの分野でのコンプライアンスを監督している。
  https://www.pdpc.gov.sg/Who-We-Are/About-Us
- 委員会の機能は次のとおりである。
  (a)シンガポールにおけるデータ保護の意識を高める。
  (b)データ保護に関連するコンサルティング、アドバイザリー、技術、管理、又はその他の専門的なサービスを提供する。
  (c)データ保護に関連するすべての事項について政府に助言する。
  (d)データ保護に関連する事項について国際的に政府を代表する。
  (e)データ保護に関するセミナー、ワークショップ等の開催・実施、及びそのような活動を行う他の組織の支援、データ保護に関する調査・研究の実施及び教育活動の推進。
  (f)データ保護の分野で、外国のデータ保護当局や国際組織又は政府間組織を含む他の組織との技術協力と交換を、政府に代わって管理する。
  (g)この法律を管理及び施行する。
  (h)他の書面による法律に基づいて委員会に与えられた機能を遂行する。
  (i)大臣が官報の命令により委員会に許可又は割り当てることができる機能を実行する。

概要

- この法律の目的は、「個人データを保護する個人の権利」と、「状況に応じて適切と考えられる目的で個人データを収集、使用、又は開示する組織の必要性」の両方を認める方法で、組織による個人データの収集、使用、及び開示を管理することにある。

データ関連文献 #20：主な調査項目

Personal Data Protection Act 2012

セキュリティ区分・水準・対策

- セキュリティ区分・水準・対策の記載なし。
- 以下は、実際に「個人データ保護委員会」によって「罰金」が科せられたケースの1例である。
- 合計9,271通の電子メールが、ファラーパーク病院マーケティング部門の2人の従業員のMicrosoft Office 365仕事用電子メールアカウントから第三者の電子メールアドレスに自動的に転送された。
  患者の名前、性別、国民登録IDカード番号、パスポートの詳細、連絡先番号、医療情報など、患者の治療に関連する個人データが含まれていた。
  医療情報には、健康状態、診断、病歴、X線などの医療レポートが含まれる。
- 2019年10月、病院のITヘルプデスクは、電子メールアカウントが、すべての受信電子メールを自動的にサードパーティに転送するように設定されていたことを確認した。
  「個人データ保護委員会」は、病院が漏洩した個人データを不正なアクセスや開示のリスクから保護するための合理的なセキュリティ対策を実施していないことを発見した。
- ファラーパーク病院は、毎日大量の機密個人データを受信して処理しているため、マーケティング部門の仕事用メールアカウントを管理するためのより強力な対策を導入する必要があった、と「個人データ保護委員会」は指摘した。
  このような対策には、部門のWebメールアクセスに対する強化されたアクセス制御、部門が機密の医療情報を収集するための別のWebポータル、及びそのような情報を電子メールアカウントからより安全なシステムに定期的に移動するプロセスが含まれる。
- その後病院は以下を行った。
  - ➢データが漏洩する前にさまざまなセキュリティ対策を実施し、従業員に対してデータ保護とサイバーセキュリティのトレーニングを実施。
  - ➢エンドユーザーの自動転送機能を無効にする。
  - ➢社内のサイバーセキュリティ トレーニングと演習の頻度を増やす。
  - ➢追加の技術的な電子メール及びネットワーク セキュリティ対策の実装。
  - ➢既存のネットワークセキュリティ対策の更新とアップグレード。
- ファラーパーク病院は、約2,000人の機密医療情報が第三者に自動的に転送されることになったデータ侵害で、58,000シンガポールドルの罰金を科された。
  https://www.channelnewsasia.com/singapore/farrer-park-hospital-data-breach-pdpc-medical-information-3089466

データ関連文献 #21：概要

個人データの保護に関する政令草案 (Dự THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)

1	概要	ベトナムのデジタルインフラストラクチャは急速に進化し、改善されている。政府は、デジタル政府とデジタル経済に向けて、電子政府の構築を加速することを指示しており、多くの重要な成果をあげている。技術の応用レベルが高くなるほど、個人情報の提供と利用が増加するため、個人情報に関する法令違反の防止と対処、と同時に憲法、ベトナム法、国際法への準拠を確実にする必要性が高まってきた。そこで、公安省の「個人データ保護委員会」が様々な機能と義務をもち、対応にあたっている。

2	書誌的情報	名称	個人データの保護に関する政令草案 (Dự THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)		
		主旨	この政令は、「個人データ」、「個人データ処理」、「個人データ保護措置」、「個人データ保護委員会」、「個人データ違反の処理」、「関連機関、組織、及び個人の個人データ保護に対する責任」を規定している。		
		文献タイプ	法令		
		国・地域	ベトナム	適用分野	個人データの取り扱い。
		策定者	公安省	対象者	個人データに関連する機関、組織、及び個人。
		順守義務	個人データの処理に関連するデータ主体に関する規制に違反した場合、50,000,000ドンから100,000,000ドンの罰金が科せられる。		
		普及状況	この法令は、2021年12月1日から発効する。		
		策定年	2021年	ページ数	23

3	データ流通における信頼性のコンセプト・セキュリティ要件	記載なし。 (第15条： 個人データ処理者は、個人データが正確かつ完全であることを保証する責任がある。) (第5条3: データ主体は、個人データ処理者に、個人データを修正するよう要求できる。)

4	セキュリティ区分・水準・対策	機密性の高いセンシティブな個人データは、処理する前に個人データ保護委員会に所定の情報を登録する必要がある。

個人データの保護に関する政令草案 (Dự THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)

5	技術的・制度的枠組	記載なし。 タイの主要法律事務所の1つであるTilleke & Gibbins(ティレケ・アンド・ギビンズ)は以下のように述べている： ベトナム公安省(Ministry of Public Security、MPS) は、この政令草案がベトナムにおける個人データ保護に関する包括的で統一された法律/規制となることを目指している。MPS によると、この政令草案が発行されると、現在散在しているデータプライバシー法と共存し、効果的なものになる、ということである。本政令案は、既存の法律を置き換える代わりに、既存の法律と共存し、両者間に矛盾がある場合、「より厳しい要件を持つ方に従う必要がある」と考えられる。 https://www.mondaq.com/data-protection/1140256/update-on-vietnam39s-draft-decree-on-personal-data-protection

関連URL	公安省ポータル(組織ポータルサイト) https://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=418 公安省(組織紹介) https://mps.gov.vn/

個人データの保護に関する政令草案 (Dự THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)

狙い

- 「個人データ保護を規制する政令を作成するための提案に関するレポート草案(V/v đề nghị xây dựng Nghị định bảo vệ dữ liệu cá nhân)」によると、ベトナムは世界で最もインターネットアプリケーションの開発速度が速い国の1つであり、インターネットユーザーの数はベトナムの人口の3分の2以上(66%)を占める。
- ベトナムのデジタルインフラストラクチャは急速に進化し、改善されている。
  政府は、デジタル政府とデジタル経済に向けて、電子政府の構築を加速することを指示しており、多くの重要な成果をあげている。
  技術の応用レベルが高くなるほど、個人情報の提供と利用が増加するため、個人情報に関する法令違反の防止と対処、と同時に憲法、ベトナム法、国際法への準拠を確実にする必要性が高まってきた。
  https://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=418
- そこで、公安省のサイバーセキュリティ及びハイテク犯罪防止管理局にある政府傘下の組織である「個人データ保護委員会」が以下のような機能と義務をもち、対応にあたっている。
  1.個人データ保護意識向上活動を実施する。
  2.個人データ保護に関するコンサルティング、技術、管理、その他の専門的なサービスを提供する。
  3.個人データ保護に関連する事項について政府に助言する。
  4.関連するセミナーやシンポジウムの開催・実施、その他個人データの保護活動への支援等、個人データ保護に関する調査・啓発活動を推進する。
  5.外国のデータ保護当局、国際組織又は政府間組織を含む他の組織との、個人データ保護の分野での技術協力及び交換を管理する。
  6.データ主体の利益を事実上保護し、個人データの誤用を防ぎ、法的規制の遵守を保証し、データ保護の意識を促進する。
  7.機関や組織の個人データ保護の信頼性を評価及びランク付けし、全国個人データ保護ポータルで公開する。
  8.個人データの分類及び個人データ保護に関する規制違反の分類を行う。
  9.個人データ保護ガイドラインを発行する。
  10.技術開発と商慣行が個人データの保護にどのように影響するかを監視、評価する。
  その他

データ関連文献 #21：主な調査項目

個人データの保護に関する政令草案 (Dự THẢO NGHỊ ĐỊNH BẢO VỆ DỮ LIỆU CÁ NHÂN)

概要

- 個人情報の提供と利用が増加しているため、個人情報に関する法令違反の防止と対処、憲法、ベトナム法、国際法への準拠を確実にする必要性が高まってきた。
  この政令は、「個人データ」、「個人データ処理」、「個人データ保護措置」、「個人データ保護委員会」、「個人データ違反の処理」、「関連機関、組織、及び個人の個人データ保護に対する責任」を規定している。
- この法令は、 個人データに関連する機関、組織、及び個人に適用される。

セキュリティ区分・水準・対策

センシティブな個人データの処理のための登録

- 機密性の高いセンシティブな個人データは、処理する前に個人データ保護委員会に以下を登録する必要がある。
  a)個人データ処理者の氏名、登記簿又は個人識別コード、事業所、居住地、その他の連絡先情報、個人データ処理の法的根拠の引用、個人データ処理の目的、データの種類などの内容、個人データ保護対策の詳細な説明、等。
  b)機密性の高い個人データの処理に関する影響評価レポート。
  c)機密性の高い個人データを処理する際の個人データ処理アプリケーション及び影響評価レポートに記載されている内容に関連する文書及び情報。

別紙 3

IoT セキュリティ・セーフティ・フレームワーク

適用手順書

内容

1. 本手順書の概要 3

2. 適用手順 4

2-1 リスクアセスメント、リスク対応に向けた事前準備 4

2-2 リスクアセスメント 13

2-3 リスク対応 17

3. 参考 22

12 変更履歴

Version	変更年月日	変更箇所	変更内容
1.0	2023/3/13	-	新規作成

13

1. 本手順書の概要

本手順書では、IoT セキュリティ・セーフティ・フレームワーク(以下、「IoT-SSF」という。) の適用方法を以下のステップごとに説明する。

1. リスクアセスメント、リスク対応に向けた事前準備 [2-1 にて詳述]
   分析対象となる範囲についてステークホルダーの合意を得たうえで、IoT 機器・システムの概要及びシステムを構成する機器の一覧、システム構成図、データフロー図、目標とするリスクの水準を整理する。
2. リスクアセスメント [2-2 にて詳述]
   適用範囲において想定されるリスクやその原因を特定し、想定される被害の大きさを「第 1 軸:発生したインシデントの影響の回復困難性の度合い」(以下、「回復困難性の度合い」という。)や「第 2 軸:発生したインシデントの経済的影響の度合い」(以下、「経済的影響の度合い」という。)に沿って整理する。
3. リスク対応 [2-3 にて詳述]
   リスク対応を行うステークホルダーが実施すべき対策を「第 3 軸:求められるセキュリティ・セーフティ要求の観点」(以下、「セキュリティ・セーフティ要求」という。) ごとに整理する。

各ステップで作成する成果物は以下のとおりである。作成手順については、各節にて説明する。

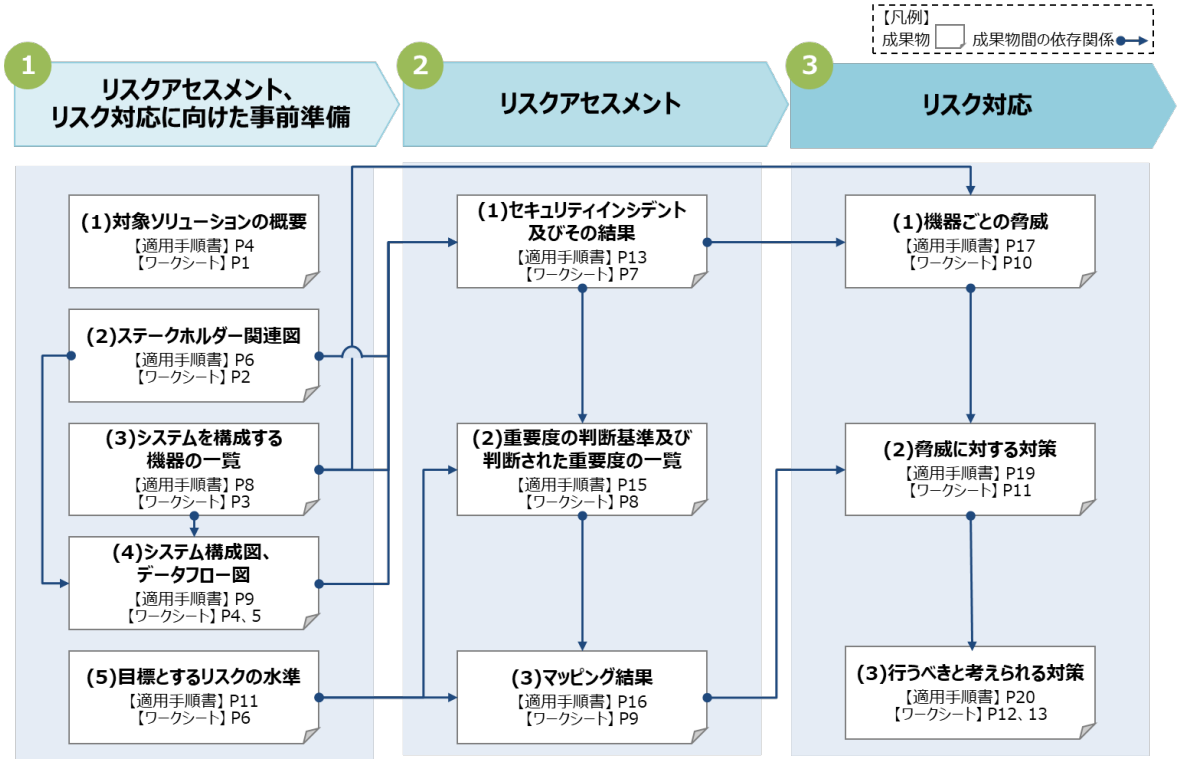


図 1 各ステップにおける成果物の一覧 [1]

[1] 図内の矢印は成果物間の依存関係を示す。手順を進める途中で、成果物間で整合性が取れない場合や内容の過不足が明らかになった際には、適宜、以前の段階に戻って内容を修正する。

IoT-SSF を参照し、IoT 機器・システム及び関連サービスにおけるリスクマネジメントを実行する主体を IoT-SSF の「適用主体」と呼ぶ。単一の事業者のみでサービス提供・利用が完結する場合は当該事業者が「適用主体」になるが、複数の事業者が協力して IoT 関連サービスを提供・利用する場合は、それぞれの事業者が、それぞれの責任範囲において「適用主体」となる。

複数の事業者が共同で適用手順を推進する場合は、各事業者間で協議した上で、結果等のとりまとめ役を決定することが望ましい。より俯瞰的な立場で IoT 関連サービスを見渡すことが可能な事業者[2]が、とりまとめ役[3]となり、後述のステークホルダー関連図やシステムを構成する機器の一覧、システム構成図、データフロー図等を活用して、他の事業者等に対して必要な対策の実施を依頼することにより、IoT 機器・システム全体の対策水準を向上させることができる。

2. 適用手順

2-1 リスクアセスメント、リスク対応に向けた事前準備

本節では、後段のリスクアセスメントやリスク対応を実施するための基礎となる以下の情報を整理する。

(1) 対象ソリューションの概要
(2) ステークホルダー関連図
(3) システムを構成する機器の一覧
(4) システム構成図、データフロー図
(5) 目標とするリスクの水準

(1) 対象ソリューションの概要

IoT-SSF を適用する IoT 機器・システムを特定し、対象ソリューションの概要を記述する。

具体的には、IoT-SSF を適用する IoT 機器・システムに関する提案書やシステム全体図[4]等を参考にして、対象ソリューションの目的や、IoT サービス利用者[5]による IoT 機器・システムの利用方法を記述する。また、必要に応じて対象とするソリューションの IoT 機器・システムに関する前提条件を記述する。

対象ソリューションの概要を記述する際には、IoT-SSF を適用させる範囲と適用の対象外とする範囲を明確化しなければならない。IoT-SSF の適用範囲は、IoT-SSF を適用する目的と整合させることが重要である。

対象の IoT 機器・システムと直接的なかかわりがない場合は OA 系の処理を行うための機器及びネットワークについては対象外としてもよい。

IoT 機器・システムを構成する要素は以下の TIPS に示す内容が参考となる。

---

[2] 「俯瞰的な立場で IoT 関連サービスを見渡すことが可能なステークホルダー」とは、IoT 関連サービス全体に責任を有するステークホルダーを指す。(例:プラント事業者、スマートホームサービス提供事業者)

[3] スキルやリソースの都合上、適切な対応が難しいステークホルダーはとりまとめ役に適さない点に留意されたい。

[4] 「システム全体図」の例：情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:システム化の方向性と計画」「システム全体図」参照。

[5] ISO/IEC 30141:2018 において定義されている IoT サービス開発者を指す。具体的には、企業利用者及び一般利用者を指す。

＜収集しておくべき情報(例)＞

- 対象機器・システムに関する提案書
- システム全体図

＜作成方法＞

1. IoT-SSF を適用する IoT 機器・システムとその範囲を特定する。
2. 対象ソリューションの目的、利用シーンや提供形態を記述する。
3. (必要に応じて)使用する IoT 機器・システムに関する前提条件を記述する。

- ２では、目的、受益者、提供する価値、運用時間、提供場所、提供形態、提供方法、利用するIoT機器、サブシステム等を記述する。
- 業界ごとに IoT 機器・システムの利用や運用等に影響を及ぼし得る規律(例:経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」、厚生労働省「ボイラーの遠隔制御基準等について」)が設けられている場合は、これらの前提を明記しておく。

＜TIPS＞

- 対象とする IoT 機器・システムの範囲を明確化する際には、情報処理推進機構(IPA)「IoT 開発におけるセキュリティ設計の手引き」(2.本書における IoT の定義)が参考となる。当該文書では IoT 機器の構成要素は以下のとおりとされている。

  - サービス提供サーバ・クラウド
    ネットワークに接続され、IoT に対応するサービスを提供するサーバやクラウドサービスを指す。
  - 中継機器
    IoT 機器・システムをネットワークに接続する中継機器を指す。例えば、ファイアウォール、ゲートウェイ、ルータが該当する。
  - システム
    中継機器経由でネットワークに接続される、複数の機器で構成されたシステムを指す。例えば、制御システム、病院内の医療ネットワークシステムが該当する。
  - 機器
    ネットワークに接続される機器を指す。例えば、情報家電やヘルスケア機器が該当する。
  - 直接相互通信する機器
    中継機器を通してネットワークに接続するだけでなく、機器自身が他の機器と直接通信する機能をもつ機器を指す。機器同士の通信機能を有するポータブルゲーム機や、車々間通信 Car2X に対応した自動車等が該当する。

＜成果物＞

- 対象ソリューションの概要

- 「IoT 機器・システムを通じて提供されるサービスの開発者」であるプラント事業者が、製造実行システム(MES)やHMI、プロセス制御PLC等からなるプラントシステムを用いて、化学物質を製造するケースを想定する。
- プラント事業者は、一般のビニール製品に広く使用される化学物質を製造する事業者であり、操業開始から既に数十年程度プラントを運用している。
- 本ケースケースでは、以下の工程のうち精製工程における蒸留工程を担う装置を扱う。
  1. 反応工程：原料や酸素等を反応させ化合物を生成する工程
  2. 洗浄工程：反応工程で生成された化合物を中和洗浄する工程
  3. 分解工程：中和洗浄された化合物を熱によって分解する工程
  4. 精製工程(蒸留工程を含む)：成分の沸点の差を利用して、分解工程までで生成された化合物を製品用に分離させる工程

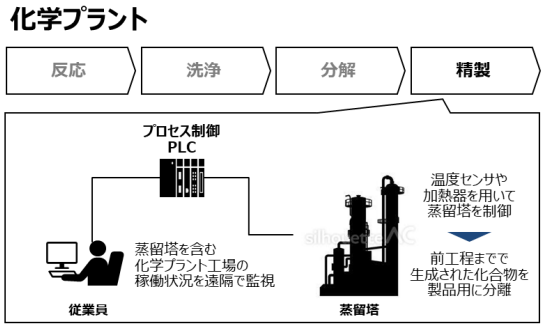


図 2 対象ソリューションの概要図(イメージ)

(2) ステークホルダー関連図

システム全体図や対象ソリューションに関する各種仕様書・契約書等を参考にして対象ソリューションのステークホルダーを洗い出し、各ステークホルダーの役割と責任を整理したステークホルダー関連図を作成する。

ステークホルダー関連図では、対象となる IoT 関連サービスにおいてセキュリティ上の責任を有する主体(例:IoT サービス開発者、IoT サービス提供者、IoT サービス利用者等)、対象サービスにおいてセキュリティ上の被害が生じた際に直接的または間接的に被害を受け得る主体をステークホルダーとして洗い出す。

ステークホルダーは、セキュリティ対策を実施する主体レベルで特定することが望ましい。

同じ企業内でセキュリティ対策を行う部署が異なる場合には、企画設計部門、運用部門のように部門を分けて記述することも検討する。

＜収集しておくべき情報(例)＞

- システム全体図
- 対象ソリューションに関する各種仕様書・契約書(例:IoT 機器・システムの提供方法、管理方法、利用許諾等に関する条文)

＜作成方法＞

1. 対象ソリューションの提供又は利用に関連するステークホルダーを洗い出す。
2. 各ステークホルダーの役割や責任を整理する。
3. 各ステークホルダー間の関係性(例:契約関係や提供機器、サービス)を整理する。

- ステークホルダーを洗い出す際には、IoT 機器・システムにおける開発、運用、保守の過程でセキュリティの責任を負う主体やセキュリティインシデントを通じて直接もしくは間接的に被害を受け得る主体を抽出する。
- 洗い出したステークホルダーの役割を明確にした上で、適用主体自身の役割や責任を明確にする。

＜TIPS＞

- セキュリティ対策上の責任を負い得る主体の抽出には、ISO/IEC 30141:2018 にて示されている以下の分類を参考にすることができる。
  - IoT サービス開発者
    - ✧ 機器メーカ
    - ✧ システムインテグレータ
  - IoT サービス提供者
    - ✧ クラウドサービス事業者
    - ✧ メンテナンス事業者
  - IoT サービス利用者
    - ✧ 企業利用者[6]
    - ✧ 一般利用者

- 上記に示されていない主体であっても、対象とする IoT 機器・システムの近傍にいる等の理由でセキュリティインシデントによる被害を受け得る第三者は、ステークホルダー[7]に含めることを検討する。例えば、以下に示す主体が含まれ得る。
  - IoT 機器の使用環境周辺にいる第三者
  - IoT 機器・システムを扱う大規模設備(例:工場やプラント)におけるセキュリティインシデントの被害を受け得る近隣住民

＜成果物＞

- ステークホルダー関連図

[6] 企業利用者は、自社のビジネス(例:製品の生産活動、供給活動)の中に IoT 機器・システム、サービスを組み込んだ上で、利用している事業者が想定される。

[7] 「サイバー・フィジカル・セキュリティ対策フレームワーク」ではステークホルダーを「意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。」と定義している。セキュリティインシデントの被害を受け得る人又は組織を「影響されることがある又は影響されると認知している、あらゆる人又は組織。」と理解することができることから、ユースケース集では IoT 機器・システムにおけるセキュリティインシデントによって被害を受け得る第三者をステークホルダーに含めている。

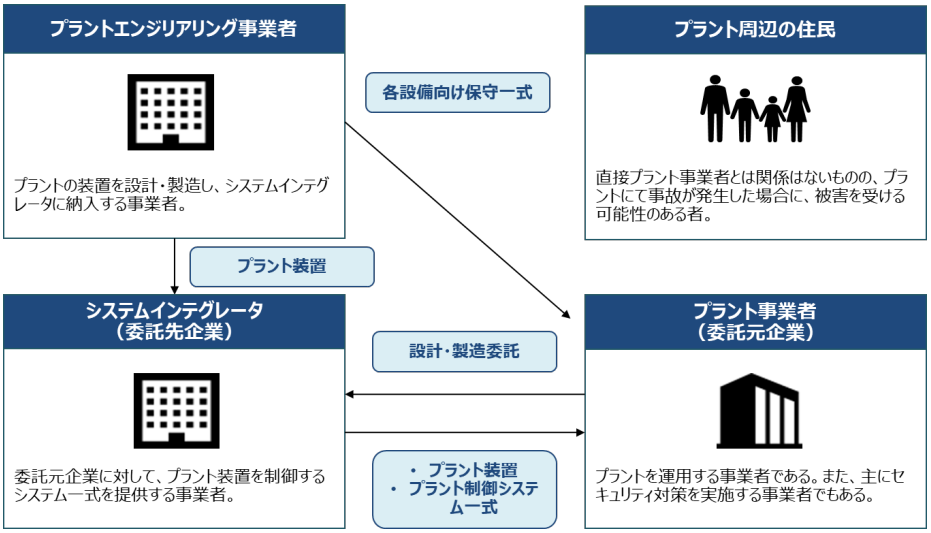


図 3 ステークホルダー関連図(イメージ)

(3) システムを構成する機器の一覧

既に整備、管理されている情報資産管理台帳 [8]等を参考にした上で、対象ソリューションを構成する機器やシステムの一覧を作成する。

システムを構成する機器は、対象となる IoT 関連サービスの範囲内で脅威が生じ得る機器を洗い出すことが望ましい。

分析対象を削減するためには、以下のように複数の機器を 1 つの機器にまとめることを検討する。

- 同じネットワークに直列に接続されているネットワーク機器を 1 つにまとめる。(例:直列に接続されているルータと FW を「ネットワーク機器(FW)」とする。)
- 以下に該当する場合は複数の機器を 1 つの資産と見なす。(例:エンジニアリング端末 1、エンジニアリング端末 2、エンジニアリング端末 3 を「エンジアリング端末」とする。)
  - 接続先ネットワークが同一である機器・システム
  - 設置場所のセキュリティレベルが同一である機器・システム
  - 同一機能、類似機能を有する機器・システム

システム構成図やデータフロー図を作成する際には、本項で整理した記載粒度で各図を作成することが望ましい。また、抜け漏れを防止するため、システムを構成する機器の記載粒度はステークホルダー間で調整し一致させることが必要となる。

＜収集しておくべき情報(例)＞

- 情報資産管理台帳

＜作成方法＞

1. システムを構成する機器の一覧を作成する。
2. システムを構成する機器ごとに、保有する機能や役割を記述する。

[8] 「情報資産管理台帳」の例:情報処理推進機構(IPA)「中小企業の情報セキュリティ対策ガイドライン」参照。

- 適用主体のみでの対応が難しい場合は、システムインテグレータや機器メーカ等と適宜情報交換を行った上で、機器の一覧を作成することが望ましい。
- 制御システムを評価対象とする場合は、情報系のネットワークに接続している OA 系の処理を行うための機器及びネットワークは対象外としてもよい。
- システムを構成する機器の記述内容には、例えば、以下の情報を含める。
  - 機器・システムの持つ機能
  - 設置場所
  - (IoT 機器の場合)スペック(大きさ・重量・走行スピード等)
  - (汎用的でない機器の場合)特記事項

＜成果物＞

- システムを構成する機器の一覧

表 1 システムを構成する機器の一覧

システムを構成する機器	内容
製造実行システム (MES: Manufacturing Execution System)	製造工程の把握や管理、作業者への指示や支援等を行うサーバ。 MES は、プラント事業者所内にサーバを設置するものとする。 なお、主な機能は以下のとおり。 - 作業のスケジュール管理機能 - 作業手配・製造指示機能 - 作業者管理機能 ・・・・
ヒューマンマシンインターフェース(HMI: Human Machine Interface)	人間の操作と機械の動作をスムーズに結合するために使用されるハードウェアとソフトウェア。 具体的には、タッチパネル式の表示器やパネルコンピュータを指す。 ヒューマンマシンインターフェースはプラント事業所内に設置するものとする。
・・・	・・・

(4) システム構成図、データフロー図

ネットワーク構成図[9]及びシステム関係図[10]、機能情報関連図[11]、(2)で作成したステークホルダー関連図、(3)で作成したシステムを構成する機器の一覧等を参考にした上で、対象となる機器・システムの構成図、データフロー図を作成する。

システムを構成する機器の一覧をもとにシステム構成図、データフロー図を整理することによって、発生し得るセキュリティインシデントやその結果に関する分析が実施しやすくなる。

9 「ネットワーク構成図」の例:情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:システム化の方向性と計画」参照。

10 「システム関係図」の例:情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:システム化の方向性と計画」参照。

11 「機能情報関連図」の例:情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:システム化の方向性と計画」参照。

＜収集しておくべき情報(例)＞

- ネットワーク構成図
- システム関係図
- 機能情報関連図
- ステークホルダー関連図(2-1(2)にて作成)
- システムを構成する機器の一覧(2-1(3)にて作成)

＜作成方法＞

1. エリア区分図を作成した上で、各システム・機器を配置する。
2. 各システム・機器のネットワーク接続状況を 1 に追記する。
3. システムを構成する機器に対する各ステークホルダーの関与方法(例:サービスの開発、サービス提供(運用を含む)、サービスの使用)を 2 に追記する。
4. 1～3 で作成したシステム構成図にデータフローを追記する。

- システム構成図を作成する際には、物理的な境界となる資産の配置とネットワーク的な境界となるルータやファイアウォールを軸とした配置を明確にする。また、エリアごとに物理的なセキュリティのレベルが異なる場合には、資産が設置されているエリア(例:執務室、サーバルーム)を分けて記述する。
- データフロー図を作成する際には、機器・システムからどの機器・システムへデータが送られているかを記述する。複数の経路が考えられる場合や初期設定時や保守設定時等、通常と異なるデータの経路が考えられる場合には、パターン分けを行った上で各経路を記述する。

複数の機器から 1 つのサーバへデータを集約させる場合等では、各機器からサーバに送信されるデータを同じ番号(例えば、全てのデータを 1 とする)で表現することとする。ただし、視認性の問題が生じる場合には各機器からサーバへ送信されるデータごとにパターン分けを行って、データフローを記述することが望ましい。

＜成果物＞

- システム構成図
- データフロー図

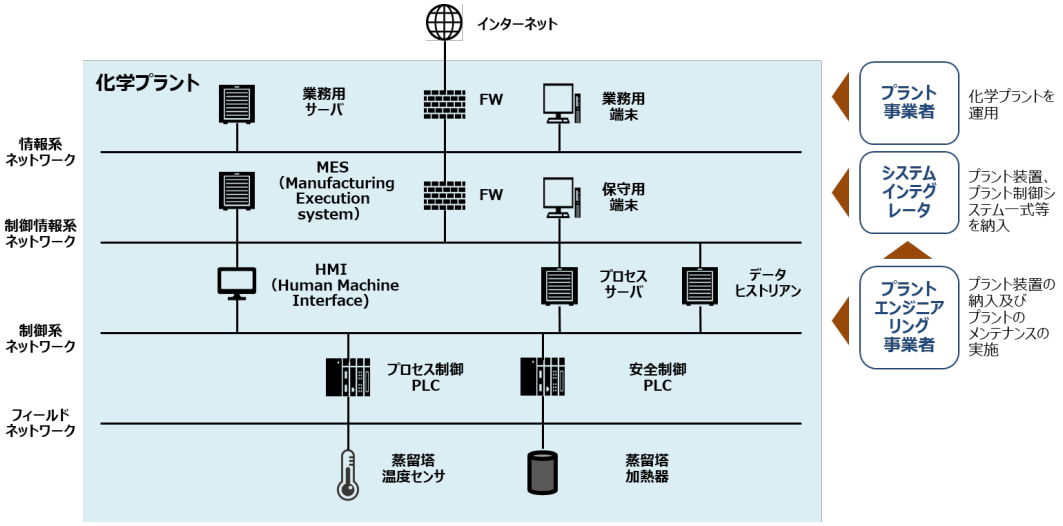


図 4 システム構成図(イメージ)

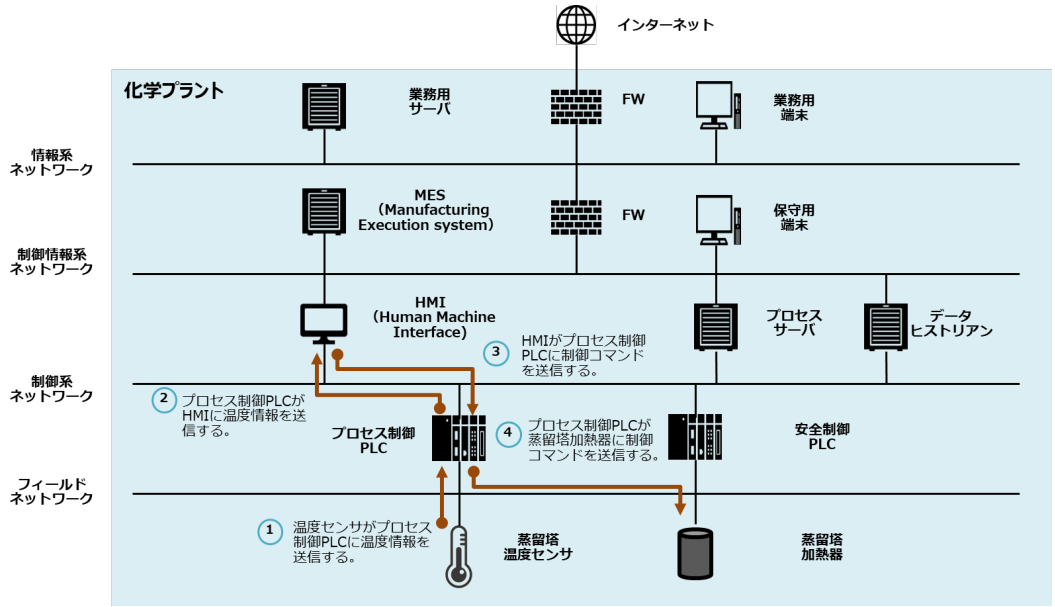


図 5 データフロー図(イメージ)

(5) 目標とするリスクの水準

組織内部における上位のセキュリティやセーフティに関する基本方針等を参考にした上で、対象ソリューションの目的に対して、受容できるリスクの大きさ及び種類をリスク水準として設定する。

「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」(以下、「ユースケース集」という。) に記載されている「発生したインシデントの影響の回復困難性の度合いの判断基準」や「発生したインシデントの経済的影響の度合いの判断基準」を参照しつつ、適用主体や各ステークホルダーにおける個別の事情等を勘案した上で、目標とするリスクの水準を設定することが望ましい。

本項にて目標とするリスクの水準を設定したとしても、後述の 2-2.リスクアセスメント「(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧」にて判断された重要度とリスクの水準の間で調整が発生する可能性がある。その際には、判断された重要度を考慮しつつ目標とするリスクの水準を変更することも検討する。

＜収集しておくべき情報(例)＞

- 適用主体内部のリスクマネジメントに関する基本方針

＜作成方法＞

1. 図 6 に示す判断基準を参考にして、受容可能な第 1 軸「回復困難性の度合い」のレベルを定める。
2. 図 7 に示す判断基準を参考にして、受容可能な第 2 軸「経済的影響の度合い」のレベルを定める。
3. 1、2 で定めたレベルから、受容できるリスク又は相対的に受容しがたいリスクの大きさを特定する。

レベル	判断基準	（参考） IoT-SSFにおける 判断基準
致命的な ダメージ	• 資産が攻撃された場合、利用者または関係者の人命が失われるおそれがある。	• 人命が失われる
重大な ダメージ	• 資産が攻撃された場合、重症を負うおそれがある。 • 資産が攻撃された際の利用状況が適切でない場合(例：想定利用方法と異なる)、人命が失われるおそれがある。 • 重要度が高い個人情報が漏洩する。	• 重症を負う • 重要な個人情報の漏洩
限定的な ダメージ	• 資産が攻撃された場合、軽傷を負うおそれがある。 • 個人情報が漏洩する。	• 軽傷を負う • メールアドレスのみの漏洩

図 6 発生したインシデントの影響の回復困難性の度合いの判断基準

レベル	判断基準	（参考） IoT-SSFにおける 判断基準
壊滅的な 経済影響	• 影響の範囲が内部に限定されず、取引先やその他の関係者に及び、長期間影響が続くことが想定される。 • 影響を受ける機器・システムの機能を他の製品・サービスで補うことができない。 • 大規模な製品等の回収等が生じ得る。	• （破産） • 社会の大混乱
重大な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及び、長期間影響が及ぶものの、**他の製品等で影響の結果を補うことができる**。 • 影響の範囲が取引先やそれ以外の関係者に及び、影響の結果は他の製品・サービスで補えないものの、**影響は短期間で収束する。** • 影響が長時間に及び、影響の結果は他の製品・サービスで補えないものの、**影響の範囲が取引先やそれ以外の関係者に及ばない。**	• 大損害 • 社会の混乱
限定的な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及ぶものの、**影響は長時間に及ばず、影響の結果は他の製品・サービスで補うことができる**。 • 影響の結果は他の製品・サービスで補えないものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響は長時間に及ばない。** • 影響が長時間に及ぶものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響の結果は他の製品・サービスで補うことができる**。	• 損害、社会の悪影響

図 7 発生したインシデントの経済的影響の度合いの判断基準

＜TIPS＞

- 目標とするリスクの水準は業界や業種によって異なるため、適用主体の判断に依存することに留意されたい。業界や業種によっては目標とするリスクの水準が一部大きくなる(例えば、第 2 軸「経済的影響の度合い」が重大な経済影響となる)こともあり得る。
- 組織内部における上位のセキュリティやセーフティに関する基本方針にて定められた内容と図 6 及び図 7 を比較した上で、目標とするリスクの水準を定めるが、各業界別のガイドラインや業法における規律を踏まえて、相対的に受容しがたいリスクを特定することで目標とするリスクの水準を明確することができる

可能性がある。

- 目標とするリスクの水準を明確にする際には、例えば、情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド 第 2 版」(4.3 事業被害と事業被害レベル)や内閣サイバーセキュリティセンター(NISC)「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)」(深刻度評価の概要)の文献が参考となる。

＜成果物＞

- 目標とするリスクの水準

以下、ユースケース集「2-3-4 化学プラント施設内の蒸留工程の自動制御」(⑤リスク基準)を例にして、「目標とするリスクの水準」の設定を説明する。

この例では、社内の安全に関する方針でプラントの従業員の安全やプラント周辺の環境汚染に対してより高い優先度で対処する規定を設けていると仮定した。

「回復困難性の度合い」に関しては、資産が攻撃された際に従業員が重症を負うとしている「重大なダメージ」は受容できず、「限定的なダメージ」とした。

プラントにおける事故は重大な事故に発展しやすいため、「経済的影響の度合い」が大きくなりやすく、セキュリティインシデントに伴う機器設備の停止等が生じた場合に「限定的な経済影響」に抑えることは現実的に難しい。仮にインシデントが発生したとしても、影響が取引先やそれ以外のステークホルダーに及ばなければ「重大な経済影響」と位置付けられることから、これらを念頭に置いて、「経済的影響の度合い」を「重大な経済影響」まで許容するとした。

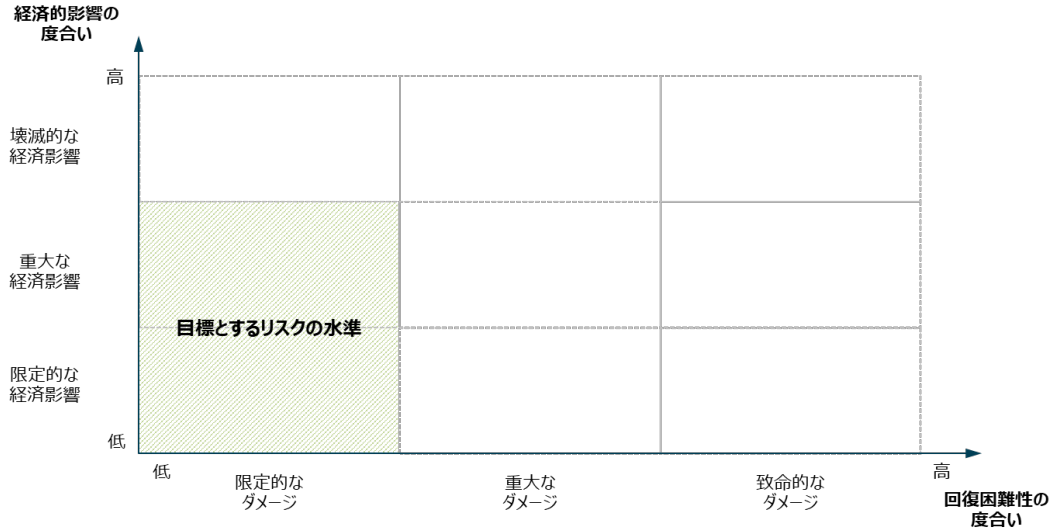


図 8 目標とするリスクの水準(イメージ)

2-2 リスクアセスメント

本節では、以下の情報を整理する。

(1) セキュリティインシデント及びその結果

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

(3) リスクのマッピング結果

(1) セキュリティインシデント及びその結果

過去に発生したセキュリティインシデントに関するメディア報道や報告書を参考としたり、脅威分析等の汎用的なセキュリティリスクアセスメント手法を活用したりすることで、適用対象となっている機器・システムにおいて想定されるセキュリティインシデントと、そのセキュリティインシデント等によって生じ得る結果を整理する。

本項では、事業リスクの観点から評価対象の機器・システムで生じ得るセキュリティインシデントとその結果を特定する。

本項にて事業影響(例:事業の停止・劣化、自社に対する信頼の低下、人的被害)及びそれにつながり得るセキュリティインシデント等を特定した上で、後述の 2-3 リスク対応「(1)機器ごとの脅威の整理」にてかかるインシデントを引き起こし得る脅威を特定する点に留意されたい。例えば、従業員の個人情報や取引先担当者等の情報が流出するケースを想定した場合、2-3 リスク対応「(1)機器ごとの脅威の整理」では、かかる被害の原因となる業務用サーバや業務用端末、MES 等に対する不正アクセスや情報漏えいを記載することとなる。

＜収集しておくべき情報(例)＞

- 社内やグループ会社、業界内において過去に発生したセキュリティインシデントに関するメディア報道や社内外の文書
- 業界内や対象機器・システムにおいて発生する可能性があると想定されているセキュリティインシデントに関する文書(研究報告等を含む)
- ステークホルダー関連図(2-1(2)にて作成)
- システムを構成する機器の一覧(2-1(3)にて作成)
- システム構成図、データフロー図(2-1(4)にて作成)

＜作成方法＞

1. 評価対象の機器・システムで生じ得るセキュリティインシデントとその結果を特定する。
   (ア) 機密性、完全性、可用性の各観点を考慮し、生じ得るセキュリティインシデントとその結果(事業被害)を特定する。
   (イ) 特定したセキュリティインシデントや事業被害が、最終的に対象機器・システム内のどの機器で生じ得るかを特定する。
   (ウ) 重大な影響を及ぼし得るセキュリティインシデントが成立するシナリオ(どのような主体が、どのような侵入経路で、どのような攻撃を行うか)を検討する。
2. セキュリティインシデントにより起こり得る結果及びその影響の度合いをステークホルダーごとに記述する。

＜TIPS＞

- 想定されるセキュリティインシデントを抽出する際には、ISO/IEC 27001:2013(6.1.2 情報セキュリティリスクアセスメント)で示された考え方を参考にすることができる。
- セキュリティインシデントによりもたらされ得る結果を特定する際には、以下に示す事業リスクを参考とすることができる。
  - 事業の停止・劣化
  - 自社に対する信頼の低下
  - 人的被害

- システム破壊
- 法令順守抵触事象の発生

- セキュリティインシデントによりもたらされ得る結果によって、企業の評判や評価、財務状況等が更なる影響を受ける可能性がある。そのため、例えば、上記に示す事業リスクに加えて、以下の観点からリスクを特定することも検討する。
  - 企業の評判や評価の低下に伴う企業イメージ・収益の悪化
  - 企業の評判や評価の低下に伴う事態収拾・信頼回復に係るコストの増大

- また、情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド 第２版」(4.3 事業被害と事業被害レベル)を参考にすることができる。

＜成果物＞

- セキュリティインシデント及びその結果

分類	想定されるセキュリティインシデント	想定される被害(例)
プラント事業者にとってのリスク	悪意のある攻撃者が、業務用サーバや業務用端末に加えて、MES等に**不正アクセス**し、**情報を漏えい**させる。	従業員の個人情報や取引先担当者等の情報が流出する可能性がある。
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、**蒸留塔等が爆発し得る。**その結果、プラント工場が停止するとともに、**従業員が重症を負うか死亡する可能性がある。**（※1）
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、蒸留工程に関する設備が停止する。	その他の工程も停止することにより、**工場全体の稼働が停止する**とともに、川下の企業の経済活動にも大きな影響を与える。
プラント周辺の住民	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、蒸留塔等が爆発することにより、環境汚染が生じた場合には、**住民等の健康や安全に多大な影響**が生じる可能性がある。また、**住民の生活にも大きな支障をきたす**可能性がある。
システムインテグレータにとってのリスク	プラント事業者に対する注意喚起(例：設定方法に関する説明等)を怠る。	サービス提供における過失が認められ得る。（※2）
プラントエンジニアリング事業者にとってのリスク	開発するアップデートプログラムが改ざんされ、そのまま配信されることで、MESやプロセス制御PLC等が**マルウェアに感染**する。	MESやプロセス制御PLCが想定していない動作をして、**蒸留塔等の設備が停止する。**（※3）

※1:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（住民被害や環境汚染の対応等）の事後的な対応が発生し得る。
※2:その結果として、契約上の責任が問われ得る。
※3:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（システムインテグレータへの補償等）の事後的な対応が発生し得る。

図 9 セキュリティインシデント及びその結果(イメージ)[12]

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

まず、「2-1. リスクアセスメント、リスク対応に向けた事前準備」における「(5)目標とするリスクの水準」や図 6、図 7 を参考として、機器・システムにおける重要度の判断基準を明らかにする。

その上で、「2-2. リスクアセスメント」における「(1)セキュリティインシデント及びその結果」で整理したセキュリティインシデント及びその結果の深刻度を勘案し、機器・システムの重要度(被害を受けた際の影響の大きさ)を一覧化する。

[12] 図 9 に示したセキュリティインシデント及びその結果は一部である。したがって、図 9 で示したもの以外についても起こり得ることに留意されたい。

機器・システムの重要度の判断基準を特定することによって、想定されるセキュリティインシデント及びその結果におけるリスクの大きさを算出することが可能となる。

＜収集しておくべき情報(例)＞

- 目標とするリスクの水準(2-1(5)にて作成)
- 想定されるセキュリティインシデント等とその結果(2-2(1)にて作成)

＜作成方法＞

1. 第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」ごとに機器・システムにおける重要度の判断基準を特定する。
2. 1 で特定された判断基準に基づいて機器・システムの重要度をステークホルダーごとに一覧化する。

- 既存の規格(例:ISO/IEC 27001)やかかる規格に基づくリスクアセスメントでは、想定される個々のリスクや脅威を単位としてリスクレベルを評価するが、IoT-SSF では想定されるセキュリティインシデントを踏まえて機器・システムという単位で重要度を評価することが求められている点に留意されたい。
- 機器・システムで生じ得るセキュリティインシデントの影響の内容や大きさは、被害を受けるステークホルダーごとに異なることが想定される。IoT-SSF では、評価対象の機器・システムを取り巻くエコシステム全体でセキュリティ等を確保する観点から、ステークホルダー関連図で整理したステークホルダーごとに重要度を評価することに留意されたい。
- 重要度の判断基準は、「2-1.リスクアセスメント、リスク対応に向けた事前準備」における「(5)目標とするリスクの水準」で作成した目標とするリスクの水準と整合をとる必要がある。

＜成果物＞

- ステークホルダーごとに判断された重要度の一覧

ステークホルダー	回復困難性の度合い	経済的影響の度合い
プラント事業者	• 爆発事故によって、従業員が死亡する可能性がある。	• 大規模な製品回収につながるおそれがある。
プラント周辺の住民	• プラント周辺の住民が重症を負う可能性がある。	• 農林水産業への打撃により、住民の生活にも大きな支障をきたすおそれがある。
システムインテグレータ	• 従業員がけがをする可能性は低い。	• サービス提供における過失が認められ得る。
プラントエンジニアリング事業者	• 従業員がけがをする可能性は低い。	• 開発するアップデートプログラムが改ざんされ、大規模な製品回収につながる可能性がある。

図 10 判断された重要度の一覧(イメージ)

(3) リスクのマッピング結果

「2-2.リスクアセスメント」における「(2)機器・システムの重要度の判断基準及び判断された重要度の一覧」で整理した重要度の一覧を参考にして、第１軸「回復困難性の度合い」及び第２軸「経済的影響の度合い」に対象機器・システムをマッピングする。

このマッピングによって、相対的にリスクが大きいとされる機器・システム(及びリスク)を把握し、リスク対応の方向性を検討することが可能となる。

＜収集しておくべき情報(例)＞

- 想定されるセキュリティインシデント等とその結果(2-2(1)にて作成)
- 判断された重要度の一覧(2-2(2)にて作成)

＜作成方法＞

1. 第１軸「回復困難性の度合い」及び第２軸「経済的影響の度合い」に機器・システムをマッピングする。

- 同じ機器・システムであってもステークホルダーによって重要度は異なるため、ステークホルダーごとに機器・システムをマッピングする。
- 機器・システムによって、生じ得るインシデントやその結果及びリスクの大きさが異なる場合には、その機器・システムごとにマッピングする。

＜成果物＞

- マッピング結果

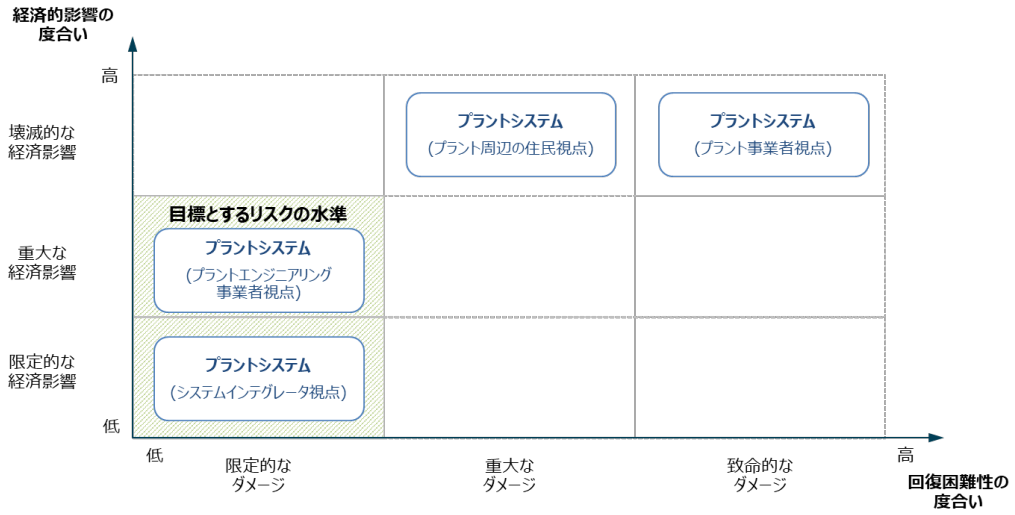


図 11 リスクのマッピング結果(イメージ)

2-3 リスク対応

本節では、以下の情報を整理する。

(1) 機器ごとの脅威

(2) 脅威に対する対策

(3) 行うべきと考えられる対策

(1) 機器ごとの脅威

「2-1. リスクアセスメント、リスク対応に向けた事前準備」における「(3)システムを構成する機器の一覧」で作成したシステムを構成する機器の一覧や「2-2.リスクアセスメント」における「(1)セキュリティインシデント及びその結果」で作成したセキュリティインシデント及びその結果より、対象の機器・システムを構成する機器ごとの脅威を特定する。

機器ごとの脅威を特定することによって、脅威に対応した対策を整理することが可能となる。

＜収集しておくべき情報(例)＞

- システムを構成する機器の一覧(2-1(3)にて作成)
- セキュリティインシデント及びその結果(2-2(1)にて作成)

＜作成方法＞

1. セキュリティインシデント及びその結果より、セキュリティインシデントが生じ得る機器の一覧を作成する。
2. セキュリティインシデントが生じ得る機器ごとに想定される脅威を記述する。
3. セキュリティインシデント及びその結果を踏まえて、脅威ごとに生じ得るインシデントを記述する。

- ユースケース集では、相対的に影響の度合いが大きいと評価された機器・システム及びかかる機器・システムにて想定されるセキュリティインシデントに関連した脅威が明示されている。しかし、実際に脅威を洗い出す際には、その前段としてある程度網羅的に脅威を洗い出しておくことが望ましい。
- セキュリティインシデントが生じ得る機器の一覧を作成する際に過不足が生じた場合、「2-2.リスクアセスメント」における「(1)セキュリティインシデント及びその結果」に戻り、セキュリティインシデント及びその結果を再整理することが望ましい。

＜TIPS＞

- 想定される脅威を洗い出す際には、ユースケース集における「(1) システムを構成する機器ごとの脅威の整理」で示した脅威を参考とすることができる。
  - STRIDE モデルにおける脅威
    - なりすまし
    - データの改ざん・消去
    - 否認
    - 情報漏えい
    - サービス不能
    - 権限の昇格
  - IoT 機器・システムにおいて追加的に想定される脅威(例)
    - 不正アクセス
    - マルウェア感染
    - 踏み台
    - 不正改造
    - 未知の脆弱性
    - 不正利用

✧　利用者によるセキュリティ設定等の誤り等

- また、情報処理推進機構(IPA)「制御システムの制御システムのセキュリティリスク分析ガイド 第 2 版」(5.3.1. 想定される脅威(攻撃手法)一覧の確認)を参照することもできる。

＜成果物＞

- 機器ごとの脅威

表 2 想定される脅威(イメージ)

システムを構成する機器	想定される脅威	生じ得るインシデント
製造実行システム (MES: Manufacturing Execution System)	データの改ざん	製造実行システムに保存された稼働情報等が改ざんされる。
	情報漏えい	製造実行システムに保存された稼働情報等が外部に漏えいする。
	…	…
…	…	…

(2) 脅威に対する対策の洗い出し

「2-3.リスク対応」における「(1)機器ごとの脅威」で作成した機器ごとの脅威を参考にして、第 3 軸「セキュリティ・セーフティ要求」における 4 つの観点ごとに脅威に対する対策を整理する。対策を整理する際には、想定される脅威ごとに個別に対策を洗い出す。

また、適用主体が実施すべき対策のほか、ステークホルダー関連図に含まれる他の事業者又は個人に対応を依頼する対策も整理する。脅威に対する対策を整理することによって、各ステークホルダーが実装する(可能性)がある対策を網羅的に整理することができる。

＜収集しておくべき情報(例)＞

- 機器ごとの脅威(2-3(1)にて作成)
- マッピング結果(2-2(3)にて作成)

＜作成方法＞

1. 第 3 軸「セキュリティ・セーフティ要求」における 4 つの観点ごとに、脅威に対して必要と考えられる対策を整理する。
   (ア) 第 1 の観点における対策を対策要件の実装先(ソシキ・ヒト及びシステム)ごとに記述する。
   (イ) 第 2 の観点における対策を対策要件の実装先(ソシキ・ヒト及びプロシージャ、システム)ごとに記述する。
   (ウ) 第 3 の観点における対策を対策要件の実装先(ソシキ・ヒト及びシステム)ごとに記述する。
   (エ) 第 4 の観点における対策を対策要件の実装先(ソシキ・ヒト及びシステム)ごとに記述する。

ただし、既存の機器・システムを対象にリスクアセスメント、リスク対応を行う場合には、上記で記述した対策の一部を既に実装している可能性がある。その場合には、以下の作業が必要となる。

2. 上記で整理した対策と既に実装している対策を照らし合わせた上で、新たに実装すべき部分のみを記述する。

＜TIPS＞

- 対策要件を整理する際には、CPSF における「添付 C 対策要件に応じたセキュリティ対策例」やユースケース集における「添付 A 対策要件」を参考とすることができる。
- 第 4 の観点では、「賠償等の対処を実施することが容易ではないケース等における社会的なセーフティネットの構築」を広く検討することが望ましい。

＜成果物＞

- 脅威に対する対策の一覧

表 3 脅威に対する対策の一覧(イメージ)

第 3 軸	実装先	想定される脅威	対策要件
第 1 の観点	ソシキ・ヒト	データの改ざん	IoT 機器・システムにおけるセキュリティポリシーの策定
		…	…
第 2 の観点			
第 3 の観点			
第 4 の観点			

(3) 行うべきと考えられる対策の整理

「(2)脅威に対する対策の洗い出し」で作成した脅威に対する対策を参考にして、優先的に行うべきと考えられる対策を整理する。

脅威に対する対策をすべて実装し、想定されるリスクを最小化することが理想であるが、対策の実施はコストを伴うので、現実的には全ての対策を実装することはできない。対策の絞り込みを行う際には、以下の＜作成方法＞に示す考え方を参考にしつつ対策の優先順位付けを行った上で、行うべきと考えられる対策を整理する。

行うべきと考えらえる対策を整理することで、コストや効率性等を考慮して各ステークホルダーが実施できる粒度で対策を整理することができるようになる。

なお、適用主体に関係する業界団体で公開されているガイドラインや基準がある場合には、かかるガイドラインや基準を参考にした上で対策の優先順位の決定に係る考え方を整理されたい。

＜収集しておくべき情報(例)＞

- 脅威に対する対策(2-3(2)にて作成)

＜作成方法＞

1. 脅威に対する対策より、適用主体にて行うべきと考えられる対策要件を抽出する。
2. 1 で抽出した対策要件ごとに実際に講じる対策を整理する。
3. 脅威に対する対策より、各ステークホルダーにて行うべきと考えられる対策要件(他のステークホルダーにて実装を依頼する対策要件)を整理する。
4. 3.で抽出した対策要件ごとに実際に講じる対策を整理する。
5. 4 で整理した対策の実装を各ステークホルダーに依頼する。

- 実際に講じる対策を抽出する際には、目標とするリスクの水準に収まっていない機器・システムを対象としたものの優先度を上げることを考慮する。
- 「対策の適用対象」、「適用する対策の内容」の観点から、以下のような観点を考慮して対策の優先

順位付けを行うことも有効である。

- 対策の適用対象

当該機器に影響を及ぼす事象が実際に生じた場合に、結果として生じ得る被害の大きさや、当該機器に悪影響を及ぼし得る事象の起こりやすさを考慮する。

- 適用する対策の内容

対策に係る費用対効果の大きさや対策に係る実施可否を考慮する。

＜TIPS＞

- 実際に講じる対策を整理する際には、CPSF における「添付 C 対策要件に応じたセキュリティ対策例」やユースケース集における「添付 B 実際に講じる対策の例」を参考とすることができる。

＜成果物＞

- 適用主体にて行うべきと考えられる対策
- 他のステークホルダーにて行うべきと考えられる対策(他のステークホルダーにて実装を依頼する対策)

表 4 適用主体にて行うべきと考えらえる対策(イメージ)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 対象となっているプラント施設におけるセキュリティポリシー(例:情報セキュリティ関連規定を含む)の見直し及び、事業部長等の適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
			…	…	…
	第 2 の観点				
	第 3 の観点				
	第 4 の観点				

表 5 他のステークホルダーにて行うべきと考えられる対策(他のステークホルダーにて実装を依頼する対策)(イメージ)

No	第 3 軸	実装先	対策要件	実際に講じる対策(例)	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	搭載するソフトウェアの改ざん検知機能の実装の要求	● MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装。	
	第 2 の観点			●	
	第 3 の観点			●	
	第 4 の観点			●	

3. 参考

- 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(CPSF)」
- 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)」
- 経済産業省「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」
- 情報処理推進機構(IPA)「IoT 開発におけるセキュリティ設計の手引き」
- 情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:システム化の方向性と計画」
- 情報処理推進機構(IPA)「超上流から攻める IT 化の事例集:要件定義」
- 情報処理推進機構(IPA)「中小企業の情報セキュリティ対策ガイドライン」
- 情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド 第 2 版」
- 内閣サイバーセキュリティセンター(NISC)「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準(初版)」
- ISO/IEC 27001: 2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture
- Microsoft” Microsoft Threat Modeling Tool の脅威”

別紙４

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

適用手順書

目次

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」の基礎情報 3

1.1 目的 3

1.2 データマネジメントのモデル 3

1.3 DMF による分析の位置づけ 4

2. 適用手順（概要） 4

3. 適用手順（詳細） 5

3-1 対象とするデータ利活用プロセスの特定 5

3-2 データ処理フロー（「イベント」）の可視化 5

3-3 必要な制度的な保護措置(「場」)の整理 6

3-4 「属性」の具体化 8

3-5 「イベント」ごとのリスクの洗い出し 11

変更履歴

Version	変更年月日	変更箇所	変更内容
β版	2022/5/24	-	適用実証実施のため、新規作成
1.0	2023/3/31		適用実証にて頂戴したご意見等を踏まえ、一部内容を変更

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」の基礎情報

1.1 目的

本文書が参照する「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)は、バリュークリエイションプロセスを通じた付加価値創出を支援するため、主体間を転々流通するデータの信頼性を確保するための考え方やプロセス等を整理したものであり、将来的な事業者による活用が期待されるものである。

ここで、バリュークリエイションプロセスとは「様々なモノやデータが動的につながって構成される付加価値の創造活動」であり、様々な組織、システム、サービス等が関与するマルチステークホルダーから構成されるものと考えられる。DMF は、このような複雑なプロセスにおいて利活用されるデータのライフサイクル全体を捉え、その全体に渡り十分な信頼性を確保するために活用されることを念頭に置いている。

本文書は、DMF に基づいたリスクアセスメントを実施しようとする事業者を対象に、かかる活動の手順を示すものである。

＜参考情報＞

- 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
  (https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework.pdf)

1.2 データマネジメントのモデル

DMF 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、「属性」、「場」、「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。DMF の 2-2 詳細編では、3 つの要素の概要を以下のように記している。

- **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、必要な措置を講ずることによって、データの適切な取扱いを実現することが可能になる。

- **場**
  「場」はデータに対して特定の規範を共有する範囲と定義される。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変動し得る。「場」は例えば、パーソナルデータの保護、知的財産(営業秘密を含む)保護、機微技術管理、適切な社会機能の維持等の観点で整理され得る。

- **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り、「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。

DMF における「データマネジメント」とは、「属性」、「場」、「イベント」という要素を考慮しつつ、対象となるデータの利活用プロセスの全体を正確に把握し、取扱われる個々のデータや適用される規律等の性質を踏まえて細やかなリスク管理を実施するものと捉えることができる。

1.3 DMF による分析の位置づけ

従来からシステム開発プロセスにおける要件定義や設計、あるいは運用段階においては、脅威分析等の手法を通じて、対象の物理的・論理的なシステム構成に基づくユーザーやサーバ等の機器、その他外部エンティティとの境界で起こり得る問題の特定や、対応すべき箇所の把握が行われている[1]。かかる手法は実装レベルの資産識別や攻撃シナリオの特定によりセキュリティリスクに関して詳細な分析を可能にするものであるが、DMF による分析は、取扱われる個々のデータの特性やそれに関連して課せられる法律や契約等の規律に着目する点、特定のシステム構成を前提としないより上位のレベルでのリスク特定に注力するという点等に特徴がある。

昨今、主にデータの取扱いに係る法規制等の複雑化やデータ利活用のあり方の多様化を通じて、パーソナルデータに係るものを中心に事業に影響を及ぼし得るデータ関連のリスクは様々な種類のものを含むようになりつつある。ひとつには、DMF はこれまでセキュリティ対策の文脈で議論されてきた、特に外部の悪意ある者により引き起こされ得る機密性、完全性、可用性に係るリスクに限らず、データの利活用に係るリスクを包括的に特定し、対処することを支援する枠組みとして位置づけられる。

また、データ利活用に係るリスク管理においては社内外の様々な部門、関係者との協力が必要になるところ、技術的に詳細なものではなく、データライフサイクルの全体においてより抽象的なレベルでリスクを特定することを通じて、IT 部門等に所属するセキュリティに知見のある者だけでなく、現にデータ利活用ビジネス等を推進する事業担当者や各国の法規制への対応や事業者間の契約等を支援する法務担当者、社外のステークホルダー等を含めた部門間・組織間のコミュニケーションを支援し、コレクティブアクションを促進することも意図している。ゆえに、DMF 及び本適用手順書の想定読者としては、事業者のセキュリティ担当者やリスク管理担当者だけでなく、現にデータ利活用ビジネスを推進する事業担当者や法規制対応等の観点からそれを支援する法務担当者等も含まれる。

なお、DMF による分析は上位レベルでのリスク特定やそれに基づく関係者間の合意形成等に資するものと捉えられる一方で、それ単体でリスク管理のプロセス全体が完結するものではなく、特に、詳細なリスクシナリオ等の作成や対策の検討等においては既存の脅威分析等と併用する形で最も効果的に機能すると考えられる点に留意されたい。

2. 適用手順（概要）

DMF 適用の目的は、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、データの利活用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にある。その際、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。(概要は、DMF 2-1-2 リスク分析手順 を参照されたい。)

---

[1] 脅威分析の概要については、例えば、「IoT 時代の脅威分析とリスク評価」（https://www.ipa.go.jp/files/000062795.pdf ）等を参照されたい。

1. データ処理フロー（「イベント」）の可視化 [3-2 にて詳述]
2. 必要な制度的な保護措置(「場」)の整理 [3-3 にて詳述]
3. 「属性」の具体化 [3-4 にて詳述]
4. 「イベント」ごとのリスクの洗い出し [3-5 にて詳述]

3. 適用手順（詳細）

3-1 対象とするデータ利活用プロセスの特定

DMF の適用対象とするデータ利活用プロセスの範囲とその概要を特定する。概要の中では、対象となる利活用プロセスに関わる「主体」(例：サービスの利用者/提供者、社内の関係部署)や取扱われる「データ」及び、「利用環境」(例：端末、サーバ、ストレージ、ネットワーク等)を特定する。この検討を通じて、「どのような情報が、どこからどこに、どのような手段を介してやりとりされるのか」という「データの流れ」を把握することができる。

本作業実施の際には、事業担当者や法務担当者等の IT やセキュリティに必ずしも知見のない要員であっても概要を理解することができるよう、共通した性質(例：取得元の機器が同一、法令上の扱いが同等)を持つデータは一括りにして表現する、意味を理解できる粒度で「データ」や「利用環境」の整理を行う等の配慮をしつつ、対象範囲を合理的に検討可能な範囲に限定することが望ましい。

＜作成にあたっての参考情報＞

- DMF 添付 A 各ユースケース冒頭部における「対象プロセスの概要」

3-2 データ処理フロー（「イベント」）の可視化

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、手順としては、対象プロセスにおいて取扱うデータを一覧化し、対象プロセスにおけるデータ処理フローに沿って、リストに含まれるデータ間の関係を整理するという順でフローの可視化を行う。

記法としては、DMF において強調されている以下の事項に注意する。

- サーバや端末等のシステム構成要素ではなく、そこで取扱われるデータを中心とした整理を行う。
- データやそれを取扱う環境に量的・質的な変化が生じる箇所を「イベント」として識別する。ここで、「量的・質的な変化」の例、識別され得るイベント類型として以下が想定される。

  - ✓ データの量的変化 (例：複数チャネルから取得したデータの集約) [生成・取得、移転・提供]
  - ✓ データの法的カテゴリや価値の大小を変更する処理(例：個人データの匿名加工、仮名加工) [加工・利用]
  - ✓ データへの実質的な管理権限を有する主体の変更 (例：データの第三者提供) [移転・提供]
  - ✓ データ保管場所の変化、特に適用される法令やポリシー等に変更が生じるもの [移転・提供]

本段階のアウトプット例を図 1 に示す。図 1 では、個々のデータを円形、イベントをブロック矢印で記述しているが、事業者における実際の適用にあたって、これらの様式は強制されるものではない。

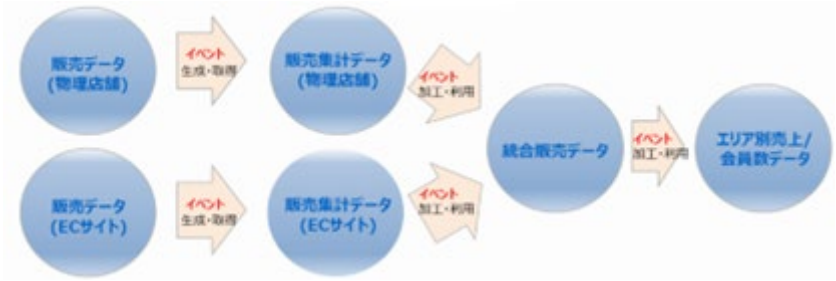


図１　データ処理フローの可視化(例)

＜収集しておくべき情報とその情報源(例)＞

・　対象とするデータ利活用プロセスにおいて取扱うデータの一覧（情報源の例：情報資産管理台帳)

・　上記データに対して実施する処理の流れ（情報源の例：設計ドキュメント、概念設計)

＜実施手順＞

1. 対象プロセスにおいて取扱うデータをリスト化する。
2. 対象プロセスにおけるデータ処理フローに沿って、リストに含まれるデータ間の関係を整理する(例：サービス利用者がスマホアプリ上で入力して「生成・取得」された個人データ A が、匿名加工処理という「加工・利用」を通じて、匿名加工情報 B へと遷移する)。当該フローには典型的に、データの生成・取得、加工・利用、移転・提供等が含まれ得る。

＜作業成果物が満たすべき要件＞

・　対象のデータ利活用プロセスで取扱われるデータが漏れや重複なく記載されている

・　上記データを対象とするイベントが、「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の区分に沿って、漏れや重複なく記載されている

＜作成にあたっての参考情報＞

・　DMF 添付 A 各ユースケースにおける「STEP 1 データ処理フロー（「イベント」）の可視化」

3-3　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」(必要な制度的な保護措置)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も想定される。

適用にあたっては、いかなる規範が「場」として識別されるかという点が第一に検討されるべきである。「データフローの可視化」において識別された各データに対して、以下の観点から各「場」に係る簡易的な該非の判断を行うことが望ましい。

・　パーソナルデータの保護（関係法令の例：個人情報保護法(日)、GDPR(EU))

　✓　(日本法の適用を想定する場合) 対象のプロセスにおいて、個人データ、仮名加工情報、匿名加工情報、個人関連情報等の、個人情報保護法の規律が適用される種類のデータが含まれるか。

・ 知的財産(営業秘密を含む)保護（関係法令の例：不正競争防止法(日)、著作権法(日)）

✓ (日本法の適用を想定する場合) 対象のプロセスにおいて、不正競争防止法において定義される営業秘密、限定提供データ、著作権法の定める著作物等として保護すべき種類のデータが含まれるか。

・ 機微技術管理（関係法令の例：外為法(日)、2018 年輸出管理改革法(米)）

✓ 対象のプロセスにおいて、外為法または外国の輸出管理関連法令にて規律の対象となるデータ、輸出行為に相当する種類のイベントが含まれるか。

・ 適切な社会機能の維持（関係法令の例：金融商品取引法(日)、秘密保持契約）

✓ 対象のプロセスにおいて、金融商品取引法におけるインサイダー取引関連規定、その他秘密保持契約(NDA)等により取扱いが規律されるデータが含まれるか。

適用される「場」を特定した後、それが適用される範囲を 3-2 にて特定したデータフローの範囲内で識別する。本段階のアウトプット例を図 2 に示す。図 2 では、個々の「場」とそれが考慮される範囲を四角形(枠線は点線)で記述しているが、事業者における実際の適用にあたって、これらの様式は強制されるものではない。

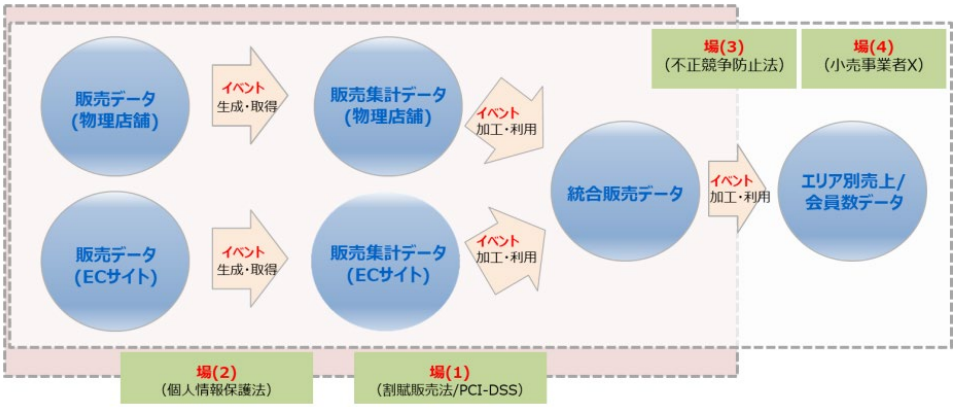


図 2 必要な制度的な保護措置の整理(例)

＜収集しておくべき情報とその情報源(例)＞

・ データ保護に関連する法令、それらの適用範囲及び、事業者に適用される規律（情報源の例：各種法令、ガイドライン文書）

・ 「場」の観点ごとに検討を深める際に利用できる参考情報として以下が挙げられる。

✓ パーソナルデータの保護

平成十五年法律第五十七号 個人情報の保護に関する法律
https://elaws.e-gov.go.jp/document?lawid=415AC0000000057
個人情報取扱事業者等に係るガイドライン・Q&A 等
https://www.ppc.go.jp/personalinfo/legal/#anc_Guide
外国における個人情報の保護に関する制度等の調査（報告書）
https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf
https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R4_03.pdf

✓ 知的財産保護

不正競争防止法の概要

https://www.meti.go.jp/policy/economy/chizai/chiteki/unfaircompetition_new.html

営業秘密管理指針

https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

限定提供データに関する指針

https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31pd.pdf

秘密情報の保護ハンドブック ～企業価値向上にむけて～（令和４年５月改訂版）

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

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

✓ 機微技術管理

輸出管理の基礎

https://cistec.or.jp/export/yukan_kiso/anpo_gaiyou/index.html

クラウドコンピューティングサービスに関する役務通達改正について

https://www.cistec.or.jp/export/jisyukanri/130627-cloud.pdf

✓ 適切な社会機能の維持

AI・データの利用に関する契約ガイドライン 1.1 版

https://www.meti.go.jp/press/2019/12/20191209001/20191209001-2.pdf

令和 3 年度我が国におけるデータ駆動型社会に係る基盤整備（データの越境流通に関連する諸外国の規制制度等調査事業）

https://www.meti.go.jp/meti_lib/report/2021FY/000377.pdf

＜実施手順＞

1. 「場」に相当する法令の規定、その他の規範を識別する。
2. 各「場」が適用される範囲を識別する。

＜作業成果物が満たすべき要件＞

・ 対象のデータ利活用プロセスに適用され得る法令、その他の規律が漏れや重複なく記載されている。
・ 識別された法令、その他の規律が適用され得る範囲がデータフロー上で記載されている。

＜作成にあたっての参考情報＞

・ DMF 添付 A 各ユースケースにおける「STEP 2 必要な制度的な保護措置（「場」）の整理」

3-4 「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。

属性としては、ユースケースの性質に応じて様々な項目が識別され得ると考えられるが、様々なケースにて共通的に適用し得ると考えられる主な項目の概要及びパラメータの例を以下に示す。

・ カテゴリ

3-3 にて特定される「場」と連動して、例えば以下のようにデータの法令等に係る位置づけ及び、管理上必要と考えられる措置を特定する。

- パーソナルデータの保護：個人データ/仮名加工情報/匿名加工情報/個人関連情報 等
- 知的財産(営業秘密を含む)保護：営業秘密/限定提供データ 等
- 機微技術管理：規制対象の技術情報 等

・ 開示範囲

関連する法令や契約による取決めや組織内規則も含め、データに定められている開示範囲(事業者、部署、担当者)を整理する。その際、3-3 にて特定される「場」との関係で考慮すべき観点の例を以下に挙げる。

- 対象データが個人情報等に該当する場合

  技術的安全管理措置の一環として、担当者及び取扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御が行われていると認められるよう開示範囲を設定する。
- 対象データが営業秘密等に該当する場合

  対象データが「秘密として管理されている」ことを確保するため、合理的と考えられる秘密管理措置の実施及び、それに対応する開示範囲を設定する。
- 対象データが契約上の規律を受ける場合

  契約等に基づいてデータを取扱ううえで、許可のない第三者への提供を認めない等の趣旨の規定が存在する場合、それに対応するよう開示範囲を制限する必要がある。

・ 利用目的

個人情報やライセンス等の取扱いにおいて、あらかじめ利用目的に制限が設けられている場合、当該目的をパラメータとして明確にしておき、後の利活用においても許可された目的からの逸脱が生じないように継続的に管理しておく必要がある。

・ データ管理主体

情報資産管理台帳等に既に規定されているもの等を参照し、対象データの管理責任者(事業者、部署、担当者)を特定する。データが複数の事業者間で共有される場合、対象のデータに対してどの事業者がいかなる管理上の責任を有しているかが不明確になりやすいと考えられる。かかるケースにおいても、事業者間の契約やサービス等の利用規約等の規定に基づき、関係者間での責任範囲の明確化を図ることが望ましい。

・ データ権利者

データ管理者とは別に、対象データに対して権利・利益を有している者(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)及びそれらに関して生じ得る措置を特定しておくことが望ましい。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い等がそれらに該当し得る。

・ 価値(重要度)

機密性、完全性、可用性の観点から生じ得る影響度等を考慮し、対象データの事業上の価値(重要度)を特定する。その際、データの分類(例：個人情報に該当するか、社内規則等で秘情報として扱うべきものか)や当該データの数量等の客観的な指標も考慮して価値算定を行うプロセスが手順化されていることが望ましい。また、ここでパラメータとして設定されるものを、組織内の情報資産管理等で既に整理されている重要度等と整合させることが望ましい。設定されるパラメータの例は以下の通り。

－ 高/中/低 等

・ 媒体・保存先

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。媒体・保存先として、設定されるパラメータの例は以下の通り。

－ 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

・ 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、関連して必要な措置を特定する。

本段階のアウトプットの例として、(1) 図２に示したフロー図の各データ(円)内に各属性項目及びパラメータを記述する方法、(2) 表形式でデータごとに属性項目に対応するパラメータを記述する方法(表１)等の様式が想定されるが、これら以外の様式の採用を否定するものではない。

表１ 「属性」の具体化方法(例)

属性項目		データA	データB	データC
カテゴリ	パーソナルデータの保護	個人データ	個人データ	匿名加工情報
	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		・・・	・・・	・・・
・・・		・・・	・・・	・・・

＜収集しておくべき情報とその情報源(例)＞

・ データの重要度、管理責任者、媒体・保存先、利用期限等 (情報源の例：情報資産管理台帳)

・ 対象プロセスにおける各データに対する事業者間の責任範囲、データの開示範囲 (情報源の例：事業者間の契約、サービスの利用規約等)

＜実施手順＞

・ 対象のプロセスにて取扱われるデータに関連して、管理すべき属性の項目を一覧化する。
・ 各データについて、上記の事例を参考に各項目のパラメータを特定する。

＜作業成果物が満たすべき要件＞

・ 上述したものを中心に、洗い出されているべき属性項目が検討され、識別されている。
・ 識別された各属性項目にもれなくパラメータが記入されている。

＜作成にあたっての参考情報＞

・ DMF 添付 A 各ユースケースにおける「STEP 3 「属性」の具体化」

3-5 「イベント」ごとのリスクの洗い出し

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する。その際、機密性(例：データ漏えい)、完全性(例：データ改ざん、破壊)、可用性(例：システム停止)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(例：パーソナルデータの保護、知的財産の保護)も踏まえてリスクを洗い出すことが有効である。その際、組織外部からのサイバー攻撃に代表される「アドバーサリ(悪意のある主体)」によるリスクだけでなく、ヒューマンエラー等の偶発的なリスク、機器の故障やソフトウェアの不具合等の構造上のリスク、自然災害等による外部環境上のリスクをそれぞれ洗い出すことで、より網羅的なリスクの洗い出しを実施することができる。また、セキュリティ対策を担当する者だけでなく、データを利活用した事業の担当者や法務担当者等の多数の視点からリスクの洗い出しや評価ができるよう、検討体制を組成することも有益である。イベント類型(生成・取得/加工・利用/移転・提供/保管/廃棄)ごとに一般的に想定されるリスクの事例については、DMF 添付 B における「B-2 イベントごとのリスクの洗い出しのイメージ」を参照されたい。

これまでのフレームワーク適用プロセスを通じて、適用主体は自身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。事業者がデータ保護等の施策に割けるリソースが限られていることを考慮すれば、特定したリスクを、影響の大きさ、起こりやすさ、現在の対策状況等の観点で評価し、優先順位づけすることが望ましい。また、かかる優先順位を決定する際には、事業担当者や法務担当者、必要な場合は社外のステークホルダーへのヒアリング等を通じて関係者間で合意形成を図るべきである。上記プロセスの結果として相対的に優先度が高いとされるリスクに対しては、より具体的な軽減策や回避策が議論される。

具体的な改善策は、特定されるリスクの種類やその影響の度合い等に依存するが、取扱われるデータの種類や環境の性質に応じて、以下を例とする様々なガイドライン等が参照され得る。なお、対策の実装にあたっては、実際のシステム構成や別途実施され得る脅威分析の結果等も踏まえて、要件定義や設計へのインプット、運用時に講じる追加の対策に反映させることが必要となる。

・ サイバーセキュリティの確保に資する対策
CPSF、ISO/IEC 27001:2013、ISO/IEC 27002:2022、NIST SP 800-53 等

・ パーソナルデータの取扱いに係る対策
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(外国にある第三者への提供編)、個人情報の保護に関する法律についてのガイドライン(仮名加工情報・匿名加工情報編) 等

・ 知的財産(営業秘密を含む)保護に資する対策
営業秘密管理指針、限定提供データ管理指針、秘密情報の保護ハンドブック ～企業価値向上にむけて～ 等

＜収集しておくべき情報とその情報源(例)＞
・ 過去に発生したインシデント等に関する情報 (情報源の例：セキュリティやデータ保護等に関する情報を取扱う各種メディア等)
・ 特定された影響度の大きい、あるいは十分に対処されていないリスクに対処する対策に関する情報(情報源の例：取扱われるデータの種類や環境の性質に応じたガイドライン等)

＜実施手順＞
・ 全体プロセスの中から、リスク特定の対象とするイベントを選択する。
・ 選択したイベントにて想定されるリスクを、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から洗い出し、一覧化する。
・ 特定したリスクを、想定される影響の大きさ、起こりやすさ、現在の対策状況等の観点から評価し、適用主体において優先的に対処すべきものを明確化する。
・ 政府機関等から公開されているガイドライン等を参照し、上記リスクを管理するために必要な措置を識別し、実行する。

＜作業成果物が満たすべき要件＞
・ 対象とするイベントにおけるリスクが、典型的に想定されるものも含め、網羅的に特定されている。
・ 特定されたリスクが、影響の大きさ、起こりやすさ、現在の対策状況等の観点で評価され、優先順位づけされている。
・ 上記の優先順位づけに基づき、ガイドラインの参照も伴いつつ、実施すべき対策が一覧化されている。

＜作成にあたっての参考情報＞
・ DMF 添付 A 各ユースケースにおける「STEP 4 「イベント」ごとのリスクポイントの洗い出し」

以上