

令和 6 年度産業サイバーセキュリティ強靱化事業
(サイバー・フィジカル・セキュリティ対策フレームワークの利活用に関する調査)

調査報告書

令和 7 年 3 月 31 日
株式会社日立製作所

目次

エグゼクティブサマリー	2
1 本事業の概要	4
1.1 目的	4
1.2 事業内容	4
1.3 実施スケジュール	7
1.4 実施体制	8
1.5 本調査報告書の構成	9
2 サイバーセキュリティに関する動向等についての調査	10
2.1 本事業項目の目的	10
2.2 本事業項目の実施内容	10
2.3 本事業項目の実施結果	11
3 CPSF 等に基づく国際標準化の推進	33
3.1 本事業項目の目的	33
3.2 本事業項目の実施内容	33
3.3 本事業項目の実施結果	33

エクゼクティブサマリー

- ・ AI や IoT、ビッグデータ等、サイバー空間とフィジカル空間を高度に融合させるシステムによって、経済発展と社会的課題の解決を両立する人間中心の社会である「Society 5.0」の実現を目指す我が国にとって、サイバー空間とフィジカル空間を高度に融合させたシステムの社会実装を進めることが必要である一方で、つながることによるネットワーク化の進展は、悪意のある者による新たな攻撃の機会にもなっていくおそれがあり、このような脅威はあらゆる産業活動に及ぶようになってきている。
- ・ このような状況下では、各企業でのサイバーセキュリティ対策に加えて、関連企業、取引先等、サプライチェーン全体としてサイバーセキュリティの確保に向けて取り組む必要があると同時に、サイバー攻撃は国境を越えて行われるものであり、そのため、サイバーセキュリティ対策も国内だけの取組では不十分であることから、欧米各国等との連携強化を通じて、我が国の取組を積極的に国際的な組織に提案するなど、国際協調を推進していくことが重要である。
- ・ 本事業では、産業サイバーセキュリティ研究会等の議論や各国政府の取組及びその他国内外のセキュリティ等に関する文献等の調査を踏まえ、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の検討及び「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」と称す）等に基づく国際標準化を目的として実施した。
- ・ 事業項目(1)「サイバーセキュリティに関する動向等についての調査」では、CPSF に関する動向を含め、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各国の取組やその他国内外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ため、既存のガイドライン等の一元的な管理・体系化を行うことを目的に「既に国内外で策定されている制度やガイドライン等の概要の調査」、「国内のガイドライン、基準に関する記載粒度、位置づけ、参照関係及び関係性等の調査」及び「今後の注力領域及び方向性(案)の整理」を実施した。
- ・ 既に国内外で策定されている制度やガイドライン等の概要の調査では、具体的に日本国内外の政府機関又は業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の概要についての調査や日本国外の政府機関又は業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細についての調査を実施した。その結果、日本では、政府及び重要インフラ分野を除く範囲では明確な省庁間の役割の切り分け等がなされておらず、サイバーセキュリティに係る各省庁や業界団体が個別にガイドラインを策定している状況であり、一元的な管理・体系化にあたっては課題が残っていることがわかった。また既存のガイドライン等の一元的な管理・体系化に関して、米国の取組は参考にはなるものの、個別のガイドラインについては、CISA や各所管省庁が個々に策定している場合があり、米国でも標準策定機能が必ずしも NIST に一元化されているとは言えないことがうかがえた。
- ・ 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の調査では、具体的に「位置づけ、参照関係、関係性等について」及び「記載内容について」の 2 つの観点で調査を実施した。その結果、前者については、サイバーセキュリティ確保のための基準への遵守が義務として定められている一方で、その基準が具体化されておらず、遵守すべき基準が不明確となっている場合があることがわかった。また、記載粒度に差異はみられるものの、ISO/IEC 27001 と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載(例:情報システムの構成要素や研修計画に盛り込む内容)が確認された。一方、後者に関しては NIST CSF(Cybersecurity Framework)と比較した際、対象となるガイドラインの要求事項がどの程度網羅されているかについて、33 の調査対象のうち、24 の基準・ガイドラインが 8 割の項目(81.8%以上:18/22 個)を満たしており、日本国内の既存の基準/ガイドラインは、少なくともコア機能のレベルでは NIST CSF の記載範囲を概ねカバーしていることがうかがえた。

-
- ・ 今後の注力領域及び方向性(案)の整理では、具体的に「文書の整理状況の可視化/今後注力すべき領域の具体化」「対処すべき現状の問題の整理」及び「今後の方向性(案)の整理」について実施した。上述の調査等も踏まえると、国内の制度やガイドライン等は大部分が体系間や体系内で整理がなされていた一方で、制度の中で遵守すべき基準が不明確となっているものもみられるなど、全ての制度やガイドライン等が体系化されているとは必ずしも言えないことから、社会全体のセキュリティレベル向上のためにも、体系化を意識した取組が必要であること及び当該取組を行うにあたり、法制度的な権限の付与やリソース面での調整が必要となることがうかがえた。
 - ・ 事業項目(2)「CPSF等に基づく国際標準化の推進」においては、CPSFをベースにした国際標準化を推進することを目的として、推進に必要な諸外国の政府、政府関連機関、業界団体又は標準化団体等によるルール形成の取組状況等の調査や、ISO/IEC及びそれに関連する会議等における必要な働きかけの実施、CPSF等に基づく国際規格(案)の作成等を実施した。具体的には、国際規格策定に向けたロードマップを策定した後、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規格の策定や維持管理を担うISO/IEC JTC1/SC27/WG4(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、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や検討を行った。
 - ・ 事業項目(3)「産業サイバーセキュリティ研究会等の運営」においては、産業サイバーセキュリティ研究会、産業サイバーセキュリティ研究会WG3、産業サイバーセキュリティ研究会WG1傘下の「サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG」、産業サイバーセキュリティ研究会WG2傘下の「サイバーセキュリティ人材の育成促進に向けた検討会」及び産業サイバーセキュリティ研究会WG3傘下の「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環(仮題)」に向けての検討会」について、構成員への委嘱作業、会議等の日程調整、開催案内(出欠確認)及び議事録の作成等といった事務的な業務を実施した。

1 本事業の概要

1.1 目的

我が国では、AI や IoT、ビッグデータ等、サイバー空間とフィジカル空間を高度に融合させるシステムにより、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となる一方で、「つながる」ことによるネットワーク化の進展は、悪意のある者にとっての新たな攻撃の機会にもなり得るおそれがある。

サイバー攻撃の起点が急激に拡大し、攻撃の手法も高度化しているため、サイバー攻撃の脅威は、あらゆる産業活動に及ぶようになってきている。このような状況下では、各企業でのサイバーセキュリティ対策に加えて、関連企業、取引先等、サプライチェーン全体としてサイバーセキュリティの確保に向けて取り組む必要がある。また、サイバー攻撃は国境を越えて行われるものであり、サイバーセキュリティ対策も国内だけの取組では不十分であり、米欧各国等との連携を強化しつつ、我が国の取組を積極的に国際的な組織に提案するなど、国際協調を推進していくことが重要である。

本事業では、産業サイバーセキュリティ研究会等の議論や各国政府の取組及びその他国内外のセキュリティ等に関する文献等の調査を踏まえ、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の検討及び CPSF 等に基づく国際標準化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 3 つの事業項目を実施した。本事業において実施した事業内容を図表 1-1 に示す。

図表 1-1 本事業の事業項目と具体的な実施内容

No	事業項目	仕様書の内容	具体的な実施内容
1	サイバーセキュリティに関する動向等についての調査	【事業内容】 本事業では、C P S F に関する動向も含め、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各国の取組やその他国内外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、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。 <調査項目例> ● 既に国内外で策定されている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） ● 国内のセキュリティ関連ガイドライン及び基準について、体系的な整理と体系化を目的とした記載 粒度、位置づけ、参照関係、関係性等についての調査 【実施方法】 ・ 公開情報（外国政府や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について、日本及び少なくとも米欧を対象として複数の国又	CPSF に関する動向を含め、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各国の取組やその他国内外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ため、既存のガイドライン等の一元的な管理・体系化を行うことを目的に「既に国内外で策定されている制度やガイドライン等の概要の調査」、「国内のガイドライン、基準に関する記載粒度、位置づけ、参照関係及び関係性等の調査」及び「今後の注力領域及び

No	事業項目	仕様書の内容	具体的な実施内容
		は地域について調査すること。 - 調査結果の妥当性確認などを目的として、必要に応じて有識者（国外の有識者やセキュリティの国際標準に精通した有識者を含む3名程度）に対して面談（リモート会議等も可）による意見交換を実施すること。 - 特に、(2)についてはISO/IEC JTC 1/SC 27 WG 4メンバーの参画が望ましく、必要に応じて国際会議（ISO/IECに係る定期会合、プロジェクト会合等の会合）に参加し、関連するISO/IECのエキスパート等と協力して可能な限り効果的な方法により行うこと。 - 調査結果、報告資料、議事録（議事概要を含む）等は日本語で作成すること。	方向性(案)の整理」を実施した。 既に国内外で策定されている制度やガイドライン等の概要の調査や国内のガイドライン、基準に関する記載粒度、位置づけ、参照関係及び関係性等の調査については、国内外において策定されている制度やガイドライン等の現状(As-Is)を調査し、国内のガイドライン等の一元的な管理・体系化を行うにあたってのあるべき姿(To-Be)を整理した。また、今後の注力領域及び方向性(案)の整理に関しては、現状(As-Is)とあるべき姿(To-Be)の比較結果から課題等を分析した上で、既存のガイドライン等の一元的な管理・体系化を行うための方向性(案)を作成した。
2	CPSF等に基づく国際規格の推進	【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等をベースにして国際標準化を推進する。具体的には、ISO/IEC JTC 1/SC 27のプロジェクトとして、NP投票を経て原案（WD）の作成段階へ移行したISO/IEC TS 5689について令和6年度中にFDIS投票を開始し、令和7年度初めの国際規格発行を目指し、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理、リスク評価、セキュリティ対策に関する、諸外国の政府又は政府関連機関、業界団体のルール形成の取組状況等の動向を調査しつつ、技術仕様書（TS）の策定に必要な働きかけや検討を行う。 ＜想定する調査項目の例＞ - CPSF等に基づく国際規格策定に向けた具体的なロードマップの提示 - ロードマップに基づく国内外の関係機関や関係者の巻き込みや	CPSFをベースにした国際標準化を推進することを目的として、推進に必要な諸外国の政府、政府関連機関、業界団体又は標準化団体等によるルール形成の取組状況等の調査や、ISO/IEC及びそれに関連する会議等における必要な働きかけの実施、CPSF等に基づく国際規格(案)の作成等を実施した。具体的には、国際規格策定に向けたロードマップを策定した後、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

No	事業項目	仕様書の内容	具体的な実施内容
		そのために必要な資料の作成等 ● C P S F 等に基づく国際規格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・認証等に関する国際規格、ガイドライン、フレームワーク、政策文書等の調査 上記（１）及び（２）は、国内外の公的機関や標準化機関の公表資料、専門誌等の文献、インターネット等の調査、意見交換等により実施する。意見交換の相手（国内外における公的機関、有識者、組織）及び内容は、本事業の実施者が提案して担当者と協議の上で決定する。 【実施方法】 ・ 公開情報（外国政府や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について、日本及び少なくとも米欧を対象として複数の国又は地域について調査すること。 ・ 調査結果の妥当性確認などを目的として、必要に応じて有識者（国外の有識者やセキュリティの国際標準に精通した有識者を含む３名程度）に対して面談（リモート会議等も可）による意見交換を実施すること。 ・ 特に、（２）については I S O / I E C J T C 1 / S C 2 7 W G 4 メンバーの参画が望ましく、必要に応じて国際会議（I S O / I E C に係る定期会合、プロジェクト会合等の会合）に参加し、関連する I S O / I E C のエキスパート等と協力して可能な限り効果的な方法により行うこと。 ・ 調査結果、報告資料、議事録（議事概要を含む）等は日本語で作成すること。	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規格の策定や維持管理を担うISO/IEC JTC 1/SC 27/WG4(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、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や検討を行った。
3	研究会等の運営	【事業内容】 本事業では、３．（１）の調査に関連し、専門的な視点からの検討、分析及び助言を得るために、以下に示す研究会（以下、「研究会等」という。）の運営を行うこと。①産業サイバーセキュリティ研究会：産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者・学識者等から構成される会 ②WG 1（制度・技術・標準化）、及び分野横断SWG（WG 1と同時に開催）：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会 ③WG 2（経営・人材・国際）：サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際 戦略を議論する会 ④WG 3（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	産業サイバーセキュリティ研究会、産業サイバーセキュリティ研究会WG3、産業サイバーセキュリティ研究会WG1傘下の「サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG」、産業サイバーセキュリティ研究会WG2傘下の「サイバーセキュリティ人材の育成促進に向けた検討会」及び産

No	事業項目	仕様書の内容	具体的な実施内容
		と国際プレイヤー創出に係る政策を議論する会 ⑤担当者との相談により、新たに設置することになった研究会 上記①～④は、令和6年度中にそれぞれ1回の開催を想定している。①～④の構成員は担当者が指定するものとし、①産学を代表する有識者10名程度、②産学の有識者15～20名程度、③④産学の有識者10～15名程度とし、⑤の構成員等の詳細は担当者と協議の上で決定するものとする。構成員は、前回開催時の委員等名簿（注釈参照）に記載の者とするが、本事業での開催において若干名の交代や増減が生じる場合がある点に留意すること。 【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、会場設営、受付、会議運営に必要な備品等の準備、議論する資料の準備／印刷、議事録の作成等といった事務的な業務を全て行い、議事録は開催後に速やかに作成して担当者に提出すること。 - 構成員に対する謝金、旅費等の支払いを行うこと。 - オンサイト開催の場合は、基本的に経済産業省（又は近郊）で開催するものとするが、経済産業省以外の開催となった場合は会場を用意すること。リモート開催の場合は、経済産業省が指定するオンライン会議システム（Teamsを想定）により会議を主催すること。 - 令和5年度に開催した研究会等に関する事務的な業務（議事録の作成等）を事後的に実施する必要がある場合、担当者と協議の上で決定すること。 - 実施に係る経費については事業費に計上すること。 - 研究会等の資料のうち、国際協調及び我が国の取組の海外発信の観点に基づき、担当者との協議に基づいて必要と判断した資料について英訳を行うこと。 - 上記3.（3）⑤の新たに設置することになった研究会については、「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」程度の開催頻度、構成員数、資料を想定している。	業サイバーセキュリティ研究会WG3傘下の「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環(仮題)」に向けた検討会」について、構成員への委嘱作業、会議等の日程調整、開催案内(出欠確認)及び議事録の作成等といった事務的な業務を実施した。

1.3 実施スケジュール

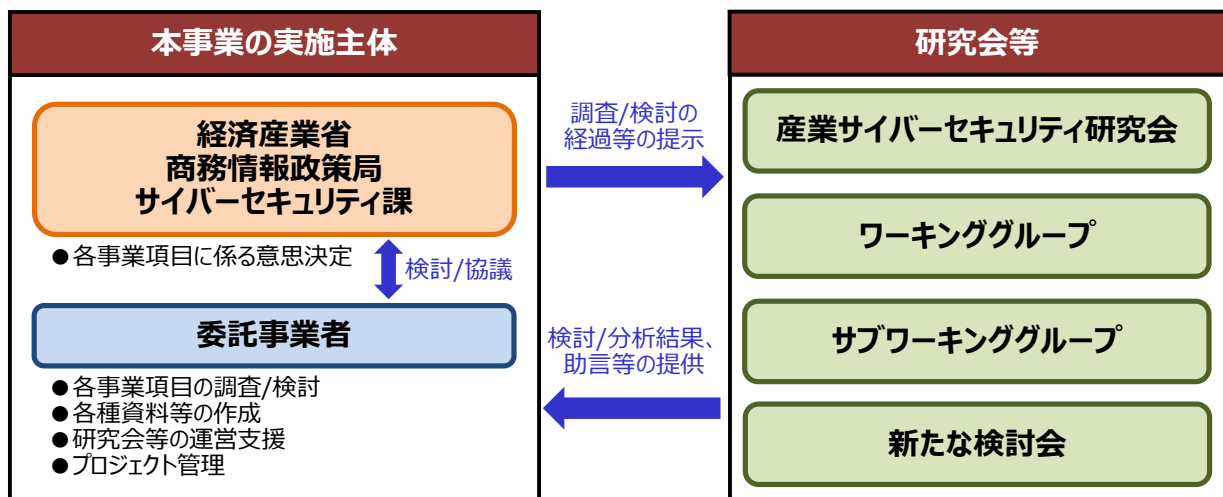
事業の実施スケジュールを図表 1-2 に示す。「CPSF に関する動向等についての調査」、「CPSF 等に基づく国際規格の推進」及び「研究会等の運営」について、産業サイバーセキュリティ研究会、WG、ならびに新たに設置した検討会等における議論や助言を踏まえて内容の検討を推進した。

図表 1-2 本事業の実施スケジュール

事業項目		令和6年度											
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
プロジェクト計画の立案	プロジェクト計画書の作成	●→											
(1) サイバーセキュリティに関する 動向等についての調査	(1) 既に国内外で策定されている制度やガイドライン等の概要についての調査	●	→										
	(2) 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等についての調査					●	→						
	(3) 注目領域の特定/今後の方向性(案)の整理								●	→			
	(4) ベンチマークとする国内外の取組みの調査								●	→			
(2) CPSF等に基づく国際標準化の推進	(1) 国際規格策定に向けたロードマップの策定	●	→										
	(2) 国内外の関係機関・関係者の巻き込み	●	→						▲同会合				▲同会合
	(3) CPSF等に基づく国際規格(案)の作成					WD作成	意見募集	WD作成	意見募集				●→
	(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	●	→										
(3) 産業サイバーセキュリティ 研究会等の運営	産業サイバーセキュリティ研究会	▲第8回											
	WG3 (サイバーセキュリティビジネス化)	▲第8回											
	サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG				▲第1回	▲第2回			▲第3回		▲第4回		
	サイバーセキュリティ人材の育成促進に向けた検討会			▲第1回	▲第2回			▲第3回			▲第4回	▲第5回	
	「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環(仮題)」に向けての検討会				▲第1回	▲第2回	▲第3回	▲第4回	▲第5回	▲第6回	▲第7回		
	報告書のとりまとめ											●→	

1.4 実施体制

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



図表 1-3 本事業の実施体制

1.5 本調査報告書の構成

本調査報告書では、3つ提示されている事業項目のうち、「研究会等の運営」を除いた、「CPSF に関する動向等についての調査」、「CPSF 等に基づく国際規格の推進」について、それぞれ目的、実施内容、実施結果を報告する。

- 第2部では、「CPSF に関する動向等についての調査」の目的、実施内容及び実施結果を報告する。
- 第3部では、「CPSF 等に基づく国際規格の推進」の目的、実施内容及び実施結果を報告する。

2 サイバーセキュリティに関する動向等についての調査

2.1 本事業項目の目的

本事業項目では、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の検討の一環で、CPSF に関する動向も含め、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各国の取組やその他国内外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ことを目的とした。

2.2 本事業項目の実施内容

各国の取組やその他国内外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にあたり、サプライチェーン全体でのサイバーセキュリティ確保に必要な事項の 1 つとして、政府側でのガイドライン等の一元的な管理、体系化が挙げられた。そこで、貴省担当者との協議の上、既存のガイドライン等の一元的な管理・体系化を行うことを見据え、各国の取組やその他国内外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した。具体的には以下の項目について調査を行った。調査結果の詳細を別紙 1 から別紙 3 に示す。

また、企業のセキュリティ対策基準の明確化の一環で、「サプライチェーン強化に向けたセキュリティ対策評価制度」についても検討を行った。検討結果の詳細を別紙 4 に示す。

＜本事業項目の調査内容＞

1. 既に国内外で策定されている制度やガイドライン等の概要の調査
2. 国内のガイドライン、基準に関する記載粒度、位置づけ、参照関係及び関係性等の調査
3. 今後の注力領域及び方向性(案)の整理

上記 1.や 2.に関し、国内外において策定されている制度やガイドライン等の現状(As-Is)を調査した上で、3.1 で国内のガイドライン等の一元的な管理・体系化を行うにあたってのあるべき姿(To-Be)を整理した。3.では、現状(As-Is)とあるべき姿(To-Be)の比較結果から課題等を分析した上で、既存のガイドライン等の一元的な管理・体系化を行うための方向性(案)を作成した。

調査内容の詳細を以下に示す。

1. 既に国内外で策定されている制度やガイドライン等の概要の調査

- 1.1 国内で策定されている制度やガイドライン等の概要
日本国内外の政府機関又は業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の概要について調査する。
- 1.2 国外で策定されている制度やガイドライン等の概要
日本国外の政府機関又は業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細について調査する。

2. 国内のガイドライン、基準に関する記載粒度、位置づけ、参照関係及び関係性等の調査

- 2.1 業種横断
日本国内の政府機関又は業界団体等が公開する業種横断のサイバーセキュリティに関するガイドライン及び基準の詳細について調査する。
- 2.2 業種別
日本国内の政府機関又は業界団体等が公開する業種別のサイバーセキュリティに関するガイドライン及び基準の詳細について調査する。

3. 今後の注力領域及び方向性(案)の整理

- 3.1 文書のあるべき姿の具体化/文書の整理状況の可視化
あるべき姿を具体化した上で、文書の整理状況を可視化する。
- 3.2 対処すべき現状の問題の整理
1.及び 2.で調査を行った結果を踏まえつつ、あるべき姿と比較した際に生じているギャップを対処すべき問題として整理する。
- 3.3 今後の方向性(案)の整理
国内外の取組を踏まえつつ、既存のガイドライン等の一元的な管理・体系化を行うための方向性(案)を具体化する。

図表 2-1 調査内容の概要

分類	調査項目	
1. 既に国内外で策定されている制度やガイドライン等の概要の調査		
1.1 国内で策定されている制度や ガイドライン等の概要	1.1.1 業種横断のガイドライン	日本国内外の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の概要について調査した。
	1.1.2 業種別のガイドライン	
	1.1.3 まとめ	
1.2 国外で策定されている制度や ガイドライン等の概要	1.2.1 米国における制度やガイドライン等	日本国内の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細について調査した。
	1.2.2 欧州における制度やガイドライン等(EU加盟国及び英国)	
	1.2.3 国際機関(ISO/IEC、ITU-T)における制度やガイドライン等	
	1.2.4 まとめ	
2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の調査		
2.1 業種横断	2.1.1 情報システム関連	日本国内の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細について調査した。
	2.1.2 制御システム関連	
	2.1.3 製品・サービス関連	
	2.1.4 IoT・CPS関連	
	2.1.5 その他	
2.2 業種別	2.2.1 政府情報システム	
	2.2.2 重要インフラ(15業種)	
	2.2.3 重要インフラ以外	
3. 今後の注力領域及び方向性(案)の整理		
3.1 文書のあるべき姿の具体化/ 文書の整理状況の可視化	3.1.1 文書のあるべき姿の具体化	1及び2で調査を行った対象を踏まえつつ、あるべき姿を具体化した上で、対処すべき現状の問題を整理し、今後の方向性(案)の整理を行った。
	3.1.2 文書の整理状況の可視化	
3.2 対処すべき現状の問題の整理	-	
3.3 今後の方向性(案)の整理	-	

2.3 本事業項目の実施結果

2.3.1 既に国内外で策定されている制度やガイドライン等の概要の調査

本項では、国内外の政府機関又は業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の概要について調査した。以下の2つから調査結果を示す。

- ① 国内で策定されている制度やガイドライン等の概要
- ② 国外で策定されている制度やガイドライン等の概要

① 国内で策定されている制度やガイドライン等の概要

国内で策定されている制度やガイドライン等のうち、貴省担当者と協議の上、特に重要と考えられる制度やガイドラインの概要を業種横断及び業種別に調査した。

業種横断のガイドラインは、認証制度に係るものを主な調査対象とした。業務別のガイドラインは、重要インフラ分野に係るものを調査対象とした。ただし、調査開始時点の2024年5月までに公開されているものを対象としている。

- 業種横断
- 業種別

● 業種横断

➤ **ISMS 適合性評価制度**

ISMS 認証の取得を希望する団体を対象として、組織の構築した ISMS が JIS Q 27001(ISO/IEC 27001) に基づいて適切に運用管理されているかを第三者である ISMS 認証機関が認証する制度。

➤ **ISMS クラウドセキュリティサービス認証**

認証取得を希望するクラウドサービスプロバイダや認証取得を希望するクラウドサービスカスタマを対象とした制度。通常の ISMS 認証に加えて、クラウドサービス固有の管理策 (ISO/IEC 27017) が適切に導入、実施されていることを認証する。

➤ **CSMS 適合性評価制度**

CSMS 認証の取得を希望する団体を対象とした制度。産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対して第三者が認証する。

➤ **端末機器の基準認証制度(技術基準適合認定の場合)**

製造事業者を対象として、電気事業法に基づき、事業者のネットワークに接続して使用される端末機器(その設計含む)について「接続の技術基準」に適合していることを登録認定機関等が認定する制度

➤ **政府機関等のサイバーセキュリティ対策のための統一基準群**

政府機関や独立行政法人等を対象としており、サイバーセキュリティ基本法に基づく、政府機関及び独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み

図表 2-2 サマリ(業種横断)

	ISMS適合性評価制度	ISMSクラウドセキュリティ認証	CSMS適合性評価制度	端末機器の基準認証制度	政府機関等のサイバーセキュリティ対策のための統一基準群
種別*1	制度	制度	制度	制度	基準
遵守義務	なし	なし	なし	あり	あり
対象分野・システム	・ 情報システム全般	・ クラウドサービス	・ 産業用オートメーション及び制御システム	・ 端末機器*2	・ 政府情報システム
対象者	・ ISMS認証の取得を希望する団体	・ 認証取得を希望するクラウドサービスプロバイダ ・ 認証取得を希望するクラウドサービスカスタマ	・ CSMS認証の取得を希望する団体	・ 製造事業者	・ 政府機関 ・ 独立行政法人 等
概要	・ 第三者であるISMS認証機関が、組織の構築したISMSが <u>ISO/IEC 27001(JIS Q 27001)に基づいて適切に運用管理されているかを証明する制度。</u>	・ 通常の ISMS認証に加えて 、クラウドサービス固有の管理策(<u>ISO/IEC 27017</u>)が <u>適切に導入、実施されていることを認証する。</u>	・ <u>産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度。</u>	・ 電気事業法に基づき、事業者のネットワークに接続して使用される端末機器(その設計含む)について「 <u>接続の技術基準</u> 」に適合していることを登録認定機関等が認定する制度。	・ 政府統一基準は、サイバーセキュリティ基本法に基づく、 <u>政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み。</u>

*1 制度/基準/ガイドラインにて分類

*2 端末機器は、アナログ電話用設備、インターネットプロトコル電話用設備、インターネットプロトコル移動電話用設備、無線呼出用設備、総合デジタル通信設備、専用通信回線設備

- 業種別

- **重要インフラのサイバーセキュリティに係る行動計画**

サイバーセキュリティ戦略を踏まえ、サイバーセキュリティ法第 4 条及び第 26 条の規定に基づき策定するもの。①「重要インフラ防護」の目的、②関係主体の責務、③基本的な考え方、④障害対応体制の強化に向けた取組等を規定。

- **重要インフラのサイバーセキュリティに係る安全基準等策定指針**

重要インフラ事業者等を対象として、重要インフラ行動計画に示された重要インフラにおける機能保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、「安全基準等」において規定が望まれる項目を整理・記載。

- **金融機関等コンピュータシステムの安全対策基準・解説書(第 12 版)**

日本の金融機関等が、事業展開を行ううえで金融情報システムを活用するに際し、開発や導入、運用等において必要と考えられる安全対策を基準として示すとともに、基準項目ごとに、具体的な事例を交えて解説するもの。

- **電気通信分野におけるサイバーセキュリティに係る安全基準**

電気通信事業者や電気通信設備提供者(メーカ等)を対象として、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準について業界団体が定めるガイドラインを、政府指針に基づき策定したもの。

- **電力制御システムセキュリティガイドライン**

電気事業者が施設する電力制御システム等に携わる者を対象として、電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載したもの。

- **自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン**

自家用電気工作物を設置する者を対象として、自家用電気工作物の遠隔監視システム等や制御システム等のライフサイクルにおけるサイバーセキュリティについて規定したもの。

- **地方公共団体における情報セキュリティポリシーに関するガイドライン**

地方公共団体における情報セキュリティポリシーの策定を行う者やセキュリティ上の職責を担う者を対象として、情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。

- **医療情報システムの安全管理に関するガイドライン**

医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象として、e-文書法等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したもの。

- **水道分野における情報セキュリティガイドライン**

水道事業者や水道用水供給事業者を対象として、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示したもの。

- **物流分野における情報セキュリティ確保に係る安全ガイドライン**

物流分野の重要インフラ事業者等を対象としてセキュリティ管理策の水準を示すことで、個々の重要インフラ事業者等が、重要インフラの担い手としての意識に基づいて自主的に取り組み、対策の実施や検証に当たっての目標を定めることを目的とするガイドライン。

- **クレジットカード・セキュリティガイドライン**

加盟店/カード会社/決済代行業者等やその事業者が対策を実施するに際し協力等を行う団体を対象として、安全・安心なクレジットカード利用環境を整備するため、関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。

- **装備品等及び役務の調達における情報セキュリティ基準**

防衛関連企業において保護すべき情報に接する全ての者を対象として、調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。

図表 2-3 サマリ(業種別(1/2))

	重要インフラのサイ バーセキュリティに係 る行動計画	重要インフラのサイ バーセキュリティに係 る安全基準等策定 指針	金融機関等コン ピュータシステムの安 全対策基準・解説書 (第12版)	電気通信分野におけ るサイバーセキュリティ に係る安全基準	電力制御システムセ キュリティガイドライン	自家用電気工作物 に係るサイバーセキュ リティの確保に関する ガイドライン
種別 ^{*1}	制度	ガイドライン	基準	ガイドライン	基準	基準
遵守義務	なし	なし	あり ^{*2}	なし	あり ^{*3}	あり ^{*4}
対象分野・シ ステム	・ 重要インフラ分野	・ 重要インフラ分野	・ 金融情報システム	・ 電気通信分野	電力制御システムや 電力制御用ネットワ ーク	・ 自家用電気工作 物の遠隔監視シス テム等、制御シス テム等
対象者	・ 政府機関 ・ 重要インフラ事業者 ・ サプライチェーン等 に関わる事業者	・ 重要インフラ事業 者等	・ 金融機関 等	・ 電気通信事業者 ・ 電気通信設備提 供者(メーカ等)	・ 電気事業者が施 設する電力制御シ ステム等に携わる 者	・ 自家用電気工作 物を設置する者
概要	・ サイバーセキュリティ 戦略を踏まえ、同 法第4条及び第26 条の規定に基づき 策定するもの。 ・ ①「重要インフラ防 護」の目的、②関 係主体の責務、③ 基本的な考え方、 ④障害対応体制の 強化に向けた取組 等を規定。	・ 重要インフラ行動計 画に示された重要イ ンフラにおける機能 保証の考え方を踏 まえ、重要インフラ サービスの安全かつ 持続的な提供の実 現を図る観点から、 「安全基準等」にお いて規定が望まれる 項目を整理・記載 している。	・ 日本の金融機関等 が、事業展開を行う うえで金融情報シ ステムを活用するに 際し、開発や導入、運 用等において必要と 考えられる安全対 策を基準として示す とともに、基準項目 ごとに、具体的な事 例を交えて解説する もの。	・ 電気通信分野にお ける「安全基準等」 の一つとして、電気 通信分野の特性を 踏まえ、取り組みこ とが望ましいと考えら れる情報セキュリティ 対策の基準につい て業界団体が定め るガイドラインを、政 府指針に基づき策 定したもの。	・ 本ガイドラインは、電 力制御システム等 のサイバーセキュリ ティ確保を目的とし て、電気事業者が 実施すべきセキュリ ティ対策の要求事 項について記載した もの。	・ 本ガイドラインは、自 家用電気工作物の 遠隔監視システム 等や制御システム 等のライフサイクルに おけるサイバーセキュ リティについて規定し たもの。

*1 制度/基準/ガイドラインにて分類

*2 あくまでも自主基準とされており強制力はないとされているが、預金等受入金融機関にとって本ガイドラインが実質的な義務となっている可能性がある。

*3 本ガイドラインは勧告的事項と推奨的事項を定めているが、「審言基準」として位置付けられている「技術基準の解釈」によって引用されているため、実質的には義務となっている。

*4 勧告的事項に該当する場合は遵守義務があるが、推奨的事項の場合には遵守義務はない。

図表 2-4 サマリ(業種別(2/2))

	地方公共団体におけ る情報セキュリティポ リシーに関するガイド ライン	医療情報システムの 安全管理に関するガイ ドライン	水道分野における情 報セキュリティガイド ライン	物流分野における情 報セキュリティ確保に 係る安全ガイドライン (貨物自動車運送/ 倉庫)	クレジットカード・セ キュリティガイドライン	装備品等及び役務 の調達における情報 セキュリティ基準
種別 ^{*1}	基準	基準	ガイドライン	ガイドライン	基準	基準
遵守義務	あり ^{*1}	あり ^{*2}	なし	なし	あり	あり
対象分野・シ ステム	・ 地方公共団体	・ 医療情報システム	・ 水道情報システム	・ 物流情報システム	クレジットカード分野	・ 防衛分野
対象者	・ 情報セキュリティポ リシーの策定を行う 者 ・ セキュリティ上の職 責を担う者	・ 医療機関等におい て、すべての医療 情報システムの導 入、運用、利用、 保守及び廃棄に 関わる者	・ 水道事業者 ・ 水道用供水供給事 業者	・ 物流分野の重要イ ンフラ事業者等	・ 加盟店/カード会 社/決済代行業者 等 ^{*3} ・ 上記の事業者が 対策を実施するに 際し協力等を行う 団体	・ 防衛関連企業に おいて保護すべき 情報に接する全て の者 ^{*4}
概要	・ 本ガイドラインは、各 地方公共団体が情 報セキュリティポ リシーの策定や見直 しを行う際の参考と して、情報セキュリ ティポリシーの考え 方及び内容について 解説したもの。	・ 本ガイドラインは、 e-文書法等の法令 等への適切な対応 を行うため、技術的 及び運用管理上の 観点から所要の対 策を示したものであ る。	・ 水道事業者等にお いて実施することが 必要な又は望まれ る情報セキュリティ 対策の項目及び水 準を示したもの。 ・ 「重要インフラにお ける情報セキュリティ 確保に係る安全基 準等策定指針(第 5版)」における「安 全基準等」に位置 づけられるもの。	・ セキュリティ管理策 の水準を示すことで、 個々の重要インフラ 事業者等が、重要 インフラの担い手とし ての意識に基づいて 自主的に取り組み、 対策の実施や検証に 当たっての目標を 定めることを目的と する。	・ 安全・安心なクレ ジットカード利用環 境を整備するため、 関係事業者が実施 すべきクレジットカード 情報漏えい及び不正 利用の防止のための セキュリティ対策の 取組を取りまとめた もの。	・ 本基準は、装備品 等及び役務の調達に 係る企業において、 当該調達に係る保 護すべき情報の適 切な管理を目指し、 防衛省として求める 対策を定めたもの。

*1 ポリシーの策定は義務であるが、ガイドラインに記載された具体的な項目の記載は必ずしも義務ではない。また、総務大臣通知による要請によって、対策の実施が義務となる場合がある。

*2 本ガイドラインにおいて優先的に取り組むべき事項を整理したチェックリストは立入検査の際に参照されるため、実質的に義務となっている可能性がある。

*3 セキュリティ対策の実施主体である「加盟店」や「カード会社(イシュアー・アクワイアー)」、「決済代行業者等(4号事業者)」、「コード決済事業者等(5号事業者)」、「コード決済事業者等の委託会社(6号事業者)」、「加盟店向け決済システム提供事業者(7号事業者)」

*4 防衛調達に関わる企業に対して遵守を義務付け

② 国外で策定されている制度やガイドライン等の概要

国外で策定されている制度やガイドライン等のうち、貴省担当者と協議の上、米国、欧州、英国、国際関連における制度やガイドラインの概要を調査した。

- 米国
- 欧州
- 英国
- 国際

- 米国

米国の制度やガイドライン等には、その既存のガイドライン等の一元的な管理・体系化にあたって参考となる点がみられたことから、米国の制度やガイドライン等の調査では、個別の制度やガイドライン等の関係性を整理した上で、[縦の関係性] 制度/基準/ガイドライン間の参照関係及び[横の関係性] ガイドライン間の参照関係から特徴を整理した。

<[縦の関係性] 制度/基準/ガイドライン間の参照関係>

- 連邦情報セキュリティ近代化法(FISMA)によって、義務的標準として NIST に標準(SP 800-53)の策定を指示している。また、FIPS199/200 において政府情報システムのレベルについて考え方を示している。
- 大統領令によって明確な位置づけがなされた上で、NIST において標準が策定されている。

<[横の関係性] ガイドライン間の参照関係>

- NIST SP800-53 を中心として、この文書を補足される形で NIST SP800 シリーズが策定されており、文書ごとの位置づけが明確化されている。
- FedRAMP の基準は、NIST SP800-53 をもとに作成されている。クラウドサービス固有の対策やパラメータが設定されており、上記と同様、FedRAMP の基準は NIST SP800-53 を中心とした文書の 1 つとして捉えられる。
- NIST Cybersecurity Framework(以下「NIST CSF」という。)に基づき、個別分野(特に重要インフラ分野)において実装ガイドラインが策定されている。
- ただし、NIST CSF は任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。各省庁の権限で基準が策定されているものもみられる。

図表 2-5 体系化の観点でみられた特徴と文書(例)

	体系化の観点でみられた特徴	文書(例)
制度/基準/ ガイドライン間の 参照関係 ↑ ↓ 縦の関係性	- 連邦情報セキュリティ近代化法(FISMA)によって、義務的標準としてNISTに標準(SP 800-53)の策定を指示している。また、FIPS199/200において政府情報システムのレベルについて考え方を示している。 - 大統領令によって明確な位置づけがなされた上で、NISTにおいて標準が策定され、OMBによる指令によって各省庁に準拠を要求している。	- FISMAとFIPS199/200、NIST SP800-53 - 大統領令14028、M-21-30、NIST SP800-213
ガイドライン間の 参照関係 △ ↔ △ 横の関係性	- NIST SP800-53を中心として、この文書を補足される形でNIST SP800シリーズが策定されており、文書ごとの位置づけが明確化されている。 - FedRAMPの基準は、NIST SP800-53をもとに作成されている。クラウドサービス固有の対策やパラメータが設定されており、上記と同様、FedRAMPの基準はNIST SP800-53を中心とした文書の1つとして捉えられる。 - NIST CSFに基づき、個別分野(特に重要インフラ分野)において実装ガイドラインが策定されている。 - ただし、NIST CSFは任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。各省庁の権限で基準が策定されている。	- NIST SP800-53とNIST SP800-63、171 等 - NIST SP800-53とFedRAMP Baselines - NIST CSF、Implementation Guidance(例:交通分野、化学分野) - HIPPA security rules Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

- 欧州

欧州において、近年その影響が大きく、特に重要と考えられる制度やガイドラインの概要を示す。

 - **EU Cyber Resilience Act**

デジタル要素を含む製品やソフトウェアを購入又は使用する消費者や企業を保護することを目的とした規定。このような製品の製造業者や小売業者に対してサイバーセキュリティに関する義務的な要件を導入することで、不十分なセキュリティ機能をなくし、この保護が製品のライフサイクル全体に及ぶようにするもの。
 - **The EU cybersecurity certification framework**

本認証の枠組みは、包括的な規則、技術要件、基準、手続きをセットとした EU 全体の認証スキームを提供する。このスキームに従って認証された ICT 製品やサービスは、指定された要件に適合していることを証明する。
 - **NIS2 指令**

EU 域内でサービスを提供する又は活動を行う中規模(従業員 50 名)以上の主要エンティティ又は重要エンティティを対象にした規制であり、化学、医療機器、電気電子機器、光学機器、機械、自動車、輸送機器、宇宙、研究などの幅広い分野を対象としている。NIS から NIS2 での変更点は、①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金の設定。

図表 2-6 サマリ(欧州)

	EU Cyber Resilience Act	The EU cybersecurity certification framework	NIS2指令
種別*1	制度	制度	制度
遵守義務	あり	なし	あり*2
対象分野・システム	デジタル製品	ICT製品やサービス	- 主要エンティティ分野*3 - 重要エンティティ分野*4
対象者	- デジタル要素を含む製品やソフトウェアの製造事業者 - デジタル要素を含む製品やソフトウェアの小売事業者	ENISA	- 主要エンティティ - 重要エンティティ
概要	本法は、デジタル要素を含む製品やソフトウェアを購入または使用する消費者や企業を保護することを目的としている。このような製品の製造業者や小売業者に対してサイバーセキュリティに関する義務的な要件を導入することで、不十分なセキュリティ機能をなくし、この保護が製品のライフサイクル全体に及ぶようにするもの。	本認証の枠組みは、包括的な規則、技術要件、基準、手続きをセットとしたEU全体の認証スキームを提供する。このスキームに従って認証されたICT製品やサービスは、指定された要件に適合していることを証明する。	- NIS2指令は、EU域内でサービスを提供するまたは活動を行う中規模(従業員50名)以上の主要エンティティまたは重要エンティティを対象にした規制であり、化学、医療機器、電気電子機器、光学機器、機械、自動車、輸送機器、宇宙、研究などの幅広い分野を対象に義務がかかる。 - NISからNIS2での変更点は、①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金。

- 英国

英国において、近年その影響が大きく、特に重要と考えられる制度やガイドラインの概要を示す。

 - **PSTI 法**

英国の消費者向けの接続可能な製品(又は「スマート」製品)の製造業者に対して、同法に定められた関連義務を遵守することを義務づけるもの。具体的な要件は、2023 年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則にて規定。
 - **Government Functional Standard**

機能基準は、独立行政法人の常任秘書、事務局長、最高経営責任者等を対象として、政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を示す文書。どのように業務を行うかは、関連する実務やガイダンスで定められている。

➤ **Cyber Essentials**

政府が支援するサイバーセキュリティ認証制度。規模の大小にかかわらず、最も一般的なサイバー攻撃全般から組織を保護するのに役立つとされる。Cyber Essentials 及び Cyber Essentials Plus という 2 種類の認証を設けている。

➤ **The Security of Network & Information Systems Regulations**

デジタル・サービスや必須サービスの運営者を対象として、デジタル・サービスや必須サービスの提供に不可欠なネットワークや情報システムのセキュリティ(サイバーと物理的な回復力の両方)の全体的なレベルを高めるための法的措置を提供する。

図表 2-7 サマリ(英国)

	PSTI法	Government Functional Standard	Cyber Essentials	The Security of Network & Information Systems Regulations
遵守義務	あり	あり	なし	あり
対象分野・システム	英国の消費者向けの接続可能な製品	政府のセキュリティ活動の計画、実施、管理に適用	業種や組織規模、システムの制約なし	- デジタルサービス^{*1} - 必須サービス^{*2}
対象者	英国の消費者向け接続可能な製品の製造事業者/輸入業者/販売事業者	独立行政法人の常任秘書、事務局長、最高経営責任者等		デジタル・サービスや必須サービスの運営者
概要	- 英国の消費者向けの接続可能な製品(または「スマート」製品)の製造業者に対して、<u>同法に定められた関連義務を遵守することを義務づける</u>。 - 具体的な要件は、2023 年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則にて規定	- 機能基準は、政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を実施するための主要な参考文献。 <u>どのように業務を行うかは、関連する実務やガイダンスで定められている。</u>	- 政府が支援する<u>サイバーセキュリティ認証制度</u>。 - 規模の大小にかかわらず、最も一般的なサイバー攻撃全般から組織を保護するのに役立つとされる。 - Cyber Essentials及び Cyber Essentials Plus という2種類の認証を設けている。	本規則は、デジタル・サービスや必須サービスの提供に不可欠なネットワークや情報システムのセキュリティ(サイバーと物理的な回復力の両方)の<u>全体的なレベルを高めるための法的措置を提供する</u>。

● 国際

セキュリティの文脈で特に重要と考えられる国際標準についてその概要を示す。

➤ **ISO/IEC 27001:2022**

本規格は、情報セキュリティマネジメントシステム(ISMS)を確立、実施、維持、継続的に改善するための要求事項を提供することを目的としている。

➤ **IEC 62443 シリーズ**

制御システムのアセットオーナーや制御システムのシステムインテグレーター、制御関連製品の製品供給者を対象として、IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群。

➤ **ISO/IEC 15408-1:2022**

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。

➤ **ISO/IEC 27402:2023**

IoT サービスプロバイダや IoT サービスデベロッパ、IoT ユーザーを対象として、IoT 機器がセキュリティとプライバシーの管理をサポートできるように、情報通信技術(ICT)要件のベースライン・セットを提供する。

➤ **ISO/IEC 27017:2015**

クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提供する。

図表 2-8 サマリ(国際)

	ISO/IEC 27001:2022	IEC 62443シリーズ	ISO/IEC 15408-1:2022	ISO/IEC 27402:2023	ISO/IEC 27017:2015
種別 ^{*1}	基準	基準	基準	基準	基準
遵守義務	なし	なし	なし	なし	なし
対象分野・システム	(業種・業態を問わない)	産業用オートメーション及び制御システム	情報技術を用いた製品やシステム全般	IoT機器分野	クラウドサービス分野
対象者	あらゆる組織が利用し、認証を取得可能。	制御システムのアセット・オーナー 制御システムのシステムインテグレーター 制御関連製品の製品供給者	-	IoTサービスプロバイダ IoTサービスデベロッパ IoTユーザ	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
概要	本規格は、 <u>情報セキュリティマネジメントシステム(ISMS)を確立、実施、維持、継続的に改善するための要求事項を提供することを目的として作成。</u>	IEC 62443シリーズは、 <u>IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群。</u>	本規格は、情報技術セキュリティの観点から、 <u>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。</u>	本規格は、 <u>IoT機器</u> がセキュリティとプライバシーの管理をサポートできるように、 <u>情報通信技術(ICT)要件のベースライン・セットを提供する。</u>	本規格は、 <u>クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提供する。</u>

③ 小括

①及び②の調査結果を踏まえて、各国、地域で制度やガイドライン塔の管理状況と体系化の状況を整理した。

日本では、政府及び重要インフラ分野を除く範囲では明確な省庁間の役割の切り分け等がなされておらず、サイバーセキュリティに係る各省庁や業界団体が個別にガイドラインを策定している状況であり、一元的な管理・体系化にあたっては課題が残っている。

前述の通り、既存のガイドライン等の一元的な管理・体系化にあたって米国の取組は参考になるが、個別のガイドラインについては、CISA や各所管省庁が個別に策定している場合がみられ、米国でも標準策定機能が必ずしも NIST に一元化されているとは言えない。

● 日本:

[管理状況]

- 重要インフラ分野では、内閣サイバーセキュリティセンター(以下「NISC」という) が全体を俯瞰しつつ、所管省庁(又は業界団体)がガイドラインを策定している。
- 重要インフラ分野を除く分野では経産省(IPA を含む)が独自にガイドラインを策定している場合もある。

[体系化の状況]

- 重要インフラ分野では、安全基準等策定指針を中心として、個別の業法との関係性も意識しつつ、ガイドラインが体系化されている。ただし、内容面でかかるガイドラインは必ずしも安全基準等策定指針と対応していない部分がある可能性があり、NISC も対応を強制できない立場にある。
- 重要インフラを除く分野では、CPSF やサイバーセキュリティ経営ガイドライン、中小企業の情報セキュリティ対策ガイドラインと関連するガイドラインは、それぞれのガイドラインを頂点として体系化されているが、横の関係性の整理はなされていない。

-
- 米国:
[管理状況]
 - FISMA や大統領令等に基づき、主に政府情報システム及び関連分野について NIST が標準策定を行う。また、OMB(米行政管理予算局)による指令は NIST が策定した標準への準拠を各省庁へ要求している。NIST に対して標準策定機能に係る明確な位置づけがされている。
 - 一方で、個別のガイドラインについては、CISA や各所管省庁が個別に策定している場合がみられ、標準策定機能が必ずしも NIST に一元化されていない。
[体系化の状況]
 - 政府情報システムにおいて、NIST SP800-53 を中心としてガイドラインが策定されている。また、それを補足する形で個別の文書が策定されており、政府機関だけではなく、民間企業においても広く参照されている。
 - 重要インフラ分野については、NIST CSF を中心として、実装のためのガイドライン等が策定されている。ただし、NIST CSF は任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。

 - EU:
[管理状況]
 - EU サイバーセキュリティ法によって権限強化された ENISA(欧州ネットワーク・情報セキュリティ機関)が任意のガイドラインを策定している。
 - EU の標準機関として、CEN(欧州標準化委員会)、CENELEC(欧州電気標準化委員会)、ETSI(欧州電気通信標準化機構)が位置付けられ、それらが欧州標準(例:IoT の場合、ETSI 303 645)を策定している。
 - 欧州委員会から提案された規則や指令等によって、規定が策定される。規則は直接適用されるが、指令は各加盟国によって国内法が策定されることで、はじめて一般的な効力を持つ。
[体系化の状況]
 - EU サイバーセキュリティ法に基づき、各分野において任意の認証制度(例:クラウド、5G)が構築されつつある。本認証制度の枠組みでは体系化がなされている。特に、制度の枠組みを構築した上で、標準を策定する点に特徴がみられる。
 - 指令が定められた領域においては各加盟国間の法律は指令に基づき整理されている。

 - 国際機関:
[管理状況/体系化の状況]
 - ISO/IEC SC27 にて ISO/IEC 27001 関連文書が策定され、IEC TC65 にて IEC 62443 関連文書が策定されている。
 - 業種横断の基準として ISO/IEC 27001 が定められるとともに、業界個別の基準が策定される際に考慮すべき標準が ISO/IEC 27009 によって定められることによって、ISO/IEC 27001 関連文書全体が関連付けられるよう整理されている。ただし、ISO/IEC 27009 は既に撤回済み¹である点に留意されたい。
-

図表 2-9 小括

分類	日本	米国	EU	国際機関
管理状況 (主体)	- 重要インフラ分野では、NISCが全体を俯瞰しつつ、所管省庁(又は業界団体)がガイドラインを策定。 - 重要インフラ分野を除く分野では経産省(IPAを含む)が独自にガイドラインを策定している場合もある。	- FISMAや大統領令等に基づき、主に政府情報システム及び関連分野についてNISTが標準策定を行う。また、OMBによる指令はNISTが策定した標準への準拠を各省庁へ要求している。NISTに対して標準策定機能に係る明確な位置づけがされている。 - 一方で、個別のガイドラインについては、CISAや各所管省庁が個別に策定している場合がみられ、標準策定機能が必ずしもNISTに一元化されていない。	- EUサイバーセキュリティ法によって権限強化されたENISAがガイドラインを策定。 - EUの標準機関として、CEN、CENELEC、ETSIが位置付けられ、EU標準(例:IoTの場合、ETSI 303 645)を策定。 - 欧州委員会から提案された規則や指令等によって、規定が策定される。規則は直接適用されるが、指令は各加盟国によって国内法が策定されることで、はじめて一般的な効力を持つ。	- ISO/IEC SC27にてISO/IEC 27001関連文書が策定され、IEC TC65にてIEC62443関連文書が策定。 - 業種横断の基準としてISO/IEC 27001が定められるとともに、業界個別の基準が策定される際に考慮すべき基準がISO/IEC 27009によって定められることよって、ISO/IEC 27001関連文書全体が関連付けられるよう整理されている。
体系化の状況 (ガイドライン)	- 重要インフラ分野では、安全基準等策定指針を中心として、個別の業法との関係性も意識しつつ、ガイドラインが体系化されている。ただし、内容面にかかるガイドラインは必ずしも安全基準等策定指針と対応していない部分がある可能性があり、NISCも対応を強制できない立場にある。 - 重要インフラを除く分野では、CPSFやサイバーセキュリティ経営ガイドライン、中小企業の情報セキュリティ対策ガイドラインと関連するガイドラインは、それぞれのガイドラインを頂点として体系化されているが、横の関係性の整理はなされていない。	- 政府情報システムにおいて、NIST SP800-53を中心としてガイドラインが策定されている。また、それを補足する形で個別の文書が策定されており、政府機関だけではなく、民間企業においても広く参照されている。 - 重要インフラ分野については、NIST CSFを中心として、実装のためのガイドライン等が策定されている。ただし、NIST CSFは任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。	- EUサイバーセキュリティ法に基づき、各分野において任意の認証制度(例:クラウド、5G)が構築されつつある。本認証制度の枠組みでは体系化がなされている。特に、制度の枠組みを構築した上で、標準を策定する点に特徴がみられる。 - 指令が定められた領域においては各加盟国間の法律は指令に基づき整理されている。	

2.3.2 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の調査

本項では、国内の政府機関又は業界団体等が公開する業種別のサイバーセキュリティに関するガイドライン及び基準の詳細について調査した。

本項の調査では、国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等を調査するため、以下の2つの項目から調査を行った。

- ① 調査項目 A:位置づけ、参照関係、関係性等について
- ② 調査項目 B:記載内容について

① 調査項目 A:位置づけ、参照関係、関係性等について

国内のガイドラインにおける位置づけ、参照関係、関係性等は以下の3のパターンに分類された。

➤ パターン 1: 制度対応に必要な基準の位置づけが明確

制度において、サイバーセキュリティ確保のための基準への遵守が義務として定められており、その基準が明示されている。また、その基準への遵守にあたって参考となるガイドラインが示されている場合がある。(なお、任意の評価制度を含む)

[例]

- 電気通信事業法/端末設備等規則/電気通信事業法に基づく端末機器の基準認証に関するガイドライン
- 防衛省通達/装備品等及び役務の調達における情報セキュリティの確保に関する特約条項/装備品等及び役務の調達における情報セキュリティ基準
- ISMS 適合性評価制度・JIS Q 27001(ISO/IEC 27001)

➤ **パターン 2: 制度対応に必要な基準とガイドライン等との関係が不明確**

制度において、サイバーセキュリティ確保のための基準への遵守が義務として定められている一方で、その基準が明示されておらず、遵守すべき基準が不明確となっている。

ガイドラインが示されている場合があるが、ガイドラインへの対応は義務とはなっていない。

[例]

- ・ 放送法施行規則/ケーブルテレビにおけるサイバーセキュリティに係る安全基準
- ・ ガス事業法施行規則/都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
- ・ 水道施設の技術的基準を定める省令/水道分野における情報セキュリティガイドライン

➤ **パターン 3: 任意のガイドラインのみを提示**

制度に該当するものがなく、ガイドラインへの遵守が任意となっている。また、安全基準等策定指針及び重要インフラ分野の各ガイドラインのように、ガイドライン間で参照されている文書がみられる。

[例]

- ・ サイバーセキュリティ経営ガイドライン関連文書
- ・ CPSF 関連文書

図表 2-10 A:位置づけ、参照関係、関係性等

分類	特徴	例
パターン 1 制度対応に必要な基準の位置づけが明確	・ 制度において、サイバーセキュリティ確保のための基準への遵守が義務として定められており、その基準が明示されている。 ・ また、その基準への遵守にあたって参考となるガイドラインが示されている場合がある。(なお、任意の評価制度を含む)	・ 電気通信事業法/端末設備等規則/電気通信事業法に基づく端末機器の基準認証に関するガイドライン ・ 防衛省通達/装備品等及び役務の調達における情報セキュリティの確保に関する特約条項/装備品等及び役務の調達における情報セキュリティ基準 ・ ISMS適合性評価制度・ISO/IEC 27001(JIS Q 27001)
パターン 2 制度対応に必要な基準とガイドライン等との関係が不明確	・ 制度において、サイバーセキュリティ確保のための基準への遵守が義務として定められている一方で、その基準が明示されておらず、遵守すべき基準が不明確となっている。 ・ ガイドラインが示されている場合があるが、ガイドラインへの対応は義務とはなっていない。	・ 放送法施行規則/ケーブルテレビにおけるサイバーセキュリティに係る安全基準 ・ ガス事業法施行規則/都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説 ・ 水道施設の技術的基準を定める省令/水道分野における情報セキュリティガイドライン
パターン 3 任意のガイドラインのみを提示	・ 制度に該当するものがなく、ガイドラインへの遵守が任意となっている。 ・ また、安全基準等策定指針及び重要インフラ分野の各ガイドラインのように、ガイドライン間で参照されている文書がみられる。	・ サイバーセキュリティ経営ガイドライン関連文書 ・ CPSF関連文書

② 調査項目 B:記載内容について

国内のガイドラインにおける記載内容は更に、以下の 2 つの項目に分けて調査を行った。

● 調査項目 B-1:記載範囲

NIST CSF 2.0 は国内外を問わず様々なガイドラインから参照されており、事実上の国際標準の 1 つとして位置付けられる。国内のガイドラインにおいて、NIST CSF 2.0 で網羅されている要求事項が最低限網羅されていれば、その偏りは少ないと考えられることから、NIST CSF 2.0 と比較を行った上で、対象となるガイドラインの要求事項がどの程度網羅されているのかを調査した。

● 調査項目 B-2:記載粒度

ガイドラインの記載粒度は、その文書の目的や想定読者、位置づけによって異なる。特に想定する読者の知識レベルによって記載粒度は異なると考えられるが、ISMS の要求事項を示した ISO/IEC 27001(なお、情報セキュリティ管理策の実践のための規範は ISO/IEC 27002 にて示されている)と比較した際に、より具体的に記載されている要求事項は、その記載粒度が一定の水準以上と考えられることから、ISO/IEC 27001 と比較を行った上で、対象となるガイドラインの要求事項がどの程度具体的に記載されているのかを調査した。

- 調査項目 B-1:記載範囲

記載範囲は、前述の通り NIST CSF 2.0 と比較した際に、対象となるガイドラインの要求事項がどの程度網羅されているのかを調査した。具体的には、NIST CSF 2.0 の 22 個のコア機能とガイドラインの要求事項を比較した上で、カバーされているコア機能の数を集計した。

主な調査結果は以下の通り。

- 33 の調査対象のうち、24 の基準・ガイドラインが 8 割の項目(81.8%以上:18/22 個)を満たしていた。日本国内の既存の基準/ガイドラインは、少なくともコア機能のレベルでは NIST CSF 2.0 の記載範囲を概ね網羅していた。
- 製品(例:IoT 機器)を対象とした基準/ガイドラインでは、組織を対象とした NIST CSF と比較した際に記載範囲に偏りがみられた。例えば、製品を対象とした基準/ガイドラインは特定/防御に係る対策が主に示されているが、スコープの違いから生じるものと考えられる。

[例]

- ・ JC-STAR
- ・ 電気通信事業法に基づく端末機器の基準認証に関するガイドライン
- 一方で、組織を対象とした基準/ガイドラインであっても記載範囲が限定的(50%以下:11/22 個)となっているものもみられた。これらの基準/ガイドラインは NIST CSF と比較した際に、記載範囲を拡大させる余地がある。ただし、対象企業(例:中小企業)の能力や位置づけ(例:義務化)によって、意図的に記載範囲が限定されていることも想定される。製品(例:IoT 機器)を対象とした基準/ガイドラインでは、組織を対象とした NIST CSF と比較した際に記載範囲に偏りがみられた。例えば、製品を対象とした基準/ガイドラインには特定/防御に係る対策が主に示されているが、スコープの違いから偏りが生じるものと考えられる。

[例]

- ・ 中小企業の情報対策セキュリティガイドライン
- ・ 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
- ・ クレジットカード・セキュリティガイドライン
- また、対象となるガイドラインにおいてみられた要求事項であっても、NIST CSF 2.0 ではみられなかったものもあった。例えば、発火・発煙防止等の安全設計(例:情報通信ネットワーク安全・信頼性基準)に係る要求事項や災害対策(例:重要インフラのサイバーセキュリティに係る安全基準等策定指針)に係る要求事項は NIST CSF 2.0 では確認されなかった。これは、NIST CSF がサイバーセキュリティのリスクを管理することを主な目的としている一方で、かかるガイドラインでは必ずしもサイバーセキュリティの文脈に限定せず、要求事項を定めているためと考えられる。

図表 2-11 NIST CSF のコア機能との比較結果(1/2)

[凡例]

0%

1-50%

51-99%

100%

コア	業界横断											業界個別					
	中小企 業の情報 策セキュ リティGL	情報セ キュリ ティ管 理基準	CSMS 認証基 準	工場シ ステム GL	ISMS クラウド セキュリ ティ認 証に関 する要 求事項	クラウド サービス 利用の ための 情報セ キュリ ティマ ネジメ ントGL	クラウド を利用 したシ ステム 運用に 関する ガイ ダンス	JC- STAR	電気通 信事業 法に基 づく端 末機器 の基準 に関する GL	IoTセ キュリ ティガ イドラ イン	サイ バー・ フィジ カル・セ キュリ ティ対 策フレ ームワ ーク	重要イ ンフラ のサイ バーセ キュリ ティに 係る 安全 基準等 策定指 針	情報通 信ネッ トワー ク安全 ・信頼 性基準	電気通 信分野 における サイバ ーセキ ュリテ ィに係 る安全 基準	ケーブ ルテレビ における サイバ ーセキ ュリテ ィに係 る安全 基準	金融分 野にお けるサイ バーセ キュリ ティに 関する ガイ ドライン	航空分 野にお ける情 報セキ ュリテ ィに係 る安全 ガイ ドライン
統制	3/6	6/6	6/6	6/6	6/6	6/6	5/6	3/6	0/6	6/6	6/6	6/6	5/6	6/6	6/6	6/6	6/6
識別	2/3	3/3	3/3	3/3	3/3	3/3	2/3	2/3	0/3	3/3	3/3	3/3	2/3	3/3	3/3	3/3	3/3
防御	3/5	5/5	5/5	5/5	5/5	5/5	3/5	4/5	4/5	3/5	5/5	5/5	5/5	5/5	5/5	5/5	5/5
検知	1/2	2/2	2/2	1/2	2/2	2/2	2/2	0/2	0/2	2/2	2/2	2/2	1/2	2/2	2/2	2/2	2/2
対応	1/4	3/4	3/4	2/4	3/4	3/4	3/4	0/4	0/4	3/4	4/4	3/4	2/4	4/4	3/4	4/4	3/4
復旧	1/2	1/2	1/2	1/2	1/2	1/2	1/2	0/2	0/2	1/2	2/2	1/2	1/2	2/2	1/2	1/2	2/2
集計	11/22	20/22	20/22	19/22	20/22	20/22	16/22	9/22	4/22	18/22	22/22	20/22	20/22	22/22	20/22	21/22	21/22

図表 2-12 NIST CSF のコア機能との比較結果(2/2)

[凡例] ☐ 0% ☐ 1-50% ☐ 51-99% ☐ 100%

コア	業界個別															
	空港分 野にお ける情 報セキ ュリテ ィに 係る 安全 ガイ ドライン	鉄道分 野にお ける情 報セキ ュリテ ィに 係る 安全 ガイ ドライン	自家用 電気工 作物に 係るサイ バーセ キュリ ティの 確保に 関する ガイ ドライン	地方公 共団体 におけ る情報 セキュ リティ に関 する ガイ ドライン	医療情 報シス テムの 安全 管理 に関 する ガイ ドライン	水道分 野にお ける情 報セキ ュリテ ィに 係る ガイ ドライン	物流分 野にお ける情 報セキ ュリテ ィに 係る 安全 ガイ ドライン	クレジ ットカ ード・ セキュ リティ ガイ ドライン	装備品 等及び 役務の 調達に おける 情報セ キュリ ティ基 準	民間宇 宙シス テムに おける サイバ ーセキ ュリテ ィ対 策ガイ ドライン	電力制 御シス テムセ キュリ ティGL	スマート メー ターシ ステム セキュ リティGL	ビルシ ステム におけ るサイ バー・ フィジ カル・ セキュ リティ 対策 GL	スマート ホーム の安心 ・安全 に向け たサイ バー・ フィジ カル・ セキュ リティ 対策 GL	政府機 関等の サイバ ーセキ ュリテ ィに 関する 統一基 準	自工会 /部工 会・サイ バーセ キュリ ティGL (Lv.1)
統制	6/6	6/6	6/6	6/6	6/6	6/6	6/6	2/6	6/6	1/6	4/6	5/6	4/6	3/6	6/6	6/6
識別	3/3	3/3	3/3	3/3	3/3	3/3	3/3	1/3	3/3	2/3	3/3	2/3	3/3	3/3	3/3	3/3
防御	5/5	5/5	5/5	5/5	5/5	5/5	5/5	3/5	4/5	3/5	5/5	4/5	5/5	3/5	5/5	5/5
検知	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	1/2	2/2	2/2	1/2	2/2	2/2
対応	3/4	3/4	3/4	4/4	4/4	4/4	4/4	4/4	4/4	0/4	2/4	3/4	4/4	1/4	3/4	3/4
復旧	2/2	2/2	2/2	1/2	2/2	1/2	1/2	1/2	2/2	0/2	0/2	0/2	2/2	0/2	1/2	1/2
集計	21/22	21/22	14/22	21/22	22/22	21/22	21/22	14/22	21/22	8/22	15/22	18/22	20/22	11/22	20/22	20/22

● 調査項目 B-2:記載粒度

記載粒度は、ISO/IEC 27001 と比較した際に、対象となるガイドラインの要求事項がどの程度具体的に記載されているのかを調査した。対象となるガイドラインの要求事項のうち、組織的管理策及び人的管理策、物理的管理策、技術的管理策の代表的なものを選択した上で、ISO/IEC 27001 の対策要件と比較を行い、具体的に記載されている内容を以下の 4 つの観点から整理した。組織的管理策の代表的な管理策として「資産の管理」、人的管理策の代表的な管理策として「情報セキュリティの意識向上、教育及び訓練」、物理的管理策の代表的な管理策として「物理的入退管理策」、技術的管理策の代表的な管理策として「ネットワーク及びネットワークサービスへのアクセス」を選択した。

- ・ 主体
- ・ 内容
- ・ 頻度
- ・ 場所

主な調査結果は以下の通り。

- 記載粒度に差異はみられるが、ISO/IEC 27001 と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載がみられた。
- 情報システムの構成要素や研修計画に盛り込む内容については、要求事項が具体的に示されており、読者が理解し実装できるレベルまで内容が記載されているものがみられた。

[例]

- ・ 情報システムの構成要素(航空分野における情報セキュリティ確保に係る安全ガイドライン)
- ・ 研修計画に盛り込む事項(地方公共団体における情報セキュリティポリシーに関するガイドライン)
- しかし、読者が理解し実装できるレベルまで内容(例:認証方法)が具体的に記載されていない要求事項もみられた。例えば、認証方法の一覧が示されているが、どのような場合にどの認証方法を選べばよいかは示されていないかった。

[例]

- ・ 認証方法(医療情報システムの安全管理に関するガイドライン/情報通信ネットワーク安全・信頼性基準/クレジットカード・セキュリティガイドライン)

以下では、各ガイドラインにおいて示された具体的な記載内容を分類ごとに示す。以下の記載内容は要求事項を更に具体化する上で参考になると考えられる。各ガイドラインの文脈を踏まえて参考とすることが望ましい。

・ 主体

- 教育対象
 - ・ 従業員、契約従業員、サードパーティ契約者
 - ・ 全要員、情報セキュリティ要員
 - ・ 統括者、管理者、保護システム管理者、保護システム担当者
- セキュリティ対策の対象者
 - ・ 経営層、システム業務に従事する人材、システムユーザ、PC 操作者(テレワーク勤務者を含む)、(必要に応じて)委託先
- 利用者アカウントの認証主体
 - ・ 代表取締役、情報セキュリティ責任者
- 認証を行う主体
 - ・ システム管理者アクセスアカウント、アプリケーション構成アクセスアカウント、リモートユーザ

図表 2-13 主体

項目	内容		対象
B-2. 主体 記載粒度	・ <u>教育対象</u>	・ [手順及び設備について]従業員、契約従業員、サードパーティ契約者	・ CSMS認証基準 ・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン ・ 金融分野におけるサイバーセキュリティに関するガイドライン
		・ [リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組]本取組に関連する要員	
		・ 全要員 ・ 情報セキュリティ要員(システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)	
	・ <u>セキュリティ対策の対象者</u>	・ 総括者 ・ 管理者 ・ 保護システム管理者 ・ 保護システム担当者	・ 装備品等及び役務の調達における情報セキュリティ基準
		・ 経営層 ・ システム業務に従事する人材 ・ システムユーザ ・ PC操作者(テレワーク勤務者を含む) ・ (必要に応じて)委託先	・ 航空分野における情報セキュリティ確保に係る安全ガイドライン
		・ <u>利用者アカウントの承認主体</u>	・ 代表取締役 ・ 情報セキュリティ責任者
・ <u>認証を行う対象</u>	・ システム管理者アクセスアカウント ・ アプリケーション構成アクセスアカウント ・ リモートユーザ(アカウント)	・ CSMS認証基準	

内容

- 情報システムの構成要素
 - ・ 端末、サーバ装置、通信回線・通信回線装置、複合機及び IoT 機器を含む特定用途機器
 - ・ 施設、ネットワーク、周辺機器、ハードウェア、システム領域、データ領域、システム運用体制、ベンダの継続能力
- 情報資産の管理にあたって表示する事項
 - ・ ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等)、格納する電磁的記録媒体のラベル、情報資産の分類(文書の隅等)
- 資産管理台帳の維持管理策
 - ・ 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする、承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する
- 認証方法
 - ・ パスワード、IC カード、電子証明書、生体認証等、本人の識別・認証
 - ・ 本人認証(EMV3-D セキュア)、本人認証(認証アシスト)、券面認証
- アクセス利用者の管理とアクセス権の管理にあたって実施すること
 - ・ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等の設定、利用者アクセス権の定期的なレビュー、管理権限のユーザー/用途ごとの設定、離職者アカウントに対して、全てのバッジ、キーカード、トークン等の失効
- 教育内容
 - ・ 情報セキュリティの重要性及び意義、「need to know の原則」(「情報は知る必要がある者のみに伝え、知る必要のない者には伝えない」という原則)の確実な履行、情報セキュリティ基本方針等の確実な履行、公私における慎重な行動、悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順、前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項、上記に掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的及び専門的な事項

- ・ 手順及び設備、リスクマネジメント、IACS のエンジニアリング、システム/保守、CSMS に影響を与える取組
- 研究計画に盛り込むこと
 - ・ 研修内容、受講対象者、e-ラーニング/集合研修、説明会等の実施方法、時期/日程/講師等

図表 2-14 内容(1/2)

項目	内容	対象
B-2. 記載粒度	・ 情報システムの構成要素 ・ 端末 ・ サーバ装置 ・ 通信回線・通信回線装置 ・ 複合機及びIoT機器を含む特定用途機器	・ 航空分野における情報セキュリティ確保に係る安全ガイドライン ・ 物流分野における情報セキュリティ確保に係る安全ガイドライン
	・ 施設 ・ ネットワーク ・ 周辺機器 ・ ハードウェア ・ システム領域 ・ データ領域 ・ システム運用体制 ・ ベンダの継続能力	・ 水道分野における情報セキュリティガイドライン
	・ 情報資産の管理にあたって表示する事項 ・ ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等) ・ 格納する電磁的記録媒体のラベル ・ 情報資産の分類(文書の隅等)	・ 地方公共団体における情報セキュリティポリシーに関するガイドライン
	・ 資産管理台帳の維持管理策 ・ 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする ・ 承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する	・ 物流分野における情報セキュリティ確保に係る安全ガイドライン
	・ 認証方法 ・ パスワード ・ ICカード ・ 電子証明書 ・ 生体認証等 ・ 本人の識別・認証	・ 医療情報システムの安全管理に関するガイドライン ・ 情報通信ネットワーク安全・信頼性基準
	・ 本人認証(EMV3-Dセキュア): ・ 本人認証(認証アシスト): ・ 券面認証	・ クレジットカード・セキュリティガイドライン

図表 2-15 内容(2/2)

項目	内容	対象
B-2. 記載粒度 (続き)	・ アクセス利用者の管理とアクセス権の管理にあたって実施すること ・ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等の設定 ・ 利用者アクセス権の定期的なレビュー ・ 管理権限のユーザ/用途ごとの設定 ・ 離職者アカウントに対して、全てのバッジ、キーカード、トークン等の失効	・ 航空分野における情報セキュリティ確保に係る安全ガイドライン
	・ 教育内容 ・ 情報セキュリティの重要性及び意義 ・ 「need to knowの原則」(「情報は知る必要がある者のみに伝え、知る必要のない者には伝えない」という原則)の確実な履行 ・ 情報セキュリティ基本方針等の確実な履行 ・ 公私における慎重な行動 ・ 悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順 ・ 前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項 ・ 上記に掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的及び専門的な事項	・ 装備品等及び役務の調達における情報セキュリティ基準
	・ 手順及び設備 ・ リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組	・ CSMS認証基準
	・ 研修計画に盛り込む事項 ・ 研修内容 ・ 受講対象者 ・ e-ラーニング/集合研修 ・ 説明会等の実施方法 ・ 時期/日程/講師等	・ 地方公共団体における情報セキュリティポリシーに関するガイドライン

- ・ **頻度**
 - 教育の頻度
 - ・ 入社時、契約時(情報セキュリティ関連規程)、運用開始時、運用終了後、情報システムや産業用制御システムに対する変更により必要になったとき、関連法令の公布・施行時(関連法令)、最低毎年度 1 回(職員等が教育を受講する頻度)
 - パスワードの変更タイミング(IoT 機器を対象)
 - ・ 初期設定時
 - アクセス権の割当において考慮すべきタイミング
 - ・ 利用者の初期登録時、情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除時
- ・ **場所**
 - 情報システム室の設置を禁止する場所
 - ・ 地階/1 階
 - 物理的セキュリティ境界
 - ・ 壁、カード制御による入口、有人の受付
 - 要管理対策区域
 - ・ 執務室、会議室、サーバ室等
 - レベルごとの物理的管理策の対象
 - ・ レベル 1:本社受付・応接スペース・商談室・倉庫
 - ・ レベル 2:本社受付・応接スペース・商談室・倉庫
 - ・ レベル 3:サーバールーム/鍵付きサーバラック

図表 2-16 頻度/場所

項目	内容		対象
B-2. 頻度 記載粒度	・ 教育の頻度	・ 入社時、契約時(情報セキュリティ関連規程) ・ 運用開始時、運用終了後 ・ 情報システムや産業用制御システムに対する変更により必要になったとき ・ 関連法令の公布・施行時(関連法令) ・ 最低毎年度1回(職員等が教育を受講する頻度)	・ 中小企業の情報セキュリティ対策ガイドライン ・ サイバー・フィジカル・セキュリティ対策フレームワーク ・ 航空分野における情報セキュリティ確保に係る安全ガイドライン
	・ パスワードの変更タイミング (IoT機器を対象)	・ 初期設定時	・ JC-STAR ・ 電気通信事業法に基づく端末機器の基準認証に関するガイドライン ・ IoTセキュリティガイドライン
	・ アクセス権の割当において 考慮すべきタイミング	・ 利用者の初期登録時 ・ 情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除時	・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン
	場所		
	・ 情報システム室の設置を禁止する場所	・ 地階/1階	・ 地方公共団体における情報セキュリティポリシーに関するガイドライン
	・ 物理的セキュリティ境界	・ 壁 ・ カード制御による入口 ・ 有人の受付	・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン
	・ 要管理対策区域	・ 執務室 ・ 会議室 ・ サーバ室等	・ 航空分野における情報セキュリティ確保に係る安全ガイドライン
	・ レベルごとの 物理的管理策の対象	・ レベル1:本社受付・応接スペース・商談室・倉庫 ・ レベル2:本社受付・応接スペース・商談室・倉庫 ・ レベル3:サーバールーム/鍵付きサーバラック	・ 中小企業の情報セキュリティ対策ガイドライン

③ 小括

- ・ 国内の制度やガイドライン等は、「制度対応に必要な基準の位置づけが明確なパターン」(パターン 1)と、「制度対応に必要な基準とガイドライン等との関係が不明確なパターン」(パターン 2)と「任意のガイドラインのみを提示している」(パターン 3)に分類された。特に、パターン 2 については、サイバーセキュリティ確保のための基準への遵守が義務として定められている一方で、その基準が具体化されておらず、遵守すべき基準が不明確となっている場合があり、事業者が判断に迷うケースが生じ得る。
- ・ 33 の調査対象のうち、24 の基準・ガイドラインが 8 割の項目(81.8%以上:18/22 個)を満たしており、日本国内の既存の基準/ガイドラインは、NIST CSF の記載範囲を少なくともコア機能のレベルでは概ね網羅していた。一方で、組織を対象とした基準/ガイドラインであっても記載範囲が限定的(50%以下:11/22 個)となっているものもみられたが、対象企業(例:中小企業)の能力や位置づけ(例:義務化)によって、意図的に記載範囲が限定されていることも想定される。助言の際にはこれらの背景情報を考慮することが重要となる。
- ・ 記載粒度に差異はみられるが、ISO/IEC 27001 と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載(例:情報システムの構成要素や研修計画に盛り込む内容)がみられた。一方で、読者が理解し実装できるレベルまで内容(例:認証方法)が具体的に記載されていない要求事項もみられた。特に技術的管理策においては具体的な記載が少なかった。これは、技術的管理策を細かく指定すると事業者による実装方法を縛ることになるためと考えられる。

2.3.3 今後の注力領域及び方向性(案)の整理

本項では、1 及び 2 で調査を行った対象を踏まえつつ、あるべき姿を具体化した上で、対処すべき現状の問題を整理し、今後の方向性(案)の整理を行った。

- ① 文書のあるべき姿の具体化/文書の整理状況の可視化
- ② 対処すべき現状の問題の整理
- ③ 今後の方向性(案)の整理

① 文書のあるべき姿の具体化/文書の整理状況の可視化

本項では、更に以下の項目に分けた上で検討結果を示す。

- 文書のあるべき姿の具体化
- 文書の整理状況の可視化

● 文書のあるべき姿の具体化

位置づけ、参照関係、関係性等と記載内容から文書のあるべき姿について整理を行った。

➤ 位置づけ、参照関係、関係性等のあるべき姿

位置付け、参照関係、関係性等が明確であり、かつ、どの読者にとって何を読めばよいかが明確となっている状態をあるべき姿とする。

<体系内>

- ・ 法律等でセキュリティ対策義務が定義されている場合には、適切な法律等(例:サイバーセキュリティ基本法や業法)に基づき基準やガイドラインが策定されている状態をあるべき姿とする。
- ・ 法律等でセキュリティ対策義務が定義されていない場合には、体系内のガイドライン間で位置づけが明確に定義されている状態をあるべき姿とする。

<体系内>

- ・ 各分野で漏れなく基準やガイドライン等が策定されている状態をあるべき姿とする。

➤ 記載内容

- 以下の条件を満たし、近年増加している脅威に対処可能な要求事項が定められている状態にあるべき姿とする。
 - 記載されている範囲に漏れがない
 - 対策要件の記載粒度が適切である

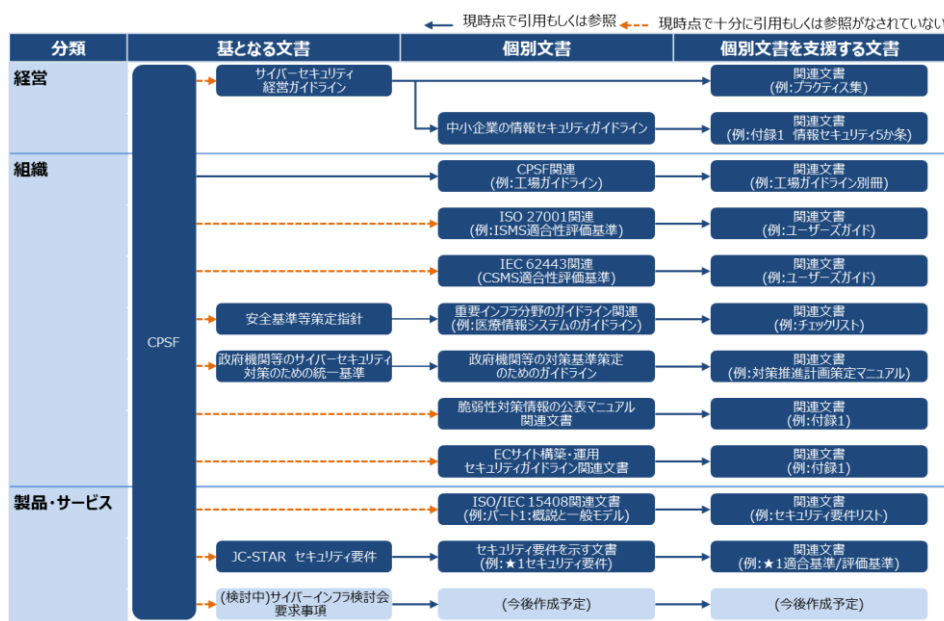
図表 2-17 文書のあるべき姿

対象	位置づけ、参照関係、関係性等	記載内容
1. 制度	■ 体系内 <法律等でセキュリティ対策義務が定義されている場合>	-
2. 基準	適切な法律等(例:サイバーセキュリティ基本法や業法)に基づき基準やガイドラインが策定されている。	近年増加している脅威に対処可能な要求事項が定められている。
3. ガイドライン	<法律等でセキュリティ対策義務が定義されていない場合> 体系内のガイドライン間で位置づけが明確に定義されている。	<記載範囲> - 記載されている範囲に漏れがない <記載粒度> - 対策要件の記載粒度が適切である
	■ 体系間 各分野で漏れなく基準やガイドライン等が策定されている	

● 文書の整理状況の可視化

これまで、制度/基準/ガイドライン等を対象として調査を行ってきた。その中でもガイドラインを更に整理を行うことで事業者にとって参考となると考えられることから、日本国内のガイドラインの文書を以下の分類で整理を行った。

- 基となる文書: 分野や企業規模が異なっていたとしても、各主体が共通して遵守すべき要求事項や原則、考え方が記載されている文書
- 個別文書: 各主体が遵守すべき要求事項が記載されている文書
- 個別文書を支援する文書: 個別文書に示された要求事項を踏まえて、各主体がセキュリティ対策を実装する際に参考となる文書



図表 2-18 日本国内のガイドラインの文書の整理結果

② 対処すべき現状の問題

本項では、1 及び 2 で調査を行った対象を踏まえつつ対処すべき現状の問題を整理した。①のあるべき姿と比較した際に生じているギャップを現状の問題とした上で、以下の分類で整理をした。

➤ 位置づけ、参照関係、関係性

- ・ [1.1]事業者にとって、どの基準やガイドライン等を参照すればよいかわ不明確となっている。
- ・ [1.2]事業者にとって参照すべき基準やガイドラインを理解できたとしても、サイバーセキュリティ確保のための遵守が義務となっている基準が具体化されておらず、遵守すべき基準が不明確となっている。

➤ 記載内容

- ・ [2.1]国際的に参照されている NIST CSF と比較した際に、ガイドライン等によっては記載範囲が限定的となっており、脅威に適切に対処できない可能性がある。
- ・ [2.2]ガイドライン等によっては、読者が理解し実装できるレベルまで要求事項が具体的に記載されておらず、脅威に適切に対処できない可能性がある。

③ 今後の方向性(案)の整理

2.3.3④で示した文書のあるべき姿や事業者での更なるガイドラインの活用に向けた取組として貴省(及びガイドラインを一元管理する団体)では、大きく分けて 3 つの施策の方向性が考えられる。

A) ガイドラインの体系化

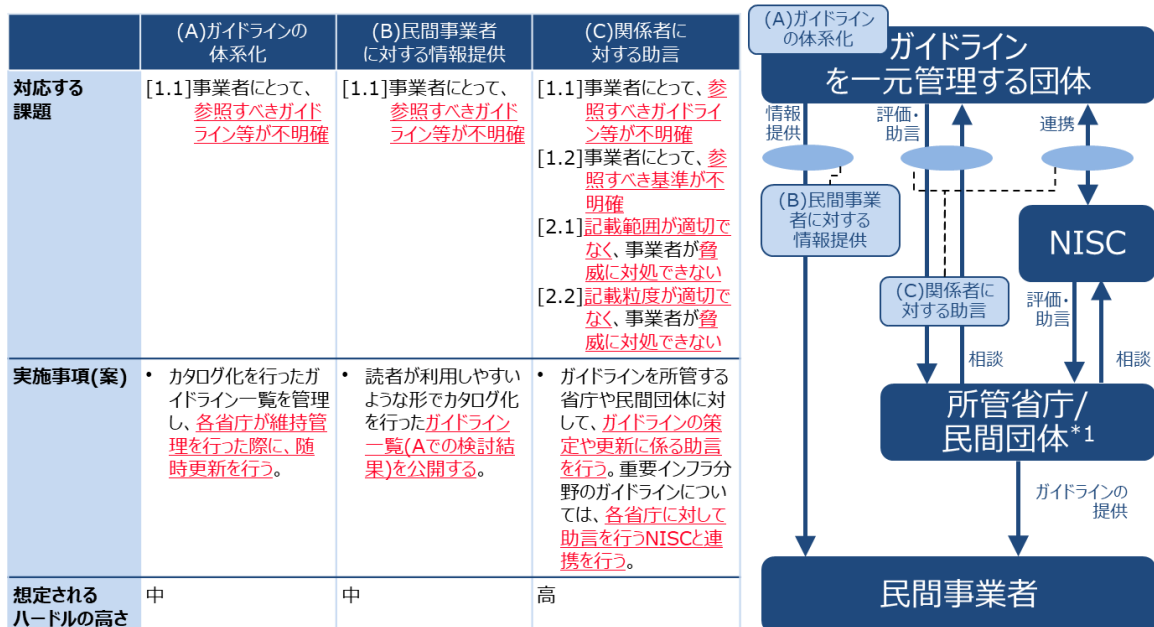
カタログ化を行ったガイドライン一覧を管理し、各省庁が維持管理を行った際に、随時更新を行う。

B) 民間事業者に対する情報提供

読者が利用しやすいような形でカタログ化を行ったガイドライン一覧(A での検討結果)を公開する。

C) 関係者に対する助言

ガイドラインを所管する省庁や民間団体に対して、ガイドラインの策定や更新に係る助言を行う。重要インフラ分野のガイドラインについては、各省庁に対して助言を行う NISC と連携を行う。



図表 2-19 サマリ

特に、C)関係者に対する助言は想定されるハードルも高く、その具体的なイメージがつきにくいことから、本事業の中で仮のケースを想定してその助言案を作成した。具体的には、貴省担当者と協議の上、位置づけ、参照関係、関係性等と記載内容の観点からガイドラインに助言が必要と考えられる分野や範囲において調査を行った。対象となる範囲・分野を絞り込む際には、近年脅威が増大していると考えられる分野(既にインシデントが多く発生している分野を含む)や 2.3.2 の調査を行った分野から、費用対効果(助言に係るコスト[経産省所管か]及び社会的なインパクト[重要インフラを含むか]の 2 軸)で絞り込みを行った。以下の分野や範囲において、米国や欧州の海外文書を参考としつつ、助言案を作成し経産省へ報告を行った。なお、助言案は委託事業の範囲内で検討結果を示すものであり、経済産業省の立場を示すものでない点に留意されたい。

<業種横断>

- 水道分野
- 電力分野

<業種個別>

- 製造分野
- サプライチェーン

また、前述の A～C に示す施策の方向性に対して、今後貴省(及びガイドラインを一元管理する団体)で想定される手段を併せて具体化した。

1. セキュリティに係るガイドラインを一元管理する団体に対する権限の付与

セキュリティに係るガイドラインを一元管理する団体に対してガイドラインの管理や助言に対する権限を付与するために、関連する規定を改正する。

2. 人材の確保(部署の設置)

ガイドラインの体系化・管理や情報提供を継続的に行うために必要な人材を確保する。

3. 会議体の設置

各省庁に対して、以下の内容を助言するための会議体を設置する。

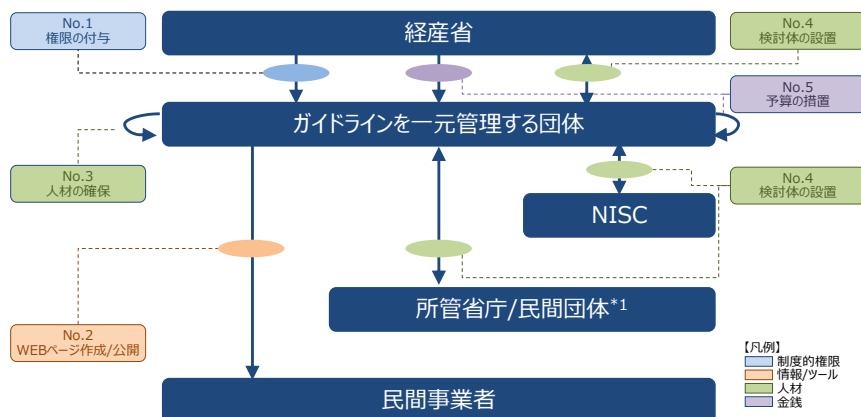
- ・ 既存の脅威に対して対応できていないガイドラインの修正
- ・ 新たな脅威に対応するためのガイドラインの更新

4. WEB ページ作成/公開

ガイドライン等の対象者を明確にした上で、事業者が必要とする情報を提供できるよう WEB ページを作成する。

5. 予算的な措置

No.2～No.4 を実施するための予算を確保する。



図表 2-20 サマリ

2.3.4 まとめ

- ・ 貴省では、これまで様々な形でサイバーセキュリティに関するガイドラインを公開しており、民間事業者におけるセキュリティ対策の推進に貢献している。一方で、省庁横断的に調整を図るような仕組みが導入されているとは言えず、ガイドラインが思うように普及していない現状に鑑み、既存のガイドライン等の一元的な管理・体系化を行うことを目的として本調査を行った。
- ・ 日本においても制度やガイドラインの体系化を意識した取組がみられた一方で、全ての制度やガイドライン等が一元的に管理・体系化されているとは言えなかった。そこでは、事業者にとって参照すべき基準やガイドライン等が不明確となっているケースや参照すべき基準やガイドライン等が明確であっても、その基準が具体化されていないケースがみられた。また、記載内容の面でも偏りや具体化の面で課題が残るケースもみられた。
 - 日本では、重要インフラ分野を除く範囲で明確な省庁間の役割の切り分け等がなされていない場合があり、各省庁や業界団体が個別にガイドラインを策定している状況である。日本では一元的な管理・体系化にあたっては課題が残っていることが確認されたが、ベンチマークの 1 つである米国でも NIST にも全ての標準策定機能が一元化されているとは言えなかった。[2.3.1 部分]
 - 国内の制度やガイドライン等を調査した結果、国内の制度やガイドライン等は大部分が体系間や体系内で整理がなされていた。一方で、制度の中で遵守すべき基準が不明確となっているものもみられ、全ての制度やガイドライン等が体系化されているとは必ずしも言えないため、社会全体のセキュリティレベル向上のため、体系化を意識した取組が必要となる。[2.3.2 部分]
- ・ 社会全体のセキュリティレベル向上のために、貴省において以下の取組が必要と考えられる。また、各取組を行うために法制度的な権限の付与やリソース面での調整が必要となると考えられる。[2.3.3 部分]
 - 短期的には、貴省によるガイドラインを一元管理する団体の明確化
 - 短中期的には、貴省やガイドラインを一元管理する団体を中心としてガイドラインのカタログ化に向けた取組の推進
 - 中長期的には、ガイドラインを一元管理する団体が旗振り役となり、カタログ化されたガイドラインに対する採番や、民間事業者へのわかりやすい情報の提供、各所管省庁等へ助言に向けた取組の推進

3 CPSF 等に基づく国際標準化の推進

3.1 本事業項目の目的

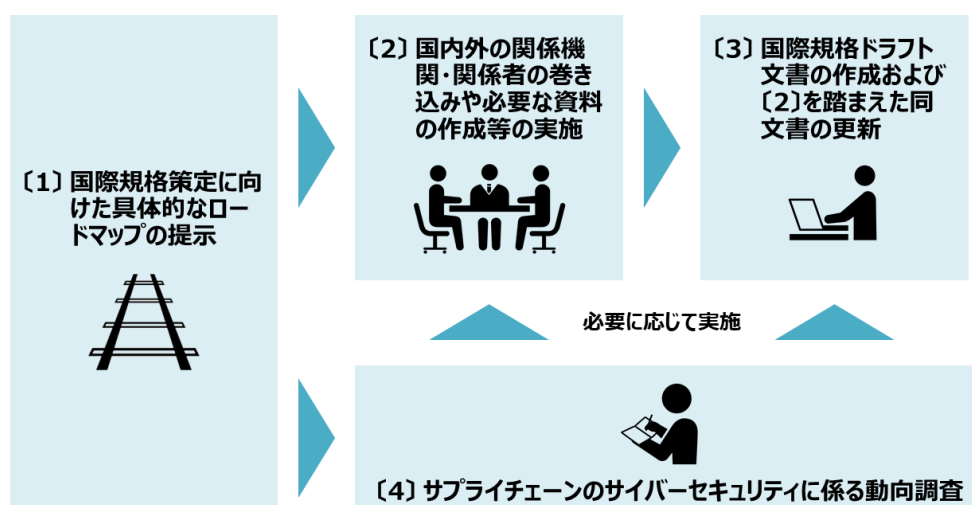
本事業では、日本企業の競争力強化に寄与する国際的なルールを形成していくことを目的とし、ルール形成を構成する一要素になりうる CPSF 等をベースにした国際標準化を推進した。

3.2 本事業項目の実施内容

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

＜本事業項目の実施内容＞

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



図表 3-1 本事業項目の実施プロセス(概要)

3.3 本事業項目の実施結果

3.3.1 国際規格策定に向けたロードマップの策定

(1) 前提：主要な国際標準化機関とその標準策定プロセス

一般に国際規格とは、「製品の品質、性能、安全性、寸法、試験方法などに関する国際的な取極め」²を指し、国際標準化機関で制定される。代表的な国際標準化機関として、ISO(国際標準化機構)が電気・電子・通信分野を除く幅広い分野の国際規格を制定しており、IEC(国際電気標準会議)は電気・電子分野の国際規格を、ITU(国際電気通信連合)は通信分野、放送・情報技術分野の国際規格を制定している³。また、情報技術(IT)の標準化について、ISO と IEC は共同で JTC

1(Joint Technical Committee 1)を設立、運用している。

以上に挙げるほか、IT 分野で国際的に広く参照される規格等の策定を担う機関としては、RFC(Request For Comments)を策定する IETF(Internet Engineering Task Force)や W3C(World Wide Web Consortium)等がある。

国際規格の制定プロセスについては、WTO(世界貿易機関)が定める協定のうち、国際規格の策定を含む基準認証分野と密接に関連している TBT(貿易の技術的障害)協定が、満たすべき条件として以下の 6 条件を提示している。

- 透明性 (規格案の早い段階からの通知、作業計画の開示等)
- 開放性 (世界各国からの自由な参加等)
- 公平性 (コンセンサスに基づく決定等)
- 効率性・市場適合性 (特定の市場が有利にならないことの確保、各国の規制体系への適応性、性能規格の重視等)
- 一貫性 (重複の回避等)
- 途上国への配慮 (標準化機関や先進国による必要な技術協力等)

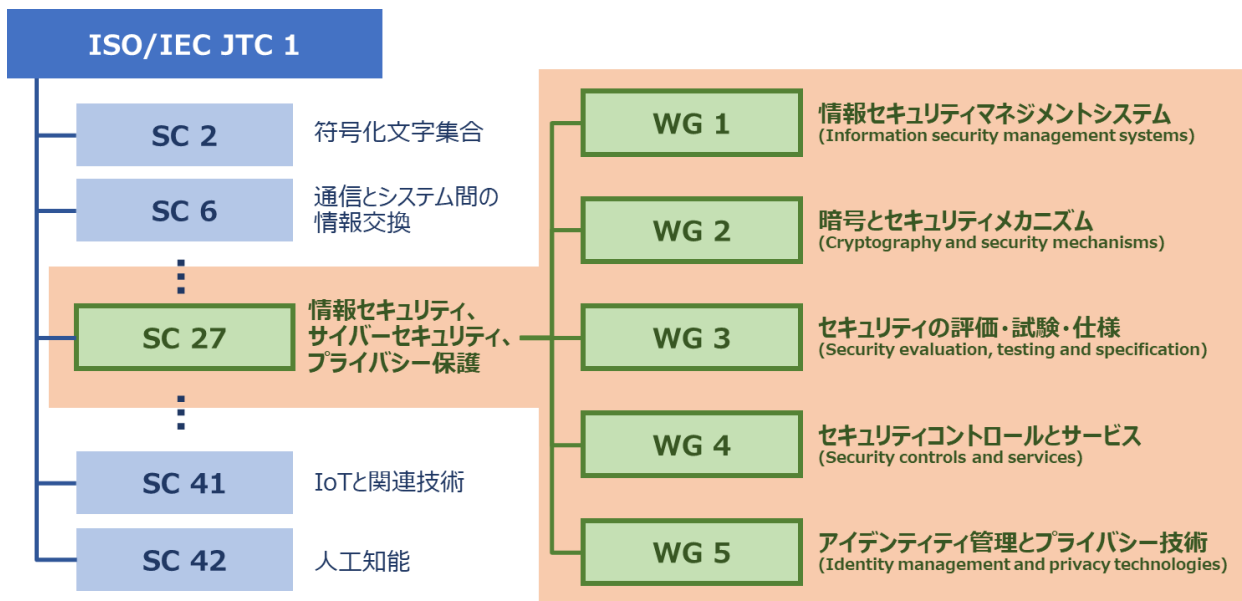
上記のハイレベルな条件を共通に参照しつつ、より具体的な規格策定プロセスが国際標準化機関や策定される文書の種別(例：IS/TS/TR)ごとに定められている。ロードマップの策定にあたっては CPSF 等に基づく国際規格の策定を行う機関や委員会、策定する文書の種別を特定し、参照されている標準的な規格策定プロセスを確認する必要がある。

■ CPSF 等に基づく国際規格の策定を行う機関や委員会

CPSF 等に基づく国際規格策定の推進は、これまでに述べた国際標準化機関のうち JTC 1 に設置された SC 27(Sub-Committee 27)⁴にて進められている。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。

図表 3-2 JTC 1/SC 27 の構成



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

わが国においては、一般社団法人 情報処理学会内に設置された情報規格調査会(ITSCJ)が、SC 27 を含む、JTC 1 に係る情報技術に関する国際規格の審議及びこれに関する調査研究、国内規格の審議等を行っている。ITSCJ には、各 SC 又は WG に対応する専門委員会又は小委員会が設置されており、本件に係るところでは、SC 27 専門委員会、SC 27/WG 4 小委員会がサイバーセキュリティ等に係る国際規格に関する国内における審議等を推進している。⁵

■ 策定する文書の種別と規格策定プロセスと規格化の現状

国際規格策定に向けたロードマップを作成する上では、策定する文書の種別とともに、図表 3-3 に示す JTC 1 における標準的な規格策定プロセスを考慮する必要がある。

ISO、IEC 及び JTC 1 が策定する文書には、以下 4 つの種別がある⁶。そのうち、本事業で開発するものは「技術仕様書」(TS)に該当する。

- 国際規格 (IS: International Standard)
- 技術仕様書 (TS: Technical Specification)
委員会は、以下の場合に TS を作成し発行することを決定してもよいとされる。
 - 対象の主題がまだ開発中である場合又は、
 - 「照会段階」又は「承認段階」において、所定の承認条件を満たさないものの、発行を望む文書を開発した場合
- 公開仕様書 (PAS: Publicly Available Specification)
委員会は、緊急の市場ニーズがある以下のような場合に、PAS を発行することを決定してもよいとされる。
 - 完全な IS を開発する前の予備的な文書とする場合又は、
 - 外部組織からの既存の発行済文書を採用する場合又は、

- 「照会段階」又は「承認段階」において、所定の承認条件を満たさないものの、発行を望む文書を開発した場合

- 技術報告書 (TR: Technical Report)

委員会は、以下の場合に TR を発行することを決定してもよいとされる。

- 一般的には IS として発行はされていない情報(例えば、国代表組織間で実施された調査から得られた情報、他の国際機関での業務に関する情報、又は特定の主題に関する国代表組織の規格に関連した「最先端」に関する情報が含まれてもよい)を発行するため。
- 関連する IS の特定の要求事項の根拠を提供するため。

TR は、要求事項、推奨事項、又は許可事項を含まず、規範であることを示唆するような事項を含んではならない。TR は、主題に関連する IS で扱われている、又は今後扱われる主題の規範側面との関係を明確に説明しなければならない。

他方、JTC 1 における標準的な規格策定プロセスは、「予備段階」(PWI)から「発行段階」に至る 7 つの段階からなる。⁷

図表 3-3 ISO/IEC におけるプロジェクトの各段階と関連文書

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

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

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

No.3「作成段階」では、当該プロジェクトを担当する委員会の指名するエキスパートが作業原案(WD)を作成する。規格を技術仕様書(TS)又は技術報告書(TR)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(IS)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。

(2) CPSF 等に基づく国際規格策定に向けたロードマップ

ISO/IEC における規格策定プロセスや実際に策定される文書の種別、JTC 1/SC 27/WG 4 における実際の議論の状況等を踏まえ、CPSF 等に基づく国際規格策定に向けたロードマップを以下のとおり作成した。なお、ここでは、策定する文書の種別が「技術仕様」(TS)である場合を想定し、2025 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. 2025 年 3 月時点までの経過

2023 年 10 月の NP 投票可決後、エディタにて作業ドラフトの第 1 版を作成し、SC 27/WG 4 エキスパート内で行った意見募集の結果に基づき、2024 年 7 月の中間会合で議論を行った。

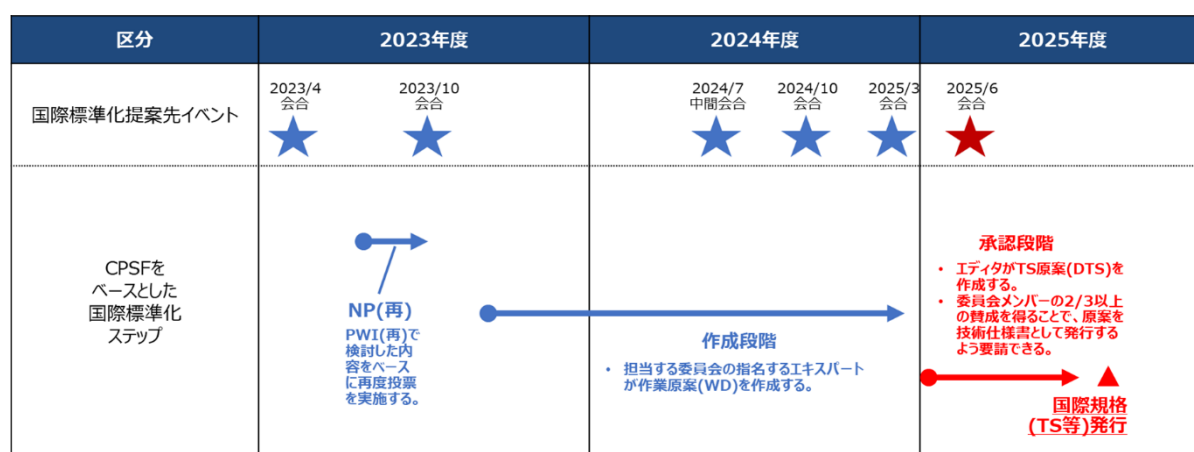
その後、2 度の WG 会合(24 年 10 月、25 年 3 月)での議論を経て、本案件は承認段階へ進むことが決議された。

B. 今後の見通し

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

今後、本案件は「承認段階」にて TS 原案(DTS)の検討を進める。具体的には、エディタにて TS 原案(DTS)を作成し、必要に応じて会合を開催して内容を詰めていくこと想定する。内容について参画する各国のエキスパートから合意を得た後、2025 年度上期中に DTS(Draft Technical Specification)投票へ進め、その後承認段階へ移行することを想定する。

図表 3-4 CPSF 等に基づく国際規格策定に向けたロードマップ



3.3.2 国内外の関係機関・関係者の巻き込み

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・関係者に対して巻き込みを行った。

図表.3-5 国内外の関係機関・関係者との意見交換の状況

	2024年										2025年		
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	
SC 27/WG 4				★ 中間会合 (リモート)	 WD (第2版)	意見募集 (CfC)	★ WG会合 (ハイブリッド)	 WD (第3版)	意見募集 (CfC)			★ WG会合 (ハイブリッド)	

3.3.3 CPSF 等に基づく国際規格(案)の作成

これまでに述べたように、ISO/IEC WD 5689 は DTS に移行する。本事業では、WD 及び DTS の作成を含め、CPSF 等に基づく国際規格(案)の作成を推進した。

3.3.4 サプライチェーンのサイバーセキュリティに係る動向調査

本事業項目では、これまでに述べた国際規格を直接的に推進する活動に加え、それを補助する目的で、米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的としたリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関する国際規格、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。調査結果の詳細については別紙を参照されたい。

図表 3-6 調査対象文献一覧

No.		
1	英国	Cyber Essentials
2	米国	Cybersecurity Maturity Model Certification
3	米国	Cross-Sector Cybersecurity Performance Goals
4	豪州	Essential Eight

<参考文献>

- 1 ISO/IEC ISO/IEC 27009:2020 (2023 年 5 月 3 日に撤回済み)
(<https://www.iso.org/standard/73907.html#lifecycle>)
- 2 日本産業標準調査会 “国際標準化について”
(https://www.jisc.go.jp/international/international_standardization.html)
- 3 貴省産業技術環境局基準認証ユニット“標準化実務入門(標準化教材)” “2.規格、標準とは”, 2016 年 1 月 7 日改定
(https://www.meti.go.jp/policy/economy/hyojun-kijun/katsuyo/jitsumu-nyumon/pdf/2015text_zenbun.pdf)
- 4 “ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection”,
(<https://www.iso.org/committee/45306.html>)
- 5 一般社団法人 情報処理学会 情報規格調査会 “委員会一覧”
(<https://itscj.ipsj.or.jp/committee-activities/committee-list.html>)
- 6 ISO/IEC 専門業務用指針第 1 部及び統合版 ISO 補足指針(2024 年版) 英和对訳版
(https://webdesk.jsa.or.jp/pdf/dev/md_6452.pdf)
- 7 参考文献 1 “第 3 節 JTC1”参照

<商標又は登録商標>

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

経済産業省 商務情報政策局 サイバーセキュリティ課 御中

サイバーセキュリティに関する動向等についての調査

- 本調査は、既存のガイドライン等の一元的な管理・体系化、企業のセキュリティ対策基準の明確化を目的として行った。
- 1章や2章において、国内外で策定されている制度やガイドライン等の現状(As-Is)を調査した上で、3.1節で国内のガイドライン等の一元的な管理・体系化を行うにあたってのあるべき姿(To-Be)を整理した。また、3.2節及び3.3節では、現状(As-Is)とあるべき姿(To-Be)の比較結果から課題等を分析した上で、既存のガイドライン等の一元的な管理・体系化を行うための方向性(案)を作成した。

<1章 既に国内外で策定されている制度やガイドライン等の概要の調査>

- 日本において、重要インフラ分野を対象にしたガイドラインは一定の体系化がなされている。また、CPSFや経営ガイドライン等では個別に体系化がなされている。
- 各国、各地域においても、体系化の観点で以下の点は参考となると考えられる。
 - 米国において、中心となる標準(NIST SP800-53)とその手段が規定されている関連文書を策定。
 - 国際機関において、業種横断と業種個別の文書が同じ枠組みで体系化されるよう整理。

<2章 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の調査>

- ガイドライン及び基準について、「A.位置づけ、参照関係、関係性」及び「B.記載内容」の2つから調査。
- 「A.位置づけ、参照関係、関係性」について、大きく以下の3つに分類した。
 - 制度対応に必要な基準の位置づけが明確
 - 制度対応に必要な基準とガイドライン等との関係が不明確
 - 任意のガイドラインのみを提示
- 「B.記載内容」について、記載範囲と記載粒度の観点から調査した。製品(例:IoT機器)を対象とした基準やガイドラインを除いて、NIST CSFの記載範囲は概ね網羅(33の調査対象のうち、24の基準・ガイドラインが8割の項目を満たす)されていた。また、ISO/IEC 27001と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載がみられたが、認証方法等の一部の要求事項には粒度が粗いものもみられた。

<3章 今後の注力領域及び方向性(案)の整理>

- ガイドライン及び基準のあるべき姿について、「A.位置づけ、参照関係、関係性」及び「B.記載内容」で整理。
 - A.位置づけ、参照関係、関係性(共通):位置付け、参照関係、関係性等が明確であり、かつ、どの読者にとって何を読めばよいかが明確となっている状態をあるべき姿とする。
 - ✓ 体系内:法律等でセキュリティ対策義務が定義されている場合には、適切な法律等(例:サイバーセキュリティ基本法や業法)に基づき基準やガイドラインが策定されている状態をあるべき姿とする。また、法律等でセキュリティ対策義務が定義されていない場合には、体系内のガイドライン間で位置づけが明確に定義されている状態をあるべき姿とする。
 - ✓ 体系間:各分野で漏れなく基準やガイドライン等が策定されている状態をあるべき姿とする。
 - B.記載内容:近年増加している脅威に対処可能な要求事項が定められている状態をあるべき姿とする。
- 1章及び2章の調査結果を踏まえつつ、対処すべき現状の問題を整理。
 - A.位置づけ、参照関係、関係性
 - [1.1]事業者にとって、どの基準やガイドライン等を参照すればよいか不明確となっている。
 - [1.2]サイバーセキュリティ確保のための遵守が義務となっている基準が具体化されておらず、遵守すべき基準が不明確となっている。
 - B.記載内容:
 - [2.1]国際的に参照されているNIST CSFと比較した際に、ガイドライン等によっては記載範囲が限定的となっており、脅威に適切に対処できない可能性がある。
 - [2.2]ガイドライン等によっては、読者が理解し実装できるレベルまで要求事項が具体的に記載されておらず、脅威に適切に対処できない可能性がある。
- 貴省(及びガイドラインを一元管理する団体)では、大きく分けて3つの施策の方向性が考えられる。
 - ガイドラインの体系化
 - 民間事業者に対する情報提供
 - 関係者に対する助言

<まとめ>

- 貴省では、これまで様々な形でサイバーセキュリティに関するガイドラインを公開しており、民間事業者におけるセキュリティ対策の推進に貢献している。一方で、省庁横断的に調整を図るような仕組みが導入されているとは言えず、ガイドラインが思うように普及していない現状に鑑み、既存のガイドライン等の一元的な管理・体系化を行うことを目的として本調査を行った。
- 日本においても制度やガイドラインの体系化を意識した取組がみられた一方で、全ての制度やガイドライン等が一元的に管理・体系化されているとは言えなかった。そこでは、事業者にとって参照すべき基準やガイドライン等が不明確となっているケースや参照すべき基準やガイドライン等が明確であっても、その基準が具体化されていないケースがみられた。また、記載内容の面でも偏りや具体化の面で課題が残るケースもみられた。
- 社会全体のセキュリティレベル向上のために、貴省において以下の取組が必要と考えられる。また、各取組を行うために法制度的な権限の付与やリソース面での調整が必要となると考えられる。
 - 短期的には、貴省によるガイドラインを一元管理する団体の明確化
 - 短中期的には、貴省やガイドラインを一元管理する団体を中心としてガイドラインのカタログ化に向けた取組の推進
 - 中長期的には、ガイドラインを一元管理する団体が旗振り役となり、カタログ化されたガイドラインに対する採番や、民間事業者へのわかりやすい情報の提供、各所管省庁等へ助言に向けた取組の推進



調査報告書(本編)

調査目的/調査内容 (1/2)

- 既存のガイドライン等の一元的な管理・体系化等を主な目的として、国内外のガイドラインの概要を調査しつつ、国内のガイドラインの位置づけ等を明らかにした上で、今後の注力領域及び方向性(案)の整理を行う。

調査目的

- 既存のガイドライン等の一元的な管理・体系化、企業のセキュリティ対策基準の明確化
- 既存ガイドライン等との整合性確保、業種横断的なセキュリティ対策レベル評価

調査内容

- 1章や2章で国内外で策定されている制度やガイドライン等の現状(As-Is)を調査した上で、3.1節で国内のガイドライン等の一元的な管理・体系化を行うにあたってのあるべき姿(To-Be)を整理する。
- 3.2節及び3.3節では、現状(As-Is)とあるべき姿(To-Be)の比較結果から課題等を分析した上で、既存のガイドライン等の一元的な管理・体系化を行うための方向性(案)を作成する。

分類	調査項目	
1. 既に国内外で策定されている制度やガイドライン等の概要の調査		
1.1 国内で策定されている制度やガイドライン等の概要	1.1.1 業種横断のガイドライン	日本国内外の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の概要について調査する。
	1.1.2 業種別のガイドライン	
	1.1.3 まとめ	
1.2 国外で策定されている制度やガイドライン等の概要	1.2.1 米国における制度やガイドライン等	日本国内の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細について調査する。
	1.2.2 欧州における制度やガイドライン等(EU加盟国及び英国)	
	1.2.3 国際機関(ISO/IEC、ITU-T)における制度やガイドライン等	
	1.2.4 まとめ	

調査内容(続き)

分類	調査項目	
2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の調査		
2.1 業種横断	2.1.1 情報システム関連	日本国内の政府機関または業界団体等が公開するサイバーセキュリティに関するガイドライン及び基準の詳細について調査する。
	2.1.2 制御システム関連	
	2.1.3 製品・サービス関連	
	2.1.4 IoT・CPS関連	
	2.1.5 その他	
2.2 業種別	2.2.1 政府情報システム	
	2.2.2 重要インフラ(15業種)	
	2.2.3 重要インフラ以外	
3. 今後の注力領域及び方向性(案)の整理		
3.1 文書のあるべき姿の具体化/文書の整理状況の可視化	3.1.1 文書のあるべき姿の具体化	1及び2で調査を行った対象を踏まえつつ、あるべき姿を具体化した上で、対処すべき現状の問題を整理し、今後の方向性(案)の整理を行った。
	3.1.2 文書の整理状況の可視化	
3.2 対処すべき現状の問題の整理	-	
3.3 今後の方向性(案)の整理	-	

1. 既に国内外で策定されている制度や ガイドライン等の概要

まとめ

- 日本において、重要インフラ分野を対象にしたガイドラインは一定の体系化がなされている。また、CPSFや経営ガイドライン等では個別に体系化がなされている。
- 各国、各地域においても、体系化の観点で以下の点は参考となる。[赤太字下線部]
 - ✓ 米国において、中心となる標準(NIST SP800-53)とその手段を規定されている関連文書が策定されている。
 - ✓ 国際機関において、業種横断と業種個別の文書が同じ枠組みで体系化されるよう整理されている。

分類	日本	米国	EU	国際機関
管理状況 (主体)	- 重要インフラ分野では、NISCが全体を俯瞰しつつ、所管省庁(又は業界団体)がガイドラインを策定。 - 重要インフラ分野を除く分野では経産省(IPAを含む)が独自にガイドラインを策定している場合もある。	- FISMAや大統領令等に基づき、主に政府情報システム及び関連分野についてNISTが標準策定を行う。また、OMBによる指令はNISTが策定した標準への準拠を各省庁へ要求している。NISTに対して標準策定機能に係る明確な位置づけがされている。 - 一方で、個別のガイドラインについては、CISAや各所管省庁が個別に策定している場合がみられ、標準策定機能が必ずしもNISTに一元化されていない。	- EUサイバーセキュリティ法によって権限強化されたENISAがガイドラインを策定。 - EUの標準機関として、CEN、CENELEC、ETSIが位置付けられ、EU標準(例:IoTの場合、ETSI 303 645)を策定。 - 欧州委員会から提案された規則や指令等によって、規定が策定される。規則は直接適用されるが、指令は各加盟国によって国内法が策定されることで、はじめて一般的な効力を持つ。	- ISO/IEC SC27にてISO/IEC 27001関連文書が策定され、IEC TC65にてIEC62443関連文書が策定。 - 業種横断の基準としてISO/IEC 27001が定められるとともに、業界個別の基準が策定される際に考慮すべき標準がISO/IEC 27009によって定められることよって、ISO/IEC 27001関連文書全体が関連付けられるよう整理されている。
体系化の状況 (ガイドライン)	- 重要インフラ分野では、安全基準等策定指針を中心として、個別の業法との関係性も意識しつつ、ガイドラインが体系化されている。ただし、内容面にかかるガイドラインは必ずしも安全基準等策定指針と対応していない部分がある可能性があり、NISCも対応を強制できない立場にある。 - 重要インフラを除く分野では、CPSFやサイバーセキュリティ経営ガイドライン、中小企業の情報セキュリティ対策ガイドラインと関連するガイドラインは、それぞれのガイドラインを頂点として体系化されているが、横の関係性の整理はなされていない。	- 政府情報システムにおいて、NIST SP800-53を中心としてガイドラインが策定されている。また、それを補足する形で個別の文書が策定されており、政府機関だけではなく、民間企業においても広く参照されている。 - 重要インフラ分野については、NIST CSFを中心として、実装のためのガイドライン等が策定されている。ただし、NIST CSFは任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。	- EUサイバーセキュリティ法に基づき、各分野において任意の認証制度(例:クラウド、5G)が構築されつつある。本認証制度の枠組みでは体系化がなされている。特に、制度の枠組みを構築した上で、標準を策定する点に特徴がみられる。 - 指令が定められた領域においては各加盟国間の法律は指令に基づき整理されている。	

1.1 国内で策定されている制度やガイドライン等の概要

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称*1	URL
1	日本	IT	ISMS-AC	ISMS適合性評価制度	https://isms.jp/isms.html
2				ISMSユーザズガイド － JIS Q 27001:2014 (ISO/IEC 27001:2013対応)	https://www.jipdec.or.jp/library/smpo_doc.html
3			JIS	JIS Q 27001	https://www.jisa.or.jp/ms-sp-1/jisq27001/
4			経済産業省	情報セキュリティ監査基準(平成15年経済産業省告示第114号)	https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf
5				情報セキュリティ管理基準(平成28年経済産業省告示第37号)	https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf
6				個別管理基準(監査項目)策定ガイドライン Ver1.0	https://www.meti.go.jp/policy/netsecurity/is-kansa/kobetsukanrikijun.pdf
7			経済産業省・IPA	サイバーセキュリティ経営ガイドライン Ver3.0	https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
8				付録C サイバーセキュリティインシデントに備えるための参考情報	https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.meti.go.jp%2Fpolicy%2Fnetsecurity%2Fdownloadfiles%2FCSM_Guideline_app_C_for_3.0.xlsx&wdOrigin=BROWSELINK
9				付録F サイバーセキュリティ体制構築・人材確保の手引き第2.0版	https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
10			IPA	中小企業の情報セキュリティ対策ガイドライン第3.1版	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
11				付録1：情報セキュリティ5か条	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055516.pdf
12		OT	ISMS-AC	CSMS適合性評価制度	https://isms.jp/csms.html
13			JIPDEC	CSMS認証基準(IEC62443-2-1) Ver.2.0	https://isms.jp/csms/doc/JIP-CSCC100-20.pdf
14			経済産業省	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer 1.0	https://www.meti.go.jp/policy/netsecurity/wq1/factorysystems_guideline_ver1.0.pdf
15			IPA	制御システムのセキュリティリスク分析ガイド(2023年3月版)	https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

* 黒字の全てを調査した場合、調査結果が煩雑となるため、文献をグループ化して調査を行った。

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称	URL
16	日本	製品	IPA	ITセキュリティ評価及び認証制度(JISEC)	https://www.ipa.go.jp/security/jisec/index.html
17				CC/CEM:2022 リリース1	https://www.ipa.go.jp/security/jisec/about/kijun.html
18			経済産業省	IT 製品の調達におけるセキュリティ要件リスト	https://www.ipa.go.jp/security/jisec/pps/certified-pps/gmcbt80000008p6e-att/cclistmetisec2018.pdf
19				IoT 製品に対する セキュリティ適合性評価制度 (仮)	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240315_1.pdf
20				☆1セキュリティ要件・適合基準	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240315_3.pdf
21			総務省	電気通信事業法	https://elaws.e-gov.go.jp/document?lawid=359AC0000000086
22				端末設備等規則	https://elaws.e-gov.go.jp/document?lawid=360M50001000031
23				電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)	https://www.soumu.go.jp/main_content/000615696.pdf
24		サービス	ISMS-AC	ISMSクラウドセキュリティ認証	https://isms.jp/isms-cls.html
25			JIPDEC	ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項	https://www.jipdec.or.jp/archives/publications/JIP-ISMS517-10.pdf
26			ISMS-AC	ISMSユーザーズガイド追補 ～クラウドを含む新たなリスクへの対応～	https://www.jipdec.or.jp/archives/publications/JIP-ISMS111-3.0_S1-10.pdf
27			経済産業省	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf
28			総務省	クラウドサービス利用・提供における適切な設定のためのガイドライン	https://www.soumu.go.jp/main_content/000843318.pdf
29			NISC	クラウドを利用したシステム運用に関するガイダンス	https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html
30			IPA	中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf
31			経済産業省	情報セキュリティサービス審査登録制度	https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html
32				情報セキュリティサービス基準第4版	https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhouukizyun4.pdf
33		IoT・CPS	経済産業省・総務省	IoT セキュリティガイドライン ver 1.0	https://www.soumu.go.jp/main_content/000428393.pdf
34			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	https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf
35				IoTセキュリティ・セーフティ・フレームワーク (IoT-SSF) Ver1.0	https://www.meti.go.jp/policy/netsecurity/wg1/IoT-SSF_ver1.0.pdf

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称	URL
36	日本	その他	経済産業省	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	https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf
37				ソフトウェア管理に向けたSBOMの導入に関する手引 Ver1.0	https://www.meti.go.jp/policy/netsecurity/wg1/sbom_tebiki.pdf
38				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 Ver1.1	https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework_1_1.pdf
39			IPA	脆弱性対処に向けた製品開発者向けガイド	https://www.ipa.go.jp/security/guide/vuln/ug65p90000019bum-att/000085024.pdf
40				ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル 第5版	https://www.ipa.go.jp/security/guide/vuln/ug65p90000019bum-att/000081019.pdf
41				ECサイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf
42			総務省	5G セキュリティガイドライン第1版	https://www.soumu.go.jp/main_content/000812253.pdf
43				テレワークセキュリティガイドライン第5版	https://www.soumu.go.jp/main_content/000752925.pdf
44				中小企業等担当者向けテレワークセキュリティの手引き	https://www.soumu.go.jp/main_content/000816096.pdf
45		政府	NISC	政府機関等のサイバーセキュリティ対策のための統一規範	https://www.nisc.go.jp/pdf/policy/general/kihanr5.pdf
46				IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ	https://www.nisc.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf
47				政府機関等のサイバーセキュリティ対策のための統一基準	https://www.nisc.go.jp/pdf/policy/general/kiyunr5.pdf
48				政府機関等の対策基準策定のためのガイドライン	https://www.nisc.go.jp/pdf/policy/general/guider5.pdf
49				対策推進計画策定マニュアル	https://www.nisc.go.jp/pdf/policy/general/sakutei-manual.pdf
50				政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書	https://www.nisc.go.jp/pdf/policy/general/R5_AuditManual.pdf
51				情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html
52				外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書	https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
53				政府機関等における情報システム運用継続計画ガイドライン	https://www.nisc.go.jp/pdf/policy/general/itbcp1-1_3.pdf
54				スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	https://www.nisc.go.jp/pdf/policy/general/smartphone28.pdf

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称	URL
55	日本	重要 インフラ 全般	NISC	重要インフラのサイバーセキュリティに係る行動計画	https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf
56				重要インフラのサイバーセキュリティに係る安全基準等策定指針	https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf
57				重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書	https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf
58	電気 通信	総務省		事業用電気通信設備規則	https://elaws.e-gov.go.jp/document?lawid=360M50001000030
59				情報通信ネットワーク安全・信頼性基準	https://www.soumu.go.jp/main_content/000908610.pdf
60				電気通信分野におけるサイバーセキュリティに係る安全基準(第1版)	https://www.tca.or.jp/information/pdf/networksecurity/anzenkijun1.pdf
61	放送	総務省		放送法施行規則	https://elaws.e-gov.go.jp/document?lawid=325M50080000010
62				ICT-ISAC 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン	-
63				放送設備サイバー攻撃対策ガイドライン(第3版)	-
64	ケーブル テレビ	日本ケーブル テレビ連盟		ケーブルテレビにおけるサイバーセキュリティに係る安全基準(第1版)	https://www.catv-jcta.jp/public2/member_a/security/item/infra_guideline.pdf
65	金融	FISC		金融機関等コンピュータシステムの安全対策基準・解説書(第11版)	https://www.fisc.or.jp/publication/guideline_pdf.php
66				金融機関等におけるセキュリティポリシー策定のための手引書	https://www.fisc.or.jp/publication/guideline_pdf.php
67				金融機関等におけるコンティンジェンシープラン策定のための手引書(第4版)	https://www.fisc.or.jp/publication/guideline_pdf.php
68	航空	国土交通省		航空分野における情報セキュリティ確保に係る安全ガイドライン(第5版)	https://www.mlit.go.jp/common/001283895.pdf
69	空港			空港分野における情報セキュリティ確保に係る安全ガイドライン(第2版)	https://www.mlit.go.jp/common/001283896.pdf
70	鉄道			鉄道分野における情報セキュリティ確保に係る安全ガイドライン(第4版)	https://www.mlit.go.jp/common/001283894.pdf
71	電力	経済産業省		電気設備に関する技術基準を定める省令	https://elaws.e-gov.go.jp/document?lawid=409M50000400052
72				電気事業法施行規則第50条第2項の解釈適用に当たっての考え方	https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/11/20221130-3.pdf
73				電気設備の技術基準の解釈	https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/dengikaishaku.pdf
74		日本電気技 術規格委員		電力制御システムセキュリティガイドライン	https://store.denki.or.jp/products/detail/676
75				スマートメーターシステムセキュリティガイドライン	https://store.denki.or.jp/products/detail/640
76		経済産業省		自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称	URL
77	日本	ガス	経済産業省	ガス事業法施行規則	https://elaws.e-gov.go.jp/document?lawid=345M50000400097
78			日本ガス協会	都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説	-
79		自治体	総務省	地方公共団体における情報セキュリティポリシーに関するガイドライン	https://www.soumu.go.jp/main_content/000805453.pdf
80		医療	厚生労働省	医療法施行規則	https://elaws.e-gov.go.jp/document?lawid=323M40000100050
81				医療情報システムの安全管理に関するガイドライン 第6.0版 (概説編)	https://www.mhlw.go.jp/content/10808000/001102570.pdf
82				医療情報システムの安全管理に関するガイドライン 第6.0版 (経営管理編)	https://www.mhlw.go.jp/content/10808000/001102573.pdf
83				医療情報システムの安全管理に関するガイドライン 第6.0版 (企画管理編)	https://www.mhlw.go.jp/content/10808000/001102575.pdf
84				医療情報システムの安全管理に関するガイドライン 第6.0版 (システム運用編)	https://www.mhlw.go.jp/content/10808000/001112044.pdf
85				医療機関におけるサイバーセキュリティ対策チェックリスト	https://www.mhlw.go.jp/content/10808000/001139055.pdf
86		水道	厚生労働省	水道分野における情報セキュリティガイドライン (第4版)	https://www.mhlw.go.jp/content/000731327.pdf
87		物流	国土交通省	物流分野における情報セキュリティ確保に係る安全ガイドライン (第4版)	https://www.mlit.go.jp/common/001283898.pdf
88		化学	石油化学工業協会	石油化学分野における情報セキュリティ確保に係る安全基準	-
89		クレジット	クレジット取引セキュリティ対策協議会	クレジットカード・セキュリティガイドライン【5.0 版】	https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_5.0_published.pdf
90		石油	石油連盟	石油分野における情報セキュリティ確保に係る安全ガイドライン	-
91		ビル	経済産業省	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版	https://www.meti.go.jp/policy/netsecurity/wg1/bill_guideline_2.pdf
92				ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編：空調システム)第1版	https://www.meti.go.jp/policy/netsecurity/wg1/wg1_kuchou_guideline.pdf
93		スマートホーム	経済産業省	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0	https://www.meti.go.jp/policy/netsecurity/wg1/smarthomeguideline_ver1.0.pdf
94		宇宙	経済産業省	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0	https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_ucho_sangyo/pdf/20240327_1.pdf
95		自動車	自工会	自工会/部工会・サイバーセキュリティガイドライン V2.1	https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_01.pdf

調査対象一覧/日本国内

No.	国・地域	分類	策定者等	文献等の名称	URL
96	日本	防衛	防衛装備庁	装備品等及び役務の調達における情報セキュリティの確保に関する特約条項	https://www.mod.go.jp/atla/cybersecurity/tokuyaku_r05.pdf
97				装備品等及び役務の調達における情報セキュリティ基準	https://www.mod.go.jp/atla/cybersecurity/kijun_r05.pdf
98				装備品等及び役務の調達における情報セキュリティ基準の解説①	https://www.mod.go.jp/atla/cybersecurity/kijun_kaisetsu01_r050712.pdf
99				装備品等及び役務の調達における情報セキュリティ基準の解説②	https://www.mod.go.jp/atla/cybersecurity/kijun_kaisetsu02_r050712.pdf

サマリ(業種横断)

- 今回の調査で扱った認証制度等のうち、「端末機器の基準認証制度」及び「政府機関等のサイバーセキュリティ対策のための統一基準群」には遵守義務がある。

	ISMS適合性評価制度	ISMSクラウドセキュリティ認証	CSMS適合性評価制度	端末機器の基準認証制度	政府機関等のサイバーセキュリティ対策のための統一基準群
種別 ^{*1}	制度	制度	制度	制度	基準
遵守義務	なし	なし	なし	あり	あり
対象分野・システム	情報システム全般	クラウドサービス	産業用オートメーション及び制御システム	端末機器^{*2}	政府情報システム
対象者	ISMS認証の取得を希望する団体	- 認証取得を希望するクラウドサービスプロバイダ - 認証取得を希望するクラウドサービスカスタマ	CSMS認証の取得を希望する団体	製造事業者	- 政府機関 - 独立行政法人 等
概要	第三者であるISMS認証機関が、組織の構築したISMSが <u>ISO/IEC 27001(JIS Q 27001)に基づいて適切に運用管理されているかを証明する制度。</u>	通常のISMS認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が適切に導入、実施されていることを認証する。	産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度。	電気事業法に基づき、事業者のネットワークに接続して使用される端末機器(その設計含む)について「<u>接続の技術基準</u>」に適合していることを登録認定機関等が認定する制度。	政府統一基準は、サイバーセキュリティ基本法に基づく、<u>政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み。</u>

*1 制度/基準/ガイドラインにて分類

*2 端末機器は、アナログ電話用設備、インターネットプロトコル電話用設備、インターネットプロトコル移動電話用設備、無線呼出用設備、総合デジタル通信用設備、専用通信回線設備

サマリ(業種別) (1/2)

- 「金融機関等コンピュータシステムの安全対策基準・解説書(第12版)」や「電力制御システムセキュリティガイドライン」のように実質的な義務となっている基準が見受けられる。

	重要インフラのサイバーセキュリティに係る行動計画	重要インフラのサイバーセキュリティに係る安全基準等策定指針	金融機関等コンピュータシステムの安全対策基準・解説書(第12版)	電気通信分野におけるサイバーセキュリティに係る安全基準	電力制御システムセキュリティガイドライン	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
種別 ^{*1}	制度	ガイドライン	基準	ガイドライン	基準	基準
遵守義務	なし	なし	あり ^{*2}	なし	あり ^{*3}	あり ^{*4}
対象分野・システム	・ 重要インフラ分野	・ 重要インフラ分野	・ 金融情報システム	・ 電気通信分野	電力制御システムや電力制御用ネットワーク	・ 自家用電気工作物の遠隔監視システム等、制御システム等
対象者	・ 政府機関 ・ 重要インフラ事業者 ・ サプライチェーン等に関わる事業者	・ 重要インフラ事業者等	・ 金融機関 等	・ 電気通信事業者 ・ 電気通信設備提供者(メーカ等)	・ 電気事業者が施設する電力制御システム等に携わる者	・ 自家用電気工作物を設置する者
概要	- サイバーセキュリティ戦略を踏まえ、同法第4条及び第26条の規定に基づき策定するもの。 ①「重要インフラ防護」の目的、②関係主体の責務、③基本的な考え方、④障害対応体制の強化に向けた取組等を規定。	重要インフラ行動計画に示された重要インフラにおける機能保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、「安全基準等」において規定が望まれる項目を整理・記載している。	日本の金融機関等が、事業展開を行ううえで金融情報システムを活用するに際し、開発や導入、運用等において必要と考えられる安全対策を基準として示すとともに、基準項目ごとに、具体的な事例を交えて解説するもの。	電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準について業界団体が定めるガイドラインを、政府指針に基づき策定したもの。	本ガイドラインは、電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載したものである。	本ガイドラインは、自家用電気工作物の遠隔監視システム等や制御システム等のライフサイクルにおけるサイバーセキュリティについて規定したものである。

^{*1} 制度/基準/ガイドラインにて分類

^{*2} あくまでも自主基準とされており強制力はないとされているが、預金等受入金融機関にとって本ガイドラインが実質的な義務となっている可能性がある。

^{*3} 本ガイドラインは勧告的事項と推奨的事項を定めているが、「審査基準」として位置付けられている「技術基準の解釈」によって引用されているため、実質的には義務となっている。

^{*4} 勧告的事項に該当する場合は遵守義務があるが、推奨的事項の場合には遵守義務はない。

サマリ(業種別) (2/2)

	地方公共団体における情報セキュリティポリシーに関するガイドライン	医療情報システムの安全管理に関するガイドライン	水道分野における情報セキュリティガイドライン	物流分野における情報セキュリティ確保に係る安全ガイドライン(貨物自動車運送/倉庫)	クレジットカード・セキュリティガイドライン	装備品等及び役務の調達における情報セキュリティ基準
種別 ^{*1}	基準	基準	ガイドライン	ガイドライン	基準	基準
遵守義務	あり ^{*1}	あり ^{*2}	なし	なし	あり	あり
対象分野・システム	・ 地方公共団体	・ 医療情報システム	・ 水道情報システム	・ 物流情報システム	クレジットカード分野	・ 防衛分野
対象者	- 情報セキュリティポリシーの策定を行う者 - セキュリティ上の職責を担う者	医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者	- 水道事業者 - 水道用水供給事業者	物流分野の重要インフラ事業者等	- 加盟店/カード会社/決済代行業者等^{*3} - 上記の事業者が対策を実施するに際し協力等を行う団体	防衛関連企業において保護すべき情報に接する全ての者^{*4}
概要	本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、<u>情報セキュリティポリシーの考え方及び内容について解説</u>したもの。	本ガイドラインは、e-文書法等の法令等への適切な対応を行うため、<u>技術的及び運用管理上の観点から所要の対策を示したものである。</u>	<u>水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示したものの。</u> 「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第5版)」における「安全基準等」に位置づけられるもの。	セキュリティ管理策の水準を示すことで、個々の重要インフラ事業者等が、重要インフラの担い手としての意識に基づいて<u>自主的に取り組み、対策の実施や検証に当たっての目標を定めることを目的とする。</u>	安全・安心なクレジットカード利用環境を整備するため、関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のための<u>セキュリティ対策の取組を取りまとめたもの。</u>	本基準は、装備品等及び役務の調達に係る企業において<u>当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。</u>

^{*1} ポリシーの策定は義務であるが、ガイドラインに記載された具体的な項目の記載は必ずしも義務ではない。また、総務大臣通知による要請によって、対策の実施が義務となる場合がある。

^{*2} 本ガイドラインにおいて優先的に取り組むべき事項を整理したチェックリストは立入検査の際に参照されるため、実質的に義務となっている可能性がある。

^{*3} セキュリティ対策の実施主体である「加盟店」や「カード会社(イシュー・アクワイアラー)」、「決済代行業者等(4号事業者)」、「コード決済事業者等(5号事業者)」、「コード決済事業者等の委託会社(6号事業者)」、「加盟店向け決済システム提供事業者(7号事業者)」

^{*4} 防衛調達に関わる企業に対して遵守を義務付け

1.2 国外で策定されている制度やガイドライン等の概要

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称* ¹	URL
1	米国	IT	NIST	SP 800-53 Rev.5 情報システム・組織向けのセキュリティ・プライバシー管理策	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092657.pdf
2				SP 800-53A Rev.5 情報システム・組織向けのセキュリティ・プライバシー管理策の評価	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf
3				SP 800-53B 情報システム・組織向け管理策ベースライン	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092658.pdf
4				SP 800-18 連邦情報システムのセキュリティ計画策定に関する手引き	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025324.pdf
5				SP 800-30 Rev.1 リスクアセスメント実施の手引き	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025325.pdf
6				SP 800-37 Rev.2 情報システム・組織向けリスクマネジメントフレームワーク	https://csrc.nist.gov/pubs/sp/800/37/r2/final
7				SP 800-60 Vol.1 Rev.1 情報及び情報システムの種別とセキュリティ分類のマッピングに関する手引き	https://csrc.nist.gov/pubs/sp/800/60/v1/r1/final
8		OT	NIST	SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security	https://csrc.nist.gov/pubs/sp/800/82/r3/final
9			CISA	ICS Recommended Practices	https://www.cisa.gov/resources-tools/resources/ics-recommended-practices
10	製品		NIAP	Common Criteria Evaluation and Validation Scheme	https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm
11			FCC	U.S. Cybersecurity Labeling Program for Smart Devices	https://www.fcc.gov/cybersecurity-certification-mark
12			NIST	NISTIR 8259: Recommendations for IoT Device Manufacturers: Foundational Activities	https://csrc.nist.gov/pubs/ir/8259/final
13				NISTIR 8259A: Core Device Cybersecurity Capability Baseline	https://csrc.nist.gov/pubs/ir/8259/a/final
14				NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline	https://csrc.nist.gov/publications/detail/nistir/8259b/final
15				NISTIR 8425: Profile of the IoT Core Baseline for Consumer IoT Products	https://csrc.nist.gov/pubs/ir/8425/final
16				Product Development Cybersecurity Handbook: Concepts and Considerations for IoT Product Manufacturers	https://csrc.nist.gov/pubs/cswp/33/product-development-cybersecurity-handbook/ipd

* 黒字の全てを調査した場合、調査結果が煩雑となるため、文献をグループ化して調査を行った。

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
17	米国	サービス	FedRAMP PMO	The Federal Risk and Authorization Management Program (FedRAMP)	https://www.fedramp.gov/program-basics/
18				FedRAMP Security Controls Baseline	https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.fedramp.gov%2Fassets%2Fresources%2Fdocuments%2FFedRAMP_Security_Controls_Baseline.xlsx&wdO_rigin=BROWSELINK
19				FedRAMP High, Moderate, Low, LI-SaaS Baseline System Security Plan (SSP)	https://www.fedramp.gov/assets/resources/templates/FedRAMP-High-Moderate-Low-LI-SaaS-Baseline-System-Security-Plan-(SSP).docx
20		政府	連邦議会	連邦情報セキュリティ近代化法(FISMA)	https://www.congress.gov/bill/113th-congress/senate-bill/2521
21			OMB	CIRCULAR NO. A-130 Revised	https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4
22			NIST	FIPS 199 連邦政府の情報および情報システムに対するセキュリティ分類規格	https://www.ipa.go.jp/security/reports/oversea/nist/uq65p9000019cp4-att/000025321.pdf
23				FIPS 200 連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項	https://www.ipa.go.jp/security/reports/oversea/nist/uq65p9000019cp4-att/000025322.pdf
24			大統領府	Executive Order 13556—Controlled Unclassified Information	https://www.presidency.ucsb.edu/documents/executive-order-13556-controlled-unclassified-information
25			NIST	SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
26				SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	https://csrc.nist.gov/pubs/sp/800/172/final
27			OMB	OMB M-04-04 連邦政府機関向けの電子認証にかかわるガイダンス	https://www.ipa.go.jp/security/reports/oversea/nist/uq65p9000019cp4-att/000025320.pdf
28			NIST	SP 800-63-4 (Initial Public Draft) Digital Identity Guidelines	https://csrc.nist.gov/pubs/sp/800/63/4/ipd
29			大統領府	Executive Order 14028—Improving the Nation's Cybersecurity	https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf
30			OMB	M-21-30 Protecting Critical Software Through Enhanced Security Measures	https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf
31			NIST	Definition of Critical Software Under Executive Order (EO) 14028	https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf
32				Security Measures for EO-Critical Software Use	https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
33	米国	政府	OMB	M-23-16 Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices	https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf
34			NIST	SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	https://csrc.nist.gov/pubs/sp/800/218/final
35		重要インフラ全般	大統領府	Executive Order 13636—Improving Critical Infrastructure Cybersecurity	https://www.presidency.ucsb.edu/documents/executive-order-13636-improving-critical-infrastructure-cybersecurity
36				Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	https://www.presidency.ucsb.edu/documents/executive-order-13800-strengthening-the-cybersecurity-federal-networks-and-critical
37			NIST	The NIST Cybersecurity Framework (CSF) 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
38				NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf
39			CISA	Cross-Sector Cybersecurity Performance Goals	https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
40		化学	CISA	Chemical Sector Cybersecurity Framework Implementation Guidance	https://www.cisa.gov/sites/default/files/publications/Chemical_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf
41		重要製造	CISA	Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance	https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation-guidance
42		防衛産業	国防総省 (DoD)	DFARS 252.204-7012	https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting
43				The Cybersecurity Maturity Model Certification 2.0	https://dodcio.defense.gov/CMMC/Model/
44		電力	NERC	Critical Infrastructure Protection Standard(CIP) Version5	https://www.federalregister.gov/documents/2013/12/03/2013-28628/version-5-critical-infrastructure-protection-reliability-standards
45				Electricity Subsector Cybersecurity Capability Maturity Model Program(ES-C2M2)	https://www.energy.gov/oe/articles/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014
46				NIST IR 7628 Guidelines for Smart Grid Cybersecurity	https://csrc.nist.gov/pubs/ir/7628/r1/final

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
47	米国	医療	健康保健省 (HHS)	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule	https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
48			FDA	Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
49				Postmarket Management of Cybersecurity in Medical Devices	https://www.fda.gov/media/95862/download
50		交通	CISA	TSS Cybersecurity Framework Implementation Guidance	https://www.cisa.gov/resources-tools/resources/transportation-systems-sector-cybersecurity-framework-implementation-guide
51				Transportation Systems Sector Cybersecurity Framework Workbook	https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.cisa.gov%2Fsites%2Fdefault%2Ffiles%2Fpublications%2Ftss-cybersecurity-framework-workbook-2016-508.xlsx&wdOrigin=BROWSELINK
52	EU	上下水道	CISA, EPA, FBI	Top Cyber Actions for Securing Water Systems	https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems
53		製品	ENISA	Cybersecurity Guide for SMEs	https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
54			EU	Cyber Resilience Act	https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html
55			ETSI	ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
56				ETSI TR 103 621 Guide to Cyber Security for Consumer Internet of Things	https://www.etsi.org/deliver/etsi_tr/103600_103699/103621/01.02.01_60/tr_103621v010201p.pdf
57				ETSI TS 103 701 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
58	EU	製品	EU	The EU cybersecurity certification framework	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
59			欧州委員会	Union Rolling Work Programme for European cybersecurity certification	https://digital-strategy.ec.europa.eu/en/library/union-rolling-work-programme-european-cybersecurity-certification
60			EU	Commission Implementing Regulation (EU) as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482&qid=1707312751025
61			ENISA	Advancing Software Security in the EU	https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework
62		IoT・CPS	ENISA	Good Practices for Security of IoT - Secure Software Development Lifecycle	https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1
63		重要インフラ	EU	Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1713176161483
64				Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)	https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive
65				Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive)	https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-3-4-directive-eu-20222555-nis-2-directive
66		医療	ENISA	Cloud Security for Healthcare Services	https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services
67				Procurement Guidelines for Cybersecurity in Hospitals	https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
68		鉄道		Railway Cybersecurity - Good Practices in Cyber Risk Management	https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
69		港湾		Guidelines - Cyber Risk Management for Ports	https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
70	英国	IT	NCSC	Cyber Essentials	https://www.ncsc.gov.uk/cyberessentials/overview
71				Cyber Essentials: Requirements for IT infrastructure v3.1	https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf
72				Cyber Essentials Plus: Illustrative Test Specification v3.1	https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-Test-Specification-v3-1-April-2023.pdf
73				Cyber Security Small Business Guide	https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf
74				Cyber Security Response and Recovery	https://www.ncsc.gov.uk/files/NCSC_A5%20Response%20and%20Recovery%20Guide_v3_OCT20.pdf
75				10 Steps to Cyber Security	https://www.ncsc.gov.uk/collection/10-steps
76		OT	NCSC	Operational Technology: Making sense of cyber security in OT environments.	https://www.ncsc.gov.uk/collection/operational-technology
77		製品	議会	The Product Security and Telecommunications Infrastructure Regulations 2023	https://www.legislation.gov.uk/ukxi/2023/1007/contents/made
78		政府	政府セキュリティグループ	Government Functional Standard GovS 007: Security	https://assets.publishing.service.gov.uk/media/613a195bd3bf7f05b694d647/GovS_007-Security.pdf
79				Government Cyber Security Policy Handbook (GCSPH)	https://www.security.gov.uk/policy/gcsph/
80				Government Secure by Design Policy	https://www.security.gov.uk/policy/secure-by-design/
81				Government Cyber Security Policy: Mobile Device Management (MDM)	https://www.security.gov.uk/policy/mdm/mdm
82				Government Security Classifications	https://www.gov.uk/government/publications/government-security-classifications
83				Secure by Design Principles	https://www.security.gov.uk/guidance/secure-by-design/principles/
84				GovAssure	https://www.security.gov.uk/guidance/govassure/
85			NCSC	The Cyber Assessment Framework (CAF)	https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
86	重要インフラ	重要インフラ	議会	The Security of Network & Information Systems Regulations (NIS Regulations)	https://www.legislation.gov.uk/ukxi/2023/1007/contents/made

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
87	国際	IT	ISO/IEC JTC 1	ISO/IEC 27000:2018 – Information security management systems – Overview and vocabulary	https://www.iso.org/standard/73906.html
88				ISO/IEC 27001:2022 – Information security management systems – Requirements	https://www.iso.org/standard/27001
89				ISO/IEC 27002:2022 – information security controls	https://www.iso.org/standard/75652.html
90				ISO/IEC 27003:2017 – Information security management system – Guidance	https://www.iso.org/standard/63417.html
91				ISO/IEC 27004:2016 – Information security management – Monitoring, measurement, analysis and evaluation	https://www.iso.org/standard/64120.html
92				ISO/IEC 27005:2022 – Guidance on managing information security risks	https://www.iso.org/standard/80585.html
93				ISO/IEC 27007:2020 – Guidelines for information security management systems auditing	https://www.iso.org/standard/77802.html
94				ISO/IEC TS 27008:2019 – Guidelines for the assessment of information security controls	https://www.iso.org/standard/67397.html
95				ISO/IEC 27014:2020 –Governance of Information security	https://www.iso.org/standard/74046.html
96		OT	ISecure	ACS Security Assurance (ACSSA)	https://isasecure.org/isasecure-site-assessment
97				System Security Assurance (SSA)	https://isasecure.org/certification/iec-62443-ssa-certification
98			IEC TC 65	IEC 62443-1-1 Terminology, concepts and models	https://webstore.iec.ch/publication/7029
99				IEC 62443-2-1 Establishing an industrial automation and control system security program	https://webstore.iec.ch/publication/7030
100				IEC TR 62443-2-3 Patch management in the IACS environment	https://webstore.iec.ch/publication/22811
101				IEC 62443-2-4 Security program requirements for IACS service providers	https://webstore.iec.ch/publication/67631
102				IEC 62443-3-2 Security risk assessment for system design	https://webstore.iec.ch/publication/30727
103				IEC 62443-3-3 System security requirements and security levels	https://webstore.iec.ch/publication/7033

調査対象一覧/日本国外

No.	国・地域	分類	策定者等	文献等の名称	URL
104	国際	製品	-	Common Criteria Recognition Arrangement (CCRA)	https://www.commoncriteriaportal.org/index.cfm
105			ISO/IEC JTC 1	ISO/IEC 15408-1:2022 Evaluation criteria for IT security Part 1: Introduction and general model	https://www.iso.org/standard/72891.html
106				ISO/IEC 15408-2:2022 Evaluation criteria for IT security Part 2: Security functional components	https://www.iso.org/standard/72892.html
107				ISO/IEC 15408-3:2022 Evaluation criteria for IT security Part 3: Security assurance components	https://www.iso.org/standard/72906.html
108				ISO/IEC 15408-4:2022 Evaluation criteria for IT security Part 4: Framework for the specification of evaluation methods and activities	https://www.iso.org/standard/72913.html
109				ISO/IEC 15408-5:2022 Evaluation criteria for IT security Part 5: Pre-defined packages of security requirements	https://www.iso.org/standard/72917.html
110				ISO/IEC 27402:2023 IoT security and privacy Device baseline requirements	https://www.iso.org/standard/80136.html
111			ISAsure	Component Security Assurance (CSA)	https://isasure.org/certification/iec-62443-csa-certification
112				Security Development Lifecycle Assurance (SDLA)	https://isasure.org/certification/iec-62443-sdla-certification
113			IEC TC 65	IEC 62443-4-1 Secure product development lifecycle requirements	https://webstore.iec.ch/publication/33615
114				IEC 62443-4-2 Technical security requirements for IACS components	https://webstore.iec.ch/publication/34421
115	サービス	サービス	ISO/IEC JTC 1	ISO/IEC 27017:2015 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	https://www.iso.org/standard/43757.html
116			ISO/IEC JTC 1	ISO/IEC 27009:2020 – Sector-specific application of ISO/IEC 27001 – requirements	https://www.iso.org/standard/73907.html
117				ISO/IEC 27011:2024 – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	https://www.iso.org/standard/80584.html
118			エネルギー	ISO/IEC 27019:2017 – Information security controls for the energy utility Industry	https://www.iso.org/standard/68091.html



米国関連

米国における制度やガイドライン等(サマリ)

- 制度/基準/ガイドライン間では、大統領令や法律によって各文書の策定が指示されており、体系化がなされている。ガイドライン間では、NIST SP800-53やNIST Cybersecurity Framework(NIST CSF)を中心として各文書が体系化されている。ただし、重要インフラ分野では分野別のプロファイルが策定されている場合があり、全ての文書がNIST CSFを中心として体系化されているわけではない。

体系化の観点でみられた特徴

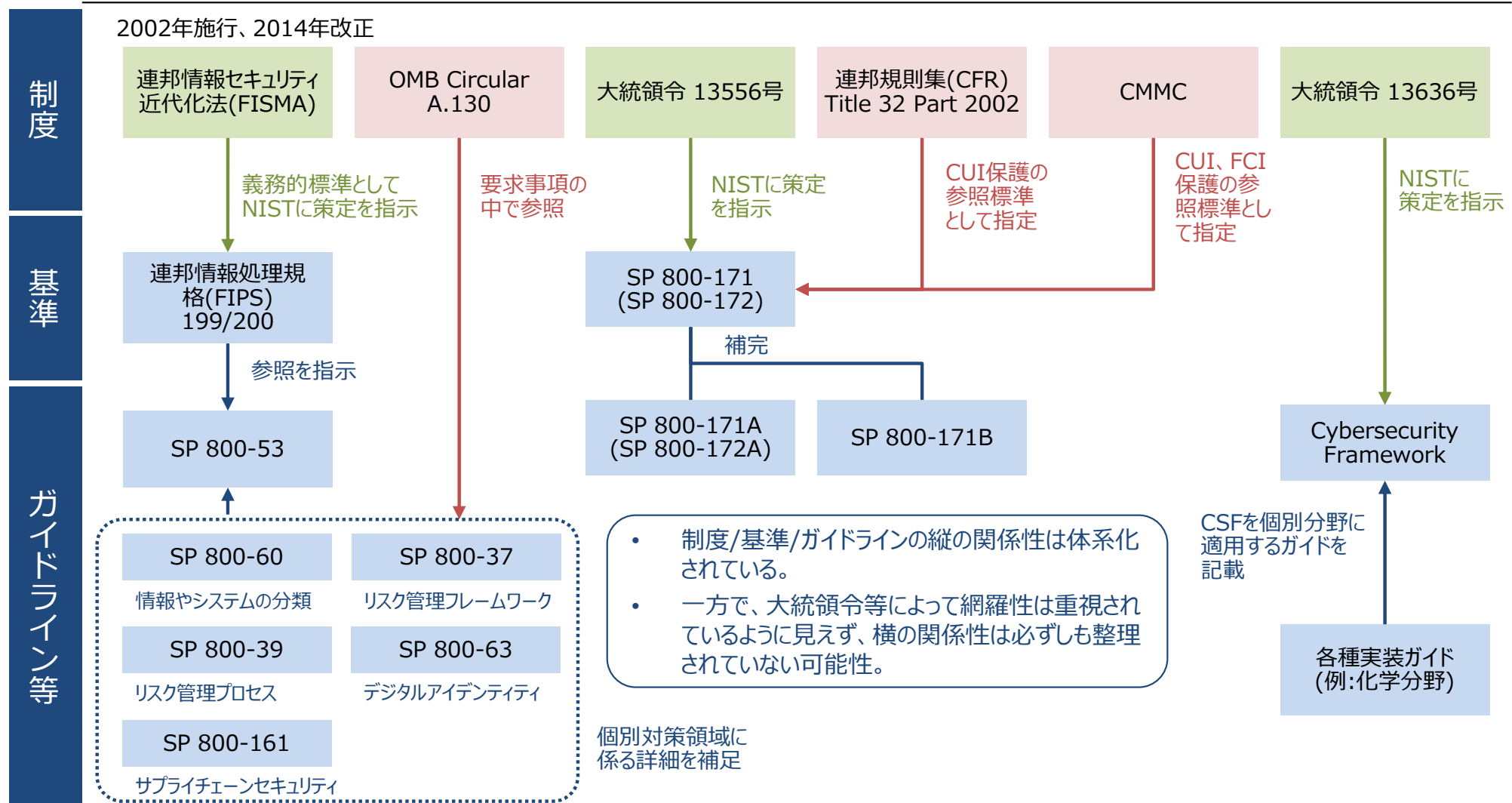
文書(例)

制度/基準/ ガイドライン間の 参照関係  縦の関係性	- 連邦情報セキュリティ近代化法(FISMA)によって、<u>義務的標準としてNISTに標準(SP 800-53)の策定を指示している</u>。また、FIPS199/200において政府情報システムのレベルについて考え方を示している。 - 大統領令によって明確な位置づけがなされた上で、<u>NISTにおいて標準が策定され、OMBによる指令によって各省庁に準拠を要求している</u>。	- FISMAとFIPS199/200、NIST SP800-53 - 大統領令14028、M-21-30、NIST SP800-213
ガイドライン間の 参照関係  横の関係性	<u>NIST SP800-53を中心として、この文書を補足される形でNIST SP800シリーズが策定</u>されており、文書ごとの位置づけが明確化されている。 <u>FedRAMPの基準は、NIST SP800-53をもとに作成</u>されている。<u>クラウドサービス固有の対策やパラメータが設定</u>されており、上記と同様、FedRAMPの基準はNIST SP800-53を中心とした文書の1つとして捉えられる。 - NIST CSFに基づき、個別分野(特に重要インフラ分野)において実装ガイドラインが策定されている。 - ただし、NIST CSFは任意の枠組みであり、重要インフラにおいて分野別のプロファイルが作られるなど個別の基準に紐づかないものがある。各省庁の権限で基準が策定されている。	- NIST SP800-53とNIST SP800-63、171 等 - NIST SP800-53とFedRAMP Baselines - NIST CSF、Implementation Guidance(例:交通分野、化学分野) - HIPPA security rules - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

米国のガイドライン等の関係性整理 (1/3)

- 大統領令や法律、通達によって標準が策定されており、制度、基準、ガイドライン等の関係性は整理されている一方で、大統領令等は柔軟に策定されていることから、横の関係性が整理されていない可能性がある。

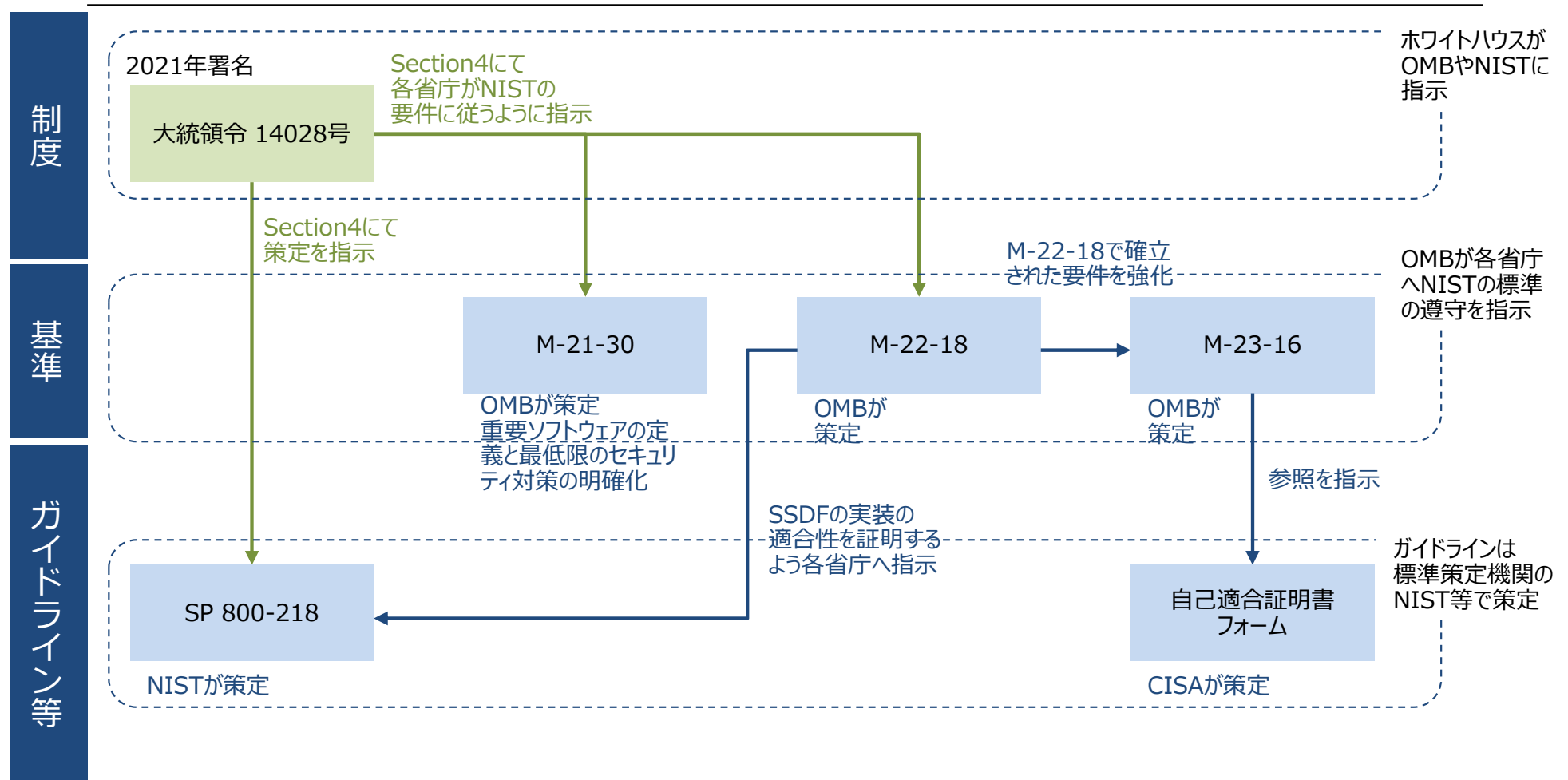
政府情報システム関連



米国のガイドライン等の関係性整理 (2/3)

- ソフトウェアサプライチェーンにテーマが限定してみた場合、大統領令とOMBの通達、NIST標準の関係性は明確となっている。

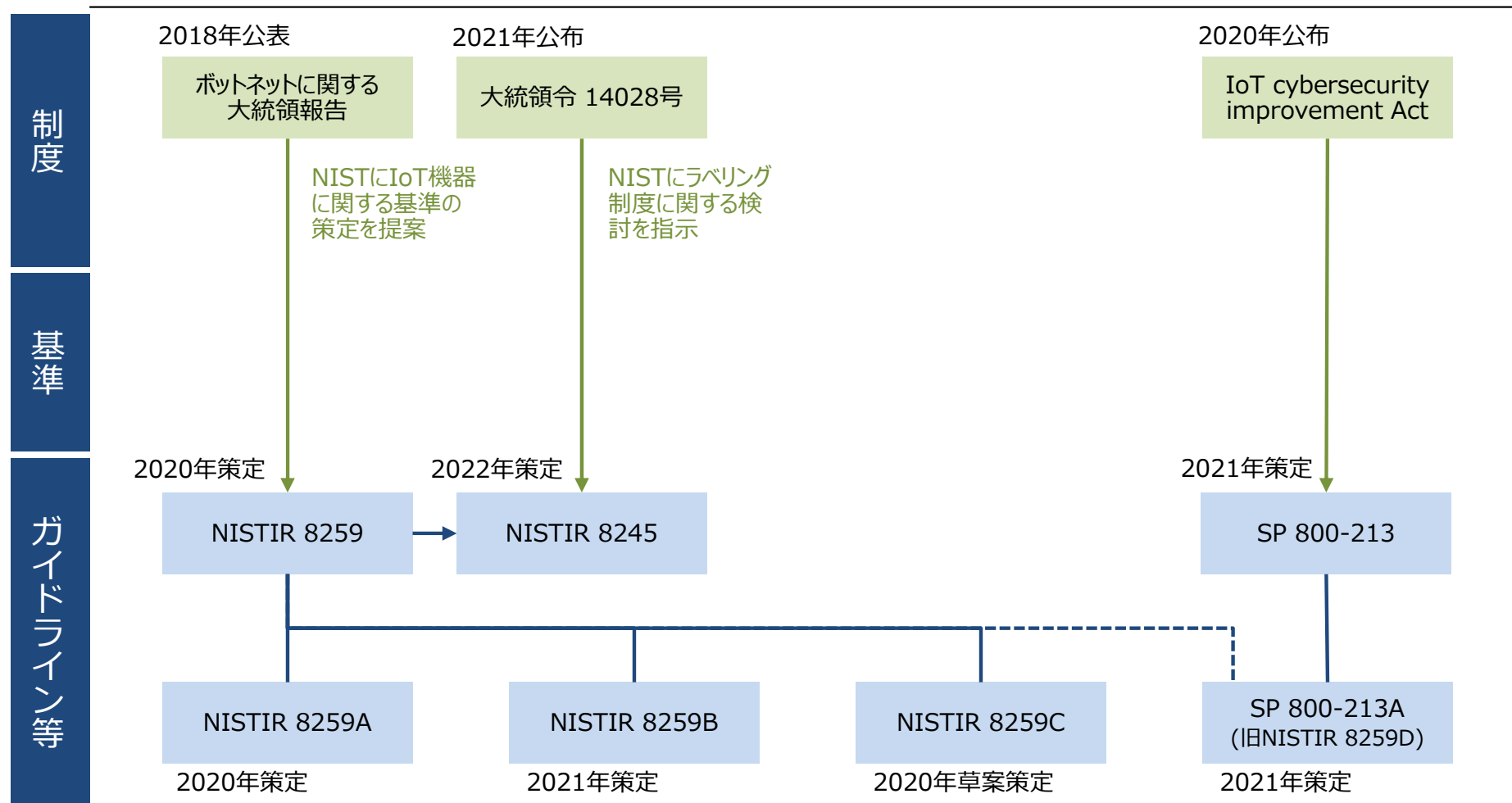
ソフトウェアサプライチェーン関連



米国のガイドライン等の関係性整理 (3/3)

- IoTの文脈においては、大統領令や大統領報告のもと、NISTIR 8259が策定された上で、その文書をベースとして、関連文書が開発された。
- また、NIST IR8259がSP800-213Aに振り替えられる等、柔軟な運用がなされている。

IoT関連





欧州関連

サマリ(欧州)

- The EU cybersecurity certification frameworkは認証スキームの枠組みを提供。
- 事業者等に直接義務を課すEU Cyber Resilience Actに対して、NIS2指令は、国内法に置き換えられることで事業者に対する拘束力を持つ。

	EU Cyber Resilience Act	The EU cybersecurity certification framework	NIS2指令
種別 ^{*1}	制度	制度	制度
遵守義務	あり	なし	あり ^{*2}
対象分野・システム	デジタル製品	ICT製品やサービス	- 主要エンティティ分野^{*3} - 重要エンティティ分野^{*4}
対象者	- デジタル要素を含む製品やソフトウェアの製造事業者 - デジタル要素を含む製品やソフトウェアの小売事業者	ENISA	- 主要エンティティ - 重要エンティティ
概要	本法は、<u>デジタル要素を含む製品やソフトウェアを購入または使用する消費者や企業を保護</u>することを目的としている。このような製品の製造業者や小売業者に対して<u>サイバーセキュリティに関する義務的な要件を導入</u>することで、不十分なセキュリティ機能をなくし、この保護が製品のライフサイクル全体に及ぶようにするもの。	本認証の枠組みは、<u>包括的な規則、技術要件、基準、手続きをセットとしたEU全体の認証スキームを提供</u>する。このスキームに従って認証されたICT製品やサービスは、指定された要件に適合していることを証明する。	- NIS2指令は、<u>EU域内でサービスを提供するまたは活動を行う中規模(従業員50名)以上の主要エンティティまたは重要エンティティを対象にした規制</u>であり、化学、医療機器、電気電子機器、光学機器、機械、自動車、輸送機器、宇宙、研究などの幅広い分野を対象に義務がかかる。 - NISからNIS2での変更点は、<u>①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・期限の明確化、④厳しい罰則金</u>。

*1 制度/基準/ガイドラインにて分類

*2 指令自体は直接拘束力をもつものではない。結果を達成するための形式・方法については、加盟国当局に選択が委ねられている。すなわち、指令は加盟国の国内法により置き換えられることによってはじめて拘束力を持つ点に留意いただきたい。

*3 主要エンティティ: エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、宇宙

*4 重要エンティティ: 郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）、デジタルプロバイダー、研究



英国関連

サマリ(英国)

- 今回の調査で扱った規則や認証制度のうち、Cyber Essentialsを除いたものには遵守義務がある。
- また、製造業者に対する遵守義務を課す一方で具体的な基準は別の規則等にて示している法律がみられた。

	PSTI法	Government Functional Standard	Cyber Essentials	The Security of Network & Information Systems Regulations
遵守義務	あり	あり	なし	あり
対象分野・システム	英国の消費者向けの接続可能な製品	政府のセキュリティ活動の計画、実施、管理に適用	業種や組織規模、システムの制約なし	- デジタルサービス*1 - 必須サービス*2
対象者	英国の消費者向け接続可能製品の製造事業者/輸入業者/販売事業者	独立行政法人の常任秘書、事務局長、最高経営責任者等		デジタル・サービスや必須サービスの運営者
概要	- 英国の消費者向けの接続可能な製品(または「スマート」製品)の製造業者に対して、<u>同法に定められた関連義務を遵守することを義務づけ</u>。 - 具体的な要件は、2023年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則にて規定	- 機能基準は、政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を実施するための主要な参考文書。 <u>どのように業務を行うかは、関連する実務やガイダンスで定められている。</u>	- 政府が支援する<u>サイバーセキュリティ認証制度</u>。 - 規模の大小にかかわらず、最も一般的なサイバー攻撃全般から組織を保護するのに役立つとされる。 - Cyber Essentials及びCyber Essentials Plusという2種類の認証を設けている。	本規則は、デジタル・サービスや必須サービスの提供に不可欠なネットワークや情報システムのセキュリティ(サイバーと物理的な回復力の両方)の<u>全体的なレベルを高めるための法的措置を提供する</u>。

*1 オンライン・マーケットプレイス、オンライン検索エンジン、クラウド・コンピューティング・サービス等が該当

*2 輸送、エネルギー、水、健康、デジタル・インフラ・サービスが該当



国際関連

サマリ(国際)

- ISO/IEC 27000シリーズは、ISO/IEC 27001を中心として個別分野の基準(例:ISO/IEC 27017:2015)が定められるとともに、その個別分野のガイドラインを策定する際の要件(ISO/IEC 27009:2020)が定められている。

	ISO/IEC 27001:2022	IEC 62443シリーズ	ISO/IEC 15408- 1:2022	ISO/IEC 27402:2023	ISO/IEC 27017:2015
種別 ^{*1}	基準	基準	基準	基準	基準
遵守義務	なし	なし	なし	なし	なし
対象分野・システム	(業種・業態を問わない)	産業用オートメーション及び制御システム	情報技術を用いた製品やシステム全般	IoT機器分野	クラウドサービス分野
対象者	あらゆる組織が利用し、認証を取得可能。	- 制御システムのアセットオーナー - 制御システムのシステムインテグレーター - 制御関連製品の製品供給者	-	- IoTサービスプロバイダ - IoTサービスデベロッパ - IoTユーザ	- 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
概要	本規格は、<u>情報セキュリティマネジメントシステム(ISMS)を確立、実施、維持、継続的に改善するための要求事項を提供することを目的として作成。</u>	IEC 62443シリーズは、<u>IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群。</u>	本規格は、情報技術セキュリティの観点から、<u>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。</u>	本規格は、<u>IoT機器がセキュリティとプライバシーの管理をサポートできるように、情報通信技術(ICT)要件のベースライン・セットを提供する。</u>	本規格は、<u>クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提供する。</u>

*1 制度/基準/ガイドラインにて分類



2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

調査対象一覧 (1/4)

- 対象文書は以下の通り。

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種横断	IT	・ ISMS適合性評価制度	・ ISMSユーザーズガイド ・ JIS Q 27001
		-	・ サイバーセキュリティ経営ガイドライン ・ 付録C ・ 付録F
		-	・ 情報セキュリティ監査基準 ・ 情報セキュリティ管理基準 ・ 個別管理基準（監査項目）策定ガイドライン
		-	・ 中小企業の情報セキュリティ対策ガイドライン第3.1版 ・ 付録1：情報セキュリティ5か条
		-	・ ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル 第5版
		-	・ ECサイト構築・運用セキュリティガイドライン
		-	・ テレワークセキュリティガイドライン第5版中小企業等担当者向けテレワークセキュリティの手引き
	OT	・ CSMS適合性評価制度	・ CSMS認証基準(IEC62443-2-1) Ver.2.0
		-	・ 制御システムのセキュリティリスク分析ガイド(2023年3月版)
		-	・ 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインVer 1.0
	サービス	・ ISMSクラウドセキュリティ認証	・ ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項 ・ ISMSユーザーズガイド追補～クラウドを含む新たなリスクへの対応～
		-	・ クラウドサービス利用のための情報セキュリティマネジメントガイドライン ・ クラウドサービス利用・提供における適切な設定のためのガイドライン
		-	・ クラウドを利用したシステム運用に関するガイダンス ・ 中小企業のためのクラウドサービス安全利用の手引き
		-	・ 情報セキュリティサービス審査登録制度 ・ 情報セキュリティサービス基準第4版

調査対象一覧 (2/4)

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種横断	製品	ITセキュリティ評価及び認証制度 (JISEC)	CC/CEM:2022 リリース1
		-	IT 製品の調達におけるセキュリティ要件リスト
		IoT 製品に対する セキュリティ適合性評価制度 (仮)	☆1セキュリティ要件・適合基準
		電気通信事業法	- 端末設備等規則 - 電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)
		-	IoT セキュリティガイドライン ver 1.0
		-	- サイバーフィジカルセキュリティ対策フレームワーク - IoTセキュリティ・セーフティ・フレームワーク (IoT-SSF) Ver1.0 - 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 - ソフトウェア管理に向けたSBOMの導入に関する手引 Ver1.0 - 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 Ver1.1
		-	脆弱性対処に向けた製品開発者向けガイド
業種個別	重要インフラ IT	重要インフラのサイバーセキュリティに係る行動計画	- 重要インフラのサイバーセキュリティに係る安全基準等策定指針 - 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
		事業用電気通信設備規則	情報通信ネットワーク安全・信頼性基準
		-	電気通信分野におけるサイバーセキュリティに係る安全基準 (第1版)
		放送法施行規則	- 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン - 放送設備サイバー攻撃対策ガイドライン (第3版)
		-	ケーブルテレビにおけるサイバーセキュリティに係る安全基準(第1版)
		-	- 金融機関等コンピュータシステムの安全対策基準・解説書(第11版) - 金融機関等におけるセキュリティポリシー策定のための手引書 - 金融機関等におけるコンティンジェンシープラン策定のための手引書(第4版)

調査対象一覧 (3/4)

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種 重要インフラ 個別 (続き)	IT (続き)	-	・ 航空分野における情報セキュリティ確保に係る安全ガイドライン(第5版)
		-	・ 空港分野における情報セキュリティ確保に係る安全ガイドライン(第2版)
		-	・ 鉄道分野における情報セキュリティ確保に係る安全ガイドライン(第4版)
		・ 電気設備に関する技術基準を定める省令	・ 電気事業法施行規則第50条第2項の解釈適用に当たっての考え方 ・ 電気設備の技術基準の解釈
		・ ガス事業法施行規則	・ 都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
		-	・ 地方公共団体における情報セキュリティポリシーに関するガイドライン
		・ 医療法施行規則	・ 医療情報システムの安全管理に関するガイドライン 第6.0版 (概説編) ・ 医療情報システムの安全管理に関するガイドライン 第6.0版 (経営管理編) ・ 医療情報システムの安全管理に関するガイドライン 第6.0版 (企画管理編) ・ 医療情報システムの安全管理に関するガイドライン 第6.0版 (システム運用編) ・ 医療機関におけるサイバーセキュリティ対策チェックリスト
		-	・ 水道分野における情報セキュリティガイドライン (第4版)
		-	・ 物流分野における情報セキュリティ確保に係る安全ガイドライン (第4版)
		-	・ 石油化学分野における情報セキュリティ確保に係る安全基準
		-	・ クレジットカード・セキュリティガイドライン【5.0 版】
		-	・ 石油分野における情報セキュリティ確保に係る安全ガイドライン
		・ 装備品等及び役務の調達における情報セキュリティの確保に関する特約条項	・ 装備品等及び役務の調達における情報セキュリティ基準 ・ 装備品等及び役務の調達における情報セキュリティ基準の解説① ・ 装備品等及び役務の調達における情報セキュリティ基準の解説②
		-	・ 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 2.0
	OT	-	・ 電力制御システムセキュリティガイドライン
		-	・ ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第2版 ・ ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編：空調システム)第1版

調査対象一覧 (4/4)

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種 個別 (続き)	重要インフラ 製品 (続き)	-	・ スマートメーターシステムセキュリティガイドライン
		-	・ 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
		-	・ スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0
	重要インフラ IT 以外	・ 政府機関等のサイバーセキュリティ対策のための統一規範	・ IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ ・ 政府機関等のサイバーセキュリティ対策のための統一基準 ・ 政府機関等の対策基準策定のためのガイドライン ・ 対策推進計画策定マニュアル ・ 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書 ・ 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル ・ 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書 ・ 政府機関等における情報システム運用継続計画ガイドライン ・ スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書
		-	・ 自工会/部工会・サイバーセキュリティガイドライン V2.1

業界団体等が自主的に策定したガイドライン (1/4)

- 政府の枠組み以外で業界団体が策定した文書を業種横断及び各業種で一覧化した。
 - ✓ 業界横断:セキュリティ系の団体を中心にガイドライン更新に積極的な団体(例:JNSAやJPCERT/CC、ISOG-J等)がみられ、その取組の歴史も古い場合があった。より専門性の高いテーマ(例:特権ID管理、オープンソフトウェアの脆弱性管理、セキュアコーディング)が選ばれ、各団体の問題意識のもと、ガイドラインが策定されている。
 - ✓ 業界個別:各業界の問題意識から、近年(2020年以降)であってもガイドライン策定に積極的に取り組んでいる業界がみられる。一方で、取組の温度感に差がみられ、必ずしも全ての業界(団体)でガイドライン策定が策定されているとは言えない。

JNSA:日本ネットワークセキュリティ協会、ISOG-J:日本セキュリティオペレーション事業者協議会、SAJ:ソフトウェア協会、CRIC CSF:産業横断サイバーセキュリティ検討会

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種横断	IT	-	- 特権ID管理ガイドライン「実践編」(JNSA:2024年5月) - 特権ID管理ガイドライン「解説編」(JNSA:2023年3月) - ID管理システム導入における現状把握チェックリスト(JNSA:2017年7月) - クラウド環境におけるアイデンティティ管理ガイドライン(JNSA:2013年6月) - エンタープライズロール管理解説書(第3版) (JNSA:2016年6月)
		-	- 脆弱性トリアージガイドライン作成の手引き(ISOG-J:2024年5月) - 細かすぎるけど伝わってほしい脆弱性診断手法ドキュメント(ISOG-J:2023年4月) - GraphQL脆弱性診断ガイドライン(ISOG-J:2021年12月)
		-	オープンソースソフトウェアの脆弱性情報管理に関する戦略策定報告書(SAJ:2020年3月)
		-	アジャイル開発におけるセキュリティ パターン・ランゲージ(ISOG-J:2022年7月)
		-	- Webアプリケーション脆弱性診断ガイドライン 第1.2.4版(ISOG-J:2023年11月) - Webシステム/Webアプリケーションセキュリティ要件書 Ver.4.0(ISOG-J:2022年6月)
		-	マネージドセキュリティサービス(MSS)選定ガイドライン Ver.2.0(ISOG-J:2020年7月)
		-	ペネトレーションテストについて(ISOG-J:2019年12月)
		-	- トラストのためのデジタル署名検証解説(JNSA:2023年12月) - デジタル署名検証ガイドライン(JNSA:2021年3月) - 電子署名保証レベル要約版(JNSA:2022年9月)
		-	セキュリティ対応組織(SOC/CSIRT)の教科書 第3.1版(ISOG-J:2023年10月)

業界団体等が自主的に策定したガイドライン (2/4)

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種横断 (続き)	IT (続き)	-	- 経営リスクと情報セキュリティ～CSIRT：緊急対応体制が必要な理由～(JPCERT/CC:2021年11月) - 組織内CSIRT構築支援マテリアル(JPCERT/CC:2021年11月) - CSIRTガイド(JPCERT/CC:2021年11月) - インシデントハンドリングマニュアル(JPCERT/CC:2021年11月)
		-	- CERT C セキュアコーディングスタンダード(JPCERT/CC:2024年7月) - C/C++ セキュアコーディング 第2版(JPCERT/CC:2014年7月) - Java セキュアコーディングスタンダード CERT/Oracle 版(JPCERT/CC:2024年7月) - Java セキュアコーディングスタンダード CERT/Oracle版(JPCERT/CC:2012年4月) - Java アプリケーション脆弱性事例解説資料(JPCERT/CC:2014年7月) 「Java セキュアコーディング 並行処理編」(JPCERT/CC:2011年8月) - クロスサイトリクエストフォージェリ(CSRF)とその対策(JPCERT/CC:2015年10月) - OWASP「ソフトウェアセキュリティ保証成熟度モデル」(JPCERT/CC:2010年4月) - OWASPアプリケーションセキュリティ検証標準(JPCERT/CC:2016年6月)
		-	- A1.産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～(CRIC CSF:時期未確認) - A2.産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～(要求知識)(CRIC CSF:時期未確認) - A3.産業横断 人材定義リファレンス～機能と業務に基づくセキュリティ人材定義～(業務区分)(CRIC CSF:時期未確認) - B.産業横断 セキュリティ対策カレンダー ～セキュリティ対策A to Z～(CRIC CSF:時期未確認) - C.産業横断 セキュリティオペレーション アウトソーシングガイド(CRIC CSF:時期未確認) - D.産業横断 人材定義リファレンスに基づくスキルマッピング(CRIC CSF:時期未確認)
		-	- ユーザ企業のためのセキュリティ統括室 構築・運用キット(統括室キット):概要編(CRIC CSF:2018年11月) - ユーザ企業のためのセキュリティ統括室 構築・運用キット(統括室キット):統括室編(CRIC CSF:2019年9月) - ユーザ企業のためのセキュリティ統括室 構築・運用キット(統括室キット):統括人材編(CRIC CSF:時期未確認)
	OT	-	- 今すぐ実践できる工場セキュリティハンドブック・リスク対策編(JNSA:2024年3月) - 今すぐ実践できる工場セキュリティハンドブック・リスクアセスメント編(JNSA:2024年3月)
		-	- OTセキュリティ人材スキル定義リファレンス(CRIC CSF:2019年7月) - OTセキュリティ人材スキル定義リファレンスガイド(CRIC CSF:2019年7月)
	製品	-	プロダクト脆弱性対策・対応成熟度シートVersion 1.1(SAJ:2020年4月)

業界団体等が自主的に策定したガイドライン (3/4)

分野	文書の対象	文書の種類	
		制度	基準/ガイドライン
業種個別	農業、林業、漁業	-	森林クラウドシステムに関わる情報セキュリティガイドライン(日本森林技術協会:2021年3月)
	建設業	-	- 建設現場における情報セキュリティガイドライン(日本建設業連合会:2024年2月) - 元請会社における情報セキュリティガイドライン(日本建設業連合会:2024年2月) - 協力会社における情報セキュリティ対策について(日本建設業連合会:2024年2月) - 建設現場ネットワークの構築と運用ガイドライン(日本建設業連合会:2024年2月) - 建設現場におけるスマートデバイス利用に関するセキュリティガイドライン(日本建設業連合会:2024年2月)
	製造業	-	ネットワーク機能付き事務機セキュリティガイドライン(ビジネス機械・情報システム産業協会:2021年6月)
	情報通信業	-	通信ネットワーク機器セキュリティ・ユーザーガイドライン Ver.2.0(情報通信ネットワーク産業協会:2020年5月)
		-	サイバーセキュリティ確保ガイドライン(日本コミュニティ放送協会:2020年3月)
		-	- ローカル5Gセキュリティガイドライン(ICT-ISAC:2022年3月) - 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン(ICT-ISAC:2021年12月) - 家庭内で安全快適に在宅勤務を行うためのリファレンスガイド(ICT-ISAC:2020年7月)
		-	証拠保全ガイドライン第9版(デジタル・フォレンジック研究会:2023年2月)
	運輸業、郵便業	-	- 船上のシステム及び機器のサイバーレジリエンスに関するガイドライン(日本海事協会:2023年11月) - 船舶におけるサイバーセキュリティデザインアプローチ(日本海事協会:2020年7月) - ソフトウェアセキュリティガイドライン(日本海事協会:2019年5月)

業界団体等が自主的に策定したガイドライン (4/4)

分野		文書の対象	文書の種類	
			制度	基準/ガイドライン
業種 個別	金融業、保険業	金融	-	- クレジットカード導入ガイド(日本クレジット協会:2024年3月) - セキュリティガイドライン(日本クレジット協会:2024年3月) - EMV3-D セキュア - クレジット取引における本人確認方法に係るガイドライン(公表版)1.1版(日本クレジット協会:2024年3月)
			-	インターネット取引における不正アクセス等防止に向けたガイドライン(日本証券業協会:2021年7月)
	学術研究、専門・技術サービス業	サービス(公認会計士)	-	公認会計士業務における情報セキュリティの指針(日本公認会計士協会:2022年10月)
	医療、福祉	医療機器	-	医療機関における医療機器のサイバーセキュリティ確保のための手引書(日本医療機器産業連合会:2023年3月)

サマリ [A:位置づけ、参照関係、関係性等について]

- 基準及びガイドラインの位置づけは大きく分けて以下の3つに分類された。

1. 制度対応に必要な基準の位置づけが明確
2. 制度対応に必要な基準とガイドライン等との関係が不明確
3. 任意のガイドラインのみを提示

分類	特徴	例
パターン1 制度対応に必要な基準の位置づけが明確	- 制度において、サイバーセキュリティ確保のための<u>基準への遵守が義務として定められており</u>、その<u>基準が明示</u>されている。 - また、その基準への遵守にあたって参考となるガイドラインが示されている場合がある。(なお、任意の評価制度を含む)	- 電気通信事業法/端末設備等規則/電気通信事業法に基づく端末機器の基準認証に関するガイドライン - 防衛省通達/装備品等及び役務の調達における情報セキュリティの確保に関する特約条項/装備品等及び役務の調達における情報セキュリティ基準 - ISMS適合性評価制度・ISO/IEC 27001(JIS Q 27001)
パターン2 制度対応に必要な基準とガイドライン等との関係が不明確	- 制度において、サイバーセキュリティ確保のための基準への遵守が<u>義務として定められている一方</u>で、その<u>基準が明示されておらず、遵守すべき基準が不明確となっている。</u> - ガイドラインが示されている場合があるが、ガイドラインへの対応は義務とはなっていない。	- 放送法施行規則/ケーブルテレビにおけるサイバーセキュリティに係る安全基準 - ガス事業法施行規則/都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説 - 水道施設の技術的基準を定める省令/水道分野における情報セキュリティガイドライン
パターン3 任意のガイドラインのみを提示	- 制度に該当するものがなく、<u>ガイドラインへの遵守が任意となっている。</u> - また、安全基準等策定指針及び重要インフラ分野の各ガイドラインのように、ガイドライン間で参照されている文書がみられる。	- サイバーセキュリティ経営ガイドライン関連文書 - CPSF関連文書

参考(2024/4/16提示資料より)

- ・ **制度**: 以下のようなものを含む。
 - 法令: 行政手続法に定めのある通り、法律、法律に基づく命令(政令、省令、規則、告示等)、条例及び地方公共団体の執行機関の規則を含む。
 - その他の制度: 「法令」の規定等に基づき運用される制度(例: 適合性評価制度)を含む。
- ・ **基準**: 法令またはその規定事項に基づき運用される制度において、審査基準、処分基準、行政指導指針(行政手続法)、その他の評価基準として用いられているものを含む。
- ・ **ガイドライン等**: 関係者らが取り組むことが望ましいとされる指針や、基準となる目安などを示したものであり、以下のようなものを含む。
 - 関係府省等、行政機関が自ら提示するもののほか、行政機関による指導など深い関与の下で、民間の業界団体等が提示するもの
 - 「ガイドライン」の名称が付されているものに加えて、ガイドラインとほぼ同様の趣旨で「指針」、「考え方」等の名を冠するもの

サマリ [B:記載内容について]

- 記載範囲[B-1]:スコープの異なる一部基準/ガイドラインを除いて、日本国内の既存の基準/ガイドラインは概ねCSFの記載範囲を網羅していた。なお記載範囲が限定的となっている基準/ガイドラインがみられた。
- 記載粒度[B-2]:記載粒度に差異はみられるが、ISO/IEC 27001と比較した際に、より具体的な記載がみられた。ただし、読者が理解し実装できるレベルまで内容が具体的に記載されていない要件もみられた。

項目	サマリ	対象(例)
B-1. 記載範囲	- 日本国内の既存の基準/ガイドラインは、CSFの記載範囲は概ね網羅されている。 33の調査対象のうち、24の基準・ガイドラインが8割の項目(81.8%以上:18/22個)を満たしていた。	-
	- 製品(例:IoT機器)を対象とした基準/ガイドラインでは、組織を対象としたCSFと比較した際に記載範囲に偏りがみられた。 - 例えば、製品を対象した基準/ガイドラインは特定/防御に係る対策が主に示されているが、スコープの違いから生じるものと考えられるため、IPAによる助言の対象とはならない可能性がある。	- JC-STAR - 電気通信事業法に基づく端末機器の基準認証に関するGL
	- 一方で、組織を対象とした基準/ガイドラインであっても記載範囲が限定的(50%以下:11/22個)となっているものもみられた。 - これらの基準/ガイドラインはCSFと比較した際に、記載範囲を拡大させる余地があるため、IPAによる助言の対象となる可能性がある。ただし、対象企業(例:中小企業)の能力や位置づけ(例:義務化)によって、意図的に記載範囲が限定されていることも想定される。助言の際にはこれらの背景情報を考慮することが重要。	- 中小企業の情報対策セキュリティGL - 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン - クレジットカード・セキュリティガイドライン
B-2. 記載粒度	記載粒度に差異はみられるが、ISO/IEC 27001と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載がみられた。	-
	情報システムの構成要素や研修計画に盛り込む内容については、要求事項が具体的に示されており、読者が理解し実装できるレベルまで内容が記載されているものがみられた。	- 情報システムの構成要素(航空分野における情報セキュリティ確保に係る安全ガイドライン) - 研修計画に盛り込む事項(地方公共団体における情報セキュリティポリシーに関するガイドライン)
	しかし、読者が理解し実装できるレベルまで内容(例:認証方法)が具体的に記載されていない要求事項もみられた。例えば、認証方法の一覧が示されているが、どのような場合にどの認証方法を選べばよいかは示されていなかった。	認証方法(医療情報システムの安全管理に関するガイドライン/情報通信ネットワーク安全・信頼性基準/クレジットカード・セキュリティガイドライン)

サマリ [B-1:記載範囲] (1/2)

- 製品(例:IoT機器)を対象とした基準やガイドラインを除いて、CSFの記載範囲は概ね網羅されている。
- 33の調査対象のうち、24の基準・ガイドラインが8割の項目(81.8%(18/22個)以上)を満たしていた。

[凡例] ☐ 0% ☐ 1-50% ☐ 51-99% ☐ 100%

コア	業界横断											業界個別						
	中小企 業の情報対策 セキュリティGL	情報セ キュリ ティ管理基準	CSMS 認証基 準	工場シ ステム GL	ISMS クラウド セキュリティ認 証に関する要 求事項	クラウド サービス 利用の ための 情報セ キュリ ティマネ ジメント GL	クラウド を利用 したシ ステム運 用に関 するガイ ダンス	JC- STAR	電気通 信事業 法に基 づく端 末機器 の基準 認証に 関する GL	IoTセ キュリ ティガイ ドライン	サイ バー・ フィジ カル・セ キュリ ティ対 策フレ ームワ ーク	重要イン フラの サイ バーセ キュリ ティに係 る安全 基準等 策定指 針	情報通 信ネット ワーク 安全・ 信頼性 基準	電気通 信分野 における サイ バーセ キュリ ティに係 る安全 基準	ケーブ ルテレビ における サイ バーセ キュリ ティに係 る安全 基準	金融分 野にお けるサイ バーセ キュリ ティに関 するガイ ドライン	航空分 野にお ける情 報セ キュリ ティ確保に 係る安全 ガイドラ イン	
統制	3/6	6/6	6/6	6/6	6/6	6/6	5/6	3/6	0/6	6/6	6/6	6/6	5/6	6/6	6/6	6/6	6/6	
識別	2/3	3/3	3/3	3/3	3/3	3/3	2/3	2/3	0/3	3/3	3/3	3/3	2/3	3/3	3/3	3/3	3/3	
防御	3/5	5/5	5/5	5/5	5/5	5/5	3/5	4/5	4/5	3/5	5/5	5/5	5/5	5/5	5/5	5/5	5/5	
検知	1/2	2/2	2/2	1/2	2/2	2/2	2/2	0/2	0/2	2/2	2/2	2/2	1/2	2/2	2/2	2/2	2/2	
対応	1/4	3/4	3/4	2/4	3/4	3/4	3/4	0/4	0/4	3/4	4/4	3/4	2/4	4/4	3/4	4/4	3/4	
復旧	1/2	1/2	1/2	1/2	1/2	1/2	1/2	0/2	0/2	1/2	2/2	1/2	1/2	2/2	1/2	1/2	2/2	
集計	11/22	20/22	20/22	19/22	20/22	20/22	16/22	9/22	4/22	18/22	22/22	20/22	20/22	22/22	20/22	21/22	21/22	

サマリ [B-1:記載範囲] (2/2)

[凡例]  0%  1-50%  51-99%  100%

コア	業界個別															
	空港分野における情報セキュリティ確保に係る安全ガイドライン	鉄道分野における情報セキュリティ確保に係る安全ガイドライン	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	地方公共団体における情報セキュリティポリシーに関するガイドライン	医療情報システムの安全管理に関するガイドライン	水道分野における情報セキュリティガイドライン	物流分野における情報セキュリティ確保に係る安全ガイドライン	クレジットカード・セキュリティガイドライン	装備品等及び役務の調達における情報セキュリティ基準	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン	電力制御システムセキュリティGL	スマートメーターシステムセキュリティGL	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策GL	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策GL	政府機関等のサイバーセキュリティ対策のための統一基準	自工会/部工会・サイバーセキュリティGL (Lv.1)
統制	6/6	6/6	6/6	6/6	6/6	6/6	6/6	2/6	6/6	1/6	4/6	5/6	4/6	3/6	6/6	6/6
識別	3/3	3/3	3/3	3/3	3/3	3/3	3/3	1/3	3/3	2/3	3/3	2/3	3/3	3/3	3/3	3/3
防御	5/5	5/5	5/5	5/5	5/5	5/5	5/5	3/5	4/5	3/5	5/5	4/5	5/5	3/5	5/5	5/5
検知	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	1/2	2/2	2/2	1/2	2/2	2/2
対応	3/4	3/4	3/4	4/4	4/4	4/4	4/4	4/4	4/4	0/4	2/4	3/4	4/4	1/4	3/4	3/4
復旧	2/2	2/2	2/2	1/2	2/2	1/2	1/2	1/2	2/2	0/2	0/2	0/2	2/2	0/2	1/2	1/2
集計	21/22	21/22	14/22	21/22	22/22	21/22	21/22	14/22	21/22	8/22	15/22	18/22	20/22	11/22	20/22	20/22

サマリ [B-2:記載粒度] (1/4)

- 記載粒度に差異はみられるが、ISO/IEC 27001と比較した際に、対象とした基準/ガイドラインにおいて具体的な記載がみられた。ただし、読者が理解し実装できるレベルまで内容が具体的に記載されていない要求事項(例:認証方法)もみられた。

項目	内容		対象
B-2. 主体 記載粒度	<u>教育対象</u>	[手順及び設備について]従業員、契約従業員、サードパーティ契約者 [リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組]本取組に関連する要員	- CSMS認証基準 - クラウドサービス利用のための情報セキュリティマネジメントガイドライン - 金融分野におけるサイバーセキュリティに関するガイドライン
		- 全要員 - 情報セキュリティ要員(システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)	サイバー・フィジカル・セキュリティ対策フレームワーク
		- 総括者 - 管理者 - 保護システム管理者 - 保護システム担当者	装備品等及び役務の調達における情報セキュリティ基準
	<u>セキュリティ対策の対象者</u>	- 経営層 - システム業務に従事する人材 - システムユーザ - PC操作者(テレワーク勤務者を含む) (必要に応じて)委託先	航空分野における情報セキュリティ確保に係る安全ガイドライン
	<u>利用者アカウントの承認主体</u>	- 代表取締役 - 情報セキュリティ責任者	中小企業の情報セキュリティ対策ガイドライン
	<u>認証を行う対象</u>	- システム管理者アクセスアカウント - アプリケーション構成アクセスアカウント - リモートユーザ(アカウント)	CSMS認証基準

サマリ [B-2:記載粒度] (2/4)

項目	内容	対象
B-2. 記載粒度	- 情報システムの構成要素 - 端末 - サーバ装置 - 通信回線・通信回線装置 - 複合機及びIoT機器を含む特定用途機器	- 航空分野における情報セキュリティ確保に係る安全ガイドライン - 物流分野における情報セキュリティ確保に係る安全ガイドライン
	- 施設 - ネットワーク - 周辺機器 - ハードウェア - システム領域 - データ領域 - システム運用体制 - ベンダの継続能力	水道分野における情報セキュリティガイドライン
	- 情報資産の管理にあたって表示する事項 - ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等) - 格納する電磁的記録媒体のラベル - 情報資産の分類(文書の隅等)	地方公共団体における情報セキュリティポリシーに関するガイドライン
	- 資産管理台帳の維持管理策 - 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする - 承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する	物流分野における情報セキュリティ確保に係る安全ガイドライン
	- 認証方法 - パスワード - ICカード - 電子証明書 - 生体認証等 - 本人の識別・認証	- 医療情報システムの安全管理に関するガイドライン - 情報通信ネットワーク安全・信頼性基準
	- 本人認証(EMV3-Dセキュア): - 本人認証(認証アシスト): - 券面認証	クレジットカード・セキュリティガイドライン

サマリ [B-2:記載粒度] (3/4)

項目	内容		対象
B-2. 内容 記載粒度 (続き)	アクセス利用者の管理とアクセス権の管理にあたって実施すること	- 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等の設定 - 利用者アクセス権の定期的なレビュー - 管理権限のユーザ/用途ごとの設定 - 離職者アカウントに対して、全てのバッジ、キーカード、トークン等の失効	航空分野における情報セキュリティ確保に係る安全ガイドライン
	教育内容	- 情報セキュリティの重要性及び意義 「need to knowの原則」(「情報は知る必要がある者のみに伝え、知る必要のない者には伝えない」という原則)の確実な履行 - 情報セキュリティ基本方針等の確実な履行 - 公私における慎重な行動 - 悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順 - 前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項 - 上記に掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的及び専門的な事項	装備品等及び役務の調達における情報セキュリティ基準
		- 手順及び設備 - リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組	CSMS認証基準
	研修計画に盛り込む事項	- 研修内容 - 受講対象者 - e-ラーニング/集合研修 - 説明会等の実施方法 - 時期/日程/講師等	地方公共団体における情報セキュリティポリシーに関するガイドライン

サマリ [B-2:記載粒度] (4/4)

項目	内容		対象	
B-2. 頻度 記載粒度	• <u>教育の頻度</u>	- 入社時、契約時(情報セキュリティ関連規程) - 運用開始時、運用終了後 - 情報システムや産業用制御システムに対する変更により必要になったとき - 関連法令の公布・施行時(関連法令) - 最低毎年度1回(職員等が教育を受講する頻度)	- 中小企業の情報セキュリティ対策ガイドライン - サイバー・フィジカル・セキュリティ対策フレームワーク - 航空分野における情報セキュリティ確保に係る安全ガイドライン	
	• <u>パスワードの変更タイミング</u> (IoT機器を対象)	初期設定時	- JC-STAR - 電気通信事業法に基づく端末機器の基準認証に関するガイドライン - IoTセキュリティガイドライン	
	• アクセス権の割当において <u>考慮すべきタイミング</u>	- 利用者の初期登録時 - 情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除時	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	
	場所	• 情報システム室の <u>設置を禁止する場所</u>	地階/1階	地方公共団体における情報セキュリティポリシーに関するガイドライン
		• <u>物理的セキュリティ境界</u>	- 壁 - カード制御による入口 - 有人の受付	クラウドサービス利用のための情報セキュリティマネジメントガイドライン
		• <u>要管理対策区域</u>	- 執務室 - 会議室 - サーバ室等	航空分野における情報セキュリティ確保に係る安全ガイドライン
		• レベルごとの <u>物理的管理策の対象</u>	- レベル1:本社受付・応接スペース・商談室・倉庫 - レベル2:本社受付・応接スペース・商談室・倉庫 - レベル3:サーバールーム/鍵付きサーバラック	中小企業の情報セキュリティ対策ガイドライン

3. 今後の注力領域及び方向性(案)の整理

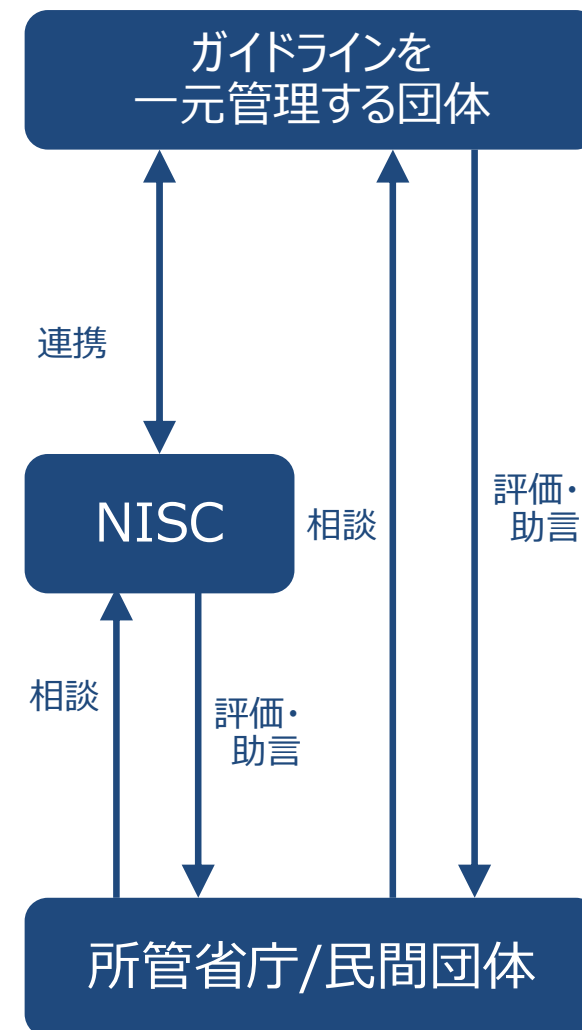
3.1.1 文書のあるべき姿の具体化

ガイドラインを一元管理する団体による助言内容と各団体の関係性

- NISCや所管省庁/民間団体に対して、「ガイドラインを一元管理する団体」は各文書のあるべき姿を踏まえて位置づけ、参照関係、関係性の観点や記載内容の観点から助言を行うことを想定。

対象	各文書のあるべき姿		ガイドラインを一元管理する団体による 所管省庁等に対する主な助言内容	
	位置づけ、 参照関係、関係性 等	記載内容	位置づけ、 参照関係、関係性 等	記載内容
1. 制度	■ 体系内 <法律等でセキュリティ対策義務が定義されている場合> <u>適切な法律等(例: サイバーセキュリティ基本法や業法)に基づき基準やガイドラインが策定されている。</u> ■ 体系間 各分野で漏れなく基準やガイドライン等が策定されている	-	■ 体系外 <法律等でセキュリティ対策義務が定義されている場合> <u>適切な法律等(例: サイバーセキュリティ基本法や業法)において参照すべき基準を明示した方がよい。</u> ■ 体系間 制度/基準/ガイドラインを新たに策定した方がよい。	-
2. 基準		近年増加している脅威に対処可能な要求事項が定められている。 <記載範囲> ・ 記載されている範囲に漏れがない <記載粒度> ・ 対策要件の記載粒度が適切である		近年増加している脅威に対処するために以下に対応した方がよい。 <記載範囲> ・ ガイドラインに記載された対策要件の記載範囲に偏りがあるため、偏りをなくした方がよい。 <記載粒度> ・ ガイドラインに記載された対策要件のガイドライン記載粒度を細かく(粗く)した方がよい。
3. ガイドライン				

■ 関係性



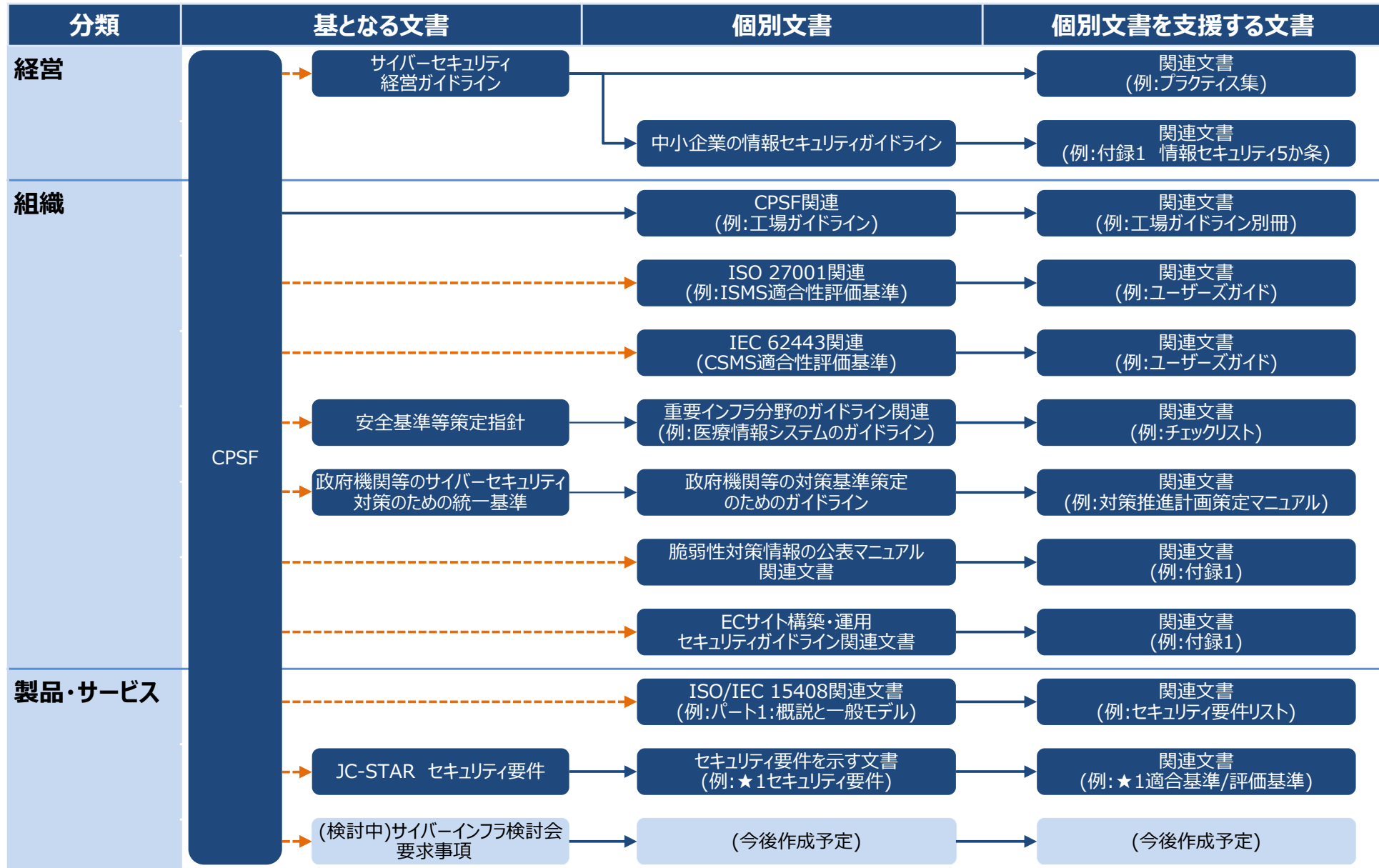


3.1.2 文書の整理状況の可視化

日本国内のガイドラインの文書の整理結果

- CPSFを頂点として、「経営」及び「組織」、「製品・サービス」で各文書を整理した。

← 現時点で引用もしくは参照 ← 現時点で十分に引用もしくは参照がなされていない



*1 三層構造は、「第1層－企業間のつながり」「第2層－フィジカル空間とサイバー空間のつながり」「第3層－サイバー空間におけるつながり」、6つの構成要素は、「ソシキ」、「ヒト」、「モノ」、「データ」、「プロセス」、「システム」からなる。

3.2 対処すべき現状の問題の整理

生じている問題

- 位置付け、参照関係、関係性及び記載内容から生じている問題は以下の4つに分類された。

- 1-1:事業者にとって、どの基準やガイドライン等を参照すればよいかわからない
- 1-2:遵守すべき基準が不明確となっている。
- 2-1:記載範囲が限定的となっており、脅威に適切に対処できない。
- 2-2:要求事項が具体的に記載されておらず、脅威に適切に対処できない。

分類	特徴
1-1 位置付け、参照関係、関係性	事業者にとって、<u>どの基準やガイドライン等を参照すればよいかわからない</u>となっている。
1-2	事業者にとって参照すべき基準やガイドラインを理解できたとしても、サイバーセキュリティ確保のための遵守が義務となっている基準が具体化されておらず、<u>遵守すべき基準が不明確</u>となっている。
2-1 記載内容	国際的に参照されているNIST CSFと比較した際に、<u>ガイドライン等によっては記載範囲が限定的</u>となっており、脅威に適切に対処できない可能性がある。
2-2	ガイドライン等によっては、<u>読者が理解し実装できるレベルまで要求事項が具体的に記載されておらず</u>、脅威に適切に対処できない可能性がある。

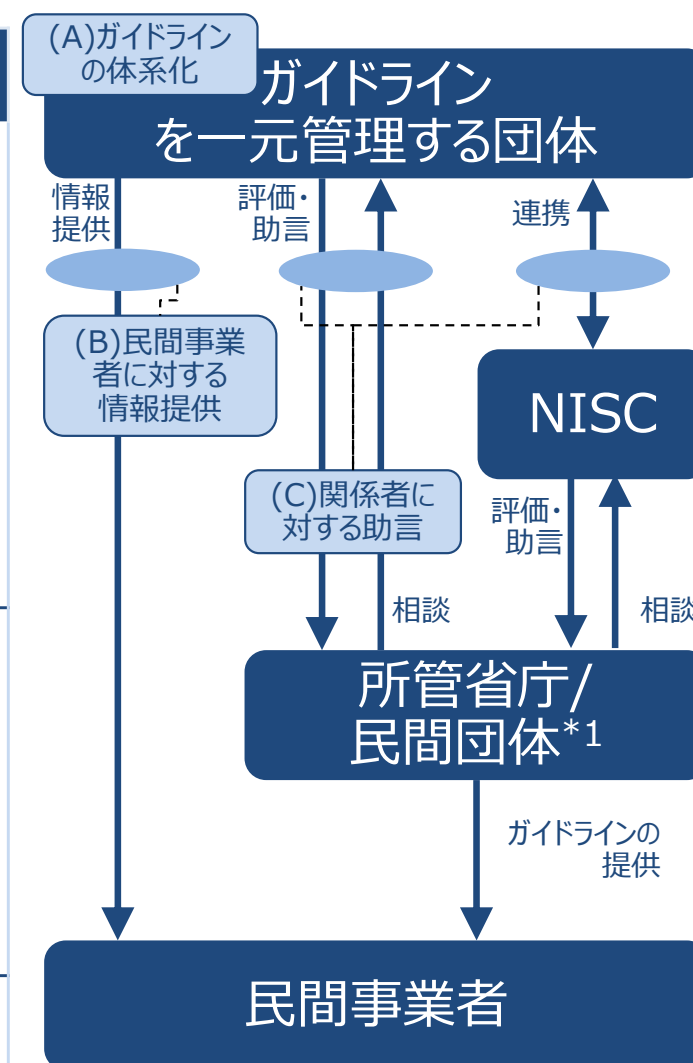
3.3 今後の方向性(案)の整理

施策案

- 「ガイドラインを一元管理する団体」側で以下の施策を行うことが考えられる。

- A) ガイドラインの体系化
- B) 民間事業者に対する情報提供
- C) 関係者に対する助言

	(A)ガイドラインの体系化	(B)民間事業者に対する情報提供	(C)関係者に対する助言
対応する課題	[1.1]事業者にとって、 <u>参照すべきガイドライン等が不明確</u>	[1.1]事業者にとって、 <u>参照すべきガイドライン等が不明確</u>	[1.1]事業者にとって、 <u>参照すべきガイドライン等が不明確</u> [1.2]事業者にとって、 <u>参照すべき基準が不明確</u> [2.1] <u>記載範囲が適切でなく、事業者が脅威に対処できない</u> [2.2] <u>記載粒度が適切でなく、事業者が脅威に対処できない</u>
実施事項(案)	カタログ化を行ったガイドライン一覧を管理し、<u>各省庁が維持管理を行った際に、随時更新を行う。</u>	読者が利用しやすいような形でカタログ化を行った<u>ガイドライン一覧(Aでの検討結果)を公開する。</u>	ガイドラインを所管する省庁や民間団体に対して、<u>ガイドラインの策定や更新に係る助言を行う。</u>重要インフラ分野のガイドラインについては、<u>各省庁に対して助言を行うNISCと連携を行う。</u>
想定されるハードルの高さ	中	中	高



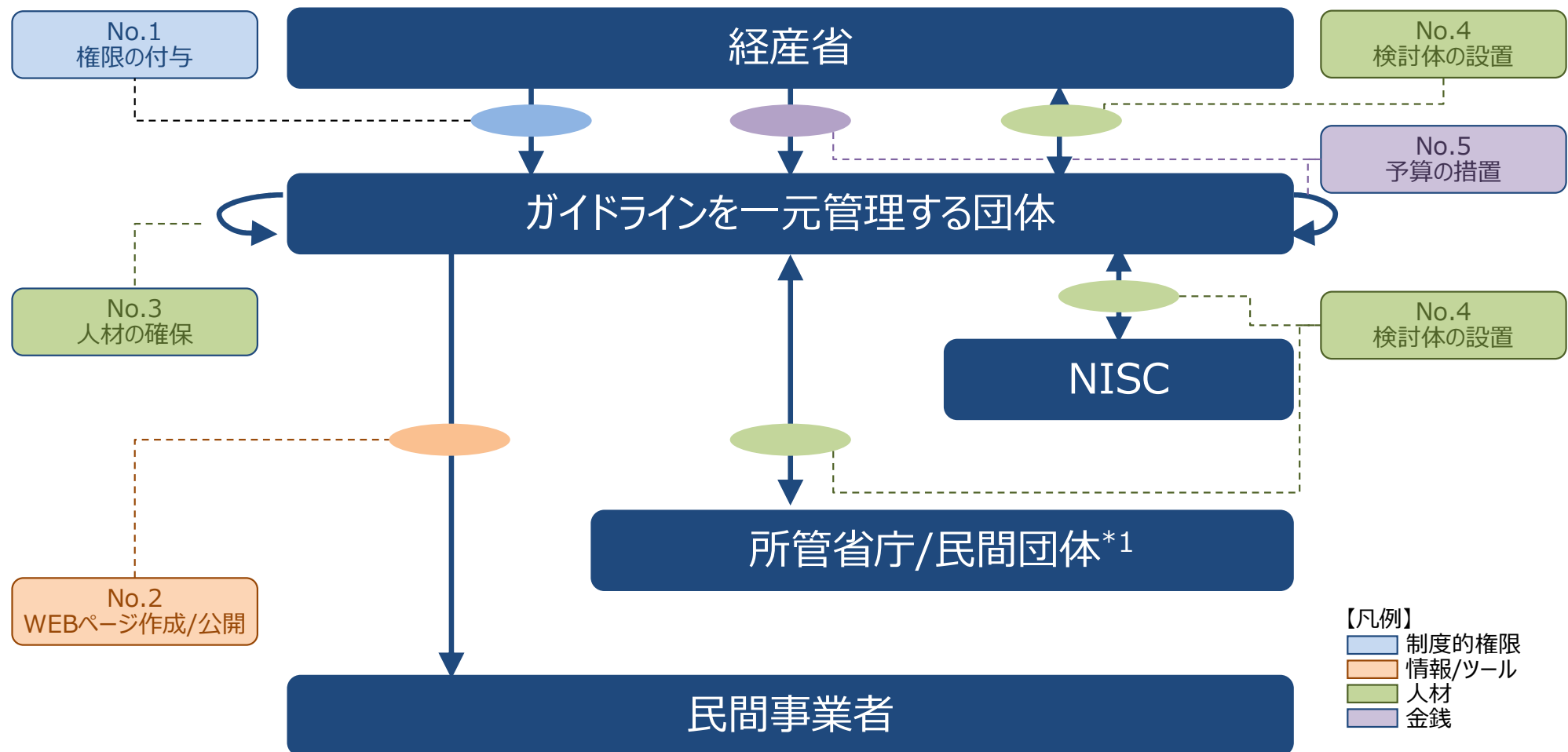
*1 「日本自動車工業会」のようなセキュリティに係るガイドラインを策定している団体を想定。

*2 考え方のみ整理している点にご留意いただきたい。

今後の施策に係る具体的な手段(1/2)

- 今後の施策を推進する際の具体的な手段を整理した。[詳細は次頁参照]

- [制度的権限] 1.制度的権限権限の付与
- [情報/ツール] 2.WEBページの作成/公開
- [人材] 3.人材の確保/4.検討体の設置
- [金銭] 5.予算の措置



今後の施策に係る具体的な手段(2/2)

- 主な主体と関連する課題と併せて、今後の施策を推進する際の具体的な手段を整理した。

分類	No.	取組	内容	主な主体	関連する課題[参考]
制度的 権限	1	IPAに対する権限の付与	IPAに対してガイドラインの管理や助言に対する権限を付与するために、「<u>情報処理の促進に関する法律</u>」を改正する。	経産省	A. IPAによる管理 C. IPAによる助言
人材面	2	人材の確保 (部署の設置)	ガイドラインの体系化・管理や情報提供を継続的に行うために<u>必要な人材を確保する</u>。	ガイドラインを一元管理する団体	A. IPAによる管理 B. IPAによる情報提供 C. IPAによる助言
	3	会議体の設置	- 各省庁に対して、<u>以下の内容を助言するための会議体を設置する</u>。 - 既存の脅威に対して対応できていないガイドラインの修正 - 新たな脅威に対応するためのガイドラインの更新	ガイドラインを一元管理する団体	A. IPAによる管理 C. IPAによる助言
情報/ ツール	4	WEBページ作成/公開	対象者を明確にした上で、<u>事業者が必要とする情報を提供できるようWEBページを作成する</u>。	ガイドラインを一元管理する団体	B. IPAによる情報提供
金銭面	5	予算的な措置	No.2～No.4を実施するための<u>予算を確保する</u>。	経産省/ガイドラインを一元管理する団体	A. IPAによる管理 B. IPAによる情報提供 C. IPAによる助言



Appendix[1章]

1.1 国内で策定されている制度やガイドライン等の概要

ISMS適合性評価制度/概要

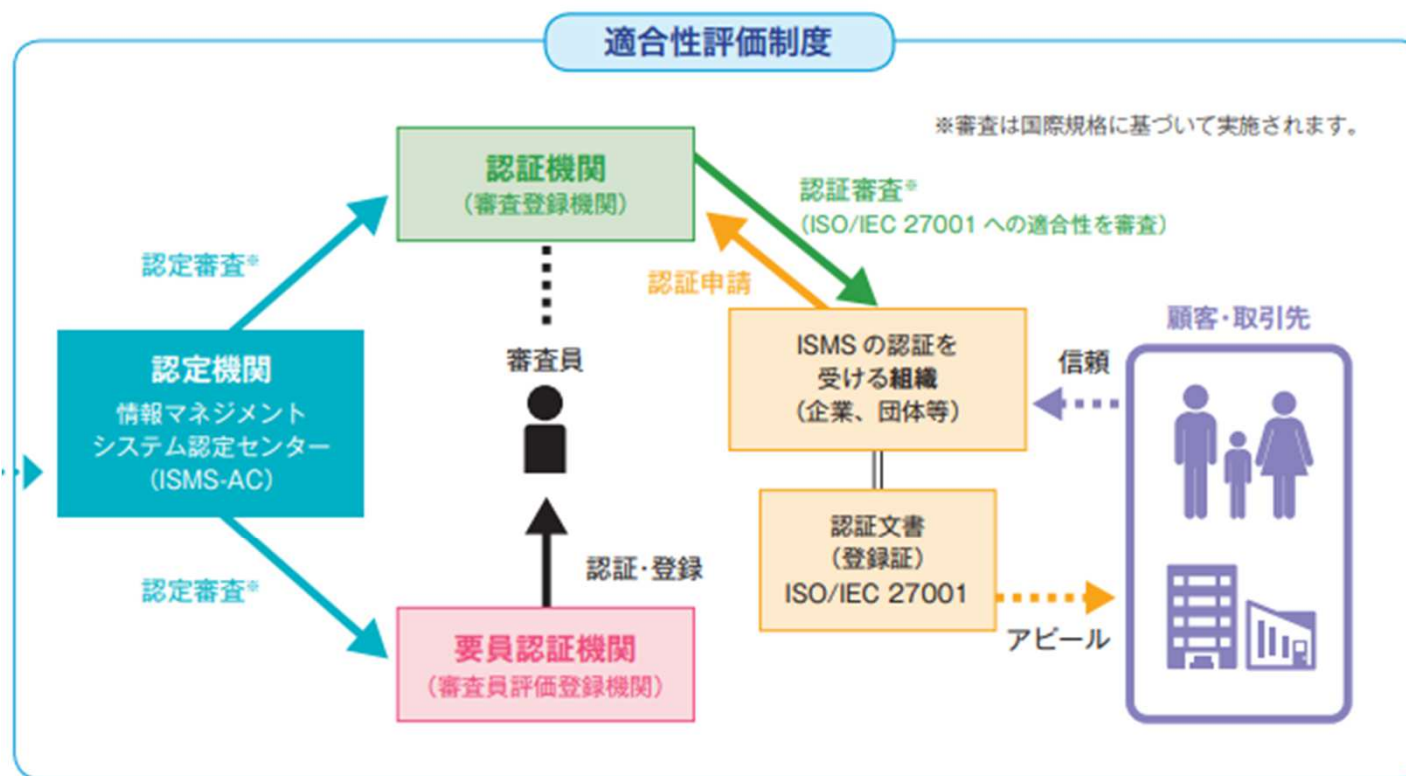
- ISMS適合性評価制度は、ISMS認証機関がISO/IEC 27001(JIS Q 27001)に基づいて適切に運用管理されているかを証明する制度。

1.1 国内で策定されている制度やガイドライン等の概要

名称	ISMS適合性評価制度		
国・地域	日本	策定者	情報マネジメントシステム認定センター (ISMS-AC)
適用分野	情報システム全般	遵守義務の有無	なし
対象者	ISMS認証の取得を希望する団体		
概要	- 第三者であるISMS認証機関が、組織の構築したISMSがISO/IEC 27001(JIS Q 27001)に基づいて適切に運用管理されているかを証明する制度。ISMS適合性評価制度によって、組織はISO/IEC 27001に沿って情報セキュリティを確保するための仕組みをもち、その仕組みを維持し継続的に改善していることを、顧客や取引先に対して客観的に示すことが可能となる。 - ISO/IEC 27001において、以下に示す対策事項を定める。 <計画(Plan)> ➢ 組織の状況(4章) ➢ リーダーシップ(5章) ➢ 計画(6章) ➢ 支援(7章) <チェック(Check)> パフォーマンス評価(9章) <改善(Act)> 改善(10章)		
普及状況	取得企業数:7,748社(2024年4月18日時点)		
URL	https://isms.jp/doc/JIP-ISMS120-70.pdf		

ISMS適合性評価制度/認証スキーム

- ISMS適合性評価制度では、情報マネジメントシステム認定センターによって認定を受けた機関が(認証を)希望する組織を認証する。



認証機関

第三者機関として組織のISMSを審査します。これを「認証審査」といいます。

認定機関

認証機関が適切に認証審査が実施できることを審査し、確認します。これを、「認定審査」といいます。

要員認証機関

認証審査に関する能力をもつ審査員を認証、登録します。

ISMS適合性評価制度の普及状況 / 業種ごとの取得企業数

- 情報通信業においてISMS認証の取得が進む一方で、農林水産業や鉱業/採石業/砂利採取業、運輸業/郵便業等では取得が進んでいない。

産業分類(※1)	ISMS取得企業数(※2)(※3) (2018年1月29日時点)	全取得企業数に 占める割合	[参考]産業分類 別企業数
情報通信業	715	62.9%	56,599
学術研究、専門・技術サービス業/生活関連サービス業、娯楽業/ 教育、学習支援業/サービス業（他に分類されないもの）	209	18.4%	214,724
製造業	80	7.0%	339,738
建設業	50	4.4%	426,155
卸売業、小売業	45	4.0%	741,239
医療、福祉	18	1.6%	298,517
金融業、保険業/不動産業、物品賃貸業	16	1.4%	30,995
電気・ガス・熱供給・水道業	2	0.2%	5,496
宿泊業、飲食サービス業	1	0.1%	426,575
複合サービス事業	0	0.0%	5,445
農業、林業、漁業	0	0.0%	35,301
鉱業、採石業、砂利採取業	0	0.0%	1,428
運輸業、郵便業	0	0.0%	66,831
合計	1,136	100%	3,684,049

※1:産業分類は日本標準産業分類(平成25年10月改定)を参考としているが、「ISMS適合性評価制度に関する調査報告書」に沿って一部分類を統合している。

※2:ISMS取得企業のうち、調査に協力した企業の内訳を示す。また、「公共・行政・教育機関」(12)「分類不明」(32)を除外している。

※3:同一の法人の中で複数の部門が個別に認証を取得している場合、重複して集計している。

[参考] 総務省 経済産業省「令和3年経済センサス-活動調査産業横断的集計「事業所に関する集計・企業等に関する集計」結果の要約」

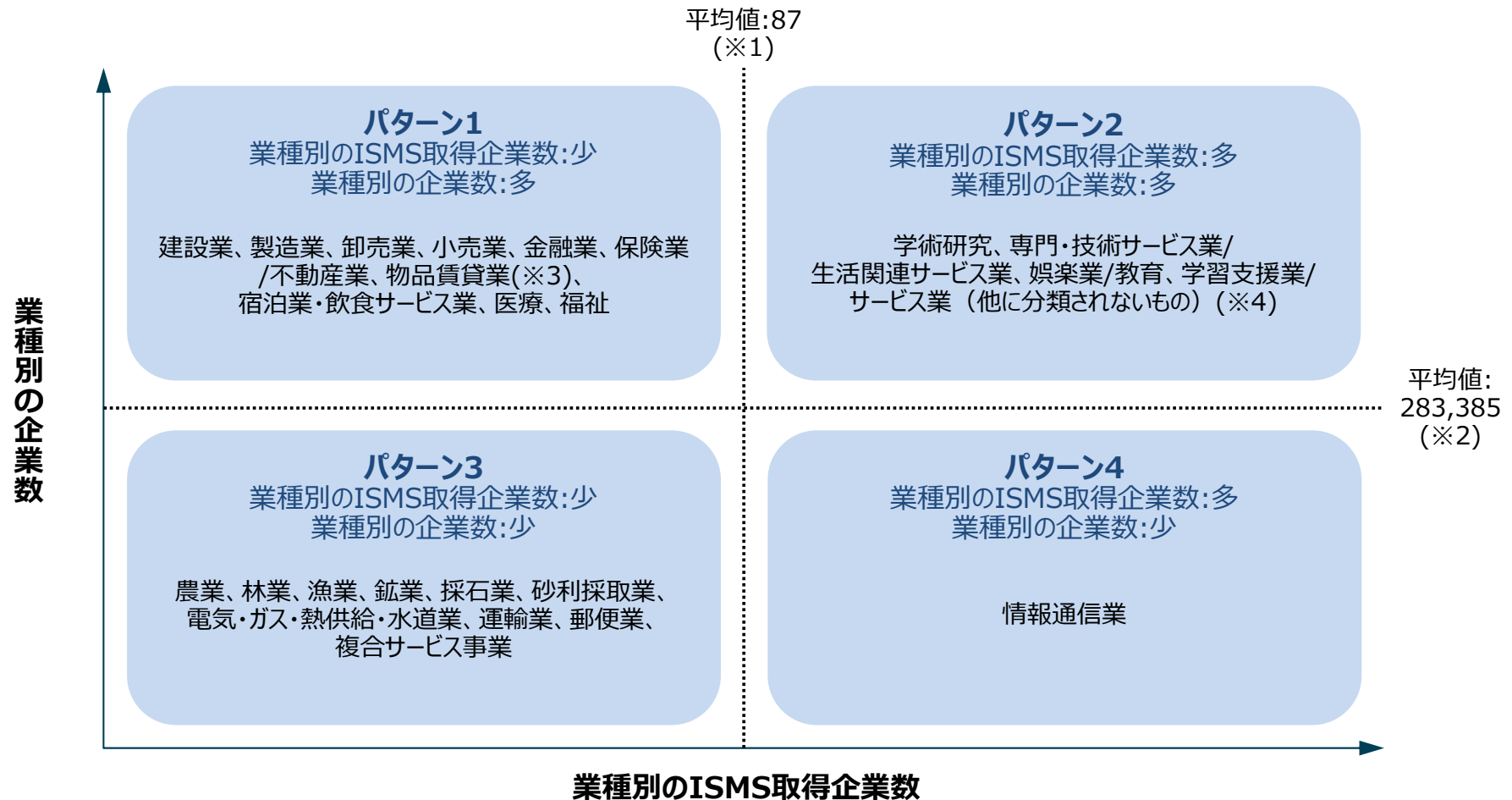
https://www.stat.go.jp/data/e-census/2021/kekka/pdf/k3_summary.pdf

[参考] 情報マネジメントシステム認定センター「ISMS適合性評価制度に関する調査報告書」

<https://isms.jp/enquete/2017/report2017.pdf>

ISMS適合性評価制度の普及状況 / 企業の全体数を考慮した分析

- 取得件数そのものが多かったとしても、業種別の企業総数を考慮すると、建設業や製造業、小売業等のように事業者数が多い分野においては、相対的に取得企業数が伸び悩んでいると捉えられる場合がある。



※1: ISMS取得企業数(1,136)/P4で用いた分類数(13)=約87

※2: 2021年6月1日時点の日本の企業数(3,684,009)/P4で用いた分類数(13)=約283,385

※3,4: 日本産業分類では別の分類となっているが、ISMS認証取得企業数と比較するため便宜上1つの分類としている点にご留意いただきたい。

[参考] 総務省 経済産業省「令和3年経済センサス-活動調査産業横断的集計「事業所に関する集計・企業等に関する集計」結果の要約」

https://www.stat.go.jp/data/e-census/2021/kekka/pdf/k3_summary.pdf

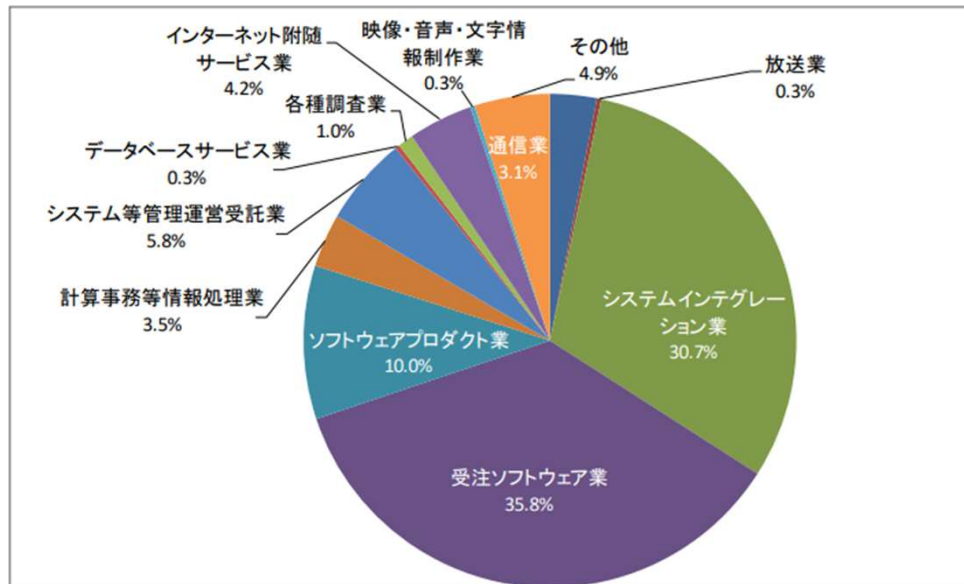
情報マネジメントシステム認定センター「ISMS適合性評価制度に関する調査報告書」

<https://isms.jp/enquete/2017/report2017.pdf>

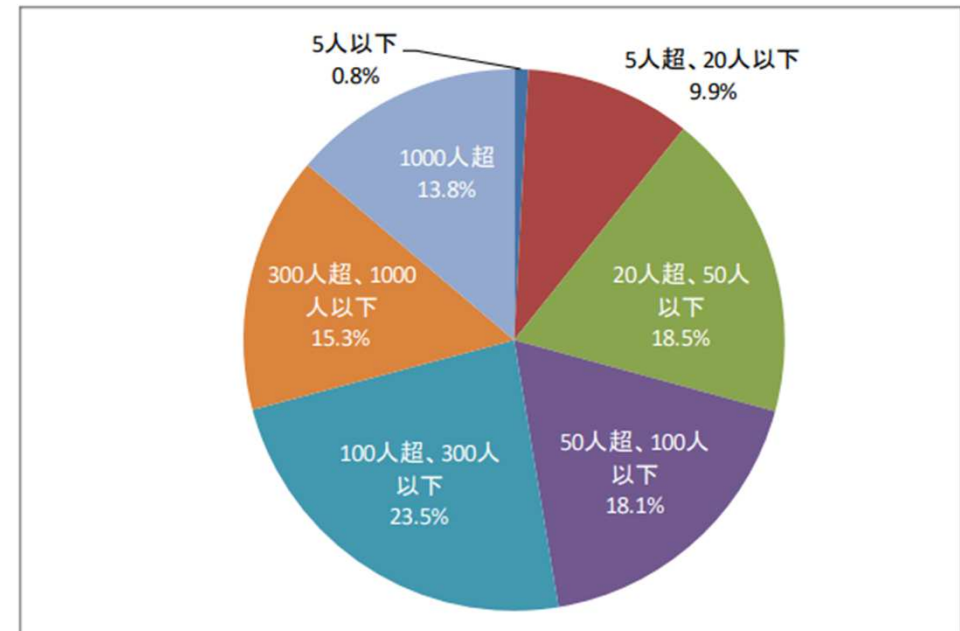
[参考] ISMS認証取得企業の内訳

- 情報通信業では、特にシステムインテグレーション業と受注ソフトウェア業の企業においてISMS認証の取得が進んでいる。
- 20人より規模が大きい企業においてISMS認証の取得が進んでいる一方で、特に5人以下の企業においてISMS認証の取得は進んでいない。

情報通信業の企業内訳



従業員規模別の内訳



ISMS適合性評価制度/認証の取得状況や取得によるメリット

- 世界的にみると、日本企業によるISMS認証取得は多い部類にあると言える。
- 調達においてISMS認証有無を確認するケースがみられ、入札や受注の条件に含まれていたためにISMS取得した企業は、調査に協力したISMS取得企業のうち半数を超えている。

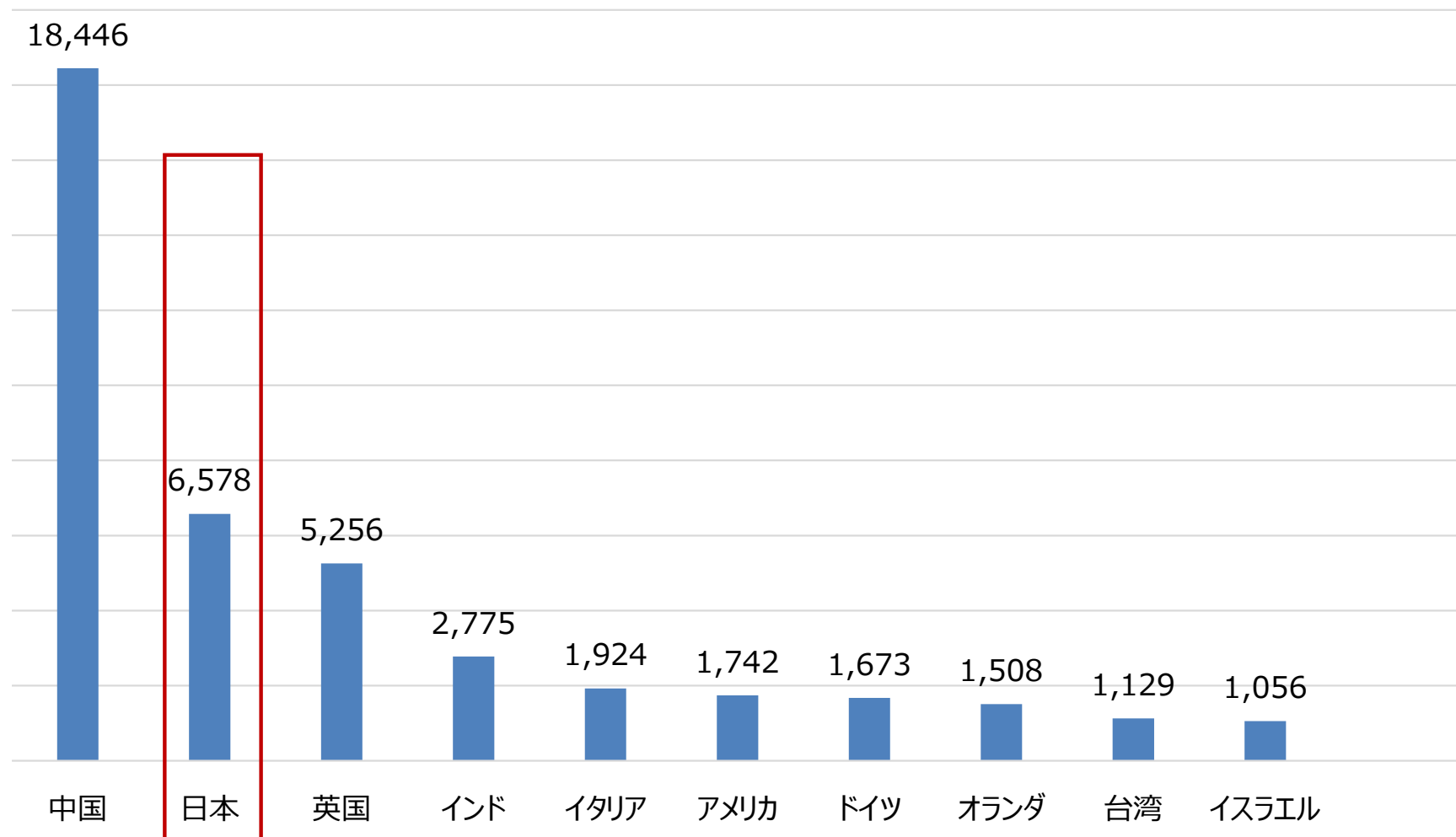
ISMS取得状況や取得によって得られたメリット等

取得状況	日本においてISMS認証を取得した企業数は6,500件を超え、中国に次いで世界第2位。<u>世界的にみると日本においてはISMSの取得が進んでいる。</u>[国別の取得件数は次頁参照]
調達先への確認状況	ISMS取得企業に対して、その調達先へISMS認証の取得有無を確認したことがあるかを尋ねたところ、46.0%が「確認し、プラス評価したことがある」と回答。次いで、36.4%が「確認のみ、実施したことがある」と回答。17.6%が「確認したことはない」と回答していることから、調査に回答した<u>ISMS取得企業のうち8割以上が調達先に対してISMS取得有無を確認している。</u>
ISMS取得の目的または理由	- ISMS取得企業が認証を取得した目的または理由について、取得企業の多くが<u>組織のセキュリティ対策や管理体制の強化を目的として認証を取得している。また、外部からの評価や要請も取得理由の1つとなっている。</u> - 組織の情報セキュリティ対策の強化のため[調査に協力したISMS認証取得企業の80.8%が「該当」と回答] - 組織の情報システム管理体制の強化のため[調査に協力したISMS認証取得企業の80.4%が「該当」と回答] - 顧客からの信頼を確保するため[調査に協力したISMS認証取得企業の81.0%が「該当」と回答] - 企業イメージの向上のため[調査に協力したISMS認証取得企業の61.1%が「該当」と回答] <u>入札、受注の条件、取引先からの要請</u>による[調査に協力したISMS認証取得企業の<u>55.4%</u>が「該当」と回答]
ISMS取得によって得られたメリット	- ISMS取得企業が感じているISMS認証取得のメリットは以下の通り。 <組織内部のメリット(例)> - 組織の社員の情報セキュリティに関する意識向上につながる[調査に協力したISMS認証取得企業の71.8%が「該当」と回答] - 組織の情報セキュリティ管理体制、情報セキュリティ対策を強化できる[調査に協力したISMS認証取得企業の70.6%が「該当」と回答] - 経営者の情報セキュリティに対する関与が深まる[調査に協力したISMS認証取得企業の50.1%が「該当」と回答] <対外的なメリット(例)> - 顧客からの信頼確保につながる[調査に協力したISMS認証取得企業の56.4%が「該当」と回答] - 企業イメージの向上につながる[調査に協力したISMS認証取得企業の44.1%が「該当」と回答]

[参考] ISMS認証の取得状況

- 日本においてISMS認証を取得した企業数は中国に次いで世界第2位。

国ごとのISMS認証の取得件数(上位10位[2021年時点])



[参考] 一般財団法人 日本品質保証機構「世界のISO認証取得動向 ISO Survey 2021」
(https://www.jqa.jp/service_list/management/iso_info/iso_network/vol37/file/isonetwork37_04world_trend.pdf)

ISMS適合性評価制度/ISMSを取得しない理由や運用上の課題

- 顧客から求められていないなど、その動機がないためISMSを取得していない企業が多くみられた。
- また、ISMSを取得した企業であっても、その後の運用の段階で課題がみられ、セキュリティの確保のためにISMSが十分に機能していないケースがある。

ISMSを取得しない理由/ISMSに関する今後の課題

ISMS取得をしない理由

- ISMS 認証を取得していない企業に対してISMS認証を取得しない理由を尋ねた際の理由は以下の通り。顧客から求められていないなど、ISMS認証を取得する動機がない企業においてISMS取得が進んでいない可能性がある。
 - 顧客から求められていないため(67.7%)
 - 国際展開を重視していない(36.3%)
 - ISO規格に基づくマネジメントシステム導入は組織の状況に合わない(24.0%)

ISMSに関する今後の課題

- ISMS認証取得企業において、ISMS 認証に関する今後の課題は以下の通り。ISMSを取得したとしても、その後の運用の段階で課題がみられ、セキュリティの確保のためにISMSが十分に機能していないケースがある。
 - ＜今後の課題(例)＞
 - マンネリ化/形骸化(例:ルールは定着したが、何のためのルールになっているのか理解されていないことがある。ある程度マネジメントシステムは定着したが、内部監査項目等が固定化されて形骸化されている。)
 - 人材の確保/育成(例:ISMSを理解し、実行できる要員が限られている。ISMSの理解が全社員に浸透していない。新しく入社された方への教育する関係者が不足している。)
 - 新技術や環境変化への対応(例:クラウド分野への進出による新たなリスクへの対応が必要。脅威のリスク評価と投資計画を長期的に計画する力量が不足している。)
 - 事業内容の変化や組織改革などへの対応(例:ISMSの活動範囲が組織変更の度に変更となり運用が困難。経営環境、事業内容、組織の変化が激しい中、ルールの改訂や周知が追い付かない。)

ISMS適合性評価制度/民間における自主的な支援活動

- JNSAの日本ISMSユーザグループにおいて、ISMSの実装・運用についての事例研究がなされており、ISMSの普及促進に向けて民間主導で取組がなされている。
※ インプリメンテーションWGでの活動を示す。その他、メジャメントWGでも活動を行っていたが、2013年度からインプリメンテーションWGに一本化

日本ISMSユーザグループの概要		活動概要(※)	
活動目的	ISMS認証取得企業(ユーザ)とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動を行う。	2006 2007	活動紹介/ISMS導入に関する課題の事例紹介/情報セキュリティ研修・啓発/効率的なリスクアセスメント
年間活動予定	- 毎月開催:インプリメンテーションWGにおけるISMSの構築や運用における課題検討 12月開催:情報セキュリティマネジメントセミナーの開催と研究結果の発表	2008	ISMS構築事例にみる有効性測定構築の傾向/業務委託先のセキュリティ評価
予定成果物	- 必要に応じて、成果物として以下に関連するものをまとめるものとする。 ➤ <u>ISMSの実装&運用についての事例研究(下記の2テーマをユーザ視点で整理)</u> ✓ リスクアセスメントについて考える(フレームワーク含めた全体整理) ✓ 委託先管理	2009	標準的なリスク分類と具体的な管理策の対応のモデル化/管理策の有効性評価を効率的に行うモニタリング手法のモデル化
		2010	標準的なリスク分類と具体的な管理策の対応のモデル化/管理策の有効性評価を効率的に行うモニタリング手法のモデル化
		2011	可視化手法を用いたリスク対策モデル/ISMS全体の有効性評価手法
		2012	可視化手法を用いたリスク対策モデルとその実践的応用/ISMS実践手法BCPのモデル化の検討
		2013	ISMS推進事務局の悩みと解決策/有効性評価に基づくISMS実践活用
		2014	ISMS推進事務局の悩みと解決策/ISMS規格改訂にともなう実装方法の検討
		2015	ISMSを成功させる理想的なCISOの条件/減らないインシデントの特効薬
		2016	サイバー攻撃を事例としたリスクマネジメントの実践/運用フェーズにおける有効性の評価
		2017	現場と連携したリスクアセスメント手法の実践活用/内部監査を有効に運用するための手法の考察
		2018	ISMS規格要求事項から紐解く最新のビジネス環境リスク/働き方改革における情報セキュリティ
		2019	最新の環境変化に伴うISMSの実装検討/各社の事例から学ぶISMSの実装について

[参考] JNSA「日本ISMSユーザグループ」(<https://www.jnsa.org/active/std.html#ismsug>)
JNSA「標準化部会 日本ISMSユーザグループ」(https://www.jnsa.org/jnsapress/vol47/3_WG-2.pdf)

ISMSクラウドセキュリティ認証/概要

- ISMSクラウドセキュリティ認証は、通常のISMS認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が適切に導入、実施されていることを認証する制度。

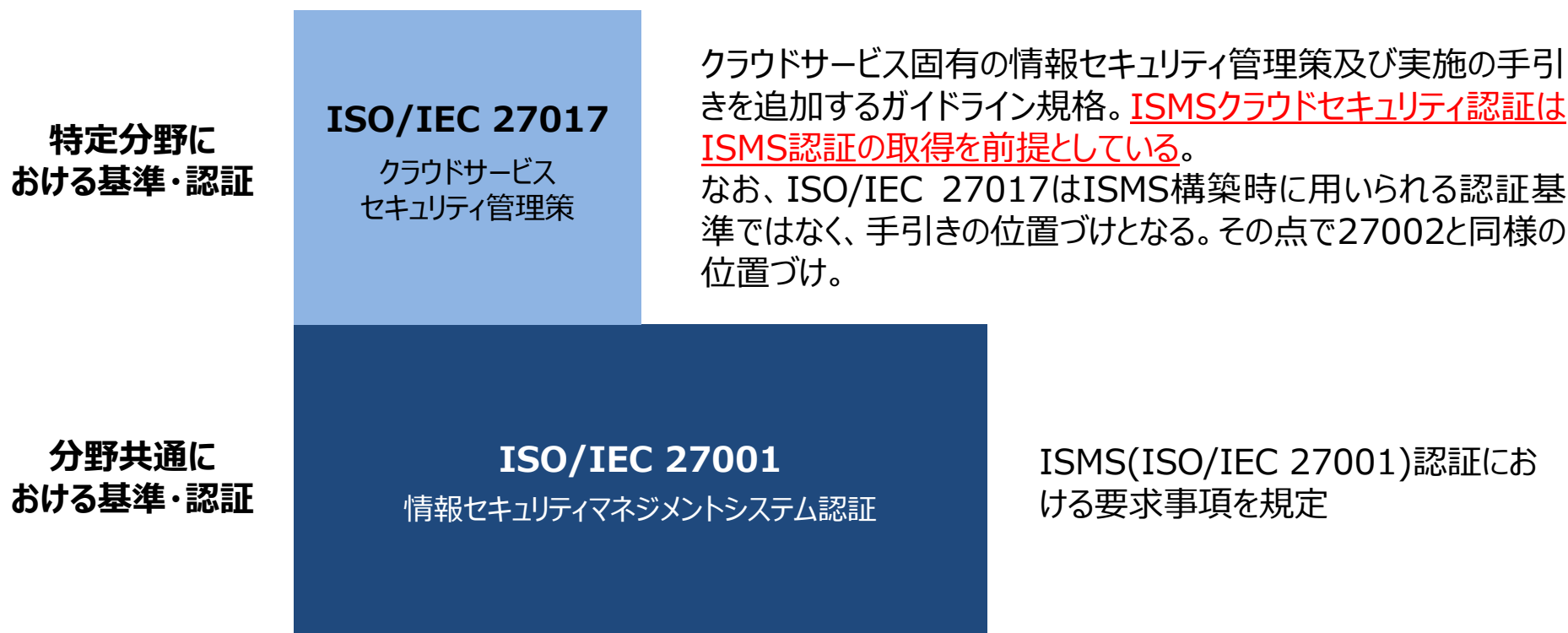
1.1 国内で策定されている制度やガイドライン等の概要

名称	ISMSクラウドセキュリティ認証		
国・地域	日本	策定者	情報マネジメントシステム認定センター (ISMS-AC)
適用分野	クラウドサービス (IaaS、PaaS、SaaSを問わない)	遵守義務の有無	なし
対象者	- クラウドサービスを提供している組織(クラウドサービスプロバイダ) - クラウドサービスを利用している組織(クラウドサービスカスタマ)		
概要	- 企業や一般ユーザが、安心してクラウドサービスを利用できることを目的として、通常のISMS認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が適切に導入、実施されていることを認証する。 - ISMSクラウドセキュリティ認証の認証基準は、ISO/IEC 27017:2015(JIS Q 27017:2016)に基づくISMSクラウドセキュリティ認証に関する要求事項を示すJIP-ISMS517。要求事項は以下の通り。 ➤ クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定(4.1) ➤ ISO/IEC 27017の規格に沿ったクラウド情報セキュリティ対策の実施(4.2) ✓ 情報セキュリティリスクアセスメント(4.2.1) ✓ 情報セキュリティリスク対応(4.2.2) ➤ 内部監査(4.3)		
普及状況	524社(2024年4月18日時点)		
URL	https://isms.jp/isms-clc.html		

ISMSクラウドセキュリティ認証/ISMS認証との関係

- ISMSクラウドセキュリティ認証はISMS認証の取得を前提としており、2階建て構造となっている。
- ISO/IEC 27017はISMS構築時に用いられる認証基準ではなく、手引きの位置づけ。

ISMSクラウドセキュリティ認証の構造



CSMS適合性評価制度/概要

- CSMS適合性評価制度は、産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度。

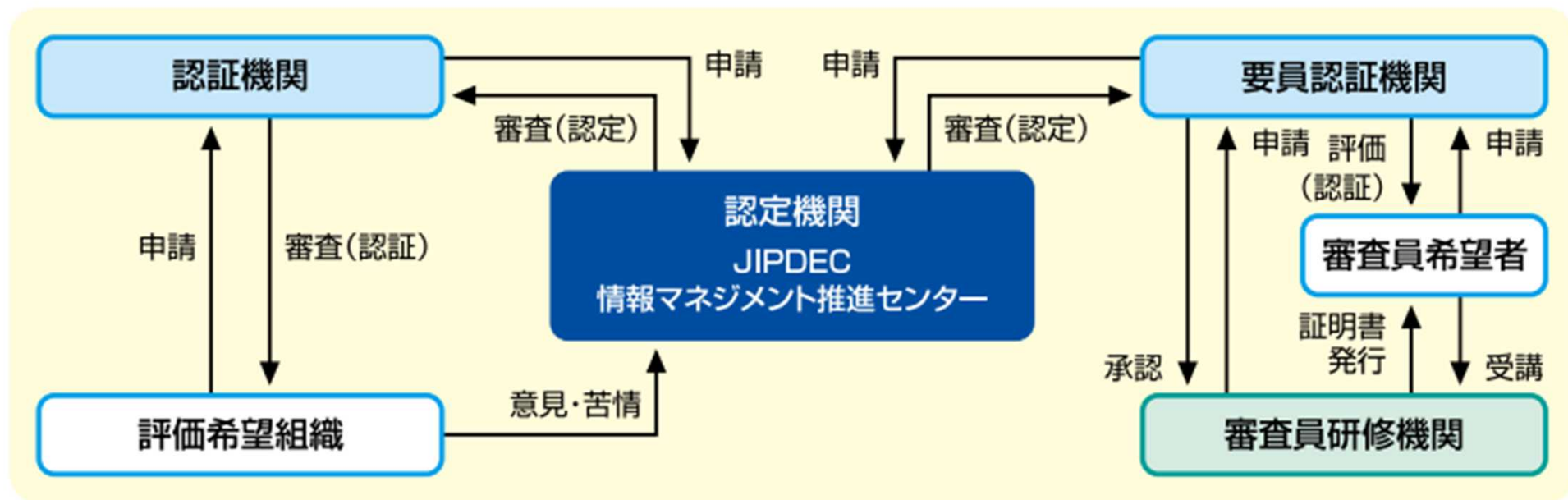
1.1 国内で策定されている制度やガイドライン等の概要

名称	CSMS適合性評価制度		
国・地域	日本	策定者	情報マネジメントシステム認定センター (ISMS-AC)
適用分野	産業用オートメーション及び制御システム (IACS: Industrial Automation and Control System)	遵守義務の有無	なし
対象者	- 制御システムを保有する事業者(アセットオーナー) - 制御システムの構築事業者(システムインテグレータ) - 制御システムの運用・保守事業者		
概要	- 組織の産業用オートメーション及び制御システムをサイバー攻撃から守るためのセキュリティ対策を確保するとともに、日本の制御システムセキュリティの向上に貢献することを目的とする。 - 産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度。 - IEC62443-2-1に準拠した制度。		
普及状況	取得企業数:3社(2024年4月18日時点)		
URL	https://isms.jp/csms/index.html https://isms.jp/csms/doc/JIP-CSCC100-20.pdf		

CSMS適合性評価制度/認証スキーム

- CSMS適合性評価制度では、JIPDECより認定を受けた機関が希望する組織を認証する。
- ISMS適合性評価制度と同様の仕組みとなっている。

適合性評価制度の運用体制



CSMS適合性評価制度/CSMS認証に対する意見等

- CSMS認証取得に係る説明会では、他の制度(例:ISMS適合性評価制度)との整合性や差分を問う意見が寄せられている。
- また、認証を取得した際のメリットの不明確さや認知率の低さを指摘するご意見等が寄せられている。

「平成26年度 CSMS適合性評価制度に関する説明会」にて寄せられた主なご意見(※)

他の制度 (例:ISMS適合性 評価制度)との差異 がわかりにくい	<u>ISMS適合性評価制度との整合性を明確にしてほしい</u> <u>ISMS適合性評価制度との統合について、重複した運用をなくしてほしい</u> <u>ISMSとの差異が明確でなかった点が今後の課題</u> - CSMSとQMSの関係がわからない(QMSでカバーできないのか。) - システムを開発する際にデザインレビューを実施しているが、CSMSと重複する項目の効率化が必要
CSMS認証取得の メリットがわからない	CSMS認証取得のメリットを明確にしてほしい
CSMSの認知率が 低い	- CSMS適合性評価制度の認知向上が必要 - マスコミ等を通じたPRを検討いただきたい - 国や業界団体として、CSMS適合性評価制度の啓蒙が課題
CSMSの対象やその 内容がわからない	- どこまでがCSMS適合性評価制度の対象となるかが不明確 - SI業務においてどこまでCSMS認証を求められているか判断できない

- 例えば、ISMS適合性評価制度との関係性は示されておらず、これらのご意見にて指摘された内容がCSMS認証取得を妨げる要因となっている可能性がある。
- 新たに評価制度を構築する場合には、当該説明会で寄せられたご意見と同様のご意見が寄せられる可能性がある。

※寄せられたご意見のうち、CSMS評価制度を対象としたご意見を抽出

端末機器の基準認証制度

- 端末機器の基準認証制度は、事業者のネットワークに接続して使用される端末機器(その設計含む)について「接続の技術基準」に適合していることを登録認定機関等が認定する制度。

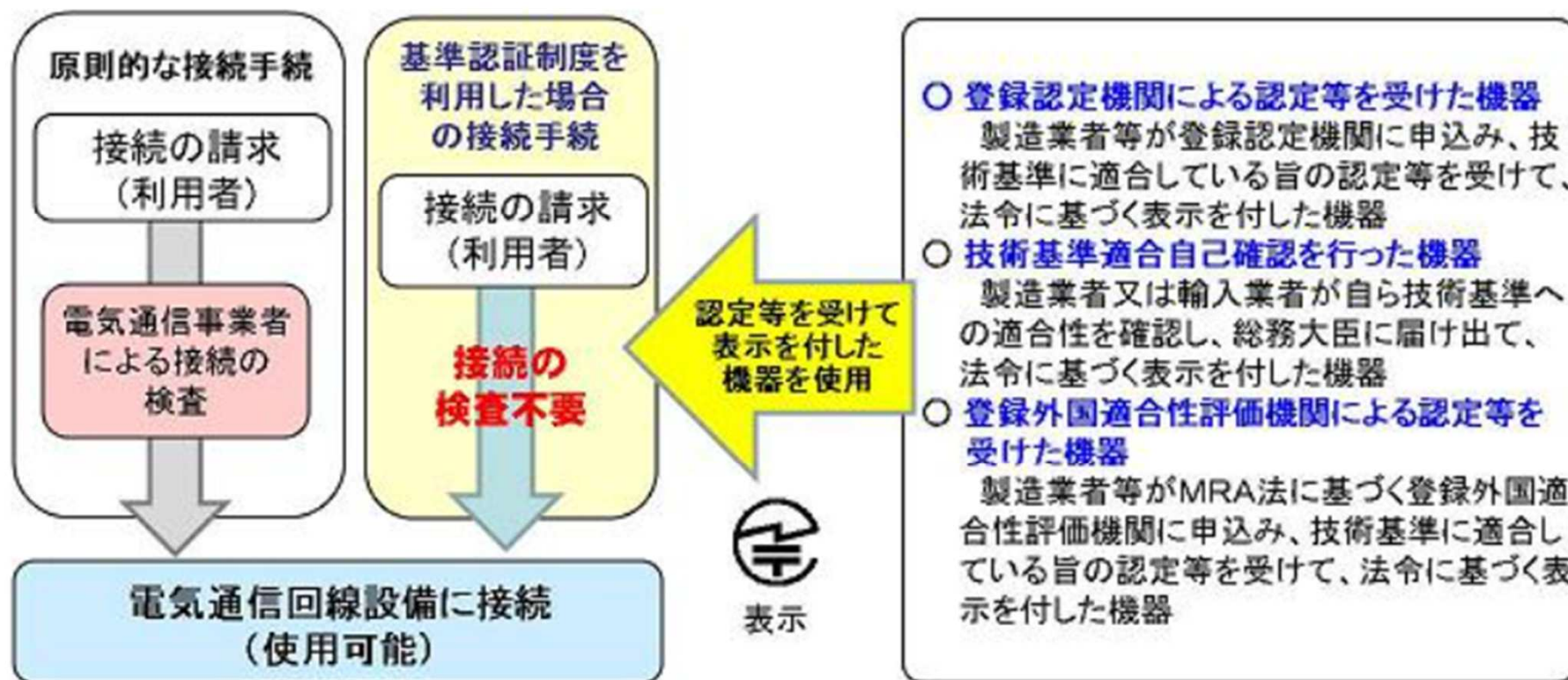
1.1 国内で策定されている制度やガイドライン等の概要

名称	端末機器の基準認証制度		
国・地域	日本	策定者	総務省
適用分野	端末機器*1	遵守義務の有無	あり
対象者	製造事業者		
概要	- 事業者のネットワークに接続して使用される端末機器(その設計含む)について「<u>接続の技術基準</u>」に適合していることを登録認定機関等が認定する制度。電気通信事業法における基準認証制度は以下の3つ。 ✓ 技術基準適合認定(電気通信事業法第53条) ✓ 設計認証(電気通信事業法第56条) ✓ 技術基準適合自己確認(電気通信事業法第63条) - 電気通信事業法の第52条第1項及び第70条第1項の規定に基づき、<u>端末設備等規則において技術基準が定められている</u>。具体的には、端末設備等規則の第34条第10項において、電気通信事業法の規定による技術基準適合認定(電気通信事業法第53条第1項)や設計認証(電気通信事業法第56条)又は技術基準適合自己確認(電気通信事業法第63条)に関連する<u>セキュリティ基準を定めている</u>。 「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」では、IoT機器を含む端末設備の技術基準にセキュリティ対策を追加した<u>端末設備等規則の各規定等に係る端末機器の基準認証に関する運用について、明確化</u>されている。		
普及状況	(義務のため対象となる全ての端末機器に適用)		
URL	https://elaws.e-gov.go.jp/document?lawid=360M50001000031 https://www.tele.soumu.go.jp/resource/j/equ/mra/pdf/30/j/08.pdf		

*1 端末機器は、アナログ電話用設備、インターネットプロトコル電話用設備、インターネットプロトコル移動電話用設備、無線呼出用設備、総合デジタル通信用設備、専用通信回線設備

端末機器の基準認証制度

- 登録認定機関から技術基準に適合していることの認定を受けるなどして総務省令で定める表示(技適マーク)が付された機器を接続する場合、当該端末機器の利用者は、電気通信事業者による接続の検査を受けることなく接続し機器を使用することが可能。



端末機器の基準認証制度

- 電気通信事業法における基準認証制度は以下の3つ。

- ✓ 技術基準適合認定(電気通信事業法第53条)
- ✓ 設計認証(電気通信事業法第56条)
- ✓ 技術基準適合自己確認(電気通信事業法第63条)

種類	内容
技術基準適合認定 (電気通信事業法第53条)	- 技術基準適合認定とは、総務大臣の登録を受けた者(登録認定機関*1)等が、端末機器について、<u>電気通信事業法に基づく技術基準に適合しているか否かについての判定を端末機器1台ごとに行う制度</u>。 - 登録認定機関は、総務省令で定めるところにより、端末機器1台1台について試験等の審査を行った上で認定を行う。 - 技適マークは、登録認定機関が、技術基準適合認定を行った端末機器に付す。
設計認証 (電気通信事業法第56条)	- 設計認証とは、<u>端末機器が技術基準に適合しているかどうかの判定について、その設計及び製造等の取扱いの段階における品質管理方法(確認の方法)を対象に、登録認定機関がその適否の判定を行う認証制度</u>。 - 端末機器そのものではなく、端末機器の設計等を対象としているため、<u>認証後に実際の端末機器が製造される点など</u>で技術基準適合認定と異なる。 - 技適マークは、設計認証を受けた者が電気通信事業法に定める設計合致義務を履行した後に、製造された端末機器に付される。
技術基準適合自己確認 (電気通信事業法第63条)	- 技術基準適合自己確認とは、端末機器のうち、<u>他の利用者の通信に著しく妨害を与えるおそれが少ないものとして総務省令で定めるもの(特定端末機器)の製造業者又は輸入業者が、その特定端末機器の設計について、電気通信事業法に基づく技術基準に適合するものであることを自ら確認</u>し、かつ、その設計に基づく特定端末機器のいずれもが、その設計に合致することを確認することができると認める場合に限り行うことができる制度。 - 技適マークは、自ら確認を行い、総務大臣に届出を行った製造業者又は輸入業者(届出業者)が電気通信事業法に定める設計合致義務を履行した後に、製造された端末機器に付される。

*1 調査時点(2024年5月13日時点)で登録認定機関の数は12

[参考] セキュリティ基準に係る認定等を求める対象

- 端末機器のうちセキュリティ基準に係る認定等を求める対象は、(1)から(3)までの全てに該当し、(4)を除くもの。
 - (1)専用通信回線設備等端末(デジタルデータ伝送用設備に接続されるものに限る。)
 - (2)デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもの
 - (3)電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能(送受信に係るものに限る。)に係る設定を変更できるもの
 - (4)条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末(例:PC、スマートフォン)

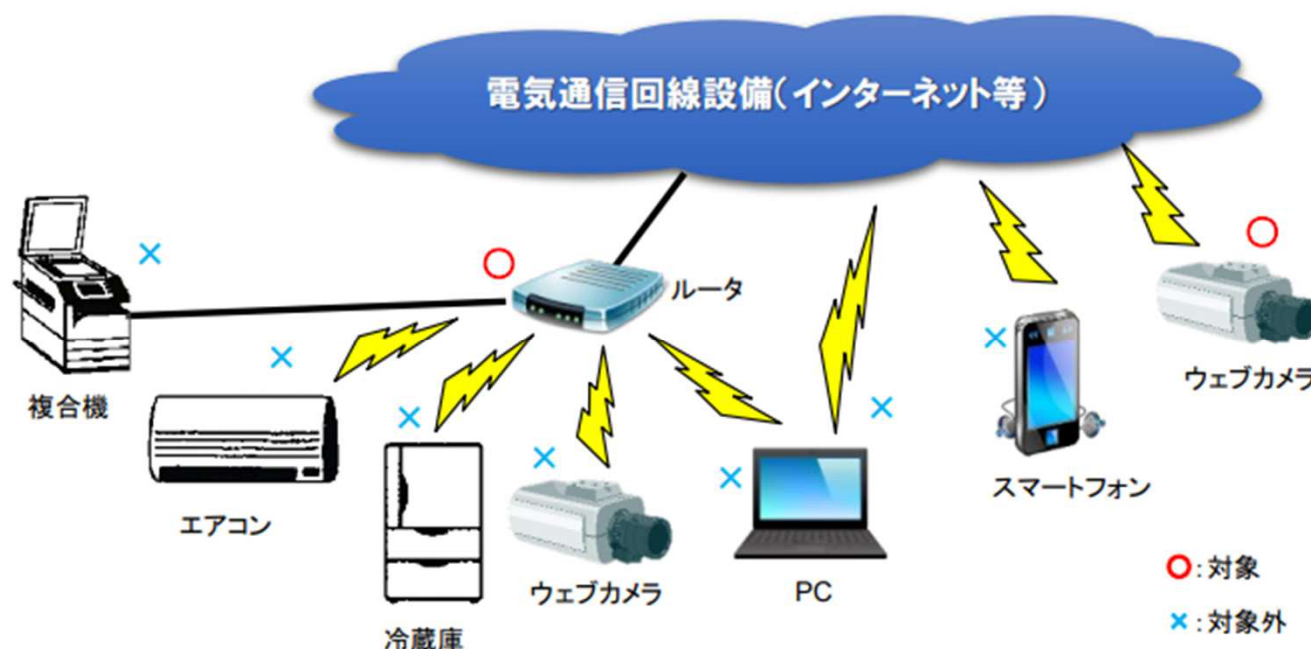


図1 セキュリティ基準(新規則第34条の10)に係る技術基準適合認定等の対象機器の範囲のイメージ

[参考] セキュリティ基準

- 「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」において、対象機器が遵守すべきセキュリティ基準を定めている。

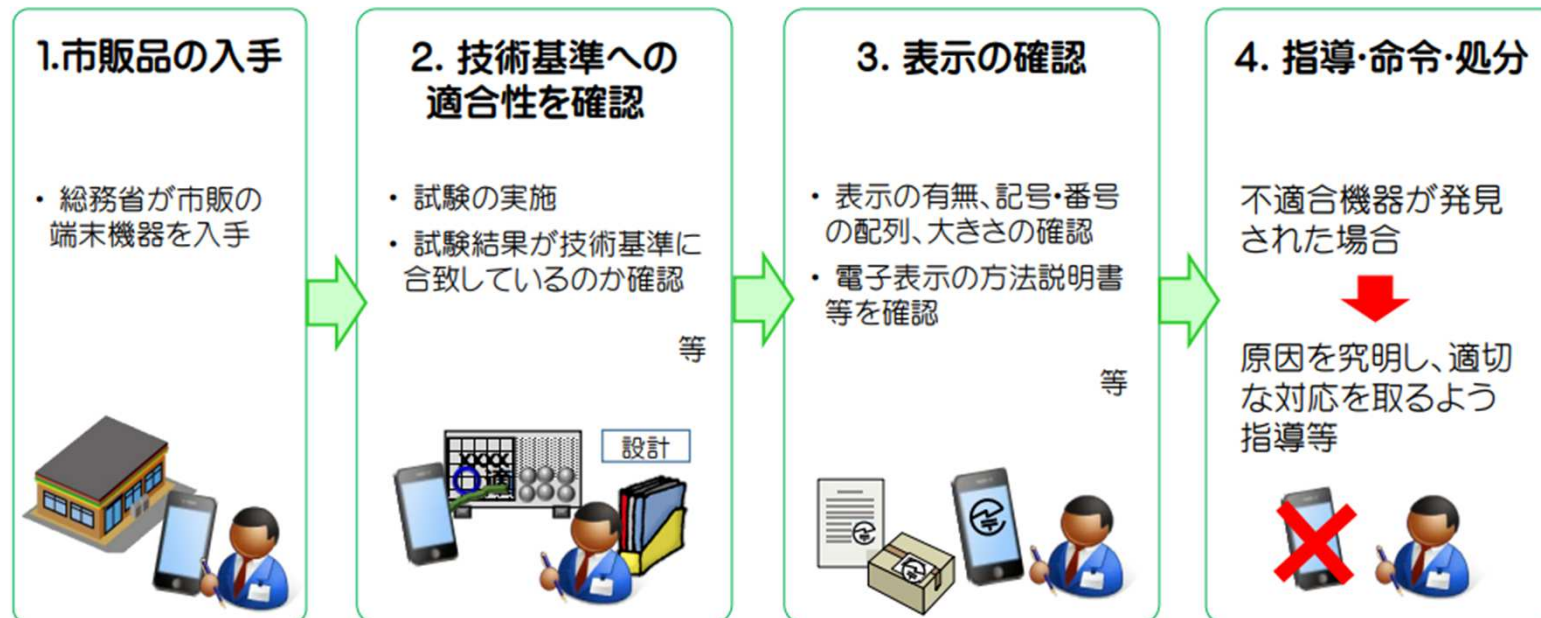
No.	セキュリティ基準	内容
1	アクセス制御機能を有すること	電気通信回線設備を介して接続されることにより、端末機器に備えられた電気通信の送受信に係る機能が不正に設定変更(操作)されないことを目的として、当該 <u>設定変更(操作)の前にアクセス制御を行うことができる機能を有していなければならない。</u>
2	識別符号の初期値の変更を促す機能もしくは機器ごとに別の識別符号が付されていること 等	アクセス制御の際に使用する識別符号が他人から容易に推測できないものとして設定されることを目的として、 <u>識別符号の初期値</u> (例えばパスワードとIDの両方による認証や複数のパスワードによる認証など、複数の符号の組合せにより初期値が設定されている場合は、少なくとも一のID又はパスワードの初期値)の <u>変更を促す機能があり、もしくは機器ごとに別の識別符号(ID/パスワード)が付されており、又は、これらに準じる機能・措置が講じられているものでなければならない。</u>
3	ソフトウェアを更新できること	端末機器に記憶されている電気通信の送受信の機能に係る <u>ソフトウェアの更新を行うことができる機能(ファームウェアの更新機能)を有していなければならない。</u>
4	電力の供給が停止した場合であっても電源オフになる直前の状態にソフトウェアを維持できること	端末機器への電力供給が停止して電源オフになった後、電力供給が再開されて電源オンに戻って電気通信の機能が復帰した際に、 <u>アクセス制御の際に使用する識別符号の設定及び更新された電気通信の送受信の機能に係るソフトウェアが、出荷時の初期状態に戻ることなく、電源オフになる直前の状態を維持できるものでなければならない。</u>
5	No.1～No.4と同等以上の対策が認められること	新規則第34条の10各号の条件に適合するものと同等以上の <u>セキュリティ対策が講じられていると認められる場合は、セキュリティ基準を満たすこととしている。</u> 具体的には、対象機器が <u>国際標準 ISO/IEC15408 に基づくセキュリティ認証(CC認証)を受けた機器</u> などがこれに該当する。

端末機器の基準認証制度

- 総務省では、基準認証制度を適正かつ健全に維持・運用するため、市場に流通する端末機器を購入し、技術基準への適合性や表示などの確認を行って実態を把握している。

基準認証制度を適正かつ健全に維持・運用するため、市場に流通する端末機器を購入し、技術基準への適合性や表示などの確認を行って実態を把握

市場調査の流れ



- 認証マークを取得した後(運用時)に適合性を確認する仕組みとして有効と考えられる一方で、対象が一般市場で購入可能な端末機器(製品)を対象としている場合に本仕組みに機能すると考えられる。
- 組織を対象とした場合(例:成熟度モデルの対象)には同じ仕組みは成り立たないため、参考とはならない点に留意。

政府機関等のサイバーセキュリティ対策のための統一基準群

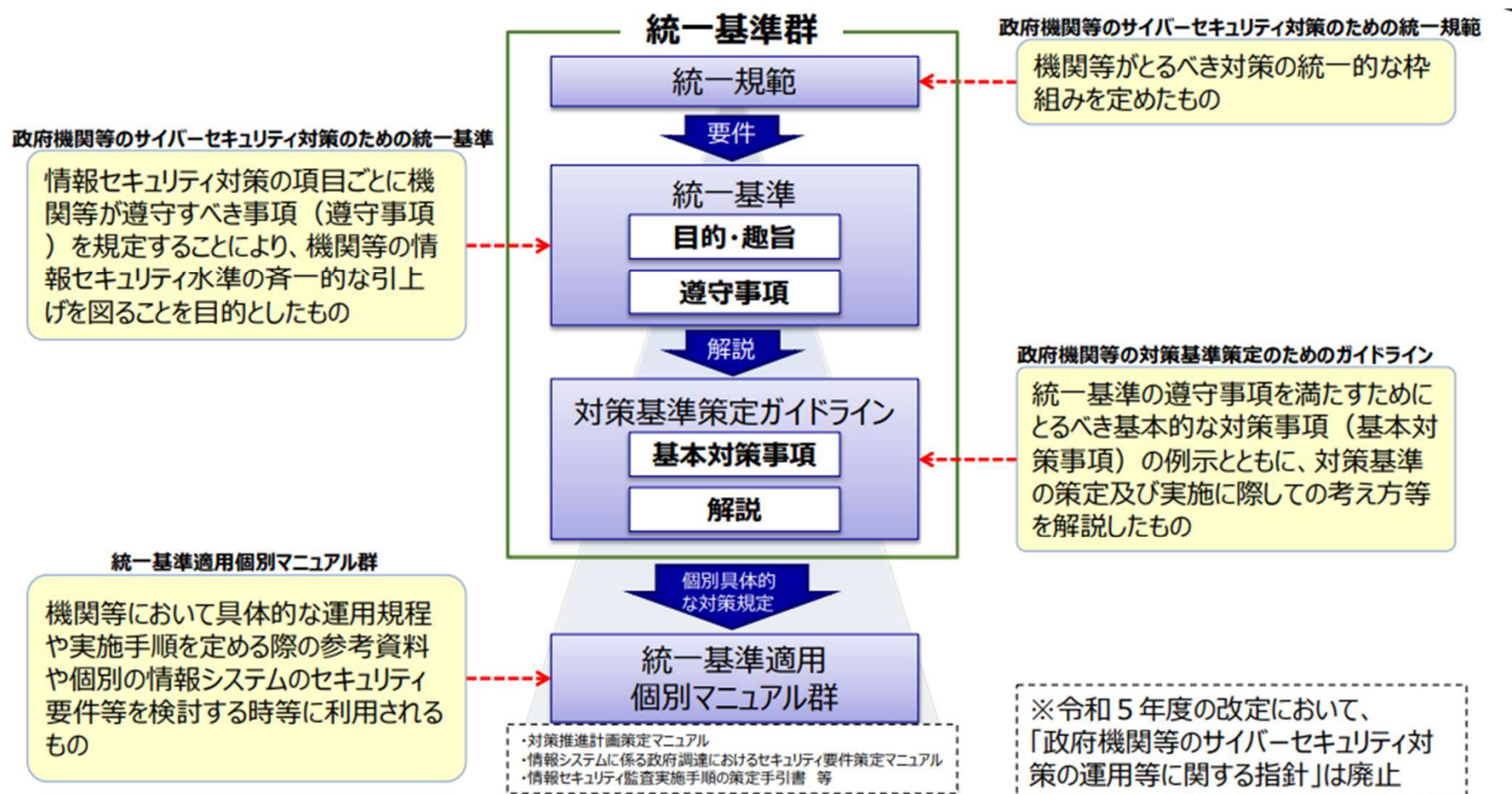
- 政府統一基準は、サイバーセキュリティ基本法に基づく、政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み。

1.1 国内で策定されている制度やガイドライン等の概要

名称	政府機関等のサイバーセキュリティ対策のための統一基準群		
国・地域	日本	策定者	内閣サイバーセキュリティセンター
適用分野	政府機関等情報システム	遵守義務の有無	あり
対象者	- 政府機関 - 独立行政法人 等		
概要	- 政府統一基準は、サイバーセキュリティ基本法に基づく、<u>政府機関および独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み</u>。統一基準群には、以下の文書が含まれる。 ➤ 政府機関等のサイバーセキュリティ対策のための統一規範 ➤ 政府機関等のサイバーセキュリティ対策のための統一基準 ➤ 政府機関等の対策基準策定のためのガイドライン - 政府機関等のサイバーセキュリティ対策のための統一規範は、<u>機関等がとるべき対策の統一的な枠組み</u>を定めたもの。 - 政府機関等のサイバーセキュリティ対策のための統一基準は、<u>情報セキュリティ対策の項目ごとに機関等が遵守すべき事項(遵守事項)を規定</u>することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的としたもの - 政府機関等の対策基準策定のためのガイドラインは、<u>統一基準の遵守事項を満たすためにとるべき基本的な対策事項(基本対策事項)の例示</u>とともに、<u>対策基準の策定及び実施に際しての考え方等を解説</u>したもの		
普及状況	(義務のため全ての政府機関等情報システムに対し遵守)		
URL	https://www.nisc.go.jp/policy/group/general/kijun.html		

政府機関等のサイバーセキュリティ対策のための統一基準群

- 政府統一基準群は、統一規範や統一基準、対策基準策定ガイドラインからなる。
- 統一基準適用個別マニュアル群は、機関等において具体的な運用規程等を定めるときや個別の情報システムのセキュリティ要件等を検討するとき等に利用される。



重要インフラのサイバーセキュリティに係る行動計画

- サイバーセキュリティ基本法に基づき策定された重要インフラのサイバーセキュリティに係る行動計画は、①「重要インフラ防護」の目的、②関係主体の責務、③基本的な考え方、④障害対応体制の強化に向けた取組等を規定している。

1.1 国内で策定されている制度やガイドライン等の概要

名称	重要インフラのサイバーセキュリティに係る行動計画		
国・地域	日本	策定者	内閣サイバーセキュリティセンター
適用分野	重要インフラ分野	遵守義務の有無	なし
対象者	- 政府機関 - 重要インフラ事業者 - サプライチェーン等に関わる事業者		
概要	- 重要インフラ行動計画は、<u>サイバーセキュリティ基本法第12条</u>の規定に基づき策定する<u>サイバーセキュリティ戦略を踏まえ</u>、同法第4条(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)及び第26条第1項第5号(サイバーセキュリティ戦略本部の所掌事務)<u>の規定に基づき策定するもの</u>。 - 重要インフラ行動計画では、<u>①「重要インフラ防護」の目的</u>、<u>②関係主体の責務</u>、<u>③基本的な考え方</u>、<u>④障害対応体制の強化に向けた取組</u>等を規定している。		
普及状況	-		
URL	https://www.nisc.go.jp/policy/group/infra/index.html		

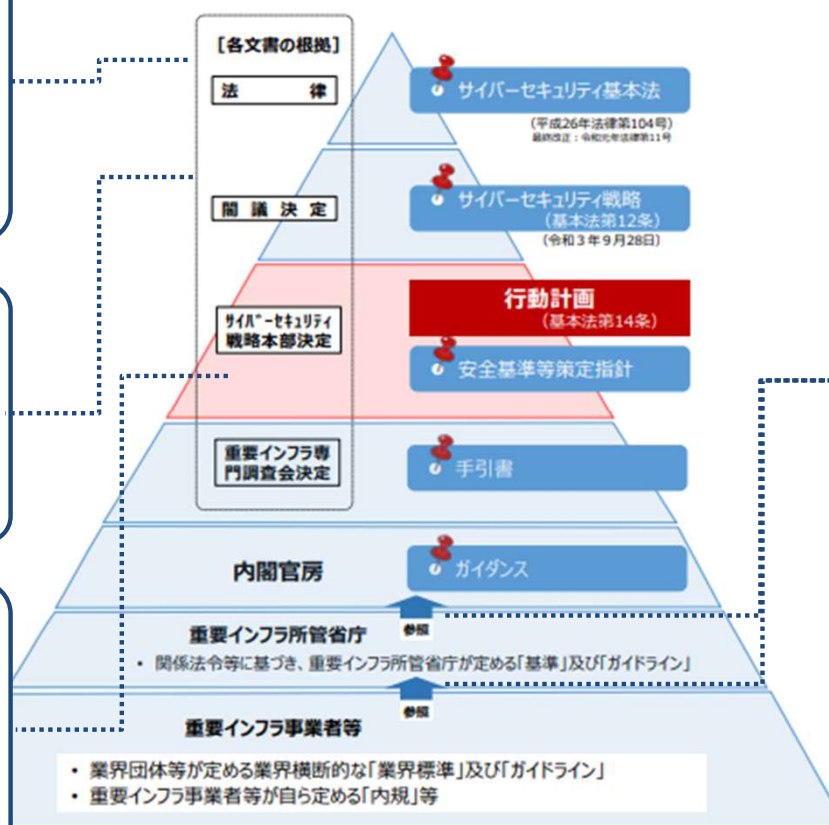
重要インフラのサイバーセキュリティに係る行動計画

- 重要インフラのサイバーセキュリティに係る行動計画に基づき、安全基準等策定指針が定められている。
- 安全基準等策定指針を参考としつつも、各所管省庁や重要インフラ事業者等によって策定されるガイドライン等における対策の項目等は各分野や重要インフラ事業者等に委ねられている。

[サイバーセキュリティ基本法第12条]
政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。

[サイバーセキュリティ戦略]
この戦略は、サイバーセキュリティ基本法第12条第5項において準用する同条第4項の規定に基づき、国会に報告するものである。

[行動計画]
行動計画は、サイバーセキュリティ基本法第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条及び第26条第1項第5号の規定に基づき策定するものである。



本指針に記載されている対策の項目及び当該項目の水
準等に関して、どの「安全基
準等」に定めるかということにつ
いては、各重要インフラ分野
の関係法令の規定及び既存
の「安全基準等」の構成等を
踏まえ、重要インフラ分野又
は重要インフラ事業者等ごと
に検討することが期待される。
(安全基準等策定指針 3.
指針の位置付けより)

重要インフラのサイバーセキュリティに係る安全基準等策定指針

- 重要インフラのサイバーセキュリティに係る安全基準等策定指針では、「安全基準等」において規定が望まれる項目を整理・記載している。
- また、かかる文書に基づき、業界ごとに安全基準が定められている。

1.1 国内で策定されている制度やガイドライン等の概要

名称	重要インフラのサイバーセキュリティに係る安全基準等策定指針		
国・地域	日本	策定者	内閣サイバーセキュリティセンター
適用分野	重要インフラ分野	遵守義務の有無	なし
対象者	重要インフラ事業者等		
概要	「重要インフラのサイバーセキュリティに係る安全基準等策定指針」は、重要インフラ行動計画に示された重要インフラにおける機能保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、<u>「安全基準等」において規定が望まれる項目を整理・記載</u>している。 - 本文書に基づき、例えば各業界ごとに以下の文書が公開されている。 ✓ 電気通信分野におけるサイバーセキュリティに係る安全基準(第1版)[電気通信事業者協会] ✓ 金融機関等コンピュータシステムの安全対策基準・解説書(第11版)[金融情報システムセンター] ✓ 航空分野における情報セキュリティ確保に係る安全ガイドライン(第6版) [国土交通省] ✓ 空港分野における情報セキュリティ確保に係る安全ガイドライン(第3版) [国土交通省] ✓ 鉄道分野における情報セキュリティ確保に係る安全ガイドライン(第5版) [国土交通省] 等		
普及状況	セキュリティ対策の実施状況は多くの項目において高い水準で推移しており、安全基準等は浸透しつつあるとされている*1		
URL	https://www.nisc.go.jp/policy/group/infra/index.html		

*1 重要インフラにおける安全基準等の浸透状況に関する調査について[2022年度]より

重要インフラのサイバーセキュリティに係る安全基準等策定指針

- 重要インフラのサイバーセキュリティに係る安全基準等策定指針では、「安全基準等」を4つに分類している。
- 電気通信分野のように、所管省庁ではなく事業者(団体を含む)にその策定や管理等が移管されている場合がある。

「安全基準等」の分類

分類	文書の種類
分類①	関係法令に基づき国が定める「 <u>強制基準</u> 」
分類②	関係法令に準じて国が定める「 <u>推奨基準</u> 」及び「 <u>ガイドライン</u> 」 <例> - 航空分野における情報セキュリティ確保に係る安全ガイドライン(第6版) - 空港分野における情報セキュリティ確保に係る安全ガイドライン(第3版) - 鉄道分野における情報セキュリティ確保に係る安全ガイドライン(第5版)
分類③	関係法令や国民からの期待に応えるべく業界団体等が定める「 <u>業界横断的な業界標準</u> 」及び「 <u>ガイドライン</u> 」 <例> 電気通信分野におけるサイバーセキュリティに係る安全基準
分類④	関係法令や国民・利用者等からの期待に応えるべく「 <u>重要インフラ事業者等が自ら定める「内規」等</u> 」

金融機関等コンピュータシステムの安全対策基準・解説書(第12版)

- 本ガイドラインは、日本の金融機関等が金融情報システムの開発や導入、運用等において必要と考えられる安全対策を基準として示すとともに、基準項目ごとに、具体的な事例を交えて解説するもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	金融機関等コンピュータシステムの安全対策基準・解説書(第12版)		
国・地域	日本	策定者	金融情報センター(FISC)
適用分野	金融情報システム	遵守義務の有無	なし ^{*1}
対象者	金融機関 等		
概要	- 日本の金融機関等が、事業展開を行ううえで金融情報システムを活用するに際し、<u>開発や導入、運用等において必要と考えられる安全対策を基準として示す</u>とともに、<u>基準項目ごとに、具体的な事例を交えて解説するもの</u>。 - 安全対策基準は、統制基準、実務基準、設備基準、監査基準の4つからなる。 - 本文書では、金融機関等がリスク特性に応じた安全対策の目標を定めるに当たり、<u>不確実性を低減させることを目的に、「基礎基準」を設定している</u>。一方で、「基礎基準」以外の基準は、リスク特性に応じて<u>選択・追加する「付加基準」</u>としている。基礎基準は、特定システム・通常システムによらず、金融情報システムが最低限適用する基準とされている。 - 銀行法施行規則(13条の7)に基づき策定された「主要行等向けの総合的な監督指針」(III-3-7 システムリスク)ではサイバーセキュリティ管理態勢の整備が求めている^{*2}が、本ガイドラインについて言及は行われていない。 - ただし、<u>「金融検査マニュアル(預金等受入金融機関に係る検査マニュアル)」^{*3}</u>において、検査官は、システムリスク管理態勢に問題点が見られ、さらに 深く業務の具体的検証をすることが必要と認められる場合には、本ガイドライン等に基づき確認することになっている。金融検査マニュアルは令和元年に廃止されているが、<u>預金等受入金融機関にとって本ガイドラインが実質的な義務となっている可能性がある</u>。		
普及状況	金融機関が情報システムを構築する際の安全対策基準として、事実上の標準ガイドラインと指摘されている ^{*4}		
URL	https://www.fisc.or.jp/publication/book/006241.php		

^{*1} あくまでも自主基準とされており強制力はないとされている。(P23)https://www.fsa.go.jp/singi/singi_kinyu/kessai_sg/siryoyou/20141208/03.pdf

^{*2} NISC「重要インフラにおける安全基準等の継続的改善状況等に関する調査について2022年度」<https://www.nisc.go.jp/pdf/council/cs/ciip/dai33/33shiryoyou02.pdf>

^{*3} 金融庁「金融検査マニュアル(預金等受入金融機関に係る検査マニュアル)」参照。ただし、本マニュアルは令和元年に廃止。
<https://www.fsa.go.jp/manual/manualj/yokin.pdf>

^{*4} 富士通「金融機関が情報システムを構築する際の安全対策基準「FISC安全対策基準」とは？」
<https://pfs.nifcloud.com/navi/beginner/fisc.htm>

金融機関等コンピュータシステムの安全対策基準・解説書(第12版)

- 社会性、公共性を有している金融機関等では、重大な外部性や情報の機微性を考慮して安全対策を実施すべきとしている。

安全対策において金融機関が考慮すべきとされる事項

- 金融機関等は、社会性・公共性を有していることから、リスクの顕在化による影響が、個別金融機関等による統制可能な範囲を超えて外部に及ぶ事態(以下、「外部性を有する」という。)や、機微情報(要配慮個人情報を含む)の流出により、プライバシーなど個人の人権が侵害される事態(以下、「機微性を有する」という。)を考慮に入れるべきである。

「重大な外部性」の考え方

- 「外部性」とは、個別金融機関等におけるシステム障害等によって、個別金融機関等のみならず、他の金融機関等やその顧客に影響を与える可能性のある性質をいう(例:為替や預金等を取り扱うシステム)。
- リスクベースアプローチに従って、適切にITガバナンスを発揮できる金融機関等であっても、「外部性を有する」情報システムに関する影響や損害額等を正確には把握できない。特に、「重大な外部性を有する」システムの障害等に伴う影響を正確に把握し、障害を防止するためのコストを事前に算定・内部化して、安全対策の立案に的確に反映させることは困難である。
- こうしたことから、金融機関等では「重大な外部性を有する」システムには、「高い安全対策」を適用することが必要となる。

<金融分野における外部性について>

金融機関等における為替や預金等を取り扱うシステムは、深刻なシステム障害が発生した場合、他の金融機関等やその顧客に対し広く影響を及ぼし、社会全体に経済的損失を与える「重大な外部性」を有する。

「情報の機微性」の考え方

- 個人情報については、個人情報保護法等のフレームワークがあり、金融機関等がシステムの安全対策を講ずる際に、これらを遵守する必要がある。
- 金融機関等が取り扱う個人情報は多種多様で、住所や氏名等の情報から、病歴等の極めて機微にわたるものまである。こうした機微性を有する情報に関しては、一般の個人情報と区別せず取り扱うことは適当でない。しかし、一般の個人情報が「機微情報(要配慮個人情報を含む)」と同一に扱われた場合、金融機関等のほとんどのシステムに存在している一般の個人情報に対し、適切な水準を超えた安全対策の目標が設定され、資源の過剰配分が行われるおそれがある。
- このような事態を避けるために、金融機関等は、個人情報を「機微情報(要配慮個人情報を含む)」と一般の個人情報に分け、「機微情報(要配慮個人情報を含む)」については、「重大な外部性を有する」システムと同様、「高い安全対策」を適用し、一般の個人情報では、そのリスク特性に応じて必要かつ適切な安全対策を実施することが必要となる。

電気通信分野におけるサイバーセキュリティに係る安全基準

- 本ガイドラインは、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準について業界団体が定めるガイドラインを、政府指針に基づき策定したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	電気通信分野におけるサイバーセキュリティに係る安全基準		
国・地域	日本	策定者	電気通信事業者協会
適用分野	電気通信分野	遵守義務の有無	なし
対象者	- 電気通信事業者 - 電気通信設備提供者(メーカ等)		
概要	- 本ガイドラインは、電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、<u>取り組むことが望ましいと考えられる情報セキュリティ対策の基準について業界団体が定めるガイドラインを、政府指針に基づき策定したもの。</u> - 本ガイドラインで規定する内容は、<u>対象とする事業者等に対し情報セキュリティ対策の強化に向けて推奨される取り組み内容を示した</u>ものであり、事業者等の具体的な取り組みにより、情報セキュリティレベルを向上させていくことが肝要とされている。		
普及状況	-*1		
URL	https://www.tca.or.jp/information/anshinkyou.html		

*1 2023/8の公開から調査時点(2024/6/3)まで1年経過しておらず、管見の限り、普及状況は確認ができなかった。。

[参考]電気通信分野におけるサイバーセキュリティに係る安全基準(第1版)

- 電気通信事業者協会の安全基準検討ワーキンググループでは、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」に基づき、「電気通信分野におけるサイバーセキュリティに係る安全基準(第1版)」を作成している。

電気通信分野における安全基準検討ワーキンググループ

分類	説明
取組内容	- 電気通信事業者協会内にワーキンググループを設置。 - 情報セキュリティ戦略本部(議長:内閣官房長官)における「重要インフラのサイバーセキュリティに係る安全基準等策定指針」に基づき、電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、<u>取り組むことが望ましいと考えられるサイバーセキュリティ対策の基準について専門的に検討を行う。</u>
成果物(例)	「電気通信分野におけるサイバーセキュリティに係る安全基準」(2023年8月31日)
参加企業	- 日本電信電話株式会社 - KDDI株式会社 - スカパーJSAT株式会社 - 株式会社オプテージ - 東京テレメッセージ株式会社 - 中部テレコミュニケーション株式会社 - ソフトバンク株式会社 - 株式会社NTTドコモ - 近鉄ケーブルネットワーク株式会社 - JCOM株式会社 - 東日本電信電話株式会社 - 西日本電信電話株式会社 - NTTコミュニケーションズ株式会社 - UQコミュニケーションズ株式会社 - 楽天モバイル株式会社

電気通信分野におけるサイバーセキュリティに係る安全基準

- 電気通信分野におけるサイバーセキュリティに係る安全基準では、電気通信事業において顕在化する可能性が高く、また、サービスの安全かつ持続的な提供への影響が大きいと思われる脅威の対策を具体化。

	共通 (一般的対策)	サイバー攻撃 (DDoS攻撃等)	ネットワーク輻そう (企画型輻そう、 災害型輻そう)	故障・災害等	重要情報漏えい (設備情報等)	クラウドサービスの 対策
組織統治におけるサイバーセキュリティ対策		○	<u>電気通信事業において顕在化する可能性が高く、また、サービスの安全かつ持続的な提供への影響が大きいと思われる脅威</u> ((1) サイバー攻撃、(2)ネットワーク輻そう、(3)故障・災害等、(4)重要情報漏えい) 毎に <u>固有の情報セキュリティ対策</u> を記述			
リスクマネジメントの活用と危機管理対策	○					
組織的対策	○	○	○	○	○	
人的対策	○					
物理的対策	○			○		
技術的対策	○	○	○		○	
クラウドサービスのセキュリティ対策						○
ランサムウェア対策	○					
重要インフラサービス障害の観点から見た事業継続性確保のための対策	○	○	○	○	○	
外部委託における情報セキュリティ確保のための対策	○				○	

電力制御システムセキュリティガイドライン

- 本ガイドラインは、電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	電力制御システムセキュリティガイドライン		
国・地域	日本	策定者	日本電気協会
適用分野	電力制御システムや電力制御用ネットワーク	遵守義務の有無	あり (本ガイドラインは勧告的事項と推奨的事項を定めているが、「審査基準」として位置付けられている「技術基準の解釈」によって引用されているため、実質的には義務となっている。)
対象者	電気事業者が施設する電力制御システム等に携わる者		
概要	- 本ガイドラインは、<u>電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載</u>したもの。 - 本ガイドラインでは、求められる水準に応じて条ごとに「<u>勧告的事項</u>」及び「<u>推奨的事項</u>」を定める。 ✓ 勧告的事項:電力制御システムに関する想定脅威に対して、電気事業者が実施すべき場合に使用 ✓ 推奨的事項:電力制御システムに関する想定脅威に対して、実施の要否及び実施方法を判断する場合に使用 - 本ガイドラインは、<u>JIS Q 27001:2014、JIS Q 27002:2014をベースとし</u>、電力制御システムの利用環境を踏まえた内容として電力の保安と運用を考慮して制定された。		
普及状況	-		
URL	https://www.jea-chugoku.jp/store/products/detail/192		

電力制御システムセキュリティガイドライン

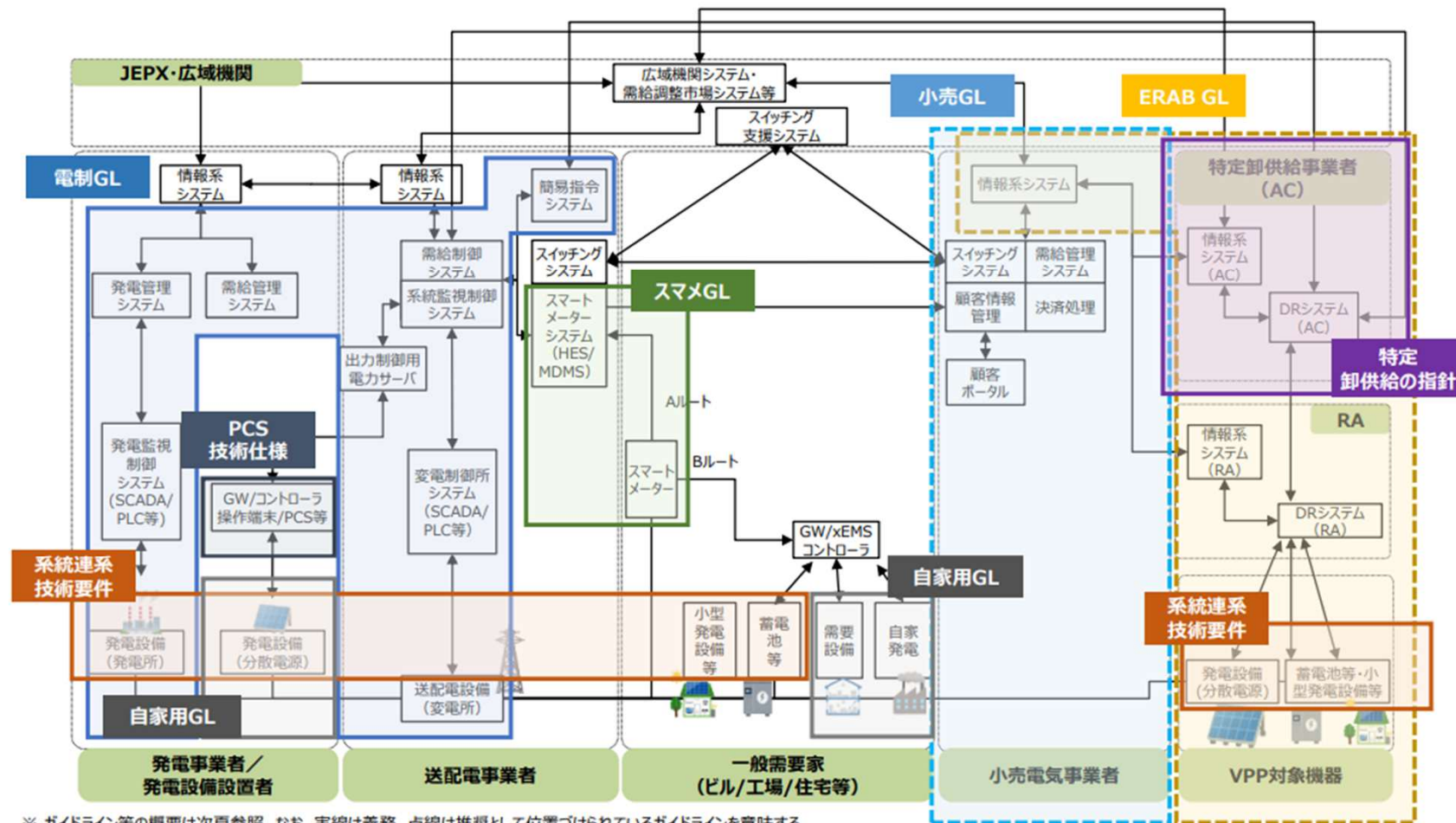
- 電気事業法や各技術基準を定める省令に基づく技術基準の解釈によって具体的な規定がなされた。
- 技術基準を定める省令により、民間機関が策定した規格も技術基準の解釈において引用可能となった。

種別	対象
制度	電気事業法
	公共の安全確保、電気の安定供給の観点から電気工作物の設計、工事及び維持に関して遵守すべき基準として、<u>電気設備や原子力設備など7つの分野の技術基準を定める</u>。
	発電用水力設備、発電用火力設備、電気設備、発電用風力設備の技術基準を定める省令 <u>保安上達成すべき目標、性能のみを規定する基準</u>を定める。
基準	技術基準の解釈
	- 技術基準を定める省令では目標や達成すべき性能のみが示されたため、<u>具体的な資機材、施行方法等の規定は基準基準の解釈に委ねられた</u>。 - 電気事業法に基づく保安確保上の行政処分を行う場合の具体的な内容を示す「<u>審査基準</u>」として<u>位置付けられている</u>。
ガイド ライン	電力制御システムセキュリティガイドライン
	本ガイドラインは、電力制御システム等のサイバーセキュリティ確保を目的として、<u>電気事業者が実施すべきセキュリティ対策の要求事項について記載したもの</u>。
	スマートメーターシステムセキュリティガイドライン
	本ガイドラインは、スマートメーターシステムのセキュリティ確保を目的として、<u>一般送配電事業者が実施すべきセキュリティ対策の要求事項について記載したもの</u>。

公正、公平な民間の機関で制定・承認された規格であれば、「電気事業法」の「技術基準への解釈」等への引用が可能^{*1}となった。

電力制御システムセキュリティガイドライン

- 電力制御システムガイドラインの他に、「スマートメーターシステムセキュリティガイドライン」、「系統連系技術要件」、「出力制御機能付きPCSの技術仕様」、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン(内規)」等への対応が電力システムに関するプレーヤーには求められている。



自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン

- 本ガイドラインは、自家用電気工作物の遠隔監視システム等や制御システム等のライフサイクルにおけるサイバーセキュリティについて規定したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）		
国・地域	日本	策定者	経済産業省
適用分野	電力分野(自家用電気工作物* ¹ の遠隔監視システム等、制御システム等)	遵守義務の有無	あり* ²
対象者	自家用電気工作物を設置する者		
概要	- 本ガイドラインは、<u>自家用電気工作物の遠隔監視システム等や制御システム等のライフサイクルにおけるサイバーセキュリティについて規定</u>したもの。 - 本ガイドラインにおいては、<u>求められるセキュリティ水準に応じて、義務に該当する「勧告的事項」と義務に該当しない「推奨的事項」を示す。</u> ✓ 勧告的事項：遠隔監視システム等、制御システム等に関する想定脅威に対して、設置者等が実施すべきこと ✓ 推奨的事項：遠隔監視システム等、制御システム等に関する想定脅威に対して、設置者等が実施の要否及び実施方法を判断すべきこと		
普及状況	-		
URL	https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/06/20220610-04.pdf		

*1 発電事業の用に供するものを除く

*2 勧告的事項に該当する場合は遵守義務があるが、推奨的事項の場合には遵守義務はない。

自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン

- 本ガイドラインの新たな制定に伴い、関連省令や基準、ガイドラインも併せて変更されている。
- 電気設備の技術基準の解釈(改正)において、本ガイドラインの位置づけがなされている。

種別	対象
制度	電気設備に関する技術基準を定める省令（改正） （サイバーセキュリティの確保） 第15条の2 事業用電気工作物の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、又は物件に損傷を与えるおそれ及び一般送配電事業又は配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。
基準	電気設備の技術基準の解釈（改正） 【サイバーセキュリティ対策】（省令第15条の2） 第37条の2 省令第15条の2に規定するサイバーセキュリティの確保は、次の各号によること。 一・二 （略） 三 自家用電気工作物（発電事業の用に供するものを除く。）に係る遠隔監視システム及び制御システムにおいては、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」（20220530保局第1号 令和4年6月10日）によること。 （略） 附 則（20220530保局第1号） 1 この規程は、令和4年10月1日から施行する。 2 この規程の施行の際現に設置され、又は設置のための工事に着手している電気工作物についてのこの規程による改正後の電気設備の技術基準の解釈第37条の2第3号の適用については、この規程の施行後最初に行う変更の工事が完成するまでの間は、なお従前の例によることができる。
ガイドライン	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規） 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）（新規制定） 電気設備の技術基準の解釈（20140215商局第4号）第37条の2第3号及び電気事業法施行規則第50条第3項第9号の解釈適用に当たっての考え方（内規）（令和4年6月10日付け20220530保局第1号）の規定に基づき、自家用電気工作物に係るサイバーセキュリティの確保のため、別紙のとおり定める。 電気事業法施行規則第50条第3項第9号の解釈適用に当たっての考え方（内規） 施行規則第50条（保安規程） 第3項第9号（その他保安上必要な事項） その他事業用電気工作物の工事、維持及び運用に関する保安に関し必要な事項

地方公共団体における情報セキュリティポリシーに関するガイドライン

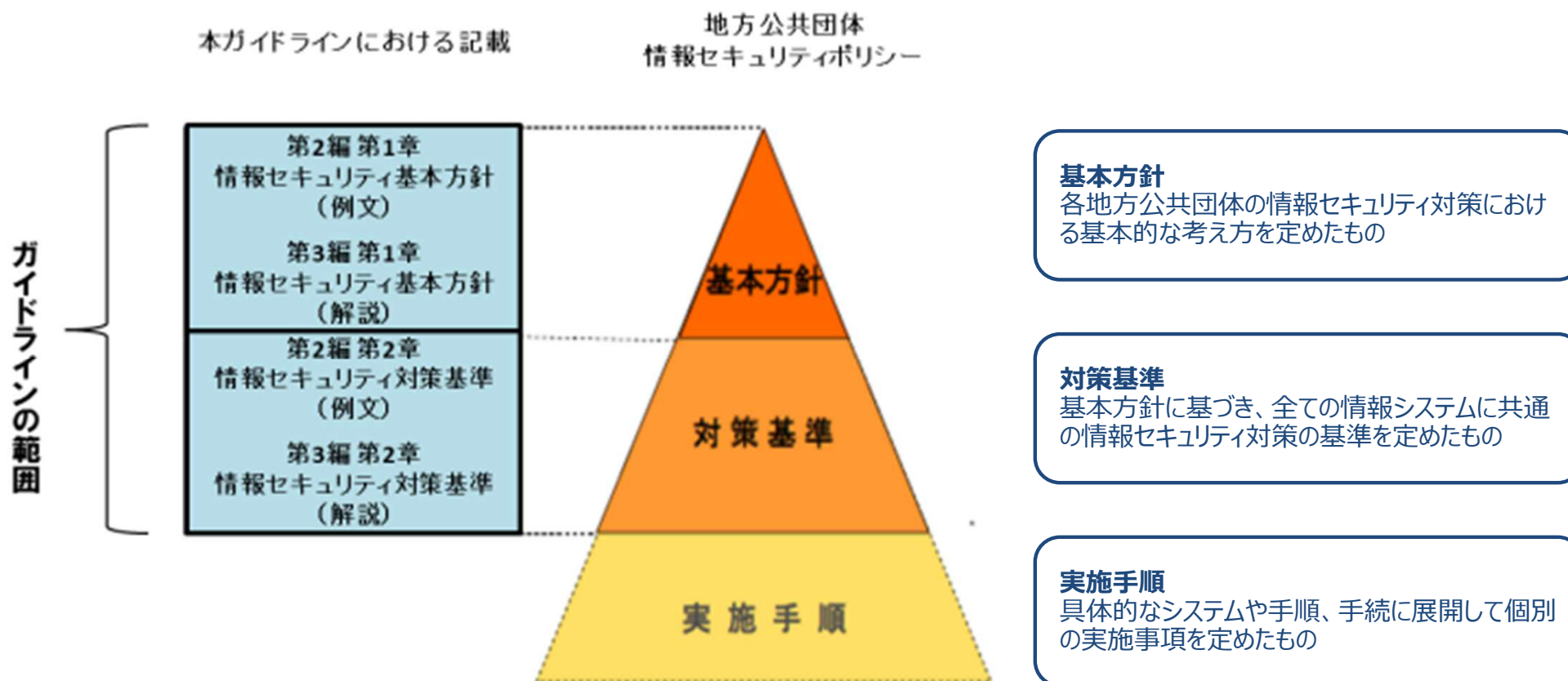
- 本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	地方公共団体における情報セキュリティポリシーに関するガイドライン		
国・地域	日本	策定者	総務省
適用分野	地方公共団体	遵守義務の有無	あり(ポリシーの策定については義務であるが、ガイドラインに記載された具体的な項目の記載は必ずしも義務ではない。また、総務大臣通知による要請によって、対策の実施が義務となる場合がある。)
対象者	- 情報セキュリティポリシーの策定を行う者 - セキュリティ上の職責を担う者		
概要	- 本ガイドラインは、<u>各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説</u>したもの。 - 本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げない。 - 情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、地方公共団体の長をはじめ、全ての職員等及び委託事業者は、業務の遂行に当たって策定した情報セキュリティポリシーを遵守する義務を負う。		
普及状況	-		
URL	https://www.soumu.go.jp/main_content/000805453.pdf		

地方公共団体における情報セキュリティポリシーに関するガイドライン

- 本ガイドラインは、以下を対象範囲とする。
 - ✓ 各地方公共団体の情報セキュリティ対策における基本的な考え方を定めた基本方針
 - ✓ 全ての情報システムに共通の情報セキュリティ対策の基準を定めた対策基準



地方公共団体における情報セキュリティポリシーに関するガイドライン

- 地方自治法に基づき「地方公共団体における情報セキュリティポリシーに関するガイドライン」が策定。
- また、総務省大臣通達による要請が実質的な義務となる場合がある。

種別	対象
制度	地方自治法 地方自治法の一部を改正する法律案 (サイバーセキュリティを確保するための方針等) 第246条の6 <u>普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たつてのサイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない。</u> 総務省大臣通達 <例:新たな自治体情報セキュリティ対策の抜本的強化について> <u>各地方自治体におかれては、三層からなる対策を講じていただくこと</u>により、情報セキュリティ対策の抜本的強化に取り組まれますようお願いいたします。特に、都道府県におかれては、自らの情報セキュリティ対策の充実を図られるとともに、「自治体情報セキュリティクラウド」の構築をはじめ、<u>貴都道府県内市区町村における必要な情報セキュリティ水準の確保のための支援にも努めていただきますようお願いいたします。</u>
基準	地方公共団体における情報セキュリティポリシーに関するガイドライン 本ガイドラインは、<u>各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。</u> 本ガイドラインで記述した構成や例文は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げない。

医療情報システムの安全管理に関するガイドライン

- 本ガイドラインは、医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(e-文書法)等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	医療情報システムの安全管理に関するガイドライン 第6.0版		
国・地域	日本	策定者	厚生労働省
適用分野	医療情報システム ^{*1}	遵守義務の有無	あり ^{*2}
対象者	医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象		
概要	- 本ガイドラインは、<u>医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(e-文書法)等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。</u> 2023年5月に公表された第6.0版では、本ガイドラインの内容の理解を促進し、医療情報システムの安全管理の実効性を高める観点から、<u>本文を以下の通り分け、各編で想定する読者に求められる遵守事項及びその考え方を示す</u>とともに、Q&A等で現状選択可能な具体的技術にも言及するかたちとすべく、構成の見直しを行った。 ✓ 概説編(Overview) ✓ 経営管理編(Governance) ✓ 企画管理編(Management) ✓ システム運用編(Control) - 本ガイドラインに記載されている内容のうち、優先的に取り組むべき事項をチェックリスト^{*3}に規定。		
普及状況	-		
URL	https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html		

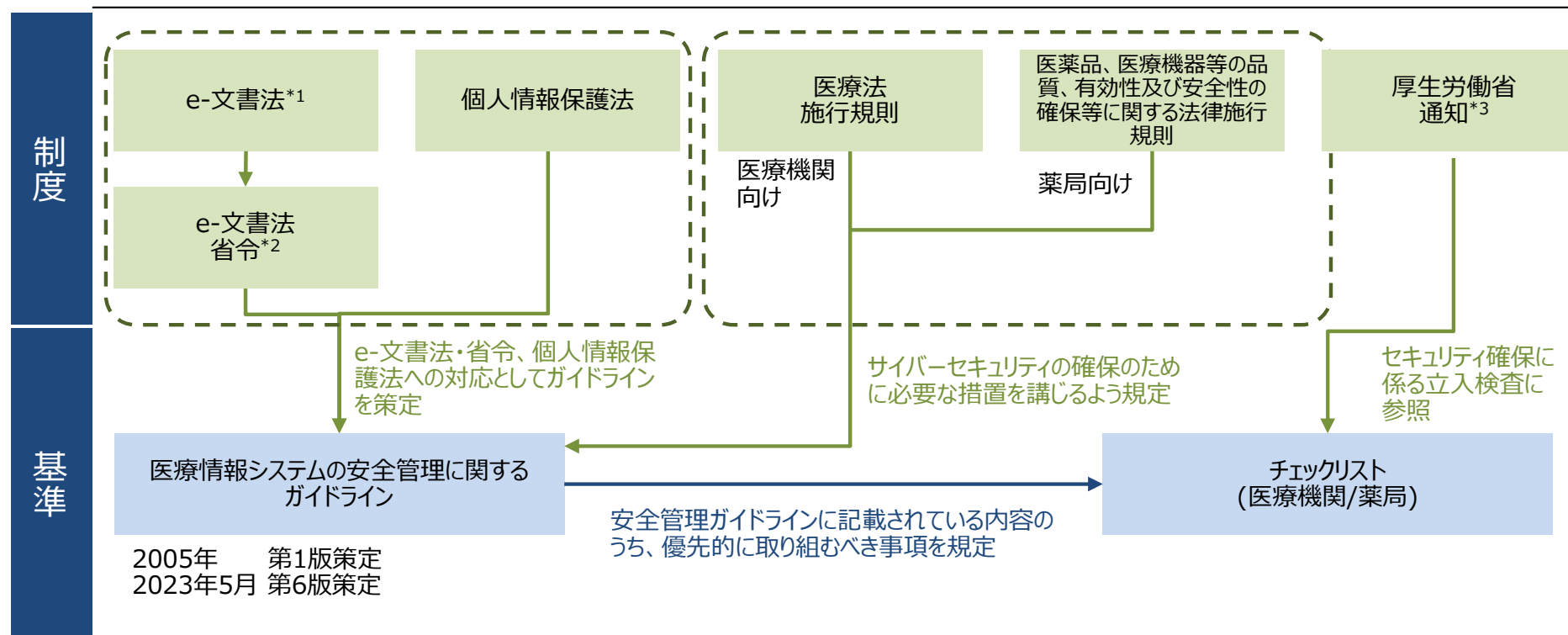
*1 本ガイドラインが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定

*2 本ガイドラインにおいて優先的に取り組むべき事項を整理したチェックリストは立入検査の際に参照されるため、実質的に義務となっている可能性がある。

*3 「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「薬局におけるサイバーセキュリティ対策チェックリスト」を指す。

医療情報システムの安全管理に関するガイドライン

- 本ガイドラインは、e-文書法・省令や個人情報保護法へ対応するために策定された。
- また、本ガイドラインにおいて優先的に取り組むべき事項を整理したチェックリストは立入検査の際に参照されるため、実質的に義務となっている可能性。



[凡例] 認証制度 法律・省令・通知 標準・チェックリスト

*1 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律

*2 厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令

*3 厚生労働省医政局特定医薬品開発支援・医療情報担当参事官通知 医療関係は医政参発0609第1号 薬局は医政参発1013第1号

[参考] 厚生労働省「医療情報システムの安全管理に関するガイドライン第6.0版」

<https://www.mhlw.go.jp/content/10808000/001102570.pdf>

厚生労働省「「薬局におけるサイバーセキュリティ対策チェックリスト」及び「薬局におけるサイバーセキュリティ対策チェックリストマニュアル～薬局・事業者向け～」等について」

<https://www.city.kobe.lg.jp/documents/60037/iryoukikanniokerusaiba-sekyurityityekuridutooyobimanyuaru.pdf>

厚生労働省「「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」について」

<https://www.mhlw.go.jp/content/001157681.pdf>

厚生労働省「安全管理ガイドラインの改定の経緯に関する年表」

<https://www.mhlw.go.jp/content/10808000/001102585.pdf>

水道分野における情報セキュリティガイドライン

- 本ガイドラインは、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	水道分野における情報セキュリティガイドライン(第4版)		
国・地域	日本	策定者	厚生労働省 (国土交通省へ移管)
適用分野	水道情報システム	遵守義務の有無	なし
対象者	- 水道事業者 - 水道用水供給事業者		
概要	- 本ガイドラインは、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示した<u>もの</u>として、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第5版)」における「安全基準等」に位置づけられるもの。また、策定にあたって、「重要インフラの情報セキュリティ対策に係る第4次行動計画」を参考としている。 - 実施すべき対策については、各水道事業等の規模(給水量、人員、財政状況)や地域水道ビジョン等における水道として目指す目標レベルに応じて、各水道事業者等が実現レベル、実現方法を決定するものとし、<u>ガイドラインに示すとおり</u>に実施することを強制しないとされている。 - 特に小規模の水道事業者等においては、その帰属する地方公共団体が運用する情報セキュリティの対策により包括的に対応すること等も含めてセキュリティ確保に努めることにより、水道事業者等による独自のセキュリティ対策組織等は簡素化できる可能性があるとしている。 - 情報セキュリティ対策の項目及び水準のうち、以下が定められている。 ✓ 最低限実施すべき取組 ✓ できる限り実施することが望ましい取組		
普及状況	-		
URL	https://www.mlit.go.jp/common/830005109.pdf		

水道分野における情報セキュリティガイドライン

- ガイドラインは、事業者に対する義務を示すものではないが、厚生労働省通知において、サイバーセキュリティの確保に必要な措置を示しており、これらの対策を講じるためにガイドラインが参考となる可能性がある。

種別	対象
制度	水道施設の技術的基準を定める省令 第1条第11の2項(新設) 施設の運転を管理する電子計算機が水の供給に著しい支障を及ぼすおそれがないように、サイバーセキュリティ(サイバーセキュリティ基本法第2条に規定するサイバーセキュリティをいう。)を確保するために必要な措置が講じられていること。
基準	厚生労働省医薬・生活衛生局水道課長 通知 水道施設の技術的基準を定める省令の一部を改正する省令が令和元年9月30日に公布され、令和2年4月1日から施行される予定である。これに伴う改正の趣旨、改正の内容及び <u>留意事項は下記のとおりであるので、御了知の上、その施行に遺漏なきよう期されたい</u> 。なお、本通知は、地方自治法第245条の4第1項の規定に基づく技術的助言である旨申し添える。 第3 <u>留意事項</u> 2 制御系システムに使用されている電子計算機について、 <u>次の措置が講じられていること</u> 。 - 電子計算機へアクセスする者について主体認証を行うことができる機能を有すること。 - 不正プログラム対策として、アンチウイルスソフトウェアが導入され、常に最新の状態が保たれていること。また、自動検査機能が有効となっていること。 - セキュリティ更新プログラムの提供等のサポートが終了したオペレーティングシステム(OS)が使用されていないこと(外部ネットワークからの分離、USBメモリ等の外部記憶媒体からの感染防止対策等、不正プログラムの進入を防ぐ措置が講じられている場合はこの限りではない)。 - 電子計算機は、障壁、施錠等により他の区域から隔離され、人の入退出を管理することができる場所に設置すること。可搬性のある電子計算機(モバイルパソコン、携帯端末等)についてはこの限りではないが、施錠できる保管庫で保管すること、常に携帯することなど、盗難等のおそれがないよう適切に管理すること
ガイドライン	水道分野における情報セキュリティガイドライン(第4版) <u>本ガイドラインは、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示す。</u> 実施すべき対策については、各水道事業等の規模(給水量、人員、財政状況)や地域水道ビジョン等における水道として目指す目標レベルに応じて、各水道事業者等が実現レベル、実現方法を決定するものとし、 <u>ガイドラインに示すとおりを実施することを強制しない。</u>

物流分野における情報セキュリティ確保に係る安全ガイドライン

- 本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	物流分野における情報セキュリティ確保に係る安全ガイドライン		
国・地域	日本	策定者	国土交通省
適用分野	物流情報システム(「集配管理システム」、「倉庫管理システム」、「貨物追跡システム」等)	遵守義務の有無	なし
対象者	物流分野の重要インフラ事業者等		
概要	- 本ガイドラインは、セキュリティ管理策の水準を示すことで、個々の重要インフラ事業者等が、<u>重要インフラの担い手としての意識に基づいて自主的に取り組み、対策の実施や検証に当たっての目標を定めることを目的</u>とする。 ✓ 物流分野(貨物自動車運送)における情報セキュリティ確保に係る安全ガイドライン ✓ 物流分野(倉庫)における情報セキュリティ確保に係る安全ガイドライン 「重要インフラのサイバーセキュリティに係る安全基準等策定指針」が示す「安全基準等」のうち、<u>本ガイドラインは関係法令に準じて国が定める「推奨基準」及び「ガイドライン」に該当</u>。国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、<u>重要インフラ事業者等が自らのセキュリティ管理策を実施する際に参考資料として活用すること</u>を想定している。 <u>「重要インフラのサイバーセキュリティに係る行動計画」に掲げる「対象となる重要インフラ事業者等と重要システム例」や「重要インフラサービスとサービス維持レベル」等の内容を踏まえ</u>、物流分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産が対象。		
普及状況	-		
URL	https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html		

クレジットカード・セキュリティガイドライン

- 本ガイドラインは、安全・安心なクレジットカード利用環境を整備するため、クレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	クレジットカード・セキュリティガイドライン		
国・地域	日本	策定者	クレジット取引セキュリティ対策協議会
適用分野	クレジットカード分野	遵守義務の有無	あり
対象者	- セキュリティ対策の実施主体である「加盟店」や「カード会社(イシューア・アクワイアラー)」、「決済代行業者等(4号事業者)」、「コード決済事業者等(5号事業者)」、「コード決済事業者等の委託会社(6号事業者)」、「加盟店向け決済システム提供事業者(7号事業者)」 - 上記の事業者が対策を実施するに際し協力等を行う「機器メーカー」、「ソリューションベンダ」、「情報処理センター」、「セキュリティ事業者」、「国際ブランド」、「業界団体」等		
概要	- 本ガイドラインは、安全・安心なクレジットカード利用環境を整備するため、<u>クレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。</u> - 本ガイドラインは、<u>割賦販売法に規定するセキュリティ対策義務の「実務上の指針」として位置づけられており</u>、ガイドラインに「指針対策」として掲げられている措置又はそれと同等以上の措置を適切に講じている場合には、割賦販売法で定めるセキュリティ対策の基準を満たしていると認められる。 - クレジット業界では「重要インフラのサイバーセキュリティに係る行動計画」に基づき、官民連携による重要インフラ防護を推進しており、具体的な取組としては、「クレジット CEPTOAR における情報セキュリティガイドライン」に基づき、重要インフラ事業者における安全基準等の整備・浸透、情報共有体制の強化等を図っている。<u>ただし、本ガイドラインが行動計画や安全基準を直接参照しているわけではない点に留意。</u>		
普及状況	-		
URL	https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_5.0_published.pdf https://www.meti.go.jp/press/2022/03/20230315001/20230315001.html		

クレジットカード・セキュリティガイドライン

- クレジットカードセキュリティガイドラインは、「割賦販売法(後払分野)に基づく監督の基本方針」によって、実務上の指針に定められている。

種別	対象
制度	割賦販売法 - 割賦販売等に係る取引の公正の確保、購入者等が受けることのある損害の防止等に必要な措置を講ずることにより、割賦販売等に係る取引の健全な発達を図るとともに、購入者等の利益を保護し、あわせて商品等の流通及び役務の提供を円滑にすることで、国民経済の発展に寄与することを目的としている。 - 経済産業省は、<u>割賦法に基づき信用購入あっせん業者に対する監督を適正に実施することを通じ</u>、当該業者の事業の健全かつ適切な運営を確保すること及び購入者等の利益保護を図り、商品等の流通及び役務の提供を円滑にし、安全かつ安心な決済手段としてのクレジット取引の健全な発達を促し、もって国民経済の発展に寄与することが求められている。
	割賦販売法(後払分野)に基づく監督の基本方針 - クレジットカード番号等の適切な管理に関しては、<u>法令においてはセキュリティ確保に不可欠な機能のみを定め</u>、その実現手段及び方法については、各事業者の創意工夫に基づく<u>多様な手法に対してオープンなものとする「性能規定」の考えの下、クレジットカード番号等取扱業者に、必要かつ適切な措置を講ずることを求めている。</u> 「必要かつ適切な措置」については、最新の技術動向等を踏まえて毎年見直しが行われる「<u>クレジットカード・セキュリティガイドライン</u>」に掲げられる<u>措置が実務上の指針となるもの</u>であり、クレジットカード・セキュリティガイドラインに掲げる措置又はそれと同等以上の措置を講じている場合には「必要かつ適切な措置」が講じられているものと認められる。
基準	クレジットカード・セキュリティガイドライン【5.0 版】 本ガイドラインは、安全・安心なクレジットカード利用環境を整備するため、クレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者が実施するべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。
	クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画 - クレジット取引セキュリティ対策協議会は、2020年の東京オリンピック・パラリンピック競技大会に向けて、クレジットカード取引において「国際水準のセキュリティ環境」を整備することを目指してきた。 - クレジットカード取引に係わる各主体がそれぞれの役割に応じて取組むべき事項を「実行計画」として取りまとめ、2020年3月末を最終的な実施期限とし実現に向けた取組を推進。

[参考] クレジット取引セキュリティ対策協議会「クレジットカード取引等におけるセキュリティ対策の現状と 2020 年度以降の取組について」

https://www.j-credit.or.jp/security/pdf/efforts_main_2020.pdf

貴省「クレジットカード・セキュリティガイドライン【4.0版】が改訂されました」

<https://www.meti.go.jp/press/2022/03/20230315001/20230315001.html>

装備品等及び役務の調達における情報セキュリティ基準

- 本基準は、装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。

1.1 国内で策定されている制度やガイドライン等の概要

名称	装備品等及び役務の調達における情報セキュリティ基準		
国・地域	日本	策定者	防衛装備庁
適用分野	防衛分野	遵守義務の有無	あり(<u>防衛調達に関わる企業に対して遵守を義務付け</u>)
対象者	防衛関連企業において保護すべき情報に接する全ての者(保護すべき情報に接する役員(持分会社にあっては社員を含む。)、管理職員、派遣社員、契約社員、パート、アルバイト等を含む*1。)		
概要	- 本基準は、<u>装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。</u> <u>「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」における具体的な基準として、「装備品等及び役務の調達における情報セキュリティ基準」が参照されている。</u> - 防衛産業におけるサイバーセキュリティ体制の強化のための施策を一層促進するため、<u>先行する米国の取組</u>*2を参考に、<u>現行より厳格な管理策を盛り込んだ本基準が整備</u>された。特にNIST CSFの「検知」、「対応」、「復旧」に相当するサイバー攻撃に関し早期発見・対処のための措置を充実させている。		
普及状況	-		
URL	https://www.mod.go.jp/atla/cybersecurity/kijun_r05.pdf		

*1 この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。

*2 米国の取組として防衛装備庁のHPではNIST SP800-171が紹介されている。

<https://www.mod.go.jp/atla/cybersecurity.html>

装備品等及び役務の調達における情報セキュリティ基準

- 装備品等及び役務の調達における情報セキュリティ基準は、「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」に組み込まれており、調達に係る企業にとって当該基準への遵守が義務となっている。

種別	対象
制度	装備品等及び役務の調達における情報セキュリティの確保に関する特約条項 • 防衛省・自衛隊の調達を担当する外局である防衛装備庁が定めている本特約条項は、<u>防衛省・自衛隊と民間企業との契約に際して、情報セキュリティの確保のために付与される契約の1つ。</u> • 特約条項第2条「情報セキュリティ基本方針等」では、保護すべき情報を取り扱うに当たり、保護すべき情報を取り扱う調達に係る事業者の業務環境等を考慮の上、<u>別紙「装備品等及び役務の調達における情報セキュリティ基準」に従って、必要な措置をとらなくてはならないと定めている。</u>
基準	装備品等及び役務の調達における情報セキュリティ基準 • 本基準は、<u>装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めるもの。</u>
ガイドライン	装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ基準について • 装備品等及び役務の調達における情報セキュリティの確保について、<u>別添装備品等及び役務の調達における情報セキュリティ確保に関する特約条項、別紙「装備品等及び役務の調達における情報セキュリティ基準」の解説資料。</u> • 「装備品等及び役務の調達における情報セキュリティ基準」の規定、規定制定の解説等を記載。

[参考] 防衛装備庁「装備品等及び役務の調達における情報セキュリティの確保に関する特約条項」
https://www.mod.go.jp/j/budget/chotatsu/naikyoku/keiyakujoko/tokuyaku/07_20230522.pdf
防衛装備庁「装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ基準について」
https://www.mod.go.jp/atla/cybersecurity/kijun_kaisetsu01_r050712.pdf

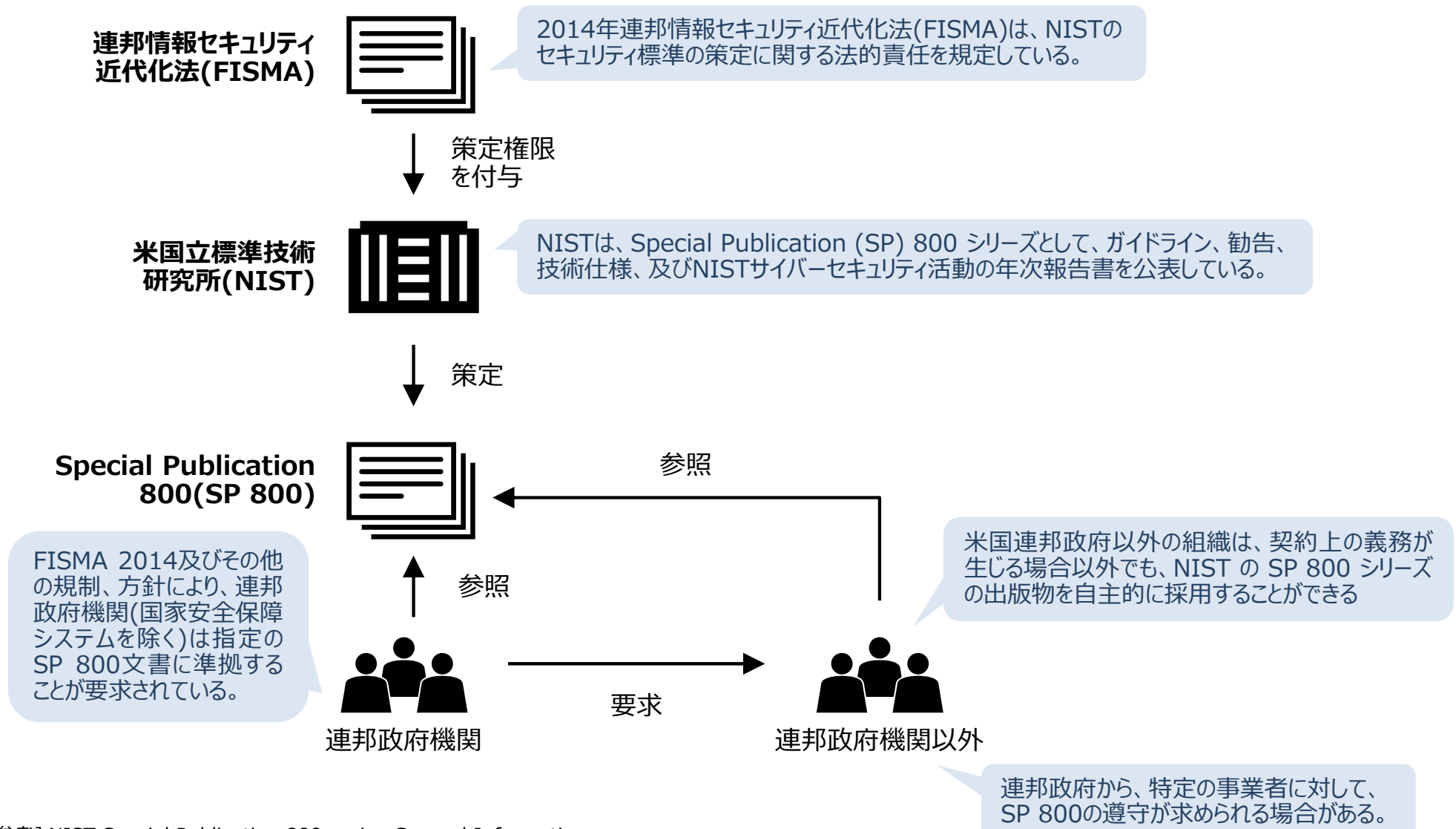
1.2 国外で策定されている制度やガイドライン等の概要



米国関連

NISTの標準策定権限の根拠と Special Publication 800 シリーズ

- Special Publication 800(SP 800)シリーズ文書は、連邦情報セキュリティ近代化法(FISMA)が付与する権限に基づいて米国立標準技術研究所(NIST)が策定するものであり、FISMA等により連邦政府機関での参照が義務化されている場合がある。



Special Publication 800 シリーズの概要

- Special Publication (SP) 800 シリーズは、SP 800-53をはじめとする全般的なガイドラインに加え、「識別及び認証」や「インシデント対応」等の個別対策分野に係るガイドラインを多数擁している。
- 対策分野によってガイドラインの整備状況(文書数等)は大きく異なっている。



[凡例] : 連邦政府機関等で拘束力があるもの : 必ずしも拘束力はないもの

主なSpecial Publication 800 シリーズ文書(1/3)

大分類	中分類	文書名	主題
全般	リスクマネジメントプロセス	SP 800-37	リスクマネジメントフレームワーク
	情報・システム分類	SP 800-59	国家安全システムの特典
		SP 800-60	情報・システム分類
	管理策集	SP 800-53	セキュリティ・プライバシー管理策
		SP 800-82	OTセキュリティ管理策
		SP 800-171	CUI保護に向けた管理策
		SP 800-172	CUI保護に向けた強化管理策
個別対策分野	アクセス制御	SP 800-162	属性ベースのアクセス制御
		SP 800-192	アクセス制御ポリシーの検証・テスト方法
	意識向上及びトレーニング	SP 800-50	サイバーセキュリティ等の学習プログラム
		SP 800-84	テスト、訓練、演習プログラム
		SP 800181	人材フレームワーク
	監査及び説明責任	-	-
	アセスメント、認可及び監視	SP 800-92	ログ管理計画
		SP 800-137	連邦情報システムの継続的モニタリング
	構成管理	SP 800-124	モバイル機器の管理
		SP 800-128	セキュリティに着目した構成管理
	緊急時対応計画	SP 800-34	緊急時対応計画
	識別及び認証	SP 800-63	デジタルアイデンティティ
		SP 800-76	PIV向け生体認証

主なSpecial Publication 800 シリーズ文書(2/3)

大分類	中分類	文書名	主題
個別対策分野	インシデント対応	SP 800-61	インシデントハンドリング
		SP 800-72	PDAフォレンジック
		SP 800-86	フォレンジック手法の統合
		SP 800-101	モバイル機器のフォレンジック
		SP 800-184	サイバーセキュリティイベント復旧
	メンテナンス	SP 800-40	パッチ管理計画
	媒体保護	SP 800-88	媒体のサニタイズ
	物理的・環境的保護	-	-
	計画	SP 800-18	システムセキュリティ計画
	プログラムマネジメント	SP-800-55	パフォーマンス測定
	職員のセキュリティ	SP 800-73	PIVインターフェース
	個人情報の取扱い及び透明性	SP 800-122	個人情報の機密性保護
	リスクアセスメント	SP 800-30	リスクアセスメント
	システム及びサービスの取得	SP 800-70	IT製品のセキュリティチェックリスト
	システム及び通信の保護	SP 800-41	ファイアウォールポリシー
		SP 800-44	ウェブサーバの保護
		SP 800-45	電子メールセキュリティ
		SP 800-46	テレワーク
		SP 800-47	情報交換のセキュリティ管理
		SP 800-81	セキュアなDNS展開方法
		SP 800-83	デスクトップ向けインシデント防御・対応
		SP 800-94	侵入検知・防御(IDPS)

主なSpecial Publication 800 シリーズ文書(3/3)

大分類	中分類	文書名	主題
個別対策分野	システム及び情報の完全性(暗号)	SP 800-38	ブロック暗号
		SP 800-49	S/MIME
		SP 800-52	TLS実装
		SP 800-56	離散対数暗号等を用いた鍵共有
		SP 800-57	鍵管理
		SP 800-71	対象ブロック暗号を用いた鍵共有
		SP 800-77	IPsec VPN
		SP 800-78	PIV向けの暗号
		SP 800-90	乱数生成
		SP 800-102	電子署名の適時性
		SP 800-121	Bluetoothのセキュリティ
		SP 800-130	鍵管理システムの設計
		SP 800-133	鍵生成
	サプライチェーンのリスクマネジメント	SP 800-161	サプライチェーンリスク管理
		SP 800-218	セキュアなソフトウェア開発フレームワーク
クラウド		SP 800-144	クラウドにおけるセキュリティとプライバシー
		SP 800-145	クラウドの定義
		SP 800-180	マイクロサービスの定義
		SP 800-190	アプリケーションコンテナのセキュリティ
IoT等		SP 800-183	モノのネットワーク
		SP 800-213	連邦政府向けIoT機器サイバーセキュリティ
ゼロトラスト		SP 800-207	ゼロトラスト

NIST Special Publication 800-53 Revision 5

- NIST Special Publication 800-53 Revision 5 (SP 800-53 Rev.5)は、主に連邦政府機関の情報システムで利用される情報システム・組織向けの管理策カタログ。

1.2.1 米国における制度やガイドライン等

名称	NIST Special Publication 800-53 Revision 5		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	主に連邦政府機関の情報システム	遵守義務の有無	あり
対象者	- 政府機関のCIO/CISOからセキュリティ担当者を中心に、官民の幅広い者を対象としている ※第5版では、タイトルから「連邦政府」の記述が削除された。		
概要	- 情報システム及び組織に課せられるセキュリティ及びプライバシー要件、ならびに、国内外で認知された他の規格と整合性があり、それらを補完するセキュリティ及びプライバシー要件を満たす管理策を以下の分類にて規定している。 - AC アクセス制御 - AT 意識向上及びトレーニング - AU 監査及び説明責任 - CA アセスメント、認可及び監視 - CM 構成管理 - CP 緊急時対応計画 - IA 識別及び認証 - IR インシデント対応 - MA メンテナンス - MP 媒体保護 - PE 物理的・環境的保護 - PL 計画 - PM プログラムマネジメント - PS 職員のセキュリティ - PT 個人情報の取扱い及び透明性 - RA リスクアセスメント - SA システム及びサービスの取得 - SC システム及び通信の保護 - SI システム及び情報の完全性 - SR サプライチェーンのリスクマネジメント - これらの管理策は、行政管理予算局(OMB)の通達(Circular) A-130 号及び連邦情報セキュリティ近代化法(FISMA)の規定により、連邦政府情報システムでの使用が義務付けられている。		
普及状況	- 米国では、連邦政府機関で義務的に活用されていることに加え、民間においても自主的に活用されている。^{*1} - 日本でも、2021年時点で6~7%程度の企業で利用されている。^{*2}		
URL	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092657.pdf		

*1 「NIST SP800-53rev.5「情報システムと組織のためのセキュリティ管理策およびプライバシー管理策」について」
(https://www.jipdec.or.jp/library/report/20201215_01.html)

*2 PwC, 2021年 Cyber IQ 調査—機先を制するセキュリティへの転換
(<https://www.pwc.com/jp/ja/knowledge/thoughtleadership/cyber-iq-survey2021.html>)

NIST Special Publication 800-53 Revision 5 の構成

- SP 800-53 Rev.5には、AとBという2つの別冊があり、AではSP 800-53 Rev.5で提示される管理策及び拡張管理策の評価方法、Bではそれらの管理策をどの情報及び情報システムに適用するかの目安(ベースライン)が提示されている。

NIST SP 800-53 Revision 5

SP 800-53A Rev. 5 組織と情報システムのための管理策の評価

- SP 800-53をベースとして、効果的なセキュリティ及びプライバシーの評価計画を構築するためのガイドラインと、システム及び組織で採用されているセキュリティ及びプライバシー管理の有効性を評価するための包括的な手順のセットを提供する。

SP 800-53B 組織と情報システムのための管理策ベースライン

- SP 800-53で規定されたセキュリティ及びプライバシー管理策、拡張管理策が、どの情報及び情報システムに適用されるかの目安(ベースライン)を提示している。
- 参照されている情報及び情報システムの分類は、連邦情報処理規格(FIPS)-199で提示されるものに準じており、低影響度/中影響度/高影響度の3つに区分されている。

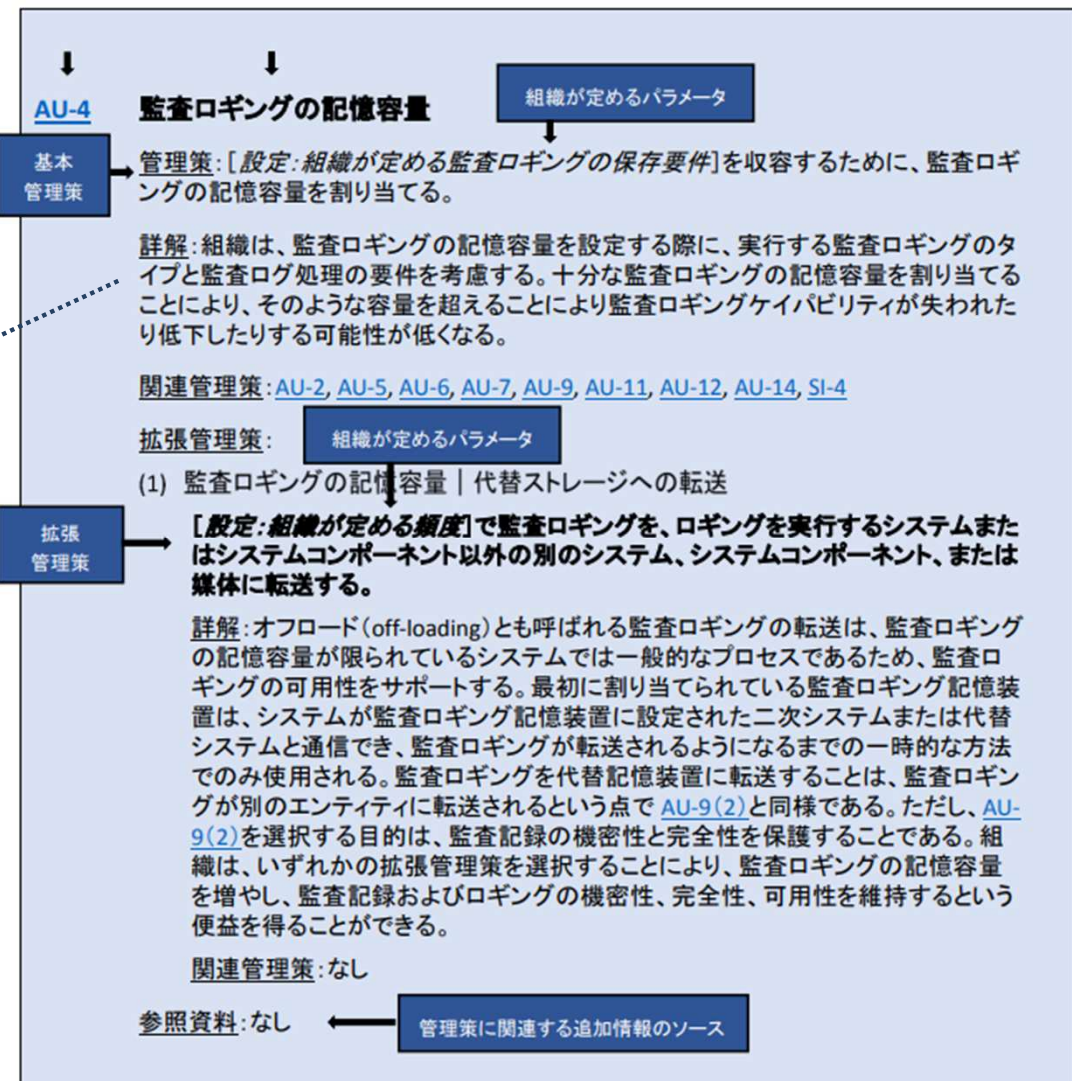
NIST Special Publication 800-53 Revision 5

- SP 800-53 Rev.5では、セキュリティ及びプライバシーに係る管理策及び拡張管理策が示されている。
- 提示される管理策は全般的に記載粒度が高く、数も非常に多い。

- 実装されるセキュリティまたはプライバシーの機能を定める。
- セキュリティ及びプライバシーの機能は、自動または手動の活動によって達成される。

- 管理策に関する追加の情報を提供する。
- 追加情報は、ミッションや事業の要件、運用環境、またはリスクアセスメントに基づいて管理策を実装するための重要な考慮事項を提供する。また、追加情報は、管理策の目的を説明するとともに、多くの場合、事例が含まれる。

- 基本管理策を強化するセキュリティ及びプライバシーの機能について説明する。
- 拡張管理策は、各管理策内で順番に番号が付けられており、基本管理策を補足するために選択する際、容易に特定することができる。
- 各拡張管理策には、拡張管理策によって提供が意図される機能を示す短い副題が付けられている。



NIST Special Publication 800-53A

- SP 800-53Aでは、SP 800-53で提示される管理策及び拡張管理策のそれぞれについて、評価目標や評価対象、評価手法を提示している。
- 評価手法は、検査(1つ以上の評価対象をレビュー、検査、観察、研究、または分析する)、インタビュー(組織内の個人またはグループと議論を行う)、テスト(指定された条件下で1つ以上の評価対象を実行し、対象の実際の状態を望ましい状態または期待される動作と比較する)の3種が定義されている。

AU-04 監査ロギングの記憶容量	
評価目標：以下の状態であるかどうかを決定する。	
AU-04_ODP*1	監査ログの保持に関する要求事項が定義されている。
AU-04	監査ログ・ストレージ容量が、組織が定める監査ログ保持に関する要求事項に対応するよう割り当てられている。
評価手法及び評価対象	
AU-04-検査(Examine)	[以下から選択： 監査と説明責任に関する方針、監査記録保存容量に関する手順、システムセキュリティ計画、プライバシー計画、システム設計文書、システム構成設定と関連文書、監査記録保持に関する要求事項、システム構成要素の監査記録保持機能、システム監査記録、その他の関連文書または記録]
AU-04-インタビュー(Interview)	[以下から選択： 監査と説明責任を担う要員、情報セキュリティとプライバシーに責任を担う要員、システム・ネットワーク管理者、システム開発者]
AU-04-テスト(Test)	[以下から選択： 監査記録の保存容量及び関連する構成設定]

*1 ODPとは、組織が各々に定義するパラメータ(Organization-Defined Parameters)の略称。

NIST Special Publication 800-53B

- NIST Special Publication 800-53Bでは、SP 800-53に記載されている管理策のうちいずれを適用すべきかが、レベルごとに提示されている。
- 以下の例では、AU-1、2、3、4はそれぞれ全ての影響度でベースラインになっている一方、拡張管理策であるAU-3(1)は高影響度のみベースラインに指定されている。

管理策 番号	管理策名 拡張管理策名	プライマリ管理策 ベースライン	セキュリティ管理策 ベースライン		
			低	中	高
AU-1	ポリシーおよび手順	x	x	x	x
AU-2	イベントログ取得	x	x	x	x
AU-2(1)	複数のソースからの監査記録の編集	W: AU-12に組み込み			
AU-2(2)	コンポーネントによる監査イベントの選択	W: AU-12に組み込み			
AU-2(3)	レビューおよび更新	W: AU-2に組み込み			
AU-2(4)	特権機能	W: AC-6(9)に組み込み			
AU-3	監査記録の内容		x	x	x
AU-3(1)	追加の監査情報				x
AU-3(2)	計画的監査記録内容の一元管理	W: PL-9に組み込み			
AU-3(3)	個人情報要素の限定	x			
AU-4	監査ログの記憶容量		x	x	x
AU-4(1)	代替ストレージへの転送				

NIST Special Publication 800-18

- NIST Special Publication 800-18は、システムセキュリティ計画を準備する方法について基本的な情報を提供する。

1.2.1 米国における制度やガイドライン等

名称	SP 800-18 連邦情報システムのセキュリティ計画策定に関する手引き		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	主に連邦政府機関の情報システム	遵守義務の有無	あり*1
対象者	基本的に連邦政府機関の関係者を想定するが、それ以外の主体による参照も妨げない。		
概要	- 本文書は、FISMAにて連邦政府機関の義務とされるシステムセキュリティ計画の作成について基本的な情報を提供する。 3章では、以下の要素からなるシステムセキュリティ計画の構成及び作成ステップについて説明されている。 - システムの名称と識別子 - システムの運用状態 - セキュリティ管理策の選択 - システムの分類 - 情報システムの種別 - 最低限のセキュリティ管理策 - システムのオーナー - 概要／目的 - 完了日および承認日 - 運用認可責任者 - システム環境 - システムセキュリティ計画の継続的保守 - その他の指定連絡先 - システム相互接続／情報共有 - セキュリティに対する責任の割り当て - 影響する法律、規程、および政策 - 上記のシステムセキュリティ計画の構成を踏まえ、付録 Aでは、情報システムセキュリティ計画のサンプルテンプレートが示されている。		
普及状況	- 米国では、連邦政府機関によるシステムセキュリティ計画の作成に際して広く参照されていると考えられる。 - 日本でもIPAから翻訳が公開されているが、その他民間企業による解説等は確認されなかったため、国内の認知は限られていると考えられる。		
URL	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025324.pdf		

*1 OMB Circular A-130では、連邦政府機関によるシステムセキュリティ計画の策定が義務とされている。
(https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

NIST Special Publication 800-18

- 付録 Aでは、情報システムセキュリティ計画のサンプルテンプレートが示されている。

情報システムセキュリティ計画のテンプレート

1. 情報システムの名称/表題:

- システムに割り当てられた一意の識別子および名称。

2. 情報システムの分類:

- FIPS 199 による適切な分類を識別する。

	低位		中位		高位

3. 情報システムのオーナー:

- システムのオーナーである担当者 の名前、役職、政府機関、住所、電子メールアドレス、および電話番号。

4. 運用認可責任者:

- 運用認可責任者として指名されている上級管理責任者の名前、役職、政府機関、住所、電子メールアドレス、および電話番号。

5. その他の指定連絡先:

- 必要な場合、その他の主な担当者 の役職、住所、電子メールアドレス、電話番号などを列挙する。

6. セキュリティに対する責任の割り当て:

- システムのセキュリティに対する責任を負う担当者 の名前、役職、住所、電子メールアドレス、および電話番号。

7. 情報システムの運用状態:

- システムの運用状態を示す。2 つ以上の状態が選択されている場合は、システムのどの部分がどの状態にあるのかを記述する。

	運用中		開発中		大規模な修正中

8. 情報システム種別:

- システムが主要アプリケーションか一般支援システムかを示す。システムに非主要アプリケーションが含まれる場合は、それを第 9 節「システムの概要/目的」に列挙する。

	主要アプリケーション		一般支援システム

11. システム相互接続/情報共有

- 相互接続されるシステムとシステム識別子(必要な場合)を列挙し、システム、名称、組織、システム種別(主要アプリケーションまたは一般支援システム)を示すとともに、ISA/MOU/MOA がファイルに記録されているかどうか、相互接続に合意した日付、FIPS 199 による分類、C&A の状態、および認可責任者の名前を示す。

システムの名称	組織	種別	合意 (ISA/MOU/MOA)	日付	FIPS 199 による分類	C&A の状態	運用認可責任者

12. 関連する法律/規程/政策

- システム内のデータの機密性、完全性、または可用性に対する具体的な要求事項を定めた法律または規程をすべて列挙する。

13. 最低限のセキュリティ管理策

NIST SP 800-53 から該当する最低限のセキュリティ管理策ベースライン(低位、中位、高位の影響レベル)を選択した上で、適用可能なベースラインに含まれる最低限のセキュリティ管理策のすべての実施方法または実施計画の方法を詳細に記述する。この記述には以下の情報を盛り込むべきである。1) セキュリティ管理策の表題、2) セキュリティ管理策の実施方法または実施計画の方法、3) 適用した詳細調査ガイダンスおよび考慮点の種別、および 4) セキュリティ管理策が共通管理策であるか、管理策の実施責任者は誰であるかの記述。

14. 情報システムセキュリティ計画の完了日:

- 計画の完了日を記入する。

15. 情報システムセキュリティ計画の承認日:

- システムセキュリティ計画が承認された日付を記入し、承認文書が添付またはファイルに記録されているかどうかを示す。

NIST Special Publication 800-30 Revision 1

- NIST Special Publication 800-30は、リスクマネジメントプロセスにおけるアセスメントの実施方法等を示すガイドラインである。

1.2.1 米国における制度やガイドライン等

名称	SP 800-30 Rev.1 リスクアセスメント実施の手引き		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	主に連邦政府機関の情報システム	遵守義務の有無	なし*1
対象者	本文書は、官民を問わず、様々なリスクマネジメント専門家の一助となることを目指している。		
概要	- 本文書では、リスクマネジメントプロセス及びそこに位置づけられるリスクアセスメントの概要及び適用方法が示されている。 - 情報セキュリティリスクをアセスメントするプロセスを以下に示す4つのステップに分類し、それぞれで実施されるべきタスクを細分化している。 - ステップ 1：リスクアセスメントの準備 アセスメントの目的及び適用範囲を特定し、リスク許容度及び優先順位・トレードオフ等を明確にする。 - ステップ 2：リスクアセスメントの実施 リスクレベルによって優先順位付けされた情報セキュリティリスク一覧を生成する。 - ステップ 3：リスクアセスメント結果の伝達 意思決定者が、リスク判断に情報を提供し、判断を導くのに必要な適切なリスク関連情報を有することを確実にする。 - ステップ 4：リスクアセスメントの保守 組織が被るリスクについての具体的な知識を最新に保つ。		
普及状況	- 米国では、連邦政府機関によるサイバーセキュリティ対策義務の遵守に際して一定の参照がなされている。 - 日本でもIPAから翻訳が公開されているが、その他民間企業による解説等は確認されなかったため、国内の認知は限られていると考えられる。		
URL	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025325.pdf		

*1 OMB Circular A-130では、参照規格としてSP 800-30が示されるものの、適用が義務とされている規定は確認されなかった。
(https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

NIST Special Publication 800-37 Revision 2

- SP 800-37 Rev.2 は、組織や情報システムにおける情報セキュリティリスクの管理方法を示したもの。
- SP 800-53が個々の管理策の詳細を示すのに対し、本文書はリスクマネジメントの全体像を示すもの。

1.2.1 米国における制度やガイドライン等

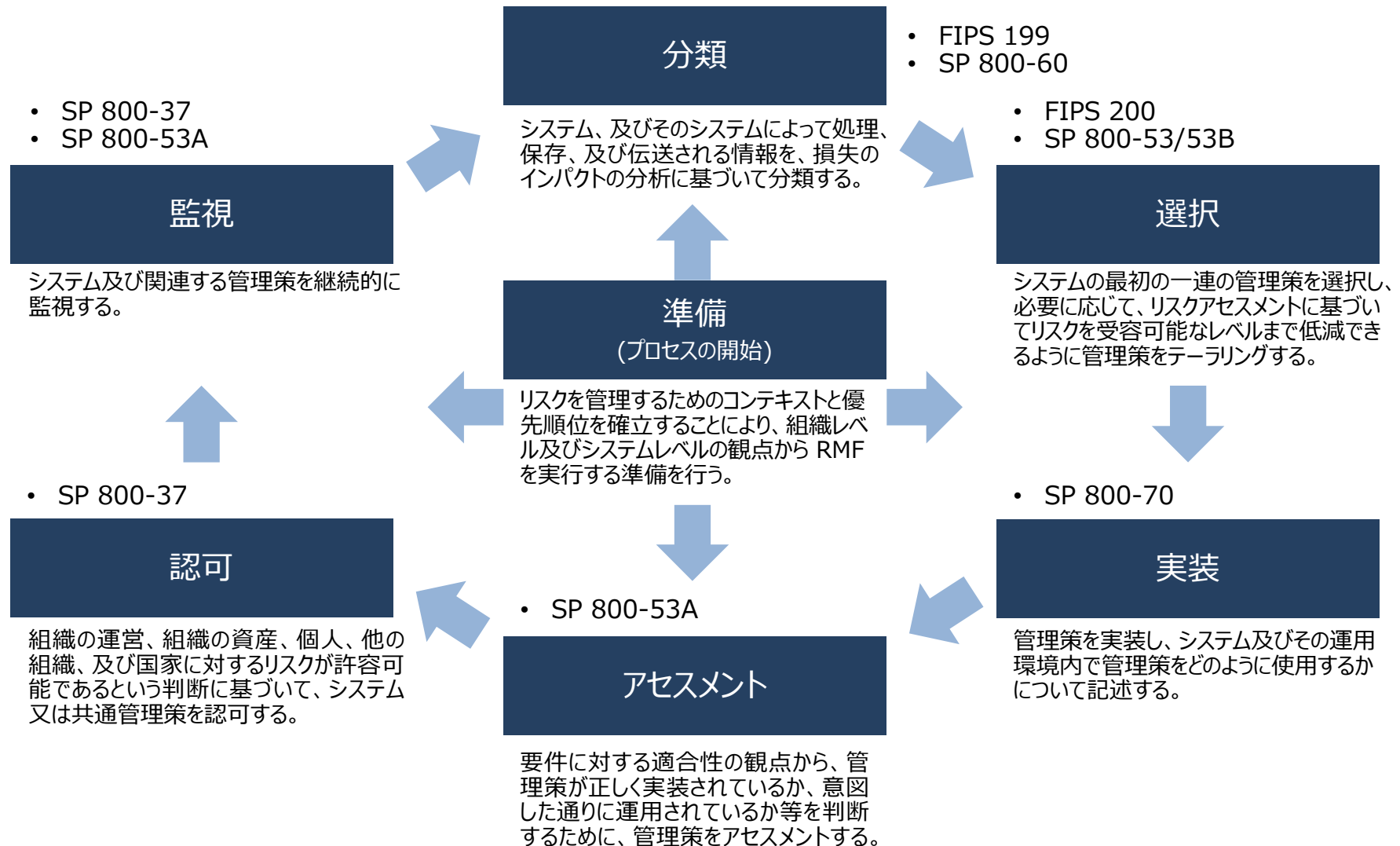
名称	SP 800-37 Rev.2 情報システム・組織向けリスクマネジメントフレームワーク		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	主に連邦政府機関の情報システム	遵守義務の有無	あり*1
対象者	- 連邦政府機関の関係者を中心に、官民の情報システムの設計、開発、実装、アセスメント、運用、メンテナンス、及び廃棄に関わる者を広く対象とする。 ※第2版では、タイトルから「連邦政府」の記述が削除された。		
概要	- リスクマネジメントフレームワーク(RMF)について説明し、セキュリティ及びプライバシーリスクを管理し、情報システム及び組織にRMFを適用するための指針を提供する。 - RMF には、組織がプロセスを実行する準備ができていることを確認するための準備ステップと、以下に示す6つの主要なステップから成る、7つのステップがある。アセスメント(Assess) - 分類(Categorize) - 選択(Select) - 実装(Implement) - 認可(Authorize) - 監視(Monitor) - また、RMF を構成するステップ及び関連タスクと、そのようなタスクを実施する選択された個人又はグループ(定義された組織の役割)が示されている。		
普及状況	- 米国では、連邦政府機関によるリスクマネジメントフレームワーク実施義務の遵守に際して広く参照されている。 - 日本でもIPAから翻訳が公開されているほか、民間企業による解説*2が執筆されており、一定の認知がある。		
URL	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/NIST.SP.800-37r2_JA.pdf		

*1 2016年にOMB Circular A-130が改訂された際に、リスクマネジメントフレームワークの実施に対する責任が盛り込まれた。
(https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

*2 NISTのリスクマネジメントフレームワーク(RMF)とは ～第1回 SP800-37 Rev2とリスクマネジメントフレームワーク(RMF)～
(<https://www.intellilink.co.jp/article/column/RMF-01.html>)

[参考] リスク管理プロセスによるSP 800規格の整理

- FIPS及びSP 800シリーズ文書は、管理策の選定や実装のみならず、評価やモニタリング等を含めたリスク管理プロセスの全体に渡り整備されている。



SP 800-60 Vol.1 Rev.1

- SP 800-60は、SP 800-37のリスクマネジメントフレームワークにおける「分類」に関して、検討方法やプロセスを詳述するガイドラインである。

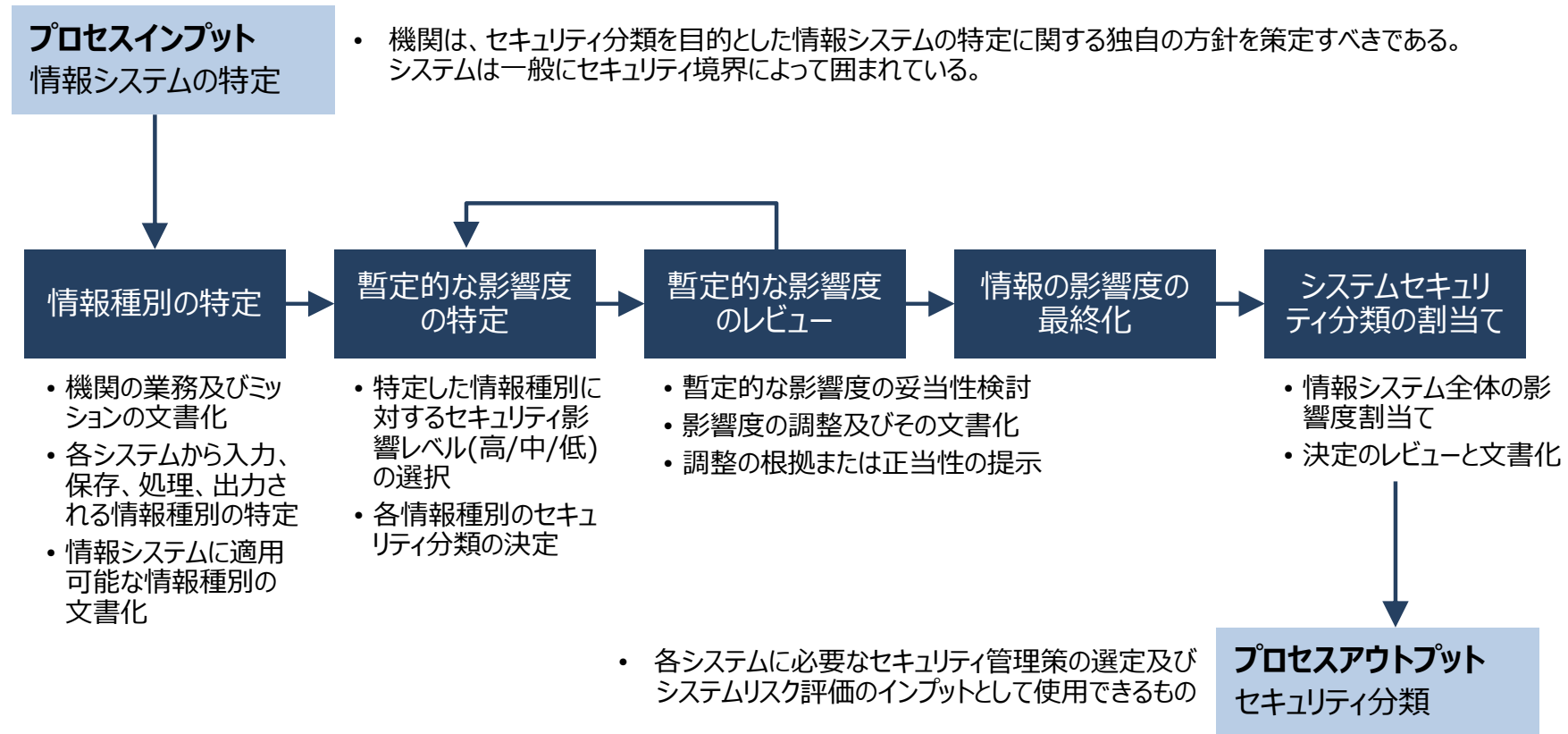
1.2.1 米国における制度やガイドライン等

名称	SP 800-60 Vol.1 Rev.1 情報及び情報システムの種別とセキュリティ分類のマッピングに関する手引き		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	主に連邦政府機関の情報システム	遵守義務の有無	あり*1
対象者	情報システム及び情報セキュリティの専門家からなる様々な連邦政府関係者		
概要	- SP 800-37のリスクマネジメントフレームワークにおける「分類」に関して、検討方法やプロセスを詳述するガイドラインである。 - 本文書では、情報及び情報システムの分類実施の流れを以下のように示している。 - 情報システムの特定 - STEP 1: 情報種別の特定 - STEP 2: 暫定的な影響度の特定 - STEP 3: 暫定的な影響度のレビュー/情報の影響度の最終化 - STEP 4: システムセキュリティ分類の割当て - 成果: セキュリティ分類 - 本文書は、第1巻と第2巻から構成されており、第1巻には情報及び情報システムの種類をセキュリティ・カテゴリーに対応付けるための基本的なガイドラインが示され、2巻にはミッション・ベースおよび管理・支援情報の種類に関するセキュリティ分類の勧告と根拠が示されている。		
普及状況	米国では、連邦政府機関による情報及び情報システムの分類に際して広く参照されている。		
URL	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf		

*1 OMB Circular A-130では、FIPS 199及びSP 800-60に沿った形でセキュリティ分類を行う義務が規定されている。
(https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

SP 800-60 Vol.1 Rev.1

- SP 800-60では、情報及び情報システムの分類実施の流れを以下のように示している。



アウトプット(例)

SC(セキュリティ分類) SCADA システム
= {(機密性, 中位), (完全性, 高位), (可用性, 高位)}

NIST Special Publication (SP) 800-82 Revision 3

- NIST Special Publication (SP) 800-82は、OTシステムにおけるサイバーセキュリティ対策の進め方や対策の詳細を示した代表的なガイドライン文書である。

1.2.1 米国における制度やガイドライン等

名称	NIST Special Publication (SP) 800-82r3 Guide to Operational Technology (OT) Security		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	OT* ¹ システム	遵守義務の有無	なし
対象者	OTシステムを、①設計・実装するインテグレータ等、②管理するシステム管理者等、③セキュリティ評価を行うコンサルタント等及び、④OTシステムを構成する製品を開発するベンダーを含む官民の主体		
概要	- 本書は、OT と典型的なシステムトポロジの概要を提供し、これらのシステムに対する一般的な脅威と脆弱性を特定し、関連するリスクを軽減するために推奨されるセキュリティ対策を提供する。 - ITとOTとの比較を含むOTの概要 (2章) - リスク軽減を目的としたOTサイバーセキュリティプログラムの開発及び展開 (3章) - OT セキュリティリスク管理と OT システムへのリスクマネジメントフレームワークの適用 (4章) - OT システムで一般的に見られるネットワークアーキテクチャにセキュリティを統合するための推奨事項 (5章) - サイバーセキュリティフレームワークを OT システムに適用するためのガイダンス (6章) - 付録(Appendix)では、用語定義やOTにおける脅威事象及びインシデント、NIST SP 800-53をOTシステムに適用する際の補足事項等を示している。		
普及状況	本文書の適用は必ずしも義務とされているわけではないが、IEC 62443等と並んで制御セキュリティに関する代表的なガイドラインとみなされており、OTセキュリティ対策実装の際に広く参照されている。^{*2}		
URL	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf		

*1 OTとは、「Operational Technology」の略称であり、物理的環境と相互作用する広範なプログラム可能なシステム及び機器を指す。
例えば、産業制御システム、ビルディング・オートメーション・システム、交通システム、物理アクセス制御システム、物理環境モニタリング・システム、物理環境測定システム等が含まれる。
(<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>)

*2 例えば、「制御システムのセキュリティリスク分析ガイド 第2版」の「ファイアウォール設定の詳細項目とセキュリティ要件」や「制御システムの境界防御の詳細項目とセキュリティ要件」では、本文書が広範に参照されている。
(<https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf>)

NIST Special Publication (SP) 800-82 Revision 3

- 付録Fでは、OTシステムの特性を踏まえたSP 800-53管理策の補足事項等を示している。

① AC-3 ACCESS ENFORCEMENT

② CNTL NO.	③ CONTROL NAME <i>Control Enhancement Name</i>	④ SUPPLEMENTED		
		⑥ CONTROL BASELINES		
		LOW	MOD	HIGH
⑤ AC-3	Access Enforcement	Select	Select	⑦ Select
AC-3 (11)	ACCESS ENFORCEMENT RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES			Add

⑧ OT Discussion: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation. The policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control. However, it may not provide sufficient granularity when users require access to different functions.

⑨ Control Enhancement: (11) OT Discussion: The organization identifies and restricts access to information that could impact the OT environment and accounts for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

⑩ Rationale for adding AC-3 (11) to HIGH baseline: The loss of availability, integrity, and confidentiality of certain types of information that reside on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals, including severe degradation or loss of mission capability, major damage to organizational assets, or harm to individuals involving the loss of life or life-threatening injuries.

- ① 管理策番号と表題
- ② 管理策及び強化管理策番号の列
- ③ 管理策及び強化管理策名称の列
- ④ ベースラインの列。ベースラインが補足されている場合は、「SUPPLEMENTED」と表示される。
- ⑤ 各管理策または強化管理策の行
- ⑥ LOW(低)、MODERATE(中)、HIGH(高)それぞれのベースラインの列
- ⑦ 「Select」は、NIST SP 800-53、Rev.5で管理策が選択されていることを示す。「Add」は、管理策がOTのベースラインに追加されていることを示す。空白のセルは、管理策が選択されていないことを示す。「Remove」は、管理策がベースラインから削除されることを示す。
- ⑧ OTに特有の事項を補足する。何もなければ、その旨が記載される。
- ⑨ 強化管理策についてOTに特有の事項を補足する。ない場合はその旨を記載する。
- ⑩ ベースラインにおける管理策追加の根拠

U.S. Cybersecurity Labeling Program for Smart Devices

- 米国では、消費者向けIoT機器の信頼性向上のため、サイバーセキュリティラベリング制度に関する検討を目下進めている。

1.2.1 米国における制度やガイドライン等

名称	U.S. Cybersecurity Labeling Program for Smart Devices		
国・地域	米国	策定者	連邦通信委員会(FCC)
適用分野	消費者向けIoT製品	遵守義務の有無	なし*1
対象者	消費者向けIoT製品を設計、開発、販売、保守する事業者		
概要	- 日常生活に浸透しているIoT機器のセキュリティに対する消費者の信頼と理解を向上させるため、IoTサイバーセキュリティ基準に準拠した製品に対して、政府が裏付けした信頼できるラベルを提供する。 - ラベルの取得にあたっては、連邦通信委員会(FCC)が今後定める規則を遵守する必要がある。 - 対象機器または製品 対象を消費者向け製品に絞るか、さらに広い範囲とするか等について今後議論がなされる見込み。 - IoTサイバーセキュリティ基準 これまでに策定されているNIST標準(NISTIR 8259等)を参照しつつ、官民の利害関係者を招集して策定される。 - ラベルの管理 ラベルの仕様(QRコードの有無等)や提供する情報の種類、貼付け場所等について今後規則が策定される見込み。		
普及状況	規則策定中につきデータなし		
URL	https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/		

*1 ラベリングプログラムへの参加自体に拘束性はないが、参加を選択した場合はサイバーセキュリティ要求事項等の所定のプログラム要件の遵守が求められる。
(<https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf>)

NIST Special Publication (SP) 800-82 Revision 3

- NIST Special Publication (SP) 800-82は、OTシステムにおけるサイバーセキュリティ対策の進め方や対策の詳細を示した代表的なガイドライン文書である。

1.2.1 米国における制度やガイドライン等

名称	NIST Special Publication (SP) 800-82r3 Guide to Operational Technology (OT) Security		
国・地域	米国	策定者	国立標準技術研究所(NIST)
適用分野	OT* ¹ システム	遵守義務の有無	なし
対象者	OTシステムを、①設計・実装するインテグレータ等、②管理するシステム管理者等、③セキュリティ評価を行うコンサルタント等及び、④OTシステムを構成する製品を開発するベンダーを含む官民の主体		
概要	- 本書は、OT と典型的なシステムトポロジの概要を提供し、これらのシステムに対する一般的な脅威と脆弱性を特定し、関連するリスクを軽減するために推奨されるセキュリティ対策を提供する。 - ITとOTとの比較を含むOTの概要 (2章) - リスク軽減を目的としたOTサイバーセキュリティプログラムの開発及び展開 (3章) - OT セキュリティリスク管理と OT システムへのリスクマネジメントフレームワークの適用 (4章) - OT システムで一般的に見られるネットワークアーキテクチャにセキュリティを統合するための推奨事項 (5章) - サイバーセキュリティフレームワークを OT システムに適用するためのガイダンス (6章) - 付録(Appendix)では、用語定義やOTにおける脅威事象及びインシデント、NIST SP 800-53をOTシステムに適用する際の補足事項等を示している。		
普及状況	本文書の適用は必ずしも義務とされているわけではないが、IEC 62443等と並んで制御セキュリティに関する代表的なガイドラインとみなされており、OTセキュリティ対策実装の際に広く参照されている。^{*2}		
URL	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf		

*1 OTとは、「Operational Technology」の略称であり、物理的環境と相互作用する広範なプログラム可能なシステム及び機器を指す。
例えば、産業制御システム、ビルディング・オートメーション・システム、交通システム、物理アクセス制御システム、物理環境モニタリング・システム、物理環境測定システム等が含まれる。
(<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>)

*2 例えば、「制御システムのセキュリティリスク分析ガイド 第2版」の「ファイアウォール設定の詳細項目とセキュリティ要件」や「制御システムの境界防御の詳細項目とセキュリティ要件」では、本文書が広範に参照されている。
(<https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf>)

NIST Special Publication (SP) 800-82 Revision 3

- 付録Fでは、OTシステムの特性を踏まえたSP 800-53管理策の補足事項等を示している。

① AC-3 ACCESS ENFORCEMENT

② CNTL NO.	③ CONTROL NAME <i>Control Enhancement Name</i>	④ SUPPLEMENTED		
		⑥ CONTROL BASELINES		
		LOW	MOD	HIGH
⑤ AC-3	Access Enforcement	Select	Select	⑦ Select
AC-3 (11)	ACCESS ENFORCEMENT RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES			Add

⑧ OT Discussion: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation. The policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control. However, it may not provide sufficient granularity when users require access to different functions.

⑨ Control Enhancement: (11) OT Discussion: The organization identifies and restricts access to information that could impact the OT environment and accounts for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

⑩ Rationale for adding AC-3 (11) to HIGH baseline: The loss of availability, integrity, and confidentiality of certain types of information that reside on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals, including severe degradation or loss of mission capability, major damage to organizational assets, or harm to individuals involving the loss of life or life-threatening injuries.

- ① 管理策番号と表題
- ② 管理策及び強化管理策番号の列
- ③ 管理策及び強化管理策名称の列
- ④ ベースラインの列。ベースラインが補足されている場合は、「SUPPLEMENTED」と表示される。
- ⑤ 各管理策または強化管理策の行
- ⑥ LOW(低)、MODERATE(中)、HIGH(高)それぞれのベースラインの列
- ⑦ 「Select」は、NIST SP 800-53、Rev.5で管理策が選択されていることを示す。「Add」は、管理策がOTのベースラインに追加されていることを示す。空白のセルは、管理策が選択されていないことを示す。「Remove」は、管理策がベースラインから削除されることを示す。
- ⑧ OTに特有の事項を補足する。何もなければ、その旨が記載される。
- ⑨ 強化管理策についてOTに特有の事項を補足する。ない場合はその旨を記載する。
- ⑩ ベースラインにおける管理策追加の根拠

U.S. Cybersecurity Labeling Program for Smart Devices

- 米国では、消費者向けIoT機器の信頼性向上のため、サイバーセキュリティラベリング制度に関する検討を目下進めている。

1.2.1 米国における制度やガイドライン等

名称	U.S. Cybersecurity Labeling Program for Smart Devices		
国・地域	米国	策定者	連邦通信委員会(FCC)
適用分野	消費者向けIoT製品	遵守義務の有無	なし*1
対象者	消費者向けIoT製品を設計、開発、販売、保守する事業者		
概要	- 日常生活に浸透しているIoT機器のセキュリティに対する消費者の信頼と理解を向上させるため、IoTサイバーセキュリティ基準に準拠した製品に対して、政府が裏付けした信頼できるラベルを提供する。 - ラベルの取得にあたっては、連邦通信委員会(FCC)が今後定める規則を遵守する必要がある。 - 対象機器または製品 対象を消費者向け製品に絞るか、さらに広い範囲とするか等について今後議論がなされる見込み。 - IoTサイバーセキュリティ基準 これまでに策定されているNIST標準(NISTIR 8259等)を参照しつつ、官民の利害関係者を招集して策定される。 - ラベルの管理 ラベルの仕様(QRコードの有無等)や提供する情報の種類、貼付け場所等について今後規則が策定される見込み。		
普及状況	規則策定中につきデータなし		
URL	https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/		

*1 ラベリングプログラムへの参加自体に拘束性はないが、参加を選択した場合はサイバーセキュリティ要求事項等の所定のプログラム要件の遵守が求められる。
(<https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf>)

連邦情報セキュリティマネジメント法(FISMA)

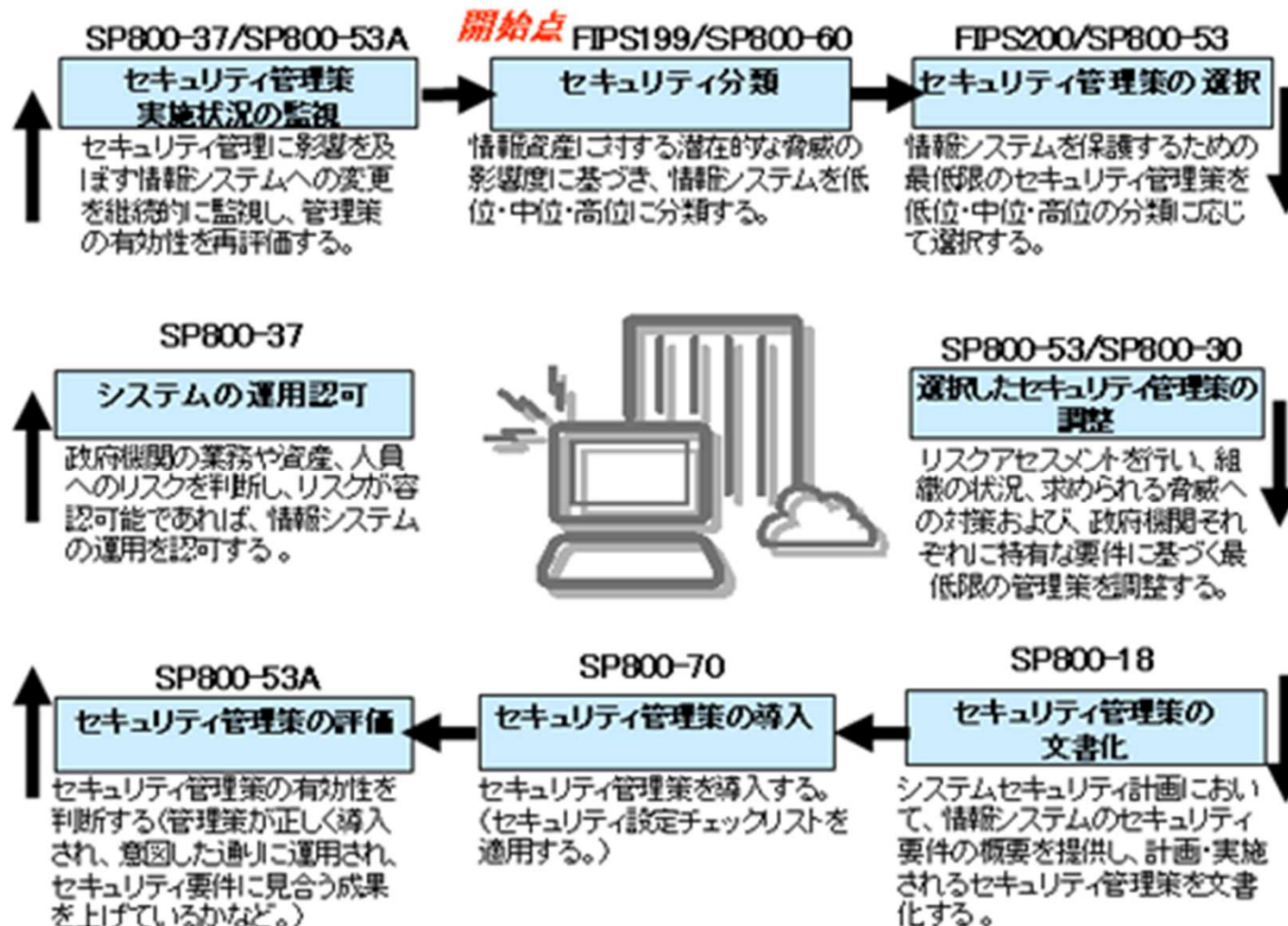
- 連邦情報セキュリティマネジメント法(FISMA)では、連邦政府機関が情報セキュリティを強化することを義務付け、NISTに対しては、そのための規格やガイドラインの開発を義務付けている。

1.2.1 米国における制度やガイドライン等

名称	連邦情報セキュリティマネジメント法(FISMA)		
国・地域	米国	策定者	連邦議会
適用分野	政府情報システム	遵守義務の有無	あり
対象者	- 米国連邦政府 - 連邦政府機関より業務委託を受けている民間の外部委託先		
概要	- 連邦情報セキュリティマネジメント法(FISMA)では、<u>各連邦政府機関に対して、情報および情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践することを義務付けている</u>。また、同法は、NIST(米国国立標準技術研究所)に対しては、連邦政府がFISMAに準拠するための支援をすることを義務付けている。 - FISMA は、次の連邦規格を公布することを命じている。 I. リスクレベルに基づいた適切なレベルの情報セキュリティを提供するために、<u>連邦政府の情報および情報システムをセキュリティ分類するための規格</u>。 II. (I)の規格に従って分類された連邦政府の情報および情報システムに対する<u>最低限のセキュリティ要求事項に関する規格</u>。		
普及状況	(義務のため全ての連邦政府の情報システム等に適用)		
URL	https://www.congress.gov/bill/113th-congress/senate-bill/2521 https://www.ipa.go.jp/security/reports/oversea/nist/fisma.html		

連邦情報セキュリティ近代化法(FISMA)

- NISTでは2003年1月に「FISMA導入プロジェクト(The FISMA Implementation Project)」を立ち上げ、情報システムのセキュリティを強化し安全に運用するための様々な規格やガイドラインを策定。



FIPS 199/200

- FIPS 199は、連邦政府における情報および情報システムのセキュリティ分類を規定する。
- FIPS 200は、連邦政府における情報システムのセキュリティ分類ごとに求めるセキュリティ要求事項の選択の考え方が示されている。

1.2.1 米国における制度やガイドライン等

名称	FIPS 199 連邦政府の情報および情報システムに対するセキュリティ分類規格 FIPS 200 連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項		
国・地域	米国	策定者	NIST
適用分野	連邦政府の情報および情報システム	遵守義務の有無	あり
対象者	• 米国連邦政府		
概要	• FIPS 199は、連邦政府における情報および情報システムの両方のセキュリティ分類を規定する。機密性、完全性、可用性の3つの観点から、情報システム上に存在する情報の各タイプごとに判断されたセキュリティ分類の中で最も高い値（つまり、最高水準）を採用する。 <u>情報システムのセキュリティ分類 = {(機密性, 影響), (完全性, 影響), (可用性, 影響)}</u> • FIPS 200は、連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項の考え方を規定する。FIPS 199を参考に判断された情報システムのレベルごとによって、NIST SP800-53Bのセキュリティ管理策を選択するよう示している。		
普及状況	(義務のため全ての連邦政府の情報システム等に適用)		
URL	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025321.pdf https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025322.pdf		

FIPS 199

- 以下の式で情報システムのセキュリティ分類を示す際、情報システム上に存在する情報の各タイプごとに判断されたセキュリティ分類の中で最も高い値(つまり、最高水準)を示す。

情報システムのセキュリティ分類 = {(機密性, 影響), (完全性, 影響), (可用性, 影響)}

セキュリティ目的	潜在的影響		
	低位	中位	高位
機密性 しかるべき承認を受けて情報へのアクセスと開示に対して制限を設けること。これには、個人のプライバシーと機密情報の保護手段が含まれる。 [44 U.S.C., SEC. 3542]	情報の不当な開示が、組織活動、組織資産、または個人に 限定的な悪影響 を及ぼすことが予想される。	情報の不当な開示が、組織活動、組織資産、または個人に 重大な悪影響 を及ぼすことが予想される。	情報の不当な開示が、組織活動、組織資産、または個人に 致命的または壊滅的な悪影響 を及ぼすことが予想される。
完全性 不適切な情報改変または破壊から情報を保護すること。これには情報の否認防止および真正性の保証が含まれる。 [44 U.S.C., SEC. 3542]	情報の不当な改変または破壊が、組織活動、組織資産、または個人に 限定的な悪影響 を及ぼすことが予想される。	情報の不当な改変または破壊が、組織活動、組織資産、または個人に 重大な悪影響 を及ぼすことが予想される。	情報の不当な改変または破壊が、組織活動、組織資産、または個人に 致命的または壊滅的な悪影響 を及ぼすことが予想される。
可用性 タイムリーかつ信頼性の高い方法で情報にアクセスでき、利用できることを保証すること。[44 U.S.C., SEC. 3542]	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に 限定的な悪影響 を及ぼすことが予想される。	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に 重大な悪影響 を及ぼすことが予想される。	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に 致命的または壊滅的な悪影響 を及ぼすことが予想される。

FIPS 200

- FIPS 200では、FIPS 199を参考に判断された情報システムのレベルごとにNIST SP800-53Bのセキュリティ管理策を選択するよう示している。

分類	セキュリティ管理策
影響レベルが高位である 情報システム	組織は、最低限、 <u>NIST SP800-53Bにおいて定義された高位ベースラインのセキュリティ管理策を採用</u> し、それを自組織の情報システムにあわせて調整し、高位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。
影響レベルが中位である 情報システム	組織は、 <u>最低限、NIST SP800-53Bにおいて定義された中位ベースラインのセキュリティ管理策を採用</u> し、それを自組織の情報システムにあわせて調整し、中位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。
影響レベルが低位である 情報システム	組織は、 <u>最低限、NIST SP800-53Bにおいて定義された低位ベースラインのセキュリティ管理策を採用</u> し、それを自組織の情報システムにあわせて調整し、低位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。

The Federal Risk and Authorization Management Program

- FedRAMPは、クラウド技術と連邦政府機関のセキュリティとリスク評価に対する標準化されたアプローチを提供することで、連邦政府全体で安全なクラウドサービスの採用を促進している。

1.2.1 米国における制度やガイドライン等

名称	The Federal Risk and Authorization Management Program(FedRAMP)		
国・地域	米国	策定者	FedRAMP PMO (政府調達局(General Service Administration)内に設置)
適用分野	政府情報システム	遵守義務の有無	あり(政府調達において)
対象者	・ クラウドサービスプロバイダ		
概要	- FedRAMPは政府全体のプログラムであり、クラウド技術と連邦政府機関のセキュリティとリスク評価に対する標準化されたアプローチを提供することで、連邦政府全体で安全なクラウドサービスの採用を促進している。米国政府機関にサービスを提供するためのクラウドサービスを対象とした認証制度であり、提供者は米国だけでなく、日本を含む世界中の企業、組織が対象となる。 - FedRAMPは、FISMA、OMB Circular A-130、FedRAMPポリシー、国防授權法の一部としてのFedRAMP授權法に従い、クラウドサービスの認可と継続的なサイバーセキュリティのためのセキュリティ要件を標準化している。 - FedRAMPの基準は、NIST SP800-53をベースに策定されており、クラウドサービスプロバイダが実装する必要があるコントロールは、FedRAMP Security Controls Baselineに規定されている。この Baseline は、セキュリティの高さで以下の3段階(FedRAMP Low、FedRAMP Moderate、FedRAMP High)のレベル分けがされている。		
普及状況	・ 認証されたサービス数:336* ¹ (クラウドサービスプロバイダ数:280* ²)		
URL	https://www.fedramp.gov/program-basics/		

*1 認証されたサービスの内訳は次の通り。[高:34 中:256 低:7 LI-SaaS:39]

*2 2024年5月7日時点で既に認証済みの企業数をカウント。したがって、審査中及び準備段階のサービス及び企業は含んでいない。

The Federal Risk and Authorization Management Program

- 調査時点では、認証済みや審査中、準備段階のサービス各段階において、中レベル(moderate)で認証されているサービスが一番多い。
- また、認証済みのサービスに加えて、審査中、準備段階のサービスも多くみられる。

分類	高 (high)	中 (moderate)	低 (low)	LI-SaaS* ¹ ('低'の軽量版)	小計
認証済み	34	256	7	39	336
審査中	27	75	2	4	108
準備段階	9	20	-	1	30
合計	70	351	9	44	474

*1 LI-SaaSはインパクトレベル「低」の軽量版で、ログイン機能に必要なもの（ユーザ名、パスワード、メールアドレス）以上の情報を保存しないSaaSアプリケーションを対象にしている。

The Federal Risk and Authorization Management Program

- インパクトレベルによって各カテゴリーの要件数が異なる。インパクトレベルが高いほど遵守すべき要件は多い。

分類 (A→Z)	高 (high)	中 (moderate)	低 (low)
ACCESS CONTROL	50	43	11
AUDIT AND ACCOUNTABILITY	27	16	10
AWARENESS AND TRAINING	6	6	5
CONFIGURATION MANAGEMENT	34	27	9
CONTINGENCY PLANNING	35	23	6
IDENTIFICATION AND AUTHENTICATION	30	27	16
INCIDENT RESPONSE	24	17	7
MAINTENANCE	12	10	4
MEDIA PROTECTION	10	7	4
PERSONNEL SECURITY	11	10	9
PHYSICAL AND ENVIRONMENTAL PROTECTION	26	19	10
PLANNING	7	7	7
RISK ASSESSMENT	13	11	8
SECURITY ASSESSMENT AND AUTHORIZATION	16	14	10
SUPPLY CHAIN RISK MANAGEMENT FAMILY	14	12	11
SYSTEM AND COMMUNICATIONS PROTECTION	35	29	14
SYSTEM AND INFORMATION INTEGRITY	35	24	6
SYSTEM AND SERVICES ACQUISITION	25	21	9
合計	410	323	156

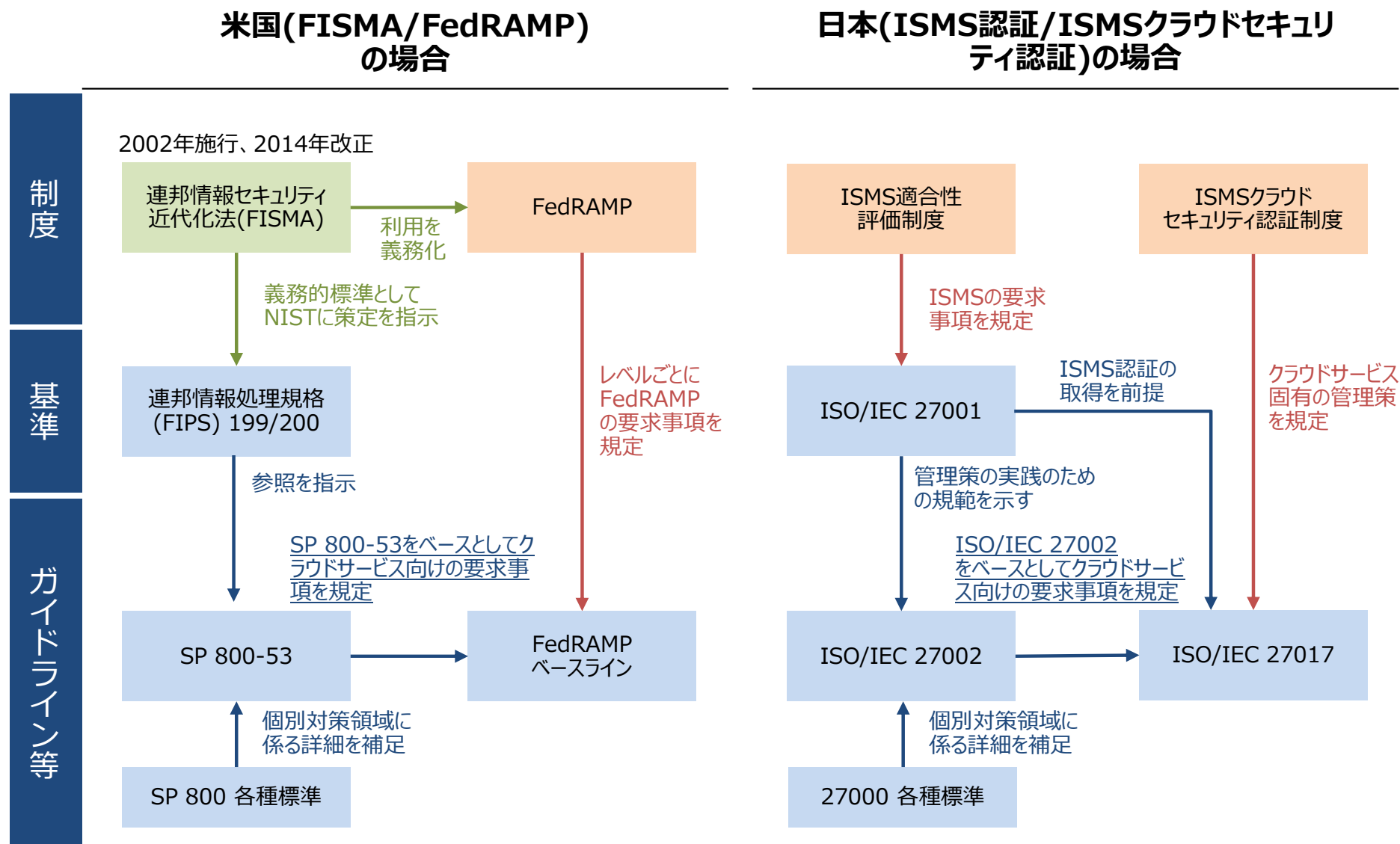
The Federal Risk and Authorization Management Program

- NIST SP 800-53の管理策の内容をFedRAMP Security Controls Baselineで引用しているが、分類に差異がみられる。
- また、個別の内容においてもFedRAMP Security Controls BaselineにFedRAMP固有の管理策やパラメータが設定されている。

比較観点	NIST SP 800-53とFedRAMP Security Controls Baselineの比較結果
各管理策の分類	• NIST SP 800-53では20分類であるが、FedRAMP baselineでは以下の項目を除いた18分類となっており、<u>2分類少ない</u>。 ✓ <u>個人情報の取扱いおよび透明性</u>: 実施要否は各機関の裁量にゆだねられる ✓ <u>プログラムマネジメント</u>: 機関側で実施するため、対象外
個別の管理策	• NIST SP 800-53の管理策の規定を<u>FedRAMP Security Controls Baseline</u>で引用しているが、<u>個別にFedRAMP baselineで追加している管理策がみられる</u>。 • 個別にFedRAMP Security Controls Baselineの<u>パラメータ(例: 調査の頻度)</u>を設けている管理策がみられる。

米国と日本の比較

- 米国(FISMA/FedRAMP)と日本(ISMS認証/ISMSクラウドセキュリティ認証の場合)を比較した場合、ベースとなるガイドラインからクラウドサービス向けのガイドラインを定めている点で共通している。



Executive Order 13636

- 大統領令13636は、民間部門と協力して、既存の自主的なコンセンサス基準と業界のベストプラクティスを特定し、それらをサイバーセキュリティフレームワークに組み込むようNISTに命じた。

1.2.1 米国における制度やガイドライン等

名称	Executive Order 13636—Improving Critical Infrastructure Cybersecurity		
国・地域	米国	策定者	ホワイトハウス
適用分野	重要インフラ分野	遵守義務の有無	なし
対象者	政府機関		
概要	- 大統領令13636は、サイバーリスクを管理するための<u>重要インフラの中核的な能力のレベルを高めることを目的</u>として、に署名された。これは、(1)情報共有、(2)プライバシー、(3)サイバーセキュリティ対策の採用という3つの主要分野に焦点を当てることによって行われるとされている。 - 重要インフラ保護強化に向けて、官民でのサイバーセキュリティ関係の情報共有体制構築に向けた課題の洗い出し、必要な法制度の検討、技術的なソリューションの策定等にむけた作業期限を設定し、DHSやDOD、NISTに作業を指示した。例えば、民間部門と協力して、<u>既存の自主的なコンセンサス基準と業界のベストプラクティスを特定し、それらをサイバーセキュリティフレームワークに組み込む</u>ようNISTに命じた。 <u>サイバー攻撃が深刻化し</u>、政府、個人、民間企業が負担した費用が、大統領令署名前年に3,000億ドルに達していたことや、<u>米国の重要インフラ</u>の安全の維持管理について<u>政府が規制してこなかった</u>ことが、<u>大統領令署名につながった</u>と指摘されている。^{*1}		
普及状況	-		
URL	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636		

^{*1} NICT北米連携センター「米国における重要インフラのサイバーセキュリティ確保に関する検討状況の調査報告書」より。その他にもサイバーセキュリティ法案(Cybersecurity Act of 2012、Cyber Intelligence Sharing and Protection Act)が2回先送りになったことも大統領令署名の一因となったと指摘されている。

The NIST Cybersecurity Framework (CSF) 2.0

- サイバーセキュリティフレームワークでは、産業界、政府機関、その他の組織がサイバーセキュリティリスクを管理するためのガイダンスを提供。2024年2月に2.0版がリリース。

1.2.1 米国における制度やガイドライン等

名称	The NIST Cybersecurity Framework (CSF) 2.0		
国・地域	米国	策定者	NIST
適用分野	サイバーセキュリティ全般	遵守義務の有無	なし
対象者	- サイバーセキュリティプログラムの策定と指導を行う個人 - リスク管理に係る主体(経営幹部、取締役会、買収の専門家、技術の専門家、リスク管理者、弁護士、人事の専門家、監査人) - サイバーセキュリティリスク管理の優先順位を設定し政策立案する主体(協会、専門家組織、規制当局)		
概要	- リスクベースの自主的なサイバーセキュリティフレームワークの開発を求めている大統領令13636に基づき、NISTによって作成されたサイバーセキュリティフレームワークは、組織がサイバーセキュリティリスクを管理するための業界標準とベストプラクティスのセット。 2014年2月に1.0版が公表され、2018年4月に1.1版が公表された後、<u>2024年2月に2.0版が正式に公表</u>された。 2.0版では、<u>産業界、政府機関、その他の組織がサイバーセキュリティリスクを管理するためのガイダンス</u>を提供している。		
普及状況	米国の約35%の企業がサイバーセキュリティフレームワークに準拠^{*1}		
URL	https://www.nist.gov/cyberframework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf		

*1 NRIセキュア「NRI Secure Insight 2022～企業における情報セキュリティ実態調査～」
<https://www.nri-secure.co.jp/download/insight2022-report>

TSS Cybersecurity Framework Implementation Guidance

- 本ガイダンスは、交通システムセクターの所有者とオペレータが、サイバーリスクの軽減を支援するためにサイバーセキュリティフレームワークの原則を適用するためのアプローチを提供する。

1.2.1 米国における制度やガイドライン等

名称	TSS Cybersecurity Framework Implementation Guidance		
国・地域	米国	策定者	CISA
適用分野	交通システム分野	遵守義務の有無	なし
対象者	- 交通システムセクターの所有者 - 交通システムセクターのオペレータ		
概要	- 本ガイダンスは、交通システムセクターの所有者とオペレータが、サイバーリスクの軽減を支援するために <u>NIST サイバーセキュリティフレームワークの原則を適用するためのアプローチを提供</u> する。 - 組織は実施ガイダンスを使用して、以下を行うことができるとしている。 ✓ 現在のサイバーセキュリティの状況を把握する。 ✓ 既存のサイバーリスク管理プログラムを強化する機会を特定する。 ✓ フレームワークの実施を支援する既存のツール、標準、ガイドを見つける。 ✓ リスク管理の課題を社内外の利害関係者に伝える。		
普及状況	-		
URL	https://www.cisa.gov/resources-tools/resources/transportation-systems-sector-cybersecurity-framework-implementation-guide		

The Cybersecurity Maturity Model Certification 2.0

- 本プログラムは、国防総省が請負業者や下請業者と共有する機密性の高い非分類情報(CUI)の保護を強化するために設計されている。本プログラムのレベル2は NIST SP 800-171に相当する。開発中のレベル3は、NIST SP 800-172要求事項のサブセットに基づいている。

1.2.1 米国における制度やガイドライン等

名称	The Cybersecurity Maturity Model Certification 2.0 (CMMC)		
国・地域	米国	策定者	DoD(米国国防総省)
適用分野	防衛分野	遵守義務の有無	あり
対象者	・ DoDと契約を行う請負業者や下請け業者		
概要	- 本プログラムは、防衛産業基盤パートナーに対する国防総省の情報セキュリティ要件に沿ったもの。<u>国防総省が請負業者や下請業者と共有する機密性の高い非分類情報(CUI)の保護を強化するために設計</u>されている。 - 本プログラムは、政府調達の際に請負業者や下請け業者が、管理された非機密情報を処理する取得プログラムやシステムに適用されるサイバーセキュリティ要件を満たしていることを、国防総省が保証する。 - CMMC 2.0 では、<u>アドバンスレベル(レベル2)は NIST SP 800-171に相当する</u>。現在*1開発中の<u>エキスパートレベル(レベル3)は、NIST SP 800-172要求事項のサブセット</u>に基づいている。		
普及状況	(CMMC 2.0 モデルは現在検討中)		
URL	https://dodcio.defense.gov/CMMC/About/		

*1 調査(2024年5月20日)時点

The Cybersecurity Maturity Model Certification 2.0

- CMMCでは、SP 800-171やSP 800-172に基づいた要求事項が規定されている。
- SP 800-172はSP 800-171の基本セキュリティ要件と派生セキュリティ要件を補足する。

CMMC Model 2.0

SP 800-171関連文書

レベル 3	✓ 以下の要求事項(110個以上)に準拠 ➤ NIST SP800-172 ➤ NIST SP800-171
レベル 2	✓ 以下の要求事項(110個)に準拠 ➤ NIST SP800-171
レベル 1	✓ 15個の要求事項に準拠

SP 800-172 Rev. 2
 CUIを保護するための拡張セキュリティ要件: NIST SP 800-171の補足

拡張セキュリティ要件は、[SP 800-171の基本セキュリティ要件と派生セキュリティ要件を補足](#)する。重要なプログラムや価値の高い資産で扱われるCUIの機密性保護に[推奨される高度なセキュリティ要件を提供](#)する。

CUIの機密性を保護するための[推奨セキュリティ要件を提供](#)する。

SP 800-171 Rev. 3
 連邦政府外のシステムと組織における管理された非格付け情報(CUI)の保護

SP 800-172A
 管理された非格付け情報向け高度セキュリティ要件の評価

SP 800-172で提示されているセキュリティ要件への準拠を[評価するための評価手順及び方法論を提供](#)する。

SP 800-171A Rev. 3
 管理された非格付け情報向けセキュリティ要件の評価

SP 800-171で提示されているセキュリティ要件への準拠を[評価するための評価手順及び方法論を提供](#)する。

[参考] FedRAMPに係る取組

- FedRAMP PMO は、NIST と共同で、Open Security Controls Assessment Language (OSCAL)と呼ばれる共通の機械可読言語の開発を通じて、承認パッケージのデジタル化に取り組んでいる。

OSCALの開発

- テキストベースの手作業によるアプローチ(例:ワークシートやスプレッドシートを使用)から、標準化された機械可読形式に移行することを目標として、FedRAMP PMOはNISTと共同でOSCALを開発。

構成要素	内容
ルート要素	ファイル本体内のコンテンツの種類(例:カタログ、プロファイル)を示す。
UUID	特定のドキュメントインスタンスを識別するID(Universally Unique Identifier)を示す。
メタデータ	- タイトル、タイムスタンプ等を示す。 - メタデータは、役割、当事者(人、チーム、組織)、場所を定義するためにも使用される。
モデル固有のボディ	ボディ部分。OSCALファイルの本文は、モデルごとに異なる。
バックマター	リンクされたリソースや添付されたリソースを示す。また、引用を含むことがある。

OSCALの開発のメリット

- システムのセキュリティ情報が OSCALで表現されることで、セキュリティ専門家は、セキュリティ評価、監査、継続的モニタリングのプロセスを自動化できるようになる。

ステークホルダー	ステークホルダーのメリット
クラウドサービスプロバイダー	<u>システムセキュリティプランをより迅速かつ正確に作成</u>し、レビューを受ける前にコンテンツの多くを検証可能。
サードパーティ評価機関(3PAO)	クラウド評価作業の<u>計画、実行、レポート作成を自動化可能</u>。
政府機関	FedRAMPセキュリティ承認パッケージの<u>レビューを迅速化可能</u>。

- 認証制度の運用が進んでいるFedrampでは認証プロセスの自動化が進められている。
- 成熟度モデルの検討にあたって優先度は低いが、必要な文書が揃った後に別途検討することもある。

SP 800-63-4 (Initial Public Draft)

- 本ガイドラインは、デジタルIDサービスを実装する連邦機関向けに技術要件を提供するもの。

1.2.1 米国における制度やガイドライン等

名称	SP 800-63-4 (Initial Public Draft) Digital Identity Guidelines ^{*1}		
国・地域	米国	策定者	NIST
適用分野	政府情報システム	遵守義務の有無	あり
対象者	- 政府機関 - 請負事業者 等		
概要	- 本ガイドラインは、<u>デジタルIDサービスを実装する連邦機関のための技術要件を提供するもの</u>であり、このガイドラインは、ネットワークを介して政府情報システムとやり取りするユーザ(職員、請負業者、個人など)の ID 証明および認証を対象としている。 - 本ガイドラインは、<u>ID 証明、登録、認証子、管理プロセス、認証プロトコル、フェデレーション、および関連アサーションの各分野における技術要件を定義</u>する。 - 本ガイドラインの関連文書として、以下が策定されている。 ✓ SP 800-63A:登録とIDの証明 ✓ SP 800-63B:認証とライフサイクル管理 ✓ SP 800-63C:フェデレーションとアサーション 2006年に初版が公開されたNIST SP 800-63は、米国各省庁および各政府機関長官宛てに発行したガイダンスである OMB M-04-04の下位文書となる。OMB M-04-04ではレベル分け(レベル1～4)をしているが、<u>SP 800-63-4では、その考え方に基づいてIAL(ID証明プロセス)、AAL(認証プロセス)、FAL(フェデレーションプロセス)においてレベル分け(レベル1～レベル3)</u>をしている。		
普及状況	-		
URL	https://pages.nist.gov/800-63-4/		

*1 調査時点(2024年5月27日)でNIST SP800-63 ver4のドラフト版は公開済み

OMB M-04-04及びNIST SP800-63-3

- OMB M-04-04では、レベル1～レベル4までの保証レベルを定義している。NIST SP800-63-3からは、下位の文書にあたるNIST SP800-63(電子的認証に関するガイドライン)では、各保証レベル別の技術的要求事項を具体化。

OMB M-04-04

レベル4	主張された身元識別情報の確実性について非常に高い信頼性が必要なトランザクションに適している。利用者は、レベル4のクレデンシャルを提示することで、追加の身元識別アサーション管理策の必要なしに、身元を主張して、アクセスが限定されているWebリソースにアクセスできる。
レベル3	主張された身元識別情報の確実性について高い信頼性が必要なトランザクションに適している。利用者は、レベル3のクレデンシャルを使用することで、追加の身元識別アサーション管理策の必要なしに、アクセスが限定されているWebサービスにアクセスできる。
レベル2	最終的には、信頼性とは、 <u>主張された識別情報が正確であることである</u> 。レベル2のクレデンシャルは、政府機関が身元識別のアサーションを最初に必要とする、国民との幅広い業務にとって適切である。
レベル1	主張された識別情報の信頼性がほぼ、あるいはまったくない。たとえば、レベル1のクレデンシャルを持つ人は、Webページ上の項目を後で参照できるように、ブックマークできる。

NIST SP800-63-3

分類	レベル	説明
Identity Assurance Level (IAL)	3	識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者
	2	サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
	1	本人確認不要、自己申告での登録でよい
Authenticator Assurance Level (AAL)	3	2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの(ハードウェアトークン等)である必要
	2	2要素認証が必要、2要素目の認証手段はソフトウェアベースのものでよい
	1	単要素認証でよい
Federation Assurance Level (FAL)	3	Lv.2に加え、Holder-of-Key Assertion(ユーザごとの鍵とIDプロバイダが発行したAssertionを紐づけてRP(サービス提供者)に送り、RP(サービス提供者)はユーザがそのAssertionに紐づいた鍵を持っているかを確認)の利用
	2	署名に加え、対象RP(サービス提供者)のみが復号可能な暗号化
	1	Assertionへの署名が必要

[参考] OMB" M-04-04 MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES"

<https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025320.pdf>

JIPDEC「NIST SP 800-63-3の概要と今回の改訂がもたらす影響」

<https://www.jipdec.or.jp/library/report/20171127.html>

第2版まではOMB M-04-04に示された保証レベルに基づき要件が定められていたが、NIST SP800-63-3からは、各機能に対応するレベルを個別に選択することを求めている。

M-21-30

- 大統領令14028に基づいて発行されたOMB M-21-30では、各省庁が利用・調達している「重要なソフトウェア」を60日以内に特定し、当該ソフトウェアに対して必要なセキュリティ対策を1年以内に実装することを各省庁へ指示。
- また、各省庁のセキュリティ対策にあたって、NISTが公開したガイダンス*¹に遵守することを求めた。

2.1 米国における制度やガイドライン等

名称	M-21-30		
国・地域	米国	策定者	OMB(米国行政管理予算局)
適用分野	政府情報システム	遵守義務の有無	あり
対象者	各政府機関(及び長官)		
概要	- OMB M-21-30では、各省庁に対し、<u>各省庁が利用・調達している「重要なソフトウェア」を60日以内に特定</u>し、当該ソフトウェアに対して<u>必要なセキュリティ対策を1年以内に実装</u>することを指示。また、各省庁のセキュリティ対策にあたって、<u>NISTが公開したガイダンスに遵守することを求めた</u>。 - NISTやCISAに対して、<u>「重要なソフトウェア」に含まれるソフトウェアカテゴリの定義</u>や、当該<u>ソフトウェアのセキュリティ対策に係るガイドラインを必要に応じて更新することを要求</u>。 - なお、大統領令14028のセクション4「ソフトウェア・サプライチェーンのセキュリティ向上」では、NISTに対し、重要ソフトウェアのセキュリティ対策に関するガイダンスを発行するよう指示し、さらにOMBに対し、各省庁がそのガイダンスに従うよう要求するよう指示している。		
普及状況	-		
URL	https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf		

M-23-16

- OMB M-23-16では、M-22-18で確立された要件を強化し、安全なソフトウェア開発プラクティスの重要性を再確認した。また、省庁がソフトウェア製作者から証明書を収集するスケジュールを延長した。

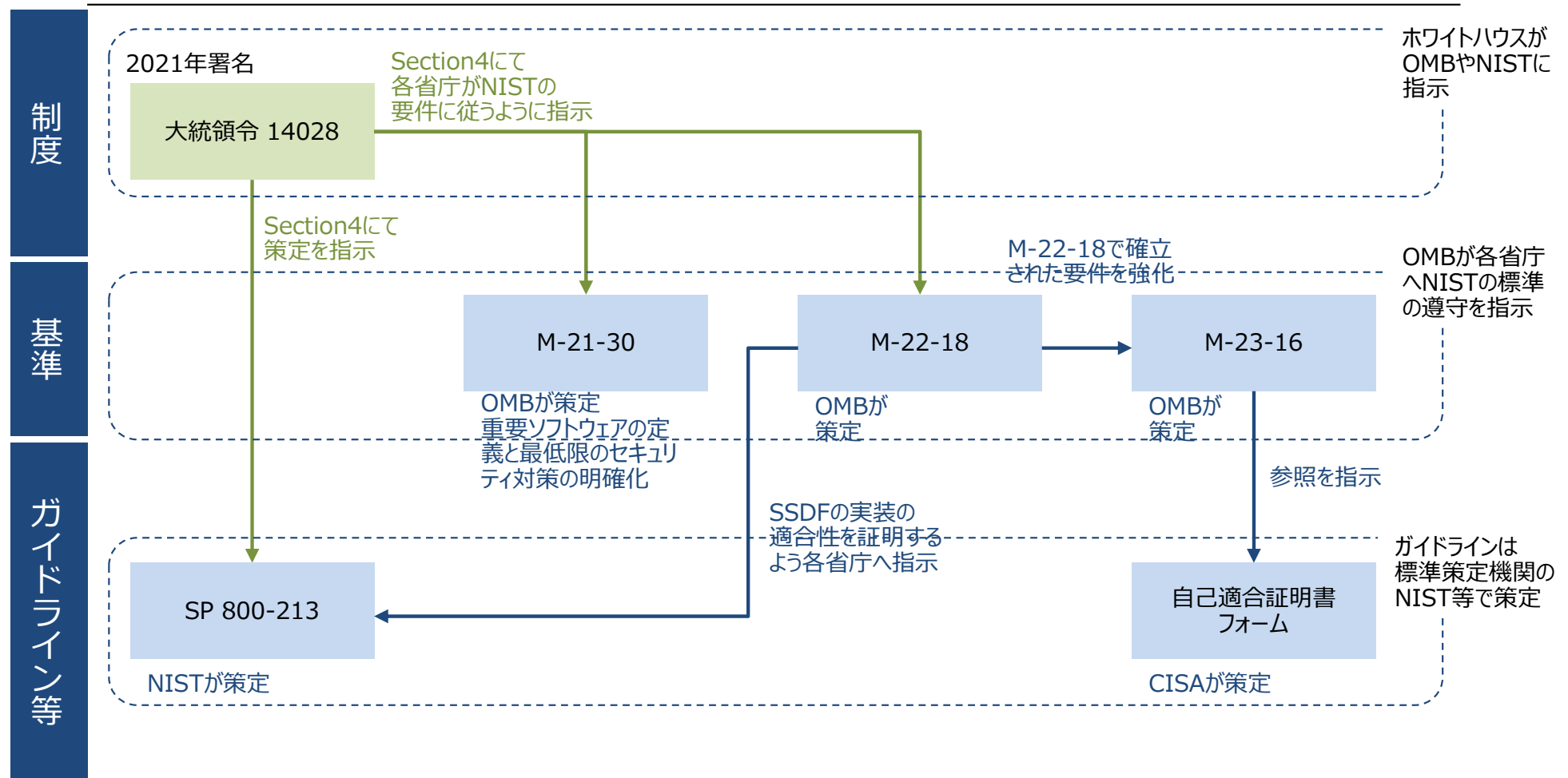
.2.1 米国における制度やガイドライン等

名称	M-23-16		
国・地域	米国	策定者	OMB(米国行政管理予算局)
適用分野	政府情報システム	遵守義務の有無	あり
対象者	各政府機関(及び長官)		
概要	- OMB M-23-16では、<u>M-22-18で確立された要件を強化</u>し、安全なソフトウェア開発プラクティスの重要性を再確認した。また、省庁がソフトウェア製作者から証明書を収集するスケジュールを延長した。具体的には以下を定める。 ✓ <u>自己適合証明書の取得期限の延長</u> ✓ <u>M-22-18の要求事項の明確化</u> ✓ <u>自己適合証明できない場合における補足的なガイダンス</u> - M-22-18では、政府関係機関は、<u>安全なソフトウェア開発手法(以下、SSDF)の実装を証明できるソフトウェアベンダーが提供するソフトウェアのみを使用すべきであるとしており</u>、機関は、以下を実施する必要があるとしている。 ✓ 機関は、ソフトウェア使用前に、SSDFの実装の適合性を証明する自己適合証明書の取得をソフトウェアベンダーへ要求する。 ✓ 機関は、必要に応じて、自己適合証明書に付随する成果物(SBOM等)をソフトウェアベンダーから入手することができる。		
普及状況	-		
URL	https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf		

ソフトウェアサプライチェーンセキュリティに関わる文書の関係性

- 大統領令14028に基づき、NIST SP 800-213等のガイドラインが策定されるとともに、各省庁へかかるガイドラインに従うよう指示をするM-21-30が公開された。

ソフトウェアサプライチェーンセキュリティに関わる文書の関係性



The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

- 本セキュリティルールは、特定の医療情報のプライバシーとセキュリティを保護する規制を策定することを義務づけたHIPAAにより策定された。個人の健康情報のプライバシー保護や新しいテクノロジーの採用を促進することを目的として規定を定めている。

2.1 米国における制度やガイドライン等

名称	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule		
国・地域	米国	策定者	米国保健社会福祉省(HHS)
適用分野	医療情報システム分野	遵守義務の有無	あり
対象者	- HHS長官がHIPAAに基づく基準を採用した取引に関連して電子形式で健康情報を送信する医療提供者 - 上記に関連するビジネスアソシエイト^{*1}		
概要	1996年に“The Health Insurance Portability and Accountability Act of 1996(HIPAA)”(医療保険の相互運用性と説明責任に関する法律)により、<u>HHSの長官は、特定の医療情報のプライバシーとセキュリティを保護する規制を策定することが義務付けられた</u>ため、この要件を満たすために、HHSは<u>HIPAAプライバシールールとHIPAAセキュリティルール</u>として知られているものを公開した。 - セキュリティ規則の主な目的は、<u>個人の健康情報のプライバシーを保護する</u>と同時に、対象事業体が患者ケアの質と効率を向上させるための<u>新しいテクノロジーを採用できるようにすること</u>。 - セキュリティ規則は、対象となる事業体に対し、電子保護医療情報を保護するための合理的かつ適切な管理上、技術上、及び物理的な保護手段を維持することを要求している。具体的には、対象となる事業体は以下の条件を満たす必要がある。 ✓ <u>作成、受信、維持、または送信するすべての電子保護医療情報の機密性、完全性、および可用性を確保する。</u> ✓ <u>情報のセキュリティまたは完全性に対する合理的に予想される脅威を特定し、保護する。</u> ✓ <u>合理的に予想される、許可されない使用または開示から保護する。</u> ✓ <u>従業員によるコンプライアンスを確保する。</u>		
普及状況	-		
URL	https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html		

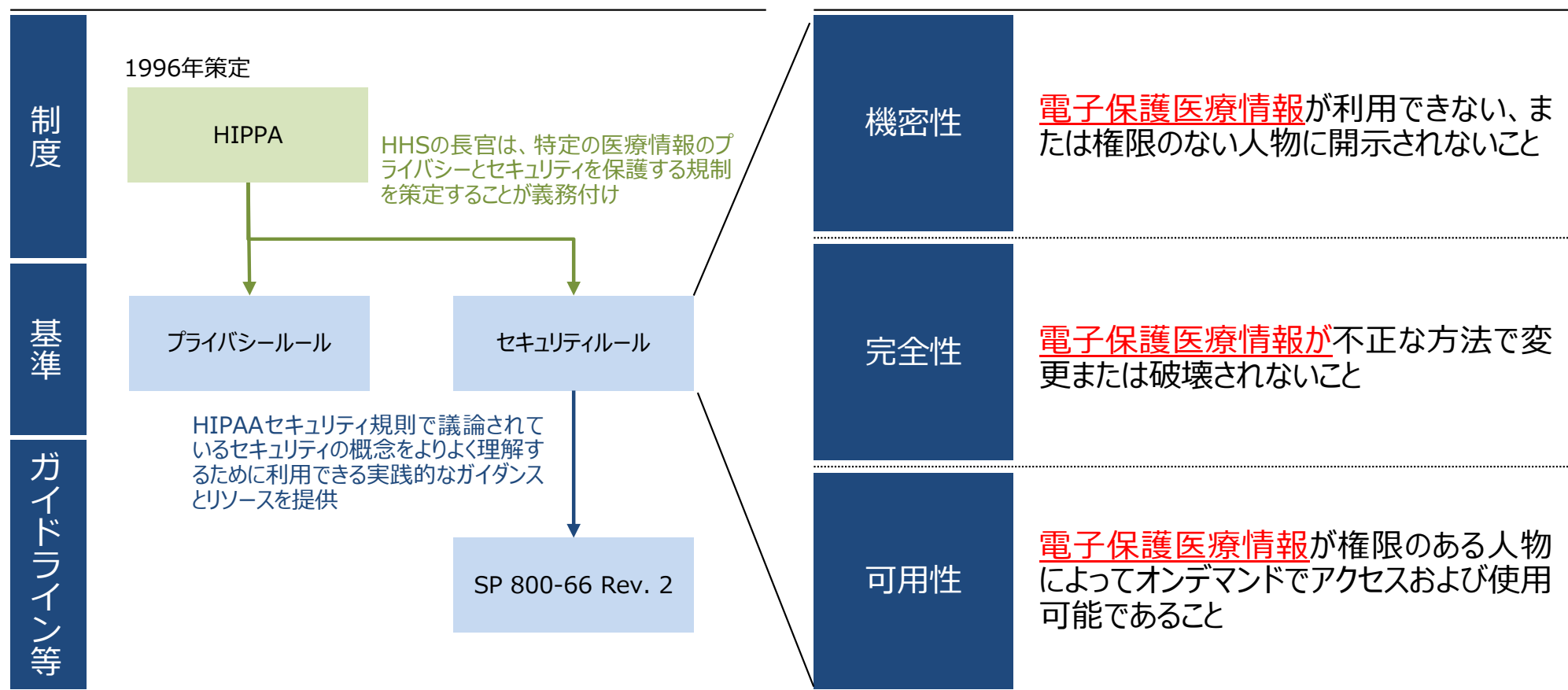
^{*1} ビジネスアソシエイト: 対象となる医療提供者に代わって保護医療情報の使用または開示を伴う活動等を行う個人/団体、または対象となる医療提供者にサービスを提供する個人/団体

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule

- HIPPAは、特定の医療情報のプライバシーとセキュリティを保護する規制を策定することをHHS長官に義務づけた。かかる規定に従い、セキュリティルール及びプライバシールールが策定。
- HIPPAの目的は、対象となる事業体が保有または送信する電子保護医療情報の完全性及び機密性、可用性を保護することであるため、セキュリティルールにおいて完全性、機密性、可用性を独自に定義。

医療情報保護に関わる文書の関係性

HIPPA Security Ruleにおける定義



Cybersecurity in Medical Devices

- FDAは、2医療機器の製造事業者が実施すべき推奨事項をまとめた以下の2つの文書を策定。
 - ✓ Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
 - ✓ Postmarket Management of Cybersecurity in Medical Devices

2.1 米国における制度やガイドライン等

名称	Cybersecurity in Medical Devices		
国・地域	米国	策定者	食品医薬品局(FDA)
適用分野	医療機器分野	遵守義務の有無	あり
対象者	ソフトウェア(ファームウェアを含むまたはプログラマブル・ロジックを含む(医療)機器^{*1}の製造事業者		
概要	- FDAは、2014年に市販前の期待に対応するサイバーセキュリティガイダンスの最終版“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”(以下、本スライド内では①と示す)を、2016年にそれを補完するガイダンス“Postmarket Management of Cybersecurity in Medical Devices”(以下、本スライド内では②と示す)を発行した。 ✓ ①は、医薬品医療機器・放射線衛生センター(CDRH)または生物製剤評価研究センター(CBER)に申請書類を提出する際に<u>掲載すべきサイバーセキュリティ情報に関する推奨事項</u>を記載したもの ✓ ②はFDAの市販後の推奨事項を明確にし、製造業者は医療機器の市販後管理の一環として、サイバーセキュリティの脆弱性と悪用を監視、特定、対処すべきであることを強調するもの - 連邦食品・医薬品・化粧品法(Federal Food, Drug, and Cosmetic Act)の第524B条「医療機器のサイバーセキュリティの確保」が記載されており、<u>製造事業者はサイバーセキュリティ要件を満たしていることを確認するための情報を提出する必要があると規定されている</u>。①はかかる義務を果たすのを支援することを意図しているとされている。 - また、①では、安全で効果的な機器を製造し、維持することを目的としてセキュア製品開発フレームワーク(Secure Product Development Framework: SPDF)によるリスクの管理について説明しているが、医療施設であればNIST CSF内でもかかるリスクを管理可能としている。また、「暗号技術」においてNISTが推奨する最新の暗号化標準(例:FIPS 140-3)の使用を推奨しており、①において既存のNIST文書を適宜参照している。		
普及状況	-		
URL	https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices		

- 本ガイダンスは、化学分野における重要インフラの所有者および運営者によるNIST Cybersecurity Frameworkの利用を支援するために開発された。

2.1 米国における制度やガイドライン等

名称	Chemical Sector Cybersecurity Framework Implementation Guidance		
国・地域	米国	策定者	サイバーセキュリティ・インフラセキュリティ庁 (CISA) 化学分野調整会議(SCC) 政府調整会議(GCC)
適用分野	化学分野	遵守義務の有無	なし
対象者	- 化学分野における重要インフラの所有者 - 化学分野における重要インフラの運営者		
概要	- 本ガイダンスは、<u>化学分野における重要インフラの所有者および運営者によるNIST Cybersecurity Frameworkの利用を支援するために開発された</u>。本ガイダンスで提供される情報は、組織が現在のサイバーセキュリティの実践を評価し、ギャップを明らかにするのに役立つツールを特定し、サイバーセキュリティの目標を決定するのに役立つ。 - 本ガイダンスにおいて、NIST Cybersecurity Frameworkの実装プロセスを説明。 - 添付Aでは、「フレームワークの実施を支援するサイバーセキュリティツールとリソース」を示す。添付Aの中で、NIST Cybersecurity Frameworkの各機能、カテゴリー、サブカテゴリーで説明されているサイバーセキュリティの成果を達成するための手法を参考文献と併せて示している。(<u>化学分野において個別に追加/削除されているカテゴリ/サブカテゴリは見当たらなかった</u>)		
普及状況	(管見の限り、その利用率については確認できなかった。)		
URL	https://www.cisa.gov/resources-tools/resources/chemical-sector-cybersecurity-framework-implementation-guidance		

Chemical Sector Cybersecurity Framework Implementation Guidance

- 添付Aでは、「フレームワークの実施を支援するサイバーセキュリティツールとリソース」を示す。添付Aの中で、NIST Cybersecurity Frameworkの各機能、カテゴリー、サブカテゴリーで説明されているサイバーセキュリティの成果を達成するための手法を参考文献と併せて示している。

NIST Cybersecurity Frameworkで示された機能、カテゴリー、サブカテゴリーを示す。

各サブカテゴリーに示された要件を満たすために化学部門のサイバーセキュリティリスク管理に係るガイダンスが利用可能かを示す。(「×」は利用可能)

Function	Category	Subcategory	CSAT	RBPS 8	RCSC	CRR	CSET	BCEB
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	X	X	X	X	X	X
		ID.AM-2: Software platforms and applications within the organization are inventoried	X	X	X	X	X	X
		ID.AM-3: Organizational communication and data flows are mapped	X	X	X	X	X	X
		ID.AM-4: External information systems are catalogued		X	X	X	X	X
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value			X	X	X	X
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established		X		X	X	X

<参考>

- CSAT(Chemical Security Assessment Tool):ウェブベースの自己評価プラットフォーム内で基準を満たす施設を特定するためのツール
- PBPS 8(Risk-Based Performance Standard 8- Cyber):サイバー妨害行為を抑止する方法に関する基準を提供
- RCSC(American Chemical Council Responsible Care Security Code Cybersecurity Guidance):NIST CSFの適用に関する実践的なガイダンスを提供
- CRR(Cyber Resilience Review):10の領域(例:リスク管理、インシデント管理)で企業のプログラムと実務を評価
- CSET(Cybersecurity Evaluation Tool):制御システム及びITシステムネットワークセキュリティ対策を評価するためのプロセスをガイド
- BCEB(Baldrige Cybersecurity Excellence Builder Version 1.1):サイバーセキュリティのリスク管理の有効性やソシキのパフォーマンス等に対する自己評価ツールを提供

Top Cyber Actions for Securing Water Systems

- CISA、EPA、FBIによって公開された本文書は、リスクを軽減し、悪意のあるサイバー活動に対するレジリエンスを向上させるために実行可能なサイバーアクションを概説。

2.1 米国における制度やガイドライン等

名称	Top Cyber Actions for Securing Water Systems		
国・地域	米国	策定者	サイバーセキュリティ・インフラセキュリティ庁 (CISA) 環境保護庁(EPA) 連邦捜査局(FBI)
適用分野	上下水道分野におけるITシステム及びOTシステム	遵守義務の有無	なし
対象者	上下水道分野においてITシステム及びOTシステムを運用している事業者		
概要	- CISA、EPA、FBIが共同でファクトシートを公開。本ファクトシートは、上下水道分野においてITシステム及びOTシステムを運用している事業者が<u>リスクを軽減し、悪意のあるサイバー活動に対するレジリエンスを向上させるために実行可能なサイバーアクションを概説する</u>。また、これらのアクションをサポートするための無料のサービス、リソース、ツールを提供する。 - サイバーアクションは以下の通り。 ✓ 公衆向けインターネットへの露出を減らす ✓ 定期的なサイバーセキュリティ評価の実施 ✓ デフォルトパスワードの即時変更 ✓ 運用技術/情報技術資産のインベントリの実施 ✓ サイバーセキュリティ・インシデント対応・復旧計画の策定と実施 ✓ OT/ITシステムのバックアップ脆弱性への露出を減らす ✓ サイバーセキュリティ意識向上トレーニングの実施		
普及状況	(管見の限り、その利用率については確認できなかった。)		
URL	https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems		

Top Cyber Actions for Securing Water Systems

- サイバーリスクを低減し、サイバー攻撃に対するレジリエンスを向上させるために、上下水道システムがすぐに実行可能なサイバーアクションが示されている。
- ITだけではなくセキュリティ面で脆弱になりやすいOTシステムを対象に含めサイバーアクションが示されている。

サイバーアクション	内容
公衆向けインターネットへの露出を減らす	サイバー・ハイジーン・サービスを利用して、重要な資産の公衆向けインターネットへの露出を減らす。 <u>コントローラーやリモートターミナルユニット(RTU)などのOTデバイスは、インターネットに接続されている場合、サイバー攻撃の標的になりやすい。</u>
定期的なサイバーセキュリティ評価の実施	定期的にサイバーセキュリティ評価を実施し、 <u>OTおよびITシステム内の既存の脆弱性を把握する。アセスメントを実施することで、OTネットワークとITネットワークの両方における脆弱性の特定、評価、および緩和の優先順位付けが可能になる。</u>
デフォルトパスワードの即時変更	接続されたインフラを含むすべての水道システムに、一意で強固かつ複雑なパスワードを要求する。弱いデフォルトパスワードや安全でないパスワードは発見されやすく、悪用されやすく、サイバー脅威者が水道システムの運用プロセスに変更を加えることを許してしまう可能性がある。これは、公衆衛生と安全性に悪影響を及ぼす可能性がある。デフォルトまたは安全でないパスワードを変更し、可能であれば多要素認証を導入する。脅威行為者が OT システムにアクセスすることを困難にするため、電子メールなどの IT インフラに MFA を多要素認証することに重点を置く。メーカーにデフォルトパスワードのデフォルトパスワードの廃止をメーカーに求めることを検討する。
運用技術/情報技術資産のインベントリの実施	ソフトウェアとハードウェアの資産目録を作成し、何を保護する必要があるかを理解する。インターネットに接続されたデバイスや、手作業が不可能なデバイスに、最初の取り組みを集中させる。モニタリングを使って、ネットワーク上で通信しているデバイスを特定する。
サイバーセキュリティ・インシデント対応・復旧計画の策定と実施	サイバーインシデントが発生する前に、インシデント対応の行動、役割、責任、連絡先、報告方法などを理解し、潜在的な標的に対する備えを確実にする。
OT/ITシステムのバックアップ脆弱性への露出を減らす	<u>OT/ITシステムを定期的にバックアップし、侵害が発生した場合に既知の安全な状態に回復できるようにする。</u> バックアップ手順をテストし、バックアップをネットワーク接続から隔離する。NIST 3-2-1ルールを実施する。 3:3つのコピーを保管する 2:バックアップは2つの異なるメディアに保存する。 1:オフサイトにコピーを1部保存する
サイバーセキュリティ意識向上トレーニングの実施	全従業員がサイバーセキュリティの重要性、サイバー攻撃の予防と対応方法を理解できるよう、最低でも毎年サイバーセキュリティに関する意識向上トレーニングを実施する。

サイバーリスクを低減し、サイバー攻撃に対する耐性を向上させるために、上下水道分野の事業者が今すぐ実行できるサイバーアクションの上位を示す

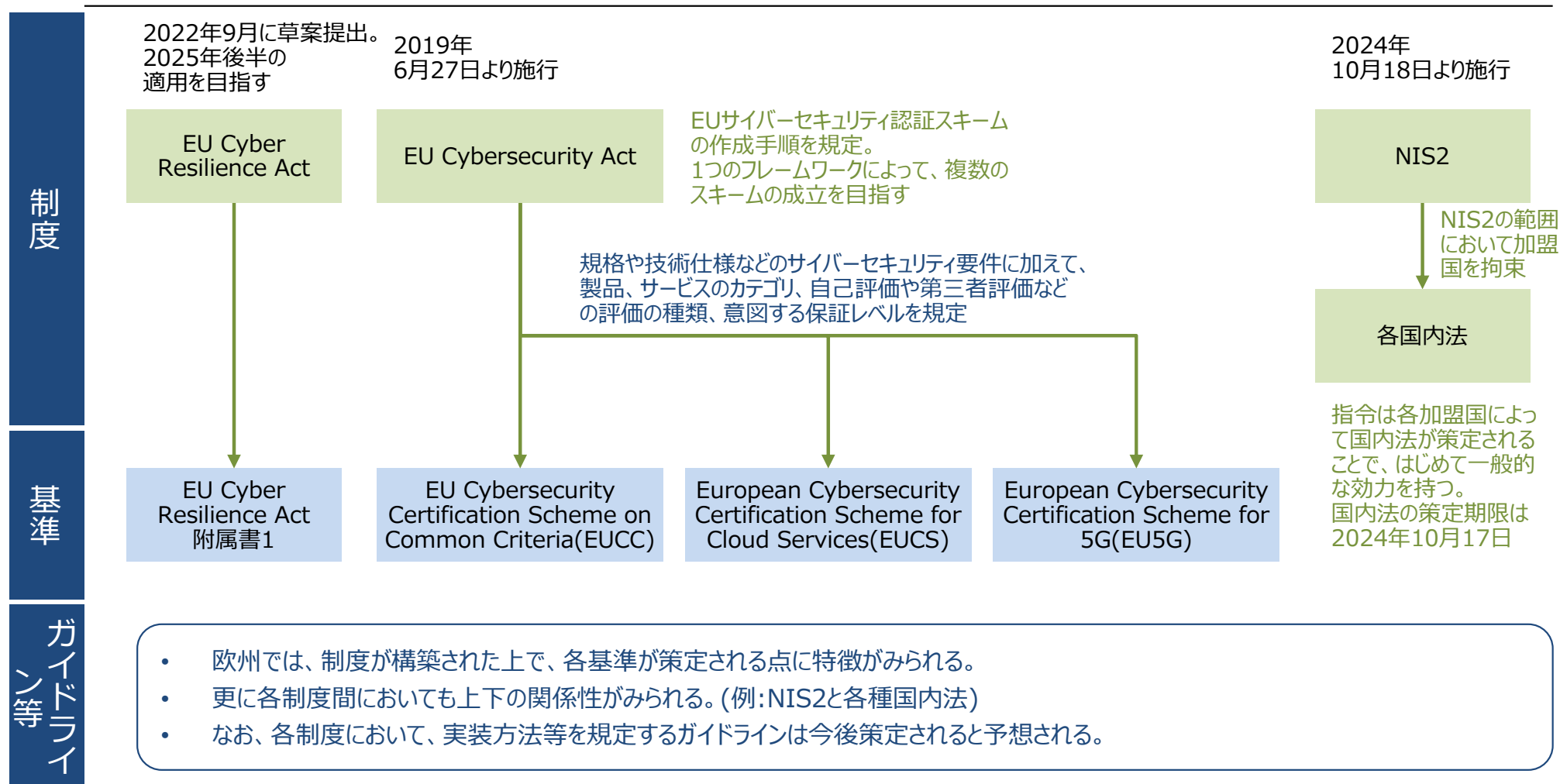


欧州関連

欧州のガイドライン等の関係性整理

- まずは制度(法/規則/指令等)が構築された上で、それらの要請を受ける形で各基準・ガイドラインが策定される点に、欧州の特徴がみられる。
- 各制度間であっても、上下の関係性がみられる場合がある。(例:NIS2と各国内法)

本調査の対象となった欧州のセキュリティ制度等



EU Cyber Resilience Act

- 本法は、デジタル要素を含む製品やソフトウェアを購入または使用する消費者や企業を保護することを目的として、製品の製造業者や小売業者に対してサイバーセキュリティに関する義務的な要件を導入。

2.1 欧州における制度やガイドライン等

名称	EU Cyber Resilience Act		
国・地域	欧州	策定者	欧州委員会
適用分野	デジタル製品	遵守義務の有無	あり
対象者	- デジタル要素を含む製品やソフトウェアの製造事業者 - デジタル要素を含む製品やソフトウェアの小売事業者		
概要	- 本法は、<u>デジタル要素を含む製品やソフトウェアを購入または使用する消費者や企業を保護</u>することを目的としている。このような製品の製造業者や小売業者に対して<u>サイバーセキュリティに関する義務的な要件を導入</u>することで、不十分なセキュリティ機能をなくし、この保護が製品のライフサイクル全体に及ぶようにするものである。 - 本法は以下のを保証する。 ✓ デジタル要素を含む製品やソフトウェアを市場に投入する際の、調和のとれたルール ✓ デジタル要素を含む製品の計画、設計、開発、保守を管理するサイバーセキュリティ要件の枠組み ✓ デジタル要素を含む製品のライフサイクル全体に対する注意義務の提供 - 本法が発効すれば、インターネットに接続されるソフトウェアや製品には、新基準に適合していることを示すCEマーキングが付けられることになる。製造業者や小売業者にサイバーセキュリティの優先順位を求めることで、顧客や企業はCEマークが付いた製品のサイバーセキュリティの信頼性を確信し、より良い情報に基づいた選択をすることができるようになる。		
普及状況	(発効前であるが、全ての事業者に遵守義務がある。)		
URL	https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act		

EU Cyber Resilience Act

- デジタル製品のうち、そのリスクの大きさによって認証方法(自己適合宣言/第三者認証)を定めている。
- デジタル製品共通のセキュリティ要求事項を附属書 I にて示している。

附属書 I にて、デジタル製品共通の「セキュリティ要求事項」を示す。

製造者は、SBOM作成、無料での更新プログラム提供を含む「脆弱性処理要件」を遵守し、製品が「セキュリティ特性要件」を満たすこと。自己適合宣言か第三者認証を選択

「デジタル製品」

重要ではあるがリスクの低いもの。第三者認証(該当する場合はEUCC)

- 以下の条件のどちらかを満たすとき、重要な製品に該当
 - ✓ 認証とアクセスの確保、侵入防止と検出、エンドポイントセキュリティまたはネットワーク保護を含む、他の製品、ネットワークまたはサービスのサイバーセキュリティにとって重要な機能を実行
 - ✓ 直接的な操作を通じて、多数の他の製品、またはそのユーザーの健康、セキュリティ、もしくは安全を脅かし、損害を与えたりする強度と能力において、重大な悪影響のリスクを伴う機能を製品が実行

「重要なデジタル製品」

「重要なデジタル製品」以外

いずれか選択

自己適合宣言

第三者認証
(型式認証)

第三者認証
(全数検査)

クラスI (低リスク)

EUCC

EUCCやEN規格
の対象外

EN規格
(欧州整合化規格)

いずれか選択

第三者認証
(型式認証)

第三者認証
(全数検査)

クラスII (高リスク)

いずれか選択

第三者認証
(型式認証)

第三者認証
(全数検査)

機密性の高いもの、
広範囲へ影響を及ぼすもの。第三者
認証を選択

The EU cybersecurity certification framework

- 認証の枠組みは、包括的な規則、技術要件、基準、手続きをセットとしたEU全体の認証スキームを提供。

2.1 欧州における制度やガイドライン等

名称	The EU cybersecurity certification framework		
国・地域	欧州	策定者	ENISA
適用分野	ICT製品やサービス	遵守義務の有無	なし
対象者	ENISA		
概要	- 認証の枠組みは、<u>包括的な規則、技術要件、基準、手続きをセットとしたEU全体の認証スキームを提供する</u>。このスキームに従って認証されたICT製品やサービスは、<u>指定された要件に適合していることを証明する</u>。 - 特に、EUサイバーセキュリティ法では、欧州の各スキームは以下を規定すべきとされている。 ✓ 対象となる製品・サービスのカテゴリー ✓ 規格や技術仕様などのサイバーセキュリティ要件 ✓ 自己評価や第三者評価などの評価の種類 ✓ 意図する保証レベル - EUサイバーセキュリティ法にのっとり、以下の分野で検討が推進されている。 ✓ <u>ICT製品</u>:EU Cybersecurity Certification Scheme on Common Criteria(EUCC) ✓ <u>クラウドサービス</u>:European Cybersecurity Certification Scheme for Cloud Services(EUCS) ✓ <u>5G</u>:The European Cybersecurity Certification Scheme for 5G(EU5G)		
普及状況	-		
URL	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework		

The EU cybersecurity certification framework

- EUサイバーセキュリティ法に基づき、各分野において任意の認証制度が立ち上がりつつある。
- EUCCでは、具体的な遵守事項等を規定した実施規則が公布されている。

EUサイバーセキュリティ法 (EU)規則2019/881

- EUサイバーセキュリティ認証フレームワークは、ICT製品、サービス、およびプロセスを対象とするEUサイバーセキュリティ認証スキームの作成手順を定めている。各スキームは、製品、サービス、またはプロセスの想定される使用に関連するリスクのレベルに基づいて、1つ以上の保証レベル(基本、実質的、高)を指定する。
- 1つのフレームワークによって、複数のスキームの成立を目指している。

EU Cybersecurity Certification Scheme on Common Criteria(EUCC)

- ICT製品を対象
- 国際スキームであるコモンクライテリアに基づく

European Cybersecurity Certification Scheme for Cloud Services(EUCS)

- クラウドサービスを対象
- ドラフトは公開済み。ECGC*¹からパブリックコメントに付される段階。

The European Cybersecurity Certification Scheme for 5G(EU5G)

- 5Gネットワークを対象
- AHWG *²内のパブリックコメントに付される予定。

実施規則(EU) 2024/482

- EUCCの実施規則は2024年02月27日に発効し、2025年02月27日に適用
- EUCCの役割、規則、義務、構造を規定

<参考>その他のスキームについて

- Artificial Intelligence**
ENISAは、人工知能に関するEU規則案の採択を踏まえ、AIがサイバーセキュリティ認証の対象となり得るかどうか等について検討中。なお、ENISAは欧州委員会から認証スキームの開発要請を受けていないため、この作業は準備段階にある。
- Managed Security Services**
Union Rolling Work Programme(URWP)に含まれており、サイバーセキュリティ法の改正には、ENISAがマネージドセキュリティサービスを認証する可能性が含まれることが予測されている。欧州サイバーセキュリティ機関は、このテーマに関する準備作業を開始。

*1 European Cybersecurity Certification Group *2 Ad Hoc Working Groups

NIS2指令

- NIS2指令は、EU域内でサービスを提供する、または活動を行う中規模(従業員50名)以上の主要エンティティまたは重要エンティティを対象にした規制。

2.1 欧州における制度やガイドライン等

名称	DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022(NIS2)		
国・地域	欧州	策定者	
適用分野	主要エンティティ分野*1 重要エンティティ分野*2	遵守義務の有無	あり
対象者	- 主要エンティティ - 重要エンティティ		
概要	- NIS2指令は、<u>EU域内でサービスを提供するまたは活動を行う中規模(従業員50名)以上の主要エンティティまたは重要エンティティを対象にした規制</u>であり、化学、医療機器、電気電子機器、光学機器、機械、自動車、輸送機器、宇宙、研究などの幅広い分野を対象に義務がかかる。 - NISからNIS2での変更点は、<u>①大幅な対象拡大、②サイバーセキュリティ・リスクマネジメントの強化、③インシデント報告内容・時限の明確化、④厳しい罰則金。</u> 2024年10月18日より施行。したがって、NIS2を踏まえた国内法の採択は2024年10月17日。		
普及状況	-		
URL	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684136497194		

*1 主要エンティティ:エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、飲料水、下水、デジタルインフラ、ICTサービスマネジメント、公的サービス、宇宙

*2 重要エンティティ:郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車・トレーラー、輸送機器）、デジタルプロバイダー、研究

NIS2指令

- 欧州の指令(Directive)によって、各欧州の国内法が規定される。
- NIS2を踏まえた国内法の採択期限は2024年10月17日。現在、法案について各国で審議中と想定。

法令	制度
規則 Regulation	• その全体において拘束力を有し、加盟国の国内法として制定し直されることなく、全ての加盟国で直接適用される。
指令 Directive	• 「達成されるべき結果」のみについて、当該指令が命じられた加盟国を拘束する。 • 結果を達成するための形式・方法については、加盟国当局に選択が委ねられている。すなわち、指令は加盟国の国内法により置き換えられることによってはじめて一般的な効力を持つことになる。
決定 Decision	• それが及ぶ範囲の者に対し、全ての点で拘束する。 • 決定は、一般的法規というよりむしろ、個別かつ具体的内容を持つ行政手段といえる。
勧告 Recommendation	• 特定の加盟国、企業・個人を対象とした行政指示 • 法的拘束力を持たない。
意見 Opinion	• 欧州委員会の意思の表明。 • 法的拘束力を持たない。

NIS2を踏まえた国内法の採択は2024年10月17日まで

- ドイツ:2024年5月に公表された「NIS-2の実施とサイバーセキュリティ強化法」案が公開。採択はなされていない。
- フランス:調査時点で法案未公開
- イタリア:調査時点で法案未公開

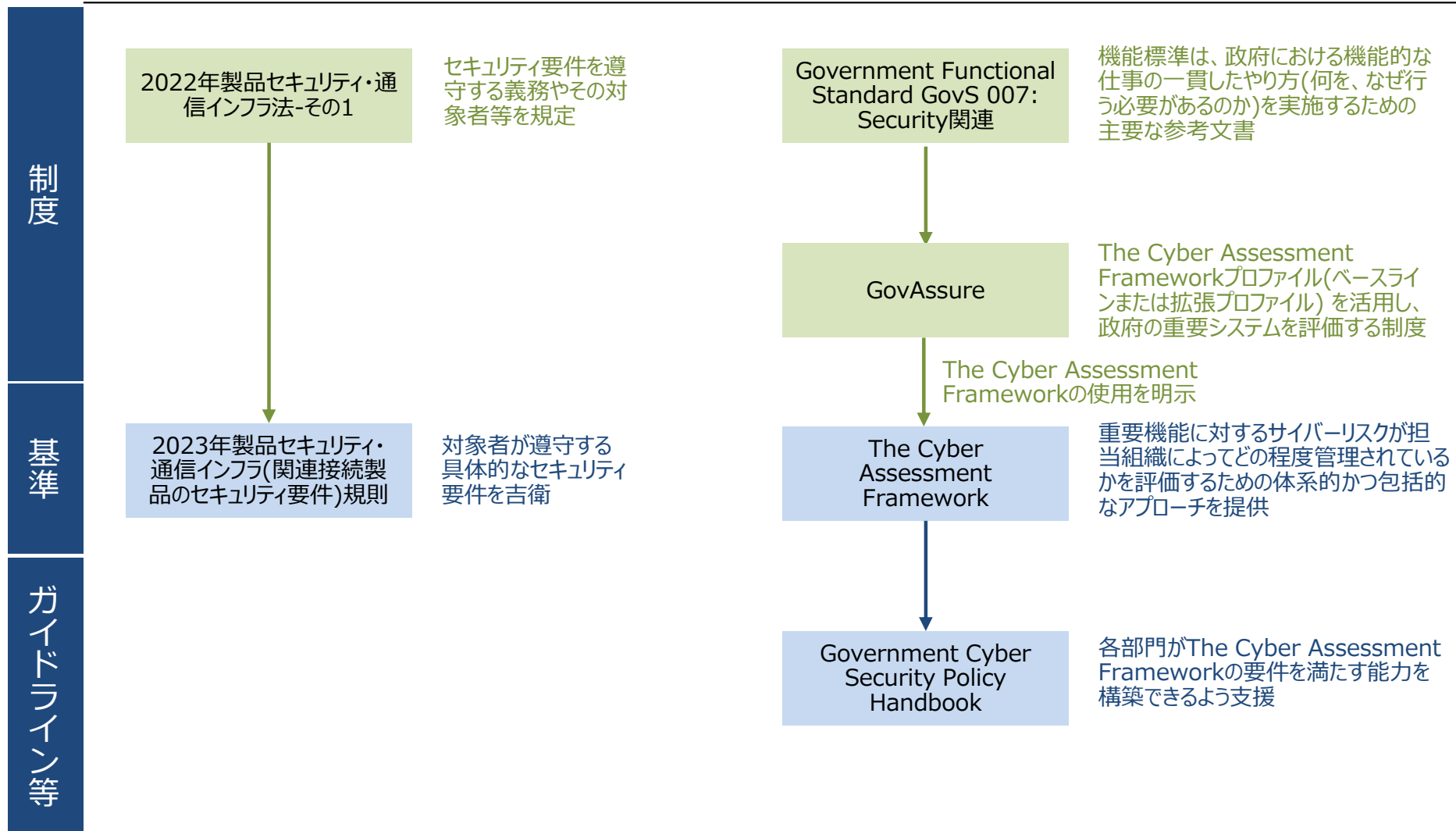


英国関連

英国のガイドライン等の関係性整理

- 本調査の対象となった制度等に限定した場合、制度、基準、ガイドラインでその役割が明確に分かれている。
- GovAssureでは、その文書の中で参照する基準を明示することによって、その関係性を明確にしている。

本調査の対象となった英国のセキュリティ制度等



Product Security and Telecommunications Infrastructure Act

- 「2022年製品セキュリティ・通信インフラ法-その1」及び「2023年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則」によって英国の消費者向け接続可能製品(または「スマート」製品)の製造業者は、同法に定められた関連義務を遵守することが義務づけられた。

2.1 欧州における制度やガイドライン等

名称	Product Security and Telecommunications Infrastructure Act 2022 - Part 1(PSTI法) The Product Security and Telecommunications Infrastructure Regulations 2023		
国・地域	英国	策定者	欧州委員会
適用分野	英国の消費者向けの接続可能な製品*1	遵守義務の有無	あり
対象者	- 英国の消費者向け接続可能製品の製造事業者 - 英国の消費者向け接続可能製品の輸入業者 - 英国の消費者向け接続可能製品の販売事業者		
概要	- 本法律により、<u>英国の消費者向け接続可能製品(または「スマート」製品)の製造業者は、同法に定められた関連義務を遵守することが義務づけられた。</u> - 以下の2つの法律によって成り立つとされている。 ✓ 2022年製品セキュリティ・通信インフラ法-その1:<u>セキュリティ要件を遵守する義務やその対象者等を規定</u> ✓ 2023年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則:<u>上記の具体的な要件等を規定</u> - 上記のどちらも2024年4月29日に発効		
普及状況	(対象事業者に遵守義務がある。)		
URL	https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime		

*1 医療機器やスマートメーター製品、電気事業者の充電ポイント、モバイルネットワークに接続する機能を持たないデスクトップコンピュータ、ラップトップコンピュータ、タブレットコンピュータは対象外となる。

- 「2022年製品安全・電気通信インフラ法」において、セキュリティ要件を遵守する義務やその対象者を規定し、「2023年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則」において、具体的な要件等を規定。

分類	文書一覧	内容
制度	2022年製品セキュリティ・通信インフラ法-その1	- スマート製品のサイバーセキュリティ対策の向上を目的とした法律。 - サイバー犯罪の継続的な脅威に対処するために、一連の改善された関連するセキュリティ保護を導入する措置が含まれる。
基準	2023年製品セキュリティ・通信インフラ(関連接続製品のセキュリティ要件)規則	- 上記の具体的な要件等を規定。別表では要件を示す。 パスワード:パスワードは製品ごとに一意である必要がある。または、製品のユーザーによって定義できる。 セキュリティ問題の報告方法に関する情報:製造事業者は、製品に関するセキュリティの問題を報告する方法に関する情報を提供する必要がある。また、製造事業者は、報告の受領の確認と、報告されたセキュリティの問題の解決までの状況の更新が、報告を行う担当者によって期待できるタイムスケールに関する情報を提供する必要がある。 最低セキュリティアップデート期間のご案内:セキュリティ更新プログラムの最小期間に関する情報は、明確でアクセス可能かつ透明性のある方法で公開され、消費者が利用できるようにする必要がある。これは、セキュリティ更新プログラムが提供される最小期間と終了日である必要がある。 - 消費者向けIoTのサイバーセキュリティに関する主要なグローバルスタンダードであるETSI EN 303 645の主要な規定に準拠。

Government Functional Standard GovS 007: Security関連

- 機能標準は、政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を実施するための主要な参考文書。

2.1 欧州における制度やガイドライン等

名称	Government Functional Standard GovS 007: Security関連		
国・地域	英国	策定者	内閣府
適用分野	政府のセキュリティ活動の計画、実施、管理に適用	遵守義務の有無	あり
対象者	中央政府^{*1}		
概要	- 機能標準は、<u>政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を実施するための主要な参考文書</u>。どのように業務を行うかは、<u>関連する実務やガイダンスで定められており</u>、一連の機能基準全体を通して「ガバナンスと管理の枠組み」と呼ばれている。 - 本文書の構成は以下の通り。 ✓ 原則 ✓ コンテキスト ✓ ガバナンス ✓ セキュリティライフサイクル(戦略と計画/予防と検知/セキュリティインシデントへの対応/経験からの学習) ✓ セキュリティプラクティス(物理セキュリティ/人員のセキュリティ/サイバーセキュリティ/技術的セキュリティ/インダストリアルセキュリティ/セキュリティリスクマネジメント/情報マネジメント/重要な資産とリソース/能力とキャパシティ、リソース/セキュリティ文化、教育、意識向上)		
普及状況	-		
URL	https://assets.publishing.service.gov.uk/media/613a195bd3bf7f05b694d647/GovS_007-Security.pdf		

^{*1} Government Functional Standard(政府機能基準)における組織とは、政府省庁、独立行政法人、その他機能基準の適用範囲内であると特定された組織を指す総称。ただし、オン政府機能基準は他の公共部門組織（分権組織、地方組織）においても有効とされてる。

Government Functional Standard GovS 007: Security関連

- GovAssureではThe Cyber Assessment Framework(CAF)を用いて政府機関を評価する。
- また、CAFの要件を組織が満たすために参考となる文書(Government Cyber Security Policy Handbook)も公開されている。

種別	対象
制度	Government Functional Standard GovS 007: Security関連 - 本機能標準は、政府における機能的な仕事の一貫したやり方(何を、なぜ行う必要があるのか)を実施するための主要な参考文献。 <u>どのように業務を行うかは、関連する実務やガイダンスで定められている。</u> GovAssure <u>本制度は、政府向けのサイバーセキュリティ保証アプローチ。</u> GovAssureの保証アプローチは、政府のサイバーセキュリティ戦略に定められている政府のサイバーセキュリティを客観的に理解するための要件を満たしている。 <u>本制度は、The Cyber Assessment Frameworkを使用する。</u> 組織は、政府の2つのターゲットThe Cyber Assessment Frameworkプロファイル(ベースラインまたは拡張プロファイル)のいずれかに対して重要なシステムを評価します。これにより、組織とセキュリティ部門は、政府全体のサイバーレジリエンスのレベルを理解するためのより効果的なメカニズムを得ることができる。
基準	The Cyber Assessment Framework - 本フレームワークは、<u>重要機能に対するサイバーリスクが担当組織によってどの程度管理されているかを評価するための体系的かつ包括的なアプローチ</u>を提供。 <u>本フレームワークに基づく評価</u>は、<u>責任組織自身</u>(自己評価)、または<u>独立した外部組織</u>(規制当局/サイバー監視機関、またはNCSCが保証する商業サービスプロバイダーなど、規制当局の代理として活動する適切な資格を有する組織)が<u>実施することができる。</u>
ガイドライン	Government Cyber Security Policy Handbook 本ハンドブックは、政府のポリシー、技術ガイダンス、利用可能なツールセットを活用し、これらを The Cyber Assessment Frameworkの言語で構造化することにより、<u>各部門がThe Cyber Assessment Frameworkの要件を満たす能力を構築できるよう支援する。</u>

Cyber Essentials

- Cyber Essentialsは、政府が支援するサイバーセキュリティ認証制度で、規模の大小にかかわらず、最も一般的なサイバー攻撃全般から組織を保護するのに役立つとされている。

2.1 欧州における制度やガイドライン等

名称	Cyber Essentials		
国・地域	英国	策定者	国家サイバーセキュリティセンター(NCSC)* ¹
適用分野	ITインフラストラクチャ全体または個別に管理されるサブセットを対象とする。(クラウドサービスやBYOD等も広く対象とする。)	遵守義務の有無	なし
対象者	• 本制度は、企業の国籍や規模について制約を持たず、広く適用され得る		
概要	• Cyber Essentials及びCyber Essentials Plusという2種類の認証を設けている。 ✓ Cyber Essentials インターネット上でのオンライン審査にて自己診断を行い、認定機関に所属する有資格の審査員が回答を評価したうえで、合格した場合は認定証が授与される。 要求事項は、それらにより80%のサイバー攻撃を防ぐと謳われる「ファイアウォール」、「セキュアな構成」、「セキュリティアップデート管理」、「ユーザーアクセス制御」、「マルウェア保護」という5つのカテゴリを含む。 ✓ Cyber Essentials Plus Cyber Essentials認証の取得を前提として、実施すべき保護は同じだが、実地検査として認定機関による実践的な技術検証を実施する。 • Cyber EssentialsまたはCyber Essentials Plusの取得が英国の公的機関との契約時に調達要件とされる場合がある。		
普及状況	2023年3月段階で、12万件以上の認定がなされている。 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview		
URL	https://www.ncsc.gov.uk/cyberessentials https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf		

*1 NCSCが基準の開発を担い、NCSCと連携するIASMEが認証機関を認定している。

*2 ※インターネットに接続したり、インターネットにつながるネットワークに接続したりしないIT機器は、申告する必要がない。この場合、インターネットに接続することが通常想定されないOT環境は対象に含まれないと解することもできる。

The Security of Network & Information Systems Regulations

- 本規則は、デジタル・サービス(オンライン・マーケットプレイス、オンライン検索エンジン、クラウド・コンピューティング・サービス)や必須サービス(輸送、エネルギー、水、健康、デジタル・インフラ・サービス)の提供に不可欠なネットワークや情報システムのセキュリティ(サイバーと物理的な回復力の両方)の全体的なレベルを高めるための法的措置を提供。

2.1 欧州における制度やガイドライン等

名称	The Security of Network & Information Systems Regulations		
国・地域	英国	策定者	英国議会
適用分野	デジタル・サービス* ¹ 必須サービス* ²	遵守義務の有無	あり
対象者	デジタル・サービスや必須サービスの運営者		
概要	- 本規則は、デジタル・サービス(オンライン・マーケットプレイス、オンライン検索エンジン、クラウド・コンピューティング・サービス)や必須サービス(輸送、エネルギー、水、健康、デジタル・インフラ・サービス)の提供に不可欠なネットワークや情報システムのセキュリティ(サイバーと物理的な回復力の両方)の全体的なレベルを高めるための法的措置を提供する。 - 政府は英国のサイバー耐性を向上させるためにNIS規制を更新する意向を発表した。変更点は以下の通り ✓ デジタル・サプライチェーンの安全性を維持するため、マネージド・サービス・プロバイダー(MSP)を規制の対象とする。 ✓ 規制当局へのサイバーインシデント報告の改善NIS規制を執行するための費用回収システムの確立 ✓ NIS規制の実効性を維持するため、将来的にNIS規制を改正する権限を政府に与える。 ✓ 情報コミッショナーがデジタルサービスを規制する際に、よりリスクベースのアプローチを取ることを可能にする。		
普及状況	-		
URL	https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018		

*1 オンライン・マーケットプレイス、オンライン検索エンジン、クラウド・コンピューティング・サービス等が該当

*2 輸送、エネルギー、水、健康、デジタル・インフラ・サービスが該当

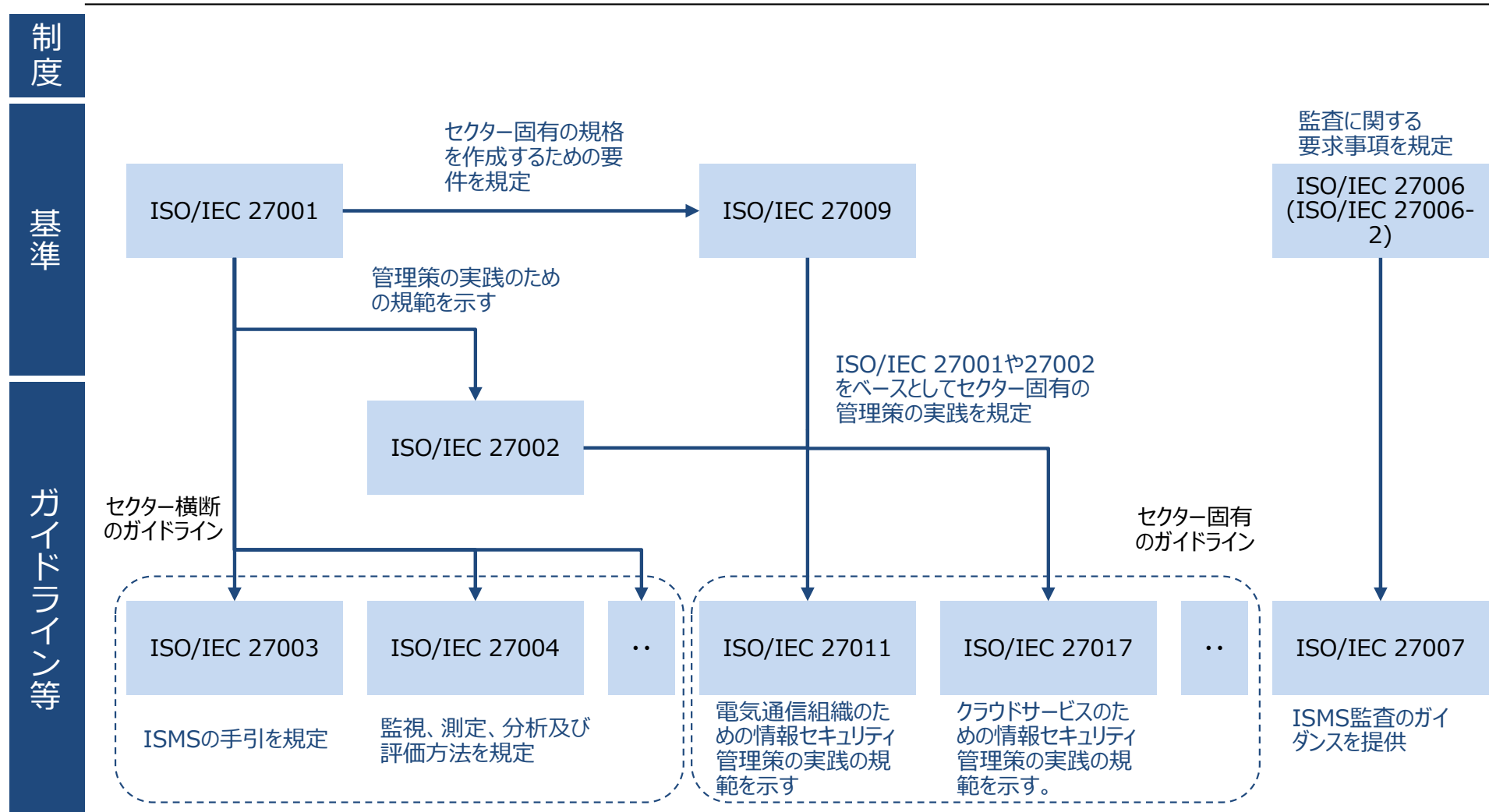


国際関連

国際のガイドライン等の関係性整理

- ISO/IEC 27001の要求事項を補足する形で、実践のための規範(ISO/IEC 27002)や手引き(ISO/IEC 27003)、評価方法等(ISO/IEC 27004)を示すガイドラインが策定されている。また、ISO/IEC 27009の要求事項を遵守する形でセクター固有のガイドライン(例:ISO/IEC 27017)が策定。

ISO/IEC 27001関連



ISO/IEC 27001:2022

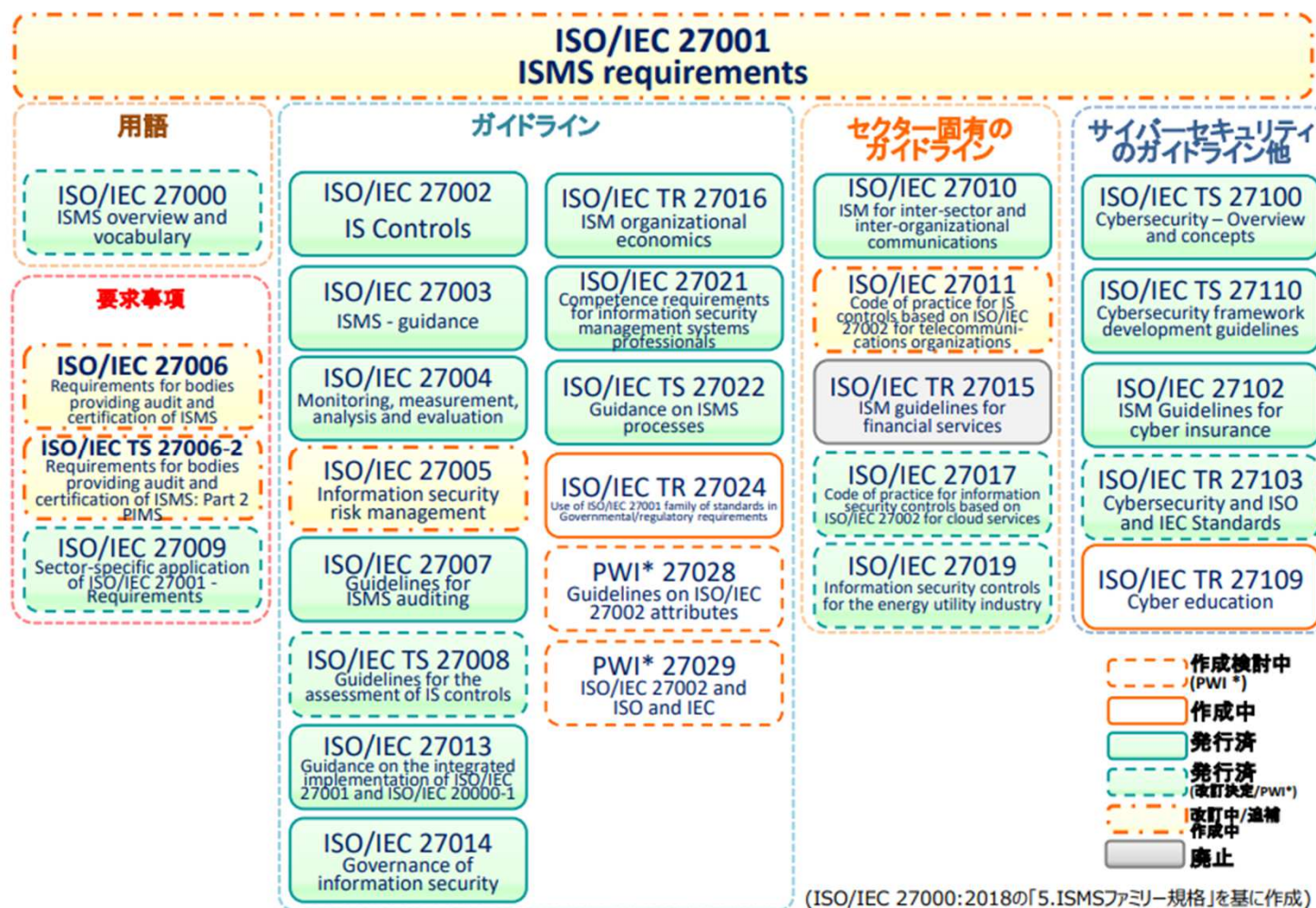
- 本規格は、情報セキュリティマネジメントシステム(ISMS)を確立、実施、維持、継続的に改善するための要求事項を提供することを目的として作成。

2.1 国際における制度やガイドライン等

名称	ISO/IEC 27001:2022		
国・地域	国際	策定者	ISO/IEC JTC 1/SC 27/WG 1
適用分野	(業種・業態を問わない)	遵守義務の有無	なし
対象者	あらゆる組織が利用し、認証を取得可能。		
概要	- 本規格は、情報セキュリティマネジメントシステム(ISMS)を確立、実施、維持、継続的に改善するための要求事項を提供することを目的として作成。 - ISMSは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えるもの。 - ISMSの導入は、その組織のニーズに合わせた規模で行うことが期待されている。本規格は、組織自身の情報セキュリティ要求事項を満たす組織の能力を以下で評価する際に用いることが可能。 ✓ 組織の内部で評価 ✓ 外部関係者が評価		
普及状況	(ISMS適合性評価制度において認証を取得した企業数は7,824(2024年6月24日時点))		
URL	https://www.iso.org/standard/27001		

ISO/IEC 27001:2022

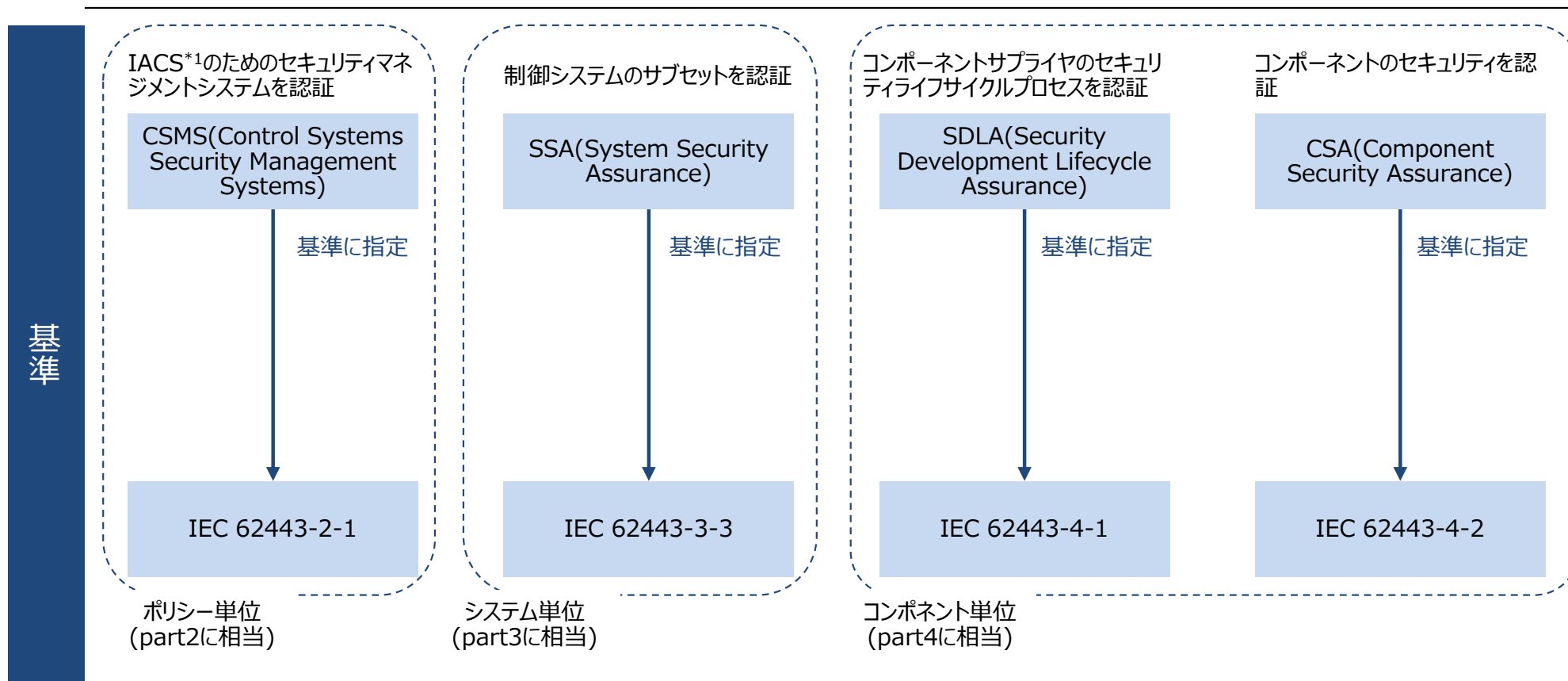
- ISMSの要求事項を定めるISO/IEC 27001:2022を中心として、用語や要求事項、ガイドライン等を定める文書が展開されている。



国際のガイドライン等の関係性整理

- 制御システム関連の各制度は、IEC62443の標準をその基準に定めており、各パートに対応している。
 - ✓ CSMS(Control Systems Security Management Systems):IEC 62443-2-1
 - ✓ SSA (System Security Assurance):IEC 62443-3-3
 - ✓ CSA (Component Security Assurance):IEC 62443-4-1
 - ✓ SDLA (Security Development Lifecycle Assurance):IEC 62443-4-2

IEC 62443関連



*1 IACS(Industrial Automation Control System):産業用オートメーション及び制御システム

IEC 62443シリーズ

- IEC 62443シリーズは、IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群。

2.1 国際における制度やガイドライン等

名称	IEC 62443シリーズ		
国・地域	国際	策定者	ISA(国際自動制御学会)(S99)及び IEC(国際電気標準会議)(TC65/WG10)
適用分野	産業用オートメーション及び制御システム	遵守義務の有無	なし
対象者	- 制御システムのアセットオーナー - 制御システムのシステムインテグレーター - 制御関連製品の製品供給者		
概要	- IEC 62443シリーズは、<u>IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群</u>。IACSとは、制御プロセスの安全、セキュリティ、信頼性(Reliability)のある運用に作用、もしくは影響する人的資産、ハードウェア及びソフトウェアの集合体を指す。したがって、セキュリティ確保の対象はソフトウェア・ハードウェアを含む制御関連のデータ処理基盤であるシステムだけでなく、システムの運用にかかわる「人」や「業務」も対象。 <u>IEC 62443-2-1はISO/IEC 27001を参考に、IACSに固有の部分を追加するよう作成されていることから、共通の要件が多数記載されている</u>。IEC 62443-2-1では、「セーフティ(人、環境等)に対するリスクの洗い出しやライフサイクル全般(開発～廃棄)までの各ステップにおけるリスクの洗い出し」、「災害時やシステム更新時にセキュリティレベルや安全性が低下しないような対策機能の実装や運用」を実施することが求められていると整理されている。		
普及状況	(IEC 62443-2-1を基準とするCSMS適合性評価制度において認証を取得した企業数は3(2024年6月24日時点))		
URL	https://webstore.iec.ch/publication/7030		

IEC 62443シリーズ

- IEC 62443シリーズは、制御システムのセキュリティ実現に活用できる基準のひとつであり、以下のパートから構成される。 ※改定・策定状況は2023年2月時点のもの
 - IEC 62443-1：規格全体の用語・概念等の定義
 - IEC 62443-2：組織に対するセキュリティマネジメントシステム
 - IEC 62443-3：システムのセキュリティ要件や技術概説
 - IEC 62443-4：部品(装置・デバイス)層におけるセキュリティ機能や開発プロセス要件
 - IEC 62443-6：規格適合性評価のための技術基準

Horizontal	OT Cybersecurity				
Part 1 General	TS 62443-1-1 Concepts & Models	62443-1-2 Reserved	62443-1-3 Performance Metrics	TR 62443-1-4 Security Lifecycle	TS 62443-1-5 Scheme for Security profiles
Part 2 Policies	62443-2-1 Security Program requirement	62443-2-2 Security protection	TR 62443-2-3 Patch management	62443-2-4 Service providers	TR 62443-2-5 Implementation guide for asset owners
Part 3 System	TR 62443-3-1 Security Technologies	62443-3-2 Security Risk Assessment	62443-3-3 System security Requirements		
Part 4 Component	62443-4-1 Secure product Development Lifecycle	62443-4-2 Security requirement for Components	PAS 62443-4-3 Application to IIoT		
Part 6 Conformity	TS 62443-6-1 Security evaluation for Service Providers (2-4)	TS 62443-6-2 Security evaluation for Components (4-2)			

改訂・作成中

黒字：IEC文書発行済または審議中
 白字：IEC文書未審議

IS:International Standard, TR:Technical Report, TS:Technical Specification,
 PAS: Publicly Available Specification

出展：IEC/TC65/WG10審議状況およびISA99 Working Groupの情報を元に作成

[参考] IEC/TC65/WG10 国際エキスパート(横河電機:星野、日立:藤田、三菱電機:神余)「IEC 62443制御システムセキュリティ規格の現状～概要と最新の状況の紹介」

https://www.jpccert.or.jp/present/2023/ICSR2023_02_YOKOGAWAElectric.pdf

© Hitachi, Ltd. 2025. All rights reserved.

IEC 62443シリーズ

- IEC 62443の各基準に準拠した認証制度が運用されている。
 - ✓ CSMS(Control Systems Security Management Systems)
 - ✓ SSA (System Security Assurance)
 - ✓ CSA (Component Security Assurance)
 - ✓ SDLA (Security Development Lifecycle Assurance)

種別	対象	対象
制度	ポリシー単位 (part2に相当)	CSMS(Control Systems Security Management Systems)
		• IACSのためのセキュリティマネジメントシステムを認証(IEC 62443-2-1準拠)
	システム単位 (part3に相当)	SSA(System Security Assurance)
		• 制御システムのサブセットを認証(IEC 62443-3-3準拠)
	コンポーネント単位 (part4に相当)	CSA(Component Security Assurance)
		• コンポーネントのセキュリティを認証(IEC 62443-4-2準拠) ※ソフトウェアアプリケーション・組込みデバイス・ホストデバイス・ネットワークデバイス
		SDLA(Security Development Lifecycle Assurance)
		• コンポーネントサプライヤのセキュリティライフサイクルプロセスを認証(IEC 62443-4-1準拠)

ISO/IEC 15408-1:2022

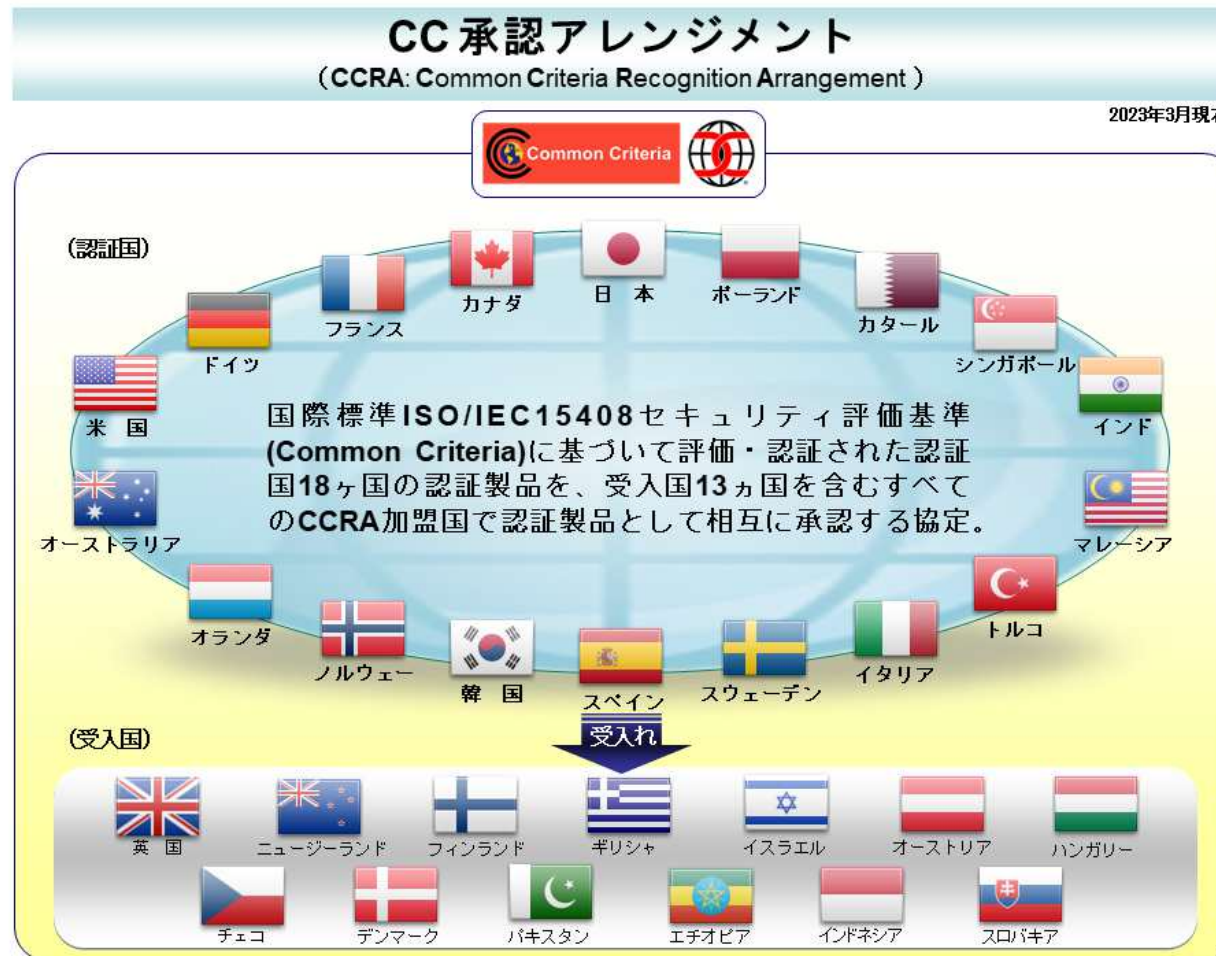
- 本規格は、情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準。

2.1 国際における制度やガイドライン等

名称	ISO/IEC 15408-1:2022		
国・地域	国際	策定者	ISO/IEC
適用分野	情報技術を用いた製品やシステム全般	遵守義務の有無	なし
対象者	-		
概要	- 本規格は、情報技術セキュリティの観点から、<u>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</u>。 - 本規格は、<u>情報技術を用いた製品やシステムのセキュリティ機能を対象</u>とする。ソフトウェアだけでなく、ハードウェア、ファームウェア、あるいは、システム全体も評価対象となる。また、製品の形態としては、ファイアウォールのように、直接セキュリティに係る機能を提供する製品に限らず、オペレーティングシステム、データベース、あるいはグループウェアなど、<u>保護すべき資源を保有する製品はすべて評価対象となる</u>。 - 本規格に基づいた評価が、異なる制度や評価機関でなされても、その評価結果が均質である必要があるため、評価に使用される手法(どのような対象を評価し、どのような判断を要するかなど)を明確にした<u>CEM(Common Evaluation Methodology: 共通評価方法)</u>が本規格とともに開発された。CEMもISO標準(ISO/IEC 18045)として発行されている。		
普及状況	-		
URL	https://www.commoncriteriaportal.org/index.cfm https://www.ipa.go.jp/security/jisec/about/about.html		

ISO/IEC 15408-1:2022

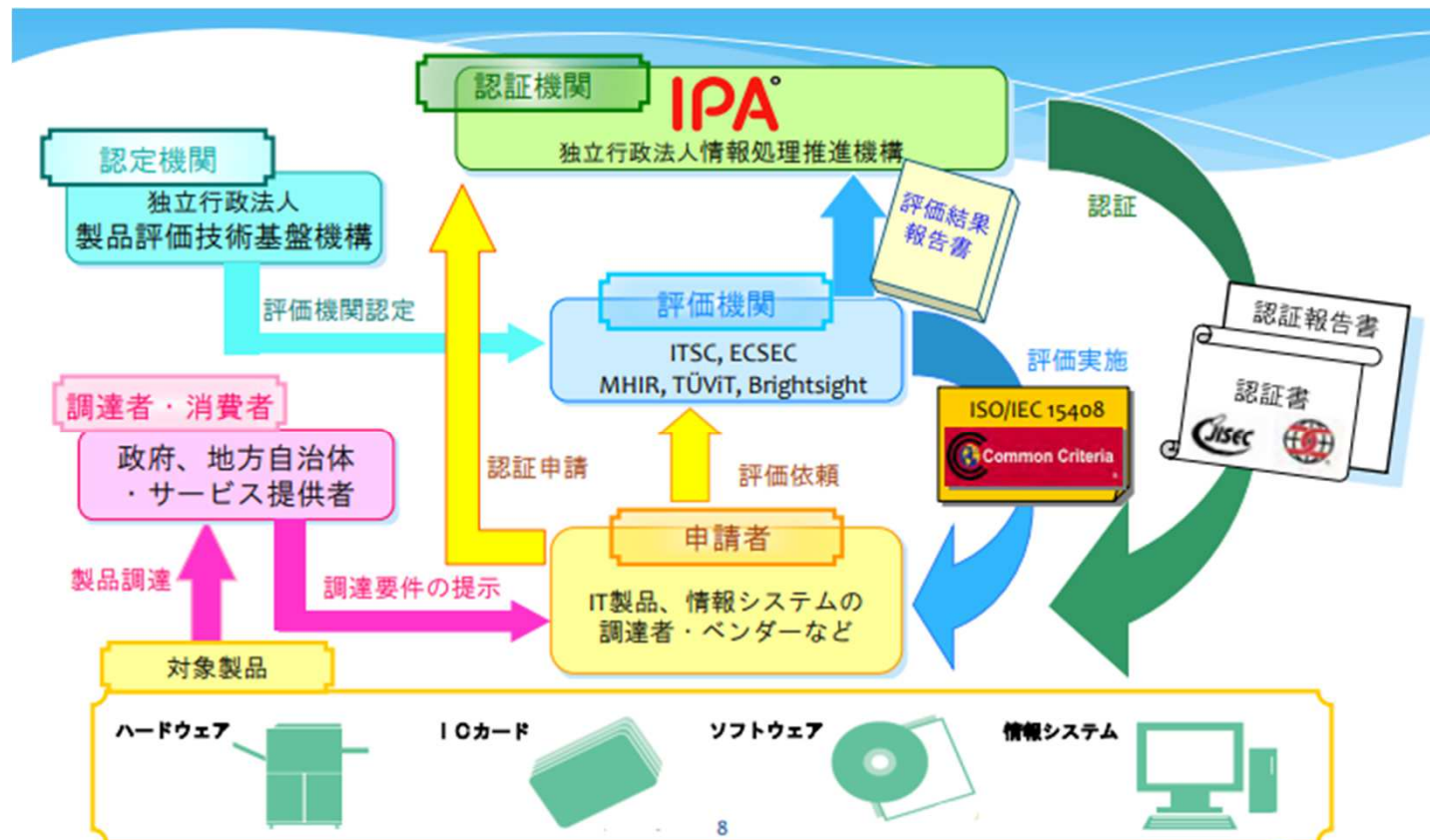
- 日本はCC承認アレンジメント(CCRA:Common Criteria Recognition Arrangement)に参加。
- 日本では、JISEC(Japan Information Technology Security Evaluation and Certification Scheme) がCC承認アレンジメントに参加。



ISO/IEC 15408-1:2022

- JISECにおいて、評価機関はISO/IEC 15408を用いて対象製品を評価し、IPAはその評価結果をまとめた報告書をもって、製品を認証する。

JISEC(Japan Information Technology Security Evaluation and Certification Scheme)



ISO/IEC 27402:2023

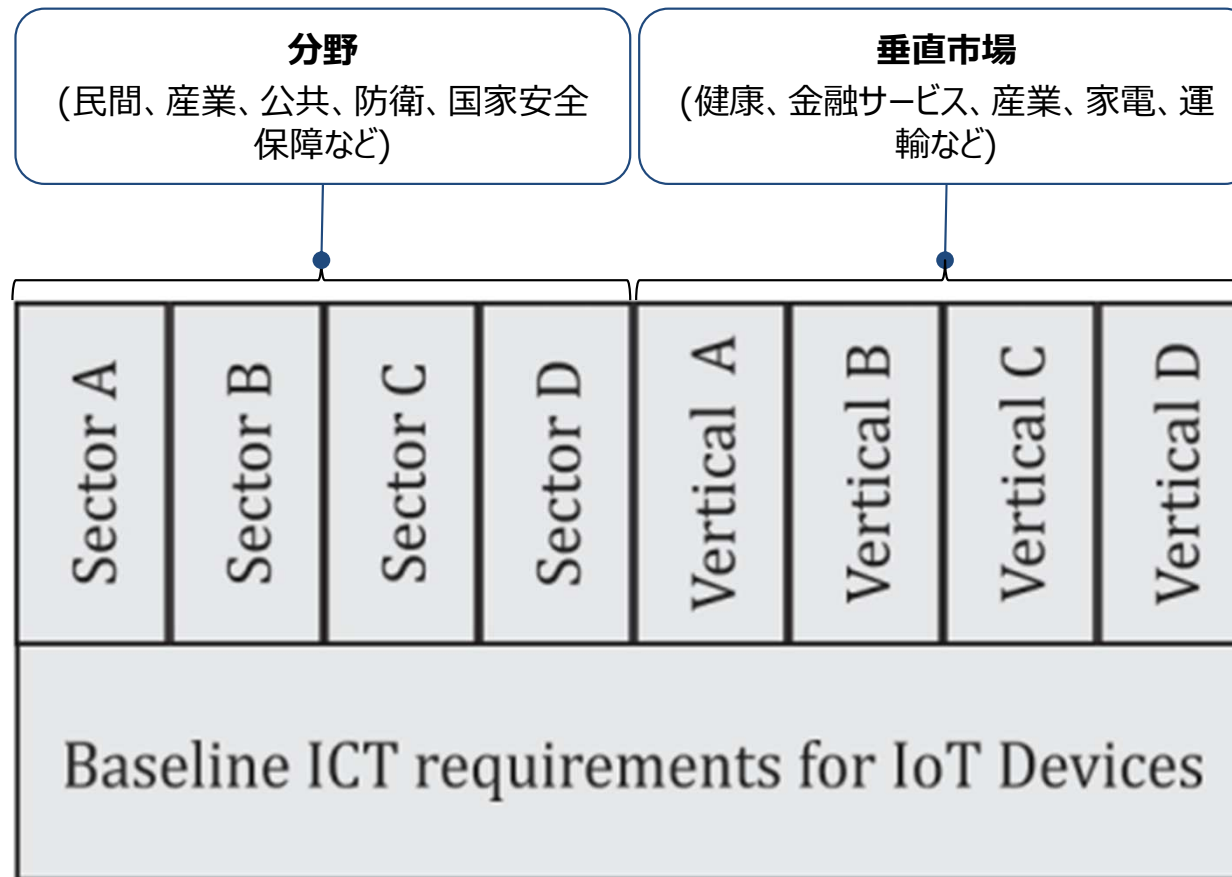
- 本文書は、IoT機器がセキュリティとプライバシーの管理をサポートできるように、情報通信技術(ICT)要件のベースライン・セットを提供する。

2.1 国際における制度やガイドライン等

名称	ISO/IEC 27402:2023		
国・地域	国際	策定者	ISO/IEC JTC 1/SC 27
適用分野	IoT機器分野	遵守義務の有無	なし
対象者	- IoTサービスプロバイダ - IoTサービスデベロッパ - IoTユーザ		
概要	- 本文書は、<u>IOT機器がセキュリティとプライバシーの管理をサポートできるように、情報通信技術(ICT)要件のベースライン・セットを提供</u>する。 - 本文書の要件は、様々な分野(民間、産業、公共、防衛、国家安全保障など)や垂直市場(健康、金融サービス、産業、家電、運輸など)で<u>IOT機器の使用とリスクに対する追加要件を構築するためのベースラインとすることを意図</u>して策定。 - 本文書は、適合性評価スキームの要件を提供することができるが、特定の分野や垂直市場の利害関係者が、<u>本文書をもとに、それぞれの状況に特有の要件についてコンセンサスを形成することを期待するもの</u>。		
普及状況	-		
URL	https://webstore.iec.ch/publication/90104&preview		

ISO/IEC 27402:2023

- 本文書の要件は、様々な分野(民間、産業、公共、防衛、国家安全保障など)や垂直市場(健康、金融サービス、産業、家電、運輸など)でIoT機器の使用とリスクに対する追加要件を構築するためのベースラインとすることを意図して策定。



ISO/IEC 27009:2020

- 本規格は、特定のセクターをサポートするためにISO/IEC27001を拡張し、ISO/IEC27002を補完等するセクター固有の規格を作成するための要件を規定。

2.1 国際における制度やガイドライン等

名称	ISO/IEC 27009:2020		
国・地域	国際	策定者	ISO/IEC JTC 1/SC 27
適用分野	(セクター固有の規格を策定するための要件を規定しているため、セクター横断的な規格の位置づけ)	遵守義務の有無	なし
対象者	-		
概要	- 本規格は、<u>特定のセクター(ドメイン、アプリケーション分野、市場)をサポートするためにISO/IEC27001を拡張し、ISO/IEC27002を補完等するセクター固有の規格を作成するための要件を規定。</u> <u>ISO/IEC 27001に関連するセクター固有の規格は、ISO/IEC 27001またはISO/IEC 27002の要求事項または指針を追加することができる。</u>セクター固有の要求事項の構成は以下の通り。 ✓ ISO/IEC 27001要求事項 ✓ 追加、改良、解釈された要求事項		
普及状況	セクター固有のガイドラインとして、ISO/IEC 27010、ISO/IEC 27011、ISO/IEC 27015、ISO/IEC 27017、ISO/IEC 27019が策定。		
URL	https://www.iso.org/standard/73907.html		

ISO/IEC 27009:2020

- セクター固有の要求事項の構成は以下の通り。
 - ✓ ISO/IEC 27001 要求事項
 - ✓ 追加、改良、解釈された要求事項



- **追加:** ISO/IEC 27001要求事項への追加が認められる。
- **改良:** ISO/IEC 27001要求事項の絞り込みが可能。ただし、ISO/IEC 27001の要求事項を削除したり無効にしたりするものではない。
- **解釈:** ISO/IEC 27001要求事項の解釈は許される。解釈は、ISO/IEC 27001の要求事項を無効にするものではなく、新たに解釈された要件はそれらを説明するものであり、また、セクター固有の文脈に置くもの。

ISO/IEC 27017:2015

- 本規格は、クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提供する。

2.1 国際における制度やガイドライン等

名称	ISO/IEC 27017:2015		
国・地域	国際	策定者	ISO/IEC JTC 1/SC 27
適用分野	クラウドサービス分野	遵守義務の有無	なし
対象者	- 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		
概要	- 本規格は、<u>クラウドサービスカスタマ及びクラウドサービスプロバイダのための情報セキュリティ管理策の実施を支援する指針を提供</u>する。指針は管理策を実施するクラウドサービスカスタマやクラウドサービスプロバイダを対象としており管理策の実施を支援するためのものである。 - この規格は、クラウドサービス固有の情報セキュリティの脅威及びリスクに対処するため、<u>ISO/IEC 27002に基づきクラウドサービス固有の追加の実施の手引を提供</u>するとともに、<u>追加の管理策を提供</u>する。 - 情報セキュリティマネジメントシステムにおけるリスクマネジメントを実施するための要求事項についてはISO/IEC 27001を参照し、情報セキュリティリスクマネジメントそのものの更なる指針については、ISO/IEC 27005を参照する。 - ISO/IEC 27002で規定する管理目的及び管理策が追加の情報を必要とすることなく適用できる場合には、ISO/IEC 27002への参照だけを示す。		
普及状況	-		
URL	https://www.iso.org/standard/43757.html		

ISO/IEC 27017:2015

- JIS Q 27002等が管理策に関連する追加のクラウドサービス固有の実施の手引を必要とする場合には、追加で実施の手引きが示される。

- JIS Q 27002で規定する管理目的及び管理策が追加の情報を必要とすることなく適用できる場合には、JIS Q 27002への参照だけを示す。
- JIS Q 27002又はこの規格の附属書Aの管理策が、管理策に関連する追加のクラウドサービス固有の実施の手引を必要とする場合には、これを「クラウドサービスのための実施の手引」の見出しの下に示す。手引は、次の2種類のうちのいずれかの形式で示す。
 - ✓ タイプ1:クラウドサービスカスタマ及びクラウドサービスプロバイダに対し、個別の手引がある場合に用いる。
 - ✓ タイプ2:クラウドサービスカスタマ及びクラウドサービスプロバイダの両者に対し、同じ手引がある場合に用いる。

■タイプ1の例(6.1.1 情報セキュリティの役割及び責任の場合)

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
クラウドサービスカスタマは、クラウドサービスプロバイダと、情報セキュリティの役割及び責任の適切な割当てについて合意し、割り当てられた役割及び責任を遂行できることを確認することが望ましい。両当事者の情報セキュリティの役割及び責任は、合意書に記載することが望ましい。 クラウドサービスカスタマは、クラウドサービスプロバイダの顧客支援・顧客対応機能との関係を特定し、管理することが望ましい。	クラウドサービスプロバイダは、その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及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化することが望ましい。

■タイプ2の例(16.1.7 証拠の収集の場合)

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
クラウドサービスカスタマ及びクラウドサービスプロバイダは、クラウドコンピューティング環境内で生成される、デジタル証拠となり得る情報及びその他の情報の提出要求に対応する手続について合意することが望ましい。	

Appendix[2章]

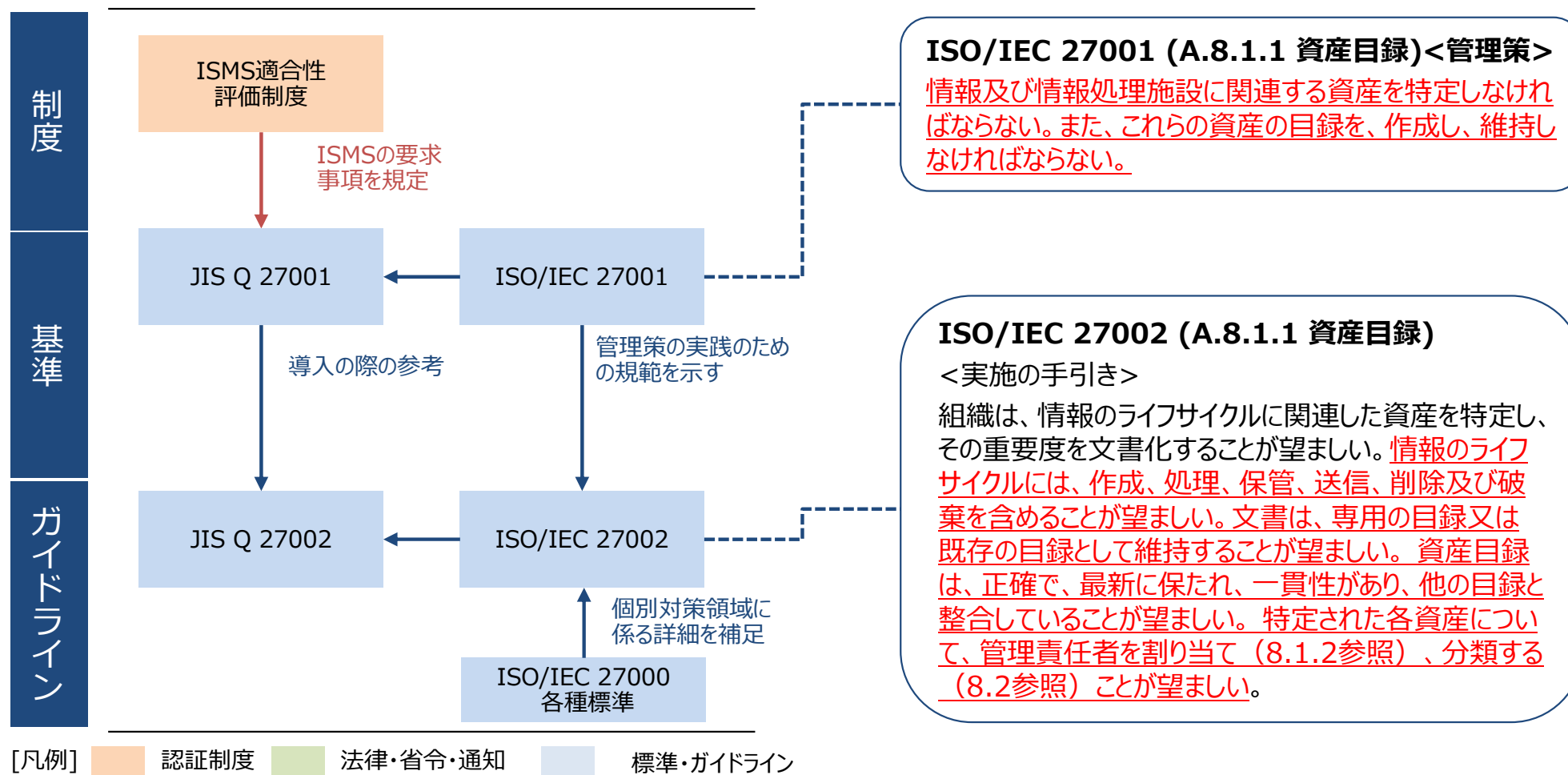


2.1 業種横断

- 制度/基準/ガイドラインの固まりで位置づけ/参照関係を具体化する。

位置づけ/参照関係

- ISMS適合性評価制度では、ISO/IEC 27001をもとに策定された国内規格であるJIS Q 27001にて要求事項を定めている。



- ISO/IEC 27001(もしくはISO/IEC 27002)を比較対象として、記載粒度を調査する。比較の観点として、要求事項が実施内容の面で具体的に補足されているかを調査する。(例:実施頻度、対象の情報)

記載粒度

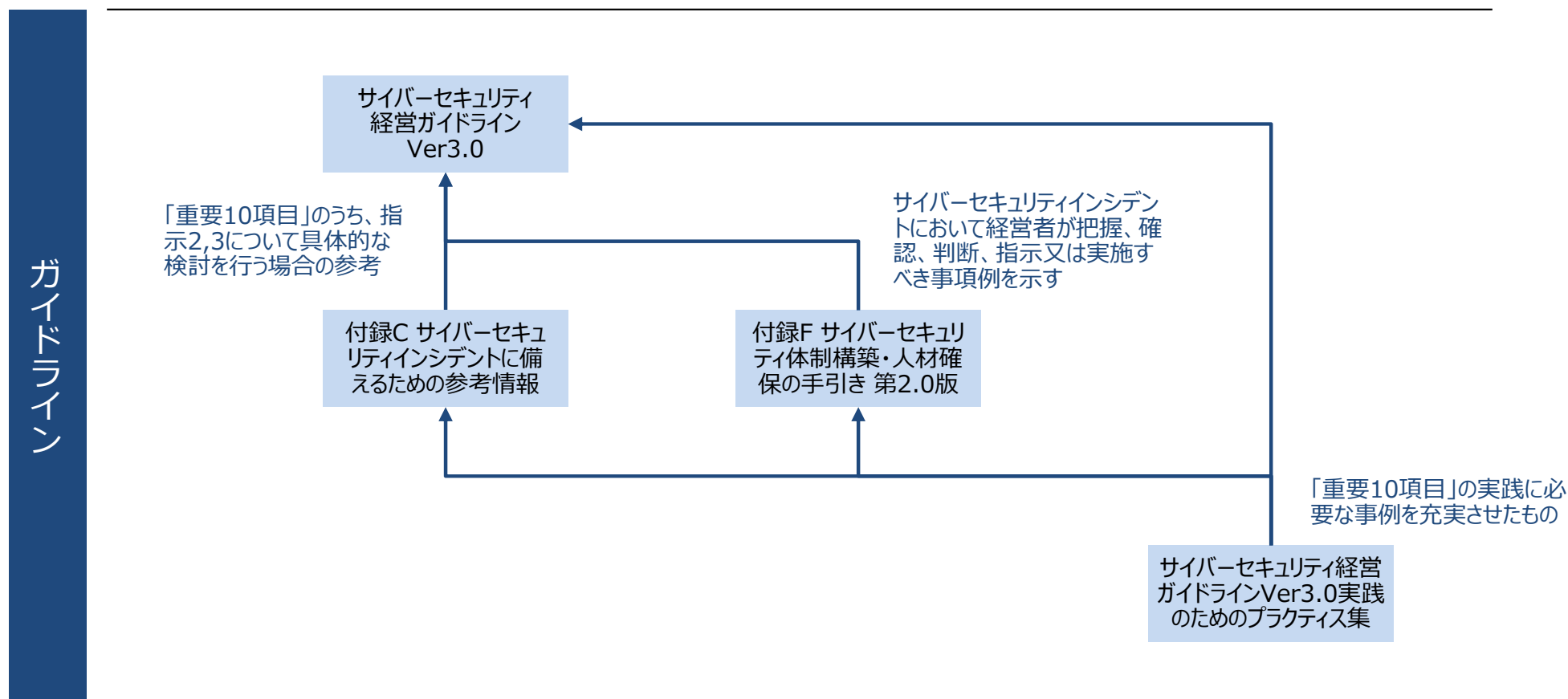
記載粒度 の比較観点	- ISO27001(もしくはISO/IEC 27002)と比較可能な要件*1のうち、その記載の具体性(どちらがより具体的か) (より具体的に記載されている場合)具体的に記載している内容(何が具体的に記載されているのか)	
ISO/IEC 27001 (A.8.1.1 資産目録)	自工会/部工会・サイバーセキュリティガイドライン V2.1 (10 情報資産の管理(情報)/11 情報資産の管理(機器))	比較結果
情報及び情報処理施設に関連する資産を特定しなければならない。	高い機密区分の情報資産(情報)を一覧化している(10.Lv.1[No.56]) 【規則】 一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと 【対象情報】 No.54 で定めた機密区分のうち、高レベルの機密に該当する情報資産 情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)について、一覧を作成している(11.Lv.1[No.60]) 【規則】 バージョン情報、管理者、管理部門、設置場所等の管理項目を含む情報機器、OS、ソフトウェアの一覧を作成すること	- 自工会/部工会・サイバーセキュリティガイドライン V2.1は、ISO/IEC 27001より具体的に記載されている。 - 自工会/部工会・サイバーセキュリティガイドライン V2.1は、資産を特定する際の、具体的な内容(対象情報、管理者名やバージョン情報、OS、ソフトウェア)を記載している。
また、これらの資産の目録を、作成し、維持しなければならない。	情報資産(情報)は機密区分に応じた管理ルールに沿って管理している(10.Lv.1[No.58]) 【規則】 No.54 に定義した管理ルールの順守状況の点検を行い、不備・違反があれば是正を行うこと 【頻度】 1回/年 以上 情報資産(機器)は重要度に応じた管理ルールに沿って管理している(11.Lv.1[No.62]) 【規則】 No.59 に定義した管理ルールに沿って管理を実施すること。不備・違反があれば是正を行うこと 【頻度】 1回/年	- 自工会/部工会・サイバーセキュリティガイドライン V2.1は、ISO/IEC 27001より具体的に記載されている。 - 自工会/部工会・サイバーセキュリティガイドライン V2.1は、管理ルールの具体的な見直し頻度(1回/年)を記載している。

*1「資産管理」に係る要件を対象とするが、比較ができない場合には別途要件で比較する。

- サイバーセキュリティ経営ガイドラインは、上位の法律等による位置づけがなされていないボランティアな文書。
- 関連文書やプラクティス集が、サイバーセキュリティ経営ガイドラインを補足説明している。

位置づけ/参照関係

- サイバーセキュリティ経営ガイドラインは、制度的な位置づけがなされていない。
- 付録Cや付録Fはサイバーセキュリティ経営ガイドラインに示された「重要10項目」の実践に必要な情報について補足するもの。



- 「サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集」の記載内容とISO/IEC 27001の要件を比較する。

項目	目的	想定読者
サイバーセキュリティ経営ガイドライン Ver3.0	経営者のリーダーシップの下で、サイバーセキュリティに関わるリスクを把握・評価した上で、適切なリスク対応の実施を通じて残留リスク10を許容範囲以下に抑制する等、企業に求められる社会的要請に応えるための適切な投資と対策の実践を促すことを目的として提供。	- 経営者(企業の代表者として、統括責任を負う者(CEO)) - 経営者から指示を受け、サイバーセキュリティ対策の実践に関する責任を負う者(CISO 等) - ただし、サイバーセキュリティ対策の実践にあたって経営者やCISO 等を直接補佐する実務者による利用も考慮
付録C サイバーセキュリティインシデントに備えるための参考情報	インシデント発生に備えて、経営者及び組織内で整理しておくべき事項を提供。	(記載なし)
付録F サイバーセキュリティ体制構築・人材確保の手引き 第2.0版	経営ガイドラインにおいて示されている重要 10 項目のうち、「指示 2 サイバーセキュリティリスク管理体制の構築」及び「指示 3 サイバーセキュリティ対策のための資源(予算、人材等)確保」について具体的な検討を行う場合の参考としていただくことを目的として提供。	- 経営者・経営層 - 最高情報セキュリティ責任者(CISO)、セキュリティ統括担当者 - 事業部門の責任者、人事部門担当者、セキュリティに関心のある方
サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集	企業が経営ガイドラインの内容を実践する際の、事例に基づく実施手順や取組の例、取り組む際の考え方、ヒントなどを提供することが、本プラクティス集の目的とする。	- サイバーセキュリティに向けてリスクマネジメントを強化したい経営者 - サイバーセキュリティ対策を実施する上での責任者となる担当幹部(以下、CISO等) - サイバーセキュリティ対策の担当者、CSIRTのメンバー等(以下、セキュリティ担当者) - 上記人材の育成や支援を担当する社内部門や社外の事業者(以下、人材育成・支援担当者)

V

- 主に経営層を対象としているサイバーセキュリティ経営ガイドラインでは、適切な投資や対策の実践を促すことを目的としており、技術的な対策事項の詳細を示すことは必ずしも主眼にはおかれていない。
- 一方で、想定読者にセキュリティ担当者を含むプラクティス集は、実装のためのヒントを提供する目的があるため、ISO/IEC 27001と比較的位置づけが近いことから、記載粒度の調査対象とする。

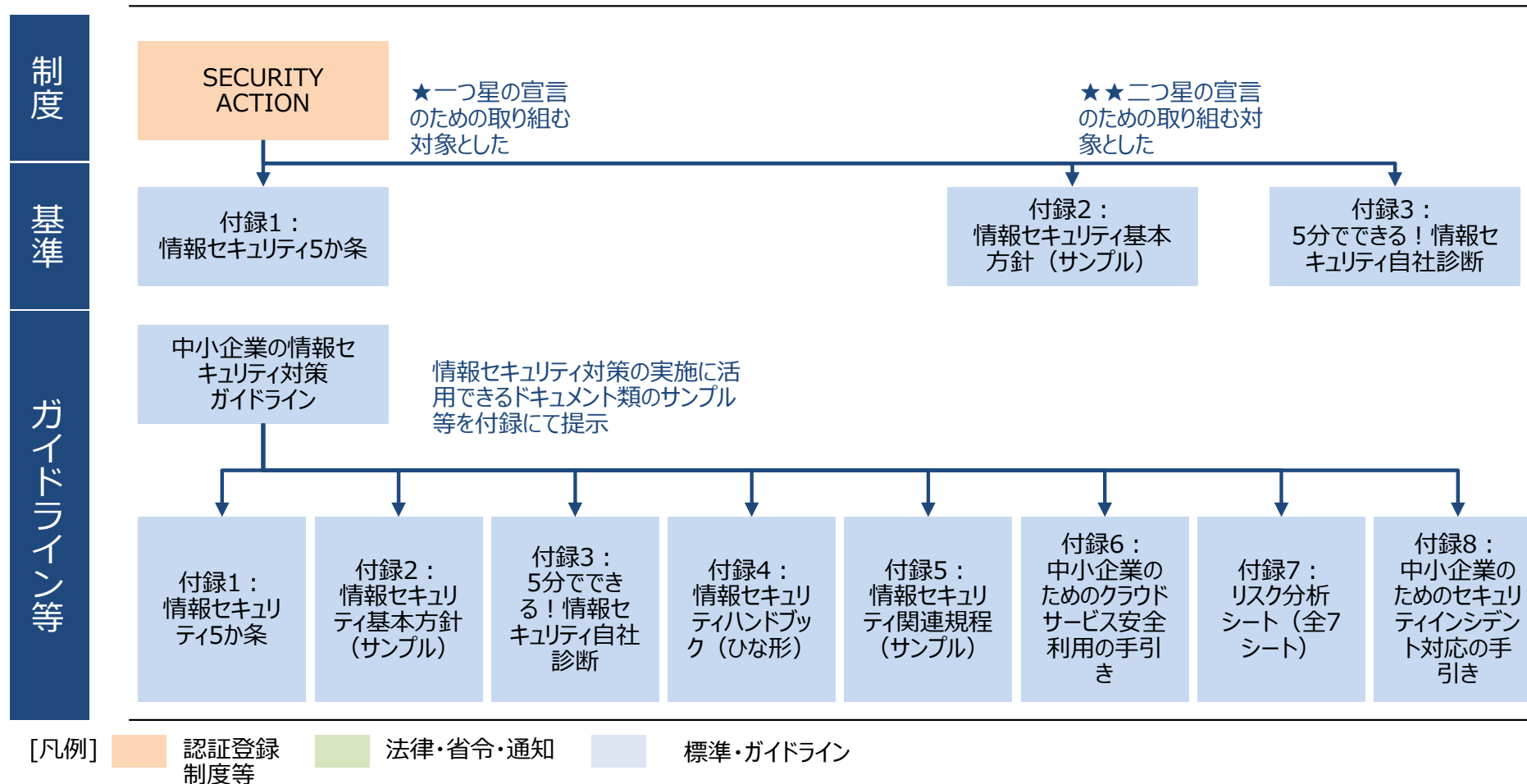
- ISO/IEC 27001と比較して、「サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集」の該当するプラクティスや取組では、対策頻度や対策場所よりも、相談先やその対象者、技術的な対策内容面で具体的な記載がみられた。
- 実施手順や取組の例、取り組む際の考え方、ヒントを紹介することを目的とする本文書では、次回の改訂において時期(例:ログの保管期限、教育の頻度)の情報を追加することも一案。

項目	記載粒度	項目	記載粒度
頻度 (when)	(頻度に関する記載なし)	主体 (who)	<組織的管理策> - 重要な資産を特定する際の相談先(経営層や事業部門等)を紹介。 - ネットワーク構成を把握するための協力先(ベンダ、工場の生産現場担当者^{※1})を紹介 <人的管理策> - 教育の対象者(経営層/部署長、スタッフ部門、事業部門)を紹介。
場所 (where)	<人的管理策> 教育内容の提供場所(社内掲示板)を紹介。	内容 (what)	<人的管理策> - 教育の対象者ごとに学習すべき内容(経営層:サイバーセキュリティが自社のコーポレートリスクに与える影響、スタッフ部門:自部署の業務内容に応じたサイバーセキュリティ上の責任、事業部門:自社セキュリティ部門との連携)を紹介 <技術的管理策> - アクセスログを取得するためのステップ(対象サーバの特定、ログの取得項目の確認)を紹介。 - アクセスログの保管方法(定期的な電子媒体へのコピー)を紹介。 - テレワークのアクセスにおける認証方法(電子証明書及びワンタイムパスワードの2要素認証)を紹介。

- 中小企業の情報セキュリティ対策ガイドラインの一部付録は、SECURITY ACTIONの★を宣言するための対象に指定。

位置づけ/参照関係

- 中小企業の情報セキュリティ対策ガイドラインは、中小企業に対して重要な情報を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介することを目的としている。



- 中小企業の情報セキュリティ対策ガイドラインは、特に中小企業の経営者や情報セキュリティ対策を実践する責任者・担当者を対象として、重要な情報を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介している。

項目	目的	想定読者
中小企業の情報セキュリティ対策ガイドライン	中小企業に情報を安全に管理することの重要性についてご認識いただいた上で、<u>重要な情報を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介</u>することを目的とする。	<u>経営者</u> <u>情報セキュリティ対策を実践する責任者・担当者</u>(対象組織:全ての業種の中小企業および小規模事業者(法人、個人事業主、各種団体も含む))
付録1：情報セキュリティ5か条	<u>組織の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ</u>説明。	(具体的な記載はなかったものの、付録であることを考慮すると「中小企業の情報セキュリティ対策ガイドライン」と同じと想定される)
付録2：情報セキュリティ基本方針（サンプル）	組織としての<u>情報セキュリティに対する基本方針書のサンプル</u>を提示。	(具体的な記載はなかったものの、付録であることを考慮すると「中小企業の情報セキュリティ対策ガイドライン」と同じと想定される)
付録3：5分でできる！情報セキュリティ自社診断	多くの<u>費用をかけることなく実行することで効果がある</u>25項目の<u>チェックシート</u>を提示。	(具体的な記載はなかったものの、付録であることを考慮すると「中小企業の情報セキュリティ対策ガイドライン」と同じと想定される)
付録5：情報セキュリティ関連規程（サンプル）	<u>中小企業向けの情報セキュリティ関連規程のサンプル</u>。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することが可能。	(具体的な記載はなかったものの、付録であることを考慮すると「中小企業の情報セキュリティ対策ガイドライン」と同じと想定される)

中小企業の情報セキュリティ対策ガイドライン

記載範囲

- 記載されている要件に大きな偏りはなく、各コアにおいて半分程度の記載がある。
- 中小企業の情報セキュリティ対策ガイドラインは、中小企業の経営者や担当者を対象としているため、特に基本的な事項に焦点をあてて要件が定められていると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	3/6	防御 (続き)	データセキュリティ	-	3/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	1/2
	監督	-			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	1/4
識別	資産管理	○	2/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	-			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							11/22

- 中小企業の情報セキュリティ対策ガイドラインでは、ISO/IEC 27001と比較してより具体的な記載はみられなかったが、「付録5:情報セキュリティ関連規程(サンプル)」でより詳細な内容を記載している。

- 中小企業の情報セキュリティ対策ガイドラインでは、ISO/IEC 27001と比較してより具体的な記載はみられなかった。
- ただし、「付録5：情報セキュリティ関連規程(サンプル)」でより詳細な内容を記載している構造となっており、読者はサンプルを適宜変更して自社のセキュリティ関連規程とすることが可能となっている。
- 以下に示す内容はその付録の内容に記載されている内容を示す。

項目	記載粒度	項目	記載粒度
頻度 (when)	<人的管理策> - 教育の頻度を例示。 - 情報セキュリティ関連規程の説明(<u>入社時、就業時</u>) - 関連法令の理解(<u>関連法令の公布・施行時</u>)	主体 (who)	<技術的管理策> <u>利用者アカウントの承認主体(代表取締役又は情報セキュリティ責任者)</u>を例示。
場所 (where)	<物理的管理策> <u>レベルごとの物理的管理策の対象を例示。</u> - レベル1:本社受付・応接スペース・商談室・倉庫 - レベル2:本社受付・応接スペース・商談室・倉庫 - レベル3:サーバールーム/鍵付きサーバーラック	内容 (what)	<人的管理策> <u>教育のテーマ(情報セキュリティ関連規程、関連法令)</u>を例示。 <物理的管理策> <u>セキュリティ領域の設定に必要な情報を例示。</u> <技術的管理策> <u>利用者の認証方法</u>を例示。 - 利用者の認証に用いるアカウントは、利用者1名につき1つを発行する。 - 同一アカウントの他者との共有および複数の利用者が共有するアカウントの発行を禁止する <u>パスワードの設定条件</u>を例示。 - 十分な強度のあるパスワードを用いる。 - 他者に知られないようにする。

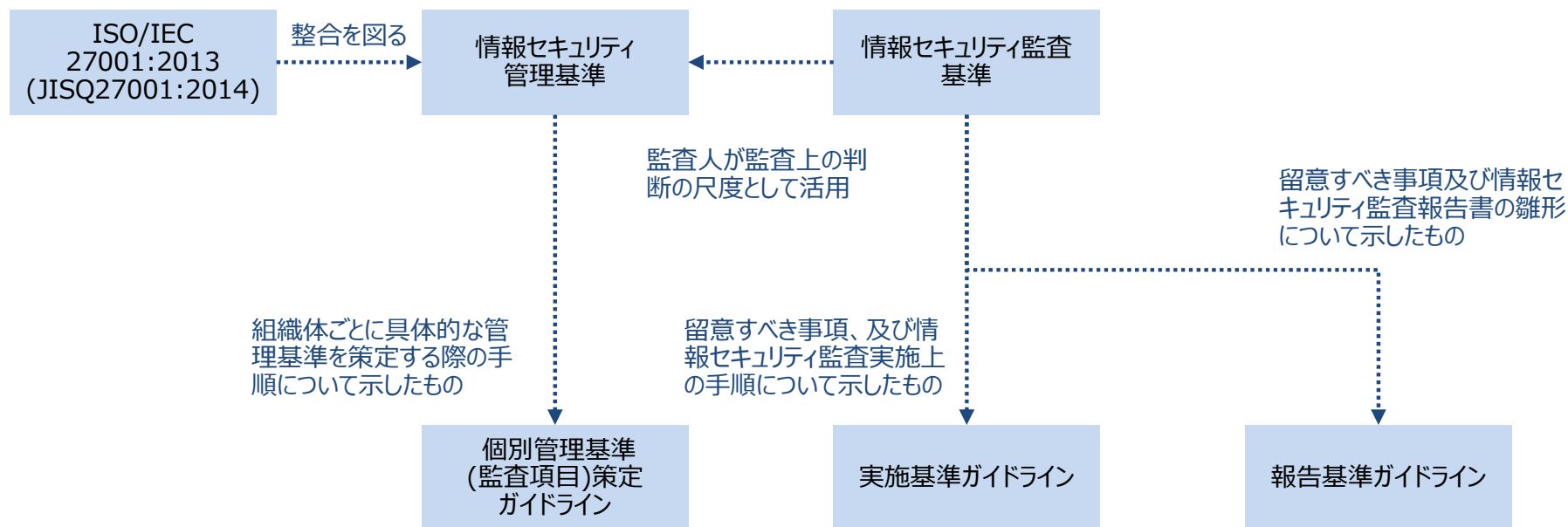
- 情報セキュリティ管理基準は、業界や事業活動を考慮して組織体が独自に管理基準を策定するための参考資料として位置づけられる。

位置づけ/参照関係

- 情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール(管理策)を整備・運用するための基準。また、情報セキュリティ監査基準は、監査を行う場合、監査人が監査上の判断の尺度として用いるべき基準

情報セキュリティ管理基準において、「組織体が属する業界又は事業活動の特性等を考慮し、必要に応じて本管理基準の趣旨及び体系に則って、本管理基準の項目等を取捨選択、追加又は統合することにより、該当する関係機関において独自の管理基準を策定し活用することが望ましい。」とされている。

ガイドライン等



[凡例] 認証制度 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

- 記載粒度の調査対象としては、情報セキュリティ管理基準が適当であったが、ISO/IEC 27001:2013との整合性を図っており、内容に大きな差異はなかった。

項目	目的	想定読者
情報セキュリティ管理基準	組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール(管理策)を整備・運用するための実践的な規範。	ISMS認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織、情報セキュリティ監査を受ける組織など幅広い利用者を想定
個別管理基準(監査項目)策定ガイドライン	本ガイドラインは、「情報セキュリティ管理基準」に従って、組織体ごとに具体的な管理基準を策定する際の手順について示したもの。	-
情報セキュリティ監査基準	情報セキュリティ監査基準は、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範。	監査人
実施基準ガイドライン	実施基準ガイドラインは、情報セキュリティ監査基準のうち実施基準に係る基本的な考え方を踏まえ、特に留意すべき事項、及び情報セキュリティ監査実施上の手順について示したもの。	-
報告基準ガイドライン	報告基準ガイドラインは、情報セキュリティ監査基準のうち、報告基準に係る基本的な考え方を踏まえ、特に留意すべき事項及び情報セキュリティ監査報告書の雛形について示したもの。	-

- 記載粒度の調査対象としては、適切なコントロール（管理策）を整備・運用するための実践的な規範情報セキュリティ管理基準が適当である。
- 一方で、当該基準は、ISO/IEC 27001:2013との整合性を図っており、内容に大きな差異はなかった。

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

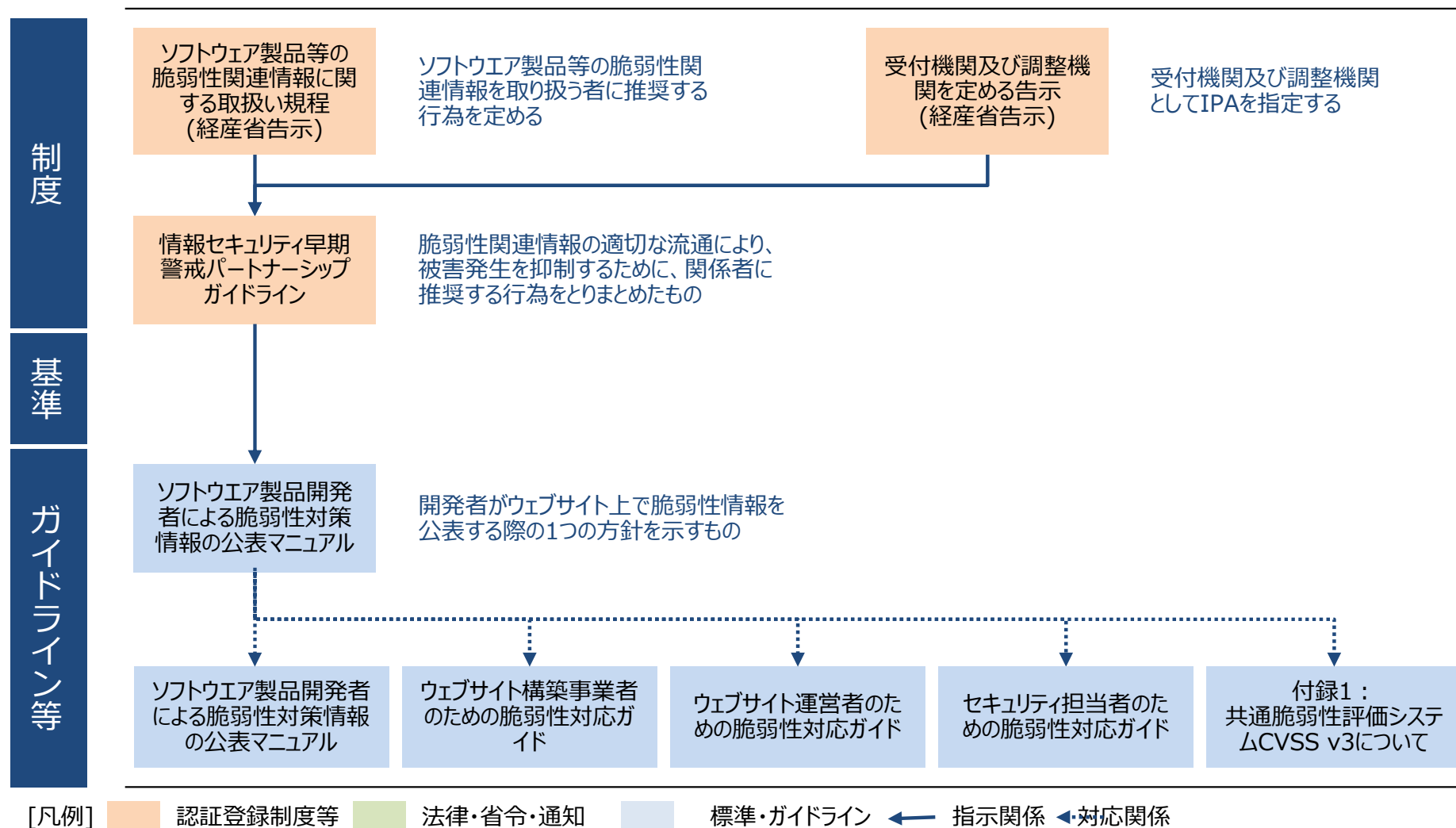
情報セキュリティ管理基準 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、全ての項目をほとんど満たしている。
- 情報セキュリティ管理基準は、ISO/IEC 27001を参照していることからマネジメントに焦点が当てられており、統制や識別、防御、検知に漏れが発生していないと考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

- 経産省告示(ソフトウェア等脆弱性関連情報取扱基準/ソフトウェア製品等の脆弱性関連情報に関する取扱規程)を踏まえ公表された「情報セキュリティ早期警戒パートナーシップガイドライン」の別冊として、情報セキュリティ早期警戒パートナーシップガイドラインが公表された。



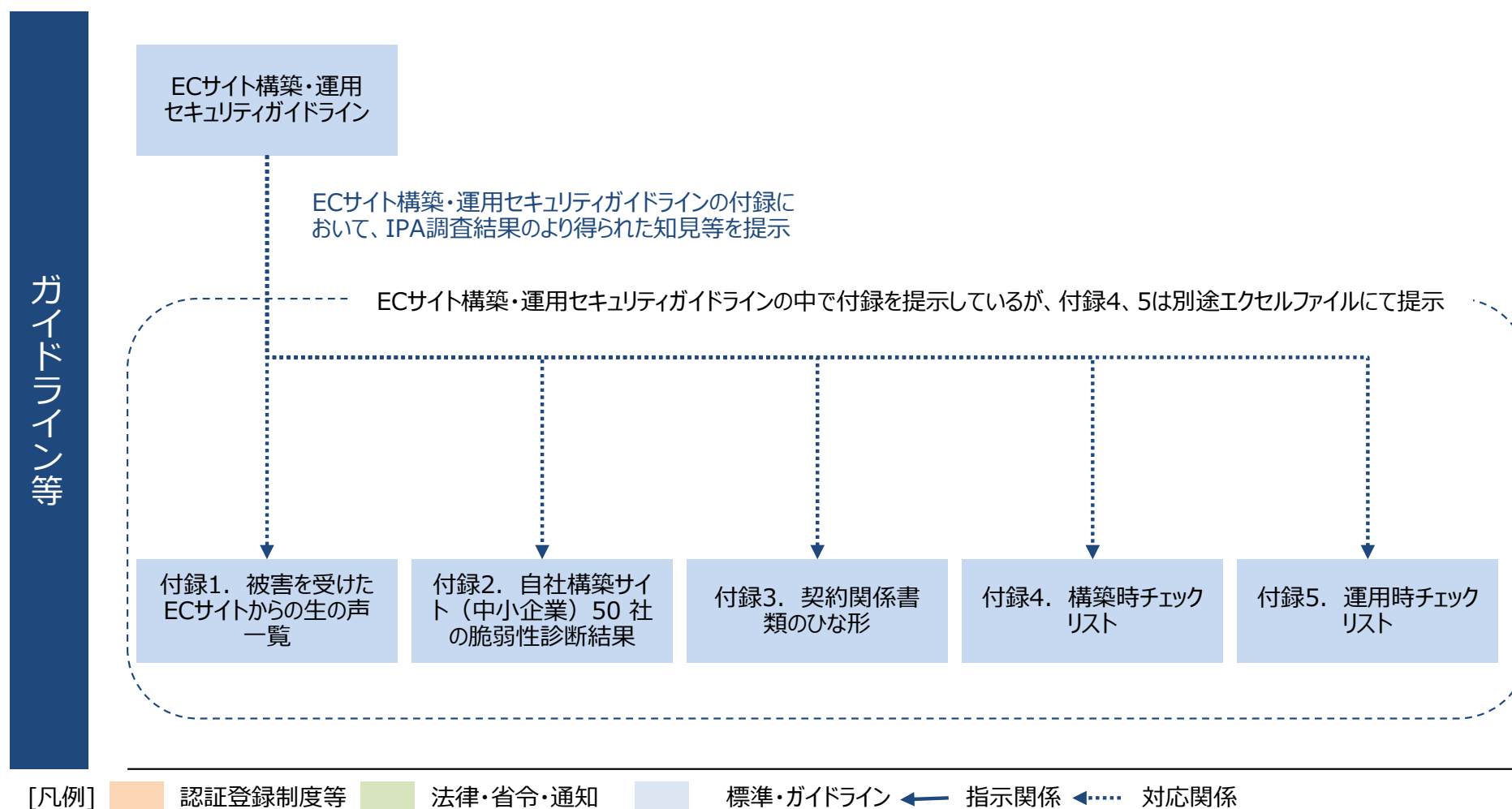
2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル
目的等

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- ソフトウェア製品開発者による脆弱性対策情報の公表マニュアルは、開発者がウェブサイト上で脆弱性情報を公表する際の1つの方針を示すもの。

項目	目的	想定読者
情報セキュリティ早期警戒パートナーシップガイドライン	本ガイドラインは、経産省告示(注:ソフトウェア等脆弱性関連情報取扱基準/ソフトウェア製品等の脆弱性関連情報に関する取扱規程)を踏まえ、<u>脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたもの。</u>	- ソフトウェアやウェブアプリケーションに<u>脆弱性を発見した方</u> <u>自組織が扱うソフトウェア製品の脆弱性について連絡を受けた方</u> <u>自組織のウェブアプリケーションの脆弱性について連絡を受けた方</u>
ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル	本マニュアルは、<u>脆弱性対策情報を必要としている利用者に的確に届けられることを目的</u>として、<u>開発者がウェブサイト上で脆弱性情報を公表する際の1つの方針を示すもの。</u>	<u>ソフトウェア製品開発者</u>
ウェブサイト構築事業者のための脆弱性対応ガイド	本ガイドでは、<u>ウェブサイトに脆弱性を残さないようにするために行うべきことはなにか、またウェブサイトの脆弱性が発見された場合にどう対処するかを紹介</u>することが目的。	<u>ウェブサイトの構築を行うウェブサイト構築事業者</u>
ウェブサイト運営者のための脆弱性対応ガイド	本ガイドは、主にウェブサイト運営者に向けて、<u>ウェブサイトの脆弱性がもたらすトラブルや必要な対策の概説、さらにウェブサイト運営者による脆弱性対応の望ましい手順</u>などを紹介。	<u>ウェブサイト運営者</u>
セキュリティ担当者のための脆弱性対応ガイド	本ガイドの目的は、セキュリティ担当者が、<u>情報システムの脆弱性に対処する基本的な考え方を紹介</u>すること。	<u>情報セキュリティを担当する方</u>(特に情報システム分野に必ずしも詳しくない方を想定)
付録1： 共通脆弱性評価システムCVSS v3について	本資料は、IPAのウェブサイト『共通脆弱性評価システムCVSSv3概説』の記載から「<u>ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル</u>」に関連する<u>CVSSv3の説明箇所を抜粋</u>したもの。	-

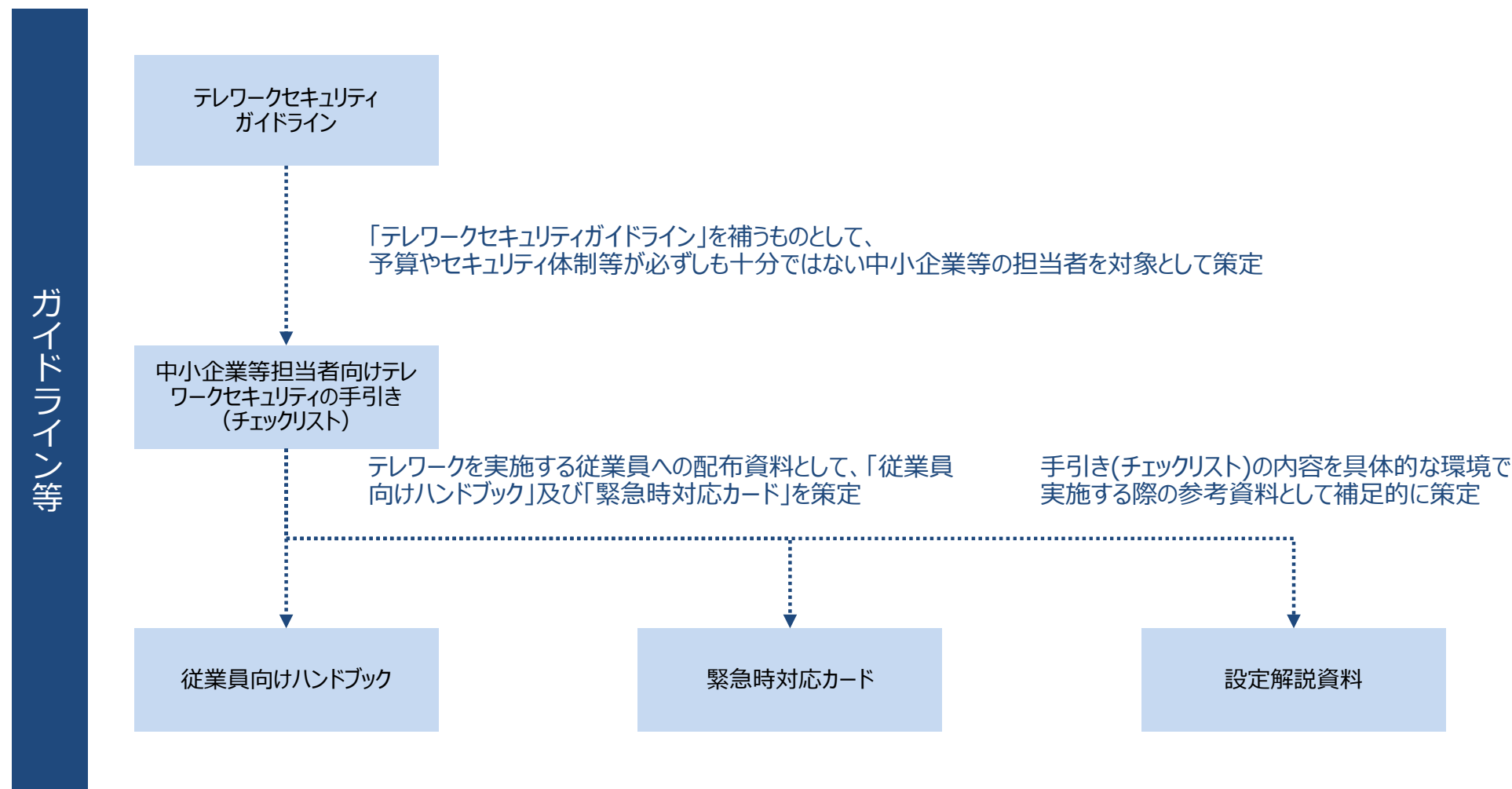
- ECサイト構築・運用セキュリティガイドラインは、経営者が実行すべき項目や、実務担当者が具体的に実践すべきセキュリティ対策の内容を示す。
- 付録において、IPAによる調査結果から得られた知見等を示している。



- ECサイト構築・運用セキュリティガイドラインは、ECサイトのセキュリティ確保のために経営者が実行すべき項目や、実務担当者が具体的に実践すべきセキュリティ対策の内容を、パッケージやスクラッチ開発による自社構築サイトを中心に記載したもの。

項目	目的	想定読者
ECサイト構築・運用セキュリティガイドライン	本ガイドラインは、ECサイトを構築、運営されている中小企業の皆様に、<u>ECサイトのセキュリティ対策を実施することがいかに重要であるかをご認識いただくため、ECサイトのセキュリティ確保のために経営者が実行すべき項目や、実務担当者が具体的に実践すべきセキュリティ対策の内容を、パッケージやスクラッチ開発による自社構築サイトを中心に記載</u>したもの。	- 中小企業の以下の方々を対象。 - ECサイトを新規に構築しようとしている経営者 - SaaS型サービスの利用も含む既にECサイトを運営している経営者 - 経営者から指示を受けたECサイトの構築および運用担当者、関係者および外部委託先事業者
付録1. 被害を受けたECサイトからの生の声一覧	被害を受けたECサイト運営事業者へのヒアリング調査結果の中から、<u>特に参考になる事例を生の声</u>として紹介。	(特に記載はないが、付録であるため「ECサイト構築・運用セキュリティガイドライン」と同じと考えられる。)
付録2. 自社構築サイト（中小企業）50社の脆弱性診断結果	中小企業のECサイトにおけるセキュリティ対策状況を把握するために実施した<u>脆弱性診断の結果</u>を詳しく紹介。	(特に記載はないが、付録であるため「ECサイト構築・運用セキュリティガイドライン」と同じと考えられる。)
付録3. 契約関係書類のひな形	外部委託先事業者とECサイトの構築契約を締結する際に、<u>外部委託先事業者に提示する仕様書の具体例を紹介</u>。	(特に記載はないが、付録であるため「ECサイト構築・運用セキュリティガイドライン」と同じと考えられる。)
付録4. 構築時チェックリスト	新規に構築する予定のECサイトが、<u>ECサイトの構築時におけるセキュリティ対策要件をどれくらい実装しているか確認する際に用いるチェックリスト</u>を提供。	(特に記載はないが、付録であるため「ECサイト構築・運用セキュリティガイドライン」と同じと考えられる。)
付録5. 運用時チェックリスト	運営中のECサイトが、<u>ECサイトの運用時におけるセキュリティ対策要件をどれくらい実装しているか確認する際に用いるチェックリスト</u>を提供。	(特に記載はないが、付録であるため「ECサイト構築・運用セキュリティガイドライン」と同じと考えられる。)

- ・ テレワークセキュリティガイドラインは、テレワークを導入・活用するための指針となるよう策定された。
- ・ 補足資料として、中小企業等の担当者を対象としたガイドライン等が策定されている。



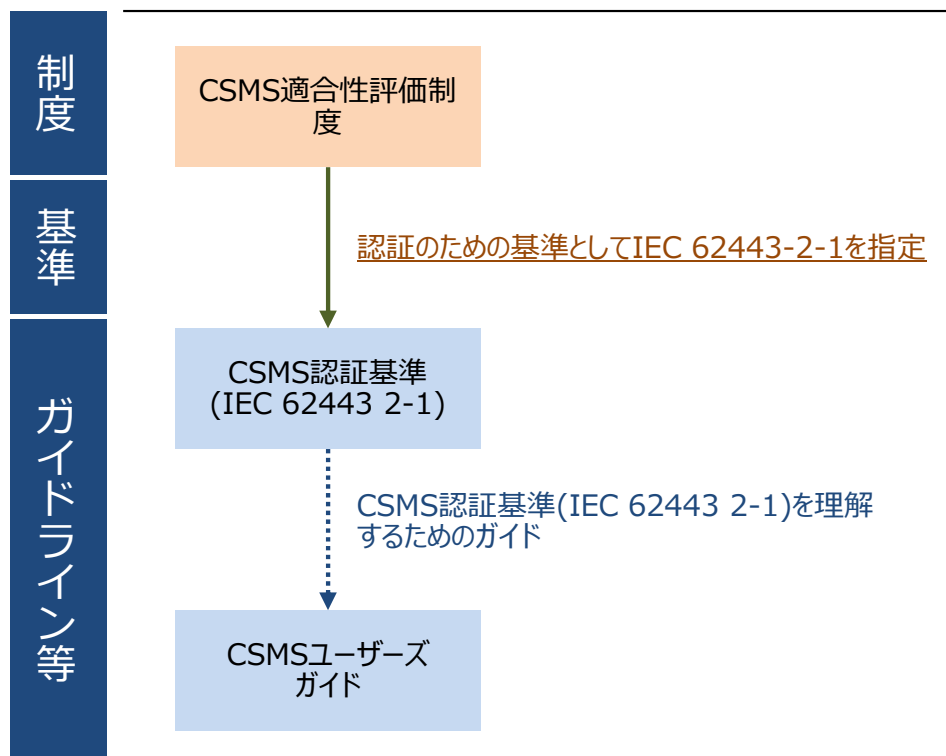
[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

- テレワークセキュリティガイドラインはテレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針となるよう策定。

項目	目的	想定読者
テレワークセキュリティガイドライン	本ガイドラインは、テレワークを取り巻く環境やセキュリティ動向の変化を踏まえた上で、テレワークの導入を検討しようとしている企業等のみならず、既にテレワークを導入している企業等においても、テレワークを業務に活用する際のセキュリティ上の不安を払拭し、<u>安心してテレワークを導入・活用するための指針となるよう策定。</u>	システム・セキュリティ管理者のほか<u>経営者やテレワーク勤務者も幅広く対象</u>
中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）	- テレワークセキュリティガイドラインを補うものとして、予算やセキュリティ体制等が必ずしも十分ではない中小企業等の担当者を対象としたもの。 - 具体的には、<u>中小企業等の担当者がテレワークを導入し、利用を進めるに当たり、中小企業等が考慮すべきセキュリティリスクを踏まえ、中小企業等においても実現可能性が高く優先的に実施すべきセキュリティ対策</u>を具体的に示す。	(中小企業における)<u>システム・セキュリティ管理者</u>
従業員向けハンドブック	本書は、テレワークを行う<u>従業員が常に反復して気を付けるべきことやもしもの時の連絡先等を記載したものの。</u>	テレワークを実施する従業員
緊急時対応カード	本書は、<u>テレワークを行う従業員が困った際にどういった行動を最優先にすべきか記載したものの。</u>	テレワークを実施する従業員
設定解説資料	設定解説資料は、手引き(チェックリスト)の内容を具体的な環境で実施する際の参考資料として、テレワークで多く利用される製品を対象として補足的に作成している資料。	(特に記載はないが、「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)」と同様と考えられる。)

- 本基準は、制御システムセキュリティにおけるサイバーセキュリティリスクマネジメントシステムを確立、実施、維持及び継続的に改善するための一般要求事項を定めている。

位置づけ/参照関係



[凡例]

オレンジ色の箱 認証登録制度等
青い箱 標準・ガイドライン
緑色の箱 法律・省令・通知

→ 指示関係 ←..... 対応関係

目的/想定読者

項目	目的	想定読者
CSMS適合性評価制度	CSMS適合性評価制度は、<u>産業用オートメーション及び制御システム</u> (IACS: Industrial Automation and Control System) を対象とした<u>サイバーセキュリティリスクマネジメントシステムに対する第三者認証制度</u>。	- 制御システムを保有する事業者 (<u>アセットオーナー</u>) - 制御システムの構築事業者 (<u>システムインテグレータ</u>) - 制御システムの<u>運用・保守事業者</u>
CSMS認証基準 (IEC 62443 2-1)	制御システムセキュリティにおけるサイバーセキュリティリスクマネジメントシステムを確立、実施、維持及び継続的に改善するための<u>一般要求事項を定める</u>。	
CSMSユーザーズガイド	CSMSパイロット事業者から得られた知見をもとに、制御システム関係者が、CSMSを構築・運用し、認証取得を目指す取組に資する<u>CSMSの基本的な考え方や認証基準の解釈、留意点を紹介</u>。	

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

CSMS認証基準
記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 多層防御を前提としている制御システムにおいて、識別、防御及びそれを支える統制に重点を置いて認証基準が策定されていると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

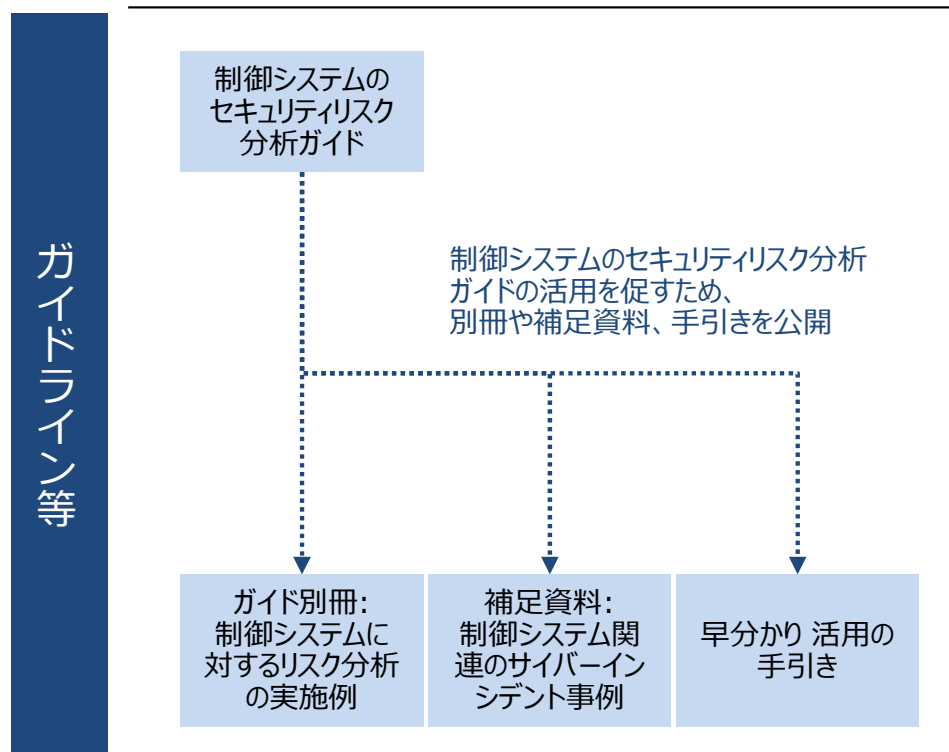
- 比較対象とした要件においては場所に係る具体的な情報は記載されていなかったが、主体や内容に係る情報が記載されている。

項目	記載粒度
主体(who)	<人的管理策> - 教育内容ごとに<u>教育対象</u>を示す。 ✓ [手順及び設備について]従業員、契約従業員、サードパーティ契約者 ✓ [リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組]本取組に関連する要員 <技術的管理策> <u>認証を行う対象</u>を示す。 ✓ システム管理者アクセスアカウント ✓ アプリケーション構成アクセスアカウント ✓ リモートユーザ(アカウント)
内容(what)	<組織的管理策> - 資産を管理するために作成する<u>ネットワーク図に記載する情報</u>を示す。 ✓ 主要装置 ✓ ネットワークの種類 ✓ 機器の設置場所 <人的管理策> <u>教育内容</u>を示す。 ✓ 手順及び設備 ✓ リスクマネジメント、IACSのエンジニアリング、システム/保守、CSMSに影響を与える取組 <技術的管理策> <u>具体的に制限するアクセスの内容</u>を示す。 ✓ 一定回数の失敗した後のログイン ✓ 一定期間経過後のリモートユーザの再アクセス
頻度(when)	<人的管理策> <u>教育のタイミング</u>を示す。 ✓ 契約時 ✓ 定期的なタイミング(期間の記載はなし)
場所(where)	(場所に関する具体的な記載なし)

- IPAにおけるノウハウを織り込んだ本ガイドは、セキュリティリスクの全体像を理解し分析を具体的に実施するための手順や手引きを示している。

本ガイドは分析を行うための手順や手引きを示すものであるため、CSFの「リスクアセスメント」(識別)に焦点を当てたガイドラインと認識。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

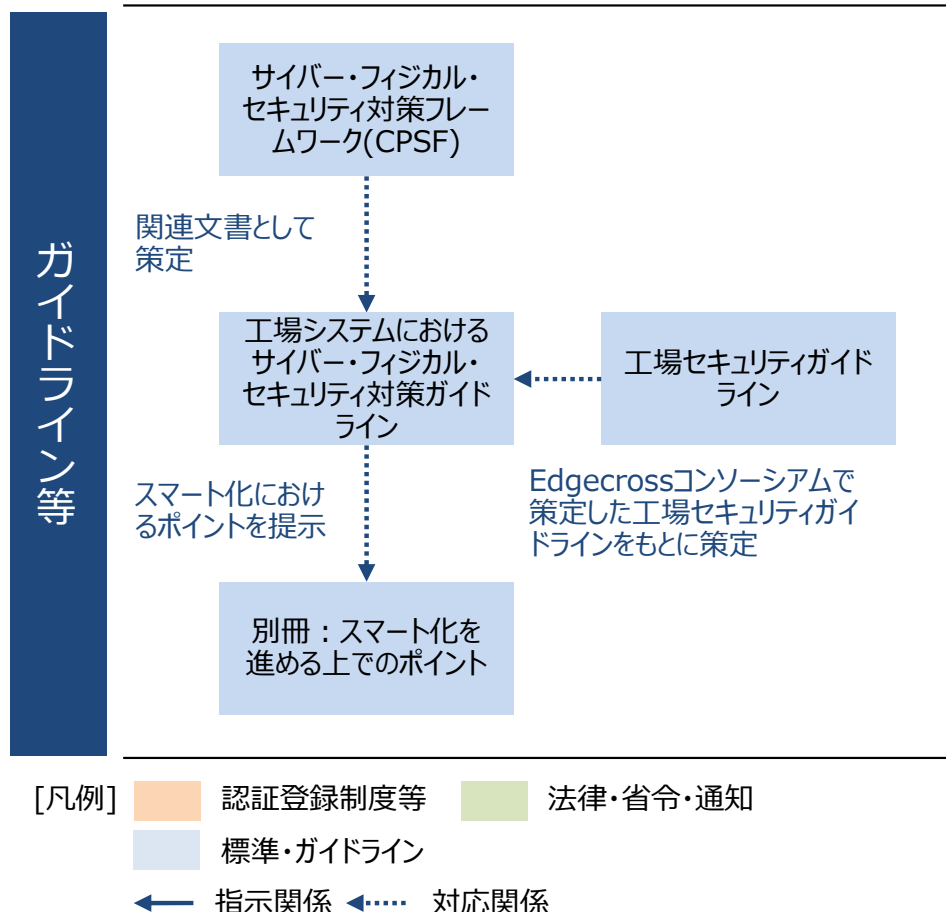
[参考] IPA「制御システムのセキュリティリスク分析ガイド 第2版」等
<https://www.ipa.go.jp/security/controlsysterm/riskanalysis.html>

目的/想定読者

項目	目的	想定読者
制御システムのセキュリティリスク分析ガイド	- 本ガイドは、以下を目的とする。 - セキュリティリスク分析の全体像の理解を深め、その取組を促す - セキュリティリスク分析を具体的に実施するための手順や手引きを示す - IPAにおいて実践したセキュリティリスク分析でのノウハウを手引き織り込む	-
ガイド別冊: 制御システムに対するリスク分析の実施例	- 典型的なモデルシステムに対して、資産ベースのリスク分析と事業被害ベースのリスク分析の実施事例を解説、提示。その目的は、以下の3点である。 - リスク分析の全体イメージと評価結果の提示 - リスク分析シートの結果の提示による全体素材の提供 - リスク分析シートのまとめ方のバリエーションの紹介	
制御システム関連のサイバーインシデント事例	本資料は、事業被害ベースのリスク分析における攻撃事例の活用を支援するための補足資料。	
早分かり 活用の手引き	セキュリティリスク分析ガイドの活用にあたって概要を示す。	

- 本ガイドラインは、業界団体や個社が自ら工場分野におけるセキュリティ対策を企画・実行するに当たり、参照すべき考え方やステップを手引きとして示す。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
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)	新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し、リスク源を明らかにしつつ、求められる<u>セキュリティ対策の全体像を整理</u>するとともに、産業界が自らの<u>セキュリティ対策に活用できる対策例をまとめたもの</u>。	「Society 5.0」において、付加価値の創造活動に取り組む主体
工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	本ガイドラインは、業界団体や個社が自ら対策を企画・実行するに当たり、<u>参照すべき考え方やステップを「手引き」として示し</u>、必要最小限と考えられる<u>対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記</u>。	工場のスマート化を進めている、または検討している企業におけるIT関係部門、生産関係部門、戦略マネジメント部門、監査部門、リスク管理部門、DX担当部門、機器システム提供ベンダ、機器メーカー
別冊：スマート化を進める上でのポイント	<u>スマート化におけるポイントを提示すること</u>を通じ、先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しすることを目的とする。	

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 検知、対応、復旧の部分について記載しつつも、統制や識別、防御の各対策においてCSFと比較して漏れがないよう策定されていると考えられる。

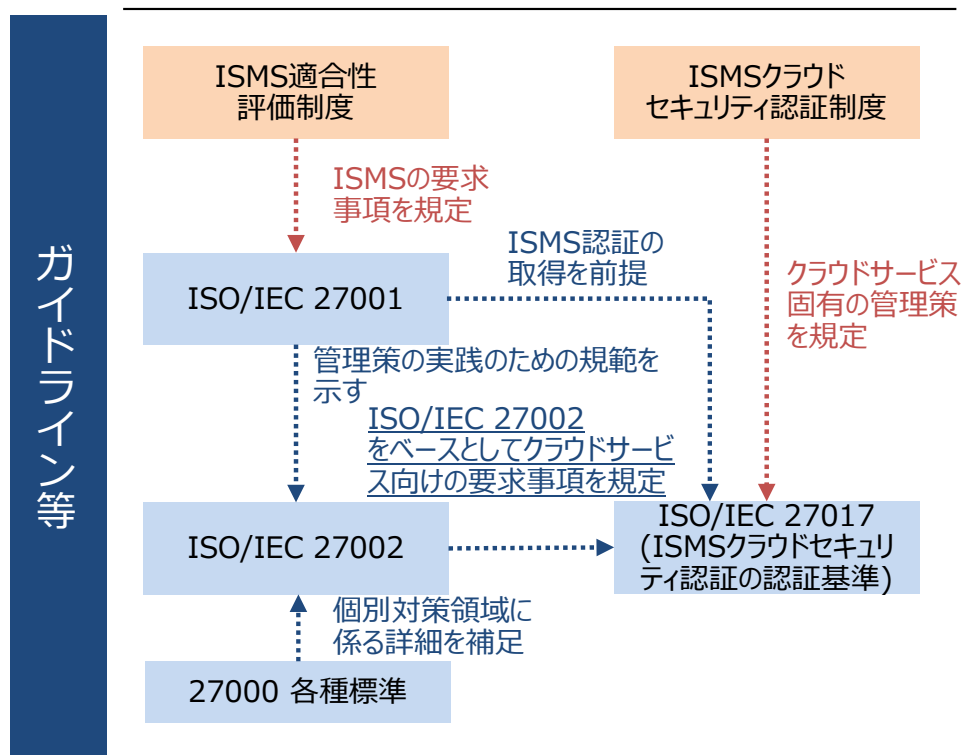
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	1/2
	監督	○			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	2/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							19/22

- 本ガイドラインでは、内容面(what)でより具体的な内容が記載されていた。
- 組織的管理策において、資産管理を行う際に参考となるよう具体的な資産の要素が記載されている。

項目	記載粒度
頻度(when)	(頻度に関する記載なし)
場所(where)	(場所に関する記載なし)
主体(who)	(主体に関する記載なし)
内容(what)	<組織的管理策> - 資産管理を行う際の参考となるよう、想定される<u>資産の要素</u>の例を示す。 ✓ <u>ネットワーク機器、及びネットワーク</u> VPN装置兼ファイアウォール、無線LAN-AP、設備系ネットワーク、生産管理系ネットワーク、情報系ネットワーク ✓ <u>装置・機器</u> MESサーバ、生産ライン、保守端末(常時非接続)、SCADA、AGV制御 PC、AGV、自動倉庫、自動倉庫遠隔保守用サーバ、OA 系サーバ、OA 端末 ✓ <u>データ</u> 生産計画、生産指示(生産機種・量)、生産レシピ、生産実績(トレサビデータ)、設備状態、設備プログラム・パラメタ・図面、部材在庫量(現場)、部材在庫量(倉庫)

- 本文書は、クラウドサービスを含む情報セキュリティマネジメントシステムを確立し、実施し、維持し、継続的に改善するためのISMSクラウドセキュリティ認証のための要求事項を提供。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
→ 指示関係 -.-> 対応関係

目的/想定読者

項目	目的	想定読者
ISMSクラウドセキュリティ認証の認証基準 (ISO/IEC 27017)	本文書は、クラウドサービスを含む情報セキュリティマネジメントシステムを確立し、実施し、維持し、継続的に改善するためのISMSクラウドセキュリティ認証のための要求事項を提供する。	- クラウドサービスプロバイダ - クラウドサービスカスタマ

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

ISMSクラウドセキュリティ認証に関する要求事項

記載範囲

A-1. 体系内の位置づけ

A-2. 体系間の位置づけ

B-1. 記載範囲

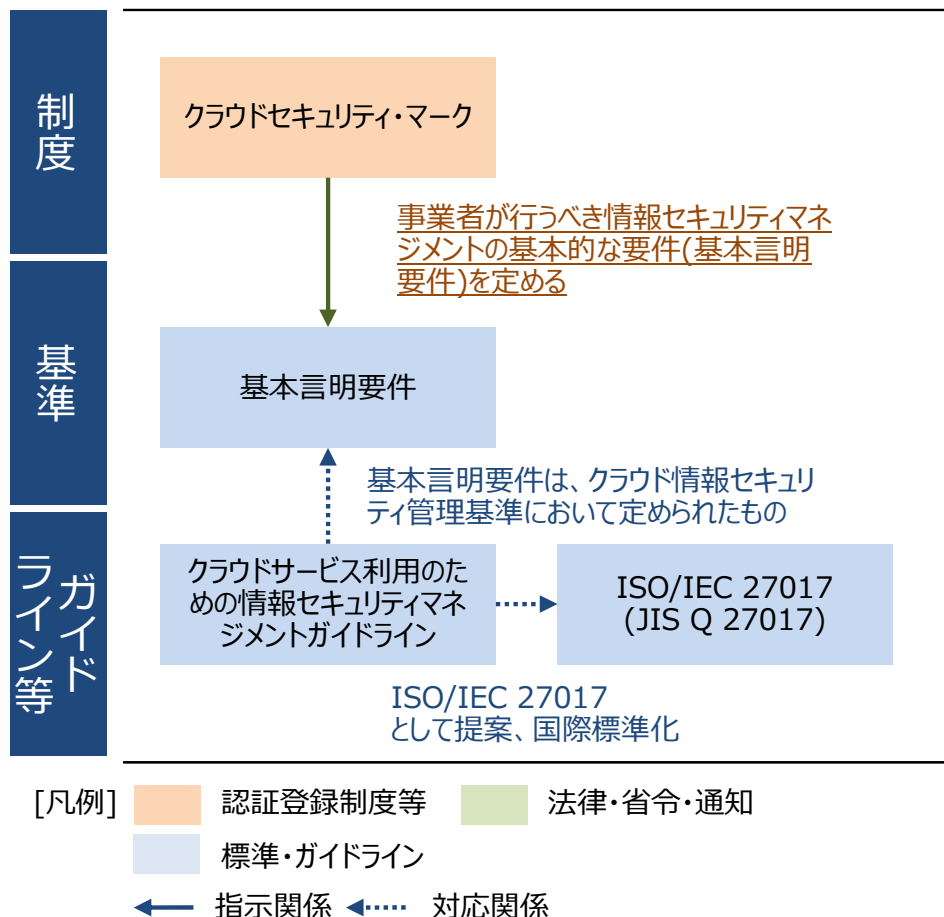
B-2. 記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- なお、ISMSクラウドセキュリティ認証はISMS認証の取得を前提としているため、ISO/IEC 27001に含まれている要求事項も含めてカウントしている点に留意いただきたい。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

- 本ガイドラインは、クラウドコンピューティングを利用する組織において情報セキュリティ対策が円滑に行われることを目的として策定された。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
クラウドセキュリティ・マーク	- 日本セキュリティ監査協会が提供するマーク。 - 要件を満たしていると認定された監査を受けた場合、CSマーク(クラウドセキュリティ・マーク)が使用可能となる。 - マークは、ゴールド(適合監査)とシルバー(自主監査)の2種類。	クラウドサービスプロバイダ
クラウドサービス利用のための情報セキュリティマネジメントガイドライン	クラウド利用者の視点から JIS Q 27002(実践のための規範)の各管理策を再考し、クラウドコンピューティングを利用する組織において情報セキュリティ対策が円滑に行われることを目的として、ガイドラインを作成。	クラウドサービスプロバイダ

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

クラウドサービス利用のための情報セキュリティマネジメントガイドライン

記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- ISO/IEC 27017の前身となっているため、ISMSクラウドセキュリティ認証に関する要求事項と本ガイドラインの記載範囲に大きな差異はみられなかった。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

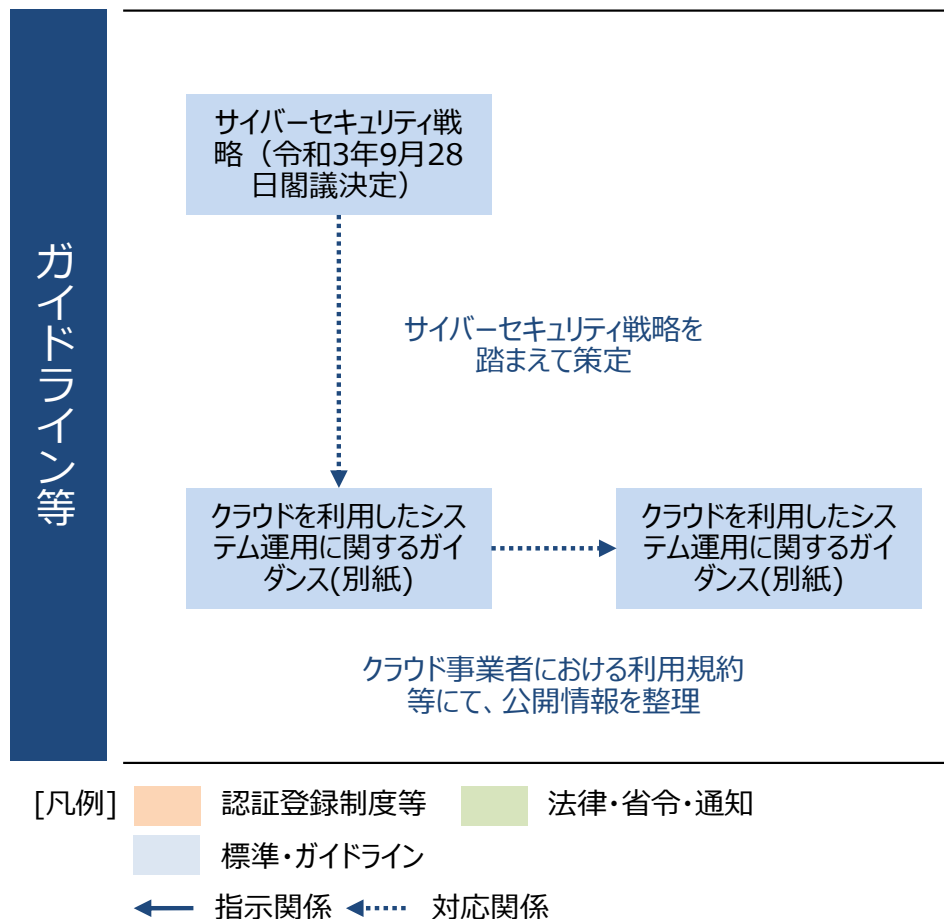
- 本ガイドラインでは、クラウドサービスの利用者及びクラウドサービス事業者がクラウドサービスの利用や提供において考慮すべき具体的な事項が記載されている。

項目	記載粒度
主体(who)	<人的管理策> - 管理策にて、教育対象を示す。 ✓ 組織のすべての従業員 ✓ 契約相手(関係する場合) ✓ 第三者の利用者(関係する場合)
内容(what)	<組織的管理策> - 管理策の関連情報にて、クラウドサービス環境にあるクラウド利用者の資産を示す。 ✓ 業務上の情報 ✓ 仮想化された装置 ✓ 仮想化されたストレージ ✓ ソフトウェア * なお、SaaSにて使用するソフトウェアは、IaaS事業者から見ると、自社の提供する IaaS サービス上にあるクラウド利用者の資産と解される場合がある旨を記載 <人的管理策> - 実施の手引きにて、クラウドサービスの情報セキュリティに関する教育・訓練内容を例示。 ✓ クラウドサービス利用のための方針、基準及び手順などの規程類 ✓ クラウドサービスごとの情報セキュリティリスク及びその対策 ✓ クラウドサービスを使用するにあたり考慮すべきシステム及びネットワーク環境におけるリスク <物理的管理策> - 管理策にて、物理的セキュリティ境界を例示。 ✓ 壁 ✓ カード制御による入口 ✓ 有人の受付

項目	記載粒度
内容(what) (続き)	<技術的管理策> - クラウド事業者の実施が望まれる事項にて、<u>サービス利用者IDの登録・削除を管理する機能においてクラウド事業者が提供することが望ましい情報</u>を示す。 ✓ 利用者 ID 登録・削除の手順 ✓ 利用者 ID 登録・削除に必要な情報 ✓ 利用者の同一性検証の仕様 ✓ サービスの一部として利用者ID管理ツールを提供している場合は、利用者ID管理ツールの仕様 - クラウド事業者の実施が望まれる事項にて、<u>サービスに係る特権を管理する機能においてクラウド事業者が提供することが望ましい情報</u>を示す。 ✓ クラウド利用者の特権の種類及び役割 ✓ クラウド利用者の特権アカウント使用の監視・管理機能の仕様 ✓ クラウド利用者の特権アカウント使用に関するログ - クラウド事業者の実施が望まれる事項にて、<u>パスワードの割当ての管理機能においてクラウド事業者が提供することが望ましい情報</u>を示す。 ✓ パスワードの発行、変更及び再発行の手順 ✓ パスワード割当てにおける認証及び認証の仕組み(例えば、多要素認証を用いた認証方法など)
頻度(when)	<技術的管理策> - 管理策の目的にて、<u>アクセス権の割当てにおいて考慮すべきタイミング</u>を示す。 ✓ 利用者の初期登録時 ✓ 情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除時
場所(where)	(場所に関する記載なし)

- 本ガイダンスは、クラウドサービスの利用者がクラウドサービスの基本を理解し、クラウドサービスにおけるインシデントの発生を可能な限り抑制することや、インシデントが発生した際の対応及びステークホルダーの連携によって事態の解決を図る重要性など、クラウドサービスの安全な運用に重点を置いた基本的なガイダンス。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
クラウドを利用したシステム運用に関するガイダンス	本ガイダンスは、増加するクラウドサービスの選定や利用、サービスを使った環境の構築や運用などを行うに当たり、クラウドサービスの利用者がクラウドサービスの基本を理解し、クラウドサービスにおけるインシデントの発生を可能な限り抑制することや、インシデントが発生した際の対応及びステークホルダーの連携によって事態の解決を図る重要性など、<u>クラウドサービスの安全な運用に重点を置いた利用者向けの基本的なガイダンス</u>。	クラウドサービス利用者
クラウドを利用したシステム運用に関するガイダンス(別紙)	クラウド事業者における利用規約等にて、公開情報をまとめたもの。	-

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

クラウドを利用したシステム運用に関するガイダンス 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- なお、B-2.記載粒度については、比較を行う要件においてISO27001と比較した際に具体的な記載がみられなかった。

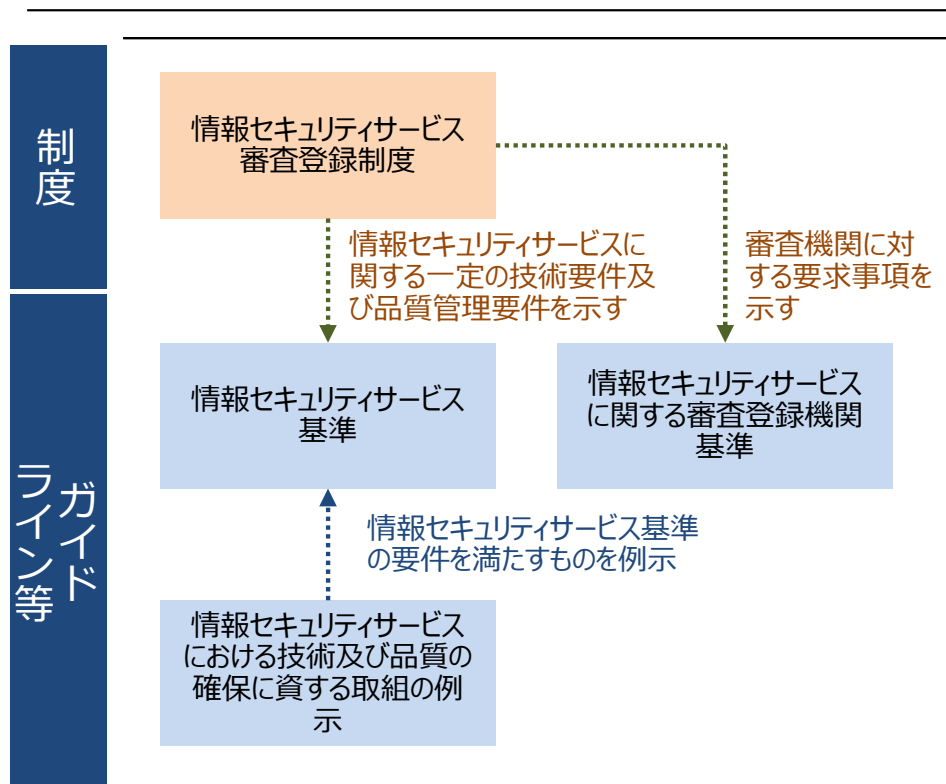
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	5/6	防御 (続き)	データセキュリティ	○	3/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	2/3		インシデント分析	○	
	リスクアセスメント	-			インシデント対応の方向とコミュニ ケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	-	
合計							16/22

* B-2.記載粒度については、比較を行う要件においてISO27001と比較した際に具体的な記載がみられなかった。

- 本基準は、情報セキュリティサービス業の普及を促進し国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的として、情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示したもの。

* 本制度は「情報セキュリティ監査サービス」、「脆弱性診断サービス及びペネトレーションテスト(侵入試験)サービス」、「デジタルフォレンジックサービス」、「セキュリティ監視・運用サービス」、「機器検証サービス」に係る審査基準等を示しており、CSFにおけるサプライチェーンリスクマネジメントにフォーカスしたものと理解している。記載範囲等の比較は行っていない点に留意いただきたい。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知

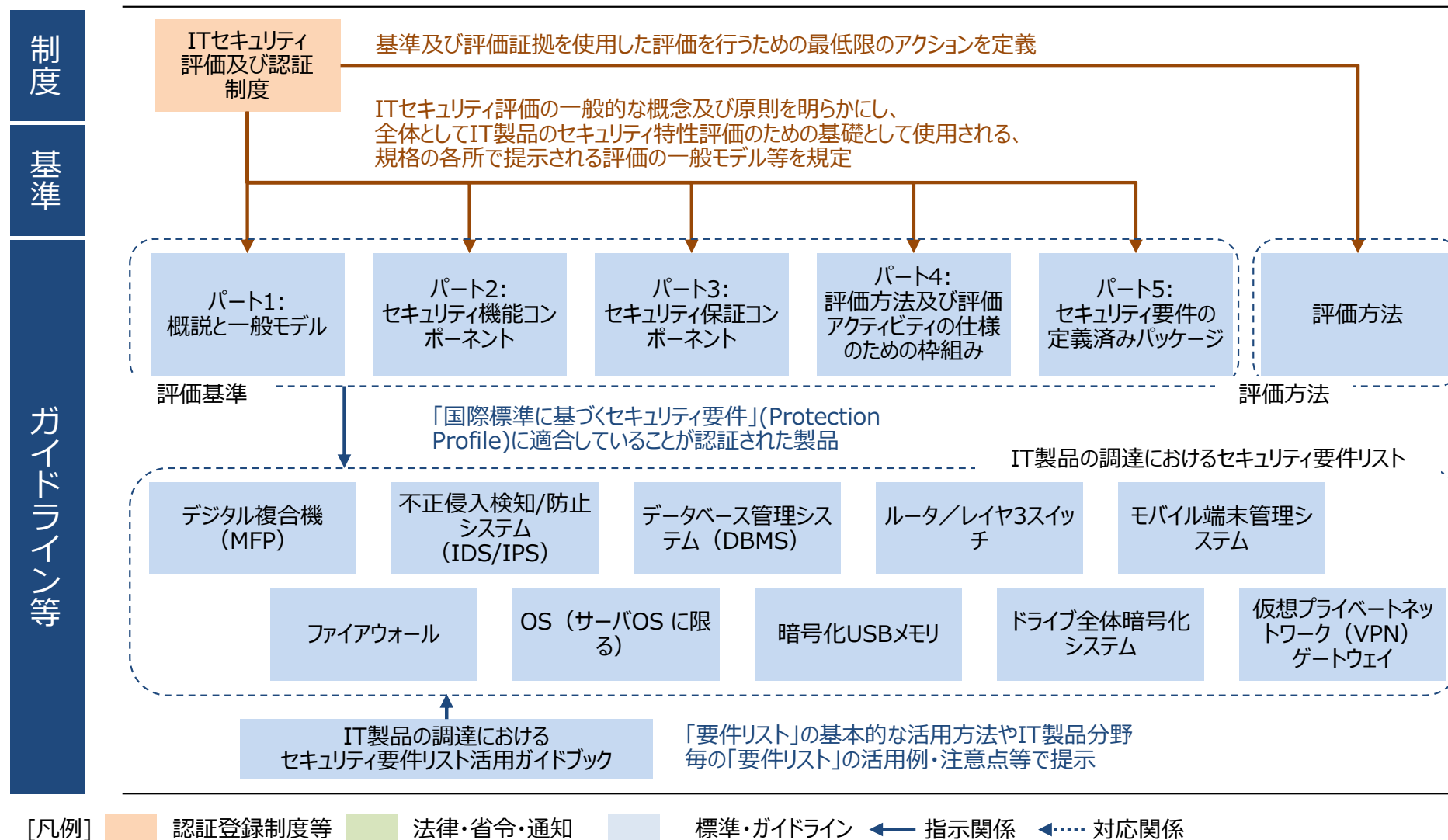
標準・ガイドライン

指示関係 対応関係

目的/想定読者

項目	目的	想定読者
情報セキュリティサービス基準	本基準は、<u>情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し</u>、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準を設けることで、情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的とする。	-
情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示	本文書は、情報セキュリティサービス基準において<u>それぞれの要件を満たすものを例示</u>することを目的とする。	-
情報セキュリティサービスに関する審査登録機関基準	本基準は、情報セキュリティサービスに関する<u>審査登録機関に対する要求事項について定めるもの</u>。	情報セキュリティサービスに関する審査登録機関

- IT製品の調達におけるセキュリティ要件リストでは、「国際標準に基づくセキュリティ要件」(Protection Profile)に適合していることが認証された製品をピックアップし掲載している。



- CC/CEM:2022におけるパート1では、ITセキュリティ評価の一般的な概念及び原則を明らかにし、全体としてIT製品のセキュリティ特性評価のための基礎として使用される、規格の各所で提示される評価の一般モデルを説明。

項目	目的	想定読者
パート1: 概説と一般モデル	本パートは、ITセキュリティ評価の一般的な概念及び原則を明らかにし、全体としてIT製品のセキュリティ特性評価のための基礎として使用される、<u>規格の各所で提示される評価の一般モデルを規定</u>する。	-
パート2: セキュリティ機能コンポーネント	本パートでは、<u>セキュリティ評価のために、セキュリティ機能コンポーネントの必要な構造及び内容を定義</u>している。これには、多くのIT製品の共通のセキュリティ機能性の要件を満たす機能コンポーネントのカatalogが含まれる	-
パート3: セキュリティ保証コンポーネント	本パートは、<u>CCの保証要件を定義</u>している。	-
パート4: 評価方法及び評価アクティビティの仕様のための枠組み	本パートは、客観的で、反復可能かつ再現可能な<u>評価方法及び評価アクティビティを規定するための標準化された枠組みを提供</u>する。	-
パート5: セキュリティ要件の定義済みパッケージ	本パートは、関係者の共通利用を支援するために有用であることが確認された<u>セキュリティ保証要件とセキュリティ機能要件のパッケージを提供</u>する。	-
評価方法	本文書は、評価者によって実施される CCで定義された基準及び評価証拠を使用した<u>CC評価を行うための最低限のアクションを定義</u>している。	-

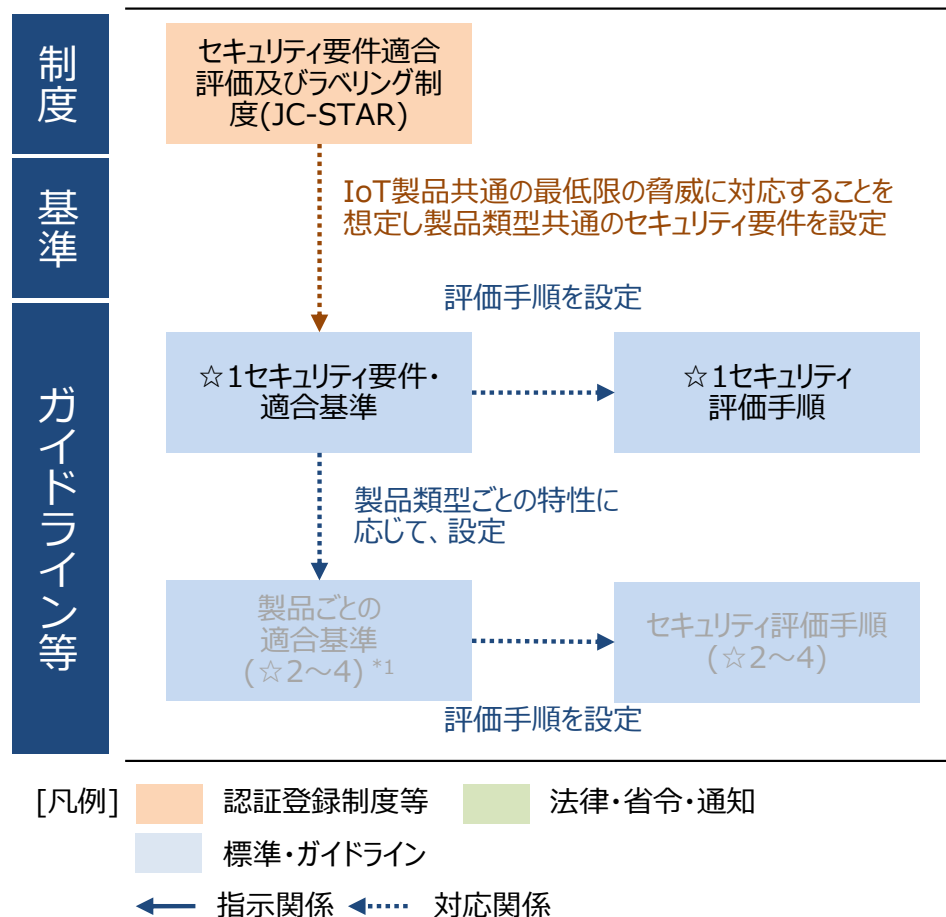
* 本制度は製品のセキュリティ機能コンポーネントの必要な構造及び内容を示すパート2は、特に「防御」に焦点を当てた規格と認識

- 本要件リストは、製品分野毎に考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめたもの。

項目	目的	想定読者
IT製品の調達におけるセキュリティ要件リスト	<u>製品分野毎に考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめたもの。</u> - 政府機関だけでなく一般企業、組織等で製品を調達する際、想定される脅威に対抗できる製品の調達に活用可能。 <以下、製品分野> デジタル複合機(MFP)、ファイアウォール、不正侵入検知/防止システム(IDS/IPS)、OS(サーバOSに限る)、データベース管理システム(DBMS)、暗号化USBメモリ、ルータ/レイヤ3スイッチ、ドライブ全体暗号化システム、モバイル端末管理システム、仮想プライベートネットワーク(VPN)ゲートウェイ	<u>政府機関</u>において、ITシステムやIT製品の調達を担当しており、NISCが策定した「政府機関の情報セキュリティ対策のための統一基準(平成28年度版)」を参照して、<u>調達要件を定めることを求められている方</u> <u>民間の企業・組織や地方公共団体</u>に所属し、ITシステムやIT製品を調達する担当の方で、「要件リスト」を活用して、<u>セキュアなIT製品を調達したい方</u>
IT製品の調達におけるセキュリティ要件リスト活用ガイドブック	本ガイドブックはIT製品の調達におけるセキュリティ要件リストを活用して、安全なIT製品を調達したい方を対象として、IT製品の調達におけるセキュリティ要件リストの<u>基本的な活用方法やIT製品分野毎の活用例・注意点等で提示</u>している。	

- セキュリティ要件適合評価及びラベリング制度(JC-STAR)では、IoT製品として共通して求められる最低限の適合基準を定めそれを満たすことをIoT製品ベンダが自ら宣言する☆1レベルで、セキュリティ適合基準やセキュリティ評価手順が示されている。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
セキュリティ要件適合評価及びラベリング制度(JC-STAR)	本制度は、インターネットとの通信が行える幅広いIoT製品を対象として、<u>共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的</u>とする。	IoT製品ベンダ(製造事業者・販売事業者)等
セキュリティ適合基準	- 適合基準は、<u>各適合性評価レベルで対象製品が適合すべき基準を示したもの。</u> <☆1評価レベル> - 製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことを製品ベンダが自ら宣言するもの	IoT製品ベンダ(製造事業者・販売事業者)等
セキュリティ評価手順	評価手順は、<u>適合基準に適合しているかを評価するための手順を示したもの。</u>	IoT製品ベンダ(製造事業者・販売事業者)等

*1 特定のレベルに求められるセキュリティ要件は、全体のセキュリティ要件の部分集合

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

セキュリティ要件適合評価及びラベリング制度(JC-STAR)

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

- IoT機器を対象とした制度であり、★1の要求事項では必ずしも対応や復旧は意識されていない。
- 組織を対象としたCSFと機器を対象とした本基準を比較しているため、偏りがみられたと考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	3/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	-	0/2
	監督	-			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	-	0/4
識別	資産管理	-	2/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	-	
合計		留意点					9/22

留意点

- ★1を対象として調査を行った点。(したがって、★2以上の要求事項で対応、復旧の点が考慮される可能性がある)

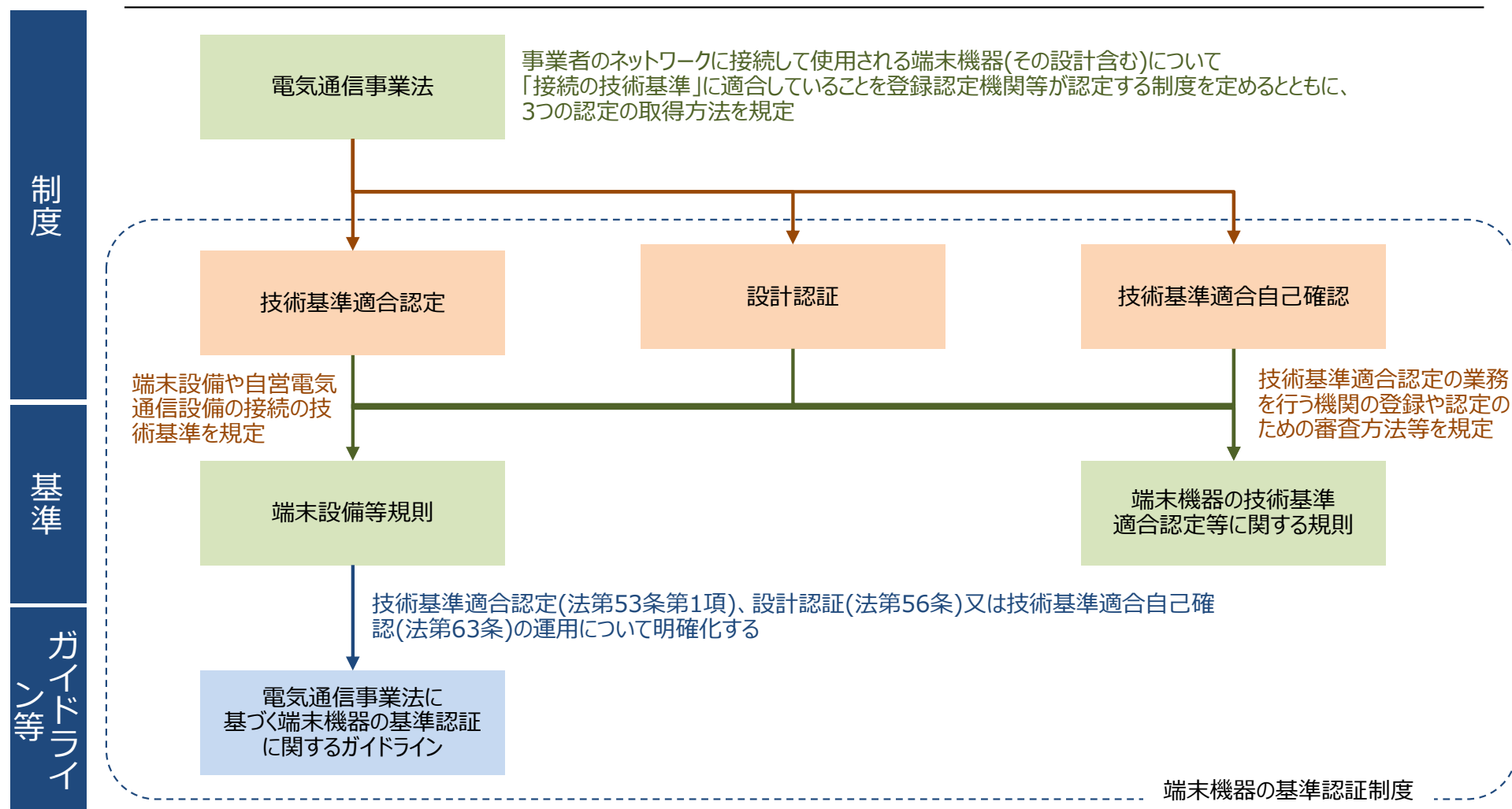
2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
セキュリティ要件適合評価及びラベリング制度(JC-STAR)
記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- JC-STARの★1では、アクセス制御を行う機能において具体的な記載がなされている。
- 初期設定時のパスワード変更にあたって遵守すべき事項を定めている。

項目	記載粒度
主体(who)	(主体に関する具体的な記載なし) 留意点 • 組織ではなくIoT機器を対象とした制度である点 • ★1を対象として調査を行った点。
内容(what)	<技術的管理策> • <u>デフォルトパスワードの変更にあって、遵守すべき事項を示す。</u> ✓ IoT機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること ✓ 初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードの設定を強制させること。
頻度(when)	<技術的管理策> • <u>パスワードの変更タイミング(初期設定時)</u>を示す。
場所(where)	(場所に関する具体的な記載なし)

- 電気通信事業法では、事業者のネットワークに接続して使用される端末機器(その設計含む)について「接続の技術基準」に適合していることを登録認定機関等が認定する制度を規定。



[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン → 指示関係 ⋯ 対応関係

- 電気通信事業法に基づく端末機器の基準認証に関するガイドラインでは、IoT機器を含む端末設備の技術基準にセキュリティ対策を追加した端末設備等規則の各規定等に係る端末機器の基準認証に関する運用について明確化。

項目	目的	想定読者
電気通信事業法	電気通信事業者の運営を適正かつ合理的なものとするとともに、電気通信役務の円滑な提供の確保と利用者の利益を保護し、公共の福祉を増進する。	-
技術基準適合認定	<u>端末機器一台毎に登録認定機関が審査し、技術基準に適合するものとして認定。</u>	-
設計認証	<u>端末機器の設計(設計に合致することの確認の方法含む)について登録認定機関が審査し、技術基準に適合する設計として認証。</u>	-
技術基準適合自己確認	<u>製造業者や輸入業者が、自ら検証し、端末機器の設計(設計に合致することの確認の方法含む)が技術基準に適合するものであることを確認し、総務大臣に届出。</u>	-
端末設備等規則	端末設備や自営電気通信設備の接続の技術基準を規定。	-
端末機器の技術基準適合認定等に関する規則	技術基準適合認定の業務を行う機関の登録や認定のための審査方法等を規定。	-
電気通信事業法に基づく端末機器の基準認証に関するガイドライン	IoT機器を含む端末設備の技術基準にセキュリティ対策を追加した端末設備等規則の各規定等に係る<u>端末機器の基準認証に関する運用について明確化。</u>	-

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

電気通信事業法に基づく端末機器の基準認証に関するガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- IoT機器のセキュリティ基準を示す本ガイドラインでは、機器に係る基準を示している。
- 防御の部分にフォーカスしてガイドラインが策定されていると考えられている。また、遵守が義務となっているため、最低限の要求事項が示されていると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	0/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	-			技術インフラのレジリエンス	○	
	ポリシー	-		検知	継続的モニタリング	-	0/2
	監督	-			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	-		対応	インシデントマネジメント	-	0/4
識別	資産管理	-	0/3		インシデント分析	-	
	リスクアセスメント	-			インシデント対応の方向とコミュ ニケーション	-	
	改善	-			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	-	
合計							4/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
電気通信事業法に基づく端末機器の基準認証に関するガイドライン
記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

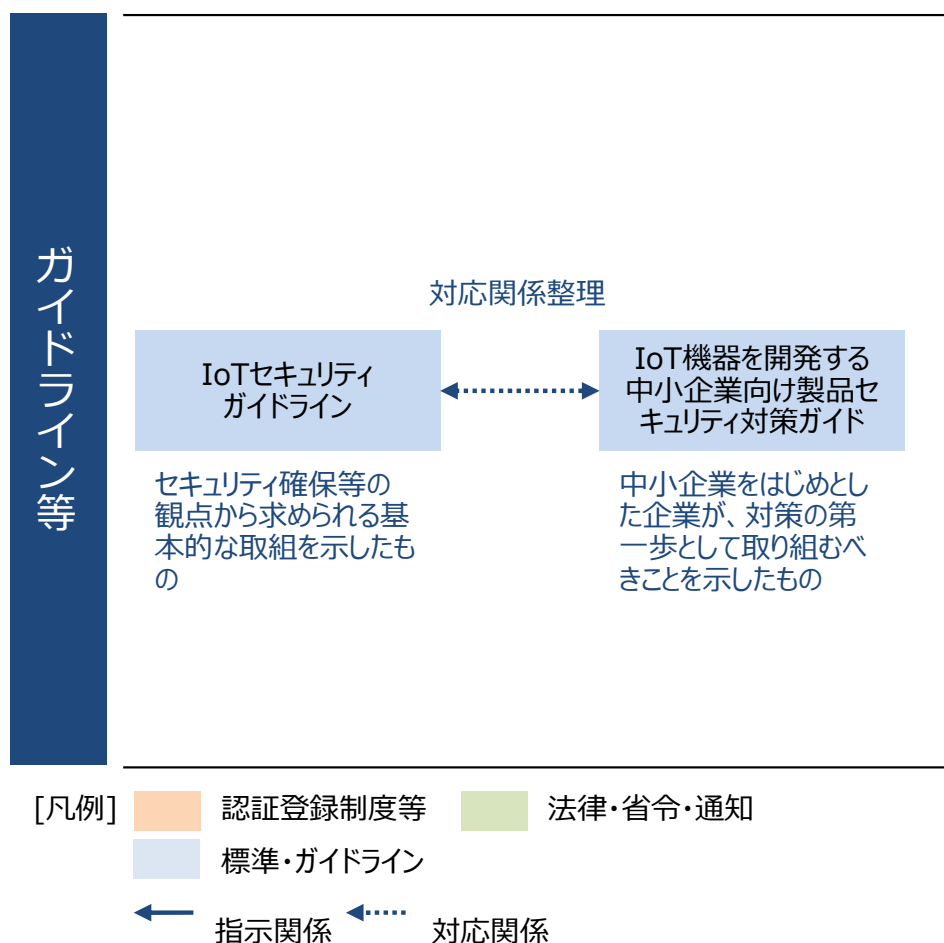
HITACHI
Inspire the Next

- 技術的管理策の中で、アクセス制御機能(パスワードやパスワードとIDを組み合わせたもの)について示されているが、より詳細な内容までは記載されていない。

項目	記載粒度
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<技術的管理策> - 電気通信の機能に係る設定を変更するための<u>アクセス制御機能</u>について例示。 ✓ <u>パスワード</u> ✓ <u>パスワードと IDを組み合わせたもの</u>
頻度(when)	<技術的管理策> <u>パスワードの変更タイミング(初期設定時)</u>を示す。
場所(where)	(場所に関する具体的な記載なし)

- 本ガイドラインは、関係者がセキュリティ確保等の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ明確化するもの。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
IoTセキュリティガイドライン	本ガイドラインは、IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT 機器やシステム、サービスについて、<u>その関係者がセキュリティ確保等の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ明確化するもの。</u>	- IoT機器・システム、サービスの供給者及びその経営者 - 機器メーカー - システム提供者 - サービス提供者 - IoT機器・システム、サービスの利用者 - 企業利用者 - 一般利用者
IoT機器を開発する中小企業向け製品セキュリティ対策ガイド	本ガイドでは、IoT機器等のセキュリティ対策を行うおうとする中小企業をはじめとした企業が、<u>対策の第一歩として取り組むべきこと</u>を示す。	- IoT機器等を開発する中小企業の経営者 - IoT機器等を開発する中小企業のセキュリティ担当者・開発担当者・品質管理者

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

IoTセキュリティガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

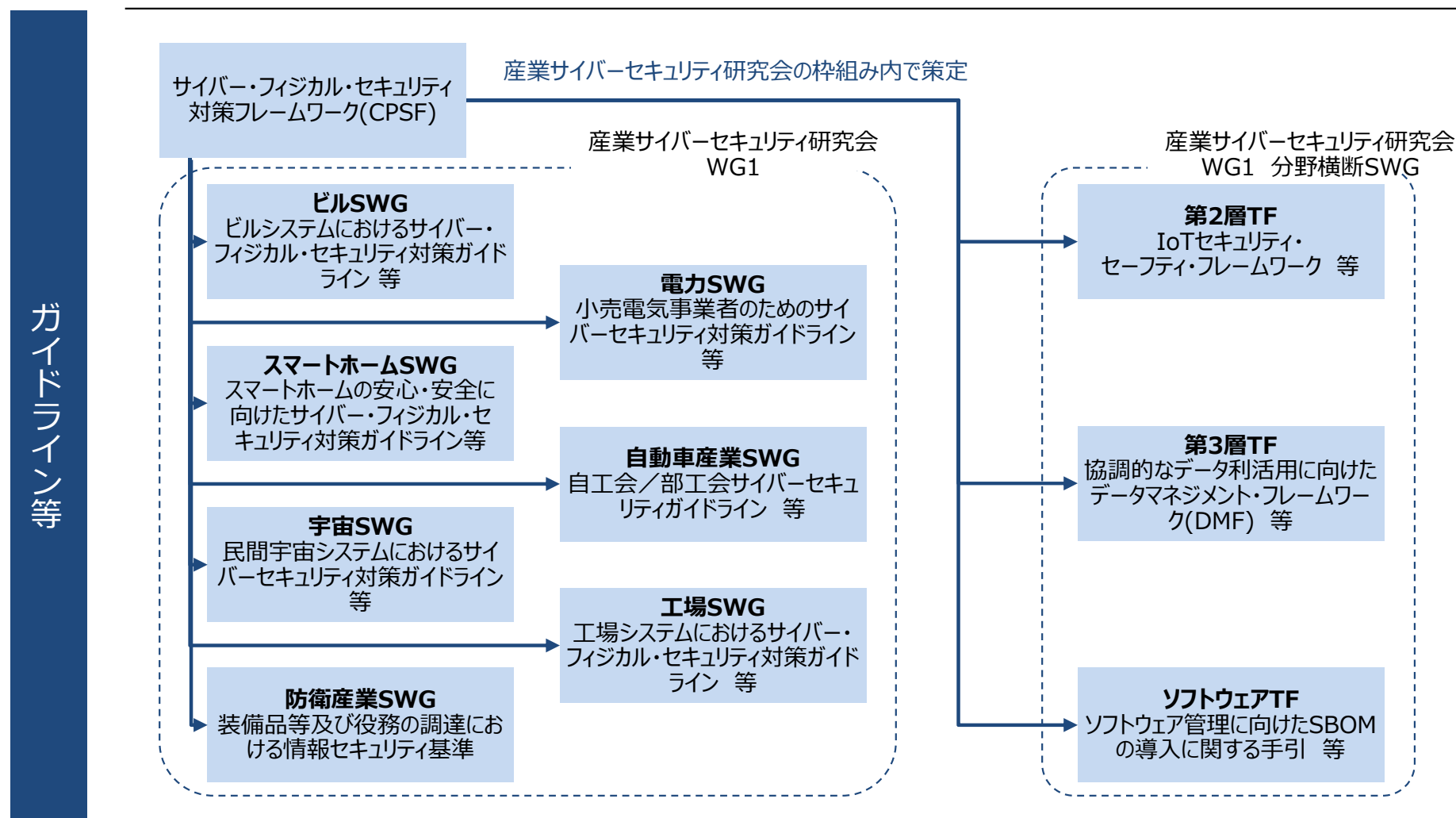
- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- ただし、インシデント対応やインシデント復旧のコミュニケーションや教育に係る要求事項は網羅されていない。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	3/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	-	
合計							18/22

- 比較対象とした要件においては主体や場所に係る具体的な情報は記載されていなかったが、内容や頻度に係る情報が記載されている。

項目	記載粒度
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<技術的管理策> - IoTシステム・サービス全体での認証方式について具体例を示す。 ✓ 接続するIoT機器のなりすましへの対策を行う。<u>IoT機器の識別子による認証、クライアント証明書による認証、メッセージ認証等</u>を行い、また、不正なIoT機器からの接続拒否設定も行う。 ✓ 利用者のなりすましへの対策を行う。<u>利用者を識別するID・パスワード、ICカード、生体認証等による認証</u>を行う。 ✓ 接続する相手のシステム・サービスのなりすましへの対策を行う。<u>接続するIoTシステム・サービス相互で鍵・電子証明書等を使用した認証</u>を行う。 - IoT機器の機能・制約を踏まえた認証方式について具体例を示す。 ✓ 暗号を用いた認証の適用 IoT機器のファームウェア更新時には、過失または故意によって、ファームウェアの改ざん等の脅威が想定される。そうした脅威に対してIoT機器のファームウェアを正しく更新するためには、更新データの正当性を担保する必要がある。IoT機器及びネットワークの機能・性能に制約のある環境下において確実なアップデートを実現するためには、<u>暗号を用いた機器認証、ユーザ認証やファームウェア検証等が有効</u>である。
頻度(when)	<技術的管理策> <u>パスワードの変更タイミング(初期設定時)</u>を示す。
場所(when)	(場所に関する具体的な記載なし)

- 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)に基づき、産業サイバーセキュリティ研究会WG1や分野横断SWGにて各種ガイドラインが策定されている。



[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

- 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)は、新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し、リスク源を明らかにしつつ、求められるセキュリティ対策の全体像を整理するとともに、産業界が自らのセキュリティ対策に活用できる対策例をまとめたもの。

項目	目的	想定読者
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)	新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し、リスク源を明らかにしつつ、求められる<u>セキュリティ対策の全体像を整理</u>するとともに、産業界が自らの<u>セキュリティ対策に活用できる対策例をまとめた</u>もの。	「Society 5.0」において、付加価値の創造活動に取り組む主体
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	本ガイドラインの目的は、ビルシステムのサイバーセキュリティに関して、その<u>確保のためのガイダンスを示すこと</u>。	- ビルオーナー、ゼネコン、サブコン、設計事務所、個別システム事業者、ビル管理会社、テナント - サービスプロバイダ、セキュリティベンダ、ネットワークシステムベンダ、自治体、関係省庁
小売電気事業者のためのサイバーセキュリティ対策ガイドライン	本ガイドラインは、<u>小売電気事業者の抱える様々な課題に対し、包括的な視点からサイバーセキュリティ対策を整理</u>したもの	小売電気事業者
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン	本ガイドラインは、市場が広がりつつあり、多岐にわたるサービスが予想されるスマートホーム分野において、IoT機器を通じた様々なサービスを受ける上で生じる、情報漏洩、サイバー攻撃、フィジカル空間への被害などに対するガイドを整備し、<u>スマートホーム利用における住まい手の安心・安全の確保を目指す</u>。	スマートホーム向けIoT機器の事業者、スマートホーム向けのIoT機器を遠隔から管理する事業者、スマートホーム向けのサービス事業者、スマートホームを供給する事業者、スマートホーム向けにメンテナンスやサポートを行う事業者、スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社、スマートホーム化された賃貸住宅の所有者や管理受託会社、スマートホームの住まい手

サイバー・フィジカル・セキュリティ対策フレームワーク
目的等(2/2)

項目	目的	想定読者
自工会／部工会 サイバーセキュリティガイドライン	自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、向こう3年の<u>対策フレームワークや業界共通の自己評価基準を明示</u>することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的とする。	自動車産業に関係する全ての会社
IoTセキュリティ・セーフティ・フレームワーク	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に着目し、リスク形態及びそうしたリスクに対応する<u>セキュリティ・セーフティ対策の類型化の手法を提示</u>するもの。	IoT を活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者、そのような新たな仕組み・サービスで活用される IoT 機器・システムの開発を行う者、そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者、そのような新たな仕組み・サービスを受ける者
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)	本フレームワークは、主体間を転々流通するデータの信頼性を確保することでバリュークリエーションプロセスが付加価値を生み出していくために、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化して<u>データに対するリスクを洗い出しのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とすることを目的</u>とする。	真正であり、適切なセキュリティを確保することが求められるデータを扱う者、特に、データを利活用して価値を創造するバリュークリエーションプロセスに参加する者、データ利活用に関するサービスを提供する者、データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者、データに求められる条件として適切なトラストを保証することが必要な場合の適切な水準のトラストサービスを提供しようとする者、データセキュリティに関わるガイドライン等のルール設定に関わる者
ソフトウェア管理に向けたSBOMの導入に関する手引	本手引では、ソフトウェア管理に向けたSBOMの作成・共有・運用・管理に関する様々な課題の解決するために、SBOMの概要やSBOM導入のメリット等、SBOMに関する基本的な情報を提供するとともに、<u>ソフトウェアサプライヤーにおけるSBOM作成に向けた環境構築・体制整備、SBOM作成・共有、そしてSBOMの運用・管理に至る一連のSBOM導入に向けたプロセス</u>を示す。	本手引では、ソフトウェアサプライヤーにおける開発・設計部門や製品セキュリティ担当部門（PSIRT等）等のソフトウェアセキュリティに関わる部門と、経営層を主な対象

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

サイバー・フィジカル・セキュリティ対策フレームワーク

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

- 記載されている要件は偏りはなく、全ての項目を網羅している。
- 文書内でCSFとの対応関係が整理されていることから、国際的に広く認知されているCSFとの関係性を意識しつつ、CPSFが策定されたと考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							22/22

- 比較対象とした要件においては場所に係る具体的な情報は記載されていなかったが、主体や内容に係る情報が記載されている。

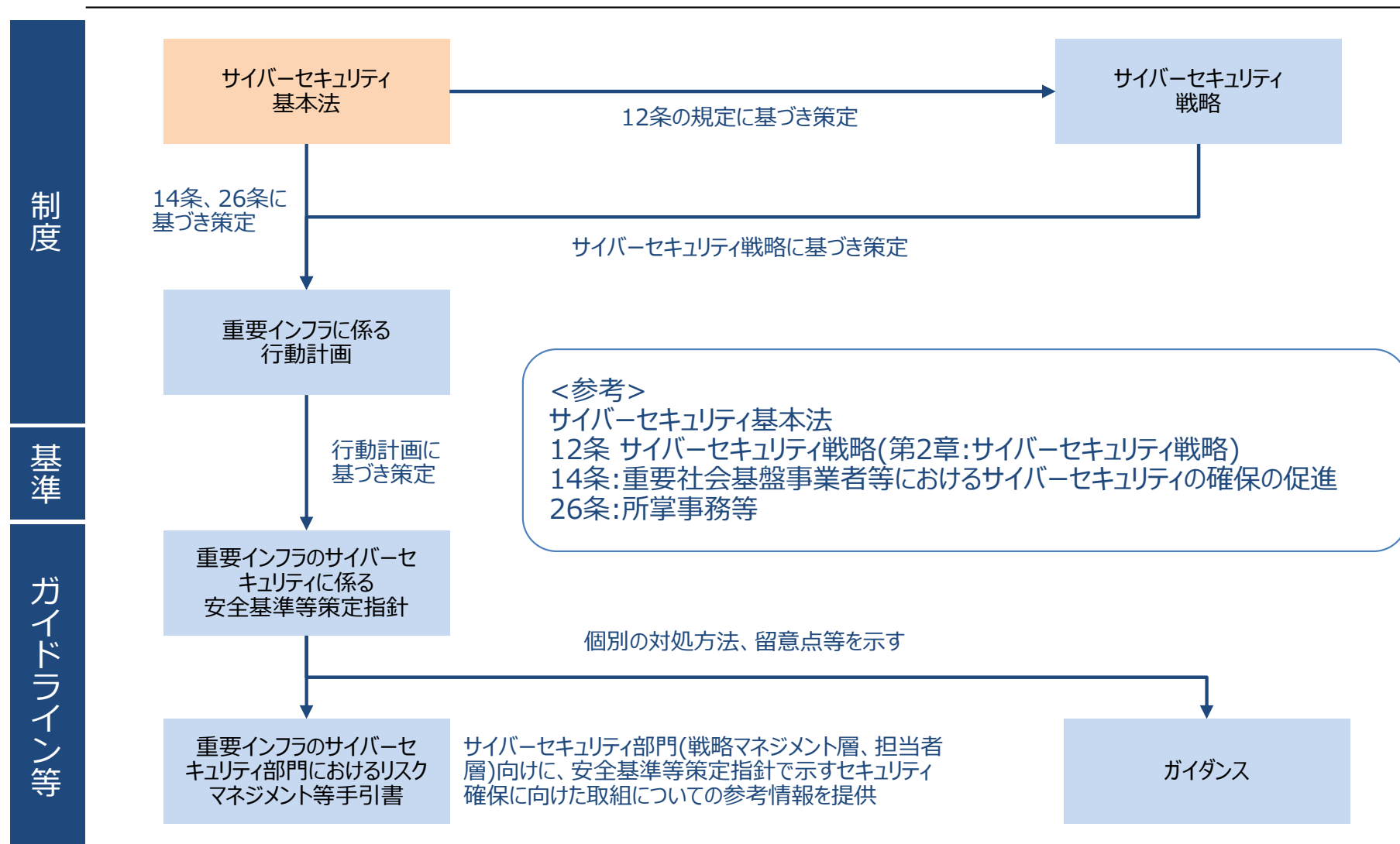
項目	記載粒度
主体(who)	<人的管理策> - 対策例(High-Advanced)にて、<u>教育の対象</u>を例示。 ✓ 全要員 ✓ 情報セキュリティ要員(システム/ソフトウェア開発者、調達担当者、システム管理者、セキュリティ対策担当者)
内容(what)	<組織的管理策> - 資産を管理するために作成する<u>ネットワーク図に記載する情報</u>を示す。 ✓ 主要装置 ✓ ネットワークの種類 ✓ 機器の設置場所 <物理的管理策> <u>対策要件にて、物理セキュリティを行うための対策</u>を示す。 ✓ IoT機器、サーバ等の設置エリアの施錠 ✓ 入退室管理 ✓ 生体認証等の導入 ✓ 監視カメラの設置 ✓ 持ち物や体重検査等 <u>対策例(High-Advanced)にて、物理セキュリティ境界でのモニタリング方法を例示。</u> ✓ 警報 ✓ 管理装置(例:監視カメラ) <u>対策例(Basic)にて、物理セキュリティ領域の管理方法を例示。</u> ✓ アクセスリストの維持管理 ✓ アクセスに必要な許可証明書の発行

項目	記載粒度
内容(what)	<技術的管理策> • <u>対策例(Basic)にて、自組織の情報システム及び産業用制御システムに対するクレデンシャル（例：パスワード、セキュリティキー）のポリシーを例示。</u> ✓ クレデンシャルに最低限必要な複雑さを確保するため、パスワードに求める要求事項を定め、運用する。 ✓ 新しいクレデンシャルが作成される際には、少なくとも組織が定めた文字数に変更させる。 ✓ 暗号によって保護されたクレデンシャルのみを保存・伝送する。 ✓ 同じクレデンシャルを組織が定めた世代にわたって再利用するのを禁止する。 • <u>対策例(High-Advanced)にて、ログオンの制限を行う機能を例示。</u> ✓ 自組織のシステムに対してユーザが連続してログオンを失敗できる上限を設定する機能 ✓ 上限以上失敗した場合には管理者が解除しなければ再ログインできない機能 • <u>対策例(Advanced)にて、ログオンの制限を行う機能を例示。</u> ✓ 手動又は自動でセッションロックを実施
頻度(when)	<人的管理策> • <u>対策例(Basic)にて、教育のタイミングを例示。</u> ✓ 職員が新たに配属されたとき ✓ 情報システムや産業用制御システムに対する変更により必要になったとき
場所(when)	(場所に関する具体的な記載なし)

2.1 業種個別

重要インフラのサイバーセキュリティに係る安全基準等策定指針
位置づけ等

- サイバーセキュリティ基本法に基づき策定された重要インフラに係る行動計画を基に、重要インフラのサイバーセキュリティに係る安全基準等策定指針が策定。



重要インフラのサイバーセキュリティに係る安全基準等策定指針
目的等

- 重要インフラのサイバーセキュリティに係る安全基準等策定指針は、各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を整理・記載している。

項目	目的	想定読者
サイバーセキュリティ基本法	この法律は、(中略)我が国のサイバーセキュリティに関する施策に関し、<u>基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定め</u>るとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって<u>経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図る</u>とともに、<u>国際社会の平和及び安全の確保並びに我が国の安全保障に寄与</u>することを目的とする。	-
サイバーセキュリティ戦略	本戦略は、中長期的視点から時代認識に立ち、<u>2020年代初めの今後3年間にとるべき諸施策の目標や実施方針を示す</u>。	-
サイバーセキュリティ行動計画	重要インフラ分野全体として<u>今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすること</u>で、<u>官民連携に基づく重要インフラ防護の一層の強化を図る</u>。	-
重要インフラのサイバーセキュリティに係る安全基準等策定指針	安全基準等策定指針には、<u>各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を整理・記載</u>する。これらの取組は原則として安全基準等に規定されることを期待しているが、組織状況に応じて採否が検討されうる取組は推奨事項として「～することが望ましい」「～することが望まれる」という表現にしている。	- 重要インフラ所管省庁 - 重要インフラ事業者 - サプライチェーンに関わる事業者等
重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書	本手引書は、<u>サイバーセキュリティ部門(戦略マネジメント層、担当者層)向けに、安全基準等策定指針で示すセキュリティ確保に向けた取組についての参考情報を提供</u>する。	サイバーセキュリティ部門（戦略マネジメント層、担当者層）

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

重要インフラのサイバーセキュリティに係る安全基準等策定指針

記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- もともと重要インフラを対象としていたNIST CSFの記載範囲を網羅することを想定してサイバーセキュリティに係る安全基準等策定指針が策定されたものと考えられる。

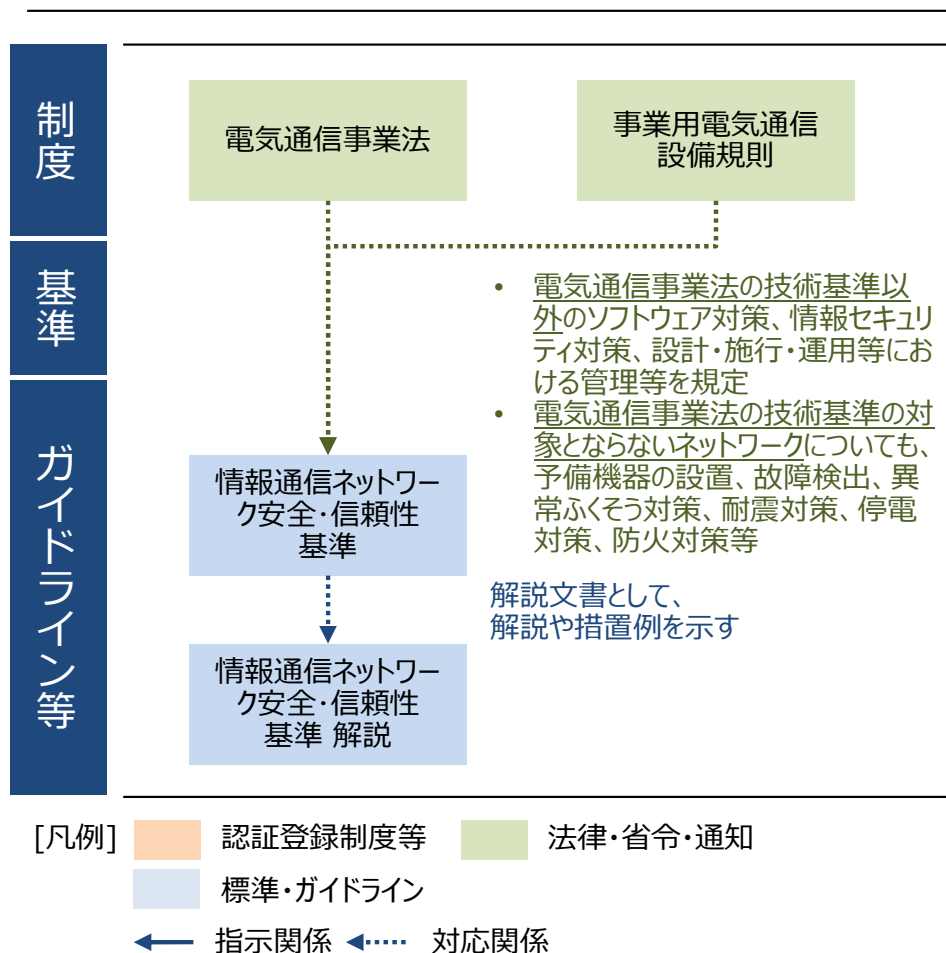
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

- 安全基準等策定指針においては、内容面でより具体的な内容が記載されていた。特に、物理的な管理策や技術的な管理策において、具体的な対策手段を記載している。

項目	記載粒度
頻度 (when)	(頻度に関する記載なし)
場所 (where)	(場所に関する記載なし)
主体 (who)	(主体に関する記載なし)
内容 (what)	<物理的管理策> - セキュリティ確保が求められる領域の設定に必要な手段(入退室の仕組みの構築、持ち込み品の確認・制御)を示す。 - 装置の管理方法(通信・電源ケーブル配線時の考慮事項、取り外し可能な記憶媒体に係る承認の仕組みの構築)を示す。 <技術的管理策> - アクセスの制限方法(ログイン失敗回数の設定、多要素認証の活用)を示す。 - 通信のセキュリティ方法(専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知)を示す。

- 本ガイドラインは、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等を総合的に取り入れた、安全・信頼性に関する推奨基準。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
電気通信事業法	この法律は、(中略)、その公正な競争を促進することにより、電気通信役務の円滑な提供を確保するとともにその利用者等の利益を保護し、もつて電気通信の健全な発達及び国民の利便の確保を図り、公共の福祉を増進することを目的とする。	-
事業用電気通信設備規則	この規則は、電気通信事業法第四十一条第一項から第三項まで及び第五項の規定に基づく技術基準を定めることを目的とする。	-
情報通信ネットワーク安全・信頼性基準	情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標としての(推奨)基準を定めることにより、安全・信頼性対策の普及を促進し、もつて情報通信ネットワークの健全な発展に寄与することを目的とする。	- ネットワーク構築者 - 利用者

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

情報通信ネットワーク安全・信頼性基準 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 設備基準や管理基準からなる情報通信ネットワーク安全・信頼性基準では、冗長性確保の観点でセキュリティに係る基準以外の基準(安全(safety)に係る基準)も含まれている。

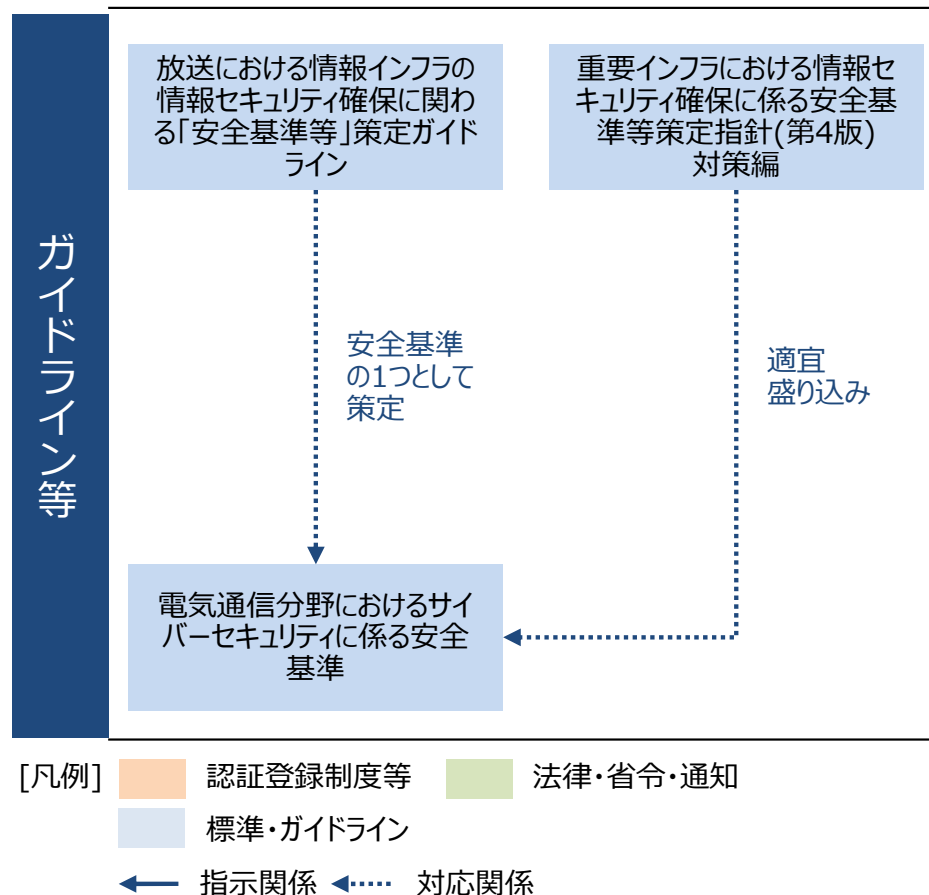
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	5/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	1/2
	監督	○			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	2/4
識別	資産管理	○	2/3		インシデント分析	-	
	リスクアセスメント	-			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

- 情報通信ネットワーク安全・信頼性基準においては、内容面でより具体的な内容が記載されていた。特に、物理的な管理策や技術的な管理策において、具体的な対策手段を記載している。

項目	記載粒度
頻度 (when)	(頻度に関する記載なし)
場所 (where)	(場所に関する記載なし)
主体 (who)	(主体に関する記載なし)
内容 (what)	<人的管理策> - 解説において、<u>教育のテーマ(通信の秘密の保護、各種データに関する守秘義務、パスワード管理の重要性及びコンピュータウイルスの脅威等)</u>を示す。 <技術的管理策> - 解説において、<u>利用者の識別方法</u>を示す。 ✓ 固有のパスワード等の情報を付与し、直接キーの入力 ✓ ID カード、IC カード等での読取 ✓ デジタル署名の使用 ✓ 声紋、指紋等の個人にとって天性として固有な事象を活用した判別

- 本安全基準は、電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準について政府指針に基づき策定したもの。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
電気通信分野におけるサイバーセキュリティに係る安全基準	本安全基準は、<u>電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準</u>について業界団体が定めるガイドラインを、<u>政府指針(重要インフラのサイバーセキュリティに係る安全基準等策定指針)</u>に基づき策定したものである	- 電気通信事業者 - 電気通信設備提供者(メーカ等)

- 記載されている要件はNIST CSFの全ての範囲を網羅している。
- なお、ISO/IEC 27002の管理策を引用する形で一部安全基準が示されている。(比較対象との差異はみられなかった*1)

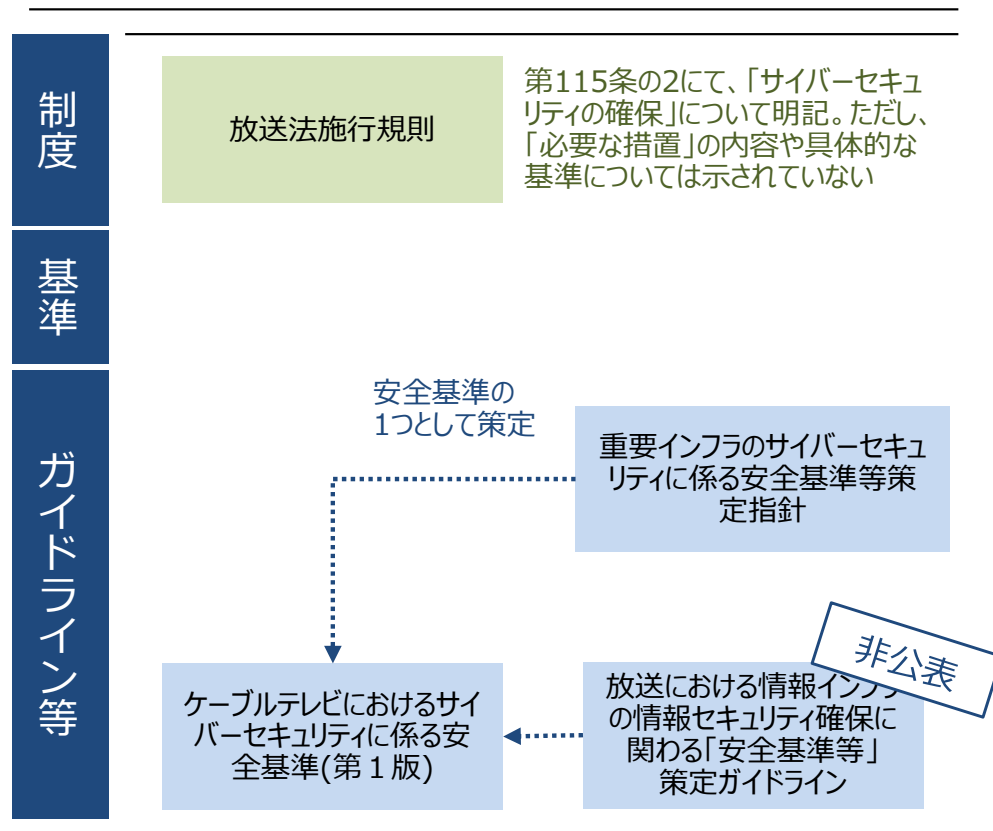
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							22/22

*1 今回の調査において、比較を行う管理策(組織的管理策(資産の管理)、人的管理策(情報セキュリティの意識向上、教育及び訓練)、物理的管理策(物理的入場管理策)、技術的管理策(ネットワーク及びネットワークサービスへのアクセス))はISO/IEC 27002の管理策を引用していたため、比較対象のISO/IEC 27001と差異はみられなかった点に留意いただきたい。

ケーブルテレビにおけるサイバーセキュリティに係る安全基準 位置づけ等 / 目的等

- ケーブルテレビにおけるサイバーセキュリティに係る安全基準は、ケーブルテレビ事業者がサイバーセキュリティ確保に関して)自らが「何をすべきか」「どの程度すべきか」を理解できることを目的とする。
- 施行規則にはサイバーセキュリティに係る項目があるものの、具体的な措置や基準は明示されていない。

位置づけ/参照関係



[凡例]

 認証登録制度等	 法律・省令・通知
 標準・ガイドライン	
→ 指示関係	⋯ 対応関係

目的/想定読者

項目	目的	想定読者
放送法施行規則	放送法の規定を施行するために必要とする事項及び法の委任に基づく事項を定めることを目的とする。	-
ケーブルテレビにおけるサイバーセキュリティに係る安全基準(第1版)	ケーブルテレビ事業に携わる全ての関係者が、<u>(サイバーセキュリティ確保に関して)自らが「何をすべきか」「どの程度すべきか」を理解できることを目的とする。</u>	<u>ケーブルテレビ事業者</u>(対象サービスはケーブルテレビ事業者が提供する全てのサービス。特に、ISP、放送、音声通話等の電気通信サ)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

ケーブルテレビにおけるサイバーセキュリティに係る安全基準 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの範囲を網羅している。
- 当初重要インフラを対象としていたNIST CSFの記載範囲を網羅することを想定して、サイバーセキュリティに係る安全基準等策定指針が策定されたものと考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

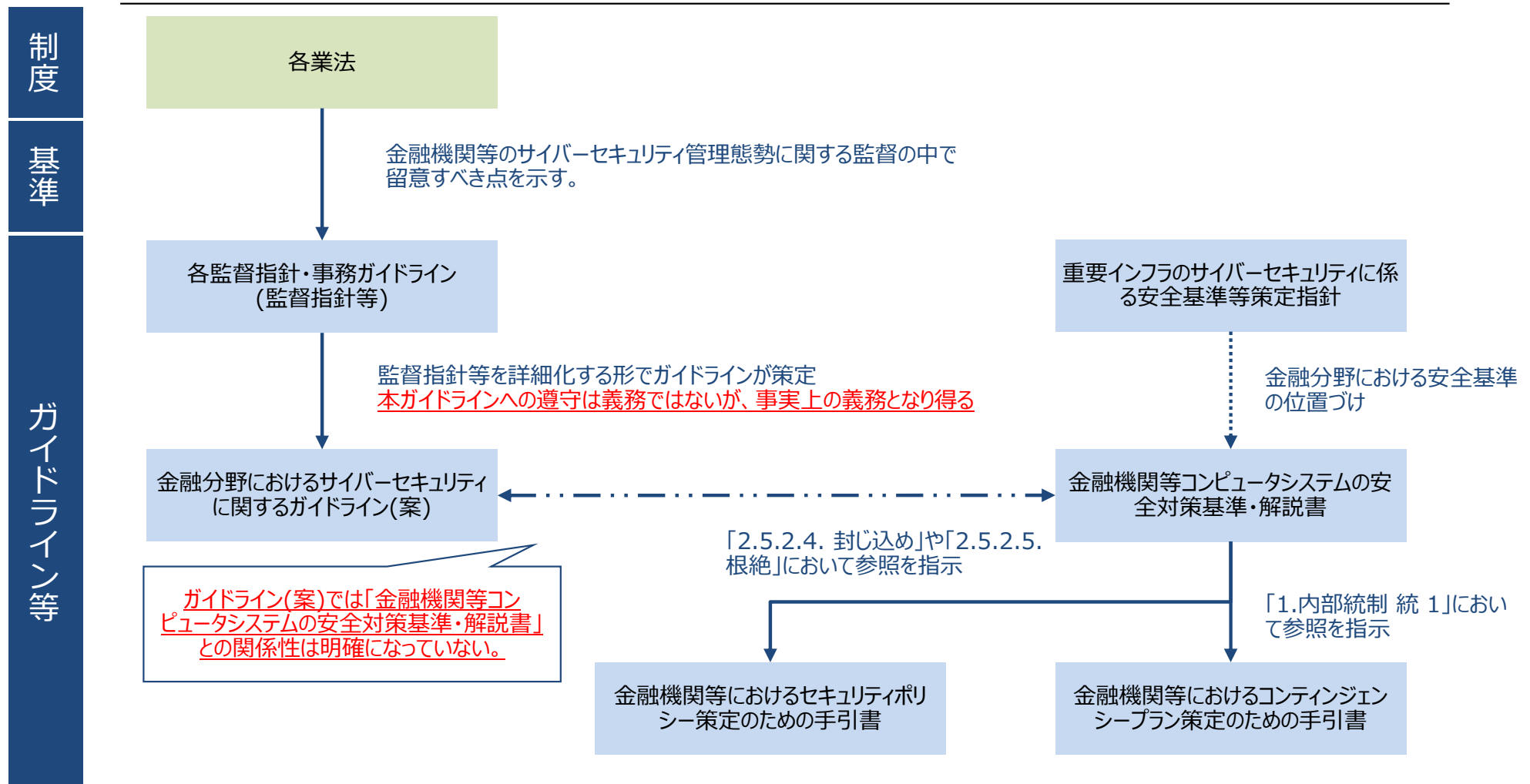
- ケーブルテレビにおけるサイバーセキュリティに係る安全基準においては、内容面でより具体的な内容が記載されていた。特に、物理的な管理策や技術的な管理策において、具体的な対策手段を記載している。

項目	記載粒度
頻度 (when)	(頻度に関する記載なし)
場所 (where)	(場所に関する記載なし)
主体 (who)	(主体に関する記載なし)
内容 (what)	<物理的管理策> - セキュリティ確保が求められる領域の設定に必要な手段(入退室の仕組みの構築、持ち込み品の確認・制御)を示す。 - 装置の管理方法(通信・電源ケーブル配線時の考慮事項、取り外し可能な記憶媒体に係る承認の仕組みの構築)を示す。 <技術的管理策> - アクセスの制限方法(ログイン失敗回数の設定、多要素認証の活用)を示す。 - 通信のセキュリティ方法(専用線や暗号技術の活用、IPv6 に関するセキュリティ対策の実施、ネットワークの分離、ログ取得及び監視によるサイバー攻撃の検知)を示す。

金融分野におけるサイバーセキュリティに関するガイドライン(案)
位置づけ等

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 本ガイドラインは、監督指針等を詳細化する形でガイドラインが策定されている。
- 本ガイドラインへの遵守は義務ではないが、事実上の義務となり得る。



[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

- 本ガイドラインは、サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理に関する着眼点から金融機関等において「基本的な対応事項」及び「対応が望ましい事項」を明確化。

項目	目的	想定読者
金融分野におけるサイバーセキュリティに関するガイドライン(案)	- 検査・モニタリングの結果及び金融セクター内外の状況の変化を踏まえ、監督指針等とは別に、(サイバーセキュリティの確保を目的として)詳細な本ガイドラインを策定。 <u>本ガイドラインでは、サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理に関する着眼点から金融機関等において「基本的な対応事項」及び「対応が望ましい事項」を明確化。</u>	<u>金融機関</u>
金融機関等コンピュータシステムの安全対策基準・解説書	日本の金融機関等が、事業展開を行ううえで金融情報システムを活用するに際し、開発や導入、運用等において必要と考えられる<u>安全対策を基準として示すとともに、基準項目ごとに、具体的な事例を交えて解説するもの。</u>	<u>金融機関等</u>

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

金融分野におけるサイバーセキュリティに関するガイドライン(案)

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 本ガイドラインの分類はCSFの分類を意識されており、CSFと比較して記載項目に大きな偏りがないよう配慮された上でガイドラインが策定されていると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							21/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

金融分野におけるサイバーセキュリティに関するガイドライン(案)

記載粒度

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

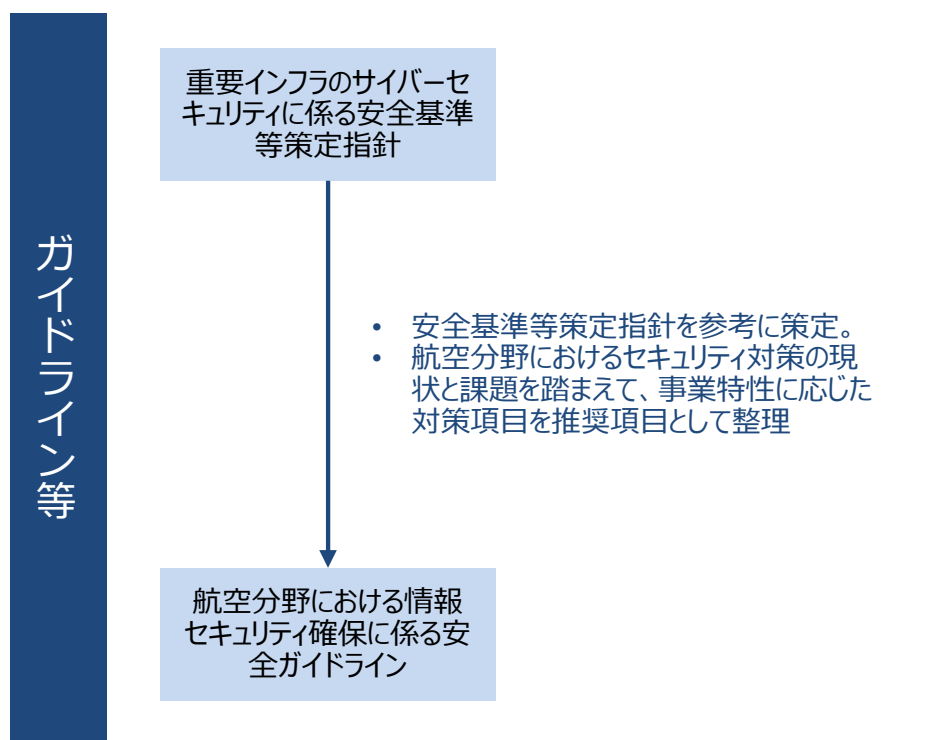
B-2.記載粒度

- 本ガイドラインでは、主体や内容面において具体的な記載がみられた。
- 特に、技術的管理策において認証方法やプロトコルが示されている。

項目	記載粒度
主体(who) /内容(what)	<人的的管理策> - 基本的な対応事項にて、<u>教育の対象者とその内容</u>を示す。 ✓ <u>経営陣を含むすべての役職員</u>[役割と責任に応じたサイバーセキュリティの意識向上に係る教育・研修/自身がインシデントの当事者となった場合に適切な対応を行うために、必要な教育・研修] ✓ <u>サードパーティ在籍の担当者</u>[業務を適切に行う上で必要となるサイバーセキュリティの教育・研修] ✓ <u>顧客</u>[サイバー攻撃の脅威及びサイバーセキュリティの意識向上に資する取組み] ✓ <u>ITまたはセキュリティを所管する部門の職員</u>[脅威及び対策の変化等、最新の知識とスキルを維持するための教育・研修] <技術的管理策> - 基本的な対応事項にて、<u>認証方法を例示</u>。また、重要なアクセスについての認証方法も併せて示す。 ✓ 多要素認証(※重要なシステムへのリモートアクセスの場合を含む) ✓ リスクベース認証 - 基本的な対応事項にて、第三者による不正行為を阻止するための仕組み(<u>メールの送信ドメイン認証の種類</u>)を示す。 ✓ SPF ✓ DKIM ✓ DMARC

- 本ガイドラインは、国が定める「ガイドライン」として推奨事項を列挙しているもの。航空分野におけるセキュリティ対策の現状と課題を踏まえて、事業特性に応じた対策項目を推奨項目として整理。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

目的/想定読者

項目	目的	想定読者
航空分野における情報セキュリティ確保に係る安全ガイドライン	- 国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に参考資料として活用することを想定。 - 本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、航空分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめた。	航空分野の重要インフラ事業者等

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

航空分野における情報セキュリティ確保に係る安全ガイドライン

記載範囲

A-1. 体系内の位置づけ

A-2. 体系間の位置づけ

B-1. 記載範囲

B-2. 記載粒度

HITACHI
Inspire the Next

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 安全基準等策定指針を考慮しつつ、重要インフラ事業者が参照する推奨事項が記載されており、幅広い要件が盛り込まれている。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							21/22

- 管理策における具体例の中で、詳細な情報を記載している。その中でも、実施内容(what)の部分において、具体的な記載が多く見られた。
- (比較した要件において分野ごとの若干の差異^{*1}はあるものの、空港分野や鉄道分野も同様。)

項目	記載粒度
主体(who)	<技術的管理策> - 具体例にて、<u>対策を行う主体</u>ごとに対策を例示。 ✓ システム管理者 ✓ 端末を利用する取扱者 - 具体例にて、<u>セキュリティ対策の対象者</u>を例示。 ✓ 経営層 ✓ システム業務に従事する人材 ✓ システムユーザ ✓ PC操作者(テレワーク勤務者を含む) ✓ (必要に応じて)委託先
内容(what)	<組織的管理策> - 具体例にて、<u>情報システムの構成要素ごと</u>に対策例を例示。 ✓ 端末 ✓ サーバ装置 ✓ 通信回線・通信回線装置 ✓ 複合機及びIoT機器を含む特定用途機器 - 具体例にて、<u>資産管理台帳の維持方法</u>について例示。 ✓ 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする ✓ 承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する <物理的管理策> - 要管理対策区域への<u>訪問者に対する確認事項</u>を例示。 ✓ 氏名 ✓ 所属 ✓ 訪問目的並びに・訪問相手の氏名及び所属

^{*1} 例えば、空港分野では不特定多数が出入りするため警戒警備システムに対して物理的な対策が必要とされ、鉄道分野でも各駅に制御システム等が設置されていることから物理的な不正侵入への対策を行う必要があるとされている。(どちらも、物理的管理策において記載)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

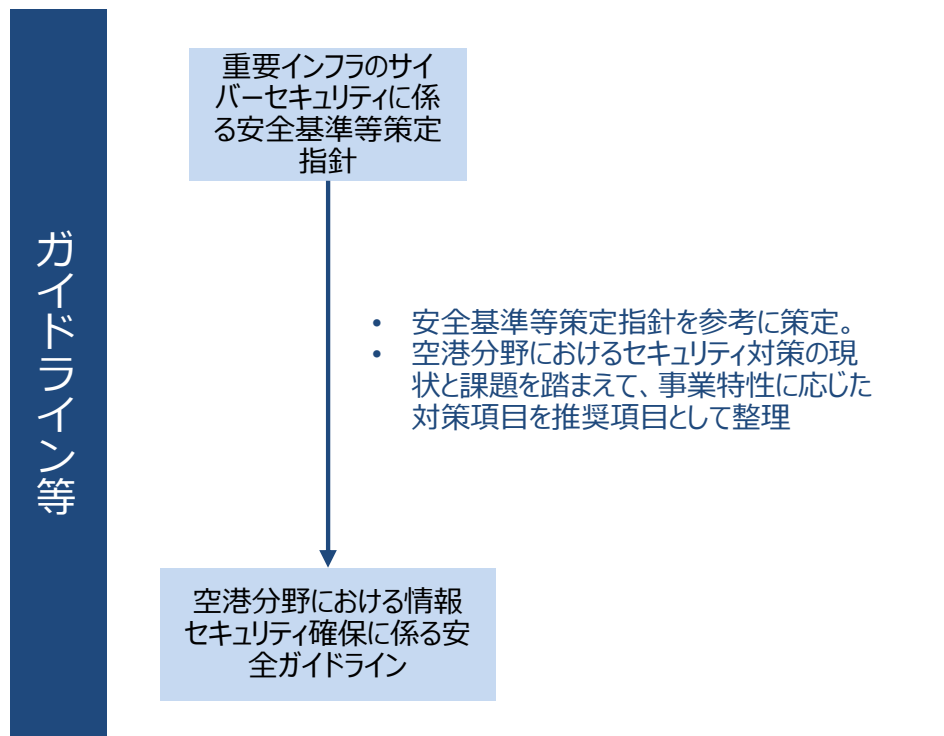
航空分野における情報セキュリティ確保に係る安全ガイドライン 記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

項目	記載粒度
内容(what) (続き)	<物理的管理策> - 具体例にて、要管理対策区域での制限事項を例示。 ✓ 重要インフラ事業者等においては、単独での作業を制限する ✓ 情報システムに関連する機器の要管理対策区域への持込み及び要管理対策区域からの持出には、システム管理者の承認を求める ✓ 定期的又は不定期に施設からの退出時に持ち物検査を行う <技術的管理策> - 具体例にて、アクセス利用者の管理とアクセス権の管理にあたって実施することを例示。 ✓ 利用者及びアクセス権の登録・変更・削除の正式なプロセスに係る申請ルート、承認者、作業者等の設定 ✓ 利用者アクセス権の定期的なレビュー ✓ 管理権限のユーザ/用途ごとの設定 ✓ 離職者アカウントに対して、全てのバッジ、キーカード、トークン等の失効 - 具体例にて、認証手段を明示。 ✓ 知識(パスワード等、利用者本人のみが知り得る情報)による認証 ✓ 所有(電子証明書を格納するIC カード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等)による認証 ✓ 生体(指紋や静脈等、本人の生体的な特徴)による認証 - 具体例にて、アクセス制御機能を例示。 ✓ 利用時間や利用時間帯によるアクセス制御 ✓ 同一主体による複数アクセスの制限 ✓ IPアドレスによる端末の制限 ✓ ネットワークセグメントの分割によるアクセス制御 ✓ 主体認証を受けたユーザのみが与えられた権限の範囲でアクセス可能となる制御
頻度(when)	<組織的管理策> - 対策の具体例にて、資産の管理にあたって対策を実施するタイミングを例示。 ✓ 運用時 ✓ 運用終了時 <人的管理策> - 対策の具体例にて、教育を行うタイミング(情報またはサービスへのアクセスを許可する前)を例示。
場所(where)	<物理的管理策> - 対策の指針にて、要管理対策区域を例示。 ✓ 執務室 ✓ 会議室 ✓ サーバ室等

- 本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、空港分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準として整理。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

目的/想定読者

項目	目的	想定読者
空港分野における情報セキュリティ確保に係る安全ガイドライン	- 国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に参考資料として活用することを想定。 - 本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、<u>空港分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準</u>としてまとめた。	空港分野の重要インフラ事業者等

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

空港分野における情報セキュリティ確保に係る安全ガイドライン

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

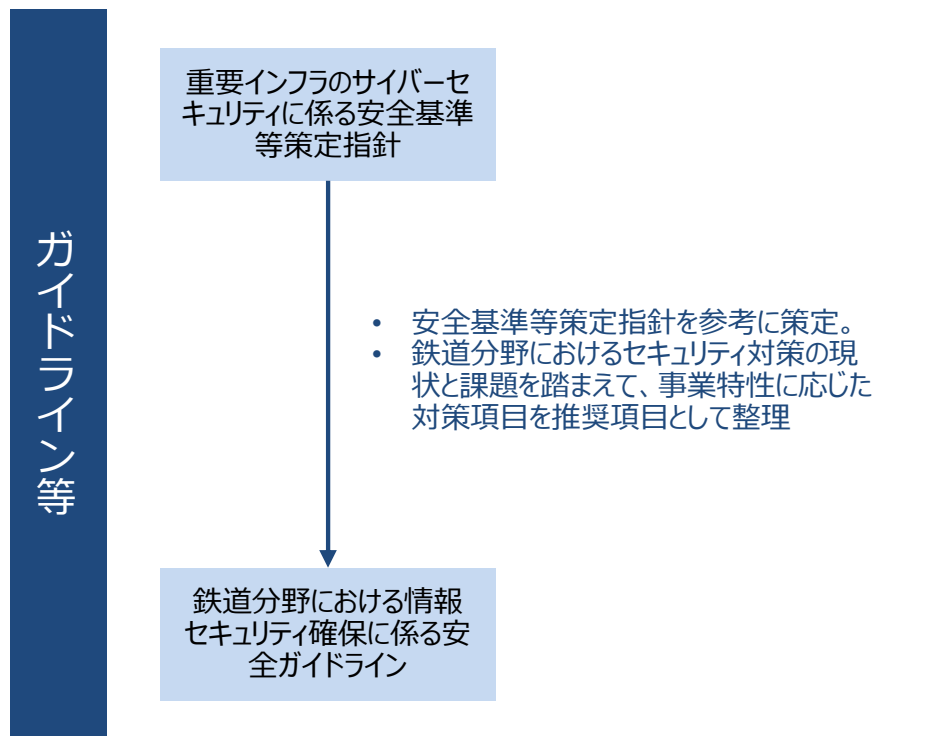
- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 細かい記載は異なるものの、記載されている範囲においては航空分野と内容に大きな差異はみられない。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							21/22

* [B-2について]本ガイドラインと「航空分野における情報セキュリティ確保に係る安全ガイドライン」を比較した際、比較に用いた要件においては対策要件や対策要件の例に大きな差異はみられなかった。

- 本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、鉄道分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準として整理。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

目的/想定読者

項目	目的	想定読者
鉄道分野における情報セキュリティ確保に係る安全ガイドライン	- 国が定める「ガイドライン」として推奨事項を列挙しているものであり、事業分野の特性に鑑み、重要インフラ事業者等が自らのセキュリティ管理策を実施する際に参考資料として活用することを想定。 - 本ガイドラインでは、分野横断的に有効な対策項目及び対策の例示に加え、鉄道分野におけるセキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめた。	鉄道分野の重要インフラ事業者等

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

鉄道分野における情報セキュリティ確保に係る安全ガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 細かい記載は異なるものの、記載されている範囲においては航空分野と内容に大きな差異はみられない。

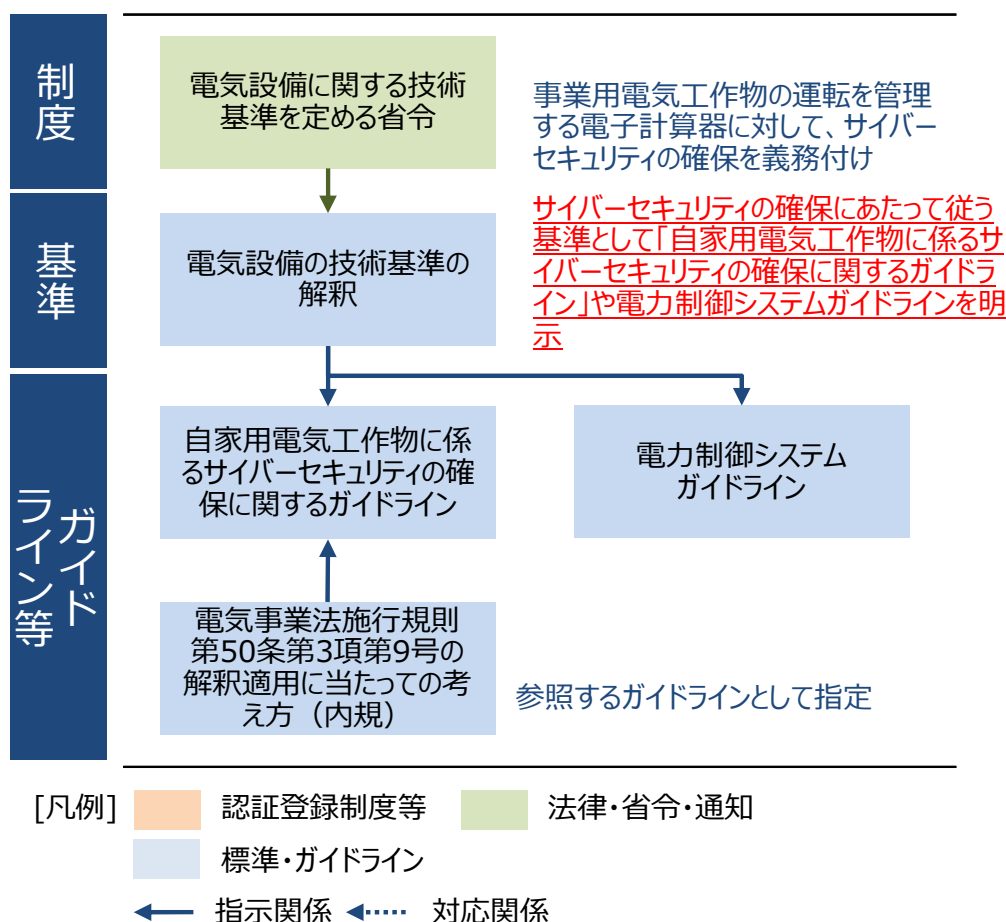
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							21/22

* [B-2について]本ガイドラインと「航空分野における情報セキュリティ確保に係る安全ガイドライン」を比較した際、比較に用いた要件において
は対策要件や対策要件の例に大きな差異はみられなかった。

- 本ガイドラインでは、自家用電気工作物*¹を設置する者が実施すべきセキュリティ対策の要求事項について規定されている。

*¹ 自家用工作物:電気を使用するために、工場、ビル等その使用の場所と同一構内(発電所又は変電所の構内を除く。)に施設されている電気工作物の総合体。 例:工事現場等で使用する10kW以上のディーゼル発電機

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
電気設備に関する技術基準を定める省令	電気事業法に基づき[2]、発電用設備の原動機などを除く電気工作物の技術基準を定める。	＝
電気設備の技術基準の解釈	電気設備に関する技術基準を定める省令に定める<u>技術的要件を満たすものと認められる技術的内容をできるだけ具体的に示したもの。</u>	＝
自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	本ガイドラインは、<u>自家用電気工作物の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、自家用電気工作物を設置する者が実施すべきセキュリティ対策の要求事項について規定したもの。</u>	<u>自家用電気工作物の遠隔監視システム及び制御システム並びにこれらのシステムに付随するネットワークに携わる者</u>

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 本ガイドラインでは一部網羅されていない要件がみられた。CSFよりも、その他の電力関係のガイドライン（例：電力制御セキュリティガイドライン）との整合性が意識され、本ガイドラインが策定されたと考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	4/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	-		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	2/4
識別	資産管理	○	2/3		インシデント分析	-	
	リスクアセスメント	-			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							14/22

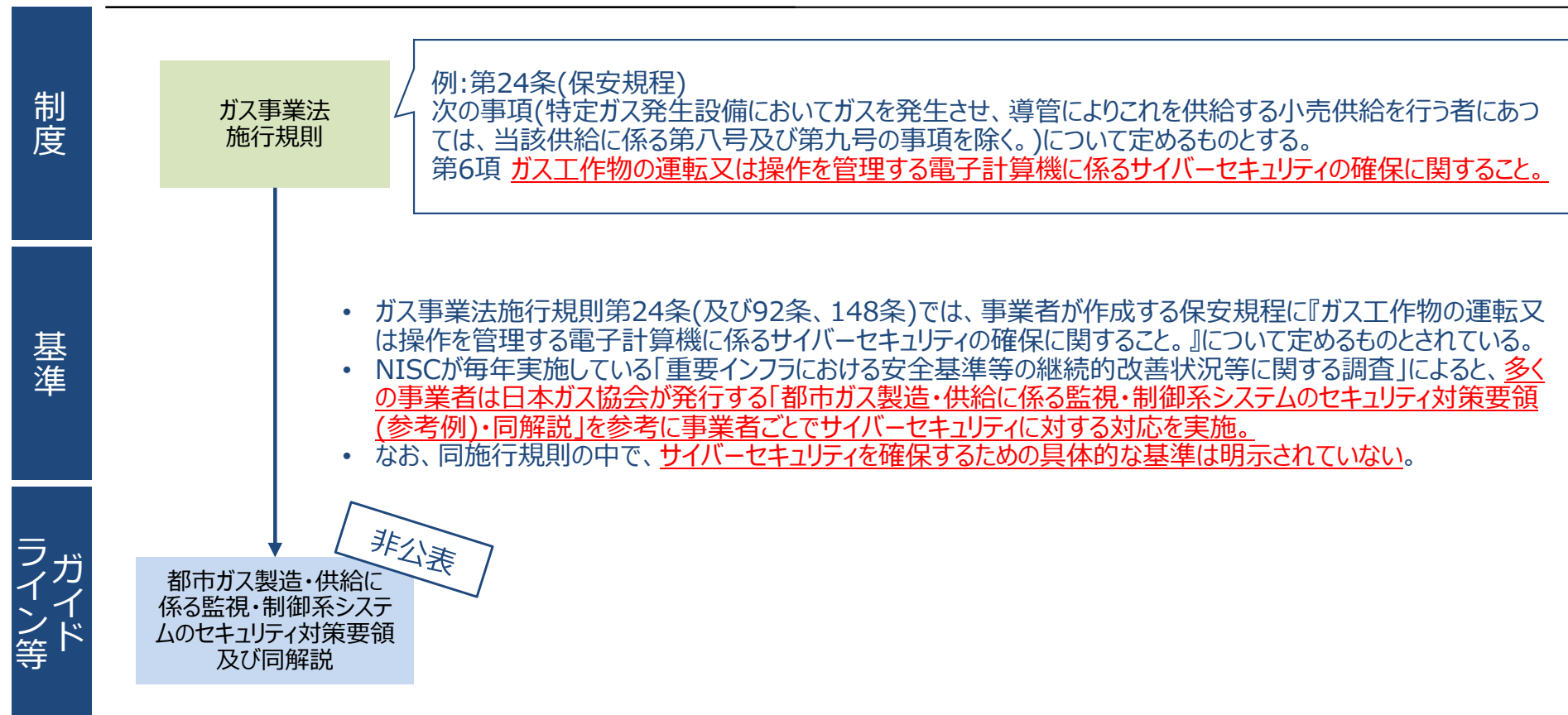
2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 組織的管理策の中で具体的な記載が一部みられたが、比較した要件においては解説も含めて具体的な記載はされていない。

項目	記載粒度
頻度 (when)	(頻度に関する具体的な記載なし)
場所 (where)	(場所に関する具体的な記載なし)
主体 (who)	(主体に関する具体的な記載なし)
内容 (what)	<組織的管理策> ・ 解説において、 <u>把握する機器の構成情報</u> を例示。 ✓ 管理番号 ✓ 設置場所 ✓ ソフトウェアのバージョン等機器に関する情報

- ガス事業法施行規則の中で、サイバーセキュリティの確保について言及されているものの、具体的な基準は示されていない。
- 一方で、ガス事業者は本ガイドラインを参照して、サイバーセキュリティに対する対応を実施。



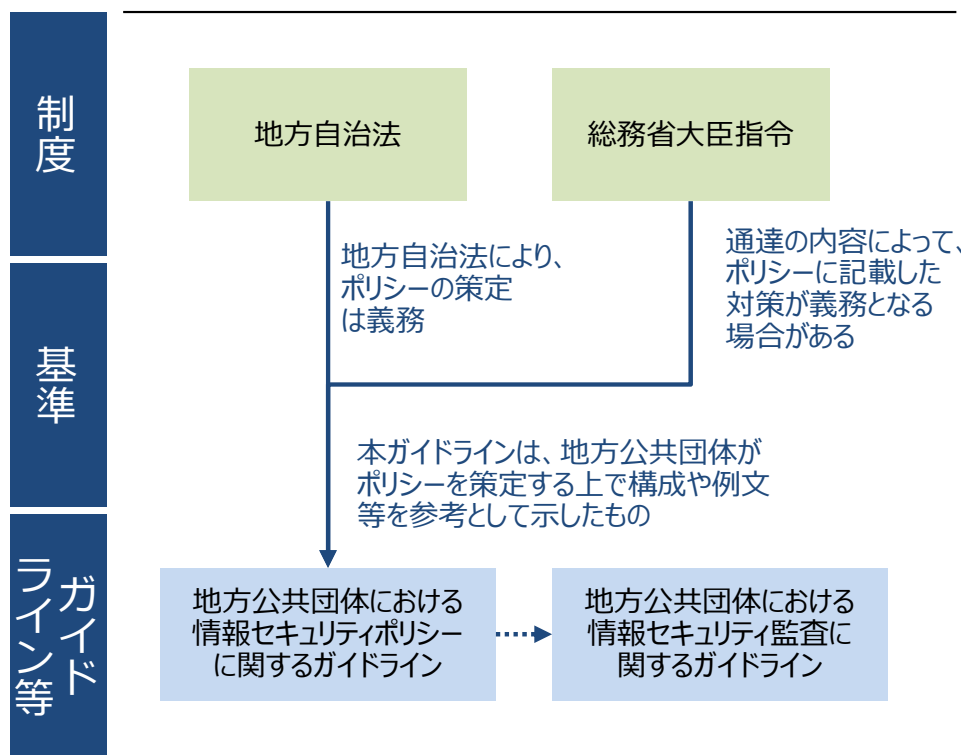
[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン → 指示関係 ⋯ 対応関係

* 「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説」は一般公開されていなかったため現時点では詳細な調査(A-2,B-1,B-2)を行っていないが、必要に応じて提供いただくガイドラインを用いた詳細調査は可能。(9/25筆者注)

[参考] NISC「重要インフラにおける安全基準等の継続的改善状況等に関する調査について」等
(https://www.nisc.go.jp/pdf/council/cs/ciip/dai37/37_shiryou2_kaizen.pdf)

- 本ガイドラインは、地方公共団体が地方自治法等に基づいて情報セキュリティポリシーを策定する上で構成や例文等を参考として示したもの。

位置づけ/参照関係



[凡例]

オレンジ色	認証登録制度等	緑色	法律・省令・通知
青灰色	標準・ガイドライン		
→	指示関係	←	対応関係

目的/想定読者

項目	目的	想定読者
地方自治法	地方公共団体の区分並びに地方公共団体の組織及び運営に関する事項の大綱を定め、併せて国と地方公共団体との間の基本的関係を確立することにより、地方公共団体における民主的にして能率的な行政の確保を図るとともに、地方公共団体の健全な発達を保障することを目的とする。	-
総務省大臣指令	- 各地方公共団体に向けて、セキュリティ対策等を依頼するもの。 ※「新たな自治体情報セキュリティ対策の抜本的強化について」の場合	- 各都道府県知事 - 各市区町村長 ※「新たな自治体情報セキュリティ対策の抜本的強化について」の場合
地方公共団体における情報セキュリティポリシーに関するガイドライン	本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したもの。	(地方公共団体における)情報セキュリティポリシーの策定を行うもの - セキュリティ上の職責を担うもの。

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

地方公共団体における情報セキュリティポリシーに関するガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 他のガイドライン等ではみられるものが少ない「インデント軽減」(例:障害発生時のネットワークからの切り離し)においても具体的な記載がなされている。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							21/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

地方公共団体における情報セキュリティポリシーに関するガイドライン 記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 情報セキュリティポリシーの例文や例文の解説において、具体的な情報が記載されている。

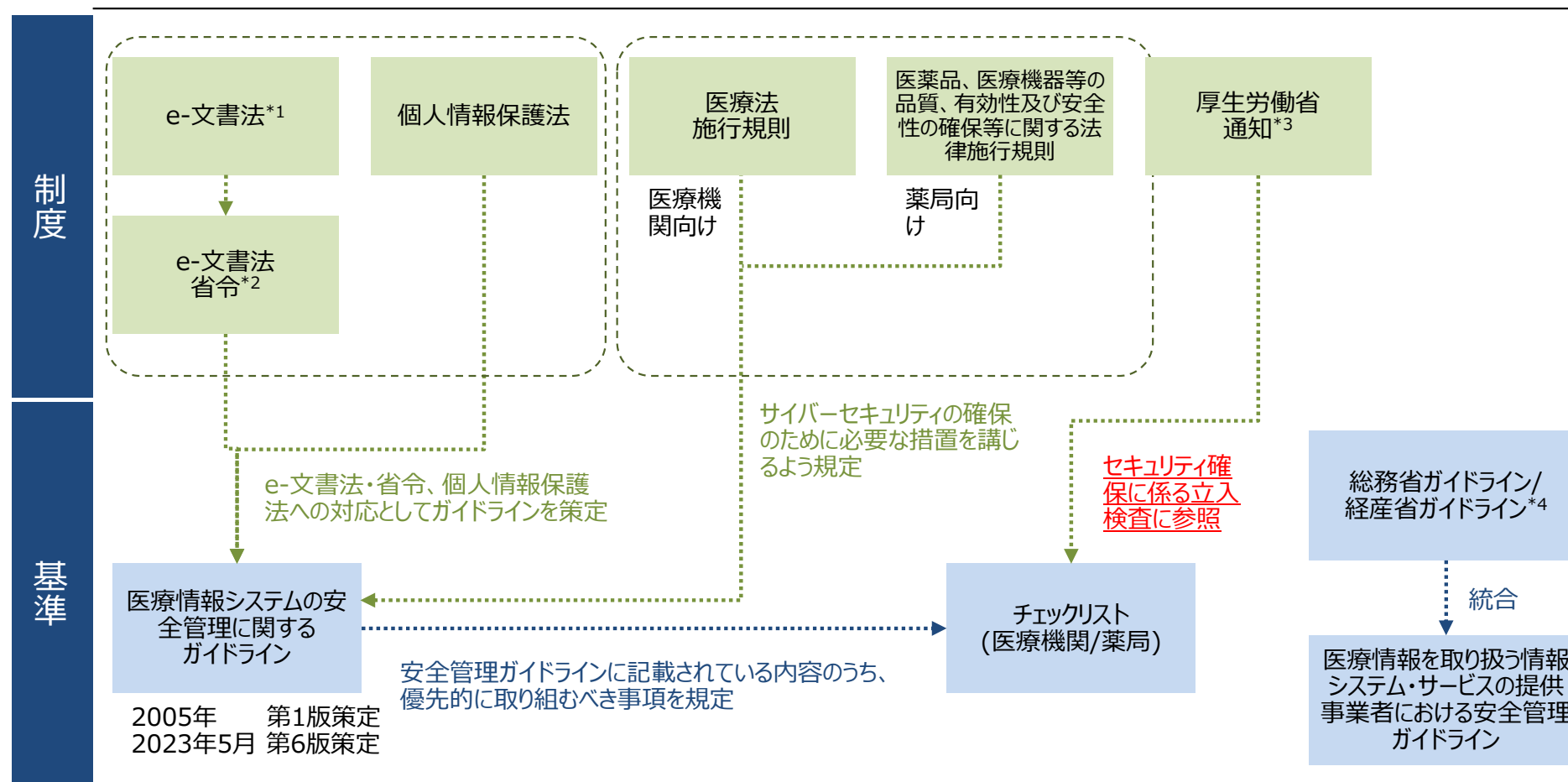
項目	記載粒度
内容 (what)	<組織的管理策> - 例文にて、<u>情報資産の管理にあたって表示する事項</u>を示す。 ✓ ファイル(ファイル名、ファイルの属性(プロパティ)、ヘッダー・フッター等) ✓ 格納する電磁的記録媒体のラベル ✓ 情報資産の分類(文書の隅等) <人的管理策> - 解説にて、<u>研修計画に盛り込む事項</u>を示す。 ✓ 研修内容 ✓ 受講対象者 ✓ e-ラーニング/集合研修 ✓ 説明会等の実施方法 ✓ 時期/日程/講師等 <物理的管理策> - 例文にて、<u>情報システム室の設置において出入りを制限する手法</u>を示す。 ✓ 鍵 ✓ 監視機能 ✓ 警報装置 - 例文にて、<u>入退室管理方法</u>を示す。 ✓ ICカード ✓ 指紋認証等の生体認証 ✓ 入退室管理簿の記載 <技術的管理策> - 解説にて、<u>アクセス制御機能の要件</u>を示す。 ✓ 利用時間や利用時間帯によるアクセス制御 ✓ 同一主体による複数アクセスの制限 ✓ IP アドレスによる端末の制限 ✓ ネットワークセグメントの分割によるアクセス制御
頻度 (when)	- ポリシーの例文にて、<u>職員等が受講する頻度(最低毎年度1回)</u>を示す。 - ポリシーの例文にて、<u>職員等の情報セキュリティ研修の実施状況についてCISOが情報セキュリティ委員会へ報告する頻度(毎年度1回)</u>を示す。
場所 (where)	例文において、<u>情報システム室の設置を禁止する場所(地階/1階)</u>を示す。その上で、無窓の外壁とするよう規定。(推奨事項)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

医療情報システムの安全管理に関するガイドライン 位置づけ等

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 本ガイドラインにおいて優先的に取り組むべき事項を整理したチェックリストは立入検査の際に参照されるため、実質的に義務となっている可能性がある。



[凡例] 認定登録制度等 法律・省令・通知 標準・ガイドライン → 指示関係 ⋯ 対応関係

*1 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律

*2 厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令

*3 厚生労働省医政局特定医薬品開発支援・医療情報担当参事官通知 医療関係は医政参発0609第1号 薬局は医政参発1013第1号

*4 総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」経産省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」

[参考] 厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版」

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 本ガイドラインは、医療情報システムの安全管理や、e-文書法等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したもの。

項目	目的	想定読者
医療情報システムの安全管理に関するガイドライン	本ガイドラインは、医療情報システムの安全管理や、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(「e-文書法」)等の<u>法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したもの。</u>	医療機関等において、すべての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者
医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	本ガイドラインは、<u>総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」及び経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」が定める要件</u>を整理・統合したガイドライン。	本ガイドラインが対象とする事業者は、医療機関等との契約等に基づいて医療情報システムやサービスを提供する事業者
チェックリスト (医療機関/薬局)	医療機関等におけるサイバーセキュリティ対策については、ガイドラインを参照の上、適切な対応を行うこととしているところ、このうちまずは<u>医療機関及び薬局が優先的に取り組むべき事項をまとめたもの。</u>	- 医療機関 - 薬局

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

医療情報システムの安全管理に関するガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 経営管理編、企画管理編、システム運用編において記載されている要件は全ての項目を網羅している。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							22/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

医療情報システムの安全管理に関するガイドライン 記載粒度

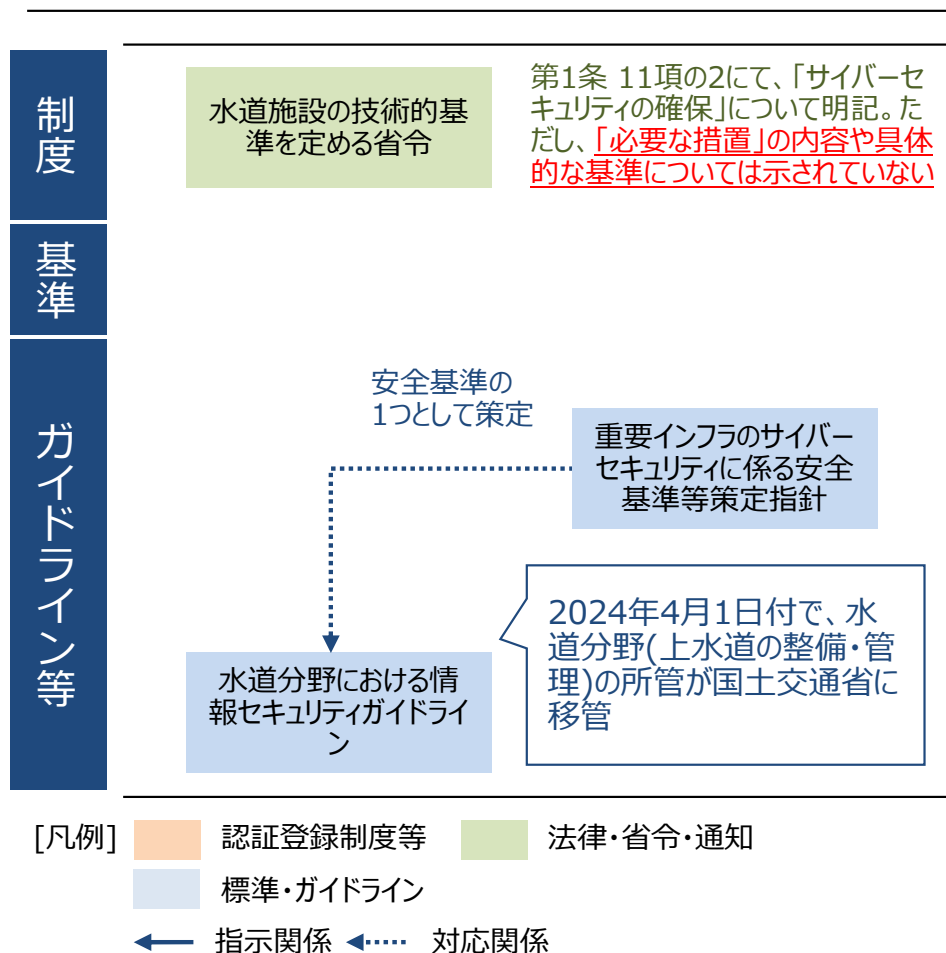
A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 比較対象とした要件においては主体や頻度、場所に係る具体的な情報は記載されていなかったが、主体や内容に係る情報が記載されている。

項目	記載粒度
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<組織的管理策> - 資産を管理する際の情報を例示。また、管理対象としてBYODを含む ✓ 使用するソフトウェア ✓ サービスのバージョン ✓ ライセンス <技術的管理策> - 利用者を認証する方法を例示。 ✓ パスワード ✓ ICカード ✓ 電子証明書 ✓ 生体認証等 ✓ 本人の識別・認証 - 認証強度を高める方法(二要素認証)を示す。 ※指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上(記憶・生体計測・物理媒体のいずれか2つ以上)の認証がなされている場合には、二要素認証とされている。
頻度(when)	(頻度に関する具体的な記載なし)
場所(where)	(場所に関する具体的な記載なし)

- 本ガイドラインは、水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準を示したもの。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
水道施設の技術的基準を定める省令	水道法(昭和三十二年法律第百七十七号)第五条第四項の規定に基づき、水道施設の技術的基準を定める。	-
水道分野における情報セキュリティガイドライン	本ガイドラインは、<u>水道事業者等において実施することが必要な又は望まれる情報セキュリティ対策の項目及び水準</u>を示したもの。	- 水道事業者 - 水道用水供給事業者

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

水道分野における情報セキュリティガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 水道分野では、異常検知やインシデント発生時の対応についても考慮した上で、ガイドラインが策定されていると考えられる。

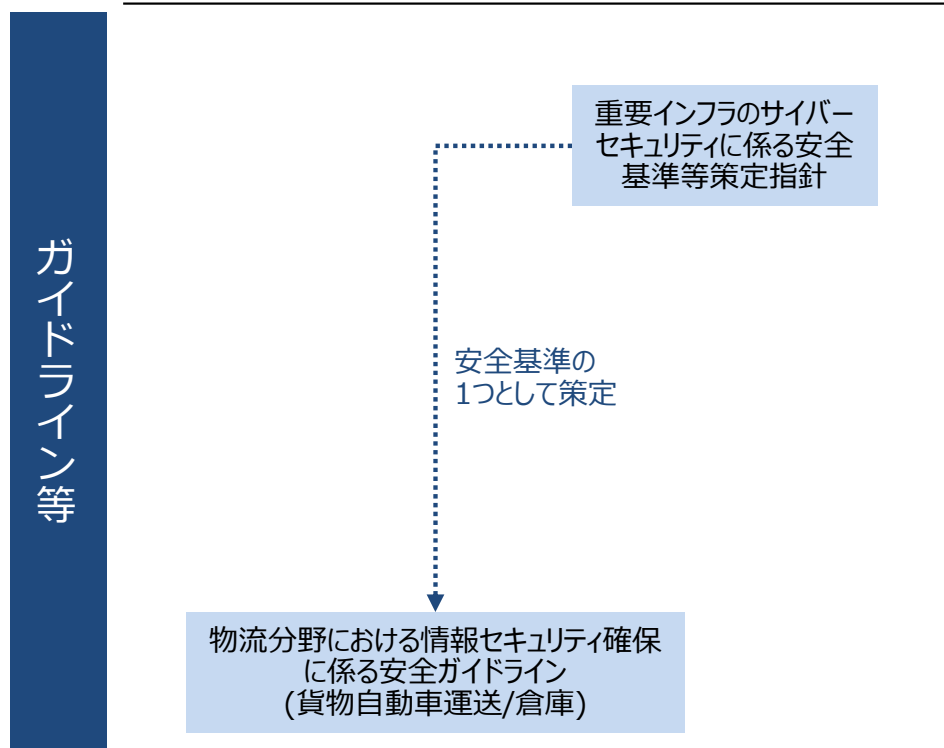
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							21/22

- 比較対象とした要件においては主体や頻度、場所に係る具体的な情報は記載されていなかったが、内容に係る情報が記載されている。

項目	記載粒度	項目	記載粒度
主体 (who)	(主体に関する具体的な記載なし)	内容 (what)	<技術的管理策> - 安全な区域を設置するための手段を例示。 ✓ 障壁、施錠 ✓ 入退室にあたって主体認証を実施 ✓ 入退室の理由や機関の記録、継続的に立ち入るものの承認手続きの採用 ✓ 入退室の承認にあたっては、その承認されているレベルを外見上で識別できるような仕組み（ストラップや IDカードの着用等）の導入 ✓ 安全区域での作業を監視するための措置(立会い、監視カメラ)の実施具体的に制限するアクセスの内容 ■ アクセス制御機能について例示。 ✓ アクセス制御を強化するため、利用者の権限管理(属性)以外のアクセス制御機能として利用時間による制御や端末指定による制御、強制アクセス制御等を導入すること ✓ 規定されたアクセス制御を実施する機能が情報システムに装備されていない場合は、利用者が運用上で注意を払うことでアクセス制御を遵守すること
内容 (what)	<組織的管理策> - 情報システムの構成要素を示す。 ✓ 施設 ✓ ネットワーク ✓ 周辺機器 ✓ ハードウェア ✓ システム領域 ✓ データ領域 ✓ システム運用体制 ✓ ベンダの継続能力 - 情報システムの資産区分を示す。 ✓ データ資産 ✓ ソフトウェア資産 ✓ ハードウェア資産 ✓ サービス資産 <人的管理策> - 訓練の流れと方法を例示。 ✓ STEP1:研修会(外部専門家等が講師として講演を実施) ✓ STEP2:ワークショップ(ワークショップ形式でリスクアセスメントを実施) ✓ STEP3:訓練(訓練シナリオを作成し、インシデント対応を図上訓練、情報システムを活用した実地訓練を実施)	頻度 (when)	(頻度に関する具体的な記載なし)
		場所 (where)	(場所に関する具体的な記載なし)

- 貨物自動車運送及び倉庫において、セキュリティ管理策の水準を示すことで、個々の重要インフラ事業者等が、重要インフラの担い手としての意識に基づいて自主的に取り組み、対策の実施や検証に当たっての目標を定めることを目的とする。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」
https://www.mlit.go.jp/jidosha/jidosha_tk4_000121.html

目的/想定読者

項目	目的	想定読者
物流分野における情報セキュリティ確保に係る安全ガイドライン	物流分野として、貨物自動車運送及び倉庫において、セキュリティ管理策の水準を示すことで、<u>個々の重要インフラ事業者等が、重要インフラの担い手としての意識に基づいて自主的に取り組み、対策の実施や検証に当たっての目標を定めることを目的とする。</u>	物流分野の重要インフラ事業者等

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

物流分野における情報セキュリティ確保に係る安全ガイドライン

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。
- 安全基準等策定指針を考慮しつつ、重要インフラ事業者が参照する推奨事項が記載されており、幅広い要件が盛り込まれている。

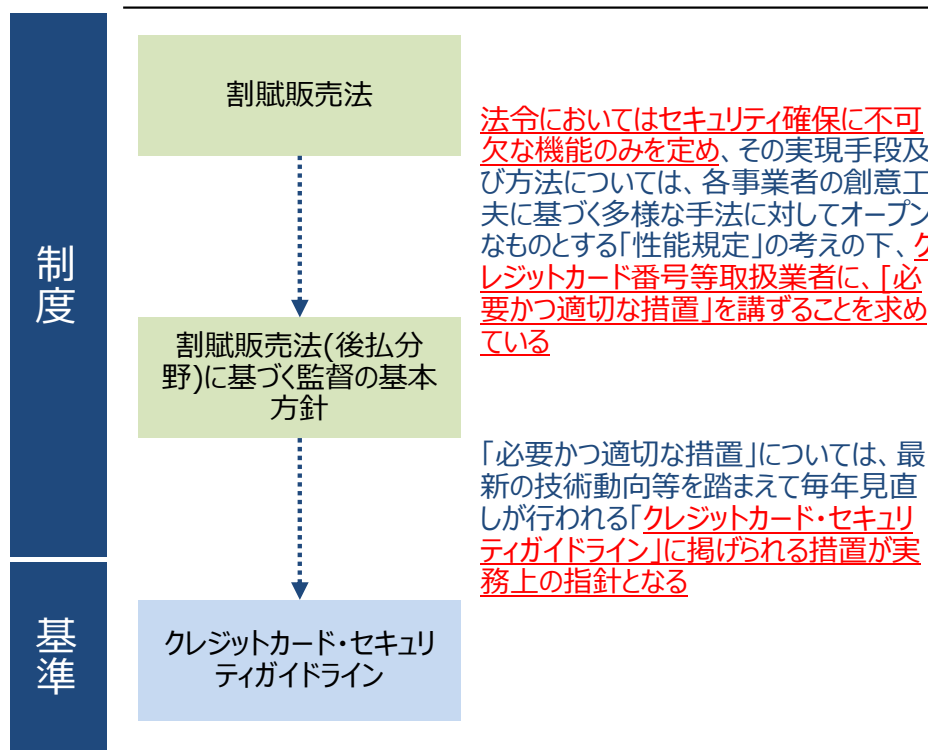
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							21/22

- 管理策における具体例の中で、詳細な情報を記載している。その中でも、実施内容(what)の部分において、具体的な記載が多く見られた。

項目	記載粒度
主体(who)	<技術的管理策> - 具体例にて、<u>対策を行う主体</u>ごとに対策を例示。 ✓ システム管理者 ✓ 端末を利用する取扱者 - 具体例にて、<u>セキュリティ対策の対象者</u>を例示。 ✓ 経営層 ✓ システム業務に従事する人材 ✓ システムユーザ ✓ PC操作者(テレワーク勤務者を含む) ✓ (必要に応じて)委託先
内容(what)	<組織的管理策> - 具体例にて、<u>情報システムの構成要素ごと</u>に対策例を例示。 ✓ 端末 ✓ サーバ装置 ✓ 通信回線・通信回線装置 ✓ 複合機及びIoT機器を含む特定用途機器 - 具体例にて、<u>資産管理台帳の維持方法</u>について例示。 ✓ 新しいハードウェア、ソフトウェア、ファームウェアを導入する際、事前承認を必要とする ✓ 承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する <物理的管理策> - 要管理対策区域への<u>訪問者に対する確認事項</u>を例示。 ✓ 氏名 ✓ 所属 ✓ 訪問目的並びに・訪問相手の氏名及び所属

- 本ガイドラインはクレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
標準・ガイドライン
指示関係 対応関係

目的/想定読者

項目	目的	想定読者
クレジットカード・セキュリティガイドライン	本ガイドラインは、安全・安心なクレジットカード利用環境を整備するため、<u>クレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者が実施すべきクレジットカード情報漏えい及び不正利用の防止のためのセキュリティ対策の取組を取りまとめたもの。</u>	「加盟店」や「カード会社(イシュー・アクワイアラー)」、「決済代行業者等(4号事業者)」、「コード決済事業者等(5号事業者)」、「コード決済事業者等の委託会社(6号事業者)」、「加盟店向け決済システム提供事業者(7号事業者)」

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

クレジットカード・セキュリティガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 「指針対策」において、PCI DSSを準拠することとする記載がみられる。防御や検知、対応、普及に係る項目が網羅されていたが、本調査結果に加えて、PCI DSSの要件が追加される点に留意いただきたい。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	2/6	防御 (続き)	データセキュリティ	○	3/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	-		検知	継続的モニタリング	○	2/2
	監督	-			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	-	1/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	-			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	○	
合計							14/22

留意点

- 「指針対策」において、PCI DSSを準拠することとする記載がみられる。
- 本調査結果に加えて、PCI DSSの要件が追加される点に留意いただきたい。

- 比較対象とした要件においては主体や頻度、場所に係る具体的な情報は記載されていなかったが、主体や内容に係る情報が記載されている。

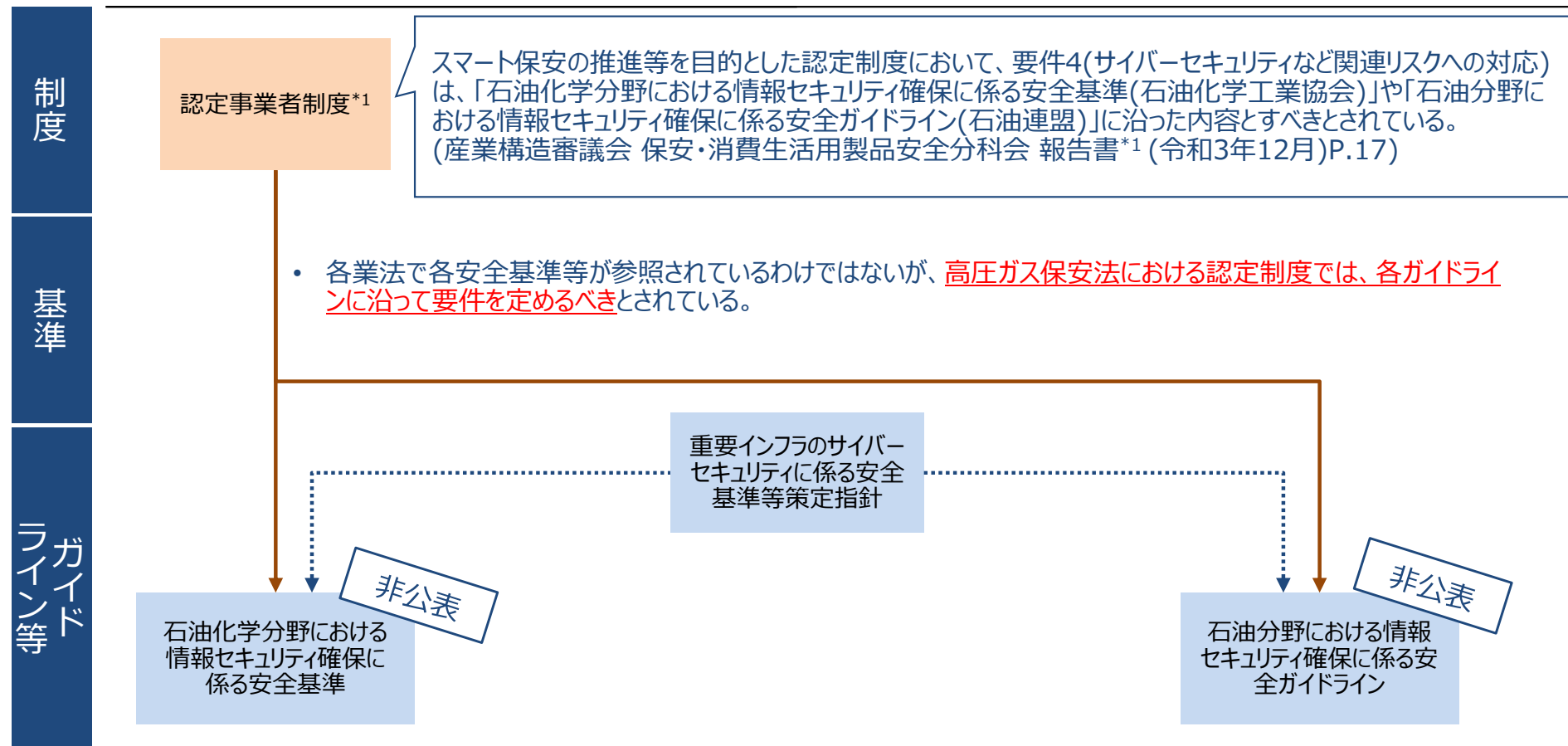
項目	記載粒度
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<技術的管理策> ・ <u>非対面不正利用対策の1つとして、認証方法を例示。</u> ✓ 本人認証(EMV3-Dセキュア):カード会員のデバイス情報等を用いて不正利用のリスク判断を行うとともに、必要に応じてパスワード入力を要求することで当該取引における安全性を確保 ✓ 本人認証(認証アシスト):取引時の属性情報とカード会社(イシューア)の登録属性情報を照合し本人を確認 ✓ 券面認証:カード券面の「セキュリティコード(数字 3～4 桁)」を入力し、カードが真正であることを確認具体的に制限するアクセスの内容を示す。
頻度(when)	(頻度に関する具体的な記載なし)
場所(where)	(場所に関する具体的な記載なし)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

石油化学分野における情報セキュリティ確保に係る安全基準/石油分野における情報セキュリティ確保に係る安全ガイドライン 位置づけ等 / 目的等

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 各業法で各安全基準等が参照されているわけではないが、高圧ガス保安法における認定制度では、各ガイドラインに沿って要件を定めるべきとされている。



[凡例] 認定登録制度等 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

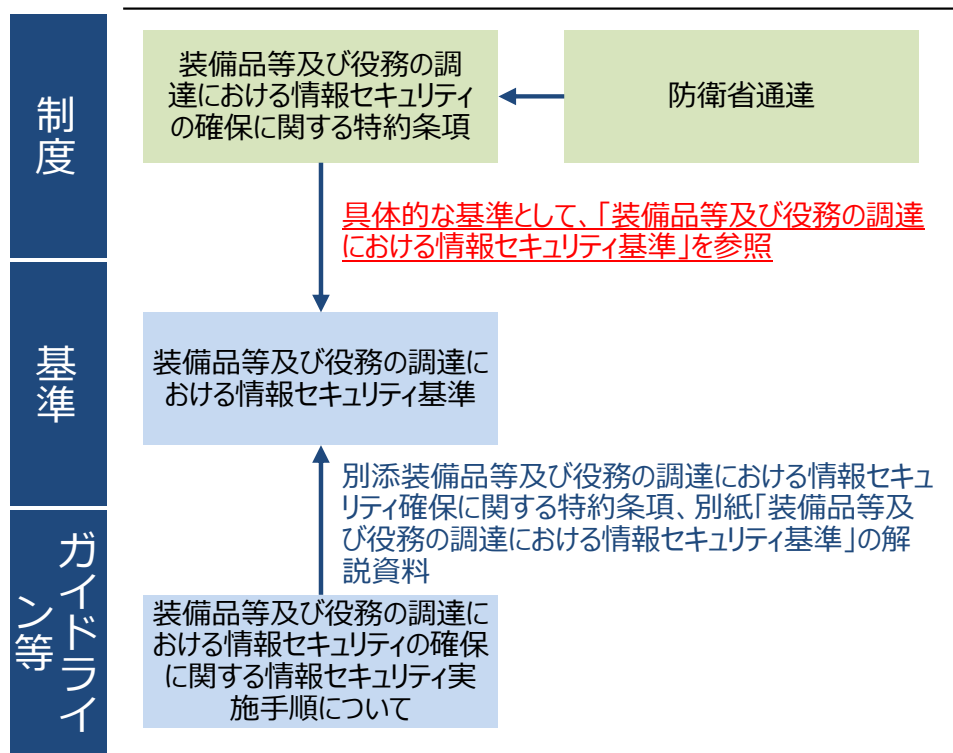
*1 貴省「認定事業者制度」参照。例えば認定事業者(スーパー認定事業者)に、ENEOSや出光興産がある。
(https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/sp-nintei/index.html)

*2 貴省「産業構造審議会 保安・消費生活用製品安全分科会 報告書」
(https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/pdf/20211221_1.pdf)

[参考] 貴省「高圧ガス保安法における新たな認定制度の詳細設計について②」
(https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/pdf/024_01_00.pdf)

- 装備品等及び役務の調達における情報セキュリティ基準は、装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。

位置づけ/参照関係



[凡例] 認証登録制度等 法律・省令・通知
 標準・ガイドライン
 指示関係 対応関係

目的/想定読者

項目	目的	想定読者
装備品等及び役務の調達における情報セキュリティの確保に関する特約条項	• 装備品等及び役務の調達において、<u>当該調達に関わる企業で取り扱われる保護すべき情報の保全のため必要な措置</u>を定め、もって企業に適切な情報セキュリティ対策を実施させることを目的とする。 • 防衛省通達の別添資料。	• 防衛省との装備品等及び役務の調達に係る企業
装備品等及び役務の調達における情報セキュリティ基準	• 本基準は、<u>装備品等及び役務の調達に係る企業において当該調達に係る保護すべき情報の適切な管理を目指し、防衛省として求める対策を定めたもの。</u>	
装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ実施手順について	• 本資料は、装備品等及び役務の調達における情報セキュリティの確保について別添装備品等及び役務の調達における情報セキュリティ確保に関する特約条項、別紙付紙「装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領」の解説資料。	

[参考] 防衛装備庁「装備品及び役務の調達における情報セキュリティの確保に関する特約条項」

(http://www.clearing.mod.go.jp/kunrei_data/j_fd/2021/jz20220331_00137_000.pdf)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

装備品等及び役務の調達における情報セキュリティ基準 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 記載されている要件に大きな偏りはなく、ほとんどの項目を網羅している。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							21/22

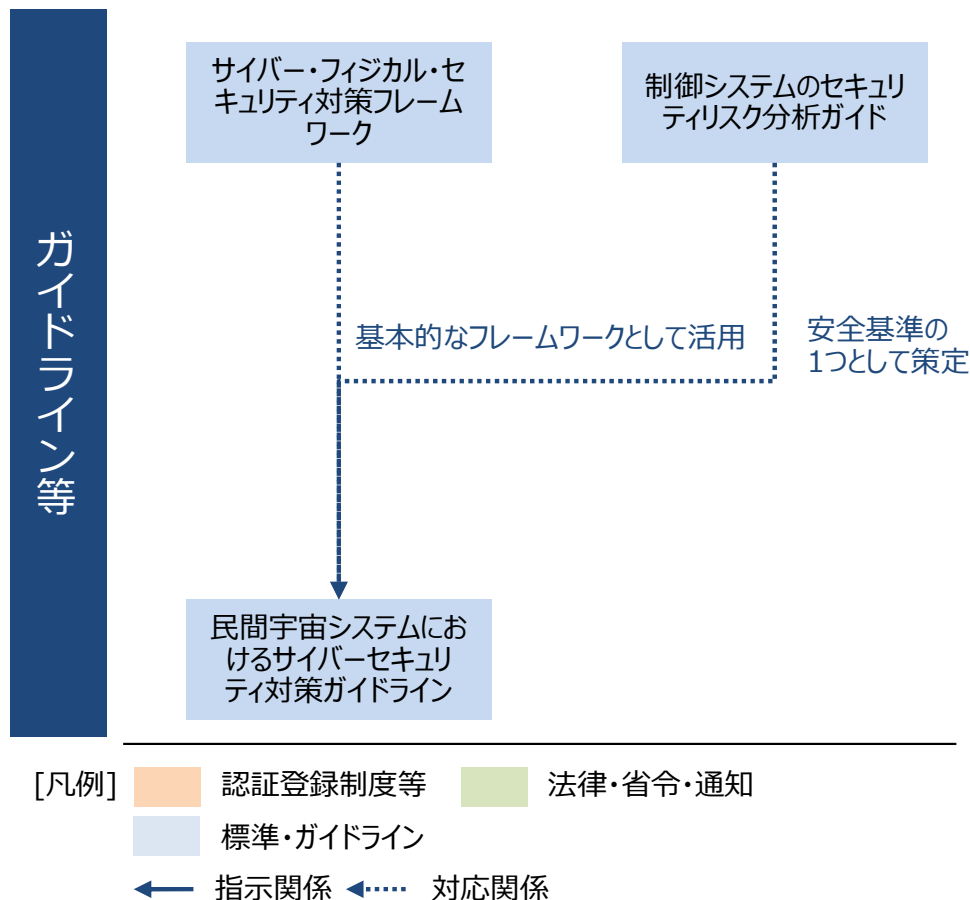
- 比較対象とした要件においては場所に係る具体的な情報は記載されていなかったが、主体や内容に係る情報が記載されている。

項目	記載粒度
主体(who)	<人的管理策> - 教育の対象者を示す。 ✓ 総括者 ✓ 管理者 ✓ 保護システム管理者 ✓ 保護システム担当者
内容(what)	<人的管理策> <u>教育内容</u>を示す。 ✓ 情報セキュリティの重要性及び意義 ✓ 「need to knowの原則」(「情報は知る必要がある者のみに伝え、知る必要のない者には伝えない」という原則)の確実な履行 ✓ 情報セキュリティ基本方針等の確実な履行 ✓ 公私における慎重な行動 ✓ 悪意のあるコードへの感染、内部不正、情報セキュリティ事象及び同事故等への対処手順 ✓ 前号に掲げる事項のほか、情報セキュリティ事故等への対処のために必要な事項 ✓ 上記に掲げる事項のほか、取扱者の役割と責任に応じて必要となる技術的及び専門的な事項 <物理的管理策> <u>物理的セキュリティ対策の対象を示す。</u> ✓ 取扱い施設 ✓ 入退管理機器 ✓ 保護システム ✓ 保管された保護すべき情報

項目	記載粒度
内容(what) ※続き	<保管された保護すべき情報> • <u>入退室管理の方法を示す。</u> ✓ 取扱施設と関係施設の境界に入退口を設置し、入退管理機器又は警備員等により、入退する者が当該入退を許可された者であることを管理すること ✓ 関係施設の外側境界に入退口を設置し、必要な管理措置により入退者を制限すること ✓ 取扱施設への入退をIDカードにより管理する場合は、当該入退の記録を電子的に取得すること ✓ 取扱施設への入退を警備員等により管理する場合は、必要に応じて入退する者の所属、氏名、入退の時間等所要の事項を記録簿に記載すること ✓ 取得した記録は、定期的に、及び保護すべき情報等への不正なアクセスの発見に資するなど必要と認められる場合には、その都度精査すること ✓ 取扱施設等において敷地を指定した場合は、十分な高さ及び強度のあるフェンス等を設置するなど必要な措置を講じること ✓ 取扱施設の入退をICカードのみで管理する場合は、当該施設の境界を警備員等、センサー装置又は監視カメラによる監視など必要な措置を講じること ✓ 取扱施設においては、当該施設の画像、動画、音声等の情報の収集・通信が可能な機器（携帯電話、デジタルカメラ、ボイスレコーダー等）の利用（持ち込みを含む。）を制限すること
頻度(when)	<人的管理策> • <u>教育のタイミングを示す。</u> ✓ 年に1度 ✓ 新たな取扱者を指定した場合 ✓ 取扱者の異動及び職務内容の変更した場合 ✓ 保護システムの変更が生じた場合
場所(where)	(場所に関する具体的な記載なし)

- 本ガイドラインは、宇宙システムに係るセキュリティ上のリスクや基本的セキュリティ対策等を示し、民間事業者における自主的な対策を促すことを目的としている。

位置づけ/参照関係



目的/想定読者

項目	目的	想定読者
民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン	- 本ガイドラインは、以下についてについて分かりやすく整理して示し、民間事業者における自主的な対策を促すことを目的としている - 宇宙システムに係るセキュリティ上のリスク - 宇宙システムに関わる各ステークホルダーが検討すべき基本的セキュリティ対策 - 対策の検討に当たり参考になる参考文献、活用可能な既存施策 等	- 衛星所有者 - 衛星運用事業者 - 衛星データプラットフォーム事業者 - 衛星データ利用サービス事業者 - 衛星開発事業者

- 本ガイドラインでは、サイバーセキュリティ管理体制の構築、自社のサイバーセキュリティリスクの特定及び対策の実装に当たっては、既存の基準等を活用することが望ましいとされている。その既存の基準にCSFが含まれている。本調査で「-」とされている項目は多いが、記載範囲の偏りがあることにはならない。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	1/6	防御 (続き)	データセキュリティ	○	3/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	-			技術インフラのレジリエンス	-	
	ポリシー	-		検知	継続的モニタリング	○	2/2
	監督	-			有害イベントの分析	○	
	サイバーセキュリティサプライチェーンリスクマネジメント	○		対応	インシデントマネジメント	-	0/4
識別	資産管理	○	留意点 サイバーセキュリティ管理体制の構築、自社のサイバーセキュリティリスクの特定及び対策の実装に当たっては、既存の基準等を活用することが望ましいとされている。その既存の基準にCSFが含まれているため、本調査で「-」となっても、記載範囲の偏りがあることにはならない。				
	リスクアセスメント	○					
	改善	-	インシデント軽減		-		
防御	アイデンティティ管理とアクセス制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケーション	-	
合計							8/22

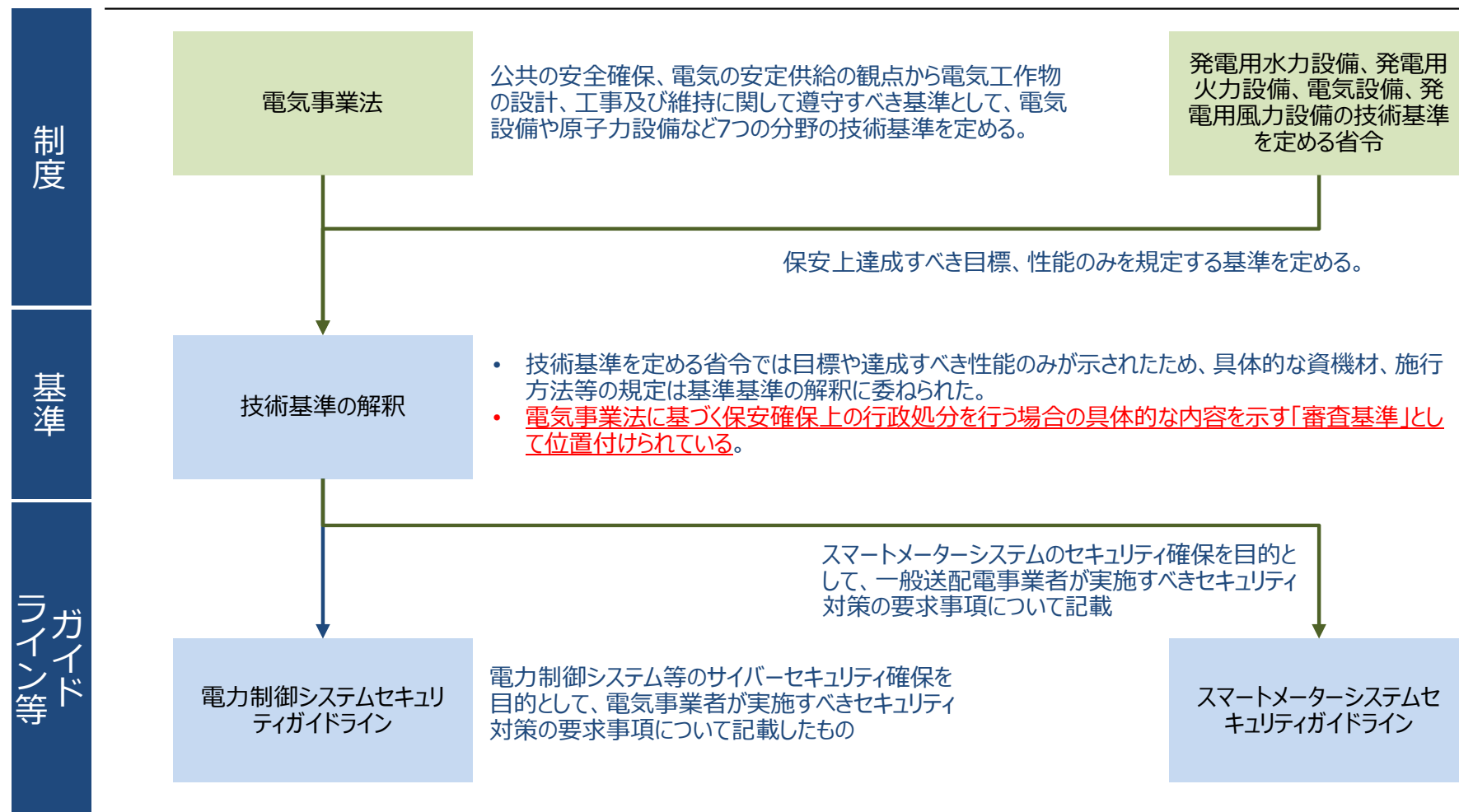
- 比較対象とした要件においては、宇宙システムの地上施設等に対する物理的な記載がみられた。
- ただし、既存の基準等でカバーしているため、要件が設けられてないわけではない点に留意いただきたい。

項目	記載粒度
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<物理的管理策> - 解説にて、<u>地上施設への物理的攻撃に対する対策を例示</u>。 ✓ 警備員の配備 ✓ ゲートの設置 ✓ 施設へのアクセスコントロール（取り扱う情報及び取り扱うエリアの制限） ✓ 攻撃を受けた場合に備えたバックアップサイトの設置 - 解説にて、<u>外部からの不審者や権限のない職員等の侵入に対する備え</u>を例示。 ✓ 衛星運用システムのうち、追跡管制・受信を行うシステム又はエリアへの立入りを制限 ✓ 衛星運用システムのうち、ネットワーク運用・ミッションコントロール等の衛星運用業務を行うシステム又はエリアへの立入りを制限 ✓ 衛星運用システムが不正利用されることを防ぐため、施錠、入退室記録又は入室検知といった対策 ✓ 衛星運用システムがほかのシステムの一部に所在する場合には、当該システムの管理者との連絡手段と体制を確認・整備する対策 ✓ 国内外の地上局（追跡管制局及び受信局）ネットワークの運用情報の漏えい・改ざんを防止するため、ネットワーク運用業務を取り扱うエリア及び情報システムを制限 ✓ 国内外の地上局との通信経路・通信情報、格納データの暗号化機能を実装する対策資産を管理するために作成する
頻度(when)	(頻度に関する具体的な記載なし)
場所(where)	(場所に関する具体的な記載なし)

留意点

- サイバーセキュリティ管理体制の構築、自社のサイバーセキュリティリスクの特定及び対策の実装に当たっては、既存の基準等を活用することが望ましいとされている。したがって、具体的な記載はみられなかったが、既存の基準等でカバーしているため、要件が設けられてないわけではない点に留意いただきたい。

- 電気事業法では、電気設備や原子力設備など7つの分野の技術基準を定める。
- 技術基準の解釈は、電気事業法に基づく保安確保上の行政処分を行う場合の具体的な内容を示す「審査基準」として位置付けられている。



[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン ← 指示関係 ←..... 対応関係

- 電力制御システムセキュリティガイドラインは、電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載したもの。

項目	目的	想定読者
電気事業法	公共の安全確保、電気の安定供給の観点から電気工作物の設計、工事及び維持に関して遵守すべき基準として、電気設備や原子力設備など7つの分野の技術基準を定める。	-
発電用水力設備、発電用火 力設備、電気設備、発電用風 力設備の技術基準を定める省 令	保安上達成すべき目標、性能のみを規定する基準を定める。	-
技術基準の解釈	- 技術基準を定める省令では目標や達成すべき性能のみが示されたため、具体的な資機材、施行方法等の規定は基準基準の解釈に委ねられた。 - 電気事業法に基づく保安確保上の行政処分を行う場合の具体的な内容を示す「審査基準」として位置付けられている。	-
電力制御システムセキュリティ ガイドライン	本ガイドラインは、電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について記載したもの。	電気事業者が施設する電力制御システム等に携わる者
スマートメーターシステムセキュ リティガイドライン	本ガイドラインは、スマートメーターシステムのセキュリティ確保を目的として、一般送配電事業者が実施すべきセキュリティ対策の要求事項について記載したもの。	一般送配電事業者

- 本ガイドラインでは、CSFと比較した際に一部網羅されていない要求事項がみられた。本ガイドラインは、電力業界にとって実質的な義務になっているため、記載されている範囲が限定されていると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	4/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	1/2
	監督	○			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	-		対応	インシデントマネジメント	○	2/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							15/22

- 組織的管理策や技術的管理策の中で具体的な記載が一部みられたが、比較した要件においては解説も含めて具体的な記載は少ない。

項目	記載粒度
主体 (who)	(主体に関する具体的な記載なし)
内容 (what)	<組織的管理策> - 資産の構成情報を示す。 ✓ 管理番号 ✓ 設置場所 ✓ ソフトウェアやファームウェアのバージョン等 ✓ 機器に関する情報 <技術的管理策> <u>アクセス制御を行うにあたって実施することが望ましい事項</u>を記載 ✓ 接続制御 ✓ 認証 ✓ ネットワーク分割
頻度 (when)	(頻度に関する具体的な記載なし)
場所 (where)	(場所に関する具体的な記載なし)

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

スマートメーターシステムセキュリティガイドライン 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 一部差異(例:サイバーセキュリティサプライチェーンリスクマネジメント)はみられたが、電力制御システムセキュリティガイドラインと比較した際に、大きな差異はみられなかった。

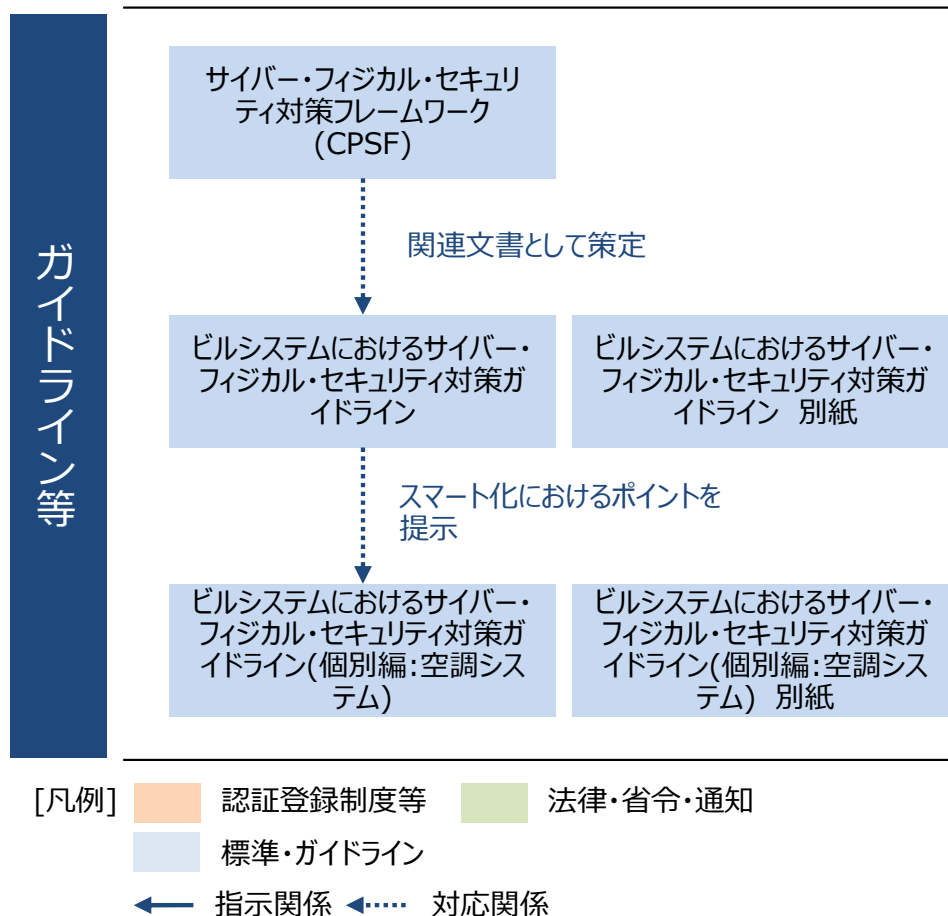
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	5/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	2/3		インシデント分析	○	
	リスクアセスメント	-			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							18/22

- スマートメータシステム特有の管理策はみられたが、記載粒度は電力制御システムガイドラインと同等程度の内容となっている。

項目	記載粒度
主体 (who)	<人的管理策> • <u>セキュリティ教育の対象</u>を示す。 ✓ スマートメータに関連する者
内容 (what)	<組織的管理策> • 資産の<u>構成情報</u>を示す。 ✓ 管理番号 ✓ 設置場所 ✓ ソフトウェアやファームウェアのバージョン等 ✓ 機器に関する情報 <技術的管理策> • スマートメータシステムにおける<u>機器認証を行う際に実施することが望ましい事項を記載</u> ✓ 安全な通信手段(暗号や専用線)
頻度 (when)	<人的管理策> • <u>セキュリティ教育の頻度</u>を示す。 ✓ 少なくとも年1回
場所 (where)	(場所に関する具体的な記載なし)

- 本ガイドラインは、ビルシステムのサイバーセキュリティに関してその確保のためのガイダンスを示すことを目的として策定された。

位置づけ/参照関係の分析



[参考] 貴省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」等
https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html

目的/想定読者

項目	目的	想定読者
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	- 本ガイドラインの目的は、<u>ビルシステムのサイバーセキュリティに関して、その確保のためのガイダンスを示すこと</u>である。 - ビルシステム概念について概要を整理し、それに対する脅威を示すとともに、これらの脅威に対する対策について、設計、建設、竣工検査、運用、改修／廃棄のビルシステムのライフサイクルに係わる各段階において整理して示すものである。 - 第2版では、さらに実際に脅威に遭遇した際に取りべき対応についても整理をしている。	- ビルオーナー - ゼネコン、サブコン - 設計事務所 - 個別システム事業者（ビル管理システム、空調、エレベータ、ビデオ監視、電力・熱供給等） - ビル管理会社 - テナント - サービスプロバイダ
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編:空調システム)第1版	本ガイドラインは、<u>ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策が含まれた共通編として作成</u>され、ビル関係者が共通に参照し、ビルシステムについての初歩的なサイバーセキュリティ対策を考えていくうえでの入り口となる情報を提供することを目指したものである。	- セキュリティベンダ、ネットワークシステムベンダ - 自治体、関係省庁等

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

- 本ガイドラインではほとんどの項目が網羅されていた。
- 本ガイドラインはインシデントレスポンスについて詳細な記載を設けており、他のガイドラインでは詳細に記載されることが少ない対応や復旧の要求事項を網羅している。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	4/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	-		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	4/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	2/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	○	
合計							20/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
記載粒度

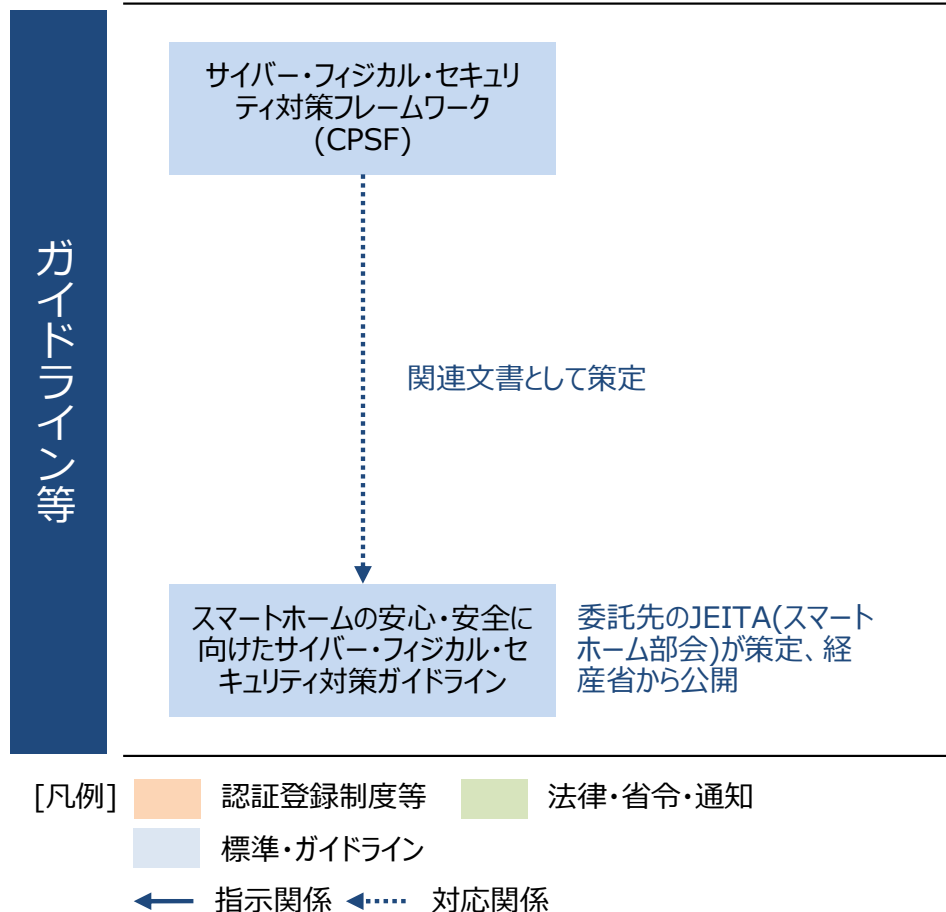
A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 組織的管理策、人的管理策の中で具体的な記載が一部みられた。
- 資産管理を行うために必要な情報はより具体的な記載がなされている。

項目	記載粒度
頻度(when)	(頻度に関する具体的な記載なし)
場所(where)	(場所に関する具体的な記載なし)
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<組織的管理策> - 資産管理を行うための文書を例示 ✓ ビルに導入されているすべてのシステムや機器を把握することのできる一覧表 ✓ ネットワーク図 ✓ 当該ビル内外の各種システムとの接続・連携構成 ✓ それぞれの担当者（担当ベンダ等） - ビルに導入されている機器の内容を例示 ✓ サーバ ✓ 端末 ✓ OS ✓ アプリケーション <人的管理策> - ビルの運転管理者(発注主側)に提示する教育に必要な情報を示す。 ✓ 教育人数 ✓ 教育テキスト ✓ 教育機関 ✓ 教育内容 ✓ 教育場所

- 本ガイドラインは、「Connected Industries」の重点分野の 1 つであるスマートライフ分野の核となるスマートホームに必要となるサイバーセキュリティ上の技術的な対策、および管理項目の明確化を目指すもの。

位置づけ/参照関係の分析



目的/想定読者

項目	目的	想定読者
スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン	本ガイドラインは、「Connected Industries」の重点分野の 1 つであるスマートライフ分野の核となる<u>スマートホームに必要となるサイバーセキュリティ上の技術的な対策、および管理項目の明確化</u>を目指すものである。	- スマートホーム向け IoT 機器の事業者 - スマートホーム向けの IoT 機器を遠隔から管理する事業者 - スマートホーム向けのサービス事業者 - スマートホームを供給する事業者 - スマートホーム向けにメンテナンスやサポートを行う事業者 - スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社 - スマートホーム化された賃貸住宅の所有者や管理受託会社 - スマートホームの住まい手

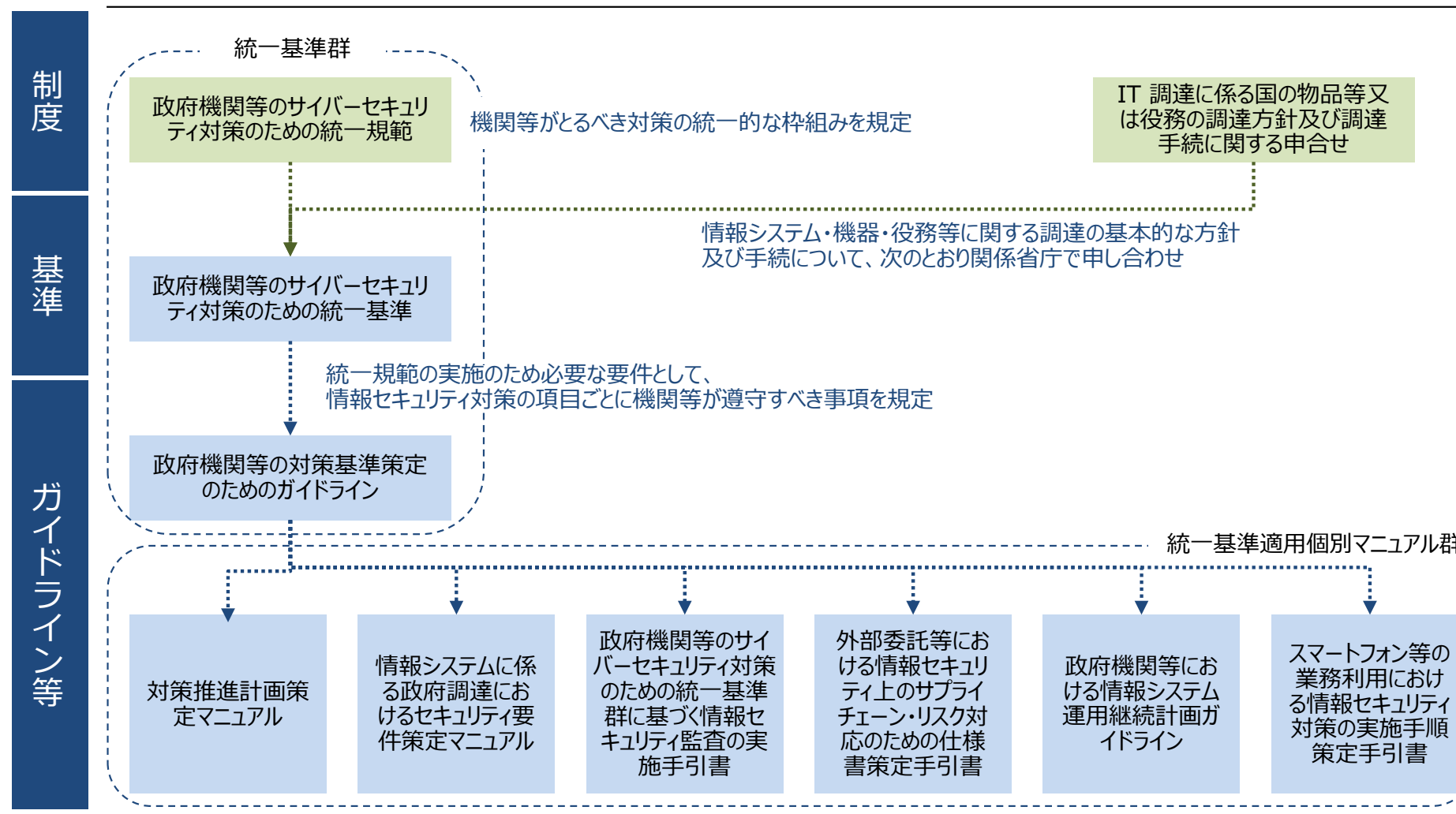
- 本ガイドラインでは、IoT機器であるスマートホームを対象とした要求事項を示している。組織を対象としたCSFと比較した際に偏りがみえるが、必ずしも記載範囲において不十分と判断されるわけではない点に留意。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	-	3/6	防御 (続き)	データセキュリティ	○	3/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	○	1/2
	監督	-			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	1/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	-	0/2
	意識向上及びトレーニング	-			インシデント復旧のコミュニケー ション	-	
合計							11/22

- 組織的管理策や技術的管理策の中で具体的な記載が一部みられた。
- 技術的管理策において、パスワード設定等のアクセス制御に係る具体的な記載がなされている。

項目	記載粒度
頻度(when)	(頻度に関する具体的な記載なし)
場所(where)	(場所に関する具体的な記載なし)
主体(who)	(主体に関する具体的な記載なし)
内容(what)	<組織管理策> - 対策例にて、<u>資産管理にあたって維持(最新化)する情報</u>を示す。 ✓ 共用スペースにおける住棟内ネットワーク、および住棟内ネットワークに接続された機器の接続情報 ✓ ソフトウェアバージョン <技術的管理策> - 対策例にて、<u>初期設定時、運用時の対策</u>を例示。 ✓ [初期設定時]IoT機器には予め個体毎に個別の初期パスワードを付与し、共通の初期パスワードを持たないような設計とする。 ✓ [初期設定時]初期パスワードが個体毎に同一である場合、初回の利用時等にパスワードを変更しない限り利用できないようにする ✓ [運用時]企業等の組織向けには規則上必要な場合もあり、定期的にパスワード等の認証情報の変更を促す機能を設ける - 対策例にて、<u>IoT機器におけるアクセスを制限する方法</u>を例示。 ✓ MACアドレスやIPアドレス等によるフィルタリングで相手先を制限してもよいし、パスワードや認証鍵、証明書等などを用いる認証技術を行ってもよい。 ✓ IoT機器がサーバに接続や通信する場合には、サーバをフィルタリングや認証した後に、接続や通信してもよい。 ✓ システムの要件によってはエンドツーエンドで相互認証できる機能を提供してもよい。 ✓ DHCPでIPを動的に割り当てる場合には、DNSスプーフィング対策として、DNSサーバの手動設定するオプション等を提供すべきである。

- 統一基準群は、「政府機関等のサイバーセキュリティ対策のための統一規範」及び「政府機関等のサイバーセキュリティ対策のための統一基準」、「政府機関等の対策基準策定のためのガイドライン」から構成される。



[凡例] 認証登録制度等 法律・省令・通知 標準・ガイドライン 指示関係 対応関係

- 政府機関等のサイバーセキュリティ対策のための統一基準は、統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項を規定。

項目	目的	想定読者
政府機関等のサイバーセキュリティ対策のための統一規範	本規範は、サイバーセキュリティ基本法第二十六条第一項第二号に定める国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準として、<u>機関等がとるべき対策の統一的な枠組みを定め</u>、機関等に自らの責任において対策を図らしめることにより、もって機関等全体のサイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図ることを目的とする。	- 国の行政機関 - 独立行政法人 - 指定法人
IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ	<u>各省庁等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、次のとおり関係省庁で申し合わせ</u>、講ずべき必要な措置について明確化を図ることを目的とする。	対象とする政府機関(内閣官房、内閣法制局、人事院、内閣府、宮内庁、公正取引委員会、個人情報保護委員会、警察庁、金融庁、消費者庁、復興庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省、会計検査院)
政府機関等のサイバーセキュリティ対策のための統一基準	本統一基準は、全ての機関等において共通的に必要とされる情報セキュリティ対策であり、政府機関等のサイバーセキュリティ対策のための統一規範に基づく機関等における統一的な枠組みの中で、<u>統一規範の実施のため必要な要件として、情報セキュリティ対策の項目ごとに機関等が遵守すべき事項を規定</u>することにより、機関等の情報セキュリティ水準の斉一的な引上げを図ることを目的とする。	- 国の行政機関 - 独立行政法人 - 指定法人
政府機関等の対策基準策定のためのガイドライン	- 本ガイドラインは、国の行政機関、独立行政法人及び指定法人が政府機関等のサイバーセキュリティ対策のための統一基準の規定を遵守するための対策基準を策定する際に参照するものである。 <u>統一基準の遵守事項を満たすためにとるべき基本的な対策事項を例示</u>するとともに、<u>対策基準の策定及び実施に際しての考え方等を解説するもの</u>である。これにより、機関等が、本ガイドラインを参照しつつ、組織及び取り扱う情報の特性等を踏まえて対策基準を定められるようにすることを目的とする。	- 国の行政機関 - 独立行政法人 - 指定法人
対策推進計画策定マニュアル	本マニュアルは、「政府機関等のサイバーセキュリティ対策のための統一基準」の遵守事項 2.1.3(4)(a)によって機関等が策定することとされている<u>対策推進計画</u>について、<u>その策定に当たっての考え方や主眼点等を示し</u>、もって機関等における当該計画の円滑な策定に資することを目的とするもの。	-

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理
政府機関等のサイバーセキュリティ対策のための統一基準
目的等(2/2)

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

項目	目的	想定読者
情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	本マニュアルは、<u>政府機関における情報システムの調達仕様書に記載する「セキュリティ要件」の策定方法を解説すること</u>によって、情報システムの企画段階からセキュリティ対策を適切に組み込むことを目的としている。	政府機関の職員のうち、情報システムの調達を担当する調達担当者及び情報システムを供給する事業者
政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書	本書は、<u>監査実施計画の策定における考え方や計画に含めるべき内容や・情報セキュリティ監査を実施するにあたり、機関等が実施すべき事項、実施手順等を具体的に示すこと</u>により、情報セキュリティ関係規程の整備・運用に関する情報セキュリティ監査の適切な実施に資することを目的と	- 機関等の情報セキュリティ監査の業務を担う、機関等の最高情報セキュリティ責任者 - 統括情報セキュリティ責任者 - 情報セキュリティ監査責任者 - 情報セキュリティ監査を実施する監査実施者
外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書	本書は、<u>当該遵守事項を適切に実施するための「目的、判断ポイント、具体的な対策の例」等を解説しており、統一基準の遵守事項に対する理解を深めるとともに、府省庁における情報セキュリティ上のサプライチェーン・リスクに対応するための調達仕様書の円滑な作成に資することを目的としている。</u>	情報システムの構築、運用等の外部委託や機器等の調達を行う機会がある行政事務従事者
政府機関等における情報システム運用継続計画ガイドライン	本書は、政府機関等の情報システム担当者が、<u>情報システム運用継続計画を策定し、計画の実施と継続的維持改善をするための手引書</u>である	政府機関等の情報システム担当者
スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書	本書は、<u>スマートフォン等を府省庁の業務に利用する場合に、政府機関の情報セキュリティ対策のための統一基準に準拠した情報セキュリティ対策の実施手順を定める際の、要件の策定の考え方や対策例等を整理したもの</u>である。	- スマートフォン等を業務利用する組織において安全管理措置に係る手順を策定する統括情報セキュリティ責任者及びその命を受けて実施手順の策定業務に携わる行政事務従事者 - スマートフォン等の安全管理措置の実施状況を管理する責任者（情報セキュリティ責任者、課室情報セキュリティ責任者）及びその命を受けて管理業務に携わる行政事務従事者 - スマートフォン等の接続先となる情報システム（例えば、府省庁 LAN）の情報システムセキュリティ責任者及びその命を受けて管理業務に携わる行政事務従事者

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

政府機関等のサイバーセキュリティ対策のための統一基準 記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- なお、今回は義務されている政府機関等のサイバーセキュリティ対策のための統一基準を対象として調査を行った。本基準ではほとんどの項目が網羅されていた。

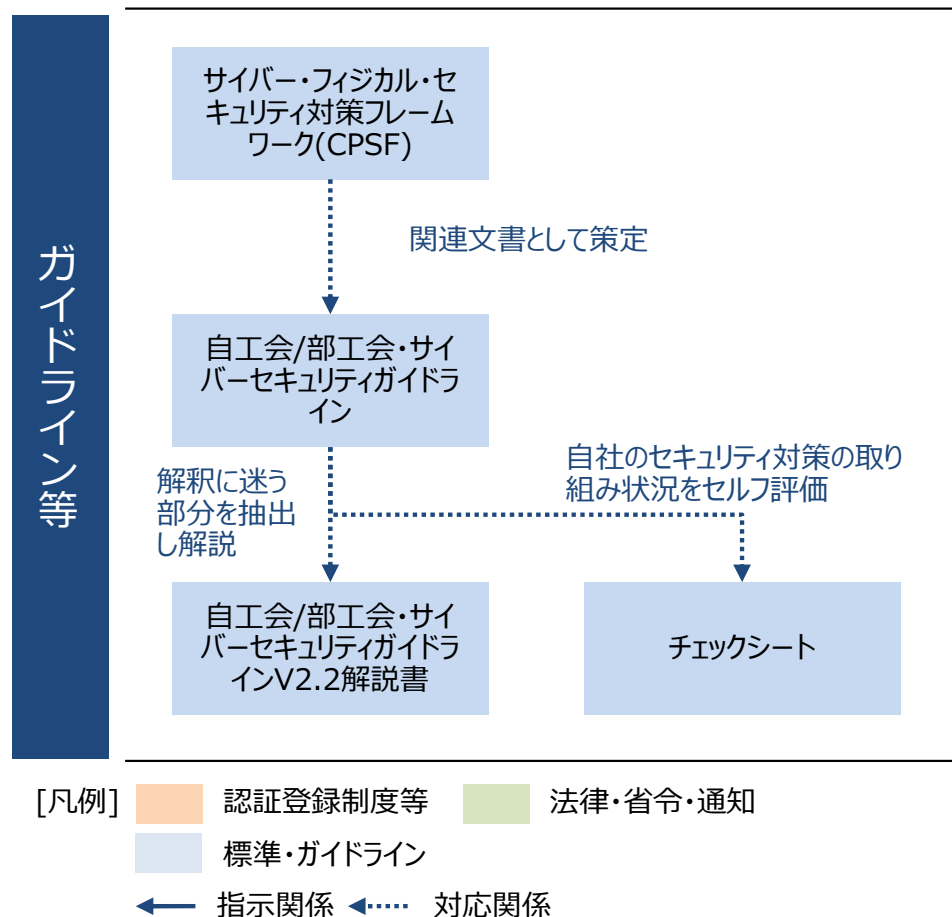
コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	○			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	3/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	○	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							20/22

- 人的管理策や物理的管理策、技術的管理策において具体的な記載がみられた。特に、人的管理策において具体的な政府機関等特有の記載がみられた。

項目	記載粒度
主体 (who)	<人的管理策> • <u>教育の対象を示す。</u> ✓ 職員[情報セキュリティ関係規程] ✓ 情報セキュリティ対策推進体制、CSIRT ✓ CYMATに属する職員
内容 (what)	<物理的管理策> • <u>物理的な対策</u>を例示。 ✓ 施錠可能な扉、間仕切り等の施設の整備 ✓ 設備の設置 <技術的管理策> • 国民・企業と機関等との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合の<u>実施事項(リスク評価)</u>を示す。 • <u>アクセス制御機能において考慮する事項</u> ✓ 情報システムの特性 ✓ 情報システムが取り扱う情報の格付及び取扱制限
頻度 (when)	(頻度に関する具体的な記載なし)
場所 (where)	(場所に関する具体的な記載なし)

- 本ガイドラインでは、自動車産業固有のサイバーセキュリティリスクを考慮した、向こう3年の対策フレームワークや業界共通の自己評価基準を明示。

位置づけ/参照関係の分析



[参考] 日本自動車工業会「自動車産業サイバーセキュリティガイドライン」等
(https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html)

目的/想定読者

項目	目的	想定読者
自工会/部工会・サイバーセキュリティガイドライン	自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、<u>向こう3年の対策フレームワークや業界共通の自己評価基準を明示</u>することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的とする。	- 自動車産業に関係する全ての会社を対象 - 主に以下の方々を対象 CISO(最高情報セキュリティ責任者)・リスク管理部門・監査部門・セキュリティ対応部門・情報システムの開発/運用部門・データマネジメント部門・サプライチェーンの管理責任を負う購買や調達部門・その他のセキュリティに関わる部門(人事・法務・総務)
自工会/部工会・サイバーセキュリティガイドライン解説書	本解説書は、自工会/部工会・サイバーセキュリティガイドライン V2.1 の用語や要求事項、達成基準などに対し、<u>解釈に迷う部分を抽出し解説</u>を行ったもの	セキュリティ部門に所属する方、及び関係部門の方を対象とする
チェックシート	自社のセキュリティ対策の取り組み状況を<u>セルフ評価し、対策レベルの効率的な点検</u>を行う目的で作成	-

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

自工会/部工会・サイバーセキュリティガイドライン(Lv.1)
記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 本ガイドラインのレベル1では、検知、復旧、対応において一部網羅されていない要件がみられた。
- 本ガイドラインのレベル1では、自動車業界として最低限実装すべき項目を記載している。統制や識別、防御の要件を特に重視していると考えられる。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	6/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	○			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	-	
	ポリシー	○		検知	継続的モニタリング	-	0/2
	監督	○			有害イベントの分析	-	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	○	2/4
識別	資産管理	○	3/3		インシデント分析	○	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							16/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

自工会/部工会・サイバーセキュリティガイドライン(Lv.2)

記載範囲

A-1.体系内の位置づけ

A-2.体系間の位置づけ

B-1.記載範囲

B-2.記載粒度

HITACHI
Inspire the Next

- 本ガイドラインのレベル2では、レベル1では網羅されていなかった要件がみられた。
- レベル1+レベル2の合算では、20/22個が網羅されている。〔「インシデント対応の方向とコミュニケーション」及びインシデント復旧のコミュニケーションを除く。〕

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	4/6	防御 (続き)	データセキュリティ	○	5/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	○			技術インフラのレジリエンス	○	
	ポリシー	○		検知	継続的モニタリング	○	2/2
	監督	-			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	-	1/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	○	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							16/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

自工会/部工会・サイバーセキュリティガイドライン(Lv.3)
記載範囲

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 本ガイドラインのレベル3では、網羅されている統制に係る要件は少なかった。ただし、レベル3はレベル1及びレベル2を満たした企業が取得するため、必ずしもレベル3において網羅されている要件が少ないことが問題となるわけではない点に留意いただきたい。レベル1～レベル3の合算では、20/22個が網羅されている。

コア	カテゴリ	有無	小計	コア	カテゴリ	有無	小計
統制	組織的文脈	○	2/6	防御 (続き)	データセキュリティ	○	4/5
	リスクマネジメント戦略	-			プラットフォームセキュリティ	○	
	役割/責任/権限	-			技術インフラのレジリエンス	-	
	ポリシー	-		検知	継続的モニタリング	○	2/2
	監督	-			有害イベントの分析	○	
	サイバーセキュリティサプライ チェーンリスクマネジメント	○		対応	インシデントマネジメント	-	0/4
識別	資産管理	○	3/3		インシデント分析	-	
	リスクアセスメント	○			インシデント対応の方向とコミュ ニケーション	-	
	改善	○			インシデント軽減	-	
防御	アイデンティティ管理とアクセス 制御	○	-	復旧	インシデント復旧計画の実行	○	1/2
	意識向上及びトレーニング	○			インシデント復旧のコミュニケー ション	-	
合計							12/22

2. 国内のガイドライン及び基準に関する記載粒度、位置づけ、参照関係、関係性等の整理

自工会/部工会・サイバーセキュリティガイドライン(Lv.1) 記載粒度

A-1.体系内の位置づけ
A-2.体系間の位置づけ
B-1.記載範囲
B-2.記載粒度

- 自工会のガイドラインは、ISO/IEC 27001と比較して、管理する項目や実施頻度、実施対象が明示されている点でより具体性がある。

項目	記載粒度	項目	記載粒度
頻度 (when)	<組織的管理策> - 資産(情報)及び資産(機器)の<u>管理ルール</u>の点検頻度(1回以上/年)を規定。 - 資産(情報)及び資産(機器)の<u>一覧表</u>の点検頻度(1回以上/年)を規定。 - 管理ルールにおいて、資産(情報)の<u>保管期限</u>を明記するよう規定。 <人的管理策> <u>教育のタイミング</u>(新規受け入れ時、かつ、1回/年以上)を規定。 <物理的管理策> <u>入退場記録のログ</u>の保管期限や情報の保管期限を規定 <技術的管理策> <u>認証ログのモニタリング頻度</u>(1回/月以上)を規定。	主体 (who)	<組織的管理策> <u>管理ルール</u>において、<u>資産(情報)及び資産(機器)の対象情報、管理者、部署名、開示先、連絡先</u>を明記するよう規定 <人的管理策> <u>教育の対象者</u>(役員、従業員、社外要員(派遣社員等)、<u>電子メールの利用者</u>)を規定 <技術的管理策> <u>パスワードに関するルールの周知対象</u>(役員、従業員、派遣社員、<u>受入出向者</u>)を規定
場所 (where)	<組織的管理策> <u>管理ルール</u>において<u>資産(情報)の保管場所や資産(機器)の設置場所</u>を明記するよう規定。 <物理的管理策> <u>施錠が出来ないエリアにサーバーが設置されている場合の対応策</u>(設置サーバーを専用ラックに入れて施錠)を規定	内容 (what)	<組織的管理策> <u>資産(資産)の対象情報及び資産(機器)のバージョン情報、OS、ソフトウェア</u>を規定 <人的管理策> <u>教育の内容</u>(電子メールのマルウェア感染、インターネットへの接続、<u>機密区分に応じた情報の取り扱い</u>)を規定。 - 教育の方法(教育資料配布・掲示、e ラーニング、集合教育等による教育)を規定。 <物理的管理策> <u>入退場記録の内容</u>(入退場日時、入場者(氏名、所属、連絡先など)、<u>入場目的、承認者</u>)を規定。 <技術的管理策> <u>多要素認証の認証方法</u>(知識、所持、生体のいずれか2つ)を規定 <u>認証ログの対象</u>(パソコン、サーバーの認証ログ、<u>重要システムのデータベースアクセスログ</u>)を規定



Hitachi Social Innovation is
POWERING GOOD

■別紙2_制度基準ガイドラインの定義

No	区分	定義
1	制度	以下のようなものを含む。 - 法令：行政手続法に定めのある通り、法律、法律に基づく命令(政令、省令、規則、告示等)、条例及び地方公共団体の執行機関の規則を含む。 - その他の制度：「法令」の規定等に基づき運用される制度(例：適合性評価制度)を含む。
2	基準	法令またはその規定事項に基づき運用される制度において、審査基準、処分基準、行政指導指針(行政手続法)、その他の評価基準として用いられているものを含む。
3	ガイドライン	関係者らが取り組むことが望ましいとされる指針や、基準となる目安などを示したものであり、以下のようなものを含む。 - 関係府省等、行政機関が自ら提示するもののほか、行政機関による指導など深い関与の下で、民間の業界団体等が提示するもの - 「ガイドライン」の名称が付されているものに加えて、ガイドラインとほぼ同様の趣旨で「指針」、「考え方」等の名を冠するもの

■別紙2「調査項目A」制度/基準/ガイドラインの関係性(業界横断)

No.	区分	制度	基準	ガイドライン
1	サイバーセキュリティ経営ガイドライン関連			サイバーセキュリティ経営ガイドライン Ver3.0 付録C サイバーセキュリティインシデントに備えるための参考情報 付録F サイバーセキュリティ体制構築・人材確保の手引き 第2.0版 サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集
2	中小企業の情報セキュリティ対策ガイドライン関連	SECURITY ACTION	付録1:情報セキュリティ5か条 付録2:情報セキュリティ基本方針（サンプル） 付録3:5分でできる！情報セキュリティ自社診断	中小企業の情報セキュリティ対策ガイドライン 付録1～8
3	情報セキュリティ管理基準関連			情報セキュリティ管理基準 個別管理基準(監査項目)策定ガイドライン 情報セキュリティ監査基準 実施基準ガイドライン 報告基準ガイドライン
4	ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル関連	ソフトウェア製品等の脆弱性関連情報に関する取扱い規程(経産省告示) 受付機関及び調整機関を定める告示(経産省告示) 情報セキュリティ早期警戒パートナーシップガイドライン		ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル ウェブサイト構築事業者のための脆弱性対応ガイド ウェブサイト運営者のための脆弱性対応ガイド セキュリティ担当者のための脆弱性対応ガイド 付録1：共通脆弱性評価システムCVSS v3について
5	ECサイト構築・運用セキュリティガイドライン関連			ECサイト構築・運用セキュリティガイドライン 付録1. 被害を受けた ECサイトからの生の声一覧 付録2. 自社構築サイト（中小企業）50 社の脆弱性診断結果 付録3. 契約関係書類のひな形 付録4. 構築時チェックリスト 付録5. 運用時チェックリスト
6	テレワークセキュリティガイドライン関連			テレワークセキュリティガイドライン 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト） 従業員向けハンドブック 緊急時対応カード 設定解説資料
7	CSMS認証基準関連	CSMS適合性評価制度	CSMS認証基準(IEC 62443 2-1)	CSMSユーザーズガイド
8	制御システムのセキュリティリスク分析ガイド関連			制御システムのセキュリティリスク分析ガイド ガイド別冊:制御システムに対するリスク分析の実施例 補足資料:制御システム関連のサイバーインシデント事例 早分かり 活用の手引き
9	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン関連			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) 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 工場セキュリティガイドライン 別冊：スマート化を進める上でのポイント
10	ISMSクラウドセキュリティ認証に関する要求事項関連	ISMSクラウドセキュリティ認証制度 ISMS適合性評価制度		ISO/IEC 27017(ISMSクラウドセキュリティ認証の認証基準) ISO/IEC 27001 ISO/IEC 27002
11	クラウドサービス利用のための情報セキュリティマネジメントガイドライン関連	クラウドセキュリティ・マーク	基本言明要件	クラウドサービス利用のための情報セキュリティマネジメントガイドライン
12	クラウドを利用したシステム運用に関するガイダンス関連			サイバーセキュリティ戦略（令和3年9月28日閣議決定） クラウドを利用したシステム運用に関するガイダンス(別紙) クラウドを利用したシステム運用に関するガイダンス(別紙)
13	情報セキュリティサービス基準関連	情報セキュリティサービス審査登録制度		情報セキュリティサービス基準 情報セキュリティサービスに関する審査登録機関基準 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示

No.	区分	制度	基準	ガイドライン
14	CC/CEM:2022 /IT製品の調達におけるセキュリティ要件リスト関連	ITセキュリティ評価及び認証制度		パート1:概説と一般モデル パート2:セキュリティ機能コンポーネント パート3:セキュリティ保証コンポーネント パート4:評価方法及び評価アクティビティの仕様のための枠組み パート5:セキュリティ要件の定義済みパッケージ 評価方法 <IT製品の調達におけるセキュリティ要件リスト> デジタル複合機（MFP） ファイアウォール 不正侵入検知/防止システム（IDS/IPS） OS（サーバOSに限る） データベース管理システム（DBMS） 暗号化USBメモリ ルータ／レイヤ3スイッチ ドライブ全体暗号化システム モバイル端末管理システム 仮想プライベートネットワーク（VPN）ゲートウェイ <ガイドブック> IT製品の調達におけるセキュリティ要件リスト活用ガイドブック
15	セキュリティ要件適合評価及びラベリング制度(JC-STAR)関連	セキュリティ要件適合評価及びラベリング制度(JC-STAR)	☆1セキュリティ要件・適合基準	☆1セキュリティ評価手順
16	電気通信事業法に基づく端末機器の基準認証に関するガイドライン関連	電気通信事業法 技術基準適合認定 設計認証 技術基準適合自己確認	端末設備等規則 端末機器の技術基準適合認定等に関する規則	電気通信事業法に基づく端末機器の基準認証に関するガイドライン
17	IoTセキュリティガイドライン関連			IoTセキュリティガイドライン
18	サイバー・フィジカル・セキュリティ対策フレームワーク関連	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)		<産業サイバーセキュリティ研究会 WG1> ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 小売電気事業者のためのサイバーセキュリティ対策ガイドライン スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン 自工会／部工会サイバーセキュリティガイドライン 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ実施手順について <産業サイバーセキュリティ研究会 WG1 分野横断SWG> IoTセキュリティ・セーフティ・フレームワーク 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) ソフトウェア管理に向けたSBOMの導入に関する手引

■別紙2_調査項目A)制度/基準/ガイドラインの関係性(業界個別)

No.	区分	制度	基準	ガイドライン
1	重要インフラのサイバーセキュリティに係る安全基準等策定指針関連	サイバーセキュリティ基本法 サイバーセキュリティ戦略 重要インフラに係る行動計画		重要インフラのサイバーセキュリティに係る安全基準等策定指針 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書 ガイダンス
2	情報通信ネットワーク安全・信頼性基準関連	電気通信事業法 事業用電気通信設備規則		情報通信ネットワーク安全・信頼性基準 情報通信ネットワーク安全・信頼性基準 解説
3	電気通信分野におけるサイバーセキュリティに係る安全基準関連			放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針(第4版)対策編 電気通信分野におけるサイバーセキュリティに係る安全基準
4	ケーブルテレビにおけるサイバーセキュリティに係る安全基準関連	放送法施行規則		重要インフラのサイバーセキュリティに係る安全基準等策定指針 ケーブルテレビにおけるサイバーセキュリティに係る安全基準(第1版) 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
5	金融分野におけるサイバーセキュリティに関するガイドライン関連	各業法		各監督指針・事務ガイドライン(監督指針等) 金融分野におけるサイバーセキュリティに関するガイドライン
6				重要インフラのサイバーセキュリティに係る安全基準等策定指針 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるセキュリティポリシー策定のための手引書 金融機関等におけるコンティンジェンシープラン策定のための手引書
7	航空分野における情報セキュリティ確保に係る安全ガイドライン関連			重要インフラのサイバーセキュリティに係る安全基準等策定指針 航空分野における情報セキュリティ確保に係る安全ガイドライン
8	空港分野における情報セキュリティ確保に係る安全ガイドライン関連			重要インフラのサイバーセキュリティに係る安全基準等策定指針 空港分野における情報セキュリティ確保に係る安全ガイドライン
9	鉄道分野における情報セキュリティ確保に係る安全ガイドライン関連			重要インフラのサイバーセキュリティに係る安全基準等策定指針 鉄道分野における情報セキュリティ確保に係る安全ガイドライン
10	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン関連	電気設備に関する技術基準を定める省令	電気設備の技術基準の解釈	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン 電気事業法施行規則第50条第3項第9号の解釈適用に当たったの考え方（内規）
11	都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説関連	ガス事業法施行規則		都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
12	地方公共団体における情報セキュリティポリシーに関するガイドライン関連	地方自治法 総務省大臣指令		地方公共団体における情報セキュリティポリシーに関するガイドライン 地方公共団体における情報セキュリティ監査に関するガイドライン
13	医療情報システムの安全管理に関するガイドライン	e-文書法 e-文書法省令 個人情報保護法 医療法施行規則 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則 厚生労働省通知		医療情報システムの安全管理に関するガイドライン チェックリスト(医療機関/薬局) 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
14	水道分野における情報セキュリティガイドライン関連	水道施設の技術的基準を定める省令		重要インフラのサイバーセキュリティに係る安全基準等策定指針 水道分野における情報セキュリティガイドライン
15	物流分野における情報セキュリティ確保に係る安全ガイドライン関連			重要インフラのサイバーセキュリティに係る安全基準等策定指針 物流分野における情報セキュリティ確保に係る安全ガイドライン(貨物自動車運送/倉庫)
16	クレジットカード・セキュリティガイドライン関連	割賦販売法 割賦販売法(後払分野)に基づく監督の基本方針		クレジットカード・セキュリティガイドライン
17	石油化学分野における情報セキュリティ確保に係る安全基準/石油分野における情報セキュリティ確保に係る安全ガイドライン 関連	認定事業者制度		重要インフラのサイバーセキュリティに係る安全基準等策定指針 石油化学分野における情報セキュリティ確保に係る安全基準 石油分野における情報セキュリティ確保に係る安全ガイドライン
18	装備品等及び役務の調達における情報セキュリティ基準関連	装備品等及び役務の調達における情報セキュリティの確保に関する特約条項 防衛省通達	装備品等及び役務の調達における情報セキュリティ基準	装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ実施手順について
19	民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン関連			サイバー・フィジカル・セキュリティ対策フレームワーク 制御システムのセキュリティリスク分析ガイド 民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン

No.	区分	制度	基準	ガイドライン
20	電力制御システムセキュリティガイドライン/スマートメーターシステムセキュリティガイドライン関連	電気事業法 発電用水力設備、発電用火力設備、電気設備、発電用風力設備の技術基準を定める省令	技術基準の解釈	電力制御システムセキュリティガイドライン スマートメーターシステムセキュリティガイドライン
21	ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン関連			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) ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 別紙 ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編：空調システム) ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編：空調システム) 別紙
22	スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン関連			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) スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン
23	政府機関等のサイバーセキュリティ対策のための統一基準関連	政府機関等のサイバーセキュリティ対策のための統一規範 IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ	政府機関等のサイバーセキュリティ対策のための統一基準	政府機関等の対策基準策定のためのガイドライン 対策推進計画策定マニュアル 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書 政府機関等における情報システム運用継続計画ガイドライン スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書
24	自工会/部工会・サイバーセキュリティガイドライン関連			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) 自工会/部工会・サイバーセキュリティガイドライン 自工会/部工会・サイバーセキュリティガイドラインV2.2解説書 チェックシート

			-----▶ 構成要素を考慮 ―――▶ 構成要素に加えて具体的な内容を考慮		
No.	大区分	小区分	基となる文書	個別文書	個別文書を支援する文書
1	経営		サイバー・フィジカル・セキュリティ対策フレームワーク	サイバーセキュリティ経営ガイドライン	
2					付録C サイバーセキュリティインシデントに備えるための参考情報
3					付録F サイバーセキュリティ体制構築・人材確保の手引き 第2.0版
4					サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集
5				中小企業の情報セキュリティ対策ガイドライン	
6					付録1：情報セキュリティ5か条
7					付録2：情報セキュリティ基本方針
8					付録3：5分でできる！情報セキュリティ自社診断
9					付録4：情報セキュリティハンドブック
10					付録5：情報セキュリティ関連規程
11					付録6：中小企業のためのクラウドサービス安全利用の手引き
12					付録7：リスク分析シート
13					付録7：リスク分析シート
14					付録8：中小企業のためのセキュリティインシデント対応の手引き
15	組織	CPSF関連			
16					
17				工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	工場セキュリティガイドライン 別冊：スマート化を進める上でのポイント
18				ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	
19					ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン別紙
20					ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編:空調システム)
21					ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン(個別編:空調システム) 別紙
22				小売電気事業者のためのサイバーセキュリティ対策ガイドライン	
23				スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン	
24				民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン	
25					【添付資料1】対策要求事項チェックリスト
26					【添付資料2】NIST CSFと宇宙システム特有の対策との対応関係

No.	大区分	小区分	基となる文書	個別文書	個別文書を支援する文書	
27				装備品等及び役務の調達における情報セキュリティ基準	装備品等及び役務の調達における情報セキュリティの確保に関する情報セキュリティ実施手順について	
28						
29			自工会/部工会・サイバーセキュリティガイドライン	自工会/部工会・サイバーセキュリティガイドラインV2.2解説書		
30						
31					チェックシート	
32				IoTセキュリティ・セーフティ・フレームワーク	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	
33						
34				IoTセキュリティ・セーフティ・フレームワークVersion 1.0 適用手順書		
35				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)	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	
36						
37				ソフトウェア管理に向けたSBOMの導入に関する手引	「ソフトウェア管理に向けたSBOMの導入に関する手引」付録 チェックリスト	
38						
39						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
40			ISO 27001関連		情報セキュリティ管理基準	情報セキュリティ管理基準
41						
42				個別管理基準(監査項目)策定ガイドライン		
43				ISMS認証基準	ユーザーズガイド	
44						
45				ISMSクラウドセキュリティ認証基準	クラウドを利用したシステム運用に関するガイダンス(別紙)	
46						
47				基本言明要件	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	
48						
49				クラウドを利用したシステム運用に関するガイダンス	クラウドを利用したシステム運用に関するガイダンス(別紙)	
50						
51				情報セキュリティサービス基準	情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示	
52						
53		IEC 62443関連			CSMS認証基準	

No.	大区分	小区分	基となる文書	個別文書	個別文書を支援する文書
54		安全基準等策定指針系			CSMSユーザーズガイド
55				制御システムのセキュリティリスク分析ガイド	
56					ガイド別冊:制御システムに対するリスク分析の実施例
57					補足資料:制御システム関連のサイバーインシデント事例
58					早分かり 活用の手引き
59				IoTセキュリティガイドライン	
60				重要インフラのサイバーセキュリティに係る安全基準等策定指針	
61					重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
62				情報通信ネットワーク安全・信頼性基準	
63					情報通信ネットワーク安全・信頼性基準 解説
64				電気通信分野におけるサイバーセキュリティに係る安全基準	
65				ケーブルテレビにおけるサイバーセキュリティに係る安全基準(第1版)	
66				金融分野におけるサイバーセキュリティに関するガイドライン	
67				金融機関等コンピュータシステムの安全対策基準・解説書	
68					金融機関等におけるセキュリティポリシー策定のための手引書
69					金融機関等におけるコンティンジェンシープラン策定のための手引書
70				航空分野における情報セキュリティ確保に係る安全ガイドライン	
71				空港分野における情報セキュリティ確保に係る安全ガイドライン	
72				鉄道分野における情報セキュリティ確保に係る安全ガイドライン	
73				自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン	
74				電力制御システムセキュリティガイドライン	
75					電気事業法施行規則第50条第3項第9号の解釈適用に当たっての考え方（内規）
76				都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説	
77				地方公共団体における情報セキュリティポリシーに関するガイドライン	
78				医療情報システムの安全管理に関するガイドライン	
79					チェックリスト(医療機関/薬局)
80				医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	

No.	大区分	小区分	基となる文書	個別文書	個別文書を支援する文書
81				→ 水運分野における情報セキュリティガイドライン	
82				→ 物流分野における情報セキュリティ確保に係る安全ガイドライン(貨物自動車運送)	
83				→ 物流分野における情報セキュリティ確保に係る安全ガイドライン(倉庫)	
84				→ 物流分野における情報セキュリティ確保に係る安全ガイドライン(船舶)	
85				→ クレジットカード・セキュリティガイドライン	
86				→ 石油化学分野における情報セキュリティ確保に係る安全基準	
87				→ 石油分野における情報セキュリティ確保に係る安全ガイドライン	
88				→ 石油分野における情報セキュリティ確保に係る安全ガイドライン	
89					
90		政府統一基準系		→ 政府機関等のサイバーセキュリティ対策のための統一基準	
91				→ 政府機関等の対策基準策定のためのガイドライン	
92					→ 対策推進計画策定マニュアル
93					→ 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル
94					→ 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリ
95					→ 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕
96					→ 政府機関等における情報システム運用継続計画ガイドライン
97					→ スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書
98					
99		その他		→ ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル	
100					→ 付録1：共通脆弱性評価システムCVSS v3について
101					→ ウェブサイト構築事業者のための脆弱性対応ガイド
102					→ ウェブサイト運営者のための脆弱性対応ガイド
103					→ セキュリティ担当者のための脆弱性対応ガイド
104				→ ECサイト構築・運用セキュリティガイドライン	
105					→ 付録1, 被害を受けた ECサイトからの生の声一覧
106					→ 付録2, 自社構築サイト（中小企業）50 社の脆弱性診断結果
107					→ 付録3, 契約関係書類のひな形

No.	大区分	小区分	基となる文書	個別文書	個別文書を支援する文書
108					付録4. 構築時チェックリスト
109					付録5. 運用時チェックリスト
110					中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）
111					
112					
113					
114					
115					
116	製品・サービス	ISO/IEC 15408 系			IT製品の調達におけるセキュリティ要件リスト活用ガイドブック
117					
118					
119					
120					
121					
122					
123					
124		JC STAR系			IT製品の調達におけるセキュリティ要件リスト
125					
126					
127					
128					
129					
130		端末設備規則系			電気通信事業法に基づく端末機器の基準認証に関するガイドライン
131					
132					
133					
134		サイバーインフラ検討会系		(仮称)サイバーインフラ検討会 要求事項	

No.	大区分	小区分	基となる文書		個別文書	個別文書を支援する文書	
135						今後、更新予定	
136							

「サプライチェーン強化に向けたセキュリティ対策評価制度 に関するサブワーキンググループ」 中間とりまとめ（案）

2025年4月

サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ

事務局

目次

1. 制度の目的と位置づけ

- 1.1 制度の目的
- 1.2 制度の位置づけ
- 1.3 「サイバーインフラ事業者に求められる役割等の検討会」との役割分担

2. 構築する評価制度

- 2.1 制度の対象とする組織
- 2.2 制度において設ける段階
- 2.3 制度で用いるセキュリティ要求事項・評価基準
- 2.4 制度における評価スキーム
- 2.5 国内外の関連制度等との連携・整合

3. 制度整備に向けた道筋

- 3.1 制度が効果的と想定される業界等
- 3.2 制度の導入促進

4. 今後の検討の進め方及びスケジュール

付録：諸外国における関連する取組



1. 制度の目的と位置づけ

1. 制度の目的と位置づけ

1.1 制度の目的

【現状認識（制度検討の背景）】

- 近年、サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発。その対策として、政府や重要インフラ企業のみならずその取引先に対しても適切なセキュリティ対策を課す必要があるが、複雑なサプライチェーン下で、様々な取引先から様々な要求事項を求められている状況。発注企業にとっては、正しいセキュリティ対策が取引先でなされているか不明確／受注企業にとっては（特に中小企業を中心に）過度な負担につながっている。結果として、サプライチェーン全体のセキュリティ底上げにつながっていない。

【制度趣旨】

- ビジネスサプライチェーン・ITサービスサプライチェーンにおける、取引先へのサイバー攻撃を起因とした情報セキュリティリスク／製品・サービスの提供途絶リスク／取引ネットワークを通じた不正侵入等のリスクに対するセキュリティ対策の成熟度を確認する。
- 2社間の契約における発注企業が、受注側に適切な段階（★）を提示し取得を促す（再委託先は発注者から見た対象にはならない（※））。

（※） 再委託先のセキュリティ対策は、委託先を通じて必要に応じて管理（一部要求項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを盛り込み）

【目指す効果】

- サプライチェーンにおけるリスクを対象にした上で（※）、その中での立ち位置に応じて必要な対策を提示することで、企業の対策決定を容易・適切なものにする。すべてのサプライチェーン企業が対象となるが、特にサプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい。

（※） 本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましいが、リソースに限りのある中小企業を中心にただちにこれを実現できていない企業が一定数存在する。本制度は、包括的なリスク分析に基づき共通して求められる対策を示すもの。将来的には、こうした企業もより自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい。

1. 制度の目的と位置づけ

1.1 制度の目的

- 発注者・受注者双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易・適切となることが期待される。
- また、取引先のセキュリティ対策が適切に実装されることで、発注企業のサプライチェーン・リスクの低減や、経済・社会全体でのサイバーレジリエンスの強化が期待される。

- 自社がどの程度のセキュリティ対策を実施すべきか明確になる。
- 発注企業等に対して、セキュリティ対策に係る説明が容易になる。
- 対策に要する費用や効果の可視化
- セキュリティサービスの標準化による選択肢拡大やコスト低減（中長期）

受注企業への効果



- 取引先に求めるセキュリティ対策の内容や水準の決定や、実施状況の把握が容易・適切になる
- 取引先におけるセキュリティ対策の適切な実装により、サプライチェーンに起因する自社セキュリティリスクの低減

発注企業への効果



- サプライチェーン全体での底上げを通じた経済・社会全体のサイバーレジリエンス※の強化
- サイバー攻撃への備えのある企業等への適切な評価
- セキュリティ製品やサービスの市場拡大・競争力向上（中長期）

社会全体での効果



※サイバーレジリエンス(Cyber resiliency)

サイバー資源を使用する、またはサイバー資源によって実現するシステムに対する不利な状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力 https://csrc.nist.gov/glossary/term/cyber_resiliency

1. 制度の目的と位置づけ

1.2 制度の位置づけ — 対象とするリスクの範囲

- 本制度では、取引先へのサイバー攻撃等を起因とした情報セキュリティリスク（機密性・可用性・完全性への影響）に加えて、製品・サービスの提供途絶リスク（事業継続性への影響）、及び取引ネットワークを通じた不正侵入等リスクを、対象とするサプライチェーンリスクとして想定

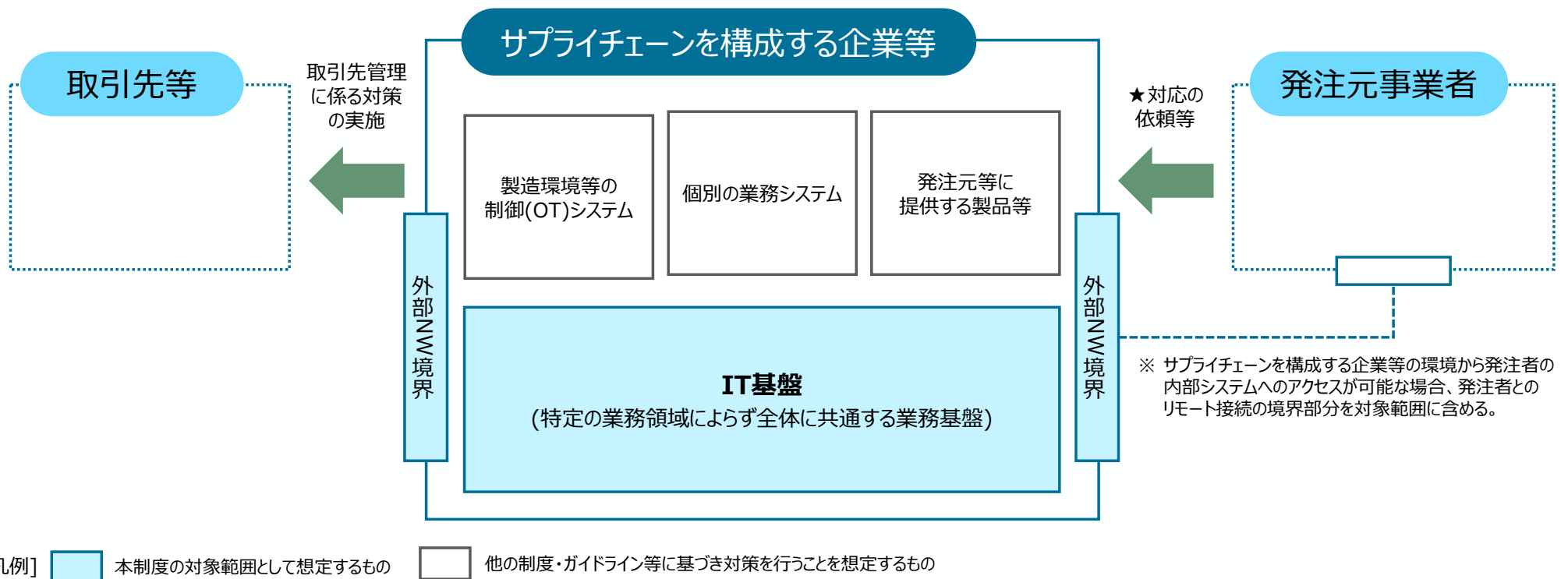
分類	想定するサプライチェーンリスク	インシデント事例	影響を受けるサプライチェーン
自社事業・サービスの提供途絶 事業継続	サプライチェーン企業へのサイバー攻撃等に起因する、調達部品の供給遅延・停止	- 自動車部品メーカー - 半導体事業者	⇒ ビジネスサプライチェーン（物品・役務の調達、業務提携、API連携など（他の類型に含まれるものを除く））
	調達したクラウドサービスへのサイバー攻撃等に起因する、クラウドサービスの停止	クラウド事業者	⇒ ITサービスサプライチェーン（MSP*、クラウドサービス等を含む） * Managed Service Provider
機密情報の漏えい、改ざん データ保護	サプライチェーン企業へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	BPO事業者	⇒ ビジネスサプライチェーン
	マネージドサービス等へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	ITベンダー	⇒ ITサービスサプライチェーン
	調達したクラウドサービスへのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	クラウド事業者	⇒ ITサービスサプライチェーン
取引先等を踏み台とした不正侵入 不正アクセス	サプライチェーン企業の環境を踏み台とした、発注者側システム環境への不正侵入	医療機関	⇒ ビジネスサプライチェーン
	マネージドサービス等の環境を踏み台とした、発注者側システム環境への不正侵入	ITベンダー	⇒ ITサービスサプライチェーン

※ 本制度の対象は、企業体におけるセキュリティ対策であり、組織のガバナンス・取引先管理、自社IT基盤への検知・防御等、組織全体に影響が及ぶ範囲を対象としている。ソフトウェア開発やIoT機器のセキュリティを対象にした評価制度・取組とは目的が異なるため、求められる対策内容や効果も基本的に異なる。

1. 制度の目的と位置づけ

1.2 制度の位置づけ — 制度の対象範囲

- 本制度は、サプライチェーンを構成する企業等のIT基盤（特定の業務領域によらず全体に共通する業務基盤）を対象とする。
[註] 制度の対象とするIT基盤としては、オンプレミス環境で運用されるものに加え、クラウド環境で運用するものも含む。
- 一般的にIT基盤には該当しないと考えられる製造環境等の制御（OT）システム、個別の業務システム、発注元等に提供する製品等については直接の対象とはせず、他の制度・ガイドライン等に基づき対策を行うことを想定する。
- 取引先管理に係る対策については、契約等を通じてサプライチェーンを構成する企業等から取引先等へ適用される。



1. 制度の目的と位置づけ

1.3 「サイバーインフラ事業者求められる役割等の検討会」との役割分担

- 本検討は、サプライチェーン構成企業による自社IT基盤を中心とした自社のセキュリティ対策の向上を通じて、サプライチェーン全体の強靱性（事業継続性、機微情報の保護、取引先等を通じた不正侵入の抑制）の確保を目指すもの。

	サプライチェーン強化に向けた セキュリティ対策評価制度に 関するSWG（本検討）	サイバーインフラ事業者 に求められる役割等の 検討会	両者の関係性 （右図参照）
対象範囲・ 事業者	- ビジネスサプライチェーン （物資・役務の調達等） - ITサービスサプライチェーン （MSP*、クラウドサービス等を含む） に係る事業者	ソフトウェア（クラウド上のもの含む）のサプライチェーン （開発・供給・運用）に係る事業者（＝サイバーインフラ 事業者）	<u>ITサービスサプライチェーンに係る事業者 は、双方の対象範囲に含まれる</u>
検討目的・ 内容	<u>サプライチェーン全体でのセキュリティリスクの低減</u>を目的に、 - 発注者（顧客）から受注者に求めるセキュリティ要件（<u>自社 IT基盤等、サプライチェーン企業自身のセキュリティ対策</u>） の整理	<u>ソフトウェアを利用する顧客等の保護</u>を目的に、 <u>ソフトウェアの提供（開発・運用・供給）において、事業者 が果たすべき具体的責務</u>（セキュアバイデザイン・デフォ ルト等）の整理	<u>目的が異なるため、求められる対策内 容や効果も基本的に異なる</u>
アウトプット	サプライチェーン企業の対策評制度（仮称）として、 ★3/4等の段階的評価制度を整備	「サイバーインフラ事業者等の責務に係るガイドライン （仮称）」に基づき、サイバーインフラ事業者による自己 適合宣言を促進	-

* Managed Service Provider

例えば、以下の業務を行うITサービスサプライチェーン構成企業は、顧客からの要請に応じて、双方の対応が必要となる場合がある

- 情報システムの開発及び構築業務・運用業務を受託する場合（自社IT基盤等のセキュリティ対策についてSC対策評価 / 開発・運用するシステムについてガイドラインに基づく対応）
- クラウドサービス事業者(IaaS/PaaS/SaaS)によるサービス提供（自社IT基盤等のセキュリティ対策についてSC対策評価制度/ 提供するクラウドサービスについてガイドラインに基づく対応）



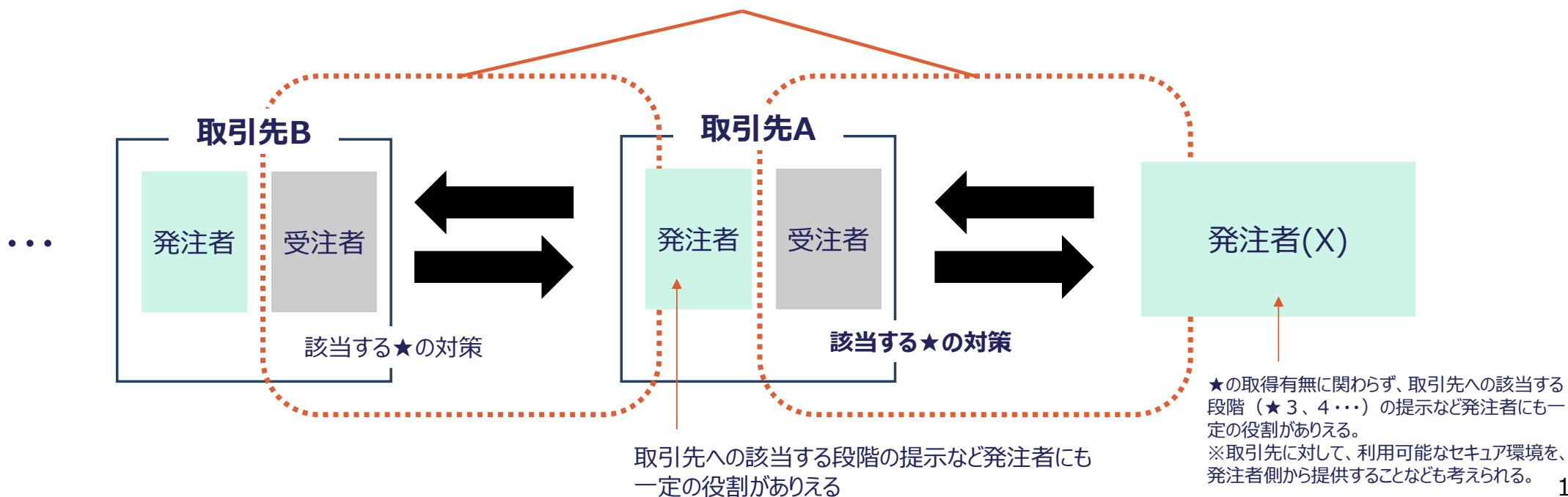
2. 構築する評価制度

2. 構築する評価制度

2.1 制度の対象とする組織

- 本制度で定めるセキュリティ対策の実施主体として想定するのは、サプライチェーン企業（2社間の契約における受注者側）。サプライチェーン企業が対策を実施するに当たって、発注者による協力が必要な場合があることから、制度が想定する対象事業者（制度利用者）の範囲は、赤枠囲いとする。なおサプライチェーン企業は、取引によっては発注者にもなりえる。
- 評価取得の申請主体は、自社IT基盤を中心とした自社のセキュリティ対策の向上に責任を有する単位（基本的には法人単位又は企業グループ単位）とする。

制度の対象事業者（制度利用者）の範囲



2. 構築する評価制度

2.2 制度において設ける段階

- 先行する海外制度等の分析を通じて、★3については、一般的なサイバー脅威に対処する水準を目指すものとして規定。
★4は、初期侵入の防御に留まらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合した事業継続を推進している点を改めて明確化。
- ★5については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定（★3・4の精査も踏まえ、今後さらに具体化）。
- 上位の段階はそれ以下の段階で求められる事項を包括するため、例えば、★3を事前に取得していなければ★4を取得できないという関係とはならない。

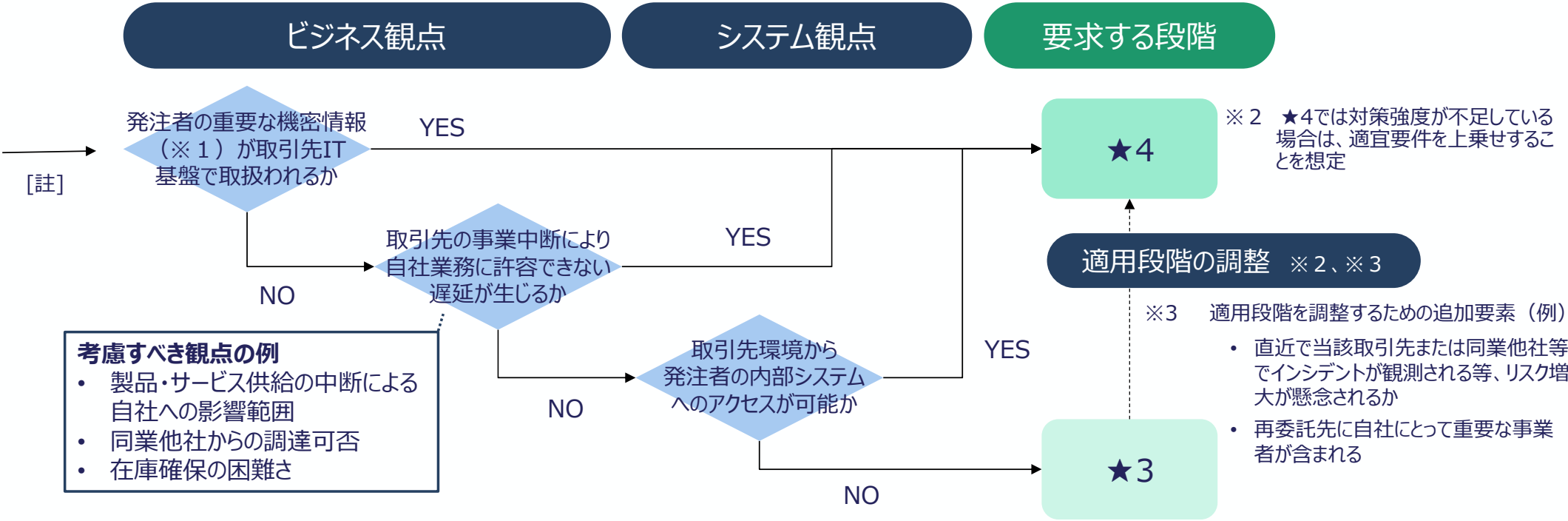
	★3	★4	★5（※）
想定される脅威	広く認知された脆弱性等を悪用する<u>一般的なサイバー攻撃</u>	<u>供給停止</u>等によりサプライチェーンに<u>大きな影響</u>をもたらす企業への攻撃 - 機密情報等、<u>情報漏えい</u>により<u>大きな影響</u>をもたらす資産への攻撃	<u>未知の攻撃</u>も含めた、<u>高度なサイバー攻撃</u>
対策の基本的な考え方	全てのサプライチェーン企業が<u>最低限実装すべきセキュリティ対策</u>として、<u>基礎的な組織的対策とシステム防御策</u>を中心に実施	サプライチェーン企業等が<u>標準的に目指すべきセキュリティ対策</u>として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等<u>包括的な対策</u>を実施	サプライチェーン企業等が<u>到達点として目指すべき対策</u>として、<u>国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策</u>を実施
脅威に対する達成水準（イメージ）	<u>組織内の役割と責任が定義</u>されている。 - 一般的なサイバー脅威への対処を念頭に、自社<u>IT基盤</u>への初期侵入、侵害拡大等への対策が講じられている。 - インシデント発生時に、<u>取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施</u>されている。	- セキュリティ対策が<u>組織的な仕組みに基づいて実施され、継続的に改善</u>している。 <u>取引先のシステムやデータを含む内外</u>への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 <u>事業継続に向けた取組や取引先の対策状況の把握</u>など、自社の位置づけに適合した<u>サプライチェーン強靱化策</u>が講じられている。	- 組織において<u>国際規格等に基づくマネジメントシステム</u>が確立されている。 <u>リスクを適宜適切に把握</u>した上で、インシデントに対して迅速に検知・対応するなど、<u>ベストプラクティスに基づくサイバーレジリエンス確保策</u>が講じられている。 - 取引先等への指導や共同での訓練の実施など、<u>自社サプライチェーン全体のセキュリティ水準向上に資する対策</u>が講じられている。
評価スキーム	自己評価 （※）記入内容については、専門家が問題ないか評価を実施	第三者評価	第三者評価
ベンチマーク （対象企業やリスクが同様であり、対策項目を検討する上で参考）	- 自工会・部工会ガイドLv1 - Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出	- 自工会・部工会ガイドLv2～3 - 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出	- ISO/IEC27001 - 自工会・部工会ガイドLv3 等 （※）ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

2. 構築する評価制度

2.2 制度において設ける段階 — サプライヤー企業への適用の考え方

- ・ サプライヤー企業への適用にあたっては、3つのサプライチェーン・リスクに照らして取引先を★4または★3の段階を割り当てる考え方を、制度の想定する使い方（モデル分岐図）として提示。
- ・ 3つのリスクに照らして★3/4に振り分けたのち、直近のインシデント発生状況等に照らしての段階調整や、対策要件自体の上乗せなどは発注者の判断で実施されることを想定

[註] ★5適用の考え方については、対策基準や評価スキームの具体的なあり方等と同様、2025年度以降に具体化を進める予定。



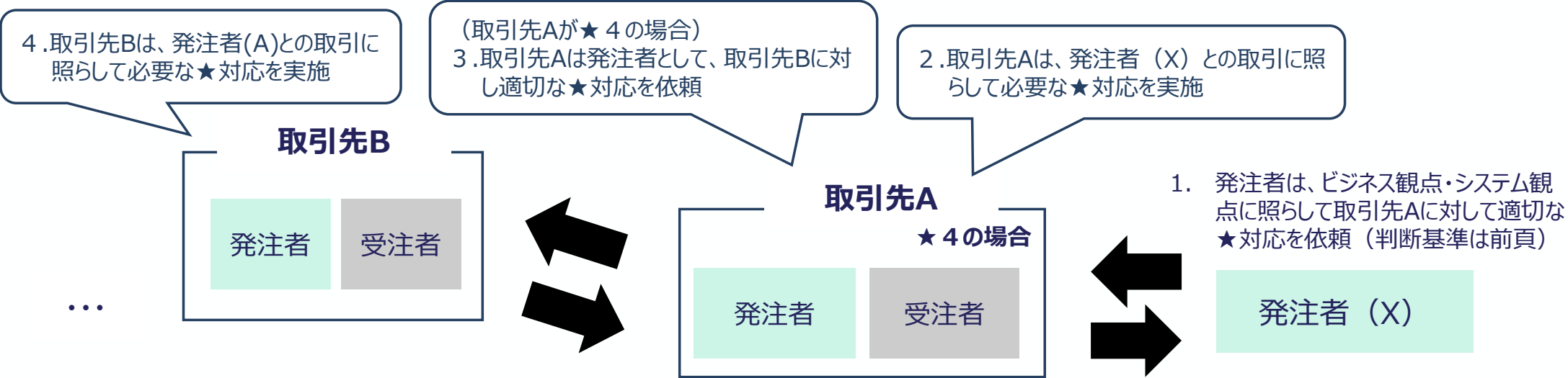
※1 当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

[註] 単発・一過性の調達や、市販品など市場で容易に代替可能な製品・サービスの調達等のうち、重要度が相対的に高いとは言えないものについては、本フローの対象から外すことも考えられる

2. 構築する評価制度

2.2 制度において設ける段階 — 再委託先への適用の考え方

- 再委託先へのサプライチェーン対策評価制度の適用は、元の発注者ではなく直接の取引先（委託先）による判断で実施
- 直接の取引先（委託先）が★4対象の場合、★4要求事項に「重要な取引先におけるセキュリティ対策状況の把握」があるため、重要な機密情報が提供されている再委託先等にも一定の適用が期待される

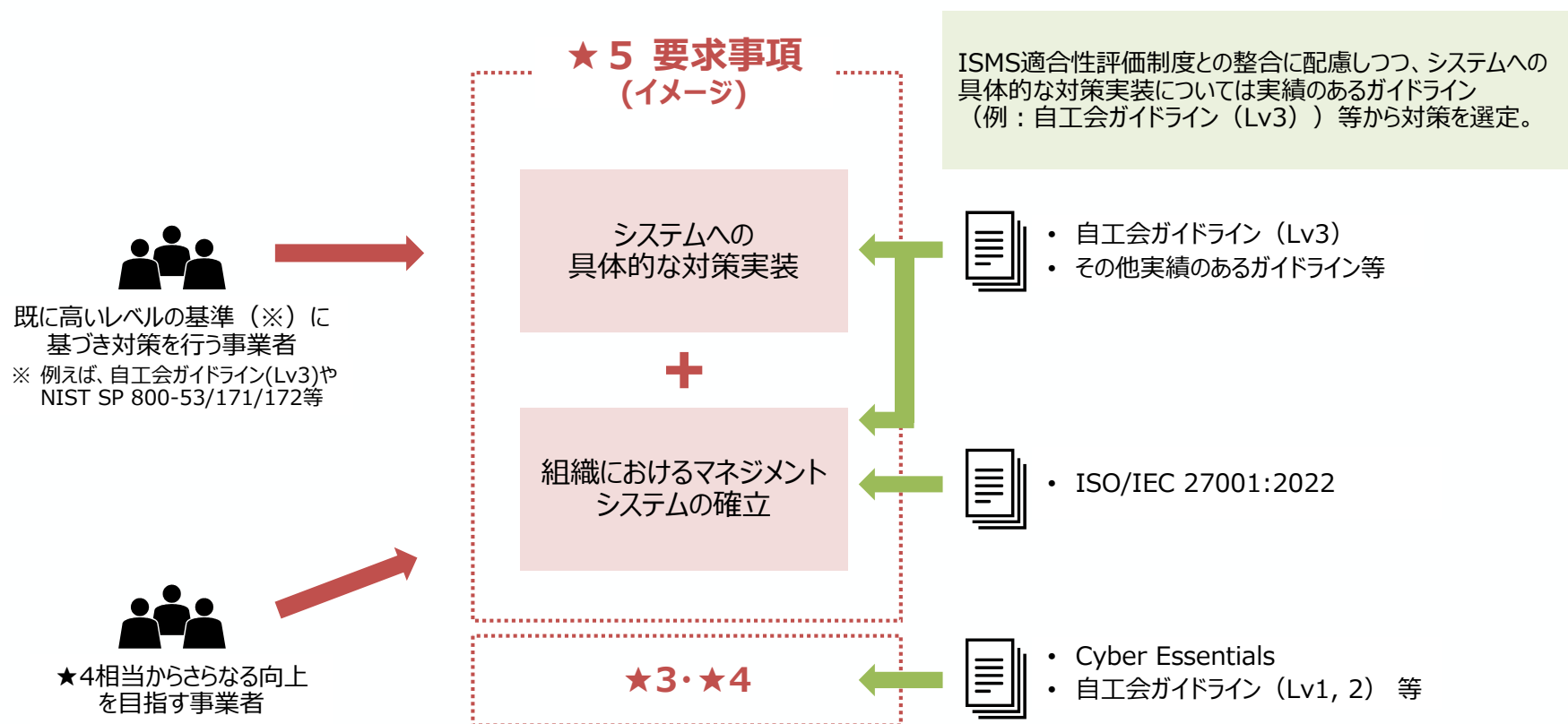


★4 要求事項（案）	★4 評価基準（案）
10 重要な機密情報等を取扱うパートナー企業のセキュリティ対策状況を把握すること。	- 以下に示す条件のいずれか又は複数に該当する子会社又は取引先を対象に、年1回以上の頻度で、以下の例を参考に対策状況を把握すること [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する

2. 構築する評価制度

2.2 制度において設ける段階 — ★5の位置づけ

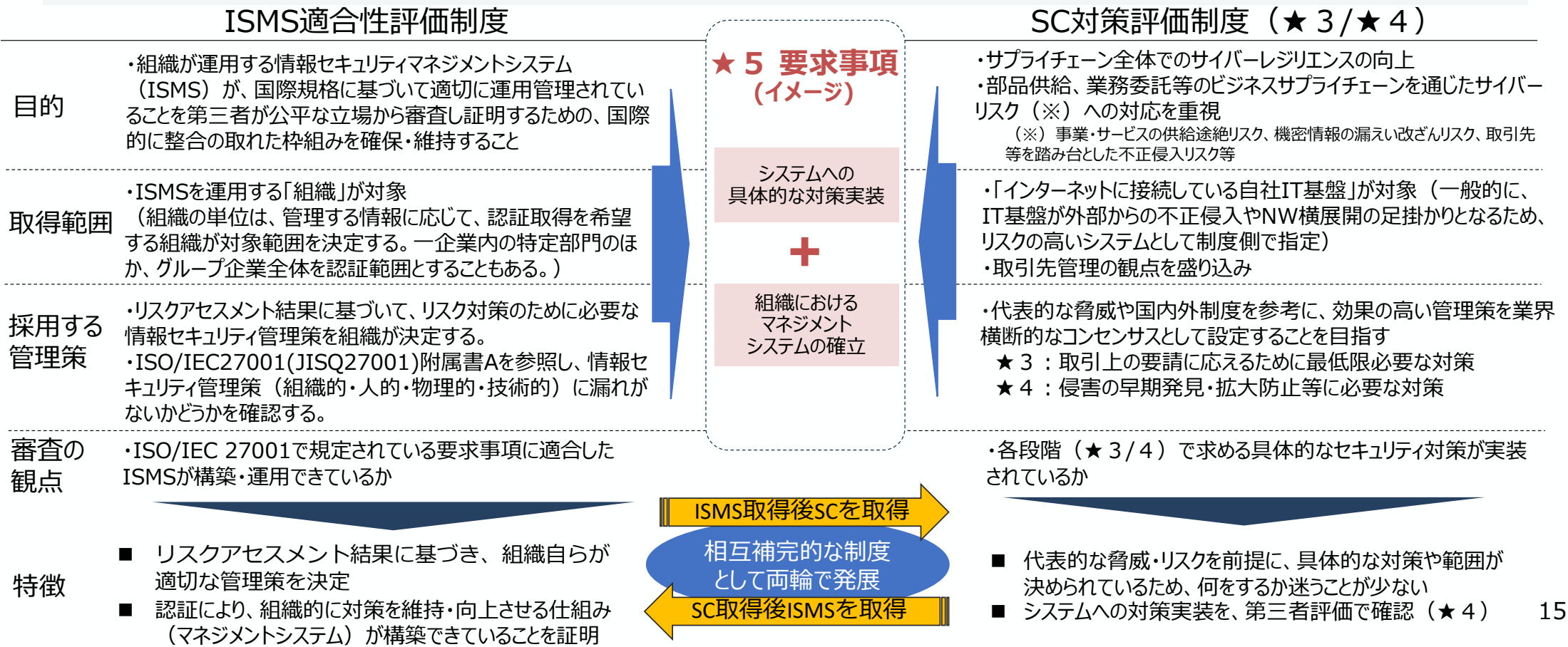
- ★5では、ISMS適合性評価制度との整合に配慮しつつ、システムへの具体的な対策実装については実績のあるガイドライン（例：自工会ガイドライン（Lv3））等から対策を選定することを想定。
- 2025年度以降、対策基準や評価スキームの具体的なあり方等を検討する予定。（再掲）



2. 構築する評価制度

(参考) ISMS適合性評価制度とサプライチェーン対策評価制度の比較

- ・ サプライチェーン対策評価（★ 3 / 4）は、代表的な脅威を参考に効果の高い管理策を抽出先行するベースラインアプローチを採用。
★ 5 段階では、組織におけるリスクベースの改善プロセスを整備した上で、システムへの具体的な対策実装が必要であり、ISMS適合性評価制度との整合に配慮しつつ、2025年度以降具体的なあり方等を検討する予定



2. 構築する評価制度

2.3 制度で用いるセキュリティ要求事項・評価基準 — 各段階のベンチマーク

- 基本的な考え方に基づき、ベンチマークとする関連制度・ガイドラインを設定。★ 3 / ★ 4 の対策事項案を具体化

米 CMMC	英 Cyber Essentials	日本 自工会・部工会ガイドライン
Lv3 Expert 110項目 + 24項目 (SP800-172)	—	Lv3 : 24類型153項目
Lv2 Advanced 110項目 (SP800-171)	—	Lv2 : 24類型124項目
Lv1 Foundational 15項目 (SP800-171より選ばれた対策)	防御、検知に特化した 5 つの分野の対策 + 前提としてIT資産管理	Lv1 : 20類型50項目

★3のベンチマークを設定

- 米CMMC LV1
- 英Cyber Essentials
- 自工会・部工会ガイドライン Lv1

- 対策を抽出、重複を整理
- ★ 3 で対処する脅威等に照らして精査

- ★ 3 対策事項（案）25項目を抽出

★4のベンチマークを設定

- 自工会・部工会ガイドライン LV1～3
- 重要インフラ分野別ガイドライン（金融、航空、電力、通信）
- ISO27001

- 対策を抽出、重複を整理
- ★ 4 で対処する脅威等に照らして精査
- ★ 3 ベンチマーク中★ 3 で除外した事項を考慮

- ★ 4 対策事項（案）44項目を抽出

★5のベンチマーク（候補）

- ISO/IEC 27001:2022
- 自工会・部工会ガイドライン LV3 等

うち11項目は★ 3 と
同一内容

2. 構築する評価制度

2.3 制度で用いるセキュリティ要求事項・評価基準

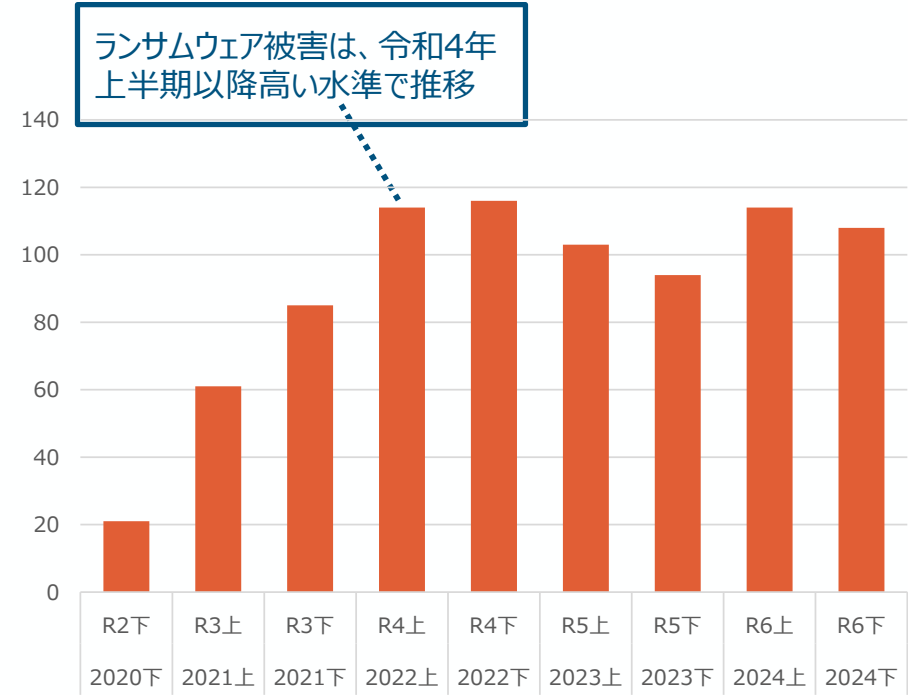
- レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」に資する対策を提案。 ※1 以下は必ずしも全要求を網羅しているわけではない点に留意されたい。
- 詳細は参考資料 1（エクセルシート）を参照されたい。 ※2 参考資料 1 の大分類のうち、ガバナンスの整備、リスクの特定、インシデントへの対応、インシデントからの復旧は「経営の責任」に、取引先管理は「サプライチェーンの防御」に、攻撃等の防御、攻撃等の検知は「IT基盤の防御」に該当

	★3 (Basic)	★4 (Standard)
経営の責任	企業として最低限のリスク管理体制構築 - 自社のセキュリティ担当の明確化 [No.1] - セキュリティ対応方針の策定 [No.3] インシデント発生に備えた対応手順の整備 - インシデント対応手順の作成 [No.25] 自社IT基盤や資産の現状把握 - 情報資産やネットワークの一覧化 [No.7,8] - 取引先等とのネットワーク接続の管理 [No.9]	継続的改善に資するリスク管理体制の構築 - 定期的な見直しの実施 [No.6] - 定期的な経営層への報告、不備の是正等 [No.7] インシデントからの復旧手順等の整備 - 復旧ポイント、復旧時間を満たす手順等の整備[No.44] 脆弱性など最新状況の把握と反映 - 脆弱性管理体制、管理プロセスの明確化 [No.17] - 定期的な見直しの実施「No.6」（再掲）
サプライチェーンの防御	取引先等に課す最低限のルールの明確化 - 接続している外部情報システムの一覧化 [No.5] - 他社との機密情報の取扱い明確化 [No.6]	サプライチェーンにおける対策状況の把握 - 機密情報共有先の一覧化 [No.8] - 重要な取引先等の対策状況把握 [No.10] 取引先等との役割と責任の明確化 - インシデント発生時の他社との役割等の明確化 [No.11]
IT基盤の防御	不正アクセスに対する基礎的な防御 - 基礎的なID管理手続き、アクセス権限の設定 [No.11,12,17] - パスワードの安全な設定及び管理 [No.15,16] - 内外ネットワーク境界の分離・保護 [No.23] 端末やサーバーの基礎的な保護 - ソフトウェアの適時のアップデート適用、不要なソフトウェアの削除 [No.20,21] - 端末等へのマルウェア対策 [No.22]	多層防御による侵入リスクの低減 - 重要な保管データの暗号化 [No.29] - 社内システムにおける適切なネットワーク分離 [No.38] - 社外への不正通信の遮断(出口対策) [No.39] - 情報機器等の状態や挙動の監視・対応 [No.41] 迅速な異常の検知 - ログの収集・定期的な分析の実施 [No.35] - ネットワーク接続やデータ転送の監視 [No.40] - 情報機器等の状態や挙動の監視・対応 [No.41]（再掲） - 監視活動で検知された事象の分析 [No.42]

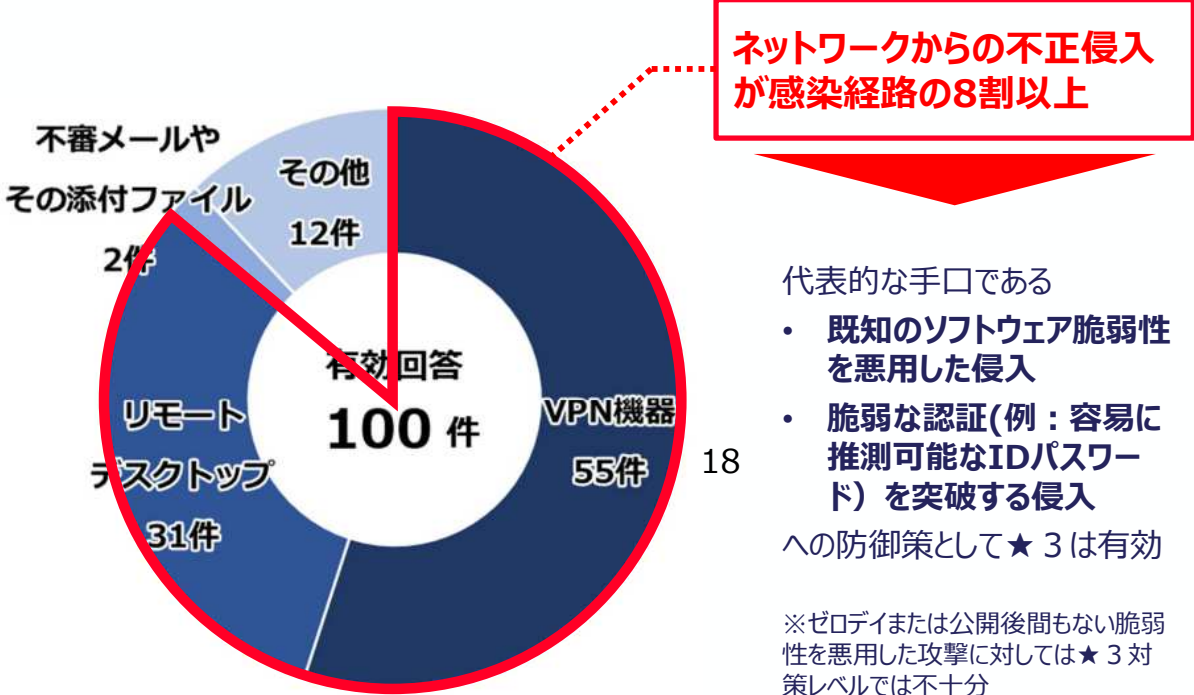
2. 構築する評価制度

2.3 制度で用いるセキュリティ要求事項・評価基準 — ★3 対策による効果

- 業種・企業規模を問わず、昨今多くの被害が出ているランサムウェア感染は、ネットワーク経由が大半を占めている（86%）
- ★3 要求事項の「ネットワークの把握と境界の防護（No.5,23）」、「アイデンティティ・アクセス管理（No.11～17）」、「ソフトウェア脆弱性へのパッチ適用（No.21,22）」を適切に実装することで、ネットワーク経由での代表的なランサムウェア攻撃を緩和できる



ランサムウェア被害の報告件数（推移）

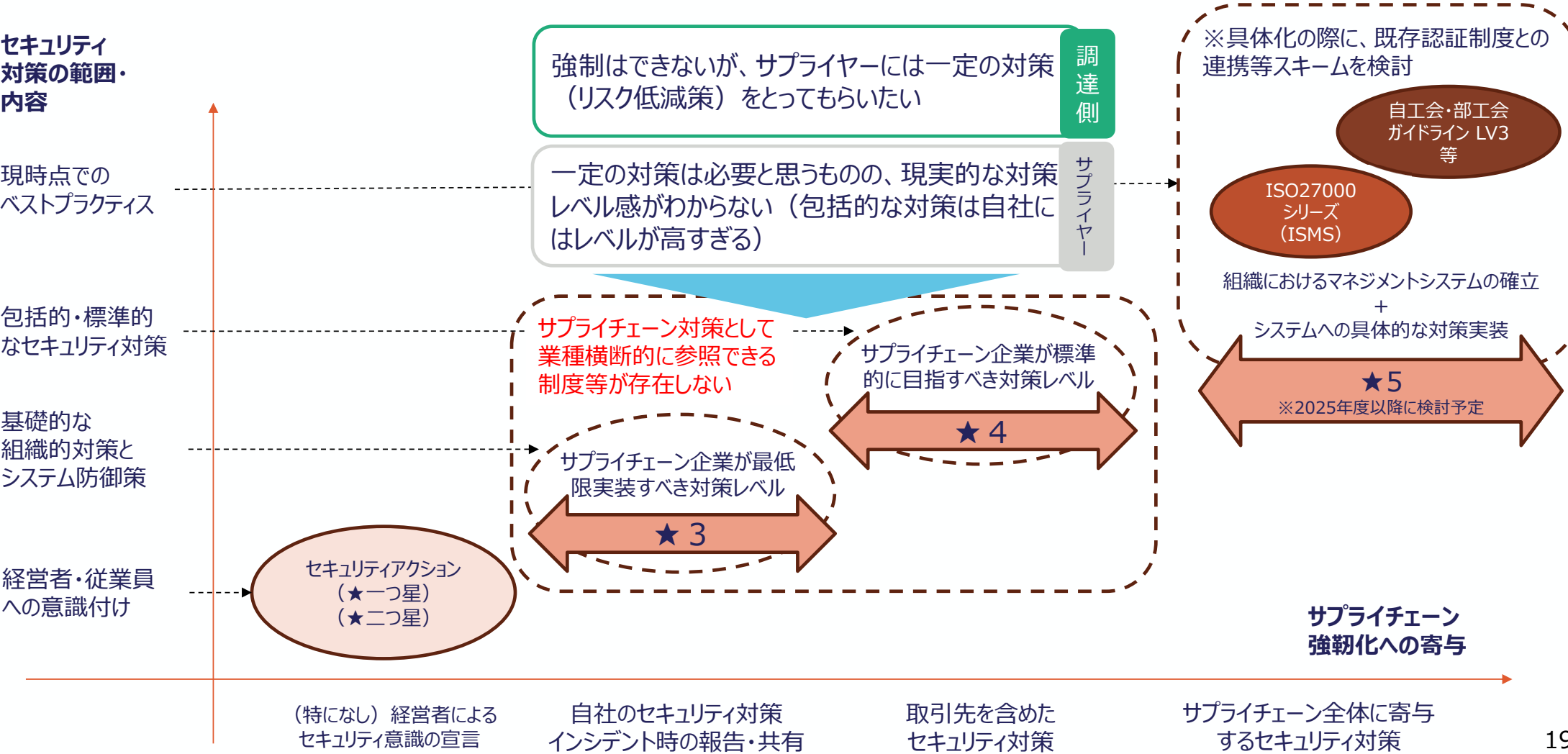


ランサムウェア感染の経路（令和6年）

[参考] 警察庁「サイバー空間をめぐる脅威の情勢等」
<https://www.npa.go.jp/publications/statistics/cybersecurity/index.html>

2. 構築する評価制度

2.3 制度で用いるセキュリティ要求事項・評価基準 — まとめ



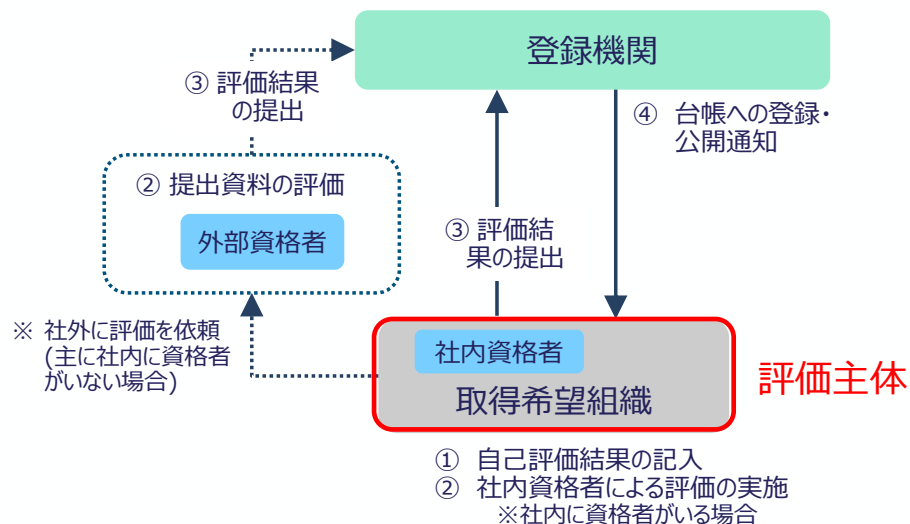
2. 構築する評価制度

2.4 制度における評価スキーム

- 英国CEや米国CMMCを参考に、★3は自己評価（ただし専門家の助言プロセスを要する）、★4は第三者評価（技術要件を中心に、一部要求事項について第三者評価を実施）スキームを想定
- ★4を自己評価型と第三者評価型の双方とする案（★4, ★4plus）や、審査品質の確保方策（評価者に求める要件、第三者評価時の対象項目・評価観点等）は、今後の実証事業や海外制度調査や想定される評価機関の状況等も踏まえつつ、引き続き精査

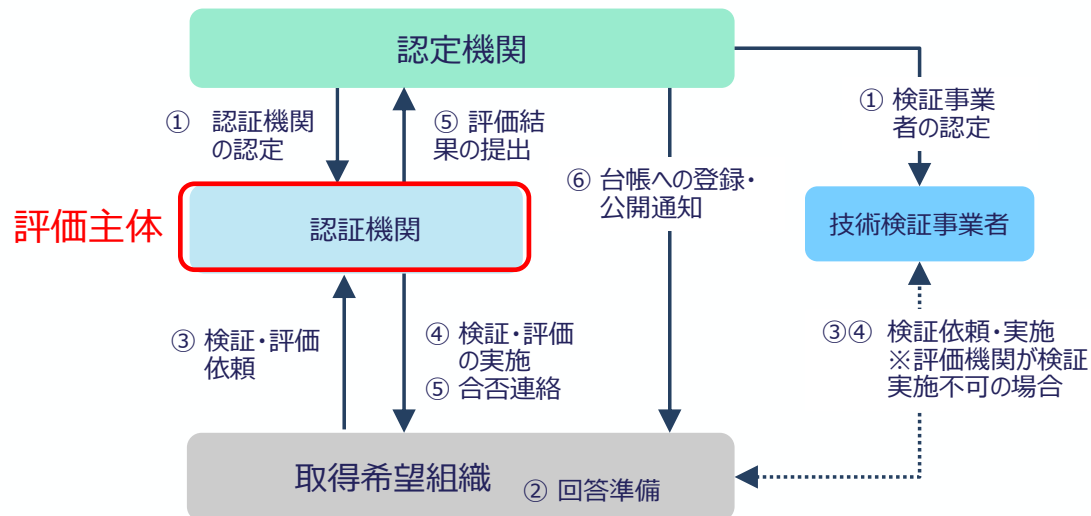
自己評価：★3

- ① 取得希望組織は、★3要求事項に基づき自己評価を記入（必要に応じ、社内外の資格者の助言を得る）
- ② 社内外の資格者は、記入内容の評価、要求事項に対する可否を判断
- ③ 取得希望組織または社内外の資格者は、登録機関に評価結果を提出
- ④ 登録機関は、申請内容に問題が認められない場合には台帳に登録・公開



第三者評価：★4

- ① 認定機関は、認証機関・技術検証事業者を認定
- ② 取得希望組織は、★4要求事項に基づき回答を準備
- ③ 取得希望組織は、認証機関または技術検証事業者へ、検証・評価を依頼
- ④ 認証機関または技術検証事業者は、検証・評価を実施
- ⑤ 評価結果を取得希望組織に通知し、認定機関に提出
- ⑥ 認定機関は、「合格」とされた組織を台帳に登録し、公開



2. 構築する評価制度

2.4 制度における評価スキーム

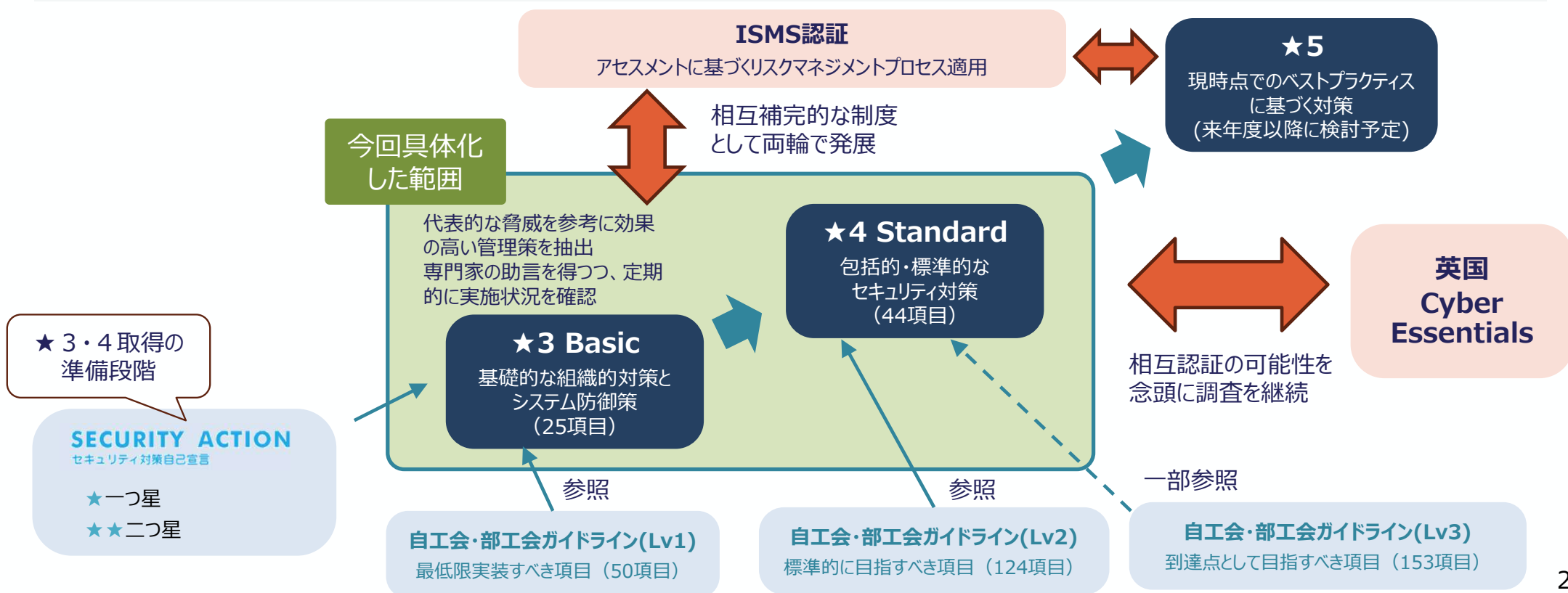
- ★ 3 については有効期間を1年とし、対策状況について年次で点検することをもって更新可能とする
- ★ 4 については複数年の有効期間とし、有効期間内は年次での自己評価（結果は評価機関に提出）をもって更新可能とする案
- 今後の実証事業や想定される評価機関の状況等も踏まえつつ、引き続き精査

	★ 3（自己評価）	★ 4（第三者評価）	★ 5
評価実施主体	適合性評価の対象となる組織自身 （自己評価）	認定機関から認定を受けた評価機関 （第三者評価）	TBD
有効期間	1年	3年	
維持に必要な手続き	有効期限を更新するため、要求事項の遵守状況について年次で自己評価 （専門家の助言プロセス有り）	・有効期間内は、1年ごとに自己評価を実施（評価機関に提出） ・有効期限を更新する際（3年に1回）は第三者評価が必要	
資格の取消し等	取得組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、評価機関または認定機関から資格の一時停止または取消しを行う場合がある		

2. 構築する評価制度

2.5 国内外の関連制度等との連携・整合

- ・ サプライチェーン対策評価制度（★ 3 / 4）は、先行する自己評価の仕組みである「SECURITY ACTION」「自工会・部工会ガイドライン」や、国際標準であるISMS適合性評価制度と相互補完的な制度として発展することを目指す。
- ・ ★ 3 / 4は、自工会・部工会ガイドラインのLv1、Lv2に対応。自工会・部工会ガイドラインに基づく自己評価結果の本制度での活用などの連携方策を引き続き検討。また、英国CEとは、将来的な相互認証の可能性も念頭に、引き続き調査・意見交換を継続。



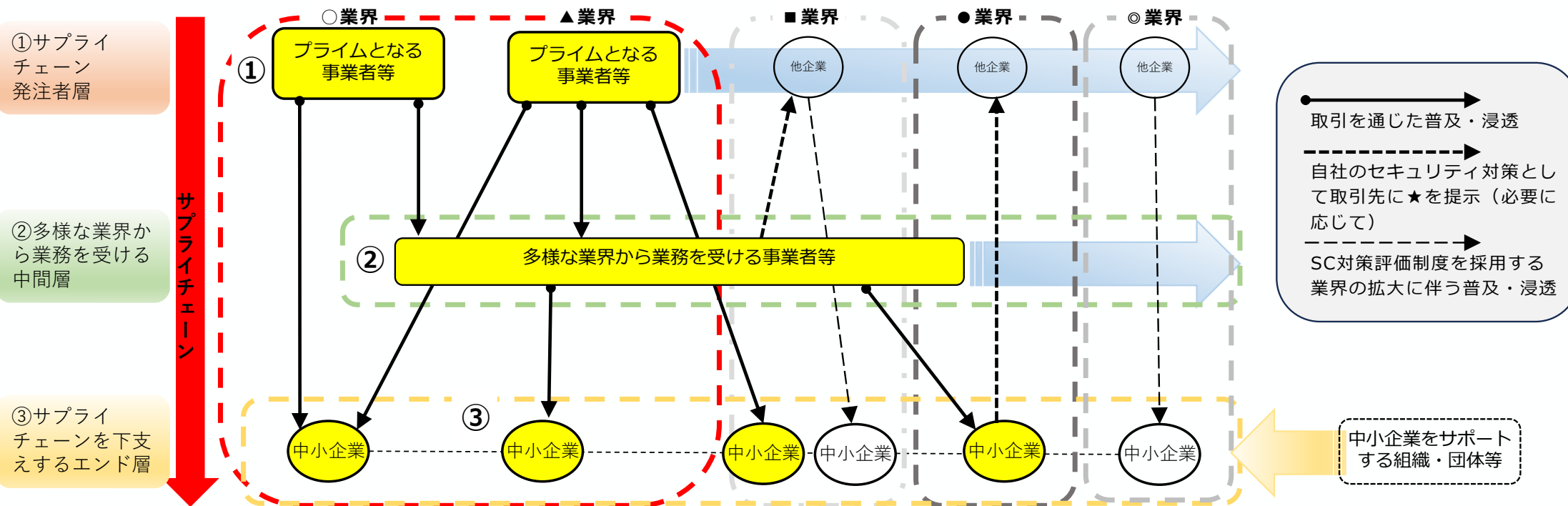


3. 制度整備に向けた道筋

3. 制度整備に向けた道筋

3.1 制度が効果的と想定される業界等 - 複雑なサプライチェーンの構造

- ・ サプライチェーンは多層構造、複雑性（N×N）を有するため、特定の企業や業界への普及策だけではサプライチェーン全体の強靱性に繋がらない可能性が存在する。
- ・ こうした点を踏まえ、①日本経済を牽引し市場への影響の大きいサプライチェーンの発注者側②多様な業界から業務を受ける中間層③中小企業を中心にサプライチェーンを下支えするエンド層に分けた上で制度普及について検討していく。



3. 制度整備に向けた道筋

3.1 制度が効果的と想定される業界等

- 下記の観点から、制度が効果的と想定される業界等については、優先的に制度活用を促進していく。
 - ✓ 発注者層では、重要な機密情報を有し、高いセキュリティレベルが求められる業界、セキュリティ要求への対応が困難な取引先が含まれる業界、サプライチェーン間の結びつきが強い業界、サプライチェーンが複雑な業界
 - ✓ 中間層では、重要な機密情報・重要な業務の委託を受け、様々な業界からセキュリティ要請を受けている業界・事業者
 - ✓ エンド層では、情報管理や事業継続において重要な役割を果たす業界・事業者

	該当する業界等	業界等におけるニーズ
① サプライチェーン発注者層	- 政府機関等 - 重要インフラ事業者 - 主要製造業 等	- 重要な機密情報を有し、高いセキュリティレベルが求められる業界：顧客情報等、重要な機密情報を委託する取引先のセキュリティ管理の実効性に課題あり。厳密な第三者評価、評価結果の開示、技術検証を制度に組み込むことにより、★4以上の活用が期待できる。(例：金融 等) - セキュリティ要求への対応が困難な取引先が含まれる業界：重要な機密情報を委託しているものの、取引先・再委託先企業の人材・予算が十分でなく、自己評価の実効性にも課題を抱えており、取引先への支援策とセットで★3活用が期待できる。(例：金融 等) - サプライチェーン間の結びつきが強い業界：サプライチェーンを構成する事業者の事業停止がサプライチェーン全体に波及するリスクのある業界については、★3～4の活用が期待できる。(例：自動車、半導体等) - サプライチェーンが複雑な業界：取引先・再委託の管理や対策状況の確認に多大なコストが生じるため、取引内容・取引先に応じて★3～4の活用が期待できる。(例：主要製造業)
② 多様な業界から業務を受ける中間層	- BPO事業者 - 製品・部品製造業 等	重要な機密情報・重要な業務の委託を受け、様々な業界からセキュリティ要請を受けている業界・事業者：様々な要請や現地審査に対応するための負担あり。BPOでは、業種・業界問わず統一的に活用されることで★3～4の活用が見込める。ISMS等を既に取得する事業者もあり、既存の取組との整合性が必要。製造業は対応負荷軽減につながれば★4の活用が期待できる。大手事業者の★取得のコスト負担の影響は少ないが、取引先が海外を含む場合は海外制度との整合性が必要。
③ サプライチェーンを下支えするエンド層	中小企業全般 (BtoB)	情報管理や事業継続において重要な役割を果たす業界・事業者：特に、比較的規模の大きな事業者(101人以上)、インシデントを経験した事業者、既に対策に取り組んでいる事業者(SA宣言者)等において、セキュリティ対策を進めるために、★3～4の活用が期待できる。エンド層にとっては、費用や人材、経営者のリテラシー等が課題となり、導入促進策とセットの展開が必要である。

※ 重要な機密情報：機密情報のうち、当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

3. 制度整備に向けた道筋

(参考) 各業界へのヒアリングから得られた意見

	業界	ヒアリング結果
①サプライチェーン発注者層	金融、クレジット	- 金融業界やクレジット業界では、高いセキュリティが求められることから、取引先のセキュリティ対策確認の実効性を高めるために、評価制度の活用ニーズはあると考えられる。 - 金融業界として、委託先へのセキュリティに関する確認事項を標準化予定であることから、本制度と連携して検討を進めていくことが望ましい。
	金融（保険）、建設	- 保険業界では、代理店におけるセキュリティ対策状況の底上げのために、★3制度に対する期待があると考えられる。 - 建設業においては、協力会社を対象としたセキュリティガイドラインが既にあり、業界のピラミッド構造を踏まえた各層への要求レベルを明確化することで、制度の活用が期待できる。ただし、小規模な企業も含まれることから、費用面での支援や相談窓口の設置等、導入促進策とセットでの展開が求められる。
	自動車、半導体	- 自動車産業や半導体産業のような、サプライチェーンの事業上の接続が強い業界においては、取引先に対するセキュリティ対策のニーズがあると考えられる。 - 特に、自動車産業においては、セキュリティガイドラインが存在し活用されていることから、本制度と連携していくことが望ましい。
	主要製造業	多数の製品・取引先を抱える製造業においては、取引先のセキュリティ対策状況をチェックリストで確認している場合も多いが、実効性には課題があり、また取引先数も多く全件の確認が困難であることから、本制度に対する期待がある。
②多様な業界から業務を受ける中間層	BPO事業者	- BPO業界においては、業界・業種問わず項目を統一することで対策要請への対応の効率化が図れることから、★取得希望がある。取引条件や調達における資格審査要件となれば、希望度合いは上がる。 - 自身が取得するだけでなく、取引先にも本制度の取得を求めるニーズがあることから、取得事業者の広がりが期待できる。
	製品・部品製造業	- 一般製品等の製造業では、様々な取引先からセキュリティ対策要請を受けており、今後も増えていくことが想定される。評価基準が統一され、一つの基準を達成することで様々な業界・業種と取引が容易になることが期待されている。 - ただし、制御系や工作機器等、グローバルでの取引が中心となる業界は、海外制度との整合性を図ることが必要である。
③サプライチェーンを下支えするエンド層		- セキュリティ対策に対する必要性が高い中小企業はあるが、費用や人材、経営者のリテラシー等が課題となり、導入促進策とセットの展開が必要である。 - 中小事業者の中でもインシデントを経験した事業者、既に対策に取り組んでいる事業者(SA宣言者等)であれば、本制度を円滑に活用できる可能性がある。

3. 制度整備に向けた道筋

3.2 制度の導入促進

- 各業界に対するヒアリングの中では、制度を活用する上で下記の施策を求める声が見受けられており、これらも踏まえて導入促進に向けた取組の具体化を進めていく。

①発注者層、②中間者層、③エンド層、④評価機関・専門家

課題	導入促進策（案）	①	②	③	④
①対策推進のための企業への支援	● 専門家の活用促進 専門家の確保・育成を行うと共に、主に中小企業と専門家のマッチングの仕組みを構築する。専門家の確保にあたっては、情報処理安全確保支援士（登録セキスベ）に加え、セキュリティ・ブレゼンターやITコーディネータ（セキュリティ関連資格保有者）等の活用も検討する。専門家による支援内容の明確化のため、過去IPAが実施した「中小企業の情報セキュリティマネジメント指導業務」等の成果を活用し、支援プロセスやアウトプットを明確にした指導要領の作成、支援ツール（企業へのヒアリングシート、作成文書雛形等）を準備する。			○	
	● 中小企業セキュリティ普及促進策との連動 SA宣言事業者に対する推奨、★取得とお助け隊サービス、情報セキュリティサービス審査登録制度、その他業界団体が提供するサービスリストなど中小企業が導入可能な具体的なサービスとセットでの普及啓発を行う。また、中小企業セキュリティ対策普及啓発コンテンツに本制度、及び★取得推奨に関して追記する。			○	
②下請法や価格転嫁への対応	● 取引先への対策の要請等に係る考え方の整理 取引先へのセキュリティ対策の支援や要請に係る独占禁止法等との明確な整理を行う。それを踏まえつつ、民民の契約において本制度の要求基準や★取得の推奨等を盛り込む際のひな型の作成、提供を行う。	○	○	○	
③国としての推進、業界の巻き込み	● 中小企業の情報セキュリティガイドラインへの追記 中小企業の情報セキュリティガイドライン、及び付録サンプル規程において、本制度の要求基準等の記載、★取得の推奨を行う。			○	
	● 業界毎の特性を踏まえた導入促進 各業界のセキュリティガイドライン等における委託先へのセキュリティ対策として、本制度の要求基準等の記載、★取得確認の推奨を推進する。また、政府の施策等との連動等により、各業界への適用に向けた検討を進める。	○	○		
	● 政府機関や重要インフラ事業者等における活用の推進 政府調達での参照や重要インフラ事業者等での活用推奨等について検討を進める。	○	○		
	● 本制度の継続的な広報、周知 国や制度オーナーが連携し、本制度の効果や取得のメリット、発注者・受注者それぞれに期待される役割等について分かりやすく発信し、制度に対する活用意欲を向上させる広報や周知活動を継続的に行う。	○	○	○	○
④評価機関の支援・育成	● 評価機関の支援 評価基準や評価手法を明確化し、評価の品質を保つとともに、企業における対応を容易なものとするため、評価者に向けた評価ガイドとして、標準的なレビュープロセス、実施事項を明確化する。				○
	● セキュリティ評価・対策支援人材の育成 セキュリティ人材不足の解消、及び評価及び対策支援をシームレスに行うため、本制度に関わる人材育成のための、コンテンツや研修機会を設ける。				○
⑤他制度との連携推進	● 他のガイドラインや関連制度との整合性確保 「SECURITY ACTION」「自工会・部工会ガイドライン」や、国際標準であるISMS適合性評価制度等との整合性の確保や、評価結果の本制度での活用などの連携方策の検討を進める。また、将来的な相互認証の可能性を念頭に、グローバルな評価制度との連携・意見交換を継続する。 サプライチェーン対策全体を俯瞰し、各制度の位置づけを明確にする利用者目線での他のガイドライン等との関係整理を行う。	○	○	○	○

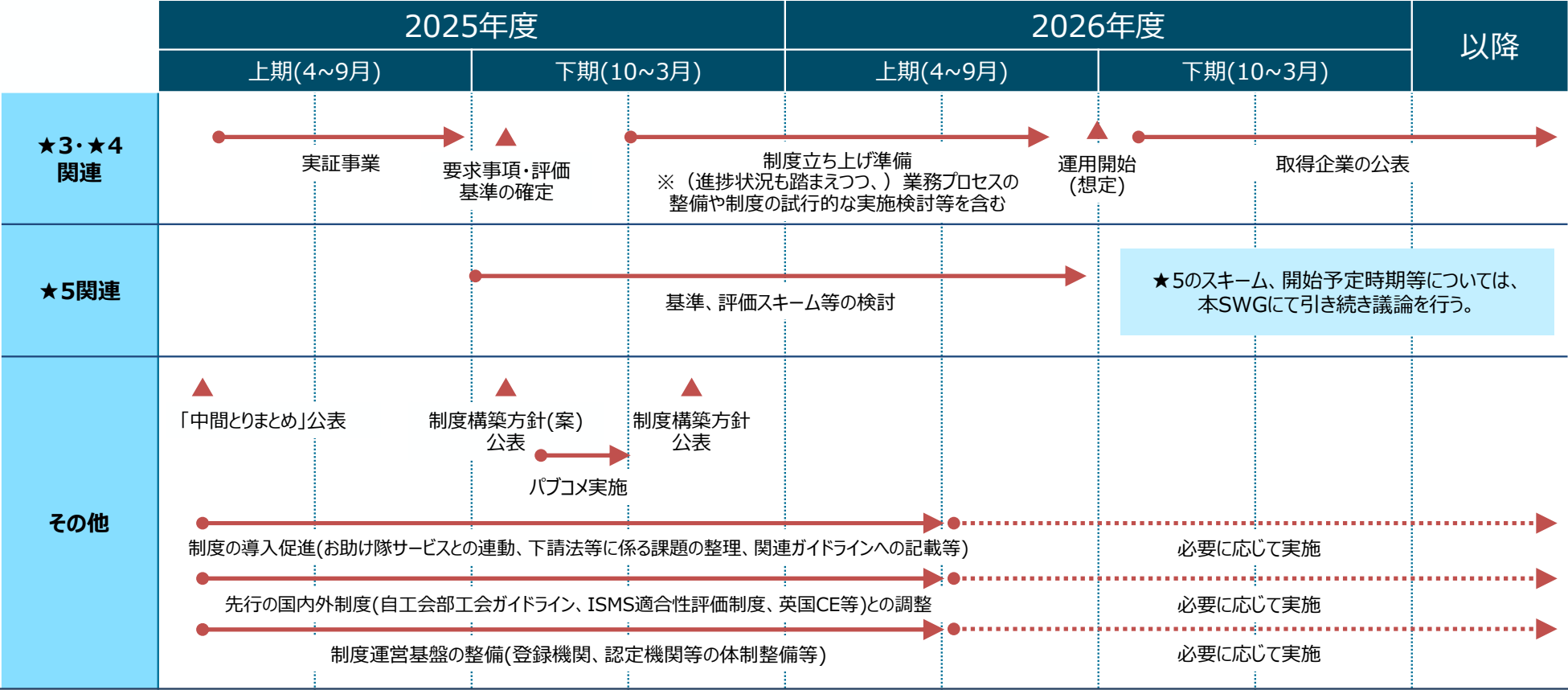


4. 今後の検討の進め方及びスケジュール

4. 今後の検討の進め方及びスケジュール

25年度以降のスケジュール

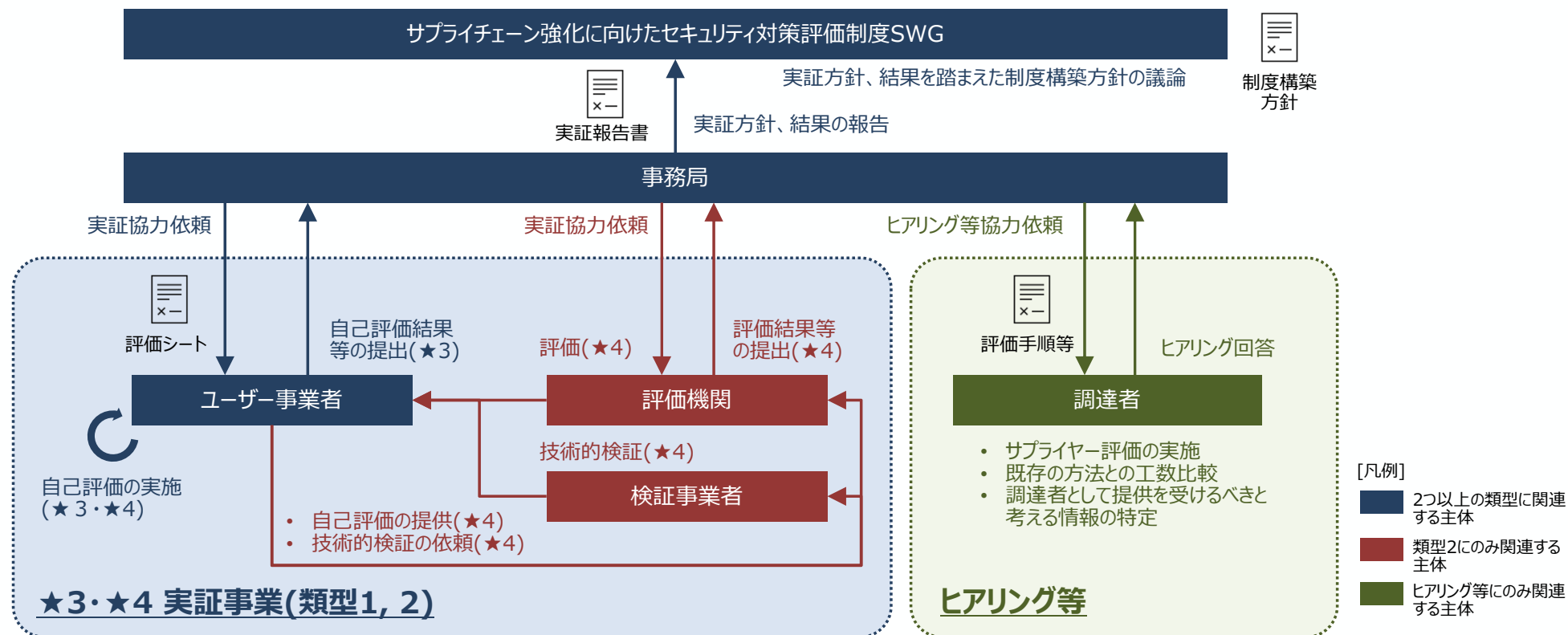
- 2026年度の制度開始を目指し、実証事業による制度案の検討と並行して、制度運営基盤の整備や利用促進等を進めていく。



4. 今後の検討の進め方及びスケジュール

実証事業の推進計画 — 実証の類型及び関係主体の役割分担等

- 実証においては類型1（★3）、類型2（★4）の2タイプを設けるとともに、調達者を対象としたヒアリング等を実施することを予定。
- 類型ごとの関係主体、それぞれの役割は以下の通りと想定。
 - 類型1（★3）：事務局、ユーザー事業者、外部専門家（必要な場合）
 - 類型2（★4）：事務局、ユーザー事業者、評価機関、検証事業者
 - ヒアリング等：事務局、調達者





付録：諸外国における関連する取組

1. 英国サイバー・エッセンシャルズ（Cyber Essentials）

- 英国サイバー・エッセンシャルズは、代表的なサイバー攻撃への普遍的な防御策として、英国セキュリティ機関NCSCが提供するフレームワーク。企業の規模によらず、一般的なサイバー攻撃全般から組織を保護するのに役立つとされている。
- 自己診断で取得可能な「Cyber Essentials」と、第三者による技術検証が必要な「Cyber Essentials Plus」の二段階
- 英国の公的機関の調達において必須要件として課される場合が多い。また、鉄道など一部民間分野でも取引要件として一般的に活用されつつある。（2023年3月段階で、12万以上の者がCEを取得）

セキュリティ要件（共通）

アセスメント要件



- ファイアーウォール
- セキュアな構成
- セキュリティアップデート管理
- ユーザアクセス制御
- マルウェア対策

の5つのカテゴリで要求事項を提示



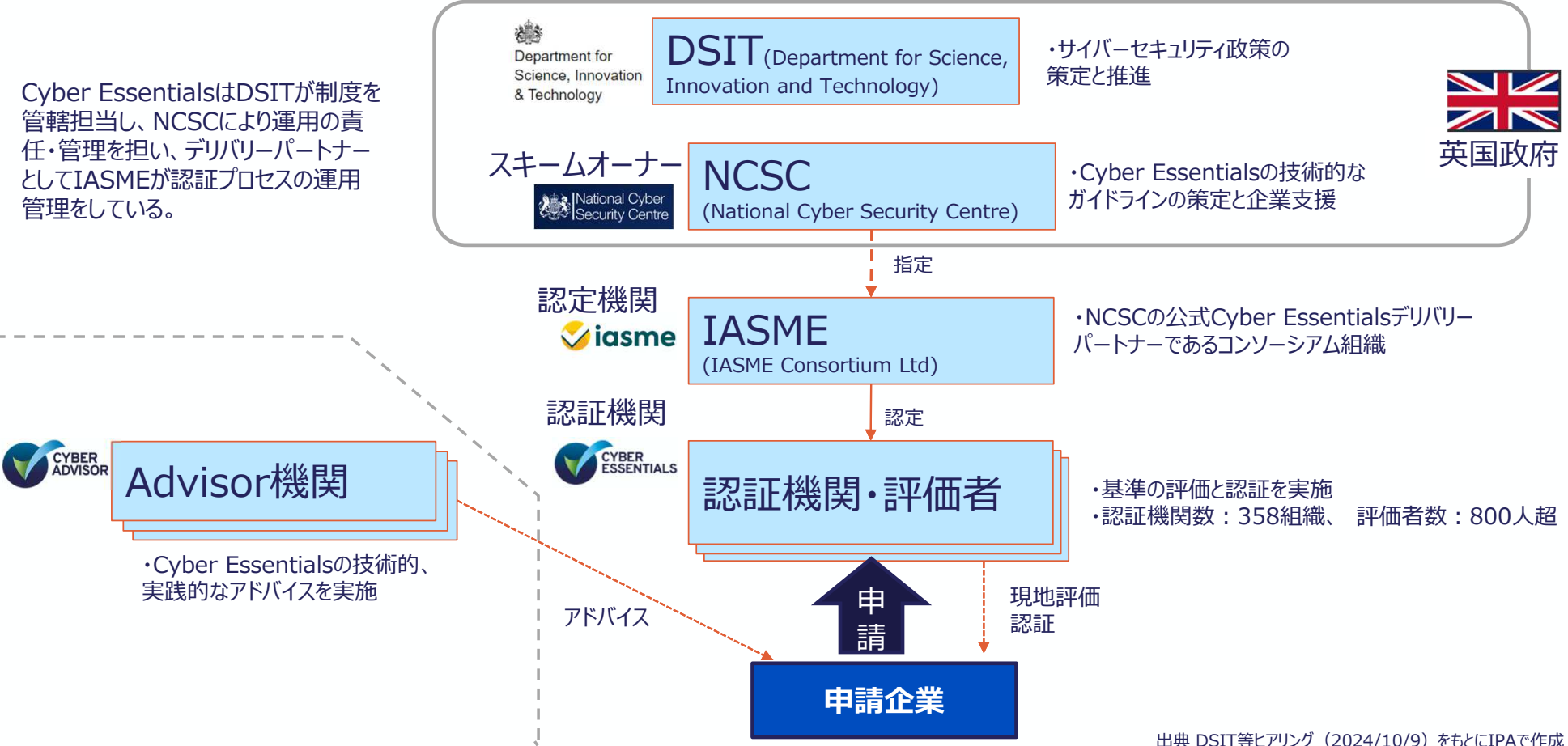
※ 認証の適用範囲の評価を行う際に、対象資産に関する設問があり、資産管理についても間接的に要求していると解釈できる

- Cyber Essentialsの取得を前提として、実地検査として認定機関による技術検証を受けることが必要（脆弱性診断、権限管理など具体的なテスト項目と仕様を提示）

- インターネット上でのオンライン審査にて自己診断を行い、認定機関に所属する有資格の審査員が回答内容进行评估。
- 合格した場合は認定証が授与され、不合格の場合は今後の助言等が示される。

1. 英国サイバー・エッセンシャルズ — 認証スキーム

- Cyber EssentialsはDSITが制度を管轄担当し、NCSCにより運用の責任・管理を担い、デリバリーパートナーとしてIASMEが認証プロセスの運用管理をしている。



出典 DSIT等ヒアリング（2024/10/9）をもとにIPAで作成

1. 英国サイバー・エッセンシャルズ — 制度の効果検証

- 英国政府は2013年にサイバー攻撃事例を分析、組織がシステムを適切に保護するために「最低限必要な5つのコントロール」を抽出しCEの要件とした。最新の攻撃動向に照らしても、5つのコントロールは有効との見解

サイバーエッセンシャルズ効果検証※（2024年10月）のポイント

- CE利用者の80%が、CEのセキュリティ要件は一般的なサイバー脅威に対して有効でありリスク低減につながっていると回答
- CEの利用者は、サイバー攻撃の被害に遭う可能性を5.8点/10点と評価（未取得組織は3.7点）。CE利用者のサイバー脅威に対するリスク意識の高まりが見られた
- CE利用者の76%が、CE要件以外の追加的な予防措置を講じたと報告
- CE利用者の約半数（48%）が、サプライヤーへのCE取得義務あるいは将来的な義務化を検討。
- NCSCの年次レビューによると、CE取得組織は、同じ保険契約を結んでいるCE未取得の組織と比べてサイバー保険の請求が80%減少（2022年請求データ）

※CE取得組織(606)と未取得組織(516)をサンプルとして比較、取得効果を検証

NCSC公式サイト（サイバーエッセンシャルズ解説ページ）



1. 英国サイバー・エッセンシャルズ — 申請費用と実績数

- Cyber Essentialsの申請費用は、企業規模に応じたものとしてIASMEで定めている（下表）。なお、コンサル経由で申請する場合などにおいては、市場原理に応じた柔軟な価格設定される場合もある。
- Cyber Essentials Plusは申請企業の規模と複雑さにより差異が大きいため、標準価格は定めず認証機関の見積による。
- Cyber Essentialsの審査の実績情報は、経年とともに増加している。
- 直近の年間認証数は約47,500件。うちCyber Essentials がその75%を占める。認証取得組織の規模は、小規模以下の組織が68%（小規模、零細ともに34%）を占める。

表. Cyber Essentialsの申請費用

企業規模	費用
零細（0-9名）	\$420（約60千円）
小規模（10-49名）	\$570（約81千円）
中規模（50-249名）	\$650（約93千円）
大規模（250名以上）	\$780（約112千円）

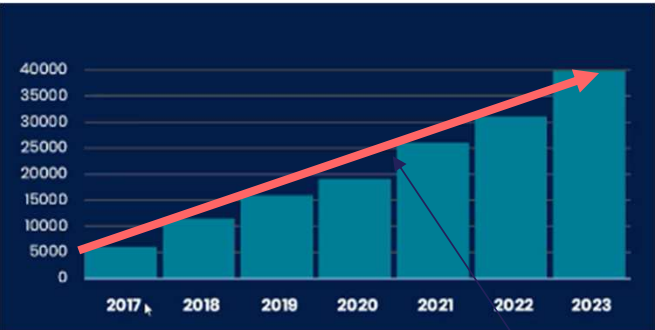


図. Cyber Essentials 認証件数の経年変化

経年で増加

出典 DSITヒアリング2024/10/9より

表. 企業規模ごとのCE認証件数

制度の種類	大規模 (250以上)	中規模 (50-249)	小規模 (10-49)	零細 (0-9)	合計	割合
Cyber Essentials	3,595	7,254	12,544	12,420	35,813	75%
Cyber Essentials Plus	1,715	2,735	3,479	3,741	11,670	25%
合計	5,310	9,989	16,023	16,161	47,483	100%
割合	11%	21%	34%	34%	100%	

小規模以下の組織で68%

Cyber Essentialsが75%

出典 英国政府サイト（2024年1月～2024年12月の集計結果）をもとにIPAにて加工
<https://www.gov.uk/government/statistical-data-sets/cyber-essentials-management-information>

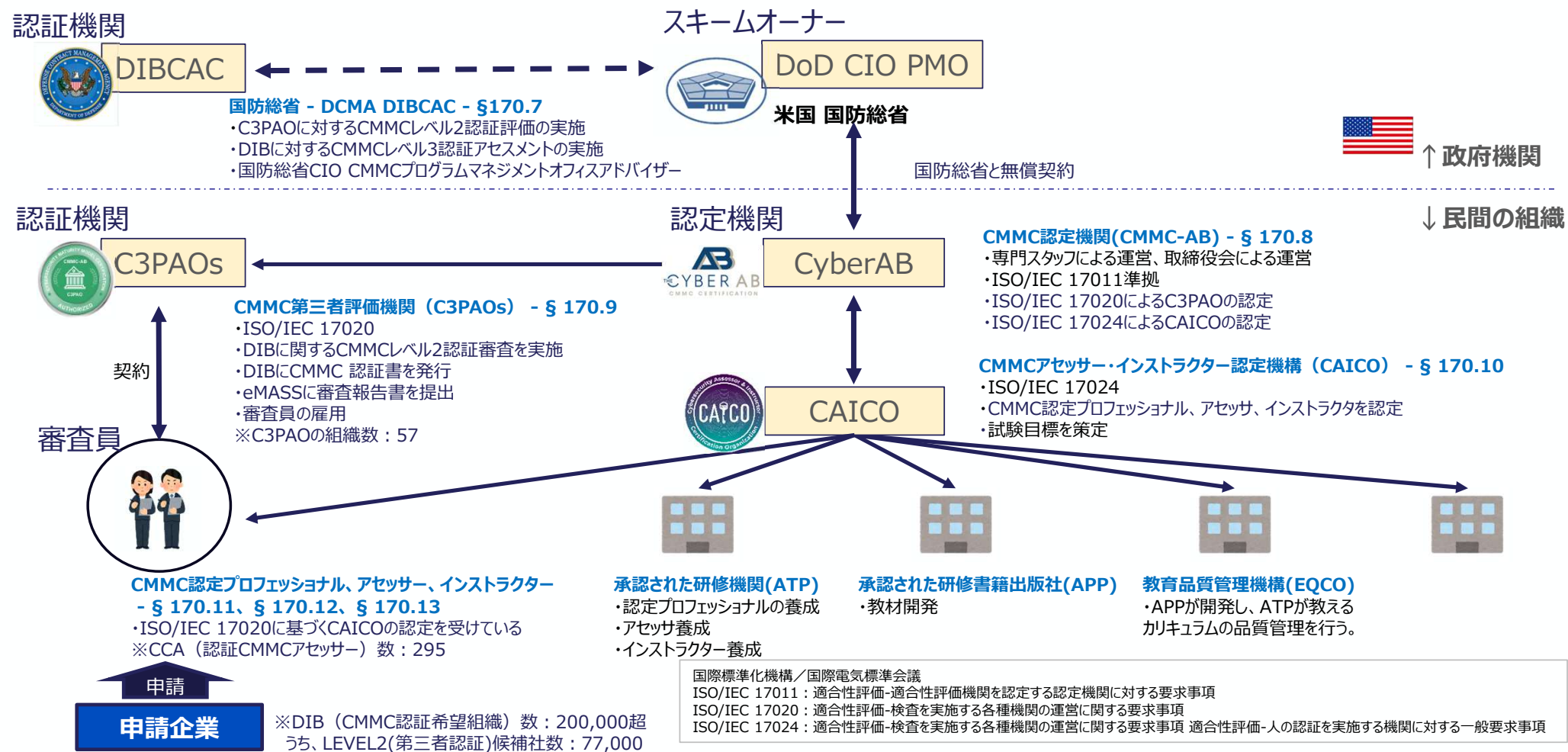
2. 米国 CMMC 2.0 — 概要

- 米国CMMC 2.0は、国防総省から発注を受ける防衛産業基盤（DIB：Defense Industrial Base）企業が「連邦契約情報（FCI）」及び「管理された非格付け情報(CUI)」を適切に保護させるための米国防総省(DoD)のプログラム。
- 2021年12月CMMC2.0を発表（CMMC 1.0と比較して基準を簡素化、レベル区分も3段階に見直し）。2024年12月にCMMC 2.0が発効。下位レベルから順次段階的に採用して数年を掛けて完全実施を予定。
- CUIの取扱い要件は、国防総省の調達ルール(DFARS)でのみ規定されたものであるが、全ての米国政府機関の調達契約に適用すべく、連邦政府の管理ルール(FAR)での規定案が2025年1月に公開され、2025年3月までパブコメを実施。^{*1}

	セキュリティ要件 (Security Requirements)	アセスメント要件 (Assessment Requirements)	確認要件 (Affirmation Requirements)
LEVEL 3	• DFARS 252.204-7012の要求 • NIST SP800-171 R2の110項目 • NIST SP800-172 Feb2021から選択された24項目	• DoD評価（DIBCAC）により、要件すべての実装を検証 • 未達の要件は、評価後180日以内に終了しなければならない行動計画(POA&M)を設定することが認められる	• 請負業者の幹部職員は、POA&Mへの対応を含む毎回の審査後及びその後毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力
LEVEL 2	• DFARS 252.204-7012の要求 • NIST SP800-171 R2*1の110項目	• 自己評価または第三者評価により、要件すべて実施されていることを検証 • 未達の要件は、評価後180日以内に終了しなければならない行動計画(POA&M)を設定することが認められる	• 請負業者の幹部職員は、POA&Mへの対応を含む毎回の審査後及びその後毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力
LEVEL 1	• FAR Clause 52.204-21で既に要求 • 15項目	• 自己評価により確認 • 評価結果をサプライヤー・パフォーマンス・リスク・システム(SPRS)に入力	• 請負業者は、毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力

参考 <https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>
^{*1} <https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information>

2. 米国 CMMC 2.0 — 認証スキーム



出典 米国のサプライチェーン企業におけるサイバーセキュリティ制度の調査報告書（2024年 エヴァアビエーション）をもとにIPAで加工

3. フランス サイバースコア法（CYBERSCORE） — 概要

- ・ フランスでは、Webサイトを対象に、サイバーセキュリティに係るスコアリングの実施を法律により義務付け。
- ・ 消費者の個人情報保護の観点から、Webサイトにおけるセキュリティ確保とデータ保護に係る信頼性を消費者に通知することを目的とするもの。
- ・ 対象は、2024年時点でフランス領土からの月間ユニークビジター数が2,500万人以上（2025年以降は月間1,500万人以上へと基準の引下げ予定）のサイト。対象サイトの運営者等に対して、サイバーセキュリティ監査の実施及び監査結果から算出されたスコアの提示を義務化。
- ・ スコアの算出は、ANSSIによって指定されたプロバイダーによる監査を通じて行われる。

スコア算出上考慮される主な基準



「組織とガバナンス」
「データ保護」
「デジタルサービスに対する知識と習熟」
「アウトソーシングのレベル」
「インターネット上での露出度」
「セキュリティインシデント対処体制」
「セキュリティ監査の実施」
等の9つのカテゴリで監査基準を提示

段階分け

Niveau
A+
A
B
C
D
E
F

スコアはFからA+の7段階で定義される
（現状、それぞれの段階の定義は公表されていない）

4. オーストラリア エssenシャル・エイト（Essential Eight） — 概要

- ・ エssenシャル・エイトは、豪州のセキュリティ機関ACSC(Australian Cyber Security Center) が策定した基準。
- ・ 4段階の成熟度を定義し、攻撃者の手口や脅威のレベルに応じて、組織が段階的に実施できるよう設計。
- ・ 豪州内のすべての組織を対象として想定。なお成熟度 2 は、パブリックガバナンス・パフォーマンス・アクト（PGPA Act）の対象となる豪州の中央政府及びその他の公的団体等では必須要件とされている。
- ・ 組織がサイバーセキュリティインシデントを軽減するため 8 分類の重要な対策を提示。
（パッチ適用、パッチ運用システム、多要素認証、特権の制限、アプリケーション管理、Microsoft Officeマクロの制限、ユーザーアプリケーションの堅牢化、定期的なバックアップ）



組織の成熟度	定義	セキュリティ要件 (レベル毎に詳細な対策を提示)
レベル 3	より適応力が高く、公開ツールやテクニックへの依存度がはるかに低い 攻撃者への対応を念頭に置く	8分類 149項目（＝全項目）
レベル 2	レベル1より高度な攻撃者で、ツールの有効性に対してより多くの時 間の投下を厭わない者への対応を念頭に置く	8分類 107項目
レベル 1	広く入手可能で汎用的な技術の活用で満足する攻撃者への対応 を念頭に置く	8分類 48項目
レベル 0	組織の全体的なサイバーセキュリティ態勢に弱点がある	－（求められるセキュリティ要件無し）



経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
<https://www.meti.go.jp/policy/netsecurity/index.html>

