（別紙）
既存評価基準・規格一覧

評価基準・規格		評価基準・規格概要													評価者の要件	参考文献（評価者）
		目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）		
ITガバナンス/DXの視点	システム管理基準	どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化・一般化	http://www.meti.go	情報システムの企画、開発、保守、運用といったライフサイクルを管理するためのITマネジメントと、経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力であるITガバナンスについて留意すべき基本的事項を体系化・一般化	前文 システム管理基準の枠組み Ⅰ ITガバナンス Ⅱ 企画フェーズ Ⅲ 開発フェーズ Ⅳ アジャイル開発 Ⅴ運用・利用フェーズ Ⅵ 保守フェーズ Ⅶ 外部サービス管理 Ⅷ 事業継続管理 Ⅸ 人的資源管理 Ⅹ ドキュメント管理				－	－	－	－	－	－	－	－
	Cobit2019 （Control Objectives for Information and related Technology）	事業体のITに関するガバナンスのフレームワークを提供する。	http://itgi.jp/cobit2019/index.html	以下の4点を踏まえ、ISACA（Information Systems Audit and Control Association）がCOBIT 5（Control Objectives for Information and related Technology）の改訂版としてフレームワークを提供している。 1.ITガバナンスからI&Tガバナンスへ（I&Tガバナンスの最適化） 2.変化する環境に相応したプロダクトであること 3.これまでに構築されたCOBI（Control Objectives for Information and related Technology）Tの強み、特定されている機会の上に構築すること 4.把握されているCOBIT 5（Control Objectives for Information and related Technology）の限界	Introduction and Methodology Governance and Management Objectives Designing an Information and Technology Governance Solution Implementing and Optimizing an Information and Technology Governance Solution	https://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx	ISACA	COBIT2019	－	－	－	－	－	－	－	－
	Val IT	IT投資に関する包括的なガイドラインで、IT投資を機軸とした変革のためのマネジメント・フレームワークを提供する。	http://www.isaca.org/About-ISACA/Press-room/News-Releases/Japanese/Pages/New-Series-from-ITGI-Focuses-on-IT-Value-Japanese.aspx	IT投資に関する包括的なガイドラインとして、価値ガバナンス、ポートフォリオ管理、投資管理の3つの観点でフレームワークを提供している。	価値ガバナンス（Value Governance, VG） ポートフォリオ管理(Portfolio Management, PM) 投資管理(Investment Management, IM)	http://www.isaca.org/knowledge-center/val-it-it-value-delivery-/pages/val-it1.aspx	ISACA	v2.0	－	－	－	－	－	－	－	－
	ISO/IEC 38500シリーズ （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission）	期待効果 ・組織のITガバナンスに対する信頼をステークホルダーに保証する。 ・組織におけるITガバナンスにおいて経営者に対する情報、及び指針を提供する。 ・ITガバナンスに対し客観的な評価を行う際の基盤を提供する。	http://kikakurui.com/q/Q38500-2015-01.html	EDM（Evaluate, Direct and Monitor）モデルに基づき、経営者が6つの原則（責任、戦略、取得、パフォーマンス、適合、人間行動）に沿って取り組むべき事項が示されている。	0. 序文 1. 適用範囲、適用及び目的 2. 用語及び定義 3. 良好なITガバナンスのための枠組み 4. ITガバナンスのための手引き	http://kikakurui.com/q/Q38500-2015-01.html	ISO	ISO/IEC 38500:2015	－	－	－	－	－	－	－	－
	ISO・JIS Q31000 （ISO：International Organization for Standardization） （JIS：Japanese Industrial Standards）	組織を取り巻くあらゆるリスクを運用管理するための、体系的、かつ透明性があり信頼ができる形での原則、及び指針を提供する。	https://kikakurui.com/q/Q31000-2010-01.html	リスクマネジメントに係る原則、及び一般的な指針を、国際標準規格として規定する。	序文 1 適用範囲 2 引用規格 3 用語及び定義 4 原則 5 枠組み 5.1 一般 5.2 リーダーシップ及びコミットメント 5.3 統合 5.4 設計 5.5 実施 5.6 評価 5.7 改善 6 プロセス 6.1 一般 6.2 コミュニケーション及び協議 6.3 適用範囲，組織の状況及び基準 6.4 リスクアセスメント 6.5 リスク対応 6.6 モニタリング及びレビュー 6.7 記録作成及び報告 参考文献	https://www.newton-consulting.co.jp/bcmnavi/guideline/iso31000.html	ISO/JIS	ISO31000:2018	－	－	－	－	－	－	－	－
	COSO-ERM （COSO：The Committee of Sponsoring Organization of the Treadway Commission） （ERM：Enterprise Risk Management）	組織のリスクマネジメントを効果的・効率的に行うことを通じて組織の目的・目標達成を促進することを狙いとするフレームワークを提供する。	https://www.pwc.com/jp/ja/japan-knowledge/pwcs-view/pdf/pwcs-view201712-04.pdf	従来のCOSO（The Committee of Sponsoring Organization of the Treadway Commission）フレームワーク（内部統制フレームワーク）を補完的に拡張して、組織のリスクマネジメントを効果的・効率的に行うことを目的に、事業体の戦略・業務・報告・コンプライアンスに係る構成要素をフレームワークとして提供している。	＜事業体の目的＞ ・戦略 ・業務 ・報告 ・コンプライアンス ＜構成要素＞ ・内部環境 ・目的の設定 ・事象の識別 ・リスクの評価 ・リスクへの対応 ・統制活動 ・情報と伝達 ・モニタリング	https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Japanese.pdf	COSO	2017年9月改訂	－	－	－	－	－	－	－	－
	DX推進ガイドライン （DX：Digital Transformation）	デジタルトランスフォーメーションの実現、及び実現するためのITシステム構築にあたり、経営者が押さえておくべき事項を明確にすること、及び取締役会や株主がデジタルトランスフォーメーションに係る取組を評価する上で、活用できるものとすること。	http://www.meti.go.jp/press/2018/12/20181212004/20181212004.html	デジタルトランスフォーメーションを推進するための経営における有り方や仕組み、及びデジタルトランスフォーメーションを実現するIT基盤を構築する際の体制や実行プロセスの構築などに関するガイドライン	1. はじめに 2. デジタルトランスフォーメーションを推進するためのガイドライン 2-(1). DX推進のための経営の在り方・仕組み 2-(2). DXを実現する上で基盤となるITシステムの構築	http://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf	経済産業省	Ver1.0	－	－	－	－	－	－	－	－

評価基準・規格		評価基準・規格概要												評価者の要件	参考文献（評価者）
		目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）		
	IT-CMF（IT Capability Maturity Framework）	グローバルで活用されているビジネスバリュー志向のITマネジメントフレームワークである。企業・組織がITを活用しビジネス貢献するために必要となるケイパビリティ（能力）とその成熟度が定義されているもの。	https://www.keieik	4 Macro-Capabilities、36 IT Management Critical Capabilities、315 Capability Building Blocks + Individual Maturity Profiles、800 Maturity Assessment Questionsから構成されている。4 Macro-Capabilitiesは右記の通り。	MANAGING IT LIKE BUSINESS MANAGING THE IT BUDGET MANAGING IT FOR BUSINESS VALUE MANAGING THE IT CAPABILITY	https://ivi.ie/it-c	IVI(Innovation Value Institute)	2nd edition	－	－	－	－	－	－	－	－
ITマネジメント	PMBOK （Project Management Body of Knowledge）	国際的に標準とされているプロジェクトマネジメントの知識体系で、プロジェクトマネージャーの支店より、プロジェクトマネジメントに係るナレッジや技法を提供すること。	https://ja.wikipedia.org/wiki/PMBOK	プロジェクトマネジメントに係る各プロセスを5個の基本的なプロセス群と10個の知識エリアに分類し、各プロセスにおける情報や実勢方法を提供する。	＜プロセス群＞ 立ち上げプロセス群 計画プロセス群 など ＜知識エリア＞ プロジェクト統合マネジメント プロジェクト・スコープ・マネジメント プロジェクト・スケジュール・マネジメント など		プロジェクトマネジメント協会	第6版	－	－	－	－	－	－	－
	PRINCE2 （projects in controlled environments, 2nd version）	英国におけるプロジェクトマネジメントのデファクトスタンダードとして開発され、組織全体としてプロジェクトを推進する観点より、プロジェクトマネジメントに係る手順やプロセスを提供すること。	https://ja.wikipedia.org/wiki/PRINCE2	プロジェクトマネジメントに係る方法論を要素、原則、テーマ、プロセスなどの観点より提供する。	＜要素＞ 原則 テーマ プロセス テーラリング ＜原則＞ ビジネスの継続の正当性 経験からの学習 定義された役割および責任 など	https://www.prince2	英国商務省	2017年版	－	－	－	－	－	－	－
	Val ITモデル	組織が、負担のできる費用で、また既知であり許容されるレベルのリスクで、情報化投資から最大の価値を実現する状況をマネジメントに確保させ、役員や経営者が情報化投資に関する自らの役割を理解し実行することを支援するガイドライン、プロセス、サポートプラクティスを提供する。	http://itgi.jp/pdf data/VALIT_FrameworkVersion1.pdf	投資の決定と利益の実現に重点を置いた、フレームワーク、プロセス、ベストプラクティス	・ValITフレームワーク ・ValITプロセスと重点管理プラクティス	http://itgi.jp/pdf data/VALIT_FrameworkVersion1.pdf	ITガバナンス協会（米国）	Ver2.0	－	－	－	－	－	－	－
開発・保守	CMMI （Capability Maturity Model Integration）	組織におけるプロセスを評価し改善につなげるための評価モデルを提供する。	https://ja.wikipedia.org/wiki/%E8%83%BD%E5%8A%9B%E6%88%90%E7%86%9F%E5%BA%A6%E3%83%A2%E3%83%87%E3%83%AB%E7%B5%B1%E5%90%88				カーネギーメロン大学ソフトウェアエンジニアリングインスティテュート	Ver2.0	○	カーネギーメロン大学のソフトウェア工学研究所（SEI：Software Engineering Institute）	大和コンピューター　等	参考文献欄参照	－	https://sas.cmmiinstitute.com/pars/pars.aspx	・SEI（Software Engineering Institute）がCMMI（Capability Maturity Model Integration）レベルを認定できる人・組織（SCAMPI（Standard CMMI Appraisal Method for Process Improvement）アプレイザー）を認定 ・成熟度の水準に応じて、評価者に求められる専門性が異なる	
	ISO 21500 （ISO：International Organization for Standardization）	プロジェクトマネジメントに係る国際規格を策定し、プロジェクトマネジメントの概念、及びプロセスに関する包括的な手引きを提供すること。	https://www.pmi-japan.org/topics/pmi1/pmbok5_2.php	プロジェクトマネジメントに係る包括的な概念と、プロセスについて、国際的な共通する理解を基本ガイドラインとしてまとめている。	・プロジェクトマネジメントの概念 ・プロジェクトマネジメントのプロセス	https://www.jisa.or.jp/it_info/engineering/tabid/1626/Default.aspx	ISO	ISO21500:2012	－	－	－	－	－	－	－
	ISO 10006 （ISO：International Organization for Standardization）	プロジェクトにおける品質マネジメントの指針として、ISO9001におけるプロジェクト部分を補完するためのガイドラインを提供する。	http://kikakurui.com/q/Q10006-2004-01.html	プロジェクトにおける品質マネジメントの手引きを提供し、品質マネジメントにおける原則、及び実践を概説する。	序文 1. 適用範囲 2. 引用企画 3. 定義 4. プロジェクトにおける品質マネジメントシステム 5. 経営者・管理者の責任 6. 資源の運用管理 7. 製品実現 8. 測定、分析及び改善	http://kikakurui.com/q/Q10006-2004-01.html	ISO	10006:2003	－ ※ISO9001に含まれるため，本基準単体での認証は無い	－	－	－	－	－		
	共通フレーム （ISO/IEC 12207:2008 の翻訳である JIS X 0160:2012 をベースとしている） （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission）	ソフトウェア、システム、サービスの構想から開発、運用、保守、廃棄に至るまでのライフサイクルを通じて必要な作業項目、役割などを包括的に定めたもので、システム開発を委託する際などに発注側と受注側の間に誤解が生じないように、汎用的な用語や各工程の内容（分類）を標準化する。	https://ja.wikiped	ソフトウェア、システム、サービスの構想から開発、運用、保守、廃棄に至るまでのライフサイクルを通じて必要な作業項目、役割等を包括的に規定した共通の枠組みを規定する。	第1部 共通フレームの必要性 第2部 共通フレーム概説 第3部 共通フレームとガイダンス 第4部 プロセス解説及び適用とテーラリング（修整）	https://www.ipa.go.	情報処理推進機構	2013年度版	－	－	－	－	－	－	－

評価基準・規格			評価基準・規格概要															評価者の要件	参考文献（評価者）
			目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）				
	運用	ISO/IEC20000 （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission）	サービスマネジメントシステムを調整のとれた形で統合し，かつ，実施することによって，継続的な管理，並びに継続的改善の機会，より高い有効性及び効率性を得ること。	JIS_Q_20000_001_2012 P1より	サービスマネジメントシステムを計画，確立， 導入，運用，監視，レビュー，維持及び改善するための，サービスの提供者に対する要求事項を規定する。	0.序文 1.適用範囲 2.引用規格 3.用語及び定義 4.サービスマネジメントシステムの一般要求事項 5.新規サービス又はサービス変更の設計及び移行プロセス 6.サービス提供プロセス 7.関係プロセス 8.解決プロセス 9.統合的制御プロセス	JIS_Q_20000_001_2012 P2より	ISO	ISO20000-1:2018	○	JIPDEC	ピューロベリタス等 （日本で8機関）	208	2018年3月末	https://www.jipdec	IEC/ISO20000（ITSMS）審査員と内部監査員 （ITSMS：Information technology-Service Management System）	http://certification.bureauveritas.jp/newsletter/071210/newsletter071210_jipdec.htm
		ITIL （Information Technology Infrastructure Library）	期待効果 ・環境変化への対応力向上 ・利用者の満足度向上 ・ビジネスのレジリエンス強化 ・サービス提供の費用対効果向上	http://www.itsmf-japan.org/aboutus/itil.html	ITサービスに関する仕事の内容、進め方、考え方など、幅広い知識と勘所の記述されたグローバルな共通言語・知識体系	＜フレームワーク＞ サービスデザイン サービストランジション サービスオペレーション サービスストラテジ 継続的サービス改善	http://www.itsmf-ja	英国商務省	v4 （2019年2月公開予定）	-	-	-	-	-	-	-	-
	セキュリティ一般	ISO27000シリーズ （ISO：International Organization for Standardization）	ISMS（Information Security Management System）の要求事項を定めた規格であり、組織がISMSを確立し、実施し、維持し、継続的に改善すること。 ※ISMS＝個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用すること。	https://isms.jp/is	組織の状況の下で，ISMS（Information Security Management System）を確立し，実施し，維持し，継続的に改善するための要求事項について規定する。この規格は，組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項についても規定する。 ※ISMS＝個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用すること。	0.序文 1.適用範囲 2.引用規格 3.用語及び定義 4.組織の状況 5.リーダーシップ 6.計画 7.支援 8.運用 9.パフォーマンス評価 10.改善	https://kikakurui.c	ISO	ISO27000:2018	○	ISMS-AC	以下ご参照ttps://	5,497	2018年3月末	https://www.jipdec	情報セキュリティマネジメントシステム審査員（ISMS審査員） （ISMS：Information Security Management System）	https://www.jsa.or.jp/datas/media/10000/md_3324.pdf
		情報セキュリティ管理基準	情報セキュリティマネジメントにおける管理策のための国際標準規格であるISO/IEC 17799:2000（JIS X 5080:2002）を基に、組織体の業種及び規模等を問わず汎用的に適用できるように、情報資産を保護するための最適な実践慣行を帰納要約し、情報セキュリティに関するコントロールの目的、コントロールの項目を規定したもの。 （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission） （JIS：Japanese Industrial Standards）	http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf	マネジメント基準と管理策基準として、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項、及び「管理策基準」として、組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を規定する。	Ⅰ．主旨 Ⅱ．本管理基準の位置づけ Ⅲ．構成 Ⅳ．マネジメント基準 Ⅴ．管理策基準	http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf	経済産業省	2018年度改正版	-	-	-	-	-	-	-	-
		ISO 22307(PIA) （ISO：International Organization for Standardization） （PIA：Privacy Impact Assessment）	個人情報の収集を伴う情報システムの企画、構築、改修にあたり、情報提供者のプライバシーへの影響を「事前」に評価し、情報システムの構築・運用を適正に行うことを促す一連のプロセスであり、設計段階からプライバシー保護策を織り込むことにより、「公共の利益」と「個人の権利」を両立させることを目的とする。	https://ja.wikipedia.org/wiki/%E3%83%97%E3%83%A9%E3%82%A4%E3%83%90%E3%82%B7%E3%83%BC%E5%BD%B1%E9%9F%BF%E8%A9%95%E4%BE%A1	システム開発の初期段階において実施すべきPIA（Privacy Impact Assessment）について要求事項を規定している。	＜PIAプロセスにおける要求事項＞ PIA計画 評価 PIA報告 PIA実施に必要な専門技能を持つ人の関与 公共的で独立した見地の関与 PIA結果を意思決定に用いることについての合意	https://ja.wikipedia.org/wiki/%E3%83%97%E3%83%A9%E3%82%A4%E3%83%90%E3%82%B7%E3%83%BC%E5%BD%B1%E9%9F%BF%E8%A9%95%E4%BE%A1	ISO	ISO27000:2008	- ※一部の海外では認定機関があるが，国内ではまだ未実施	-	-	-	-	-	-	-	-
		ISAE3000 （ISAE：International Standard on Assurance Engagements）	国際監査基準(ISA：International Standards on Auditing)及び国際レビュー業務基準(ISRE：International Standard on Review Engagements)で取り扱われている、過去財務情報の監査又はレビュー以外の保証業務に適用される。（CSR報告書や持続可能性報告書に記載される環境パフォーマンス指標や社会パフォーマンス指標に係る保証業務が多い） 保証業務には、業務実施者以外の者が規準に照らして主題を測定又は評価する場合の証明業務と、業務実施者が規準に照らして主題を測定又は評価する場合の直接業務の両方が含まれている。本基準は合理的保証業務及び限定的保証業務の証明業務並びに業務状況に応じた直接業務に対し適用される。	https://jicpa.or.jp/specialized_field/20180606ufe.html	目的欄参照のこと	序説 範囲 目的 要求事項 適用及びその他の説明指針 など	https://jicpa.or.jp	国際監査・保証基準審議会（IAASB）	2018年改訂版	○	第三者機関（監査補人など）	同左	不明 （CSR（Corporate Social Responsibility）報告書や統合報告書の開示企業数におおよそ相当）	-	-	・保証対象の情報を理解し、レビューするために必要な知識、スキル及び力量を有していること ・独立性を確保する上でIFACの倫理規則（IFAC Code of Ethics for Professional Accountants）を遵守すること （IFAC：International Federation of Accountants）	-

評価基準・規格			評価基準・規格概要											評価者の要件	参考文献（評価者）
			目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）		
セキュリティ	サイバーセキュリティ	ISO/IEC 27101シリーズ （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission）	サイバーセキュリティ枠組みの策定、サイバー保険の利用、及び既存の企画（（ISO：International Organization for Standardization/IEC：International Electrotechnical Commission）をサイバーセキュリティフレームワークに活用するためのガイドラインを提供することを目的とする。	https://isms.jp/27000family/27000family_20180620.pdf	サイバーセキュリティに係るフレームワーク策定におけるガイドラインを提供する。	＜ISO 27101＞ 5 Overview 6 Concepts 6.1 Identify 6.2 Protect 6.3 Detect 6.4 Respond 6.5 Recover	http://www.iso27001security.com/html/27101.html	ISO	- ※現在作成中	-	-	-	-	-	-	-	-
		NIST CyberSecurity Framework （NIST：National Institute of Standards and Technology）	重要インフラ事業者・運営者におけるサイバーセキュリティに係るリスクマネジメントを改善するためのフレームワークを提供する。	https://www.ipa.go.jp/files/000071204.pdf	サイバーセキュリティに係るリスクマネジメントの観点より、フレームワークの基本理念、使い方、及びセルフアセスメントの実施手順を規定する。	・フレームワークの照会 ・フレームワークの基本的な考え方 ・フレームワークの使い方 ・フレームワークを利用したサイバーセキュリティリスクの自己アセスメント	https://www.ipa.go.jp/files/000071204.pdf	NIST	Ver1.1	-	-	-	-	-	-	-	-
		政府機関の情報セキュリティ対策のための統一基準	共通的に必要とされる情報セキュリティ対策であり、政府機関等の情報セキュリティ対策のための統一規範（サイバーセキュリティ戦略本部決定）に基づく機関等における統一的な枠組みの中で、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（以下「遵守事項」という。）を規定することにより、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。	https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf	機関等が行うべき対策について、目的別に部、節及び款の３階層にて対策項目を分類し、各款に対して目的及び趣旨並びに遵守事項を示している。	第1部　総則 第2部　情報セキュリティ対策の基本的枠組み 第3部　情報の取扱い 第4部　外部委託 第5部　情報システムのライフサイクル 第6部　情報システムのセキュリティ要件 第7部　情報システムの構成要素 第8部　情報システムの利用	https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf	サイバーセキュリティ対策本部（NISC）	平成30年度改訂版	-	-	-	-	-	-	-	-
		重要インフラにおける情報セキュリティ確保係る安全基準など策定指針	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・記載することによって、「安全基準等」の策定・改定を支援することを目的としている。	https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf	重要インフラ事業者等が自主的な取組や継続的な改善を行う際に参照しやすいよう、情報セキュリティの対策項目をＰＤＣＡサイクルに沿って記載している。	１．目的及び位置づけ １．１　重要インフラにおける情報セキュリティ対策の重要性 １．２　「安全基準等」とは何か １．３　指針の位置づけ １．４　指針を踏まえた「安全基準等」の継続的改及び浸透への期待 ２．「安全基準等」で規定が望まれる項目 ２．１　策定目的 ２．２　対象範囲 ２．３　関係主体の役割 ２．４　対策項目	https://www.nisc.go.jp/active/infra/pdf/shishin5.pdf	NISC	第5版	-	-	-	-	-	-	-	-
		サイバーセキュリティ経営ガイドライン	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対する適切な投資が行われ、企業のサイバーセキュリティ対策強化が行われることを最大の目的としている。	http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf	大企業及び中小企業（小規模事業者を除く）の経営者を対象 として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者が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（CISO：Chief Information Security Officer 等）に指示すべき「重要１０項目」を記載している。	１．はじめに ２．経営者が認識すべき3原則 ３．サイバーセキュリティ経営の重要１０項目	http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf	経済産業省	Ver.2.0	-	-	-	-	-	-	-	-
		サイバーフィジカルセキュリティ対策フレームワーク（案）	IoTやAIによって実現される「Society5.0」、「Connected Industries」におけるサプライチェーン全体のサイバーセキュリティ確保を目的としたもの。	http://www.meti.go	サイバー空間とフィジカル空間が融合することで新たな価値を生み出していく「Society5.0」における産業社会では、一方で、サイバー攻撃の起点が拡大するとともに、サイバー攻撃による被害がフィジカル空間に及ぼす影響も増大し、これまでとは異なる新たなリスクを伴うことになる。本フレームワークは、新たな産業社会におけるこうした環境において、付加価値を創造する活動が直面する新たなリスクに対応していくための指針を示すものである。	フレームワークの全体構成 第Ⅰ部（コンセプト）では、バリュークリエイションプロセスにおけるサイバーセキュリティの観点からリスク源を整理するためのモデル(三層構造アプローチと６つの構成要素)と基本的なリスク認識、それに対するアプローチを、信頼性の確保という形で整理する。 第Ⅱ部（ポリシー）では、第Ⅰ部で示したモデルを活用して、リスク源を整理するとともに、こうしたリスク源に対応する対策要件を提示する。 第Ⅲ部（メソッド）では、第Ⅱ部で示した対策要件を対策の種類に応じて整理し、更に、付録の形で、セキュリティの強度を踏まえて分類した対策例を示す。	http://www.meti.go.	経産省	現段階では案。 2019年1月9日リリース http://www.meti.go.jp/press/2018/01/20190109001/20190109001-2.pdf	-	-	-	-	-	-	-	-
		ISO/IEC 27030 （ISO：International Organization for Standardization） （IEC：International Electrotechnical Commission）	IoT（Internet of Things）のセキュリティとプライバシーに係る原則、及びリスク管理に係る国際標準規格を提供し、IoTの設計、製造者、及び利用者に、IoT（Internet of Things）に係るサイバーセキュリティリスクへの認識を向上させ、リスク管理における成熟度を向上させることを目的とする。	http://www.iso27001security.com/html/27030.html	- ※現時点でDraft版となり、内容の詳細までは公開されていない	- ※現時点でDraft版となり、内容の詳細までは公開されていない	http://www.iso27001security.com/html/27030.html	ISO	- ※現時点でDraft版となる	-	-	-	-	-	-	-	-

評価基準・規格		評価基準・規格概要												評価者の要件	参考文献（評価者）
		目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）		
IoTセキュリティ（Internet of Things）	IoTセキュリティガイドライン （IoT：Internet of Things）	IoT（Internet of Things） 機器やシステム、 サービスについて、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3 を基本原則としつつ明確化するものである。これによって、産業界による積極的な開発等の取組を促すとともに、利用者が安心して IoT（Internet of Things）機器やシステム、サービスを利用できる環境を生み出すことにつなげること。	http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf	IoT（Internet of Things）機器・システム、サービスの供給者である経営者、機器メーカ、システム提供者・サービス提供者（一部、企業利用者を含む）を対象とした IoT（Internet of Things）セキュリティ対策の５指針、及び利用者向けの注意事項を記載している。	第1章　背景と目的 第2章　IoTセキュリティ対策の5つの指針 第3章　一般利用者のためのルール 第4章　今後の検討事項	http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf	IoT推進コンソーシアム/総務省/経済産業省	Ver1.0	－	－	－	－	－	－	－	－
	STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS	IoT（Internet of Things）機器の開発・製造・実装・使用時におけるセキュリティ検討、及び関連するステークホルダーに対するベストプラクティスを提供することを目的とする。	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf	IoT（Internet of Things）機器のセキュリティに関する戦略的原則、及び関連するベストプラクティスを記載している。	＜戦略的原則＞ 設計段階からセキュリティを組み込むこと 脆弱性管理およびセキュリティアップデートを行うこと 確立されたセキュリティ対策を採用すること 想定される影響に応じ、優先度をつけてセキュリティ対策を行うこと IoT全体において透明性を促進すること ネットワーク接続には注意を重ね、慎重に検討すること	https://www.ipa.go.jp/files/000057264.pdf	米国土安全保障省	Ver1.1	－	－	－	－	－	－	－	－
	Security Guidance for Early Adopters of the Internet of Things	IoT（Internet of Things）機器の導入において、各業界での実装要件に応じたセキュリティ評価を行うための、基本的なセキュリティコントロール群を提供することを目的とする。	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf	IoT（Internet of Things）機器におけるセキュリティ対策について、「端末」、「ゲートウェイ/アプリケーション」、「エンタープライズ・コンピューティング/クラウド/データ分析」の大きく3つに分類し、セキュリティの手引きを記載している。	1. Introduction 2. Purpose 3. IoT Threats to Individuals and Organizations 4. Challenges to Secure IoT Deployments 5. Recommended Security Controls 6. Future Efforts	https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf	CSA（Cloud Security Aliance）	2015/April	－	－	－	－	－	－	－	－
	Industrial Internet Security Framework		https://www.iicons	クラウドから通信経路、プロトコルなどIoT（Internet of Things）を構成する様々な要素において想定すべきリスクと対策の概論を提供する。 なお、実用的な対策群については、実証実験による結果を別途IIC（ Industrial Internet Consortium）メンバー向けに公開している。	1 Overview 2 Motivation 3 Key System Characteristics Enabling Trustworthiness 4 Distinguishing Aspects of Securing the IIoT 5 Managing Risk 6 Permeation of Trust in the IIoT System Lifecycle 7 IISF Functional Viewpoint 8 Protecting Endpoints 9 Protecting Communications and Connectivity 10 Security Monitoring and Analysis 11 Security Configuration and Management 12 Looking Ahead–The Future of the IIoT	https://www.iiconsortium.org/IISF.htm	インダストリアル・インターネット・コンソーシアム	2016年9月版	－	－	－	－	－	－	－	－
制御系	制御機器認証プログラム(EDSA)マネジメントシステム（IEC 62443-4-1/4-2） （EDSA：Embedded Device Security Assurance）	国際計測制御学会のメンバーを中心としたISCS(ISA Security Compliance Institute)が開発した制御機器認証プログラム(EDSA：Embedded Device Security Assurance)に係る認証制度。主に製品向け。	http://www.cssc-cl	以下3つの評価項目で構成される。 ①：ソフトウェア開発の各フェーズにおけるセキュリティ評価(SDSA：Software Development Security Assessment) ②：セキュリティ機能の実装評価(FSA：Functional Security Assessment) ③：通信の堅牢性テスト(CRT：Communication Robustness Testing)	同左	http://www.cssc-cl.	ISO/IEC	2010年	○	ISO/IEC	技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center ）	5社程度	2017年	－	特になし （特定の認証機関にのみ認証権限が付与されている）	－
	制御系システムのセキュリティマネジメントシステム（IEC 62443-2-1：CSMS適合性評価制度） （CSMS：Cyber Security Management System）	国際電気標準会議（IEC：International Electrotechnical Commission）が、IEC 62443に基づき、制御システムの製造やオペレーションを行う企業がセキュリティに関して取り組むべき組織マネジメントについて規定した国際標準（IEC 62443-2-1）、 制御系システムのセキュリティマネジメントシステムに係る認証基準。	https://isms.jp/csm	基本的にISMS（Control System Security Center ）に加え、制御系システム固有の項目が追加された構成	同左	https://isms.jp/csm	ISO/IEC	2010年	○	ISO/IEC	・一般財団法人日本品質保証機構 ・BSIグループジャパン株式会社	6社程度	2018年12月	https://isms.jp/c	特になし （特定の認証機関にのみ認証権限が付与されている）	－
	金融機関などコンピュータシステムの安全対策基準・解説書FISC （FISC：Center for Financial Industry Information Systems）	金融庁が金融機関のシステム管理体制を検査する際に使用する、金融システムの導入・運用に係る業界標準ガイドラインを提供することを目的とする。	https://www.fisc.or.jp/publication/『金融機関等コンピュータシステムの安全対策基準（第9版）』（解説書、FISCガイドライン検索システム）	金融システムの導入・運用に係るガイドラインとして、「統制」「実務」「設備」「監査」の4つに分類し、業界標準のガイドラインを提供している。 第9版では、FinTechやクラウドによるビジネス環境の変化に対応し、旧基準（第8版）の分類「技術」「運用」「設備」から見直されている。	＜基準分類＞ ・統制（1～26） ・監査(1) ・実務（1～141） ・設備（1～137）	https://www.fisc.or.jp/publication/『金融機関等コンピュータシステムの安全対策基準（第9版）』（解説書、FISCガイドライン検索システム）	FISC	第9版	－	－	－	－	－	－	－	－
	PCIデータセキュリティスタンダード (PCI-DSS：Payment Card Industry Data Security Standard)	クレジットカード情報のセキュリティを強化するために、クレジット業界におけるグローバルセキュリティー基準を提供することを目的とする。	https://ja.pcisecuritystandards.org/minisite/env2/	カード会員データのセキュリティの強化、及びデータの保護に係る技術面・運用面の要件のベースラインとして6つの要件（詳細は12つ）を提供する。	＜PCIデータセキュリティ基準 - 概要＞ 安全なネットワークとシステムの構築と維持 カード会員データの保護 脆弱性管理プログラムの維持 強力なアクセス制御手法の導入 ネットワークの定期的な監視およびテスト 情報セキュリティポリシーの維持	https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3%202_JA-JP_20180801.pdf	PCI SSC	v3.2.1	○	PCI-CSS	NRIセキュアテクノロジーズ株式会社等 ※QSA（Qualified Security Assessors:認定審査機関）	参考文献欄参照	2018年9月時点	https://www.jcdsc.org/qsa-asv.php	PCI SSC（Payment Card Industry Data Security Standard）が認定した審査機関（QSA）、及びセキュリティベンダー（ASV）であることが求められる。	－

評価基準・規格		評価基準・規格概要												評価者の要件	参考文献（評価者）
		目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）		
金融	製品分野別セキュリティガイドライン：金融端末（ATM）分野（重要生活機器連携セキュリティ協議会）CCDS（CCDS：Connected Consumer Device Security Council）	重要生活機器を利用者が安全・安心に利用できる環境を実現するため、重要生活機器のセキュリティ技術に関するガイドラインや標準化の検討、普及啓発を行い、産業発展・新規事業創造・国民生活の向上に寄与することを目的とする。 ※当該評価基準は重要生活機器のうち、ATM（Automatic Teller Machine）に関する基準	https://www.ccds.or.jp/about/index.html	過去に発生したATM（Automatic Teller Machine）に係る犯罪手口等を踏まえ、ATM（Automatic Teller Machine）に係る具体的なセキュリティ対策を必要となる対策案や影響分析等をベースリアンを提供する。	1 前書き 2 セキュリティ対策立案手順 2.1 犯罪事例分析と対策案リストアップ 2.2 対策の業務への影響分析 2.3 対策案の比較評価 2.4 未出現犯罪に対する適用拡張 3 まとめ 付録 リスク評価式 参考文献	https://www.ccds.or.jp/public/document/other/guidelines/[CCDS]ATM%E7%B7%A8%E5%88%A5%E5%86%8A_%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%A4%E3%83%86%E3%82%A3%E5%AF%BE%E7%AD%96%E6%A4%9C%E8%A8%8E%E5%AE%9F%E8%B7%B5%E3%82%AC%E3%82%A4%E3%83%89_Ver1.0.pdf	一般社団法人重要生活機器連携セキュリティ協議会	Ver.1.0	－	－	－	－	－	－	－	－
	製品分野別セキュリティガイドライン：オープン分野CCDS（CCDS：Connected Consumer Device Security Council）	重要生活機器を利用者が安全・安心に利用できる環境を実現するため、重要生活機器のセキュリティ技術に関するガイドラインや標準化の検討、普及啓発を行い、産業発展・新規事業創造・国民生活の向上に寄与することを目的とする。 ※当該評価基準は重要生活機器のうち、オープンPOS（Point Of Sales）に関する基準	https://www.ccds.or.jp/about/index.html	オープンPOS（Point Of Sales）を導入・運用するにあたり、システム構成・運用モデル、セキュリティ上の脅威とその対策等のガイドラインを提供する。	1 はじめに 2 システム構成と運用モデル 3 想定されるセキュリティ上の脅威 4 セキュリティ対策指針 5 開発フェーズとセキュリティの取組み 6 まとめ 参考文献	https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%A4%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%AA%E3%83%BC%E3%83%97%E3%83%B3POS%E7%B7%A8_Ver2.0.pdf	一般社団法人重要生活機器連携セキュリティ協議会	Ver.2.0	－	－	－	－	－	－	－	－
	xxxx事業者向けの総合的な監督指針	各事業者に対して、監督事務の基本的考え方、監督上の評価項目、事務処理上の留意点について、体系的に整理し、必要な情報を極力集約したオールインワン型の行政部内の職員向けの手引書を提供することを目的とする。	https://www.fsa.go.jp/common/law/index.html	各事業者向けに監督指針・事務ガイドラインを提供する。	＜監督指針＞ 主要行等向けの総合的な監督指針 中小・地域金融機関向けの総合的な監督指針 保険会社向けの総合的な監督指針 少額短期保険業者向けの監督指針 認可特定保険業者向けの総合的な監督指針 金融商品取引業者等向けの総合的な監督指針　など	https://www.fsa.go.jp/common/law/index.html	金融庁	※各事業者向けの監督指針により異なる	－	－	－	－	－	－	－	－
	FFIEC Cyber Security Assesment Tool（Federal Financial Institutions Examination Council）	NIST（National Institute of Standards and Technology：米国国立標準技術研究所）が定めているサイバーセキュリティを強化するためのフレームワークであり、金融機関がサイバーセキュリティ対策を実施する際のアセスメントツールを提供することを目的とする。	https://www.ffiec.gov/cyberassessmenttool.htm	サイバーセキュリティの成熟度評価として、右記の5つの領域に対して、固有リスクのレベルと成熟度のレベルをそれぞれ5段階で評価フレームワークを提供する。	領域 1：サイバーリスクの管理と監督 領域 2：脅威情報の収集と共有 領域 3：サイバーセキュリティ統制 領域 4：外部依存関係の管理領域 領域5：サイバーインシデント管理とレジリエンス	https://www.fsa.go.jp/common/about/research/20160815-1/01.pdf	FFICE	May 2017. 1	－	－	－	－	－	－	－	－
	金融機関等コンピュータシステムのシステム監査基準	金融機関等のシステム監査導入と推進のための業界標準ガイドラインを提供することを目的とする。	https://www.fisc.or.jp/publication/『金融機関等のシステム監査指針（改訂第3版追補）』（解説書、FISCガイドライン検索システム）	金融システムのシステム監査、導入に係る要素を13項目に分類し、ガイドラインを提供する。	＜要素＞ 1.情報システムの計画と管理 2.情報システムリスクの管理 3.情報セキュリティ 4. システム開発 5.システム運用 6.システム利用 7.入出力等の処理 8.ネットワーク 9.システム資産・資源管理 10.外部委託 11.コンティンジェンシープラン 12. ドキュメンテーション 13. クラウドサービスの利用	https://www.fisc.or.jp/publication/『金融機関等のシステム監査指針（改訂第3版追補）』（解説書、FISCガイドライン検索システム）	FISC	改訂第3版追補	－	－	－	－	－	－	－	－
電力	JESC Z0004（JESC：Japan Electrotechnical Standards and Codes Committee）	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規定することを目的とする。	http://www.jesc.gr.jp/jesc-assent/private/jesc_Z0004_00.html https://www.nisc.go.jp/conference/cs/ciip/dai07/pdf/07shiryou0601.pdf	電力制御システムにおけるサイバーセキュリティ対策として、ファシリティ面、運用・管理面、また、セキュリティ事故が発生した場合のガイドラインを提供する。	第1章　総則 第2章　組織 第3章　文書化 第4章　セキュリティ管理 第5章　設備・システムのセキュリティ 第6章　運用・管理のセキュリティ 第7章　セキュリティ事故の対応	https://www.denki.or.jp/wp-content/uploads/2016/07/d20160707.pdf	JESC（Japan Electrotechnical Standards and Codes Committee：日本電気技術規格委員会）	2016年版	－	－	－	－	－	－	－	－
	JESCZ0003（JESC：Japan Electrotechnical Standards and Codes Committee）	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、スマートメーターシステムの設計調達段階から保守運用段階までの一連の工程における、セキュリティ対策の要求事項を規定することを目的とする。	http://www.jesc.gr.jp/jesc-assent/private/jesc_Z0003_00.html	スマートメーターシステムにおけるサイバーセキュリティ対策として、セキュリティ管理、機器・通信・システムに係るセキュリティ対策、また運用面のセキュリティに関するガイドラインを提供する。	第1章　総則 第2章　組織 第3章　文書化 第4章　セキュリティ管理 第5章　機器のセキュリティ 第6章　通信のセキュリティ 第7章　システムのセキュリティ 第8章　運用のセキュリティ	https://www.denki.or.jp/wp-content/uploads/2016/07/s20160609.pdf	JESC（（JESC：Japan Electrotechnical Standards and Codes Committee）：日本電気技術規格委員会）	2016年版	－	－	－	－	－	－	－	－
	ISO 26262（ISO：International Organization for Standardization）	社会が許容する安全性とのバランスを確保する為にIEC 61508で国際規格化されていた機能安全の考え方を自動車産業に適用する為に策定された。（IEC：International Electrotechnical Commission）	https://ja.wikipedia.org/wiki/ISO_26262	自動車に搭載されているセンサー等の電子機器などのハードウェア、ソフトウェアを対象に、自動車の構想段階から廃車に至るまでのライフサイクル全体で機能安全の考え方を記載している。	１．用語 ２．機能安全の管理 ３．コンセプトフェーズ ４．製品開発：システムレベル ５．製品開発：ハードウェアレベル ６．製品開発：ソフトウェアレベル ７．生産、運用、廃棄 ８．サポートプロセス ９．ASIL １０．ガイドライン	https://monoist.atmarkit.co.jp/mn/articles/1108/30/news002.html	ISO		○	JQA等	－	品質安全マネジメント認証：2社 機能安全マネジメント認証：1社 ※第三者認証機関により公開されているため、上記はJQA（Japan Quality Assurance）の場合	2019年2月時点	－	特になし（公認内部監査員制度を持たない）	https://www.tuv-sud.jp/jp-jp/press-media-centre/news-archive-1/201808-iso-26262

評価基準・規格			評価基準・規格概要															評価者の要件	参考文献（評価者）
			目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）				
セキュリティ（インダストリー別）	自動車	製品分野別セキュリティガイドライン：車載分野CCDS（CCDS：Connected Consumer Device Security Council）	IPAにて検討、公開されたは「つながる世界の開発指針～安全安心な IoT（Internet of Things）の実現に向けて開 発者に認識してほしい重要ポイント」について、個々の製品分野（車載機）における具体的なセーフティとセキュリティをカバーした設計・開発を進めるためのガイドラインを提供すること。	https://www.ccds.or.jp/public/document/other/guideline s/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E8%BB%A4%E8%BC%89%E5%99%A8%E7%B7%A8_Ver2.0.pdf	車載機器において適切なセキュリティ対策を実施するための、設計から製品リリース後までに考慮すべき設計・開発プロセスをガイドラインとしてまとめている。	1 はじめに 2 車載ガイドラインのシステムモデル 3 想定されるセキュリティ上の脅威 4 ライフサイクルのフェーズとセキュリティの取組み 5 脅威分析について 6 リスク評価の方法 7 リスク評価の結果 8 リスク評価の傾向分析 9 まとめ 10 「つながる世界の開発指針」と本書との関係 11 「自動車の情報セキュリティへの取組みガイド」と本書との関係 12 「IOT セキュリティガイドライン」と本書との関係	https://www.ccds.or.jp/public/document/other/guideline s/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E8%BB%A4%E8%BC%89%E5%99%A8%E7%B7%A8_Ver2.0.pdf	一般社団法人重要生活機器連携セキュリティ協議会	V2.0	－	－	－	－	－	－	－	－
		Postmarket Management of Cybersecurity in Medical Devices	医療機器の製造業者が、サイバーセキュリティにおいて対応が必要な事項について、FDA（Food and Drug Administration）としての推奨事項をガイドラインとして提供するもの。	https://www.fda.go	医療機器に係るサイバーセキュリティのリスク管理、コントロール等のフレームワークを提示する。	I.　INTRODUCTION II.　BACKGROUND III.　SCOPE IV.　DEFINITIONS V.　GENERAL PRINCIPLES VI.　MEDICAL DEVICE CYBERSECURITY RISK MANAGEMENT VII.　REMEDIATING AND REPORTING CYBERSECURITY VULNERABILITIES VIII. RECOMMENDED CONTENT TO INCLUDE IN PMA PERIODIC REPORTS IX.　CRITERIA FOR DEFINING ACTIVE PARTICIPATION BY A MANUFACTURER IN AN ISAO X.　APPENDIX: ELEMENTS OF AN EFFECTIVE POSTMARKET CYBERSECURITY PROGRAM	https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf	FDA（米国）	2016年度末版	－	－	－	－	－	－	－	－
		医療情報システムの安全管理に関するガイドライン	「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」、「診療録等の外部保存に関するガイドライン」の見直し、及び個人情報保護に資する情報システムの運用管理に関わる指針とe-文書法への適切な対応を行うための指針を統合的に提供することを目的としている。	https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf	医療情報システムの安全管理やe-文書法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ている。	1 はじめに 2 本指針の読み方 3 本ガイドラインの対象システム及び対象情報 4 電子的な医療情報を扱う際の責任のあり方 5 情報の相互運用性と標準化について 6 情報システムの基本的な安全管理 7 電子保存の要求事項について 8 診療録及び診療諸記録を外部に保存する際の基準 9 診療録等をスキャナ等により電子化して保存する場合について 10 運用管理について	https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf	厚生労働省	第5版	－	－	－	－	－	－	－	－
	医療	HISPRO適合性評価（ 支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス） （HISPRO：Health Information Security Performance Rating Organization） （Ipsec：Security Architecture for Internet Protocol） （IKE：Internet Key Exchange）	保健医療福祉の各分野において、国の提唱する「医療情報システムの安全管理に関するガイドライン」に基づいた 安全な情報基盤を効率よく実現することを目的とする。 補足： サービス提供事業者による各種製品・サービスの紹介・説明に下記マーク（※）が付けられたものは、当協会により該当する安全管理ガイドライン（厚生労働省、経済産業省、総務省発行）への適合性が評価済であることを表す。 ※ HISPRO HSP-C-Cxxxx-20xx	http://www.hispro.(	評価指針は右記の通り。 http://www.hispro.or.jp/open/pdf/20090915shinseihoushin.pdf#toolbar=0	①接続中継地点がある場合は電気通信事業法に従い、事業の届出を行っている事業者であること ②評価対象となるサービスの契約書およびサービス仕様書が提示されていること ③サービスの提供範囲、責任範囲が明確になっていること ④顧客情報を適切に管理することが明文化されていること ⑤サービス拠点の物理セキュリティや災害に対する対応が明確になっていること ⑥サービス設備のセキュリティが確保されていること ⑦サービス設備のシステム障害などを考慮した BCP（business continuity plan）が確立していること ⑧システム監視や障害発生時の連絡方法、故障復旧体制について記述されていること ⑨合意された内容に沿った通信設定がされていること（通信の合意をしていない拠点との通信やアクセスができないようになっていること）が明確になっていること ⑩暗号化通信において適正な技術を適用していること ⑪サービスに使用する医療機関の終端装置の製品情報および仕様が明確になっていること ⑫医療機関のセキュリティを守るために終端装置の設置個所から医療機関外までの セキュリティ対策実施を喚起していること	「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」チェックリスト項目集 http://www.hispro.or.jp/open/pdf/20090915shinseihoushin.pdf#toolbar=0	一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）	評価手順・指針、およびチェックリストは以下のとおり。 評価手順・指針 http://www.hispro.or.jp/open/pdf/20090915shinseihoushin.pdf#toolbar=0 チェックリスト http://www.hispro.or.jp/open/pdf/20090915shinseihoushin.pdf#toolbar=0	○	一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）	－	※組織ではなくサービス（システム）単位。認定サービスは以下にて閲覧可能 http://www.hispro.or.jp/open/kekka.htm	－	－	評価者は、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）のみ	http://www.hispro.or.jp/open/outline.htm
		HISPRO適合性評価（ 民間事業者による医療情報の外部保存及びASP・SaaSサービス） （HISPRO：Health Information Security Performance Rating Organization） （ASP：Application Service Provider） （SaaS：Software as a Service）	保健医療福祉の各分野において、国の提唱する「医療情報システムの安全管理に関するガイドライン」に基づいた 安全な情報基盤を効率よく実現することを目的とする。 補足： サービス提供事業者による各種製品・サービスの紹介・説明に下記マーク（※）が付けられたものは、当協会により該当する安全管理ガイドライン（厚生労働省、経済産業省、総務省発行）への適合性が評価済であることを表す。 ※	http://www.hispro.(	評価の視点は右記の通り。 http://www.hispro.or.jp/open/pdf/201212ASPSaaSshinseihoushin.pdf#toolbar=0	３．評価の視点 １）協会は利用者代わって評価する立場 利用者に開示する情報が評価対象になる。 ２）ISMS 又はP マークの第三者認証を取得が条件 当協会の確認は、ガイドラインの要求事項に対する対策内容と申請者内部の審査者が何をもって確認したか、適切なエビデンスであるかの確認。 対策内容の実施の現場確認自体の責任は申請者内の審査者側にあるとの整理。 ３）医療機関とのSLA やサービス契約書事項の雛型文書が評価対象 「責任分界点の説明」と「利用者へのセキュリティ遵守事項説明」の利用者へ提供。 代理店を通す場合には誰が責任を持って行うのかの規定化が必須。 ４）評価は原則書類審査 エビデンスの実在性が疑われる場合、あるいは審査者の審査の実行性が確認出来ない場合は立入調査もありえる。また、2 年後の更新評価でサービス利用者としての医療機関等の利用環境等への立ち入り、その実効性を評価する場合がある。 ５）「HISPRO 評価」の標榜表現の評価 評価申請者であるサービス提供者が「HISPRO 評価」を標榜するならば、その文章を申請時添付する。HISPRO による評価範囲と齟齬がないか、記載が明確であることを評価する。	「民間事業者による医療情報の外部保存及びＡＳＰ・ＳａａＳサービス」チェックリスト項目集 http://www.hispro.or.jp/open/pdf/201212ASPSaaS%20koumoku.pdf#toolbar=0	一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）	2012年12月 評価手順・指針、およびチェックリストは以下のとおり。 評価手順・指針 http://www.hispro.or.jp/open/pdf/201212ASPSaaS%20koumoku.pdf#toolbar=0 チェックリスト http://www.hispro.or.jp/open/pdf/201212ASPSaaS%20koumoku.pdf#toolbar=0	○	一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）	－	※組織ではなくサービス（システム）単位。認定サービスは以下にて閲覧可能 http://www.hispro.or.jp/open/kekka-gaibu.htm	－	－	評価者は、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）のみ	http://www.hispro.or.jp/open/outline.htm

評価基準・規格		評価基準・規格概要												評価者の要件	参考文献（評価者）
		目的	参考文献（目的）	規定内容	目次	参考文献（規定内容）	作成主体	最新Ver.	認証基準	認定機関	認証機関	認定取得組織数	集計時点	参考文献（組織数）	
	IEC 60601 （IEC：International Electrotechnical Commission）	医療用電気機器において、安全確保に必要となる一般要求事項を規定し，個別規格に対する基礎を与えること。 ※個別企画（各医療電子機器ごとの企画）は、IEC60601-2-33などで規定されている。 （IEC：International Electrotechnical Commission） HISPRO HSP-C-Cxxxx-20xx	https://webstore.iec.ch/publication/2603	医療用電子機器における基礎安全と基本性能に関する一般要求事項を規定している。	1 適用範囲，目的及び関連規格 2 引用規格 3 用語及び定義 4 一般要求事項 5 ME 機器の試験に対する一般要求事項 6 ME 機器及び ME システムの分類 7 ME 機器の標識，表示及び文書 8 ME 機器の電気的ハザードに関する保護 9 ME 機器及び ME システムの機械的ハザードに関する保護 10 不要又は過度の放射のハザードに関する保護 11 過度の温度及び他のハザードに関する保護 12 制御及び計器の精度並びに危険な出力に対する保護 13 ME 機器の危険状態及び故障状態 14 プログラマブル電気医用システム（PEMS） 15 ME 機器の構造 16 ME システム 17 ME 機器及び ME システムの電磁両立性	http://www.kanrigakkai.jp/housyasen/shiryou/img/26-00.pdf	IEC	60601-1:2018	○	IEC	JQA（Japan Quality Assurance：日本品質機構）など	※組織ではなく製品単位となり、製品数は不明。 認定製品は以下にて閲覧可能 https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0026.html	－	－	IECに基づく	－
	ISO 14971 （ISO：International Organization for Standardization）	医療機器のリスク管理に関する国際的基準であり、医療機器に係るリスクマネージメントプロセスの設立、文書化、維持を目的としている。	http://kikakurui.com/t14/T14971-2012-01.html	製造業者が体外診断用医療機器を含む医療機器に関連するハザードを特定し，リスクの推定及び評価を行い，これらのリスクをコントロールし，そのコントロールの有効性を監視する手順について規定している。	0. 序文 1. 適用範囲 2. 用語及び定義 3. リスクマネジメントの一般要求事項 4. リスク分析 5. リスク評価 6. リスクコントロール 7. 残留リスクの全体的な受容可能性の評価 8. リスクマネジメント報告書 9. 製造及び製造後情報	http://kikakurui.com/t14/T14971-2012-01.html		ISO14971:2007	－	－	－	－	－	－	－	－
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	各事業分野（鉄道、物流、航空、空港）において、その特性に応じた必要又は望ましい情報セキュリティの水準を明示し、個々の事業者が、重要インフラの担い手としての意識に基づいて自主的な取り組みにおける努力や検証をするための目標を定めること	http://www.mlit.go.jp/common/001127563.pdf	各事業分野（鉄道、物流、航空、空港）において、分野横断的に有効な対策項目及び対策の例示に加え、各分野における情報セキュリティ対策の現状と課題を踏まえ、安全ガイドラインとして事業特性に応じた対策項目を推奨基準としてまとめている。	1. 「安全ガイドライン」策定の背景 2. 鉄道分野における「安全ガイドライン」の概要 3. 鉄道分野における「安全ガイドライン」の対象範囲等 4. 推奨される対策項目 5. 参考文献 6. 用語集	http://www.mlit.go.jp/common/001127563.pdf	国土交通省	第3版	－	－	－	－	－	－	－	－
物流	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	※「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」と同様	http://www.mlit.go.jp/common/001127564.pdf	※「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」と同様	1. 「安全ガイドライン」策定の背景 2. 物流分野における「安全ガイドライン」の概要 3. 「安全ガイドライン」の対象範囲等 4. 推奨される対策項目 5. 参考文献 6. 用語集	http://www.mlit.go.jp/common/001127564.pdf	国土交通省	第3版	－	－	－	－	－	－	－	－
航空	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	※「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」と同様	http://www.mlit.go.jp/common/001127526.pdf	※「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」と同様	1. 「安全ガイドライン」策定の背景 2. 航空分野における「安全ガイドライン」の概要 3. 航空分野における「安全ガイドライン」の対象範囲等 4. 推奨される対策項目 5. 参考文献 6. 用語集	http://www.mlit.go.jp/common/001127526.pdf	国土交通省	第4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	※「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」と同様	http://www.mlit.go.jp/common/001229687.pdf	※「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」と同様	1. 「安全ガイドライン」策定の背景 2. 空港分野における「安全ガイドライン」の概要 3. 空港分野における「安全ガイドライン」の対象範囲等 4. 推奨される対策項目 5. 参考文献 6. 用語集	http://www.mlit.go.jp/common/001229687.pdf	国土交通省	第1版	－	－	－	－	－	－	－	－
水道	水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	水道事業者が自ら実施する情報セキュリティ対策の参考となるような考えられる措置を示すことに加えて、水道事業者の情報セキュリティに対する現状認識や今後必要となる対策のレベルへの理解を深めることを意図したもの。	https://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000046638.pdf	水道事業者が情報セキュリティ対策を行うため、組織、体制、資源等も含めた観点より、情報セキュリティ対策を行うことの趣旨、及び具体的な実施内容について記載している。	1 総則 2 組織・体制及び資源の対策 2.1 組織・体制及び人的資源の確保 2.2 情報セキュリティ人材の育成等 2.3 外部監査等による情報セキュリティ対策の評価 3 情報セキュリティ対策 3.1 情報についての対策 3.2 情報セキュリティ要件の明確化に基づく対策 3.3 情報システムについての対策 3.4 IT 障害の観点から見た事業継続性確保のための対策 3.5 情報漏えい防止のための対策 3.6 外部委託における情報セキュリティ確保のための対策 3.7 IT 障害発生時の利用者の対応ための情報の提供等の対策 3.8 IT に係る環境変化に伴う脅威のための対策	https://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000046638.pdf	厚生労働省	第3版	－	－	－	－	－	－	－	－