クラウドサービスに関連する
国内外の制度・ガイドラインの紹介

２０２４年７月１２日

JIPDEC

一般財団法人日本情報経済社会推進協会

はじめに

インターネットの普及や新型コロナウイルス対策により、世界中の企業行動、個人の生活様式等は大きく変革（Transformation）している。我が国は、「Society 5.0」と呼ばれるデータ主導の社会を目指し、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実現を目指している。このようなインターネットを通じたデータ利活用の基盤となる仕組みとして、クラウドサービスが提供されている。初期導入コストが小さく、IT 資産の管理やシステム保守に係る負荷を軽減するクラウドサービスは、中小企業、公的機関等において、幅広く普及が進んでいる。

他方、クラウドサービスは、データが組織の外部に立地するデータセンターに置かれるとともに、IaaS（インフラ機能を提供するサービス）、PaaS（プラットフォームを提供するサービス）、SaaS（ソフトウェアを提供するサービス）等のレイヤー毎の事業者が存在することから、従来のオンプレミスとは異なる観点に基づく安全性の確保が重要となっている。クラウドサービスの安全性は、サービス提供者（以下「クラウドサービスプロバイダ」という。）とサービス利用者（以下「クラウドサービスカスタマ」という。）の適切な責任分界点のもとで担保されるべきものであるが、多種多様なクラウドサービスの出現において、クラウドサービスカスタマが適切なクラウドサービスを選択することは容易ではない。特に、クラウドサービスプロバイダが外国企業である場合は、データセンターが国外にあることが通例であり、クラウドサービスの導入に二の足を踏むサービス利用者も存在する。

このため、諸外国は、官民ともに、様々な視点に基づき、クラウドサービスの安全性評価の制度・ガイドライン等を整備している。クラウドサービスの政府調達においては、米国では FedRAMP 等の評価制度が運用されており、我が国でも同様に、政府情報システムのためのセキュリティ評価制度（ISMAP）が運用されているところである。これらの制度・ガイドライン等では、情報セキュリティマネジメントシステム（以下、ISMS という。）の国際規格である ISO/IEC 27001（Information security, cybersecurity and privacy protection – Information security management systems – Requirements）が引用されている場合が見られる。

国内でも、2016 年 8 月、ISMS 適合性評価制度（情報セキュリティマネジトシステム適合性評価制度）の一環として、JIPDEC 情報マネジメントシステム認定センター※がクラウドサービスプロバイダ又はクラウドサービスカスタマがクラウドサービス固有の管理策を追加して実施していることを認証する「ISMS クラウドセキュリティ認証」を開始した。ISMS クラウドセキュリティ認証は、500 を超えるクラウドサービスプロバイダ又はクラウドサービスカスタマに対する実績があり、クラウドサービスのセキュリティに関する認証が行なわれている。

JIPDEC は、クラウドサービスに関連する国内外の様々な制度・ガイドライン等について、とりわけ、ISMS との関連性に注目して、文献調査等に基づき 2019 年 5 月に本書をとりまとめた。その後、主に国内の制度・ガイドラインについて更新し、加えて、近年発行された ISO/IEC 27001:2022（JIS Q 27001:2023）の内容も反映し、本書を改訂した。

本書が、ISMS 適合性評価制度に係る実務者は勿論のこと、クラウドサービスに係る多くの関係者に活用され、我が国のクラウドサービスの健全な普及に寄与することを期待するものである。

※ 2018 年 4 月に認定業務を行う「一般社団法人情報マネジメントシステム認定センター（ISMS-AC）」となった。

目　次

1.　概要 1
1.1　本書の主旨 1
1.2　本書の構成 1
2.　国内外のセキュリティ関連制度 3
2.1　国内の制度・ガイドライン等 3
2.1.1　ISMS クラウドセキュリティ認証 3
2.1.2　CS マーク 4
2.1.3　政府情報システムのためのセキュリティ評価制度（ISMAP） 5
2.1.4　DX 認定制度 6
2.1.5　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 7
2.1.6　総務省によるクラウド事業者のためのガイドライン 8
2.1.7　医療分野のガイドライン 9
2.1.8　金融分野のガイドライン 10
2.2　国際的な制度・ガイドライン等 11
2.2.1　CSA STAR（本部：米国） 11
2.2.2　ECE StarAudit Certification（本部：ルクセンブルク） 12
2.2.3　EU-SEC（EU の HORIZON 2020　におけるプロジェクトの１つ）／EUCC 13
2.3　諸外国の制度・ガイドライン等 14
2.3.1　FedRAMP（米国政府） 14
2.3.2　G-Cloud（英国政府） 15
2.3.3　NIS 指令（EU） 16
2.3.4　NIS2 指令（EU） 17
2.3.5　クラウドコンピューティングコンプライアンスコントロールカタログ（C5）（ドイツ） 18
2.3.6　IRAP（オーストラリア） 19
2.3.7　MTCS（シンガポール） 20
2.4　クラウドに関連する規格・ガイド等 21
2.4.1　ISO/IEC 27017 21
2.4.2　ISO/IEC 27018 21
2.4.3　ISO/IEC 27036-4 22
2.4.4　ISO/IEC 20000-1 23
2.4.5　SOC2、SOC2+ 23
2.4.6　クラウドに関連する NIST 文書 25
おわりに 27

1. 概要

1.1 本書の主旨

デジタル社会の加速とともにクラウドサービスの導入・活用が増加している中で、それらのサービスの情報セキュリティをどのように確保するかが重要な課題となっている。製品・サービスの調達の際には、調達側がベンダの提供する製品・サービスに対して情報セキュリティ要件の確保を求めることが一般的だが、クラウドサービスにおいては、サービスの利用者側、プロバイダ側の双方の立場から情報セキュリティ対策を検討する必要がある。

ISMS は、情報の機密性、完全性、可用性を保護するための情報セキュリティ対策の包括的な仕組みであり、ISO/IEC 27001 は ISMS の構築、実施、維持、改善を行うための要求事項を定めた国際規格として幅広く活用されている。

本書では、国内外で実施されているクラウドサービスの提供や利用に対する適合性評価制度、個人情報保護が強く求められる医療分野等におけるクラウドサービスの扱いに関する制度やガイドライン等について、その概要・特徴、ISMS との関連性等を紹介することによって、クラウドサービスを利用する際の有益な情報を提供することを目的としている。

なお、クラウドサービスを利用する際に留意すべき点としては、安全性、継続性、準拠性等があげられるが、本書ではその中でも特に安全性について紹介することとした。

1.2 本書の構成

クラウドサービスに関連する制度、ガイドライン、国際規格等について紹介する。

図 1-1 に示す通り、2.1、2.2、2.3 では、それぞれ国内、国際、諸外国の制度・ガイドラインを紹介し、また 2.4 ではクラウドに関連する国際規格等を紹介する。

なお、本書は、制度及び各ガイドライン等の公開情報に基づいて調査した結果をもとに作成しており、活用される場合においては、必要に応じ、各制度、ガイドラインの最新版を参照されたい。また、国内外の全ての制度・ガイドラインを網羅するものではないことに留意されたい。

2.1 国内

名称	制度		ガイドライン類
	ISMSクラウドセキュテリィ認証	CSマーク	国内のガイドライン類＊
• 関連規格又は参照規格	• ISO/IEC 27001 • ISO/IEC 27017	• ISO/IEC 27017	• ISO/IEC 27001 • ISO/IEC 27002 • ISO/IEC 27017 • ISO/IEC 27018、他

＊2.1.5～2.1.8参照

本書に追加された制度：

- 政府情報システムのためのセキュリティ評価制度（ISMAP）： 2.1.3
- DX 認定制度： 2.1.4

2.2 国際

名称	制度		ガイドライン類
	CSA STAR	ECE Star Audit Certification	EU-SEC/EUCC
• 関連規格又は参照規格	• ISO/IEC 27001 • ISO/IEC 27017、他	• ISO/IEC 27001 • ISO/IEC 20000-1	• ISO/IEC 27001 • ISO/IEC 27017、他

2.3 諸外国

名称	FedRAMP（米国）	G-Cloud（英国）	NIS指令/NIS2指令（EU）	C5（ドイツ）	IRAP（オーストラリア）	MTCS（シンガポール）
• 関連規格又は参照規格	• ISO/IEC 27001	• ISO/IEC 27001	• ISO/IEC 27001	• ISO/IEC 27001 • ISO/IEC 27017	• ISO/IEC 27005	• ISO/IEC 27001

2.4 規格・ガイド等

国際規格	その他（グローバルな基準、各国基準等）
• ISO/IEC 27001 • ISO/IEC 27002 • ISO/IEC 27017 • ISO/IEC 27018 • ISO/IEC 27036-4 • ISO/IEC 20000-1	• SOC2 • SOC2＋ • NIST文書

図 1-1 クラウドサービスに関連する制度・ガイドライン

＊「関連規格又は参照規格」は、「2 国内外のセキュリティ関連制度」に示している「ISMS との関連性」に記載しているものであり、参照されている全ての規格を網羅するものではない。

2. 国内外のセキュリティ関連制度

本章では、国内外におけるセキュリティ関連の制度・ガイドライン等について、概要と特徴を一覧にして示す。これらは、クラウドサービスに関連するものとして、JIPDEC が選んだものであり、当該制度・ガイドライン等の作成者がクラウドサービスのセキュリティ対策を主眼にしているかは明らかではないものも含まれていることに留意されたい。

2.1 国内の制度・ガイドライン等

2.1.1 ISMS クラウドセキュリティ認証

調査・分析項目	詳細
名称 （運用組織）	ISMS クラウドセキュリティ認証 （一般社団法人情報マネジメントシステム認定センター（以下「ISMS-AC」という。）及び ISMS-AC によって認定されている ISMS 認証機関）
対象（適用範囲）	クラウドサービスプロバイダ（クラウドサービスを提供する組織） クラウドサービスカスタマ（クラウドサービスを利用する組織）
概要・特徴	• ISO/IEC 27001※1 に基づく ISMS 認証を前提として、その適用範囲内に含まれるクラウドサービスの提供もしくは利用に関して、ISO/IEC 27017※2 に規定されるクラウドサービス固有の管理策が実施されていることを認証する仕組みであり、ISMS 適合性評価制度※3 のもとで実施される。 • 認証基準は、JIPDEC が定めた「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（JIP-ISMS517）」である。 • 認証の有効期間は ISMS 認証の有効期間と一致し、認証を維持するためには 1 年毎のサーベイランスと 3 年毎の再審査・再認証が必要である。 • JIPDEC は、クラウドサービスを提供又は利用する組織の ISMS の構築・運用に携わっている方及び責任者を対象とした参考資料として「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～」を発行している。
ISMS との関連性	ISMS 認証を前提としており、ISO/IEC 27001 の管理策に ISO/IEC 27017 の管理策が追加される。
関連 URL	https://isms.jp/isms.html

※1 ISO/IEC 27001： 名称は「Information security, cybersecurity and privacy protection – Information security management systems – Requirements」であり、組織による ISMS の確立、実施、維持及び改善についての要求事項を規定する国際規格。同規格の内容を変えることなく翻訳し、国内規格化したものが JIS Q 27001（情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項）であり、ISMS 適合性評価制度における認証基準として利用されている。

※2 ISO/IEC 27017： ISMS を前提としたクラウドサービス固有の管理策のベストプラクティスを示した国際規格であり、クラウドサービスを提供する組織と利用する組織の両方を対象としている。本規格の内容を変えることなく翻訳し、国内規格化したものが JIS Q 27017 である（本書の 2.4.1 を参照）。

※3 ISMS 適合性評価制度： 一般社団法人情報マネジメントシステム認定センター（略称 ISMS-AC）によって認定された認証機関が、組織の ISMS を審査・認証する枠組みのこと。

2.1.2 CS マーク

調査・分析項目	詳細
名称 （運用組織）	クラウドセキュリティ・マーク（CS マーク） （特定非営利活動法人日本セキュリティ監査協会(JASA)）
対象（適用範囲）	クラウドサービスプロバイダ（クラウドサービスを提供する組織）
概要・特徴	• JASA のクラウド情報セキュリティ監査制度のもとで付与されるマークである。 • クラウド情報セキュリティ監査とは、標準的なサービスを多数の顧客に提供するクラウドサービスの特性を踏まえて、事業者が行うべき情報セキュリティマネジメントの基本的な要件（基本言明要件）を定め、事業者がそのとおりに実施しているかをクラウド情報セキュリティ管理基準に基づき評価し、安全性が確保されていることを顧客に明確にする仕組みである。 • 基本言明要件は、経済産業省が公開している「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」に基づくクラウド情報セキュリティ管理基準において定められたものである。 • JASA 発行のクラウド情報セキュリティ管理基準（平成 28 年版）は、JIS Q 27017:2016 に準拠した形で作成されている。 • 監査において要件を満たしていると認定された場合に、監査を受けた基本言明書に、CS マーク（クラウドセキュリティ・マーク）を付与する。 • CS マークは、ゴールド（適合監査）とシルバー（自主監査）の 2 種類がある。 • マークの使用許諾期間は、CS 言明書に対する自主監査の監査報告日から 3 年 6 ヵ月であり、延長申請の期間内に届け出ることにより 3 年間延長することが可能である。
ISMS との関連性	ISMS におけるクラウドサービス固有の管理策である、ISO/IEC 27017:2015（JIS Q 27017:2016）と整合がとられている。
関連 URL	https://jcispa.jasa.jp/

2.1.3 政府情報システムのためのセキュリティ評価制度（ISMAP）

調査・分析項目	詳細
名称 （運用組織）	政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ）） （内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省）**独立行政法人情報処理推進機構（IPA）が、制度運用に係る実務、評価に係る技術的な支援を行っている。
対象（適用範囲）	クラウドサービス事業者
概要・特徴	• 国際標準等を踏まえて策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、クラウドサービスを登録する制度。政府機関は、原則として「ISMAP クラウドサービスリスト」に掲載されたサービスから調達を行うこととなる。 • 本制度は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的としている。 • 2021 年 3 月に初回となる ISMAP クラウドサービスリストの登録・公開を行い、政府機関による本制度の利用を開始した（ISMAP クラウドサービスリストは、IPA が運用する ISMAP ポータルサイトにて公開されている）。 • 監査の対象となる ISMAP 管理基準は、「ガバナンス基準」、「マネジメント基準」、「管理策基準」の 3 種類から構成される。ガバナンス基準は経営陣に対する要求事項であり、全体の組織に対するガバナンスを効かせるという観点から規定されている。「マネジメント基準」は、管理者に対する要求事項であり、個別の管理策を実施するためのマネジメント体制の確立について規定されており、「管理策基準」では、技術的かつ具体的なセキュリティ管理策が規定されている。 • 本制度のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みとして、2022 年 11 月 1 日に新たに ISMAP-LIU（ISMAP for Low-Impact Use）制度の運用が開始された。
ISMS との関連性	ISMAP 管理基準は、JIS Q 27001、JIS Q 27002、JIS Q 27014、JIS Q 27017 等を基礎として作成されている。また、「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」（本書の 2.1.5 参照）への対応も図られている。 インシデント対応に関連する内容を中心に国際規格及び統一基準に含まれない観点を、SP800-53 を参照して追加されている。
関連 URL	https://www.ismap.go.jp/

2.1.4 DX 認定制度

調査・分析項目	詳細
名称 （運用組織）	DX 認定制度 （経済産業省）＊ *独立行政法人情報処理推進機構（IPA）が、本制度に関わる「DX 認定制度事務局」として各種問合せ、及び認定審査事務を行っている。
対象（適用範囲）	• 全ての事業者（法人と個人事業者。法人は会社だけではなく、公益法人等も含む）。
概要・特徴	• 「情報処理の促進に関する法律」に基づき、デジタル技術による社会変革に対して経営者に求められる事項を取りまとめた「デジタルガバナンス・コード」（経済産業省）の基本事項に対応する企業を、国が認定する制度。 • DX 認定の審査では、デジタルによって自らのビジネスを変革する準備ができている状態「DX-Readyの状態」であるかを「認定基準」とする。特に重要な点として、経営者自身のリーダーシップが問われ、DX により自社をどのように変革させるかの方向性や、その実現に向けた具体的な戦略が立てられていること、また戦略の推進状況の管理も行えること等の準備ができていることを確認する。 • 「認定基準」の内容は、「デジタルガバナンス・コード」に基づいており、コードの各項目に対応する内容を申請書に記入する。 • DX 認定制度に関連して、DX の実現に必要なクラウド技術の活用に向けたデジタル関連投資に対し、税額控除や特別償却を含む「DX 投資促進税制」の措置が施行されている。
ISMS との関連性	申請書の項目は、以下のとおり。 (1) 企業経営の方向性及び情報処理技術の活用の方向性の決定 (2) 企業経営及び情報処理技術の活用の具体的な方策（戦略）の決定 (2) ① 戦略を効果的に進めるための体制の提示 (2) ② 最新の情報処理技術を活用するための環境整備の具体的方策の提示 (3) 戦略の達成状況に係る指標の決定 (4) 実務執行総括責任者による効果的な戦略の推進等を図るために必要な情報発信 (5) 実務執行総括責任者が主導的な役割を果たすことによる、事業者が利用する情報処理システムにおける課題の把握 (6) サイバーセキュリティに関する対策の的確な策定及び実施 上記（６）は、ISMS やサイバーセキュリティ経営ガイドライン※1 などと関係性が強い。 また、申請項目全般を通じて、ISO/IEC 20000-1※2 との関連性も強いと考えられる。
関連 URL	https://www.ipa.go.jp/digital/dx-nintei/about.html https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html 情報処理の促進に関する法律の一部を改正する法律： https://elaws.e-gov.go.jp/document?lawid=345AC0000000090

※1 サイバーセキュリティ経営ガイドライン：経済産業省が IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため策定し、Ver3.0 を令和 5 年 3 月 24 日公開した。（https://www.meti.go.jp/policy/netsecurity/mng_guide.html）

※2 ISO/IEC 20000-1：（IT）サービスマネジメントシステムの国際規格。 第一部は、要求事項であり、ISO/IEC 20000-1:2018 は、2018 年 9 月 15 日に発行された。（「ITSMS ユーザーズガイド-JIS Q 20000-1:2020 (ISO/IEC 20000-1:2018)対応-」参照）

2.1.5 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

調査・分析項目	詳細
名称及び構成	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（旧名称：「政府機関等の情報セキュリティ対策のための統一基準群」）（以下「統一基準群」という。） 統一基準群は、以下の 3 つの文書から構成される。 ① 政府機関等のサイバーセキュリティ対策のための統一規範 ② 政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版） ③ 政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）
対象（適用範囲）	政府機関（府省庁）
概要・特徴	• 政府のサイバーセキュリティ戦略本部（事務局：内閣サイバーセキュリティセンター(NISC)）は、サイバーセキュリティ基本法（平成 26 年法律第 104 号）に基づき、国の行政機関等のサイバーセキュリティに関する対策の基準を決定している。 • ②は、政府機関（府省庁）が守るべき基準の目的や趣旨、遵守事項を示している。政府機関等がクラウドサービスを利用する場合は、②の「第 4 部 外部委託」の「4.1 業務委託」及び「4.2 クラウドサービス」に示された各遵守事項を満たす必要がある。特に、要機密情報を取り扱う場合にクラウドサービスを利用する際の選定基準は、取り扱う情報の格付及び取扱制限を踏まえてセキュリティ要件を定めると共に、当該セキュリティ要件を踏まえて原則として ISMAP 等クラウドサービスリストから選定する必要がある。 • ③は、②に示された遵守事項を満たすためにとるべき基本的な対策事項が例示され、個々の組織が対策基準を自ら策定し、それを実施する際の考え方を解説している。
ISMS との関連性	「4.1.1 業務委託」に対応する③の解説において、委託先の選定基準の一例として、ISO/IEC 27001 等に基づく認証制度の活用が示されている。
関連 URL	https://www.nisc.go.jp/policy/group/general/kijun.html

2.1.6 総務省によるクラウド事業者のためのガイドライン

調査・分析項目	詳細
名称	総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）」
対象（適用範囲）	クラウド事業者
概要・特徴	• クラウドサービスの利用が企業等の生産性向上の健全な基盤となることを目標に、クラウド事業者が実施すべき情報セキュリティ対策をまとめたガイドライン。 • 2018 年 7 月に第 2 版として発行された本ガイドラインは、「ASP・SaaS における情報セキュリティ対策ガイドライン（2008 年 1 月）」及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（2014 年 4 月）」を統合したものである。 • 2021 年 9 月に発行された第 3 版では、クラウドサービスにおける責任分界のあり方や国際規格等との整合性を考慮した改定が行われた。
ISMS との関連性	本ガイドラインではセキュリティ対策として、組織的取組み等を取りまとめた「共通編」、物理的・技術的取組み等を取りまとめた「SaaS 編」「PaaS/IaaS 編」等に分類してまとめているが、各対策において ISMAP 管理基準、ISO/IEC 27017 及び NIST SP800-53 を参照している。
関連 URL	https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html

2.1.7　医療分野のガイドライン

調査・分析項目	詳細
名称	３省が定めた以下のガイドラインは、通称として、「3 省 2 ガイドライン」と呼ばれることがある。 ①　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」（令和 5 年 5 月） ②　経済産業省・総務省「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　第 1.1 版」（令和 5 年 7 月改定）
対象（適用範囲）	医療情報システム
概要・特徴	• 国内でクラウドを活用した医療情報システムを使用する場合、旧 3 省 4 ガイドラインに準拠することが求められてきた。各ガイドラインは数年おきに改訂を重ね、平成 30 年 7 月に総務省の 2 つのガイドラインが 1 つに集約され、「3 省 3 ガイドライン」となった。 • その後、令和 2 年 8 月に経済産業省と総務省のガイドラインが 1 つに集約され、「3 省 2 ガイドライン」となった。 参考情報：米国では、HIPAA 法（医療保険の携行性と責任に関する法律）／HITECH 法（経済的及び臨床的健全性のための医療情報技術に関する法律）に基づき、医療 IT 化インセンティブ制度（Meaningful Use）が導入されると同時に、プライバシー／セキュリティに係る規則が拡張された。医療機関、医療保険者等の適用対象主体（CE）に代わり、保護対象保健情報（PHI）の生成、収集、維持、交換を行うクラウドサービス事業者も、事業提携者（BA）として、事前の事業提携契約書（BAA）締結及びリスク評価、データ漏えい時の通知、外部監査対応等の要求事項が適用される。なお 2019 年度の Meaningful Use から Promoting Interoperability への制度変更に伴い、HIPAA／HITECH 法／プライバシー／セキュリティ規則の改正に向けた作業が行われている。
ISMS との関連性	①では、ISMS の策定及び実施を遵守事項としている。また、委託する事業者を選定する場合にも、JIS Q 27001 又はこれと同等の規格の認証を受けているシステム関連事業者の選定を遵守事項としている。 ②では、「4.4 対象事業者の適格性を評価する第三者認証等の取得に係る要件」において、ISMS 認証やプライバシーマーク認定の取得を必須としている。加えて、クラウドセキュリティ認証等として、ISO/IEC 27017、ISO/IEC 27018 に基づく認証にも触れている。
関連 URL	https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

2.1.8 金融分野のガイドライン

調査・分析項目	詳細
名称 （作成組織）	「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）」 （公益財団法人金融情報システムセンター(FISC)）
対象（適用範囲）	金融機関
概要・特徴	• 日本国内の金融機関等の情報システムで守るべき安全対策の具体的な指針として、FISC により策定されたガイドライン。 • 初版は 1985 年に金融機関の自主基準として策定され、当初は金融機関が所有するオンプレミスを対象としていた。その後改訂が行われ、2013 年の第 8 版追補にてクラウドサービス利用に関する安全対策が盛り込まれた。最新版は 2024 年 3 月に発行された第 12 版であり、「統制基準」「実務基準」「設備基準」「監査基準」の 4 つの対策基準群に分類して、具体的な取組みが示されている。 • 第 11 版及び第 12 版では、クラウドサービスを導入・運用する際の留意点を中心に記載内容の更新が行われた。
ISMS との関連性	統制におけるクラウドサービス事業者の管理方法の一つとして、ISO/IEC 27001 及び ISO/IEC 27017 に基づく第三者認証によって確認する例が示されている。 また監査基準の中で、外部委託先の監査の方法の例として、第三者認証に関する情報を確認する方法が示してあり、第三者認証の代表例として ISMS（ISO/IEC 27001、ISO/IEC 27017）や PCI DSS、プライバシーマークが挙げられている。
関連 URL	https://www.fisc.or.jp/publication/

2.2 国際的な制度・ガイドライン等

2.2.1 CSA STAR（本部：米国）

調査・分析項目	詳細
名称 （運用組織）	CSA Security, Trust & Assurance and Risk（CSA STAR） （The Cloud Security Alliance (CSA)）
対象（適用範囲）	クラウドサービスプロバイダ（CSP）
概要・特徴	• CSP の提供する様々なクラウドコンピューティングのセキュリティコントロールについて登録・公開しており、これを参照することでユーザが CSP のセキュリティ対応能力について確認し、判断する際に利用できるようにしている。 • STAR プログラムには、次の 3 つのレベルがあり、このうちレベル 2 が、第三者認証である。 ✧ レベル 1 － 自己評価（Self-Assessment） CSA CCM（クラウドコントロールマトリクス）を利用し、CAIQ（コンセンサスアセスメントイニシアティブクエスチョネア）を自己評価として提出（2022 年 7 月より、CCM/CAIQ のバージョンが 3.1 から 4.0 に変更）。 CSA STAR EBSA (エビデンスベースセルフアセスメント)：ISMS または SOC2 を取得した中小 CSP を対象とする自己評価プログラムを開発・検証中。 ✧ レベル 2 － 第三者認証（3rd party certification） ✓ CSA STAR 実践認証（Attestation）： SOC2※対応の認証。 ✓ CSA STAR 認証（Certification）：ISMS 認証取得が前提。 認証基準は、CSA CCM（クラウドコントロールマトリクス）を利用。 ✧ レベル 3 － 継続的監視（continuous auditing） • CSA STAR 認証の種類（アワード） 認証審査では、CSA CCM で規定する管理策領域についてスコアが付けられ、そのスコアに基づいて、ブロンズ、シルバー、ゴールドのアワードが付与される。 • Zero Trust Advancement Center を開設し、連邦政府機関の CIO／CISO を巻き込んだ調査、トレーニング、資格認定などを提供。 （https://cloudsecurityalliance.org/zt）
ISMS との関連性	CSA STAR 認証は、ISMS 認証を取得していることが要件の一つとなっている。 また、CSA CCM では、ISO/IEC 27017 を含む規格等とのマッピングが示されている。
関連 URL	https://www.cloudsecurityalliance.jp/site/?page_id=429 https://cloudsecurityalliance.org/star/#_overview

※ SOC2： 本書の「2.4.5 SOC2、SOC2＋」を参照。

2.2.2 ECE StarAudit Certification（本部：ルクセンブルク）

調査・分析項目	詳細
名称 （運用組織）	StarAudit Certification （EuroCloud Europe (ECE)）
対象（適用範囲）	クラウドサービスプロバイダ（CSP）の提供するクラウドサービス
概要・特徴	• 確認すべき要件には、クラウドサービスのセキュリティに加えて、運用に関連する領域（ISO/IEC 27001 に加えて、ISO/IEC 20000-1 に関連）も含む。 • 具体的には、認証審査にはクラウドサービスで確認すべき要件を 7 つの領域に分けて記載したカタログ（管理策集）を用いる。カタログでは、Star3～5 というレベルが設定されており、レベル毎に管理策数が異なる（数字が大きいほどレベルが高い。レベルが高くなるにつれて管理策が追加される）。なお、カタログは、クラウドサービスの特徴に応じて次の 7 つの領域に分類されている。 1 CSP の情報、2 契約関連事項、3 情報セキュリティ、4 データセンターの運用、5 クラウドサービスの運用プロセス、6 クラウドの形態（IaaS、PaaS、SaaS）ごとの要件、7 データ保護 • ECE が認定した AAO（StarAudit Audit Organisation）が審査を実施し、その結果を ECE に報告する。その結果を受けて ECE が認証書を発行する。 • 審査では、申請した CSP が作成したアセスメントレポート※の内容と関連文書を AAO が確認する。 審査の流れ：https://staraudit.org/news/article/how-to-get-a-staraudit-certificate-and-how-much-does-it-cost/（HOW TO GET A STARAUDIT CERTIFICATE AND HOW MUCH DOES IT COST） • 認証の有効期間は 3 年で、1 年毎に維持審査（refresh audit）が、3 年毎に更新審査（full audit）が実施される。
ISMS との関連性	• カタログの領域のうち、「3 情報セキュリティ」では、Star5 のレベルを満たす要件として「ISO/IEC 27001 を取得している」と記載している管理策がある。 • カタログの領域のうち、「5 クラウドサービスの運用プロセス」では、Star5 のレベルを満たす要件として「ISO/IEC 20000-1 を取得している」と記載している管理策がある。
関連 URL	https://staraudit.org/

※ アセスメントレポート： ECE のアセスメントツールを利用して、カタログ（管理策集）の中の認証を受けたいレベル（Star3～5）に対応した管理策について、自己評価とその評価の根拠となるエビデンスの参照を付して作成したもの。アセスメントツールは有料。

2.2.3 EU-SEC（EU の HORIZON 2020[1]におけるプロジェクトの１つ）／EUCC

調査・分析項目	詳細
名称 （検討実施組織）	The European Security Certification Framework（EU-SEC）Project （EU-SEC Consortium (Fraunhofer Fokus, CSA, PwC Germany 含む 8 組織)） The European Cybersecurity Scheme on Common Criteria (EUCC) （European Commission 及び ENISA）
対象	クラウドサービスプロバイダ（CSP）
概要・特徴	• EU-SEC は、クラウドインフラのセキュリティを確保するための認証のスキームと評価の考え方についての欧州における枠組みを策定することを目指している。 • 既存のクラウドセキュリティスキーム（制度）間において、審査プロセスの一貫性も担保可能な、相互承認（multiparty recognition）の枠組み創設を目的としている（CSP が新たに別のクラウドセキュリティ認証を取得しようとする際に、取得済みの認証との差分※審査で認証取得が可能となるような仕組みの検証を実施した）。 • 最終的には「D.2.5 EUSEC Framework – Final Version」を含む 24 本の成果物を発行している。 • この枠組みの主な 3 つの柱は、「相互承認の枠組み」、「継続的な審査・認証スキーム」、「プライバシー行動規範」である（D.2.5 を参照）。 • 本プロジェクトの成果は、EU サイバーセキュリティ法に基づく EU サイバーセキュリティ認証スキーム（EUCC）などの取組みに継承されている。 • EU-SEC2020 は、2020 年に報告書が公開されプロジェクトが終了した。現在、EU のサイバーセキュリティ法に基づいて、ENISA を中心にサイバーセキュリティ認証制度を策定する作業が進められており、その中でクラウド部分については、上記の EU-SEC の内容が参照されている。EU サイバーセキュリティ認証スキームの Common Criteria（Ver.1.1）について、2024 年 1 月に欧州委員会で採択。クラウドサービスだけでなく、AI サービスも含む形になっている。
ISMS との関連性	差分分析のなかに、ISO/IEC 27001、ISO/IEC 27017 も含まれる。 Common Criteria の中で、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005 を参照している。また、Common Criteria の Annex 2 は、ISO/IEC 27001 の Annex A の構成に沿っている。
関連 URL	https://www.sec-cert.eu/ https://www.enisa.europa.eu/news/an-eu-prime-eu-adopts-first-cybersecurity-certification-scheme

※ クラウドセキュリティ関連の基準の内容・違い等を CSA CCM をベースに分析したもの（D.1.2 – Security and Privac Requirements and Controls）等がある。

[1] HORIZON 2020： 複数のパートナによる研究・イノベーションプロジェクトを助成する欧州連合（EU）の枠組みであり、7 年間（2014 年～2020 年）にわたる総額 800 億ユーロの資金助成制度

2.3 諸外国の制度・ガイドライン等

2.3.1 FedRAMP（米国政府）

調査・分析項目	詳細
名称 （運用組織）	The Federal Risk and Authorization Management Program（FedRAMP） （FedRAMP Program Management Office（FedRAMP PMO）※1）
対象 （適用範囲）	製品やサービス等幅広いものが対象であり、その中にクラウドサービスプロバイダが提供するクラウド製品・サービスがある。
概要・特徴	• 連邦政府機関が使用するクラウド製品・サービスが適切な保護を講じていることを評価・承認することが目的。 • １つの省庁の評価結果を他の省庁と共有可能にすることにより、迅速かつ費用対効果の高いサービスの政府調達を可能にする。 • クラウドサービスの評価を行う第三者機関である 3PAO（Third-Party Assessment Organization）が評価し、その結果を合同承認委員会（JAB：Joint Authorization Board）が検討・承認する。 • 3PAO は、ISO/IEC 17020 に従って A2LA（American Association of Laboratory Accreditors）の認定を受ける必要がある。 • その他、関連当局による認定もある（ATO：Agency Authority to Operate）。 • FedRAMP の基準は、NIST SP 800-53※2 をベースに策定されており、CSP 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。ISO/IEC 27001 とのマッピングがとられている。 • この Baseline は、セキュリティの高さで以下の 3 段階のレベル分けがされている。 FedRAMP Low、FedRAMP Moderate、FedRAMP High • 米国大統領行政府が、ゼロトラストサイバー セキュリティ原則を採択した※3 ことを受けて、FedRAMP も FedRAMP Rev 5 baselines 改定作業と並行して、ゼロトラストアプローチを組み込む準備を開始すると 2022 年 1 月 26 日に発表※4 があった。 • 2022 年 12 月、FedRAMP 承認法（FedRAMP Authorization Act）が 23 年度米国国防権限法（NDAA）の一部として署名された。同法は、FedRAMP プログラムを、非機密扱いの連邦情報を処理するクラウドコンピューティングの製品・サービスのためのセキュリティ評価と承認の標準化アプローチとして成文化したものである。
ISMS との関連性	NIST SP 800-53 では、ISO/IEC 27001 とマッピングがとられている。
関連 URL	https://www.fedramp.gov/

※1 FedRAMP PMO： GSA（General Services Administration－独立政府機関）内に設置されている。
※2 NIST SP 800-53： NIST（National Institute of Standards and Technology：米国国立標準技術研究所）発行の文書（詳細は、本書の 2.4.6 参照）。
※3 米国大統領行政府が、ゼロトラストサイバー セキュリティ原則を採択：Moving the U.S. Government Toward Zero Trust Cybersecurity Principles （https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf）
※4 ゼロトラストアプローチを組み込む準備を開始：FedRAMP Prepares for 'Zero Trust' Stance（https://www.fedramp.gov/2022-03-02-prepares-for-zero-trust-stance/ ）

2.3.2 G-Cloud（英国政府）

調査・分析項目	詳細
名称 （運用組織）	G-Cloud framework （Government Digital Services（GDS））
対象（適用範囲）	クラウドサービス供給者（Cloud service supplier）
概要・特徴	• 政府とクラウドサービス供給者間の合意であり、契約通知が Official Journal of the European Union（OJEU）に掲載された後に、両者間で利用に関する基本事項（the basic terms of use）について合意する。 • 個別に調達契約を交わすよりも、この枠組み（Framework）を利用することによってサービスのより迅速かつ費用対効果の高い調達が可能になる。調達可能なサービスは、クラウドホスティング、クラウドソフトウェア、クラウドサポートに分類される。 • 調達に際しては、Digital Marketplace の「View G-Cloud 13 supplier services」から、クラウドサービス供給者を検索できる。 「Digital Marketplace」の URL： https://www.digitalmarketplace.service.gov.uk/buyers/direct-award/g-cloud/start • クラウドサービス供給者の申請プロセスでは、主に法的な要求事項準拠の確認（the supplier declaration）と、自組織のサービスに関する情報の提供（サービスの概説・特徴・技術・利点・費用・セキュリティ等）が求められる。申請が認められると、合意後に上記 Web 上で提供サービスの情報が公開される。 • クラウドサービスのセキュリティ評価には、Cloud Security Principle が用いられる。 Cloud Security Principle： https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles
ISMS との関連性	Cloud Security Principle では、ISO/IEC 27001 等が参照されている。
関連 URL	https://www.gov.uk/guidance/the-g-cloud-framework-on-the-digital-marketplace https://www.gov.uk/guidance/g-cloud-suppliers-guide https://www.gov.uk/guidance/g-cloud-buyers-guide

2.3.3 NIS 指令（EU）

調査・分析項目	詳細
名称	Network and Information Security Directive（NIS 指令：ネットワーク及び情報セキュリティ指令。欧州議会・理事会指令 2016/1148）
対象（適用範囲）	NIS 指令の対象は、以下の 2 つがある。 ① 重要サービスオペレーター（OESs）：エネルギー、運輸、銀行、金融市場インフラストラクチャ、医療、飲料水供給・配送、デジタルインフラストラクチャ（ドメインネームサービス（DNS）プロバイダ、インターネットエクスチェンジ（IXP）、トップレベルドメイン（TLD）レジストリ） ② デジタルサービスプロバイダ（DSP）：オンラインマーケットプレース、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
概要・特徴	• EU 全域に渡るネットワーク・情報システム全体のセキュリティとレジリエンス（障害許容力）のレベルを向上させることを目的とする。 • NIS 指令は 2016 年 8 月に発効され、EU 各加盟国は 2018 年 5 月を期限として適用し、国内関連法制を整備した。 • クラウドサービスプロバイダは DSP としての責務を有し、さらに、デジタルインフラストラクチャに該当する場合、重要サービスオペレータ（OESs）としての責務も有する。 • OESs は、クラウドサービスを利用する場合、クラウドサービスカスタマとしての責務を有することとなる。 • セキュリティ評価に必要な情報を提供する（適用対象：DSP 及び OESs）。 • セキュリティポリシーの有効な導入を示す証跡を提供する（適用対象：OESs）。 • EU 域内に常備設備を持たずにサービスを提供する場合、代表者を指名する（適用対象：DSP）。 • サービス継続に深刻な影響があるインシデントを遅滞なく所管当局に通知する（適用対象：DSP 及び OESs）。 • 第三者の DSP に依存している場合、インシデントによる重要な影響を通知する（適用対象：DSP 及び OESs）。OES が依存する DSP の事故は、OES が通知しなければならない。 • 通知を受けた所管当局からの要請に応じて、個々のインシデント情報を公表する（適用対象：DSP）。 • NIS2 指令（欧州議会・理事会指令 2022/2555）により 2024 年 10 月 18 日に廃止予定。
ISMS との関連性	ENISA（The European Union Agency for Network and Information Security）が NIS 指令関連文書の中で、ISO/IEC 27001 及び NIST サイバーセキュリティフレームワークを推奨している。
関連 URL	https://www.enisa.europa.eu/topics/nis-directive https://jipsti.jst.go.jp/sti_updates/2018/09/10789.html

2.3.4 NIS2 指令（EU）

調査・分析項目	詳細
名称	Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) （NIS2 指令：改正ネットワーク及び情報セキュリティ指令(EU 全域における高度な共通レベルのサイバーセキュリティ対策に関する指令)。欧州議会・理事会指令 2022/2555）
対象	NIS 指令と比較すると、NIS2 指令の対象は、より広いグループに拡大され、「重要（important）」又は「不可欠な（essential）」に分類される大規模・中規模なエンティティに調和のとれたルールが盛り込まれた。 NIS 指令箇条 4(4)「不可欠な（essential）サービスの運営者」は、１．エネルギー、２.輸送、３．金融、４．金融市場インフラストラクチャ、５．医療分野、６．飲料水供給、７．デジタルインフラの 7 つであったが、NIS2 指令における重要分野（sectors of high criticality）では、６．の飲料水供給が６．飲料と７．廃水に分かれ、９．ICT サービスマネジメント（B to B）、10.行政、11.宇宙の計 11 分野となった。 関連する国内の製造業においても大きな影響を与える可能性がある。
概要・特徴	• NIS 指令の附属書 II の「デジタルインフラストラクチャ」には、①IXPs、②DNS サービスプロバイダー、③TLD ネームレジストリのみが記載されていたが、NIS2 指令の附属書 I の「デジタルインフラストラクチャ」に記載された事業者は、①IXPs、②（ルートネームサーバー事業者を除く）DNS サービスプロバイダー、③TLD ネームレジストリに加えて、④クラウドコンピューティングサービスプロバイダー、⑤データセンターサービスプロバイダー、⑥コンテンツデリバリーネットワークプロバイダー、⑦トラストサービスプロバイダー、⑧公衆電気通信ネットワークプロバイダー、⑨一般に利用可能な電子通信サービスのプロバイダーである。 • 2022 年 12 月 27 日に EU の official journal で公表され、2023 年 1 月 16 日発効。 • 2024 年 10 月 17 日までに、加盟国は NIS 2 指令遵守のために必要な措置を講じなければならない。当該措置は 2024 年 10 月 18 日以降適用される。
ISMS との関連性	NIS2 の第 24 条において、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005 を参照した欧州サイバーセキュリティ認証スキーム（EUCC）との関係について明記している（EUCC は、本書の 2.2.3 を参照）。 Preamble 79 に 27000 シリーズが例示として登場する。
関連 URL	https://eur-lex.europa.eu/eli/dir/2022/2555 https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

2.3.5 クラウドコンピューティングコンプライアンスコントロールカタログ（C5）（ドイツ）

調査・分析項目	詳細
名称 （発行者）	Cloud Computing Compliance Control Catalogue（C5） （ドイツ情報セキュリティ庁（BSI）：Bundesamt für Sicherheit in der Informationstechnik）
対象（適用範囲）	クラウドサービスプロバイダ（CSP）
概要・特徴	• クラウドサービスの情報セキュリティを評価するために既存の国際・国内規格等をもとにして作成されたカタログであり、クラウドコンピューティングのセキュリティ要求事項を提供している。2016 年に初版が発行され、2020 年に改訂された。 • 2020 年の改訂に当たり、例えば DevOps といった新しい概念に関する基準の変更又は拡大を行った。 • セキュリティレベル向上のためにクラウドセキュリティに対する理解を深め、かつ、審査の重複や不要な取組みを避けることを目的としている。 • C5 の要求事項は、17 のセクションで構成されている（例：情報セキュリティのための組織、要員、資産管理、物理的セキュリティ、運用等）。 • 要求事項は、ISO/IEC 27001、Cloud Security Alliance の Cloud Controls Matrix（CSA CCM）、ドイツ国内規格、各国の規格等を参照して作成されている。 • C5 と上記の規格等とのマッピングも公開されており、CSP における自組織のセキュリティレベルと C5 の要求事項とのギャップ分析等に役立つツールとして提供されている。 • C5 の監査・報告は、ISAE 3000[2]（及び必要に応じて審査に関する国際・国内規格）を適用して実施される。
ISMS との関連性	C5 の要求事項は、ISO/IEC 27001 を含めた国際・国内規格をもとに作成されていることから、監査でも ISO/IEC 27001 等の認証を取得している場合は、作業の軽減が見込まれる。
関連 URL	https://www.bsi.bund.de/EN/Home/home_node.html https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf

[2] International Standard on Assurance Engagements（ISAE）3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information（原文公表：2013 年 12 月） 国際保証業務基準 3000 号「過去財務情報の監査又はレビュー以外の保証業務」

2.3.6 IRAP（オーストラリア）

調査・分析項目	詳細
名称 （運用組織）	The Information Security Registered Assessors Program（IRAP）： オーストラリア政府情報セキュリティ登録評価プログラム （Australian Signals Directorate（ASD））
対象（適用範囲）	クラウドサービスプロバイダ（CSP）－クラウドセキュリティガイダンスの場合 （IRAP は Australian Government Information Security Manual (ISM)等オーストラリア政府の規定に準拠しているか証跡に基づき評価する制度であり、クラウドサービスのみを対象とするものではない。）
概要・特徴	• オーストラリア政府に対して、高品質な ICT セキュリティ評価サービスを提供するためのプログラムである。 • ASD が一定の要件を満たす ICT 専門家を IRAP 評価者（IRAP Assessor）として承認（endorse）する。 • ASD では、セキュリティ評価サービスを提供する資格として、IRAP 評価者の資格認定の制度を実施している。 [組織の認証について] ASD は、以下のクラウドサービス認証制度を実施していたが、2020 年 3 月に本制度を終了し、クラウドセキュリティガイダンスを公開した。 • クラウドセキュリティガイダンスは、政府機関、CSP、IRAP 評価者を含む組織が CSP とそのクラウドサービスを包括的に評価する方法に関する手引を示し、組織のデータ取扱いの適切性についてリスク情報に基づく判断を実施できることを目的とする。 • IRAP 評価者は、CSP とそのクラウドサービスの評価を支援するために、クラウドセキュリティコントロールマトリックス（CSCM）を使用してセキュリティ管理策の実施を把握できる。最新の CSCM は、情報セキュリティマニュアル（ISM）の Web ページに掲載されている。参考：過去のクラウドサービス認証制度の概要 • ASD は、CSP のクラウドサービスの認証（ASD Certified Cloud Services）を実施しており、そのセキュリティアセスメント審査は、IRAP 審査員が行う。審査では、組織のセキュリティ管理策の実施状況、適切性、有効性を評価する。 • ASD は、認証した CSP に対して、Certification Letter と Certification Report を発行し、CSP を ASD Certified Cloud Services List（CCSL）に掲載する。 • オーストラリア政府機関は、クラウドサービス調達に際して、Certification Report 等に基づいて、CSP を認定（accreditation）する。認定では、特に審査・認証プロセスで特定された残存リスクが容認できるかを確認する。 認証プロセスは、The Attorney-General's Department が策定する Protective Security Policy Framework（PSPF）と Information Security Manual（ISM）に基づいて実施する。
ISMS との関連性	ISM の中で参考文書として、ISO/IEC 27005 が紹介されている。
関連 URL	https://www.cyber.gov.au/acsc/government/cloud-security-guidance https://www.cyber.gov.au/resources-business-and-government/assessment-and-evaluation-programs/infosec-registered-assessors-program

2.3.7 MTCS（シンガポール）

調査・分析項目	詳細
名称 （運用組織）	Multi-Tier Cloud Security Standard For Singapore（MTCS SS 584） （情報通信メディア開発庁（IMDA）：Infocomm Media Development Authority of Singapore）
対象（適用範囲）	クラウドサービスプロバイダ（CSP）
概要・特徴	• 2013 年に発行された世界初のクラウドセキュリティの規格で、クラウドコンピューティングにおける健全なリスクマネジメントとセキュリティ慣行の導入を促進することを目的としている。 • ユーザや審査員等がクラウドセキュリティの要件を理解できるようにするために、またCSPがクラウド環境におけるセキュリティ対策を強化し実証できるようにするために、関連するクラウドセキュリティの要求事項と管理策を提供している。 • 3 段階のレベルがあり、Tier1 が基本レベルで、Tier3 が最も高いレベルとなっている。 • 認定された認証機関（BSI Group Singapore Pte Ltd、SOCOTEC CERTIFICATION SINGAPORE PTE. LTD、TUV SUD PSB Certification 等）による、第三者認証が実施されている。 • 第三者認証に加えて、CSP は自己開示文書（self-disclosure document）を作成することが要求されている。開示には、データ管理、プロバイダのパフォーマンス(例：可用性、BCP/DR)、サービス支援(例：変更管理、インシデント及び問題管理)等の分野が含まれる。 • 認証は 3 年間有効で、毎年サーベイランス審査が実施される。
ISMS との関連性	ISO/IEC 27001 との対応ガイダンス等が発行されている。
関連 URL	https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Cloud-Computing-and-Services https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Compliance-and-Certification

2.4 クラウドに関連する規格・ガイド等

2.4.1 ISO/IEC 27017

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

（情報技術－セキュリティ技術－ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）

クラウドサービスプロバイダ（クラウドサービスの提供者）とクラウドサービスカスタマ（クラウドサービスの利用者）の双方に、情報セキュリティ管理策の実施要項を提供するガイドライン規格である。

この規格は、情報セキュリティ管理策の実践のための規範である ISO/IEC 27002 の管理策（管理目的、管理策、実施の手引）に対して、クラウドサービスにおいて必要となる追加の事項を規定している。ISO/IEC 27002 は、ISO/IEC 27001 に基づく ISMS において、情報セキュリティ管理策を実施するための手引であり、ISO/IEC 27017 は、ISMS におけるクラウドサービスを対象とした追加の管理策（実施の手引）という位置づけである。

本ガイドライン規格には Annex B（附属書 B（参考）クラウドコンピューティングの情報セキュリティリスクに関する参考文献）に、クラウドサービスの提供及び利用におけるリスク源及びリスクの説明を含む参考文献のリストが記載されている。

リスク源及びリスクはサービスの種類及び性質並びにクラウドコンピューティングの新技術に応じて変化することに留意し、必要に応じて各文献の最新版を参照することが望ましい。

2.4.2 ISO/IEC 27018

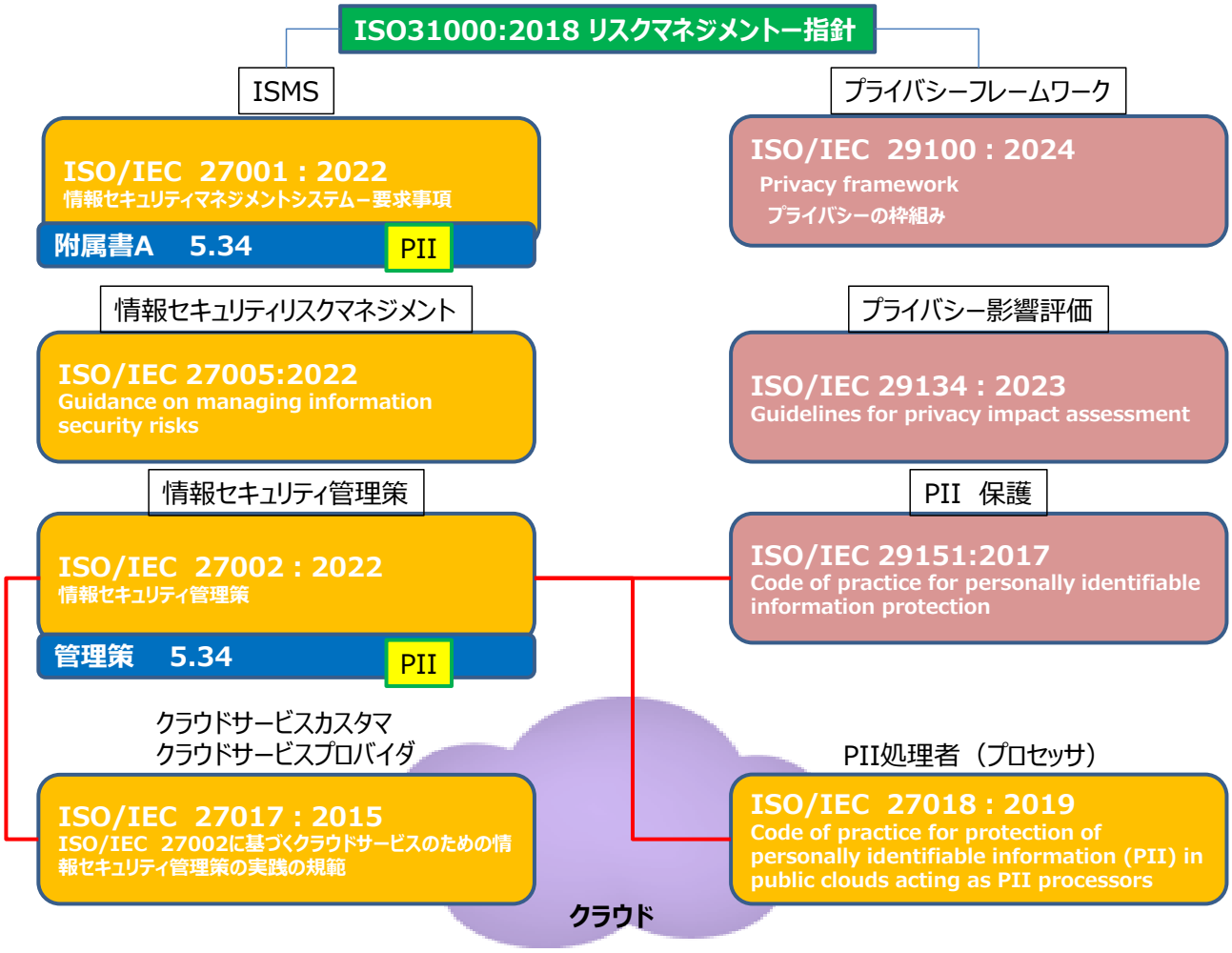
Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

（情報技術－セキュリティ技術－PII 処理者としてパブリッククラウドにおいて PII を保護するための実践の規範）

ISO/IEC 27018 は、PII（Personally Identifiable Information:個人識別可能情報）を PII 処理者※として取り扱うパブリッククラウドサービスプロバイダに対して、PII を保護するためのガイドラインを提供する規格である。ISO/IEC 27002 をベースとしており、パブリッククラウドサービスプロバイダが PII 処理者として PII を取り扱う場合の追加の事項（管理目的、管理策、実施の手引）を規定している。

パブリッククラウド上で、「PII 処理者」は、ISO/IEC 27018 のガイドをもとに、「PII 処理者」としての業務をマネジメントしていることを証明することにより、PII 管理者は、PII 管理者と PII 処理者の責任を理解した上で、PII 処理者の個人情報保護マネジメントの概要を証明書等で確認及び監督することで、PII 処理者が ISO/IEC 27018 に沿って PII をマネジメントしていることを確認することができる。クラウドサービスプロバイダ（IaaS、コンピューティング機能を提供する）が主な対象となる。

※PII 処理者（PII プロセッサ）とは、PII 管理者（PII コントローラ）の代行として、PII 管理者の指示に従って PII を処理する者のことである。PII 管理者は、PII を取り扱うための利用目的と手段を決定する者である。詳細は、ISO/IEC 29100 を参照。
ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework
（JIS X 9250:2017 情報技術―セキュリティ技術―プライバシーフレームワーク (プライバシー保護の枠組み及び原則)）



2.4.3 ISO/IEC 27036-4

Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

（情報技術－セキュリティ技術－供給者管理のための情報セキュリティ－第 4 部：クラウドサービスのセキュリティのためのガイドライン）

ISO/IEC 27036 は、組織が製品やサービスを外部から調達する際の供給者（サプライチェーン）関係における情報セキュリティ対策や管理のためのガイドラインで、サプライチェーン全体のリスク管理の重要性や課題を明らかにした上で、計画策定、供給者選定、契約、運用管理、契約終了までの一連のプロセスについて規定している。 ISO/IEC 27036 は 4 部構成であり、第 4 部は、特にクラウドサービスプロバイダとクラウドサービスカスタマに対して、クラウドサービスの利用に関連する情報セキュリティリスクを可視化し、効果的に管理する方法に関するガイダンスや、クラウドサービスを利用する組織に情報セキュリティ上の影響を及ぼし得る、クラウドサービスの調達又は提供に特有のリスクへの対応に関するガイダンスを提供している。

ISO/IEC 27036 の他のシリーズは以下の通り。

Part 1: Overview and concepts（概要※）

Part 2: requirements（(供給者管理における)汎用的な要求事項※）

Part 3: Guidelines for hardware, software, and services supply chain security（ICT サプライチェーンにおける情報セキュリティのガイド※）

なお、ISO/IEC 27036-4 における引用規格（Normative references）であった ISO/IEC 17788 Cloud

computing ― Overview and vocabulary（概要と用語※）は廃止され、ISO/IEC22123-1 Cloud computing ― vocabulary（用語※）、ISO/IEC22123-2 Cloud computing ―Concepts（概念※）として 2023 年に発行された。

また、ISO/IEC 27036-4 における参考文献（Bibliography）であった ISO/IEC 17789 Cloud computing ― Reference architecture は廃止され、ISO/IEC22123-3 Cloud computing ― Reference architecture（レファレンスアーキテクチャ※）として、2023 年に発行された。

（※）内は仮訳

2.4.4 ISO/IEC 20000-1

Information technology - Service management - Part 1: Service management system requirements

（情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項）

ISO/IEC 20000-1 は、サービス提供者が IT サービスの品質を効率的・効果的に確保、改善するための仕組みを定めた要求事項であり、IT サービスマネジメントシステム（ITSMS）認証の認証基準として活用されており、国内の大半のクラウドサービスプロバイダやデータセンター事業者等が認証を取得している。サービスマネジメントシステムは、サービスの計画、設計、移行、提供、改善を含むサービスライフサイクルのマネジメントを支援するものであり、SMS を実施・運用することによって、継続的な可視化、サービス管理、そして継続的な改善を実施できるため、効果と効率の改善へとつながる。この規格では、供給者管理、インシデント管理、サービス継続管理、可用性管理、情報セキュリティリ管理等のプロセスについて規定しており、IT サービスの情報セキュリティ・運用等の品質確保に必要な要求事項を包括的に規定している。

2.4.5 SOC2、SOC2+

SOC（System and Organization Controls）とは、米国公認会計士協会（AICPA）が定義した、業務受託会社（Service Organization）における内部統制保証報告やサイバーセキュリティに関する内部統制保証報告の枠組みである。AICPA では、「SOC for Service Organization」として、業務受託会社（アウトソーシング事業者）向けに 3 つの内部統制の保証報告の枠組み（SOC1、SOC2、SOC3）を定めている。本書では SOC2 を中心に紹介する。

SOC2

SOC2 は、AICPA が定めたトラストサービスの原則と規準（Trust Service Criteria）に従って、受託会社（データセンター、クラウドサービス等のアウトソーシング事業者）が記述したセキュリティ、可用性、処理のインテグリティ、機密保持、及びプライバシーの 5 分野に関連する内部統制に対して、監査法人が手続を実施した結果と意見を表明した報告書である。

SOC2 では、この中から一つ以上を選択（複数選択可能、但し「セキュリティ」は必須）し、評価が行われる。

評価の結果は、「受託会社監査人の意見」、「受託会社の経営者の確認書」、「システムの記述」、「監査人が実施した運用評価手続とその結果」の 4 パートで構成された「SOC2 保証報告書」として詳細がまとめられ、サービスの利用者（委託先等）がこれを利用することができる。特に「SOC2 保証報告書」内の「システムの記述」のパートには、受託会社が整備し、運用する内部統制の仕組みが詳細に記述されるため、クラウドサービスカスタマにとって、クラウドサービスプロバイダの提供するサービスに関する統制を確認する際に有用である。

SOC2+

アウトソーシング事業者（受託会社）によっては、トラストサービスの原則と規準に準じるのみでは物足りない、あるいは、顧客のニーズを十分に満たせないといったケースも考えられることから、AICPA では SOC2 報告書の範囲拡張を認めており、これを「SOC2+」報告書と位置付けている。このことにより、アウトソーシング事業者（受託会社）は、任意の評価規準（例えば、ISO/IEC 27001、政府統一基準群等）の追加が可能であり、追加された評価基準に対する監査人の意見等を「SOC2+報告書」に織り込ませることも可能である。米国では、「HIPAA」や「NIST SP 800-53」を追加する等の取組みが多数みられる。アウトソーシング事業者（受託会社）にとっては、複数の追加評価基準を組み合わせ対応することで、複数の顧客の要求に個別に対応する負荷を軽減することを可能とする。

2.4.6 クラウドに関連する NIST 文書

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は、米国の連邦政府機関の１つで、産業技術等に関する規格の標準化を支援している。

NIST が発行する文書の中でも、SP 800 シリーズは、米国の連邦政府機関を対象にした情報システムのセキュリティ対策についてまとめた文書であり、セキュリティマネジメント、リスクマネジメント等の様々なセキュリティに関する内容を網羅したものとなっている。特に、ISMS、クラウドに関するものとしては、次の文書が発行されており、本文書の 2.3.1 FedRAMP（米国政府）でもベースとして用いられているように、クラウド関連の制度や文書で参照されている。

NIST SP 800-53（Rev.5）

Security and Privacy Controls for Information Systems and Organizations

組織と情報システムのためのセキュリティ及びプライバシー管理策

セキュリティとプライバシーの管理策の包括的かつ柔軟なカタログを提供しており、情報システムおよび組織におけるセキュリティとプライバシーの対策として参照されている。これらの管理策は、変化する脅威、脆弱性、要件、およびテクノロジーに基づいて、現在および将来の保護ニーズを満たすために使用できる。管理策は、従来の企業 IT から IoT、産業自動制御システムまで、情報を処理、保管、または送信するいかなる組織やシステムにも実装可能である。

米国連邦政府機関の情報システムでは、行政管理予算局の通達（OMB CircularA-130）や連邦情報セキュリティ近代化法（FISMA）により、SP800-53 の管理策を使用することが義務付けられている。

本書は、SP800-37（連邦政府情報システムに対するリスクマネジメントフレームワーク）のような他の文書と共に、連邦組織が FISMA や 1974 年プライバシー法、行政管理予算局規程等のセキュリティおよびプライバシー要件を満たすために必要な管理策を識別できるように設計されている。カタログにある管理策を、リスクベースで選択することにより（管理策選択プロセス）、組織が、求められるセキュリティおよびプライバシー要件に準拠し、システムに適切なセキュリティ対策を行い、個人のプライバシーを保護することができるようになっている。

また、本書では、組織内および組織間のコミュニケーションを向上させるため共通の用語集も提供し、セキュリティ、プライバシー、リスクマネジメントの概念に関して共通の用語でディスカッションすることをサポートしている。

管理策の選択プロセスは、組織全体のリスクマネジメントプロセスやシステムのエンジニアリングプロセス、リスクマネジメントフレームワーク、サイバーセキュリティフレームワーク、またはプライバシーフレームワークの一部として適用することができる。

管理策を選択する基準は、ミッションやビジネスのニーズ、ステークホルダーの保護ニーズ、脅威、脆弱性、法律、行政命令、指令規則ポリシー、基準、ガイドラインに準拠するための要件など、さまざまな要因によってもたらされる情報によって導き出すことができる。

（出典：https://www.jipdec.or.jp/library/report/20201215_01.html）

NIST 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の保護

Protecting Controlled Unclassified Information in Nonfederal Systems and Organization

米国では、2010 年 11 月の大統領令（Executive Order 13556）により、機密と指定されていないが管理対象となる重要情報（Controlled Unclassified Information：以下 CUI という）が定義された。CUI は、電子ファ

イル・メール、取引先や委託先等の情報（契約等）、物理的な記録（紙媒体等）等もその対象とみなせる広範囲なもので、機密とまではいかないが流出した場合には損害を与える可能性が出てくる情報であり、そのため CUI を扱う民間企業に対してもその保護が義務付けられている。

NIST SP 800-171 は、連邦政府機関に対して、連邦政府外のシステムと組織に存在するこの CUI 保護のために推奨されるセキュリティ要件を提供しており、この要件は 17 分野 97 項目にわたる詳細なものとなっている。

サイバーセキュリティフレームワーク（CSF）（ver.2.0）

重要インフラのサイバーセキュリティの改善を目的として 2014 年 2 月に NIST により策定・公表されたのがサイバーセキュリティフレームワーク（CSF：Cyber Security Framework）である。

このフレームワークの Ver.1 は、サイバーセキュリティリスクを管理するためのリスクベースアプローチであり、組織のサイバーセキュリティリスク対策の現状（今の状態）とビジネスニーズをもとにした期待される成果（目指す状態）とのギャップ分析を実施し、対策の改善を特定して組織としての対策レベルの底上げを図ることができるようにしている。

その中で、「特定」「防御」「検知」「対応」「復旧」という 5 つの機能が示されているが、これはリスクマネジメントプロセスに取って代わるものではなく、（普段用いているマネジメントやリスク管理の言葉によって）役員や従業員がサイバーセキュリティリスクの基本概念を簡単につかめるようにするためのものである。また、このフレームワークの特徴として、サイバー攻撃の特定と防御、サイバー攻撃を検知したときの対応、サイバー攻撃を受けたときの被害からの復旧、といったようにサイバー攻撃の観点でまとめられている点がある。他にも、利害関係者に関するサプライチェーンについても、このフレームワークで考慮されている点等があげられる。

詳細な技術的なセキュリティ対策については記載されていないが、それはサイバーセキュリティリスクの許容度は組織によって異なり、サイバーセキュリティ対策を組織のリスクレベルに応じて実施するように設計されているからである。

2024 年 2 月に発行された Ver.2.0 では、対象が重要インフラから、あらゆる組織に拡大された。また、CSF を構成する機能に、新たにガバナンスが追加され、ガバナンスの中の 1 カテゴリにサプライチェーンリスクマネジメントが含められ 10 のサブカテゴリ（サプライチェーンに関するリスクマネジメント、役割責任等）が設けられる等の変更が加えられている。

その他の文書

上記の他、次の文書も発行されている。

NIST SP 800-144 パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン

NIST SP 800-146 クラウドコンピューティングの概要と推奨事項

おわりに

2016 年 1 月に閣議決定され、日本政府が策定した「第 5 期科学技術基本計画」の中において、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する超スマート社会（Society 5.0）の概要が公開された。超スマート社会の情報インフラは、巨大なクラウド群と無数のセンサ、バイオテクノロジー、アクチュエータ等で構成された IoT 機器群から成ると考えられている。そのため、様々なクラウドサービスに関連する制度・ガイドライン等の策定が国家レベル又は国際レベルの組織で進められている。クラウドサービスを選定・利用する際に、このような制度・ガイドライン等を参照することは、クラウドサービスの安全性や品質を確認するうえで役立つと思われる。

今回、本書で紹介した制度・ガイドライン等は全体の一部に過ぎないが、クラウドサービスに関連する制度・ガイドライン等の多くが ISO/IEC 27001 を基盤とする若しくは参照するとともに、ISO/IEC 27017 等と整合が図られている又はこれらの規格が参照されていることが、本調査によって確認された。これらのことから、ISO/IEC 27001 及びその関連規格は、クラウドセキュリティマネジメントにおける共通基盤としての役割を果たしていると言えるだろう。

また、ISO/IEC 27017 は、ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範であり、管理策の具体性に関しては他のガイドラインと比較されることも多いが、クラウドサービスカスタマによる、クラウドサービスの活用を含む情報セキュリティマネジメントシステムの構築においては、クラウドサービスプロバイダ側とクラウドサービスカスタマ側における責任分掌を考慮し、必要な対策を実装することが重要であると考えられており、クラウドサービスカスタマ側向けの管理策を網羅している点においては、ISO/IEC 27017 が代表的な管理策の実践の規範であることが調査でわかった。さらに、ISO/IEC 27017 を補う管理策の規範として、ISO/IEC 27018 及び ISO/IEC 27036-4 の規範も、クラウドサービスカスタマ側の責任に配慮した管理策を紹介していることが、今回の調査によって再認識された。

本書では、クラウドサービスの中でも特に安全性の点から記載したが、クラウドサービスにおいては、その継続性（導入後の安定した運用）も重要であり、ISO/IEC 20000 や事業継続のためのマネジメントシステムを定めた ISO 22301 を参考にすることも有用であると考える。今後の課題としては、クラウドサービスの安全性、継続性等の品質確保のためには、このような制度・ガイドライン等を参照・確認するとともに、今回の調査で認識されたとおり、クラウドサービスカスタマ側、クラウドサービスプロバイダ側の双方の立場からクラウドサービスの安全性、継続性等の品質確保のための対策を検討する必要性を挙げたい。特にクラウドサービスの責任分界点を明確にしつつ、クラウドサービスの発注者が、クラウドサービスに係るすべてのリスクを認識して、自ら情報セキュリティマネジメントを行うことが必要であり、そのための方策については、別途、検討していく予定である。

最後に、ISMS 専門部会の委員、関係者の皆様に対しては、本書の作成、レビューのために多くの時間を費やしていただいたことに、この場を借りて厚くお礼を申し上げる。

一般財団法人日本情報経済社会推進協会（JIPDEC）

ISMS 専門部会

（順不同・敬称略）

氏名	会社・機関名
委員	
【主査】 駒瀬　彰彦	株式会社アズジェント
相羽　律子	株式会社日立製作所
河野　省二	日本マイクロソフト株式会社
笹原　英司	一般社団法人日本クラウドセキュリティアライアンス
佐藤　慶浩	オフィス四々十六
澤部　直太	ナオサイバーテック株式会社
中村　良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）
オブザーバ	
池田　佳高	経済産業省商務情報政策局サイバーセキュリティ課
和田　友英	経済産業省産業技術環境局　国際電気標準課
保木野　昌稔	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

〒106-0032 東京都港区六本木１丁目９番９号 六本木ファーストビル
一般財団法人 日本情報経済社会推進協会
TEL 03-5860-7561　FAX 03-5573-0561
URL https://www.jipdec.or.jp/