（案）

ISMAP 管理基準

令和２年６月３日
（令和●年●月●日最終改定）

ISMAP 運営委員会

改定履歴

日付	改定内容
令和２年　６月　３日	ISMAP に関する規程等を施行
令和２年　８月２０日	誤記の修正などの軽微な改定
令和２年１２月２５日	別紙１を追加 誤記の修正などの軽微な改定
令和３年　３月１２日	「1.3.15 暗号」の定義を改定 誤記の修正などの軽微な改定
令和３年　６月２２日	「2.2.5 監査の対象となる期間」の記載を改定 誤記の修正などの軽微な改定
令和４年　４月　１日	第 5 章の管理策基準に管理目的を追記 「政府機関等の情報セキュリティ対策のための統一基準」の 2021 年 7 月の改定に伴い詳細管理策を改定 「1.2 基準の特質」の記載を改定 「2.2.3 システムと内部統制の全体像」の記載を改定 「2.2.4 基本言明要件」の記載を改定 誤記の修正などの軽微な改定
令和４年１１月　１日	ISMAP-LIU に関する記載を追加
令和５年　７月　３日	2.2.4 の改定 附則の新設
令和５年　９月２２日	2.2.4(3)の改定 2.2.4(4)の新設
令和６年　７月　１日	「政府機関等のサイバーセキュリティ対策のための統一基準群」の 2023 年 7 月の改定に伴い、第 5 章管理策基準及び別表３～５の詳細管理策を改定 （新設） 8.1.5.4.P 12.2.1.15 13.2.3.7.P 16.1.5.10 （改定） 7.2.2.18 9.1.1.16 9.2.3.11.PB 13.1.3.1 13.1.3.5 誤記の修正などの軽微な改定
令和６年　８月１日	別表８の改定
令和●年　●月●日	参照規格の改定に伴う全般的な改定

目次

第1章

1.1　ISMAP 管理基準の目的

ISMAP 管理基準(以下「本管理基準」という。)は、クラウドサービス事業者が ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト(以下「ISMAP 等クラウドサービスリスト」という。)への登録申請を行う上で実施すべきセキュリティ対策の一覧及びその活用方法を示すことを目的としており、ISMAP(以下「本制度」という。)の情報セキュリティ監査基準等に従って監査を行う場合、原則として監査人が監査の前提として用いる基準となる。

1.2　基準の特質

本制度においては、情報セキュリティ監査の仕組みを活用した枠組みを活用することとしている。これは、民間において実施されている情報システムに関するセキュリティ監査により、既に一定程度の知見が集積していること、一定の評価水準を確保することが可能なこと、運用後の継続的な確認が可能であることといった観点による。

こうした観点から、本管理基準は、国際規格に基づいた規格(JIS Q 27001:2023、JIS Q 27002:2024、ISO/IEC 27014:2020) に準拠して編成された「情報セキュリティ管理基準(令和７年改正版)」(以下「情報セキュリティ管理基準」という。)及び国際規格に基づいた規格 (JIS Q 27001:2014、JIS Q 27002:2014、JIS Q 27017:2016) に準拠して編成された「クラウド情報セキュリティ管理基準(平成 28 年 3 月版)」(以下「クラウド情報セキュリティ管理基準」という。)を基礎としつつ、「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 (令和７年度版)」(以下「統一基準」という。)及び「NIST Special Publication 800-53 Revision 5」(以下「SP800-53」という。)を参照して作成されている。

本管理基準の主な特徴は次の通りである。

⑴　クラウドサービス事業者を実施主体とした管理基準としている。

⑵　政府において最も多く扱われる情報の格付けの区分である機密性 2 の情報を扱うことを想定して策定している。

⑶　暗号化消去もデータの消去(若しくは抹消)の方法の一つと定義している。

1.3　用語及び定義

本項に示す用語及び定義以外に関しては、ISMAP 基本規程、ISMAP クラウドサービス登録規則、ISMAP-LIU クラウドサービス登録規則及び以下の規格の用語の定義に準じる。

- JIS Q 27001:2023 (ISO/IEC 27001:2022)
- JIS Q 27002:2024 (ISO/IEC 27002:2022)
- ISO/IEC 27014:2020
- JIS Q 27017:2016 (ISO/IEC 27017:2015)

1.3.1　情報セキュリティガバナンス

社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること。

1.3.2　クラウドコンピューティング

共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーション等）について、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態。

＜注記＞これよりも広い定義が使われることもある。

1.3.3　クラウドサービス

クラウドコンピューティングを提供するサービス。

1.3.4　クラウドサービス事業者

クラウドサービスを提供する事業者又は組織。

クラウドサービスを用いて情報システムを開発・運用する又は他のクラウドサービスを用いて自らのクラウドサービスを提供することもある。

1.3.5　クラウドサービス利用者

クラウドサービスを利用する組織。

1.3.6　クラウドサービスのユーザ

クラウドサービス利用者（クラウドサービスを利用する組織）において、クラウドサービスを利用する者。

1.3.7　供給者

事業者がクラウドサービスの提供を行うためのリソース等の一部について、当該事業者に対して供給する者。

1.3.8　委託先

情報処理業務の一部又は全てを実施させる外部の者。

1.3.9　情報

「クラウドサービス事業者が扱う情報」、「クラウドサービス利用者が扱う情報」について特に区別しない場合の呼称。

1.3.10　クラウドサービス事業者が扱う情報

クラウドサービス事業者が扱う各種の情報のうち、クラウドサービス派生データ及び契約データを指す。

1.3.11　クラウドサービス利用者が扱う情報

クラウドサービス利用者の扱う各種の情報のうち、クラウドサービスに入力した又はクラウドサービスの公開インタフェースを使ってクラウドサービス利用者又はその代理人がクラウドサービスの能力を実行して生じるデータで、クラウドサービス利用者に管理責任があるもの。例えば、クラウドサービス利用者が、クラウドサービス上に作成し、保有するデータなど。

1.3.12　クラウドサービス派生データ

クラウドサービス事業者が扱う情報のうち、クラウドサービス利用者がクラウドサービスを利用することによって、クラウドコンピューティング環境上に派生的に生成されるデータで、クラウドサービス事業者に管理責任があるもの。例えば、クラウドサービス利用者の属性、アカウント情報、データ検索用のタグなど。

1.3.13　契約データ

クラウドサービス事業者が扱う情報のうち、契約に関するデータであり、クラウドサービス事業者に管理責任があるもの。

1.3.14　消去(若しくは抹消)

消去には、媒体を物理的に破壊する物理的消去、媒体を消磁装置により抹消する電磁的消去に加え、暗号化消去も含む。暗号化消去とは、元のデータを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能にする方法を指す。

1.3.15　暗号

暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された電子政府推奨暗号又はそれと同等以上の安全性を有する暗号を指す。

1.3.16　利用者

「クラウドサービス利用者」の様に対象を限定する形容がなされず単に「利用者」という場合、当該管理策において関係するシステムを何らかの形において利用若しくは取り扱う者を指す。

1.3.17　統制目標

クラウドサービス事業者が、リスクに対応するために達成するべき統制の目標とする項目。ガバナンス基準及びマネジメント基準のうち（X.X.X）という３桁の番号で表現される。管理策基準のうち（X.X）という２桁の番号で表現される。

1.3.18　詳細管理策

クラウドサービス事業者が、統制目標を実現するために実施して満たすべき事項。ガバナンス基準及びマネジメント基準のうち（X.X.X.X）という４桁の番号で表現される。管理策基準のうち（X.X.X）という３桁の番号で表現される。

1.3.19　個別管理策

クラウドサービス事業者が、詳細管理策のそれぞれに対して、自身のクラウドサービスにおいて具体的に設計した個々の統制。

1.3.20　整備状況評価

クラウドサービス事業者が本管理基準に準拠して統制目標としての管理策及び詳細管理策を実施し、必要な統制を監査の対象期間内のある時点において整

備していることを評価することをいう。

1.3.21　運用状況評価

クラウドサービス事業者が本管理基準に準拠して統制目標としての管理策及び詳細管理策を実施し、整備した統制が監査の対象期間にわたり有効に運用していることを評価することをいう。

1.3.22　業務依頼者

本制度における監査業務を依頼するために、業務実施者と業務契約を締結する者を指し、クラウドサービス事業者を指す。

1.3.23　業務実施者

監査機関に所属する者のうち、本制度における監査業務を実施する者をいう。

第2章

2.1　本管理基準の構成

本管理基準は、「ガバナンス基準」、「マネジメント基準」及び「管理策基準」から構成される。それぞれの基準は、統制目標と詳細管理策で構成される。それぞれの基準が対象として想定する主体や各項目の粒度の関係を示した概念図が下記のものとなる。（図１）

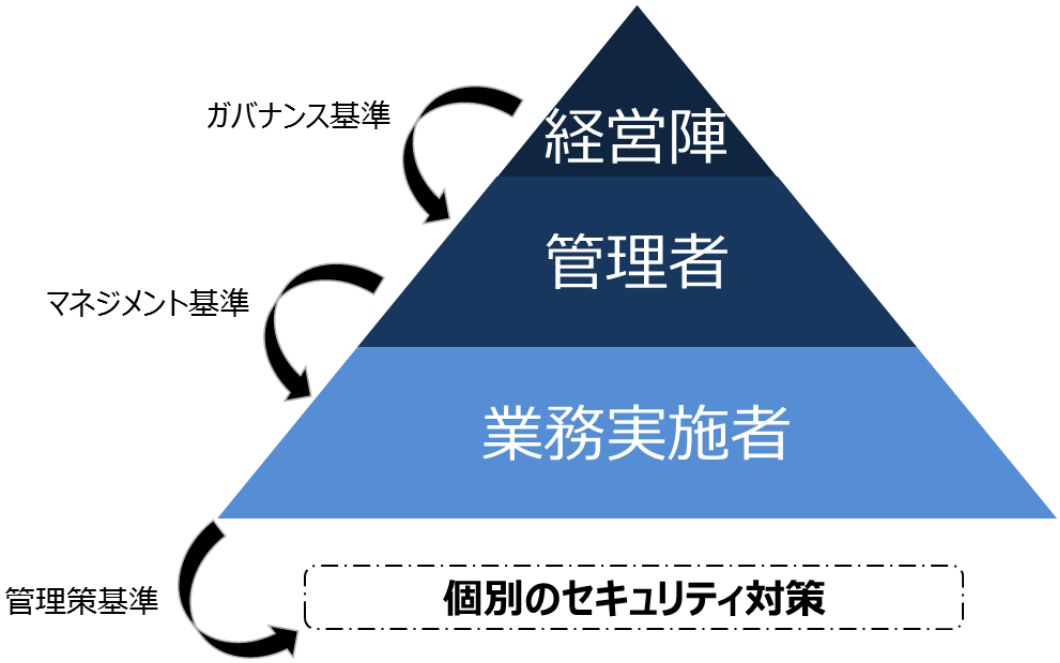

図１：管理基準の構成

「ガバナンス基準」は、組織体のガバナンスのうち、情報セキュリティガバナンスを確立するための目的及びプロセスを定めている。

「マネジメント基準」は、管理者が実施すべき事項として、情報セキュリティマネジメントの確立、運用、レビュー、維持及び改善、文書化した情報の管理並びに情報セキュリティリスクコミュニケーションに必要な事項を定めている。

「管理策基準」は、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実施する際の選択肢を与えるものである。なお、「管理策基準」における詳細管理策を実施するための参考情報（例示）として、手引きを定めている。

2.2　基本言明要件

クラウドサービス事業者は、言明の対象となる管理策として、以下の内容を実施し、書面にて言明を行わなければならない。また、特に変更の言明が行われていない限りにおいて、その言明はクラウドサービス事業者が責任を負うものとして有効であると見なされる。なお、言明の対象となるクラウドサービスの基盤に言明の対象外となるサービスを利用している場合において、当該対象外のサービスが ISMAP クラウドサービスリストに登録されている場合には、当該対象外のサービスが実施している統制を引き継ぐことで当該統制に係る監査の手続を省略することができる。

⑴　ガバナンス基準

全て実施しなければならない。

⑵　マネジメント基準

全て実施しなければならない。

⑶　管理策基準

全ての統制目標としての管理策について、原則として実施しなければならない。また、詳細管理策（X.X.X）も原則として実施すべきものとする。

他方、クラウドサービス事業者は自身の提供するサービスと照らし、合理的な適用が不可能若しくはリスク分析の結果、実施不要と適切に判断した統制目標としての管理策及び詳細管理策については、その理由を示すことで対象外とすることができる。

第3章　ガバナンス基準

3.1　情報セキュリティガバナンスの概要

情報セキュリティガバナンスでは、組織体における複数のガバナンスの領域のうち、組織体の情報セキュリティ確保の達成に関するガバナンスを扱う。情報セキュリティに関するガバナンスモデルの策定にあたっては、情報技術等の他のガバナンスの領域とのモデルの対象範囲の重複の可能性があり、コーポレートガバナンスの観点からそれぞれの整合についての考慮が求められる。

ガバナンス主体は、組織体内に情報セキュリティマネジメントシステムを構築する。情報セキュリティマネジメントシステムの目的は、組織のサイズ、スケール及び構造により異なる可能性があり、それらを整合させるようにする。

なお、本管理基準の「第４章　マネジメント基準」に示す管理策にも、情報セキュリティマネジメントシステムにおけるガバナンスに対応する内容が含まれている。

3.2　情報セキュリティガバナンスの目的

ガバナンス主体は、以下に示す目的に照らして適切であるような、組織体における情報セキュリティガバナンスの目的を設定する。

目的１：組織体全体の統合された包括的情報セキュリティを確立する
目的２：リスクに基づく取組を採用して意思決定を行う
目的３：投資の方向性を決定する
目的４：内部及び外部の要求事項との適合性を確実にする
目的５：セキュリティに積極的な文化を醸成する
目的６：セキュリティのパフォーマンスが現在及び将来の組織体の要求事項を満たすことを確実にする

3.3　情報セキュリティガバナンスのプロセス

ガバナンス基準における統制目標及び詳細管理策は、別表 1 のとおりとする。

第4章　マネジメント基準

4.1　マネジメント基準

マネジメント基準は、JIS Q 27001:2023 を基に、情報セキュリティについて組織を指揮統制するために調整された活動である、情報セキュリティマネジメントの確立、運用、レビュー、維持及び改善、文書化した情報の管理並びに情報セキュリティリスクコミュニケーションを行うための基準を定める。

4.2　記載内容について

クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。当該情報セキュリティリスクコミュニケーションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9 に規定する。

4.3　凡例

4.4 以降は、以下の構成をとる。なお、統制目標及び詳細管理策は、別表 2 のとおりとする。

4.4　情報セキュリティマネジメントの確立　[27001-4.4]
4.4.1　組織の役割、責任及び権限　[27001-5.3 / 5.1]
4.4.1.1　トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。　[27001-5.1b) / 5.1e) / 5.1f)]
:
[27001-X.X.X]は、JIS Q 27001:2023 において関連する条項(X.X.X)を示す。

4.4　情報セキュリティマネジメントの確立［27001-4.4］

情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを

実施し、その対応を計画し実施する。それにより、必要なプロセス及びそれらの相互作用を含む、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。

4.5　情報セキュリティマネジメントの運用［27001-8］

4.6　情報セキュリティマネジメントの監視及びレビュー［27001-5.1 / 8.2 / 9 / 10.2］

4.7　情報セキュリティマネジメントの維持及び改善［27001-10］

4.8　文書化した情報の管理［27001-7.5］

4.9　情報セキュリティリスクコミュニケーション

利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。

マネジメント基準における統制目標及び詳細管理策は、別表2のとおりとする。

第5章　管理策基準

管理策基準は、情報セキュリティ管理基準における管理策の整理体系を踏襲した「5 組織的管理策」、「6 人的管理策」、「7 物理的管理策」及び「8 技術的管理策」並びにクラウド情報セキュリティ管理基準の一部の管理策を基礎とした「9 クラウドサービス固有の管理策」で構成される。

管理策基準における統制目標及び詳細管理策は、別表3のとおりとする。

附則（令和５年７月３日 施行）
（施行期日）
１ この規程は、令和５年７月３日から施行する。

附則（令和５年９月２２日 施行）
（施行期日）
１ この規程は、令和５年９月２２日から施行する。
ただし、2.2.4(4)の規定は、監査対象期間の開始日が令和５年 10 月１日以降となる手続に対して適用する。

附則（令和６年７月１日 施行）
（施行期日）
１ この規程は、令和６年７月１日から施行する。
ただし、管理策基準 7.2.2.18、8.1.5.4.P、9.1.1.16、9.2.3.11.PB、12.2.1.15、13.1.3.1、13.1.3.5、13.2.3.7.P 及び 16.1.5.10 は、監査対象期間の末日が令和７年３月３１日以降となる手続に対して適用する。

附則（令和●年●月●日 施行）
（施行期日）
１ この規程は、令和●年●月●日から施行する。