ISMAP 管理基準マニュアル

令和３年７月１２日

(令和４年７月１日最終改定)

ISMAP 運用支援機関

目次

改定履歴

日付	改定内容
令和３年７月１２日	新規作成
令和４年７月１日	2.2 章：ISMAP 管理基準においてベースとなった各種基準の改定時における ISMAP 管理基準の改定の進め方を記載。 2.4 章：調達省庁と CSP 間の責任分解に関する参考資料について追記 2.5 章：ISMAP 管理基準におけるレベル分けに関する参考資料について追記 2.7 章：2.7.2 の「利用者の定義」に関する定義の見直しを追記 2.7.6 の「セキュリティインシデント通知の考え方」の章に関しては記載誤りのため、削除 2.7.8 に 2021 年 7 月に統一基準改定に伴う新規追加技術となるゼロトラストアーキテクチャに関する考慮事項について追記 全般：管理策番号及び管理策内容に関する誤字・脱字及び規定類の修正に伴う変更点の修正 全般：統一基準において「論理的消去」を「暗号化消去」と表現していることから ISMAP 管理基準においても同様の表現に修正。

第1章　総則

1.1　目的

ISMAP 管理基準マニュアル（以下、「本マニュアル」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への登録を行うにあたり、クラウドサービスに対するセキュリティ対策の進め方及び管理基準の理解の一助となることを目的とする。

1.2　本マニュアルの構成

1 章では ISMAP に関する用語説明及び本マニュアルの説明を記載する。

2 章では、ISMAP 管理基準の概要及び制度作成までの背景を記載する。また、併せて ISMAP において前提となっている責任共有モデルに関する説明及び、ISMAP 適用においてクラウドサービスプロバイダ(CSP)が実施する個別管理策の策定作業の流れの説明や参考資料を記載する。

3 章以降では、各管理基準(ガバナンス基準、マネジメント基準、管理策基準)の各章の概要や、ISMAP 管理基準の基礎となったクラウド情報セキュリティ管理基準(※)からの変更点に関する説明、詳細管理策に関する説明について記載する。

※クラウド情報セキュリティ管理基準は、「情報セキュリティ管理基準（平成 28 年改正版）」（平成 28 年経済産業省告示第 37 号）を基礎として、2019 年時点の ISO/IEC27000 シリーズの規格体系の変更を考慮し、改正を行った基準である。ISMAP 管理基準との関係性に関しては、後述となる「2.2 章 ISMAP 管理基準と他の情報セキュリティ管理基準との関係」を参照されたい。

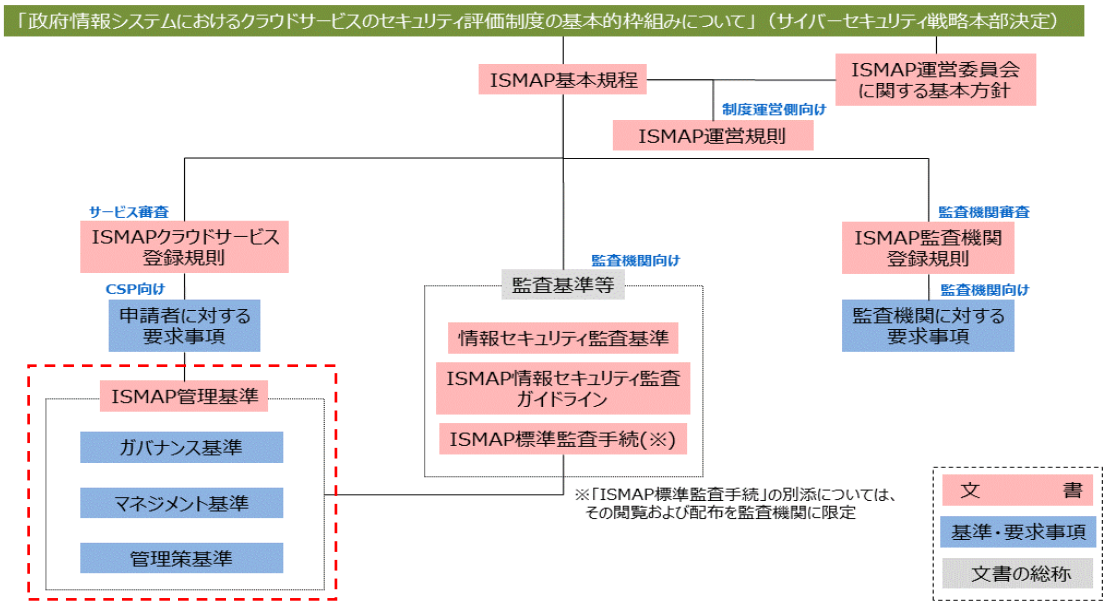
なお、ISMAP 管理基準は、JIS 規格を基礎として作成しているため、JIS 規格を由来とした項目については説明の対象外としている。

1.3　本マニュアルの位置づけ(ISMAP 管理基準との関係)

本マニュアルは以下の赤枠部分に示す ISMAP に関する規程等のうち「ISMAP 管理基準」の補足資料としての位置付けとなる。その他の各種規程については、以下の URL を参照されたい。

https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010007

ISMAPに関する規程等



1.4　ISMAP で定義されている用語

本マニュアルで用いる用語の定義は、「政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程」（以下、「基本規程」という。）及び「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」（以下、「ISMAP 管理基準」という。）における定義に準ずる。ISMAP 管理基準に関しては以下を参照されたい。
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028

また、ISMAP 管理策の中にはクラウドサービスカスタマー(CSC)として、「利用者」、「全ての利用者」、「クラウドサービス利用者」及び「クラウドサービスのユーザ」の４種類の利用者が登場する。該当する管理策の「利用者」がどのような位置づけに当たるかについては、2.7 において後述する「「利用者」の定義」を参照されたい。

1.4.1 クラウドサービス

「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(平成 30 年 6 月 7 日各府省情報化統括責任者（CIO）連絡会議決定のあとに定義された「事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」をいう。(ISMAP 基本規程 1.4.1)

なお、パブリッククラウドとプライベートクラウドとを組み合わせたハイブリッドクラウド環境におけるプライベートクラウド部分や、プライベートクラウド単体のサービスに関しては、顧客ごとにカスタマイズが行われるものであり、CSP が言明に対する監査・評価が難しい類のクラウドサービスであれば、本制度の対象外となる。

1.5　本マニュアルの 3 章～18 章の記載内容

3 章には、ガバナンス基準について、以下の内容を記載している。
- 目的,概要：JIS Q 27014：2015 5.3 章を基に記載。

4 章には、マネジメント基準について、以下の内容を記載している。
- 目的：「情報セキュリティ管理基準（平成 28 年改正版)」の内容を基に記載。
- 概要
- 「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(平成 30 年度版)（以下、統一基準という)」由来の変更点
- 「NIST SP800-53 rev4」由来の変更点
  ISMAP 管理基準の基礎となったクラウド情報セキュリティ管理基準に対する、「統一基準」及び「SP800-53 rev4」由来の変更点を記載する。
  - 変更点の説明は、詳細管理策の単位で行う。
  - 詳細管理策に追加された「統一基準」及び「SP800-53 rev4」の具体的な観点を記載する。
  - ISMAP 管理基準に追加／修正された詳細管理策を記載するとともに、変更箇所を明記する。

5 章～18 章には、管理策基準について、以下の内容を記載している。
- 目的及びクラウドサービス固有の管理策
  クラウド情報セキュリティ管理基準の 5 章～18 章の目的及び JIS Q 27017:2016 を参考にクラウドサービス固有の管理策に関する説明を記載。
- 「統一基準」由来の変更点、「NIST SP800-53 rev4」由来の変更点
  各詳細管理策における「統一基準」及び「SP800-53 rev4」由来の変更点を記載する。

・詳細管理策に追加された「統一基準」及び「SP800-53 rev4」の具体的な観点を記載し、変更箇所を明記する。
・詳細管理策の解説
統制目標（3 桁管理策）及び詳細管理策（4 桁管理策）に対する解説(補足説明)を記載する。

また、3 章～18 章において、赤字及び下線を引いている部分はクラウド情報セキュリティ管理基準からの変更箇所を示す。

1.6　本マニュアルの利用ガイド

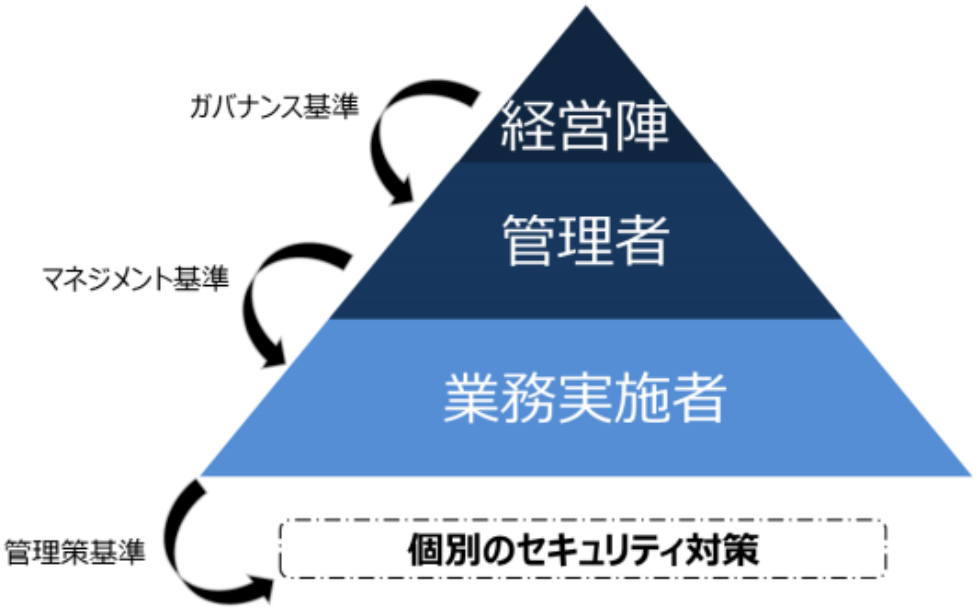
本マニュアルの利用方法に関して、以下に記載する。

#	利用の目的	参考章
1	ISMAP 全体構成及び他の制度基準との関係性について確認したい	2.1 章 2.2 章
2	ISMAP 管理基準の読み方について知りたい	2.3 章 2.7 章
3	クラウドサービスの登録/責任範囲、登録に向けたアセスメントの考え方や参考資料を知りたい	2.4 章～ 2.7 章
4	ISMAP 管理策の各管理策において以下を知りたい ・目的 ・作成に関する背景 ・3 桁,4 桁管理策の意図・内容	-
4-1	・ガバナンス基準について知りたい	3 章
4-2	・マネジメント基準について知りたい	4 章
4-3	・管理策基準について知りたい ※管理策番号と章番号が連動	5 章～18 章

第2章　ISMAP 管理基準の概要

2.1　ISMAP 管理基準の構成

ISMAP 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を以下に示す。



・「ガバナンス基準」は、経営陣が実施すべき事項として、JIS Q 27014(ISO/IEC 27014)の内容を精査し、監査の実施可能性の観点から JIS Q の実施の手引きのような具体的な実施タスクに再構成したものである。

・「マネジメント基準」は、情報セキュリティマネジメントの計画、実行、点検、処置、及び、リスクコミュニケーションに実施事項を定めたものである。

・「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決定する際の選択肢を与えるものである。

2.2　ISMAP 管理基準と他の情報セキュリティ管理基準との関係

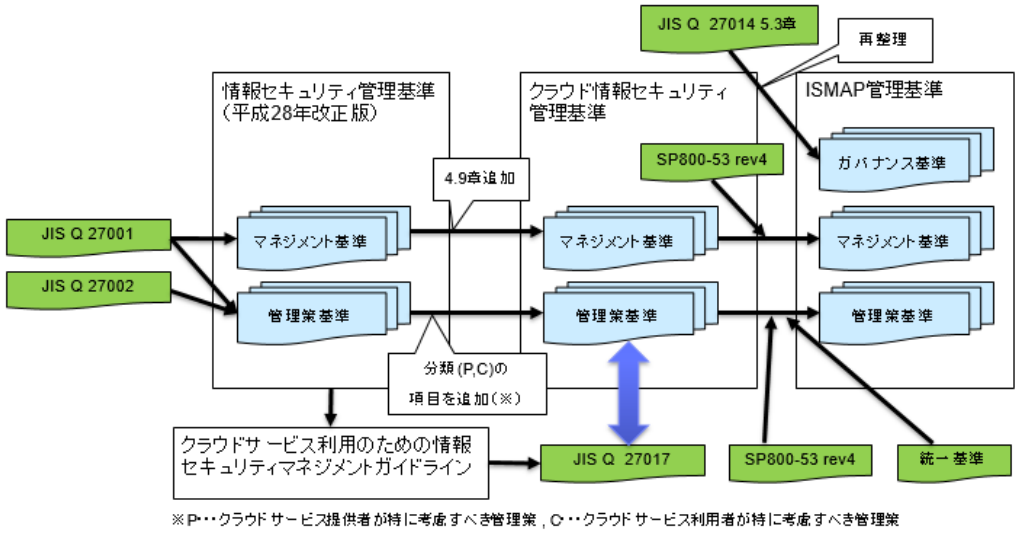
ISMAP 管理基準は、情報セキュリティに関する JIS Q 27001:2014, JIS Q 27002:2014 と、クラウドサービスの情報セキュリティに関する JIS Q 27017:2016 に準拠して編成された「クラウド情報セキュリティ管理基準(平成 28 年度版)」(以下、「クラウド情報セキュリティ管理基準」という)を基礎としている。

それぞれ、ガバナンス基準、マネジメント基準、管理策基準に関して、以下のような観点の追加を行っている。

- ガバナンス基準については、クラウド情報セキュリティ基準の策定以降に発行された JIS Q 27014:2015 を参考としている。
- マネジメント基準については、NIST SP800-53 rev4 の内容を参考としている。
- 管理策基準については、政府機関等の情報セキュリティ対策のための統一基準(以下、「統一基準」という)の内容を、その趣旨を残したままクラウドサービス事業者向けに書き換えて追記し、NIST SP800-53 rev4 の内容から、インシデントレスポンスに関連する内容を中心に、JIS Q 27001, 27002, 27014, 27017 及び統

一基準に含まれない観点を追加している。

以下の遷移図に ISMAP 管理基準の基礎となっている各基準との関係及び追加要素を示す。



今後、ISMAP においてベースとなった

- クラウド情報セキュリティ管理基準（マネジメント基準、管理策基準）
- NIST SP800-53 （コントロール）
- 統一基準（遵守事項、基本対策事項）
- JIS Q 27014（ガバナンス基準）

が改定される際には、以下の観点に関する影響調査を実施の上、ISMAP 管理基準の改訂を行う。

- 各基準の改定箇所と既に ISMAP 管理基準に取込箇所を確認。ISMAP 管理基準への取込箇所であった場合、改訂による ISMAP 管理基準の影響を確認。

- 各基準の改定時に新規技術要素が含まれている場合、該当技術要素の取込みの要否及び、影響を確認。

2.3 ISMAP 管理基準の読み方

2.3.1 3 桁管理策と 4 桁管理策の関係性

管理基準の構成に関しては「ISMAP 管理基準」の「2.1 章 管理基準の構成」 を参照されたい。また、言明に関しては、「ISMAP 管理基準」の「2.2 章 言明書に記載すべき内容」を参照されたい。

ガバナンス基準及びマネジメント基準は、原則として全て実施しなければならない。管理基準は、統制目標とされる 3 桁管理策(A.X.X.X)と、それを達成するための手段となる詳細管理策である 4 桁管理策(A.X.X.X.X)で構成される。原則として、3 桁管理策を必須とし、4 桁管理策を選択制とし、「一部の重要な管理策」を必須とする。

管理策の中でも考慮が必要となる管理策に関して以下の表に記載する。

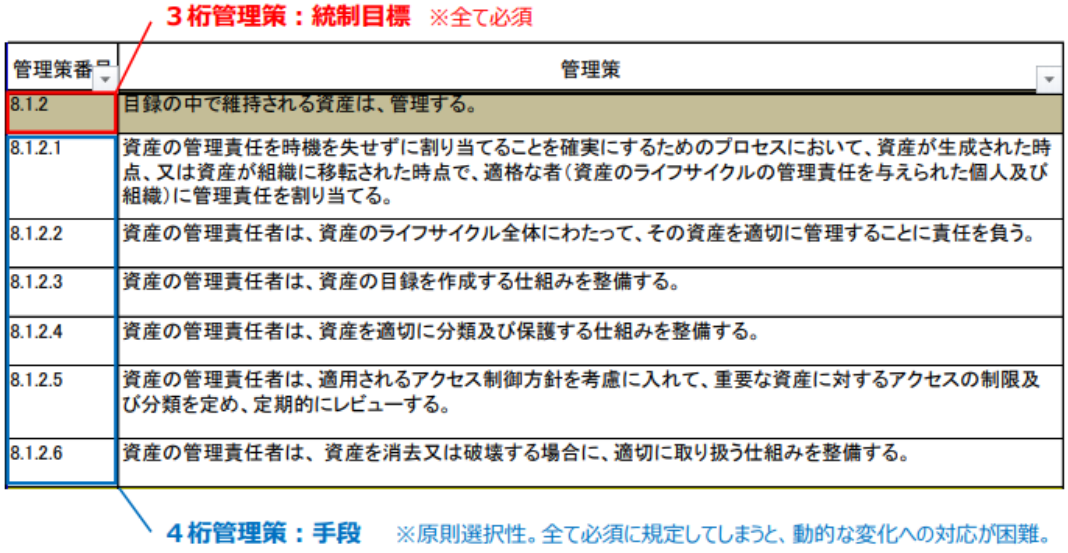
#	管理策種別	説明
1	管理策番号.P	クラウドサービスに特有のものとして、クラウドサービス事業者が特に考慮すべき管理策。
2	管理策番号.B	管理策を実装するための単なる選択肢ではなく、それ自体が基本言明要件(※)である管理策。原則必須。
3	管理策番号.PB	「管理策番号.P」と「管理策番号.B」の両方を示す管理策。原則必須。

※基本言明要件は、言明の対象となる管理策として、以下の内容を実施しなければならない。
- ガバナンス基準　：原則全て実施しなければならない。
- マネジメント基準　：原則全て実施しなければならない。
- 管理策基準　：すべての統制目標としての管理策について、原則実施しなければならない。

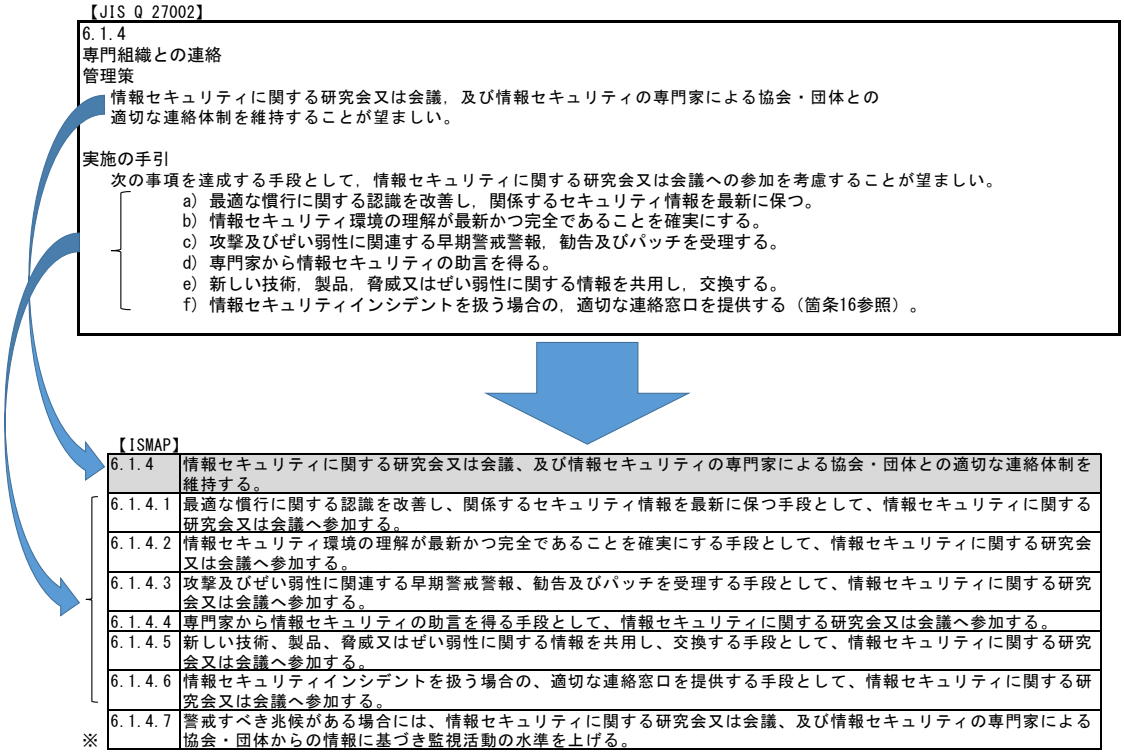
ただし、CSP は自身の提供するサービス内容に照らし、**合理的な適用が不可能な統制目標（3 桁管理策）については、その理由を示すことで対象外とすることができる。**この場合、対象外とした統制目標（3 桁管理策）としての管理策に含まれる詳細管理策（4 桁管理策）のうち「管理策番号.B」又は「管理策番号.PB」の管理策も対象外とすることができる。

詳細管理策（4 桁管理策）については、選択制だが、選択しない場合、選択しない理由を詳細管理策ごとに記載する必要がある。

※選択しない理由の参考例は、以下の URL にある「FAQ：クラウドサービス登録に関すること：Q13」を参照されたい。
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010094



詳細管理策（4 桁管理策）は、JIS Q 27002 において、各管理策の「実施の手引」に記載されている内容を分割して表記する形となっている。



なお、JIS Q 27002 の実施の手引のうち、選択肢となっている項目を基にした 4 桁管理策について、本マニュアルの別紙において、以下のような形で明示している。

管理策基準		変更種別	JIS Q 27002の実施手引きの選択肢を基に作成された管理策
5	情報セキュリティのための方針群		
5.1	情報セキュリティのための経営陣の方向性		
5.1.1	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注) 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者 (administrator) は除かれる。		
5.1.1.1	組織は、経営陣によって承認され、組織の情報セキュリティ目的の管理に対する取組みを示すものとして、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。		
5.1.1.2	情報セキュリティ方針は、事業戦略によって生じる要求事項を取り扱う。		○
5.1.1.3	情報セキュリティ方針は、規制、法令及び契約によって生じる要求事項を取り扱う。		○
5.1.1.4	情報セキュリティ方針は、現在の及び予想される情報セキュリティの脅威環境によって生じる要求事項を取り扱う。		○
5.1.1.5	情報セキュリティ方針には、情報セキュリティに関する全ての活動の指針となる、情報セキュリティの定義、目的及び原則に関する記載を含める。		○
5.1.1.6	情報セキュリティ方針には、情報セキュリティマネジメントに関する一般的な責任及び特定の責任の、定められた役割への割当てに関する記載を含める。		○
5.1.1.7	情報セキュリティ方針には、逸脱及び例外を取り扱うプロセスに関する記載を含める。		○
5.1.1.8	方針群のより低いレベルでは、情報セキュリティ方針は、トピックに応じて定める個別方針 によって支持されるようにする。		○
5.1.1.9	個別方針のトピックとして、アクセス制御を含める。		○
5.1.1.10	個別方針のトピックとして、情報分類（及び取扱い）を含める。		○
5.1.1.11	個別方針のトピックとして、物理的及び環境的セキュリティを含める。		○
5.1.1.12	個別方針のトピックとして、エンドユーザ関連のトピック（資産利用の許容範囲、クリアデスク・クリアスクリーン、情報転送、モバイル機器及びテレワーキング、ソフトウェアのインストール及び使用の制限）を含める。		○
5.1.1.13	個別方針のトピックとして、バックアップを含める。		○
5.1.1.14	個別方針のトピックとして、情報の転送を含める。		○

2.3.2 4 桁管理策を読むときの注意事項

① 4 桁管理策だけを読むのではなく、1 桁管理策の内容、2 桁管理策の内容とその目的及び 3 桁管理策の示す統制目標を確認の上、4 桁管理策の内容を理解する。なお、本マニュアルの第 5 章～第 18 章には、2 桁管理策ごとの目的が記載されている。

② 管理策の中で主語が記載されていない場合、「クラウドサービス事業者」が主語となる。

③ 管理策の中には、「利用者」、「全ての利用者」、「クラウドサービス利用者」及び「クラウドサービスのユーザ」の 4 種類の利用者が登場する。該当する管理策の「利用者」がどのような位置づけに当たるかについては、後述する「「利用

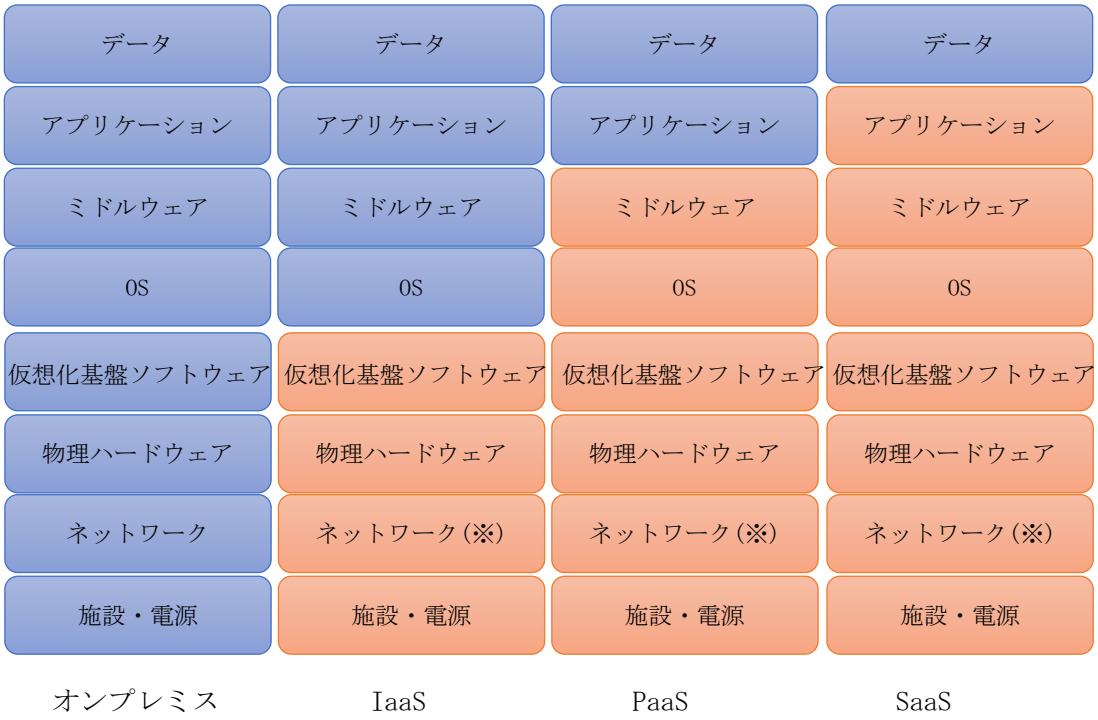
者」の定義」を参照。

④ ISMAP 管理基準の基となった JIS Q 27002 も内容の理解の参考となる。
ISMAP 管理基準の 3 桁管理策番号と JIS Q 27002 の 3 桁管理策番号は一部を除いて同様の番号が割り当てられているため、3 桁管理策番号を基に JIS Q 27002 の管理策内容を確認できる。

2.4　クラウドサービス提供形態における登録プロセス及び責任範囲

2.4.1 責任共有モデル

オンプレミス及びクラウドサービスモデル(IaaS/PaaS/SaaS)における責任共有モデルは以下のようになる。



【凡例】

※「ネットワーク」部分はサービス受領側(顧客)管理部分ではなく、クラウドサービス内のネットワーク環境を示す。

また、調達省庁と CSP 間の責任分解については、以下のドキュメントを参照。

・クラウドサービスの安全性評価に関する検討会中間とりまとめ[1]

1．5．クラウドサービスの利用に係るセキュリティ確保の責任

2.4.2　ISMAP への登録プロセスと契約時の責任の考え方

代表的なクラウドサービス提供形態のパターンを以下に示す。

・パターン 1：IaaS/PaaS/SaaS 垂直統合モデル

アプリケーション～施設・電源までの全階層を 1 社のクラウドサービスにて提供するケース

・パターン 2：SaaS のみのモデル：

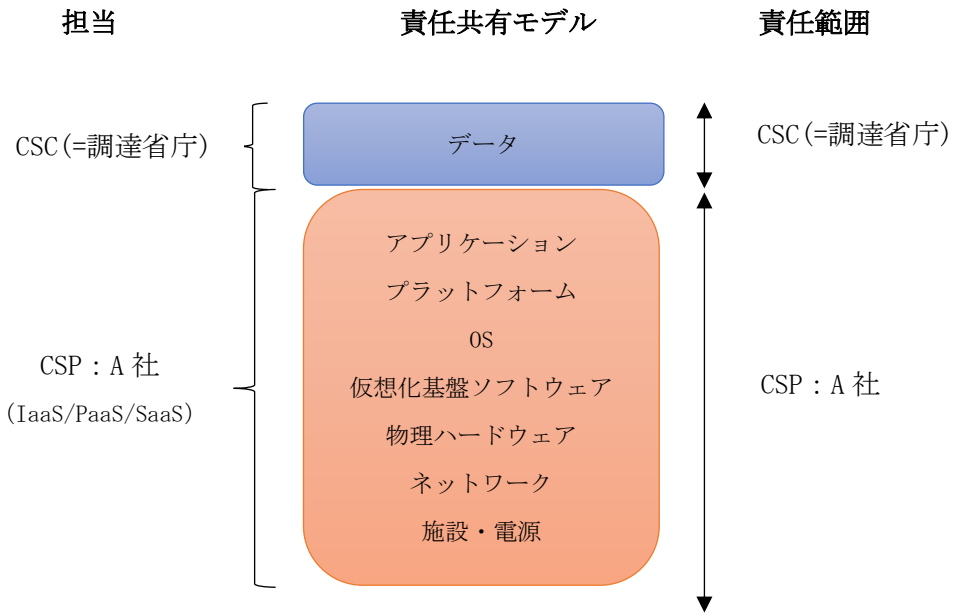
別会社が提供している IaaS/PaaS(プラットフォーム～施設・電源までの領域)サービスを使用し、アプリケーションのみを提供するケース

各パターンにおける登録プロセス及び責任の考え方を以下に示す。

[1] https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/20200130_report.pdf

2.4.2.1　　パターン 1：IaaS/PaaS/SaaS 垂直統合モデル

本モデルにおける責任共有モデルの各階層の担当と責任範囲を以下に示す。



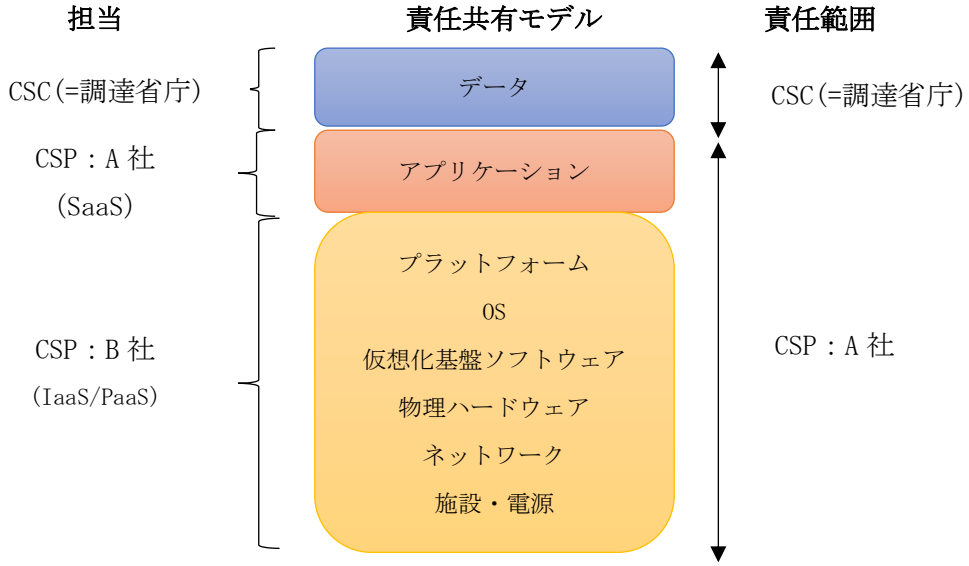
クラウドサービス事業者(CSP:A 社)が実施すべき登録プロセス及び責任の考え方を以下に示す。

・登録プロセス
　○言明：すべての管理策の中で、サービス全体として満たすべき管理策を選択・設計・実施する。
　○監査：すべての管理策に対して、通常の手続きに則って監査を実施。
　○登録審査：全ての管理策に対して、通常の登録基準に従って確認。

・責任の考え方
　提供するサービス全体の管理策の選択・実装は CSP:A 社が実施する。また、政府との契約も CSP:A 社が担当する。そのため、本クラウドサービスにおけるトラブル発生時の解決に関しても CSP:A 社が実施する。

2.4.2.2　　パターン 2: SaaS モデル

本モデルにおける責任共有モデルの各階層の担当と責任範囲を以下に示す。



クラウドサービス事業者(CSP:A 社)が実施すべき登録プロセス及び責任の考え方を以下に示す。

・登録プロセス

○言明

①すべての管理策の中で、サービス全体として満たすべき管理策を選択。

②(a)自身(=CSP:A 社)が満たすべき管理策と、(b)IaaS/PaaS 部分(=CSP:B 社)の管理策を引継ぐ部分を明示。

③(a)について、自身で個別管理策を設計し、実施。

④(b)について、IaaS/PaaS 部分(=CSP:B 社)が A 社の求める管理水準を満足できるように管理策を選択・適用していることを示す。

○監査

①(a)について、通常の手続きに則って監査を実施。

②(b)について、CSP:A が CSP:B の対策内容を第三者の監査証跡等で確認をしている事を確認。

○登録審査

①(a)について、通常の登録基準に従って確認。

②(b)について、IaaS/PaaS 部分が登録されているということを確認。

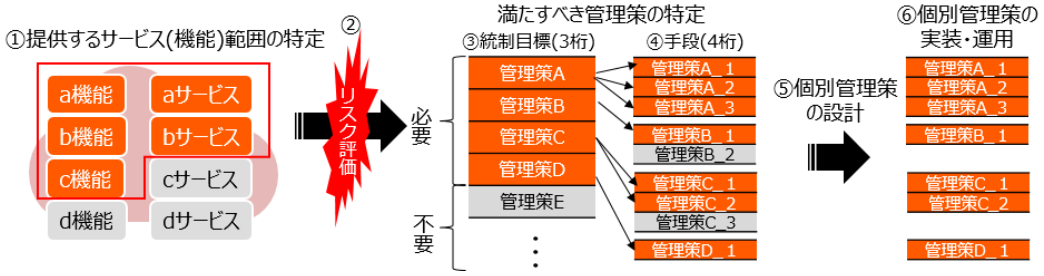
・責任の考え方

提供するサービス全体の管理策の選択・実装は CSP:A 社が実施する。また、政府との契約も CSP:A 社が担当する。そのため、SaaS 部分にてトラブルが発生した場合、CSP:A 社の責任で解決に当たる。IaaS/PaaS 部分にてトラブルが発生した場合、CSP:A 社が政府に対して解決責任を負い、CSP:A 社が CSP:B 社との契約に基づいて民間同士で解決を図る。

2.5　言明に向けた個別管理策の策定

言明に向けた個別管理策の策定は、情報セキュリティマネジメントに関する「確立・導入」、「運用」、「監視」、「維持及び改善」の活動のうち、「確立」フェーズにおいて実施する。

「確立」フェーズ内において実施する管理策の策定に向けた流れを以下の図に示す。



CSP は提供するクラウドサービス(機能)範囲の特定を行い、リスク評価を実施する。リスク評価の結果を基に満たすべき管理策の特定を行い、個別管理策の策定を行う。

「ISMAP では「機密性」「完全性」「可用性」の観点からセキュリティ水準を 3 段階にレベル分けを行っており、ISMAP 管理基準においては、以下の資料に示すところの機密性 2 の情報を取り扱うことを想定して策定している。

○参考資料

・クラウドサービスの安全性評価に関する検討会中間とりまとめ
「2. 3. 今後の望ましい情報システムのクラス分けの考え方」、及び
「3. 3. 1. 管理基準及び監査基準」

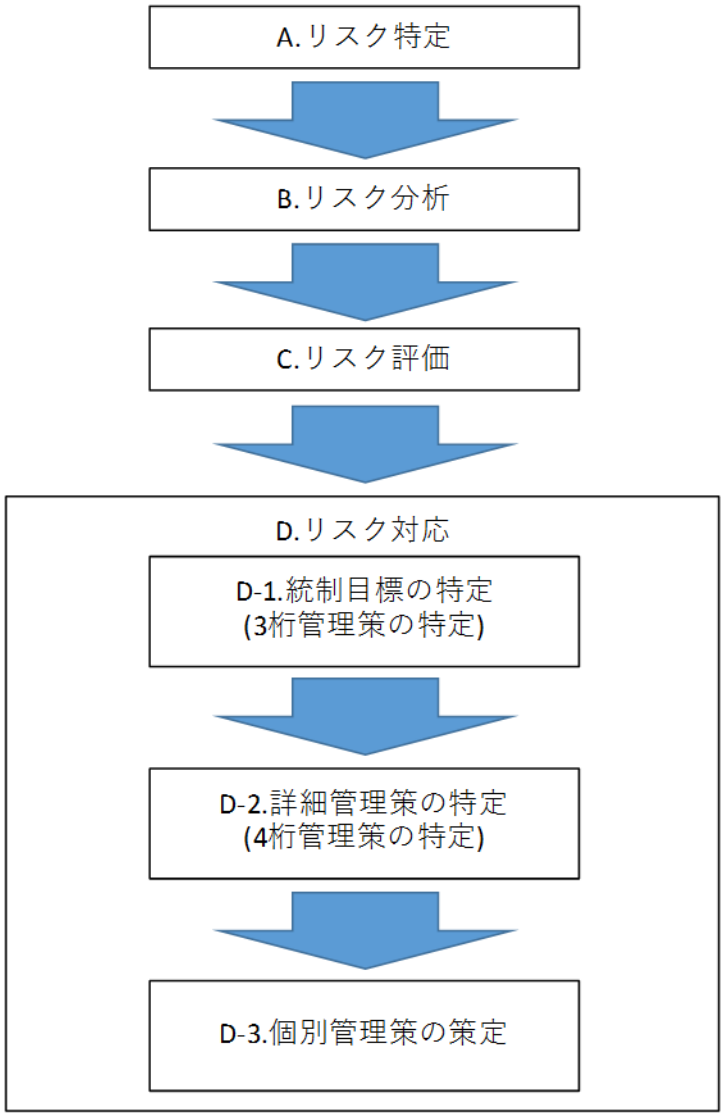
https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/20200130_report.pdf

・機密性の定義
政府機関等の対策基準策定のためのガイドライン（令和 3 年度版）
1.5 統一基準で定義されている用語
（1）情報の格付の区分

https://www.nisc.go.jp/pdf/policy/general/guider3.pdf

2.5.1 個別管理策の策定に向けた作業タスク

個別管理策の策定に向けて実施すべき作業フローを以下に記載する。



2.5.2 各作業タスクにおける考慮事項及び参考情報

2.5.1 の各作業タスクにおいて、考慮すべき観点を以下に記載する。

A. リスク特定、B. リスク分析、C. リスク評価

〇概要

リスク特定では、組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し，認識し，記述する。リスク分析では、必要に応じてリスクのレベルを含め，リスクの性質及び特徴を理解する。リスク評価では、影響度に基づき対応優先度を判定する。

〇参考情報

・情報セキュリティ管理基準の 4.4.1 章～4.4.8 章
https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

リスクアセスメント(リスク特定～リスク評価)及びリスク対応に関するプロセス全体が記載されている。なお、ISMAP 管理基準第４章（マネジメント基準）にも、同様の内容が記載されている。

・JIS Q 31000:2019 リスクマネジメント指針　6 章（プロセス）に、リスクマネジメントに関するプロセス(方針，手順及び方策を，コミュニケーション及び協議，状況の確定，並びにリスクのアセスメント，対応，モニタリング，レビュー，記録作成及び報告の活動)が記載されている。

・「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版)」
https://www.nisc.go.jp/active/general/pdf/guide30.pdf

特に、「2.1.2 対策基準・対策推進計画の策定」の章を参照。

・欧州 ENISA のクラウドのセキュリティに関するガイドライン
※本ガイドラインは独立行政法人 情報処理推進機構(IPA)が日本語に翻訳している。
https://www.ipa.go.jp/security/publications/enisa/documents/Cloud%20Computing%20Security%20Risk%20Assessment.pdf
https://www.ipa.go.jp/security/publications/enisa/documents/enisa%20jp-en%20doc.pdf

クラウドコンピューティングに関する一般的なリスクに関して、具体例や参考となる観点が記載されており、リスク特定時に参考となる。

・ISMS 認証に関するガイド類
https://www.jipdec.or.jp/library/publications/smpo_doc.html

D.リスク対応

D-1.統制目標の特定(3 桁管理策の特定)

3 桁管理策はクラウドサービス事業者が、リスクに対応するべき統制目標であり、全て満たすべき必須項目である。

クラウドサービスを提供する上で、その提供不可欠な基盤や機能の一部として、他社のサービスを活用する場合、他社サービスが ISMAP に登録されている場合と、ISMAP に登録されていない場合で対応が異なる。他クラウドサービスを活用する場合における登録に関するプロセス及び責任の考え方については、「2.4 クラウドサービス提供形態における登録プロセス及び責任範囲」を参照されたい。

D-2.詳細管理策の特定(4 桁管理策の特定)

ガバナンス基準及びマネジメント基準の 4 桁管理策は、原則として全て実施しなければならない。

管理策基準の 4 桁管理策は、基本的には選択制であり、リスク分析の結果に基づき、3 桁管理策を満たすように選択する。そのため、必ずしも全ての 4 桁管理策を実施する必要はない。ただし、一部の重要な管理策は必須である（2.3.1 を参照)。また、除外した 4 桁管理策に対しては、除外した理由を明記する必要がある。

管理策基準の 4 桁管理策は、ISMAP 管理基準の別表 3 から選択する。

D-3.個別管理策の策定

D-2 までに選定した 4 桁管理策を基に、各システム個別の管理策を策定する。

2.6　個別管理策の選定例

クラウドサービス事業者の視点から特定した、具体的なリスク及びその対策の選定例が、「**クラウドサービスにおけるリスクと管理策に関する有識者による検討結果 2011 年度版**」（特定非営利活動法人 日本セキュリティ監査協会）に示されている。
https://jcispa.jasa.jp/wp-content/uploads/docs/pdf2012/2012_cloud_doc04.pdf

この資料には、クラウドサービスにおいて目指すべき水準、脅威/ぜい弱性の観点から想定される具体的なリスク、クラウド事業者における対策の要点について記載されている。

ただし、この資料において、各リスクの「対応するクラウド管理基準」の欄には、古い版の「クラウド情報セキュリティ管理基準」の管理策が記載されており、ISMAP 管理基準が基礎とした「クラウド情報セキュリティ管理基準(平成 28 年)」とは管理策の番号などが異なっている。そのため、記載されている管理策については、ISMAP 管理策基準への読み替えが必要となる。

2.7　ISMAP 管理基準を理解するために重要な考え方

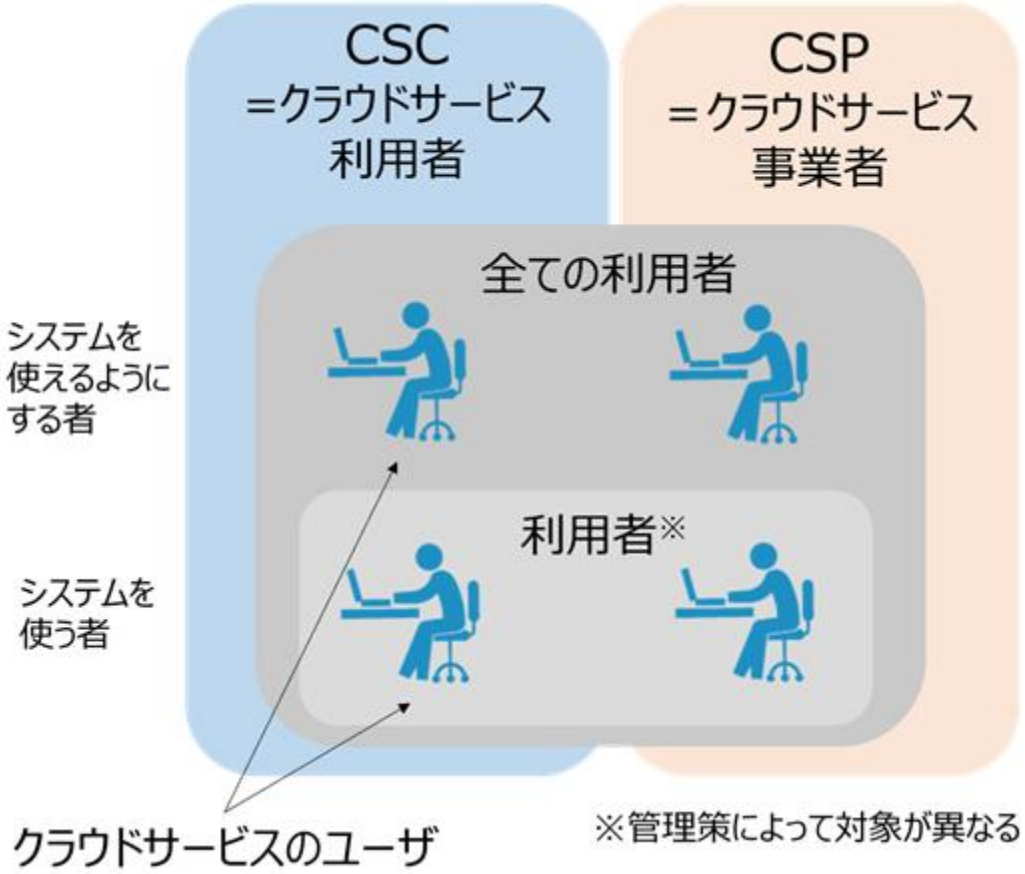
2.7.1 クラウドサービス内で扱われる情報の整理

クラウドサービス内で扱われる情報について、管理基準では以下のように整理している。

#	CSP内に存在するCSC情報	JIS X 9401:2106	情報例	情報の管理者（所有者）	保管場所
1	クラウドサービスカスタマデータ (Cloud Service Customer Data)	クラウドサービスカスタマの（法的又はその他の理由によって）管理下にあるデータオブジェクトの種類であって，クラウドサービスに入力したデータオブジェクト，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カスタマ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オブジェクト。	CSCが、保存する各種情報（要保護情報）	CSC	CSPのサービス提供設備
2	クラウドサービス派生データ (Cloud Service Derived Data)	クラウドサービスカスタマがクラウドサービスを利用した結果として派生した，クラウドサービスプロバイダの管理下にあるデータオブジェクトの種類。	サービス提供情報 CSCサービス利用情報 (Availability, サービス利用ログ、ビリング情報等)	CSP	CSPのサービス管理設備

2.7.2 「利用者」の定義

管理策の中には、「利用者」、「全ての利用者」、「クラウドサービス利用者(クラウドサービスカスタマ)」及び「クラウドサービスのユーザ」の４種類の利用者が登場する。また、クラウドサービスの利用者には、「人」以外に、「人」の代わりにシステムを利用するものも含まれる。そのため、利用者には、システムを使う「人」だけでなく、「プロセス」も含むこととする。大まかな概念としては、以下の包含関係となる。



- 利用者

CSC においてシステムを使う者と、CSP においてサービス提供に直接関わらないシステムを使う者の両方を包含する。ここで、「サービス提供に直接関わらないシステム」とは、例えば、運用環境（クラウド基盤システム、顧客管理システム、NMS、課金システムなど)、開発環境・試験環境（プロジェクト管理システム、バージョン管理システム、テスト設計システム、テスト実行システムなど）を指す。

管理策によって、「利用者」が指す対象が異なるため、注意が必要である。

- 全ての利用者

CSC 及び CSP において、システムを使う者（＝利用者）のほか、システムを使えるようにする者(管理者、実務管理者(特権を与えられた利用者)、運用担当者)を含む。

- 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」を意味する。

➢　クラウドサービスのユーザ
CSC において、システムを使う者（＝利用者）のほか、システムを使えるようにする者（管理者、実務管理者（特権を与えられた利用者）、運用担当者）を含む。

2.7.3　暗号化・暗号鍵の管理に対する考え方
CSP の内部及び外部からの不正アクセスの双方に対する対応を示す。
①　内部からの不正アクセスへの対応
CSC が対策を必要と判断した情報に関して、以下の対策の実施が必要である。
・暗号化（機能の提供もしくは暗号化を行うための情報提供）
CSP に対する監査が可能である限り、暗号化の実施主体は CSP/CSC の何れでもよい。
・CSC の意図しない形で暗号鍵が利用されないような管理
CSP に対する監査が可能である限り、CSP が実施してもよい。
・CSC による暗号鍵の削除
CSP に対する監査が難しいため、CSC が実施する。

これを踏まえ、管理策基準に以下の管理策を必須の項目として追加している。

8.1.2.7.PB
クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。
(a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能
(b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するための情報

併せて、暗号化・暗号鍵の管理に関する管理策に対して、以下の下線部分の文言を追記している。

10.1.1.9.PB クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境について、情報を提供する。

10.1.2.20.PB クラウドサービス事業者は、クラウドサービス利用者に、暗号化した情報の暗号鍵をクラウドサービス利用者が管理する機能を提供し、または、クラウドサービス利用者が暗号鍵を管理する方法について、情報を提供する。

②　外部からの不正アクセスへの対応
管理策基準は、CSP 側においても漏えいに対するリスク管理の観点から、暗号化とその暗号鍵の管理を求めている。この対応については、以下の管理策で規定している。

10.1.1 情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。

10.1.2 暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。

注：暗号鍵の管理の定義
　ここで言う暗号鍵の管理とは、「CSC の意図しない形で暗号鍵が利用されない」ことを CSC が確認できることを指す。従って、必ずしも鍵の保管を CSC が行うことを求めるものではなく、監査によって鍵が意図せず生成・読出し・配布・削除等が行われていないことを確認できればよい。

2.7.4 データ消去に対する考え方
　消去(抹消)の用語定義の中で、暗号化消去、すなわち「もと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とする方法」も消去の方法の一つとして認めている。
　その上で、暗号化と同様に CSP の内部及び外部からの不正アクセスの２つの視点で示す。

① 内部からの不正アクセスへの対応
　記録媒体は CSC の管理下にないが、CSC が暗号化消去を行う必要がある。そのため、CSP には、その機能又はその機能を実装するための情報の提供を求める。

8.1.2.7.PB
クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。
(a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能
(b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するための情報

② 外部からの不正アクセスへの対応
　上記①の対応によって、CSP 側に残った情報は CSC により暗号化され、データが復号できない状態にあるため、消去の目的が達せられていると考えることもできるが、多層防御の観点からも CSP による削除を求める。CSP 側における削除方法については、管理策基準 11.2.7 などで規定されているように、物理的消去・電磁的消去・暗号化消去のいずれでも CSP の選択した方法でよいものとする。

11.2.7
記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。

2.7.5 バックアップに対する考え方

通常の資産管理と同様の管理、すなわち、暗号化されて記録されている情報について、CSP の内部及び外部からの不正アクセスへの対応を考慮する。

① 内部からの不正アクセスへの対応

管理策基準 8.1.2.7.PB、12.3.1.18.P で規定されているように、CSC が管理している暗号鍵を用いて、記録媒体に記録する（バックアップを含む）前に暗号化を行う。

8.1.2.7.PB
クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。
(a) 当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能
(b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するための情報

② 外部からの不正アクセスへの対応

管理策基準 12.3.1.11 に規定されているように、暗号化されて記録されていればよい。

12.3.1.11
機密性が重要な場合には、暗号化によってバックアップ情報を保護する。

2.7.6 ガバナンス基準に関する考え方

① ISMAP ガバナンス基準における JIS Q 27014:2015 からの修正点

・主語を「経営陣」に統一した。
・「業務執行幹部」を「管理者」に読み替えた。
・ガバナンス基準で関連の深い内容を 1 つの基準として、具体化及び再整理した。

例：3.1.4 モニタ

JIS Q 27014		ISMAP:ガバナンス基準	
5.3.4	モニタ	3.1.4	モニタ
	“モニタ”は，経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。		モニタは、経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。
	“モニタ”プロセスを実施するために，経営陣は次のことを行うことが望ましい。		“モニタ”プロセスを実施するために、経営陣は次のことを行う。
	– 情報セキュリティマネジメント活動の有効性を評価する。	3.1.4.1	**経営陣は、**情報セキュリティマネジメント活動の有効性を評価する。 (ア)**経営陣は、管理者に、**事業の観点から適切なパフォーマンス指標を選択**させる。** (イ)**経営陣は、管理者に、**経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む、情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣へ提供**させる。**
	– 内部及び外部の要求事項への適合性を確実にする。	3.1.4.2	**経営陣は、**内部及び外部の要求事項への適合性を確実にする。
	– 変化する事業，法制度，規制の環境，及びそれらの情報リスクへの潜在的影響を考慮する。	3.1.4.3	**経営陣は、**変化する事業、法制度、規制の環境、及びそれらの情報リスクへの潜在的影響を考慮する。
	“モニタ”プロセスを可能にするために，業務執行幹部は次のことを行うことが望ましい。		
	– 事業の観点から適切なパフォーマンス指標を選択する		
	– 経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む，情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣に提供する。		
	– 情報リスク及び情報セキュリティに影響する新規開発案件について，経営陣に注意を喚起する。	3.1.4.4	**経営陣は、管理者に、**情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起**させる。**

② ガバナンス基準の実施主体は「経営陣」である。マネジメント基準の実施主体は業務の「管理者」であり、実施主体が異なることに注意する。

様々な部門・事業地域を擁する事業者（含：グローバル事業者）の場合、ガバナンス基準を実施すべき「経営陣」とは、事業者全体の「経営陣」を指す。ただし、クラウドサービス関連の事業部等に対して、その実施を委任することを妨げるものではなく、委任している場合は当該決定が経営方針の中で行われていることと、委任を受けた主体がその内容を実施していることが求められる。なお、責任主体が経営陣であることに変わりは無い。

2.7.7 ゼロトラストの考え方と整合していないと解釈される可能性がある管理策について

「政府機関等の情報セキュリティ対策のための統一基準」について、2021年7月に改定されており、本改訂において、新規技術要素として、**「常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ）」**が追加されている。

※「常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ）」の詳細に関しては、9.4章 詳細管理策の解説を参照。

政府統一基準の改定では、従来の境界防御型によるアクセス制御を否定するものではなく、ゼロトラストによる制御の要件も考慮する旨で記載されているが、ISMAP管理策基準の一部は、以下のような観点から、ゼロトラストの考え方と整合していないと解釈されてしまう可能性があるため、ゼロトラストアーキテクチャを適用する際にはこれらに該当する管理策に留意の上、言明を行う。

① ゼロトラストの考え方に整合していないと判断されてしまう表現が含まれているケース
② 管理策中の表現から境界型と判断されてしまうケース

参考文献

[1] JIS Q 27001:2014
情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項
Information technology -- Security techniques -- Information security management systems - Requirements,2014,32p

[2] JIS Q 27002:2014
情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範
Information technology -- Security techniques -- Code of practice for information security controls ,2014,96p

[3] JIS Q 27014:2015
情報技術―セキュリティ技術―情報セキュリティガバナンス
Information technology -- Security techniques -- Governance of information security,2015,16p

[4] JIS Q 27017:2016
情報技術―セキュリティ技術―ＪＩＳ　Ｑ　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
Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services,2016,54p

[5] NIST Special Publication 800-53 Revision 4
連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策ジョイントタスクフォースによる変革への取り組み,
NIST National Institute of Standards and Technology U.S. Department of Commerce

※参考資料は「独立行政法人 情報処理推進機構」が2014年に原典を元に翻訳した資料となります。519p

[6] 打川　和男. 図解入門ビジネス　最新ISO27017とISO27018がよ～くわかる本,東京,株式会社 秀和システム,2017,222p