ISMAP 管理基準

令和２年６月３日
（令和４年１１月１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 4 桁管理策基準を改定 「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

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若しくは 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 27001:2014、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)を基礎としつつ、「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)、及び「SP800-53 rev.4」（以下、「SP800-53」という）を参照して作成されている。

また、ガバナンス基準については、クラウド情報セキュリティ管理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。

本管理基準の主な特徴は次の通りである。

(1)　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。
(2)　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。
(3)　暗号化消去もデータの消去(もしくは抹消)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、及び以下の規格の用語の定義に準じる。

- JIS Q 27001:2014（ISO/IEC 27001:2013）
- JIS Q 27002:2014（ISO/IEC 27002:2013）
- JIS Q 27014:2015（ISO/IEC 27014:2013）
- 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内、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内、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内、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内、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(もしくは抹消)

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も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。管理基準のうち（X.X.X）という３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選択して満たすべき事項。管理基準のうち（X.X.X.X）という 4 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、自身の選択した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 ISMAP 管理基準に準拠して統制目標及び詳細管理策を選択し、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 ISMAP 管理基準に準拠して統制目標及び詳細管理策を選択し、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　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）

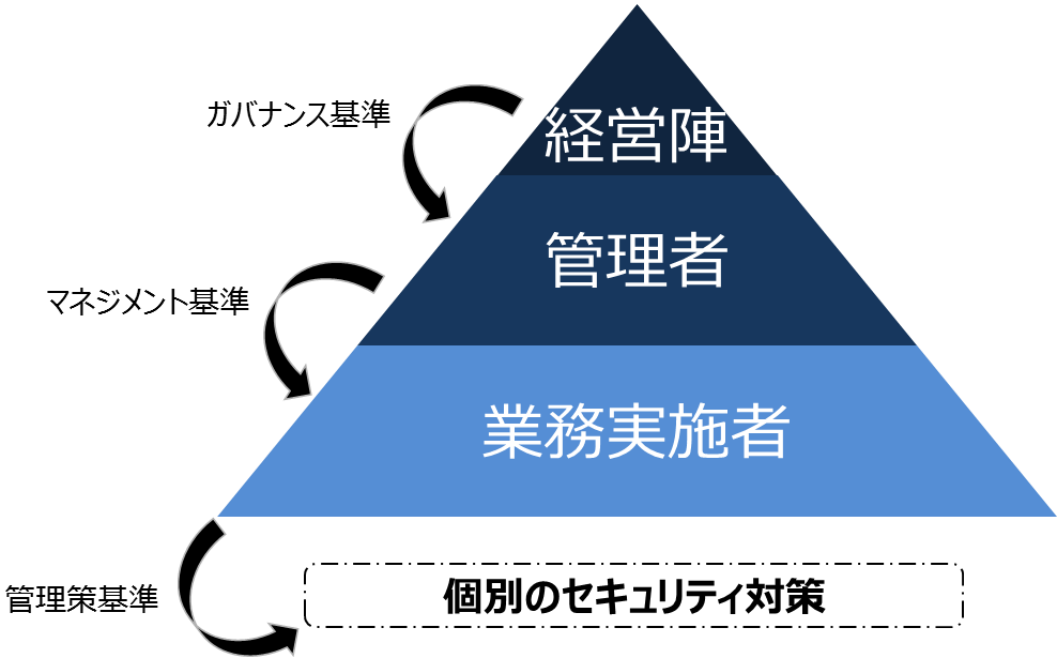

図１：管理基準の構成

「ガバナンス基準」は、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「プロセス」の 4 桁部分(X.X.X.X)を再構成し、ガバナンス基準とした。

「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計画、実行、点検、処置、及び、リスクコミュニケーションに必要な実施事項を定めている。

「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選択する際の選択肢を与えるものである。「管理策基準」のそれぞれの事項は、管理目的と詳細管理策で構成される。

なお、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については、「管理策番号.P」と表記している。また、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については「管理策番号.B」と表記している。そして、「管理策番号.PB」はその両方の意味を示している。

2.2　言明書に記載すべき内容

クラウドサービス事業者は、言明に際しては「ISMAP クラウドサービス登録規則」若しくは「ISMAP-LIU クラウドサービス登録規則」で定める様式に従って、以下の内容について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、以下項目のうち、「クラウドサービスの名称」、「言明の対象範囲」、「基本言明要件」のうち実施している統制目標としての管理策、「監査対象期間」、「後発事象」については、ISMAP 等クラウドサービスリストにおいて一般に公開することとする。

2.2.1クラウドサービスの名称

対象としたクラウドサービスの名称を記載する。

2.2.2言明の対象範囲

一つのクラウドサービスの名称であっても、その傘下に複数のサービスがある場合等、どのサービスを対象にしているのか具体的に記載する。

また、この言明の対象外となるサービスを利用してここに記載するサービスを提供している場合、その範囲及び利用しているサービスを明示し、言明書の対象外になる旨記載をする。ただし、サービスの基盤に言明の対象外となるクラウドサービスを利用している場合には、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ことが求められる。

また、対象となるリージョンを記載する。

2.2.3システムと内部統制の全体像

クラウドサービス事業者自身の概要、クラウドサービスの概要、クラウドサービスを提供するためのシステムの論理構成(物理層からアプリケーション層まで)及び言明書の対象となるサービス範囲、詳細な内部統制の状況等を記載する。

2.2.4基本言明要件

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。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。

(1)　　ガバナンス基準

原則としてすべて実施しなければならない。

(2)　　マネジメント基準

原則としてすべて実施しなければならない。

(3)　　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、末尾にBが付された詳細管理策(X.X.X.X.B及びX.X.X.X.PB)も原則として実施すべきものとする。

その他の詳細管理策は、言明の対象となるサービスにおける組織・環境・技術等に応じて必要とする事項を選択しなければならない。

必須の詳細管理策と選択された詳細管理策のそれぞれに対して、個別管理策を記載しなければならない。なお、監査対象期間において個別管理策の内容が変更されている場合は、変更前後の個別管理策の内容とその適用期間を記載すること。

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な統制目標としての管理策については、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としての管理策に含まれる詳細管理策のうち末尾にBが付された詳細管理策も対象外にすることができる。また、詳細管理策については、前述のとおり選択制であるが、選択しない詳細管理策についてはその理由を記載する必要がある。ただし、選択しない理由については監査の対象外である。

選択制の詳細管理策の項目については、別表３を参照すること。また、詳細管理策の選択及びその運用に当たっては、別紙１の内容に留意すること。

2.2.5監査の対象となる期間

言明内容のうち、監査対象となる期間を記載する。

監査の対象期間は最大１年とし、次の登録申請を行う際の監査対象期間は、前回の監査対象期間の末日の翌日とすることで、期間の隙間なく監査が行われなければならない。監査の対象期間を１年より短くする場合においては、３ヶ月の最低運用期間を経る必要がある。

2.2.6後発事象

監査の対象期間もしくは監査基準日以降、実施結果報告書の日付までに発生した後発事象を記載する。

2.2.7特記事項

本制度の監査を実施する上で特記すべき事項がある場合には、その旨及び内容を記載する。

2.3　経営者確認書に記載すべき内容

クラウドサービス事業者は、「ISMAP クラウドサービス登録規則」若しくは「ISMAP-LIU クラウドサービス登録規則」で定める様式に従って、以下の事項を確認するため又は他の監査証拠を裏付けるため、経営者による陳述を書面にて監査人に対して行わなければならない。

(1)　　言明の対象となるクラウドサービスに関して、サービスの内容及びセキュリティリスク分析の結果を踏まえて、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選択し、必要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることの言明を行う責任を有している旨

(2)　言明の記載内容が正確であることを自ら評価するための体制を整備し、評価を実施している旨

(3)　管理基準の要求事項の解釈についての責任を負う旨

(4)　本制度における監査業務が情報セキュリティ監査基準等に準拠したものであることを、クラウドサービス事業者が承知している旨

(5)　実施結果報告書の配布及び利用制限が存在する旨

(6)　業務実施者が要請した全ての情報、面接及び質問の機会を提供した旨

(7)　監査の対象期間の末日以降、経営者確認書の日付までの間において、言明対象となるクラウドサービスの統制及び情報セキュリティの状況に重大な変更を及ぼしうる事象の発生の有無（ある場合には、その内容）

(8)　業務の実施に影響を与える可能性のある不正及び違法行為等に関する情報の有無（ある場合には、その内容）

第3章　ガバナンス基準

3　情報セキュリティガバナンス

情報セキュリティガバナンスは、組織の情報セキュリティ活動を指導し、管理するシステムである。情報セキュリティの目的及び戦略を、事業の目的及び戦略に合わせて調整する必要があり、法制度、規制及び契約を遵守する必要がある。また、情報セキュリティガバナンスは、内部統制の仕組みによって遂行されるリスクマネジメント手法を通じて、評価、分析及び実施する。

3.1　情報セキュリティガバナンスのプロセス

3.1.1 概要

経営陣は、情報セキュリティを統治するために、評価、指示、モニタ及びコミュニケーションの各プロセスを実行する。さらに、保証プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。

3.1.2　評価

評価とは、現在のプロセス及び予定している変更に基づくセキュリティ目的の現在及び予想される達成度を考慮し、将来の戦略的目的の達成を最適化するために必要な調整を決定するガバナンスプロセスである。

“評価”プロセスを実施するために、経営陣は、次のことを行う。

3.1.2.1　経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。

経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。

3.1.2.2　経営陣は、情報セキュリティのパフォーマンス結果に対応し、必要な処置の優先順位を決めて開始する。

3.1.2.3　経営陣は、管理者に、重大な影響のある新規情報セキュリティプロジェクトを経営陣に付託するようにさせる。

3.1.3　指示

指示は、経営陣が、実施する必要がある情報セキュリティの目的及び戦略についての指示を与えるガバナンスプロセスである。指示には、資源供給レベルの変更、資源の配分、活動の優先順位付け並びに、方針、適切なリスク受容及びリスクマネジメント計画の承認が含まれる。

“指示”プロセスを実施するために、経営陣は次のことを行う。

3.1.3.1　経営陣は、その組織のリスク選好を決定する。

3.1.3.2　経営陣は、情報セキュリティの戦略及び方針を承認する。

(ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。

(イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。

3.1.3.3　経営陣は、適切な投資及び資源を配分する。

3.1.3.4　経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。

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”プロセスを実施するために、経営陣は次のことを行う。

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。

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。

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。

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。

3.1.5　コミュニケーション

コミュニケーションは、経営陣及び利害関係者が、双方の特定のニーズに沿った情報セキュリティに関する情報を交換する双方向のガバナンスプロセスである。

コミュニケーションの方法の一つは、情報セキュリティの活動及び課題を利害関係者に説明する情報セキュリティ報告書である。

“コミュニケーション”プロセスを実施するために、経営陣は次のことを行う。

3.1.5.1　経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。

3.1.5.2　経営陣は、管理者に、情報セキュリティ課題を特定した外部レビューの結果を通知し、是正処置を要請する。

3.1.5.3　経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。

3.1.5.4　経営陣は、管理者に、注意が必要な問題、また、できれば決定が必要な問題について、経営陣へ助言させる。

3.1.5.5　経営陣は、管理者に、関連する利害関係者に対し、経営陣の方向性及び決定を支援するためにとるべき詳細な行動を、経営陣の方向性及び決定に沿って説明させる。

3.1.6　保証

保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。

“保証”プロセスを実施するために、経営陣は次のことを行う。

3.1.6.1　経営陣は、要求している情報セキュリティ水準に対し、どのように説明責任を果たしているかについて、独立した客観的な意見を監査人等に求める。

3.1.6.2　経営陣は、管理者に、経営陣が委託する監査、レビュー又は認証をサポートさせる。

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、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を確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。

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、クラウドサービス事業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―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 章に規定する。

4.3 凡例

4.3 4.4 章以降は、以下の構成をとる。

4.4　情報セキュリティマネジメントの確立

4.4.1　組織の役割、責任及び権限

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。

：

4.4 情報セキュリティマネジメントの確立

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、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。

4.4.1　組織の役割、責任及び権限

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)]

・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。

・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。

・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。

また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。

・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。

・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。

・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。

・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。

・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。
・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。

4.4.1.2 トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。［27001-5.3］
・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。
・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。

また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。
・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限
・リスクアセスメントにおいて、リスクを運用管理する責任･権限を持つリスク所有者
・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限
・セキュリティ要求事項を満たしているか監査する責任・権限
・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限
・各プロセスの結果及び効果を組織内に周知する責任・権限

4.4.1.3 トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。［27001-5.1h)］

管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。

4.4.2　組織及びその状況の理解

4.4.2.1 組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。［27001-4.1］
・外部の課題
・内部の課題

これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。

a)　外部状況
・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
・組織の目的に影響を与える主要な原動力及び傾向
・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観

b)　内部状況
・統治、組織体制、役割及びアカウンタビリティ
・方針、目的及びこれらを達成するために策定された戦略
・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術）
・情報システム､情報の流れ及び意思決定プロセス(公式及び非公式の双方を含む｡)
・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
・組織文化
・組織が採択した規格、指針及びモデル

・契約関係の形態及び範囲

4.4.3 利害関係者のニーズ及び期待の理解

4.4.3.1 組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。[27001-4.2]

・情報セキュリティマネジメントに関連する利害関係者
・利害関係者の、情報セキュリティに関連する要求事項

利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。

・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。

-情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等)
-セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等)
-情報セキュリティ監査を行う人又は組織(監査室等)
-組織内の情報セキュリティ専門家

・取引先、パートナー、サプライチェーン上の関係者
・親会社、グループ会社
・当該組織のセキュリティを監督する省庁、政府機関
・所属するセキュリティ団体、協会

4.4.4 適用範囲の決定

情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。

4.4.4.1 組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。[27001-4.3]

a)組織は以下の点を考慮して適用範囲及び境界を定義する。

・自らの事業
・体制
・所在地
・資産
・技術の特徴
・外部及び内部の課題
・利害関係者の情報セキュリティに関連する要求事項
・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

b)情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。

c)情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。

・外部状況には、以下のようなものが含まれる。

－国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
－組織の目的に影響を与える主要な原動力及び傾向
－外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観

・内部状況には、以下のようなものが含まれる。

－統治、組織体制、役割及びアカウンタビリティ

－方針、目的及びこれらを達成するために策定された戦略
－資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術）
－情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。）
－内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
－組織文化
－組織が採択した規格、指針及びモデル
－契約関係の形態及び範囲

4.4.5 方針の確立

4.4.5.1 トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。[27001-5.2]
・組織の目的に対して適切であること。
・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組
・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。
・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。
また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。

4.4.5.2 組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。[27001-6.2]
a)情報セキュリティ目的は、以下を満たすこととする。
・情報セキュリティ方針と整合していること。
・（実行可能な場合）測定可能であること。
・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。
b)情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。
・実施事項
・必要な資源
・責任者
・達成期限
・結果の評価方法

4.4.5.3 トップマネジメントは、以下によって、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。[27001-5.1a)]
・情報セキュリティ方針及び情報セキュリティ目的を確立すること。
・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。
また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。
・文書化された情報セキュリティ方針への署名
・情報セキュリティ方針が議論された会議の議事録
これらはトップマネジメントの責任を明確にするために実施する。

4.4.6 リスク及び機会に対処する活動

4.4.6.1 リスク及び機会を決定する。[27001-6.1.1]

a)組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。

・情報セキュリティマネジメントが、組織が意図した成果を達成する。
・望ましくない影響を防止又は低減する。
・継続的改善を達成する。

当該決定の際、組織は、以下を計画する。

・決定したリスク及び機会に対処する活動
・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法
・リスク及び機会に対処する活動の有効性の評価方法

b)リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。

4.4.7 情報セキュリティリスクアセスメント

4.4.7.1 組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a)/6.1.2b)]

a)以下を含む情報セキュリティのリスク基準を確立し、維持する。

・リスク受容基準
・情報セキュリティリスクアセスメントを実施するための基準

b)リスク受容基準に、以下を反映するよう、考慮する。

・組織の価値観
・目的
・資源

c)リスク受容基準を策定する際には、以下の点を考慮する。

・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法
・発生頻度
・発生頻度、結果を考える時間枠
・リスクレベルの決定方法
・利害関係者の見解
・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。

d)情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。

・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。
・情報セキュリティリスクアセスメントの結果が比較可能であること。

なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。

4.4.7.2 組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)]

a)情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全

性及び可用性の喪失に伴うリスクを特定する。
b)リスクを特定する過程において、リスク所有者を特定する。
c)リスクを特定する際には、以下について考慮する。
・リスク源が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。
・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。
・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ
・全ての重大な原因及び結果
・以下を特定すること。
－リスク源
－影響を受ける領域、事象
－原因及び起こり得る結果
この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。
4.4.7.3 組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2d)]
a)以下の手順によりリスク分析を行う。
・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。
・特定されたリスクの発生頻度の分析を行う。
・リスクレベルを決定する。
・特定した脅威やぜい弱性を基に、以下の点を考慮する。
－セキュリティインシデントが発生した場合の事業影響度
－セキュリティインシデントの発生頻度
－管理策が適用されている場合はその効果
b)リスク分析の際には、以下の点についても考慮する。
・リスクの原因及びリスク源
・リスクの好ましい結果及び好ましくない結果
・リスクの発生頻度
・リスクの結果及び発生頻度に影響を与える要素
なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。
4.4.7.4 組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)]
・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。
・リスク対応のための優先順位付けを行う。
・リスク評価の結果は今後の改善に利用するため保管する。
なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。

4.4.8 情報セキュリティリスク対応
4.4.8.1 組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)]
情報セキュリティリスク対応の選択肢には、以下が含まれる。

・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避
・ある機会を目的としたリスクの引受け又はリスクの負担
・リスク源の除去
・発生頻度の変更
・結果の変更
・(契約及びリスクファイナンスを含む) 他者とのリスクの共有
・情報に基づいた意思決定によるリスクの保有
さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。
4.4.8.2 組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)]
リスク対応のための方針を決めた上で、管理策の目的 (管理目的) 及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。
・リスクの受容可能レベル
・関連する法令
・規制や契約上の要求事項
・その他の社会的責任
なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。
4.4.8.3 組織は、管理策が見落とされていないことを検証する。[27001-6.1.3c)]
必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。
4.4.8.4 組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)]
a)情報セキュリティリスク対応計画には、以下を含む。
・期待される効果を含む、対応選択肢選定の理由
・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者
・対応内容
・必要な資源
・費用・労力、制約
・後日の報告、監視に必要な要求事項
・対応工程における節目ごとの目標
・対応時期及び日程
b)責任及び権限について
情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。
一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。
リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。
4.4.8.5 組織は、リスク所有者から、情報セキュリティリスク対応計画について承認

を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)]

すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。

・技術的に対応可能になる時期
・コスト的に対応可能になる時期

残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営時やその他の利害関係者に認識させることを考慮する。

また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。

4.5 情報セキュリティマネジメントの運用

4.5.1 資源管理

4.5.1.1 組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1]

管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。

4.5.1.2 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必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。[27001-5.1c)]

・情報セキュリティマネジメントの各プロセスに必要な人又は組織
・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム
・上記に必要な費用

4.5.2 力量、認識

4.5.2.1 トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。[27001-5.1d)]

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ついて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。

また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。

4.5.2.2 組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。[27001-7.2a)]

情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。

・役職名
・業務内容
・担当者の責任範囲
・業務に必要な知識
・業務に必要な資格
・業務に必要な経験

知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。

4.5.2.3 組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。[27001-7.2b)]

適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。

4.5.2.4 組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)]

必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。

教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。

・知識の確認テスト
・スキルの実習テスト
・チェックリストなどによるベンチマーク

実施結果については記録し、要員選択の客観性を確保する。

4.5.2.5 組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)]

教育、訓練については以下を検討し、定期的に実施する。

・教育・訓練基本計画
・教育・訓練実施計画
・確認テスト又は評価報告

教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。

4.5.2.6 組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)]

情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。

4.5.2.7 組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)]

以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。

・情報セキュリティマネジメントにおけるそれぞれの役割
・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。）
・これらが記載された文書の所在

4.5.2.8 組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]

4.5.3 コミュニケーション

4.5.3.1 組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4]

a)内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。

・コミュニケーションの内容（何を伝達するか）
・コミュニケーションの実施時期
・コミュニケーションの対象者
・コミュニケーションの実施者
・コミュニケーションの実施プロセス

b)内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。

・トップマネジメント
・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者
・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者
・組織内の従業員

c)外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。

・取引先、パートナー、サプライチェーン上の関係者
・親会社、グループ会社
・当該組織のセキュリティを監督する省庁、政府機関
・所属するセキュリティ団体、協会

4.5.4 情報セキュリティマネジメントの運用の計画及び管理

4.5.4.1 組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]

4.5.4.2 組織は、情報セキュリティ目的を達成するための計画を実施する。[27001-8.1]

4.5.4.3 組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。[27001-8.1]

文書化した情報に、以下の情報が集められているかどうかを確認する。

・管理策の実施状況
・管理策の有効性
・管理策を取り巻く環境の変化

また、これらの情報を把握し判断する体制を構築する。

4.5.4.4 組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。[27001-8.1]

4.5.4.5 組織は、外部委託するプロセスを決定し、かつ、管理する。[27001-8.1]

4.5.5 情報セキュリティリスクアセスメントの実施

4.5.5.1 組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2]

・あらかじめ定めた間隔
・重大な変更が提案された場合

・重大な変化が生じた場合

4.5.5.2 組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3]

情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。

4.5.5.3 トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。

情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。

・管理策の導入及び運用にかかる費用、人員、作業工数、技術
・セキュリティインシデント発生時の一時対応にかかる費用
・その他のリスク対応にかかる費用

運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。

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

4.6.1 有効性の継続的改善

4.6.1.1 組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2/8.2/9.2/9.3]

・定期的な情報セキュリティリスクアセスメント
・定期的な情報セキュリティ内部監査
・トップマネジメントによる定期的なマネジメントレビュー

継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。

4.6.1.2 トップマネジメントは、継続的改善を促進する。[27001-5.1g)]

4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。

4.6.2 パフォーマンス評価

4.6.2.1 組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。[27001-9.1]

・必要とされる監視及び測定の対象(情報セキュリティプロセス及び管理策を含む。)
・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。）
・監視及び測定の実施時期及び頻度
・監視及び測定の実施者
・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度
・監視及び測定の結果の、分析及び評価の実施者
・分析及び評価の結果に応じた対応措置
・分析及び評価の結果の報告頻度

4.6.2.2 組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a)/9.2b)]

a)内部監査を実施する際は、以下を確認する。

・以下に適合していること。

－情報セキュリティマネジメントに関して、組織自体が規定した要求事項
－本マネジメント基準の要求事項

・情報セキュリティマネジメントが有効に実施され、維持されていること。

b)内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。
・内部監査基本計画
・内部監査実施計画
・内部監査報告書
基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。
c)適合性の監査においては、以下の項目を対象に含む。
・関連する法令又は規制の要求事項
・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項
d)情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。
・管理策の有効性及び維持
・管理策が期待通りに実施されていること
4.6.2.3 組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。[27001-9.2c)]
監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。
監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。
・監査の目的と重点目標
・対象となる監査プロセスの状況と重要性
・対象となる領域の状況と重要性
・前回までの監査結果
4.6.2.4 組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)]
監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。
・監査の基準（以下の内容も含む。）
－目的、権限と責任
－独立性、客観性と職業倫理
－専門能力
－業務上の義務
－品質管理
－監査の実施方法
－監査報告書の形式
・監査の範囲
・監査の頻度又は時期
・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）
4.6.2.5 組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2e)]
監査人の選定においては監査基準に従い、以下の点を考慮する。

・外観上の独立性
・精神上の独立性
・職業倫理と誠実性
なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。
4.6.2.6 組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2f)]
4.6.2.7 組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2g)]
監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。
・監査の計画・実施に関する責任及び要求事項
・結果報告・記録維持に関する責任及び要求事項
要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。

4.6.3 マネジメントレビュー
4.6.3.1 トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。[27001-9.3]
あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。
・マネジメントレビュー基本計画
・マネジメントレビュー実施計画
・マネジメントレビューのための実施報告
基本計画では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。
4.6.3.2 トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3]
・前回までのマネジメントレビューの結果とった処置の状況
・情報セキュリティマネジメントに関連する外部及び内部の課題の変化
・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック
-不適合及び是正処置
-監視及び測定の結果
-監査結果
-情報セキュリティ目的の達成
・利害関係者からのフィードバック
・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況
・継続的改善の機会
また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。
4.6.3.3 マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。[27001-9.3]

マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。
・情報セキュリティマネジメントの有効性の改善
・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新
・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正
・必要となる経営資源の特定
・パフォーマンス測定方法の改善
なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。

4.6.3.4 組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。[27001-9.3]
マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。

4.7 情報セキュリティマネジメントの維持及び改善

4.7.1 是正処置

4.7.1.1 組織は、不適合が発生した場合、不適合の是正のための処置を取る。[27001-10.1a)]
a)是正措置を取る際は、以下を実施する。
・その不適合を管理し、是正するための処置
・その不適合によって起こった結果への対処
・是正処置を手順どおりに実施するために、以下について文書化する。
－不適合の再発防止を確実にするために選択した処置の必要性の評価
－必要な是正処置の決定
－必要な是正処置の実施
－実施した処置の記録
－実施した是正処置のレビュー
b)不適合は以下の活動によって検出される。
・定期的な情報セキュリティリスクアセスメント
・定期的な情報セキュリティ内部監査
・定期的なマネジメントレビュー
・不適合を手順どおりに検出するために、以下について文書化する。
－情報セキュリティマネジメントに対する不適合の特定
－情報セキュリティマネジメントに対する不適合の原因の決定
なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。

4.7.1.2 組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。[27001-10.1b)]
必要性を評価する際は、以下を実施する。
・その不適合のレビュー
・その不適合の原因の明確化
・類似の不適合の有無、又はそれが発生する可能性の明確化

4.7.1.3 組織は、必要な処置を実施する。[27001-10.1c)]

4.7.1.4 組織は、とった全ての是正処置の有効性をレビューする。[27001-10.1d)]

4.7.1.5 組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。[27001-10.1e)]

4.7.1.6 組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。[27001-10.1]

4.7.1.7 組織は、是正処置の証跡として、以下の文書化した情報を保持する。[27001-10.1f)/10.1g)]

・不適合の性質及びとった処置
・是正処置の結果

4.8 文書化した情報の管理

4.8.1 文書化の指針

4.8.1.1 組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。[27001-7.5.1]

・情報セキュリティ方針
・情報セキュリティ目的
・情報セキュリティリスクアセスメントのプロセス
・情報セキュリティリスク対応のプロセス
・情報セキュリティリスクアセスメントの結果
・情報セキュリティリスク対応計画
・パフォーマンス測定の結果

これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。

4.8.2 文書の作成・変更及び管理

4.8.2.1 組織は、以下を行うことによって、文書化した情報を作成及び更新する。[27001-7.5.2]

・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号）
・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択
・適切性及び妥当性に関する、適切なレビュー及び承認
・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定
・文書を発行する前における、適正性のレビュー及び承認
・必要に応じた、文書の更新及び再承認
・廃止文書の誤使用の防止
・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述
・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新

また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。

4.8.2.2 組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。[27001-7.5.3]

・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。
・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。

・文書化した情報の配付、アクセス、検索及び利用
・文書化した情報の読みやすさが保たれることを含む、保管及び保存
・文書化した情報の変更の管理（例えば、版の管理）
・文書化した情報の保持及び廃棄
また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。

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。

4.9.1 リスクコミュニケーションの計画

4.9.1.1 リスクコミュニケーション計画を策定する。
リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。
・通常運用のためのリスクコミュニケーション計画
・緊急事態のためのリスクコミュニケーション計画
リスクコミュニケーション計画は、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。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。
・適切な利害関係者の参画による、効果的な情報交換／共有
・法令、規制及びガバナンスの要求事項の順守
・コミュニケーション及び協議に関するフィードバック及び報告の提供
・組織に対する信頼を醸成するためのコミュニケーションの活用
・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施

4.9.2 リスクコミュニケーションの実施

4.9.2.1 リスクコミュニケーションを実施する仕組みを確定する。
リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（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。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。
・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達
・枠組み、その有効性及び成果に関する適切な内部報告
・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供
・内部の利害関係者との協議のためのプロセス
仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。

4.9.2.2 リスクコミュニケーションを実施する。
リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。
・組織のリスクマネジメント結果の保証を提供する

・リスク情報を収集する
・リスクアセスメントの結果を共有しリスク対応計画を提示する
・意思決定者と利害関係者（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。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する
・意思決定を支援する
・新しい情報セキュリティ知識を入手する
・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する
・意思決定者及び利害関係者（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。）にリスクについての責任を意識させる
・セキュリティ意識を改善する

リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。

第5章　管理策基準

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

管理目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。

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。

5.1.2 情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。

6 情報セキュリティのための組織

6.1 内部組織

管理目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1 全ての情報セキュリティの責任を定め、割り当てる。

6.1.1.13.PB クラウドサービス事業者は、クラウドサービス利用者、クラウドサービス事業者及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。

6.1.2 相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。

6.1.3 関係当局との適切な連絡体制を維持する。

6.1.3.3.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、クラウドサービス事業者の組織の地理的所在地、及びクラウドサービス事業者がクラウドサービス利用者のデータを保管する可能性のある国々を通知する。

6.1.4 情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。

6.1.5 プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。

6.2 モバイル機器及びテレワーキング

管理目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

6.2.1 モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。

6.2.2 テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。

6.3.P クラウドサービス利用者及びクラウドサービス事業者の関係

管理目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。

6.3.1.P クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。

6.3.1.1.PB クラウドサービス事業者は、クラウドサービス利用の一環としてクラウ

ドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス事業者の情報セキュリティ管理策及び責任を文書化し、通知する。

7 人的資源のセキュリティ

7.1 雇用前

管理目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.1.1 全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。

7.1.2 従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。

7.2 雇用期間中

管理目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。

7.2.1 経営陣は､組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。

7.2.2 組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。

7.2.2.19.PB クラウドサービス事業者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データの適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。

7.2.3 情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。

7.3 雇用の終了及び変更

管理目的:雇用の終了又は変更のプロセスの一部として､組織の利益を保護するため。

7.3.1 雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。

8 資産の管理

8.1 資産に対する責任

管理目的：組織の資産を特定し、適切な保護の責任を定めるため。

8.1.1 情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。

8.1.1.6.PB クラウドサービス事業者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。

8.1.2 目録の中で維持される資産は、管理する。

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に必要となる情報

8.1.3 情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。

8.1.4 全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。

8.1.5.P クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。

8.2 情報分類

管理目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.1 情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。

8.2.2 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.2.7.PB クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。

8.2.3 資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.3 媒体の取扱い

管理目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。

8.3.1 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。

8.3.2 媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。

8.3.3 情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

管理目的：情報及び情報処理施設へのアクセスを制限するため。

9.1.1 アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。

9.1.2 利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。

9.2 利用者アクセスの管理

管理目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

9.2.1 アクセス権の割当てを可能にするために、利用者の登録及び登録削除について

の正式なプロセスを実施する。

9.2.1.6.PB クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス事業者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。

9.2.2 全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。

9.2.2.8.PB クラウドサービス事業者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。

9.2.3 特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.11.PB クラウドサービス事業者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術を提供する。

9.2.4 秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.9.PB クラウドサービス事業者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。

9.2.5 資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。

9.2.6 全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。

9.3 利用者の責任

管理目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

9.3.1 秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。

9.4 システム及びアプリケーションのアクセス制御

管理目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため。

9.4.1 情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。

9.4.1.8.PB クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。

9.4.2 アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。

9.4.2.2.B強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。

9.4.3 パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。

9.4.4 システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。

9.4.5 プログラムソースコードへのアクセスは、制限する。

9.5.P 共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御
管理目的:共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。

9.5.1.P クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。

9.5.2.P クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。

9.5.2.1.PB クラウドサービス事業者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする)、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得)を実施する。

10 暗号

10.1 暗号による管理策

管理目的:情報の機密性、真正性及び/又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

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。

10.1.1.9.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、当該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の情報を提供する。

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。

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、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理し消去する機能を提供し、または、当該利用者が暗号鍵を管理し消去する機能を実装するために必要となる情報を提供する。

11 物理的及び環境的セキュリティ

11.1 セキュリティを保つべき領域

管理目的:組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.1.1 取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

11.1.2 セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。

11.1.3 オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。

11.1.4 自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。

11.1.5 セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

11.1.6 荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。

11.2 装置

管理目的:資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止する

ため。

11.2.1 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。

11.2.2 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。

11.2.3 データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。

11.2.4 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。

11.2.5 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。

11.2.6 構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。

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。

11.2.7.4.PB クラウドサービス事業者は、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。

11.2.8 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。

11.2.9 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。クリアデスク・クリアスクリーン方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応するリスク及び文化的側面を含める。

12 運用のセキュリティ

12.1 運用の手順及び責任

管理目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。

12.1.1 操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。

12.1.2 情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。

12.1.2.11.PB クラウドサービス事業者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報を、クラウドサービス利用者に提供する。

12.1.3 要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。

12.1.3.9.PB クラウドサービス事業者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。

12.1.4 開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。

12.1.5.P クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。

12.1.5.1.PBクラウドサービス事業者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。

12.2 マルウェアからの保護

管理目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。

12.2.1 マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

12.3 バックアップ

管理目的：データの消失から保護するため。

12.3.1 情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。

12.4 ログ取得及び監視

管理目的：イベントを記録し、証拠を作成するため。

12.4.1 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。

12.4.1.15.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、ログ取得機能を提供する。

12.4.2 ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。

12.4.3 システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。

12.4.4 組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。

12.4.4.4.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、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。

12.4.5.P クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。

12.5 運用ソフトウェアの管理

管理目的：運用システムの完全性を確実にするため。

12.5.1 運用システムに関わるソフトウェアの導入を管理するための手順を実施する。

12.6 技術的ぜい弱性管理

管理目的：技術的ぜい弱性の悪用を防止するため。

12.6.1 利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。

12.6.1.18.PB クラウドサービス事業者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。

12.6.2 利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。

12.7 情報システムの監査に対する考慮事項

管理目的：運用システムに対する監査活動の影響を最小限にするため。

12.7.1 運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。

13 通信のセキュリティ

13.1 ネットワークセキュリティ管理

管理目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

13.1.1 システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。

13.1.2 組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。

13.1.3 情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。

13.1.4.P 仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。

13.2 情報の転送

管理目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

13.2.1 あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。

13.2.2 情報転送に関する合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。

13.2.3 電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.4 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。

14 システムの取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

管理目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

14.1.1 情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。

14.1.2 公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。

14.1.3 アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。

・不完全な通信
・誤った通信経路設定
・認可されていないメッセージの変更
・認可されていない開示
・認可されていないメッセージの複製又は再生

14.2 開発及びサポートプロセスにおけるセキュリティ

管理目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。

14.2.1 ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。

14.2.1.13.PB クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。

14.2.2 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

14.2.3 オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

14.2.4 パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。

14.2.5 セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。

14.2.6 組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。

14.2.7 組織は、外部委託したシステム開発活動を監督し、監視する。

14.2.8 セキュリティ機能（functionality）の試験は、開発期間中に実施する。

14.2.9 新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。

14.3 試験データ

管理目的：試験に用いるデータの保護を確実にするため。

14.3.1 試験データは、注意深く選定し、保護し、管理する。

15 供給者関係

15.1 供給者関係における情報セキュリティ

管理目的：供給者がアクセスできる組織の資産の保護を確実にするため。

15.1.1 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。

15.1.1.14.B組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。

15.1.1.16.B当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を指定する。

15.1.2 関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。

15.1.2.18.PB クラウドサービス事業者は、クラウドサービス事業者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス事業者が実行する適切な情報セキュリティ対策を、合意の一環として定める。

15.1.3 供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品

のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.2 供給者のサービス提供の管理

管理目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

15.2.1 組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。

15.2.2 関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む）を管理する。

16 情報セキュリティインシデント管理

16.1 情報セキュリティインシデントの管理及びその改善

管理目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

16.1.1 情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。

16.1.2 情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。

16.1.3 組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。

16.1.4 情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。

16.1.5 情報セキュリティインシデントは、文書化した手順に従って対応する。

16.1.6 情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。

16.1.7 組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。

16.1.7.13.PB クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。

17 事業継続マネジメントにおける情報セキュリティの側面

17.1 情報セキュリティ継続

管理目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。

17.1.1 組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。

17.1.2 組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。

17.1.3 確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。

17.2 冗長性

管理目的：情報処理施設の可用性を確実にするため。

17.2.1 情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。

18 順守

18.1 法的及び契約上の要求事項の順守

管理目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

18.1.1 各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。

18.1.2 知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。

18.1.2.13.PB クラウドサービス事業者は、知的財産権の順守に対応するためのプロセスを確立する。

18.1.3 記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

18.1.3.13.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、クラウドサービスの利用に関して、クラウドサービス事業者が収集し、蓄積する記録の保護について、情報を提供する。

18.1.4 プライバシー及び個人識別情報（PII）の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。

18.1.5 暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。

18.1.5.7.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、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供する。

18.2 情報セキュリティのレビュー

管理目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

18.2.1 情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。

18.2.2 管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。

18.2.3 情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。

（別紙１）詳細管理策の選択及びその運用における留意点

ISMAP クラウドサービスリストへの登録を申請するクラウドサービス事業者は、ISMAP 管理基準に準拠して詳細管理策を選択し、整備した統制を有効に運用する必要がある。その際、クラウドサービス事業者は、クラウドサービスの情報セキュリティに深刻な影響を与え重大な事故につながるリスクを低減するための重要な領域について、特に十分な対応を行い、重大な事故につながるリスクの低減に努めること。

なお、上記重要な領域としては、以下の４つが挙げられる。

１．アクセス管理（特権の管理、ID 管理、物理セキュリティ等）
２．システムの開発・変更に係る管理（開発管理、変更管理）
３．システムの運用管理（ぜい弱性管理、暗号による処理、媒体の処分、障害管理、システム運用監視、ネットワーク管理、冗長性の確保等）
４．外部委託先管理（１.～３.に関するもの）

（参考１）各規格類の参照における考え方

第１章に規定しているとおり、本管理基準は国際規格をベースに「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）」、「SP800-53rev.4(以下、SP800-53)」を参照して作成した。ここでは、これらの規格を参照するにあたっての考え方を記述する。

ガバナンス基準における JIS Q 27014:2015（ISO/IEC 27014:2013)の参照は以下の考え方による。

- 「一般」「概要」「原則」については監査対象とはせず、監査実施時の「参考情報」と位置付ける。
- 「プロセス」の統制の目標についても、詳細管理策の「解説」と位置付ける。

また、内容の伝わりやすさの観点から、JIS Q 27014:2015（ISO/IEC 27014:2013)から下記の修正を行っている。

- 主体を「経営陣」に統一
- 「業務執行幹部」を「管理者」に読み替え
- 関連の深い内容を１つの基準の具体化として再整理

統一基準は政府機関等が順守すべき事項を規定している。これらの事項は、クラウドサービス事業者が実施すべき対策に加えてクラウドサービス利用者が追加的な対策をして初めて達成されるものであり、統一基準の項目をそのままクラウドサービス事業者に求めるのは適切ではない。このため、政府統一基準の目的趣旨に則して、クラウドサービス事業者が主体として行うべき内容を勘案し、基準項目としての読み替えを行った上で、「クラウドサービス事業者が実施しなければ、クラウドサービス利用者が統一基準を満たすことに支障を来す内容か否か」の観点から、クラウドサービス事業者に求めるべき内容であると判断されるものについて追加、及び内容を一部追加する形で整理を行った。

また、統一基準をはじめ参考としている基準の多くはオンプレミスの情報システムの利用者が実施主体であり、クラウドサービス事業者を実施主体として策定されたものではない。係る観点から、以下の 3 つの定型管理策への読み替え作業を行った。

- 定型管理策 1：クラウドサービス事業者が自ら該当管理策を実施すべきもの
- 定型管理策２：政府機関が該当管理策を実現するために、クラウドサービス事業者が機能提供すべきもの
- 定型管理策３：政府機関が該当管理策を実施できるように、クラウドサービス事業者が情報提供すべきもの

SP800-53 は、海外の基準の中で運用実績が長く、複数回の基準更新が行われてきたことから、基準を検討する上で参考とした。この際、クラウドサービスを対象としていること、政府として最も多く扱われる機密性 2 の情報を扱うことを想定した水準としたこと、国際規格との対応関係という観点から、FedRAMP において Moderate の要求事項とされている項目であって、ISO/IEC 27001 との比較において、ISO/IEC27001 では対応が取れていないとされている項目について検討の対象を絞り込み追加、及び内容を一部追加する形で整理を行った。

(参考２)別表に関する留意点

別表 2. マネジメント基準

・変更種別の欄において「変更」と記載されている管理策は、クラウド情報セキュリティ管理基準の管理策を一部変更した管理策であることを表す。

別表 3. 管理策基準

・変更種別の欄の凡例

変更：クラウド情報セキュリティ管理基準の管理策を一部変更した管理策。

追加：クラウド情報セキュリティ管理基準の管理策には存在せず、本管理基準で追加された管理策。

欠番：クラウド情報セキュリティ管理基準の管理策においてクラウドサービス利用者向けの管理策であり、クラウドサービス事業者を実施主体とした本管理基準において削除された管理策。

別表 4. マッピング(管理基準 vs 統一基準)、別表 5. マッピング(統一基準 vs 管理基準)

・本マッピングは、他の基準との関係について参考となるよう、詳細管理策を踏まえた上で、統制目標レベルで関係する項目についてマッピングしたものであるが、あくまでも関連が深いものを示したものであり、マッピングされた個々の項目が互いに必要十分な関係にあることを示したものでないことに留意が必要である。

・また、別表５において、本基準は 1.2 に規定しているとおり、クラウドサービス事業者を実施主体とした管理基準であるため、本マッピングにおける統一基準４部のマッピングは、クラウドサービス事業者が委託元となる場合を想定して行っている。

別表 6. マッピング(管理基準 vs SP800-53)、別表 7. マッピング(SP800-53 vs 管理基準)

・本マッピングは、他の基準との関係について参考となるよう、詳細管理策を踏まえたうえで、統制目標レベルで関係する項目についてマッピングしたものであるが、あくまでも関連が深いものを示したものであり、マッピングされた個々の項目が互いに必要十分な関係にあることを示したものでないことに留意が必要である。

・なお、本管理基準の策定の過程において、SP800-53 において示されている対応関係に追加している管理策が存在する。

別表 8. 個別管理策の実施頻度の例

・個別管理策は、クラウドサービス事業者がサービス内容及びセキュリティリスク分析の結果等を踏まえて定めた頻度で実施することが原則であるが、その頻度を決定する上での参考として、示すものである。

個別管理策の実施頻度の例

No	主たる監査対象※	実施頻度の例
1	規定等	最低年１回
2	根拠となる文書・記録等① サンプルテストを実施しないもの （設計書、仕様書、手順書等）	最低年１回、変更が発生した都度
3	根拠となる文書・記録等② サンプルテストを実施するもの （申請書、承認記録、システムログ、台帳等）	随時（統制の性質に応じて、日次・週次・月次・四半期等に一度）
4	根拠となる設定等 （パラメータ、ステータス、コマンド等）	最低年１回、変更が発生した都度
5	設備、建物等	最低年１回（施設へのアクセスログのレビュー等は上記 No.3 に同じ）

※個別管理策の監査手続の対象となるもの。詳細は ISMAP 標準監査手続において定義。