# 情報セキュリティ管理基準

# （令和７年改正版）

# 目次

# Ⅰ．概要

## 1.1 主旨

インターネットをはじめとする情報技術（IT）が組織体の活動や社会生活に深く浸透することに伴い、情報セキュリティの確保は、組織体が有効かつ効率的に事業活動を遂行するための必要な条件、安全・安心な社会生活を支えるための基盤要件となっている。一般に組織体に求められる情報セキュリティ対策は、組織、人、運用、技術、法令など多様な観点からみた具体的な対策が要求されており、ITが浸透した企業においては、これらに加えて内部統制（法令順守、情報管理等）の仕組みを情報セキュリティの観点から構築・運用する体制の確立も強く望まれている。

このような状況を踏まえ、経済産業省では、平成15年に、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール（管理策）を整備・運用するための実践的な規範として、「情報セキュリティ管理基準」（平成15年経済産業省告示第112号）を策定した。その後、情報セキュリティマネジメントに関する国際規格であるISO/IEC 27001（JIS Q 27001[1]）及びISO/IEC 27002（JIS Q 27002）の策定及び改訂を受けて、平成20年及び平成28年にそれぞれ管理策等の見直しを実施した改正版を策定している。本管理基準は、改正時点での情報セキュリティマネジメントに関する最新規格であるJIS Q 27001:2023及びJIS Q 27002:2024に準拠させたものである。

## 1.2 本管理基準の位置付け

本管理基準は、組織体における情報セキュリティマネジメントの円滑で効果的な確立を目指して、マネジメントサイクル構築の出発点から具体的な管理策に至るまで、包括的な適用範囲を有する基準となっている。一方で、包括的な基準（参照基準）であるゆえに、組織体個別の事情への対応に最適化したものではない。また、情報セキュリティ監査を実施するにあたっては、判断の尺度をより具体的に規定する必要も生じ得る。そこで、本管理基準を適切に活用するためには、組織体が属する業界又は事業活動の特性等を考慮し、必要に応じて本管理基準の趣旨及び体系に則って、本管理基準に記載の管理策を取捨選択、追加、統合又は具体化することにより、該当する関係機関を取り巻く状況に適応させた個別管理策体系を策定する必要がある[2]。

なお、本管理基準は、旧版と同様に、本管理基準と姉妹編をなす「情報セキュリティ監査基準」に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。本管理基準は、日本におけるISMS認証制度である「ISMS適合性評価制度」において用いられる適合性評価の尺度にも整合するように配慮している。ただし、前述の通り包括的な基準である関係で、監査における判断の尺度として不十分な管理策（例：強力なパスワードを選択する）が想定され得るので、監査人は監査で用いる基準として十分と判断される程度に具体化させた管理策を個別管理基準としてとりまとめることが望ましい。

[1] JIS規格については、日本工業標準調査会（JISC）のウェブサイト（ http://www.jisc.go.jp/ ）で検索することにより閲覧することができる。

[2] 策定にあたっては、本管理基準の関連文書である「情報セキュリティ管理基準活用ガイドライン」を参照のこと。

## Ⅱ. 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。

### 2.1 ガバナンス基準

「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について示すものである。記載している事項は、情報セキュリティガバナンスに関する国際規格であるISO/IEC 27014:2020における規定事項を参考に策定している。

「ガバナンス基準」の内容は以下のとおりである。

3.1 情報セキュリティガバナンスの概要

3.2 情報セキュリティガバナンスの目的

3.3 情報セキュリティガバナンスのプロセス

### 2.2 マネジメント基準

「マネジメント基準」では、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項を定めている。それぞれの事項は、JIS Q 27001:2023を基にして策定しているが、抽出に当たっては次の３点を考慮した。

- ISMS認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織、情報セキュリティ監査を受ける組織など幅広い利用者を想定した記述とする。
- 情報セキュリティマネジメントの計画、実行、点検、処置の各プロセスで行うべき事項を明確にする。
- 「マネジメント基準」の章構成は、情報セキュリティマネジメントのプロセスを考慮し、JIS Q 27001:2023における構成順序を一部変更する。その際、JIS Q 27001:2023との対応が分かるように記載する。

「マネジメント基準」は、原則、全て実施すべき事項である。

「マネジメント基準」の内容は以下のとおりである（なお、[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。）。

4.1 マネジメント基準

4.2 記載内容について

4.3 凡例

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］

4.4.2 組織及びその状況の理解［27001-4.1］

4.4.3 利害関係者のニーズ及び期待の理解［27001-4.2］

4.4.4 適用範囲の決定［27001-4.3］

4.4.5 方針の確立［27001-5.2 / 6.2 / 5.1］

4.4.6 リスク及び機会に対処する活動［27001-6.1］

4.4.7 情報セキュリティリスクアセスメント［27001-6.1.2］

4.4.8 情報セキュリティリスク対応［27001-6.1.3］

4.5 情報セキュリティマネジメントの運用［27001-8］

4.5.1 資源管理［27001-7.1 / 5.1］

4.5.2 力量、認識［27001-7.2 / 7.3 / 5.1］

4.5.3 コミュニケーション［27001-7.4］

4.5.4 情報セキュリティマネジメントの運用の計画策定及び管理［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［27001-8.2 / 8.3］

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］

4.6.1 有効性の継続的改善［27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1］

4.6.2 パフォーマンス評価［27001-9］

4.6.3 マネジメントレビュー［27001-9.3］

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］

4.7.1 是正処置［27001-10.2］

4.8 文書化した情報の管理［27001-7.5］

4.8.1 文書化の指針［27001-7.5.1］

4.8.2 文書の作成・変更及び管理［27001-7.5.2 / 7.5.3］

## 2.3 管理策基準

「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、JIS Q 27001:2023附属書A「管理目的及び管理策」、JIS Q 27002:2024をもとに、既存のISMS認証などとの整合性にも配慮しつつ、専門家の知見を加えて作成している。

JIS Q 27002:2024においては、個別の管理策（Control）毎にその目的（Purpose）と管理策活用のための手引（Guidance）が規定されている。本管理基準では活用上の便宜の観点から、手引に示されている内容のうち、原則として「～ことが望ましい。」という表現で記述され、情報セキュリティマネジメントを実践する際に管理策の具体化に役立つと判断される項目を「詳細管理策」として付番し、それ以外の内容を「参考」として整理している。詳細管理策として規定した内容が管理策を実践する上で有効かどうかは組織体が属する業界又は事業活動の特性等によって異なり、すべての項目を取り入れる必要はない。詳細管理策に含まれる箇条書き形式の項目には、列挙されている項目をすべてに対処すべきもの、包含した上でさらに追加を考慮すべきもの、又は例示にとどまるものなどの種類があり、詳細管理策の内容によって意味が異なるため留意する必要がある。

また、本管理基準においては、個別管理策策定における便宜を図る観点から、JIS Q 27002:2024における管理策の整理体系に加えて、以下の２種類の構造化を行っている。

**① 管理策の構造化**：JIS Q 27002:2024では「5 組織的管理策」に37項目、「8 技術的管理策」に34項目の管理策がそれぞれ含まれるが、目的や対象の類似性を踏まえてこれらを最大7つのグループに分類し、5a,5b,･･･のように章番号にアルファベット小文字を付加することで識別可能とした。この結果、本管理基準では個別の管理策は「5a-5.1」のようにJIS Q 27002:2024の管理策番号の前にグループを示す記号を付加して表記されている。

**② 詳細管理策の構造化**：JIS Q 27002:2024では手引内に下線の付いた小見出しが設けられている（例：「5.9 情報及びその他の関連資産の目録」における「目録」や「管理責任」等）。本管理基準でもこれらを利用し、詳細管理策内で同様の小見出し（**【】**で括られている事項）を設けている（付番無し）。

「管理策基準」の内容は次のとおりである。

5 組織的管理策

5a 組織的管理

5a-5.1 情報セキュリティのための方針群

5a-5.2 情報セキュリティの役割及び責任

5a-5.3 職務の分離

5a-5.4 管理層の責任

5a-5.5 関係当局との連絡

5a-5.6 専門組織との連絡

5a-5.7 脅威インテリジェンス

5a-5.8 プロジェクトマネジメントにおける情報セキュリティ

5b 資産管理

5b-5.9 情報及びその他の関連資産の目録

5b-5.10 情報及びその他の関連資産の許容される利用

5b-5.11 資産の返却

5b-5.12 情報の分類

5b-5.13 情報のラベル付け

5b-5.14 情報の転送

5c アクセス権管理

5c-5.15 アクセス制御

5c-5.16 識別情報の管理

5c-5.17 認証情報

5c-5.18 アクセス権

5d 供給者管理

5d-5.19 供給者関係における情報セキュリティ

5d-5.20 供給者との合意における情報セキュリティの取扱い

5d-5.21 ICTサプライチェーンにおける情報セキュリティの管理

5d-5.22 供給者のサービス提供の監視、レビュー及び変更管理

5d-5.23 クラウドサービスの利用における情報セキュリティ

5e インシデント管理

5e-5.24 情報セキュリティインシデント管理の計画策定及び準備

5e-5.25 情報セキュリティ事象の評価及び決定

5e-5.26 情報セキュリティインシデントへの対応

5e-5.27 情報セキュリティインシデントからの学習

5e-5.28 証拠の収集

5f 事業継続における情報セキュリティ管理

5f-5.29 事業の中断・阻害時の情報セキュリティ

5f-5.30 事業継続のためのICTの備え

5g コンプライアンス管理

5g-5.31 法令、規制及び契約上の要求事項

5g-5.32 知的財産権

8b 情報資産運用に関する管理

8b-8.7 マルウェアに対する保護

8b-8.8 技術的ぜい弱性の管理

8b-8.9 構成管理

8b-8.10 情報の削除

8b-8.11 データマスキング

8b-8.12 データ漏えい防止

8b-8.13 情報のバックアップ

8b-8.14 情報処理施設・設備の冗長性

8b-8.15 ログ取得

8b-8.16 監視活動

8b-8.17 クロックの同期

8b-8.18 特権的なユーティリティプログラムの使用

8b-8.19 運用システムへのソフトウェアの導入

8c 情報システムの適正利用の管理

8c-8.20 ネットワークセキュリティ

8c-8.21 ネットワークサービスのセキュリティ

8c-8.22 ネットワークの分離

8c-8.23 ウェブフィルタリング

8c-8.24 暗号の利用

8d 情報システム開発／導入の管理

8d-8.25 セキュリティに配慮した開発のライフサイクル

8d-8.26 アプリケーションセキュリティの要求事項

8d-8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

8d-8.28 セキュリティに配慮したコーディング

8d-8.29 開発及び受入れにおけるセキュリティテスト

8d-8.30 外部委託による開発

8d-8.31 開発環境、テスト環境及び本番環境の分離

8d-8.32 変更管理

8d-8.33 テスト用情報

8d-8.34 監査におけるテスト中の情報システムの保護

## Ⅲ. ガバナンス基準

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について示すものである。

### 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[3]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[4]。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「Ⅳ. 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 [27014-7.2]

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 [27014-7.3]

#### 3.3.1 概要

情報セキュリティガバナンスは、評価、指示、モニタ及びコミュニケーションの各プロセスで構成される。次項以降において、各プロセスにおいて、ガバナンス主体及び各情報セキュリティマネジメントシステムの責任者[5]が実行する内容を示す。

#### 3.3.2 評価

3.3.2.1　ガバナンス主体は、以下を実行する。

・事業に取り組む際の関連するリスク及び機会の確実な考慮

---

[3] 本基準における情報セキュリティガバナンスの目的の設定及びプロセスの定義に関する責任を担う主体として、「ガバナンス主体」という用語を用いる。これはISO/IEC 27014:2020における“governing body”に対応し、組織における経営者又は取締役会が該当する。

[4] 組織体の事情により、複数の情報セキュリティマネジメントシステムを構築することもあり得る。

[5] 情報セキュリティマネジメントシステムの運用の責任を担う個人又はグループ。ISO/IEC 27014:2020においては“top management”が用いられている。

・情報セキュリティに関する報告に対応するための、情報セキュリティマネジメントシステムにおける目的と優先度の規定

3.3.2.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。

・組織体の目的を適切に支援し、維持するような情報セキュリティの確立

・重大な影響を伴う新規の情報セキュリティプロジェクトを実施する際の、組織体のガバナンス主体への承認依頼

### 3.3.3 指示

3.3.3.1　ガバナンス主体は、以下を実行する。

・組織体全体の戦略の方向性と目的の設定

・その組織体のリスク選好の決定

・情報セキュリティ戦略の承認

3.3.3.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。

・適切な投資及び資源の配分の実施

・組織体の目的に合致するように情報セキュリティの目的を調整

・情報セキュリティに関する役割と責任の割当

・情報セキュリティポリシーの規定

### 3.3.4 モニタ

3.3.4.1　ガバナンス主体は、以下を実行する。

・各情報セキュリティマネジメントシステムの活動の有効性に関する報告の受領

・組織体の優先度の文脈での、前項で報告された内容の評価

・各情報セキュリティマネジメントシステムの責任者への優先度の伝達

3.3.4.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。

・情報セキュリティマネジメントシステム活動の有効性の評価

・内部及び外部の要求事項への確実な適合の確保

・組織体に関わる変化、法令及び規制の環境、並びに情報リスクへの潜在的影響の考慮

・適切なパフォーマンス指標を選定し、組織的な観点から適切なタイミングで報告が実施されるよう要求を伝達

・情報セキュリティの実績に関する結果のフィードバックを組織体の経営陣に提供

・情報リスク及び情報セキュリティに影響する新規の開発についての、組織体の経営陣への注意喚起

### 3.3.5 コミュニケーション

3.3.5.1　ガバナンス主体は、以下を実行する。

・外部の利害関係者を対象とする、組織体がその活動及び優先度の実態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の報告

・規制上の義務、利害関係者の期待及び情報セキュリティに関する組織体の要求事項の特定及び優先度の決定

・注意及び決定が必要な問題についての、各情報セキュリティマネジメントシステムの責

任者への助言

・関連する利害関係者に向けた、情報セキュリティの優先度決定を支援するために採用すべき詳細な対象に関する指導

・情報セキュリティに積極的な文化の奨励

・スタッフ及びその他の人々を対象とする、情報セキュリティマネジメントシステムの適用範囲での責任を果たすための訓練とコミュニケーション

# Ⅳ. 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

JIS Q 27001:2023を基に、情報セキュリティマネジメントの計画、実行、点検、処置等の活動に必要な事項を定める。

## 4.3 凡例

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　[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)]**

その際は、以下を行うこととする。

・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。

：

[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。

### 4.4.1 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[6]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。 [27001-5.1b) / 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

[6] 情報セキュリティマネジメントを行う組織の長（または責任者）
（注）「情報セキュリティマネジメントを行う組織」は部門単位であることがあり、複数の組織が一つの企業や機関の中に存在することがある。

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に基づく是正処置、マネジメントレビュー議事録等に、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、組織内に伝達する。 [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、組織の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不可欠な責任・権限を明確にしたうえで、それぞれに適切な割り当てが行われていることを確認する。責任・権限の例を以下に示す。

・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･権限をもつリスク所有者[7]
・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、その他の関連する管理層[8]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)]**

その他の関連する管理層が、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 [27001-4.1]**

**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

[7] リスク所有者とは、リスクを運用管理することについて、責任及び権限をもつ人を指す（以下同じ。）。
[8] 組織のそれぞれの階層にある部署の責任者を指す。ISO/IEC 27001:2022におけるmanagementに対応する。

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、以下に例示するものが含まれ得る。

a) 外部状況

・国外、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 [27001-4.2]

#### 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
・利害関係者に関連する要求事項
・要求事項のうち、情報セキュリティマネジメントを通じて取り組むもの

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る場合もあるが、利害関係者には、以下に例示する人又は組織が含まれ得る。

・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・権限をもつ人又は組織。以下にその例を示す。
  －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 [27001-4.3]

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、以下に例示するものが含まれ得る。

－国外、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、以下に例示するものが含まれ得る。

－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 [27001-5.2 / 6.2 / 5.1]**

**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、これを監視し、関係者に伝達し、必要に応じて更新し、文書化した情報として利用可能な状態にするとともに、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記録として保管する。記録の例を以下に示す。

・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 [27001-6.1]

#### 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 [27001-6.1.2]

#### 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、法律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) 情報セキュリティリスク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ことなどが必要になる。

#### 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[9]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

[9] リスク源とは、それ自体又は他との組合せによって、リスクを生じさせる力を潜在的にもっているものを指す（以下同じ。）。

・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、法律、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 [27001-6.1.3]**

**4.4.8.1 組織は、情報セキュリティリスク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[10]

・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[11]

---

[10] リスクが発生する要因や前提となる活動を開始又は継続しないと決定することにより、リスクの発生を回避すること。例えば、地震などが頻発する地域への事業所等の新設を中止することなど。

[11] ある機会を得る機会のために、情報セキュリティ管理策の実施に要する費用対効果などを考慮しつつ、リスクを引き受ける又は負担すること。例えば、市場を拡大するために、営業所を増設した結果、営業所からの情報漏えいのリスクが増加するなど。

・リスク源の除去[12]

・発生頻度の変更[13]

・結果の変更[14]

・（契約及びリスクファイナンス[15]を含む）他者とのリスクの共有[16]

・情報に基づいた意思決定によるリスクの保有[17]

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[18]。

**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

---

[12] リスクの発生し易さや結果に与える影響の源を除去することにより、リスクを減少させること。例えば、記憶媒体等の持出・持込を禁止することにより、記憶媒体を原因とする情報漏えいを防止するなど。

[13] リスクの発生し易さを変更すること。例えば、物理的な設置場所を地震や洪水の頻発する地域から、発生しない地域に移設するなど。

[14] リスクが組織にもたらす結果を変更すること。例えば、情報のバックアップを実施することで、情報の破壊が発生しても、損害が生じないようにするなど。

[15] リスクファイナンスとは、財務的な損害が発生した際の資金面での対応のことを指す。損害が発生した時のために、資金を組織内に保有する対応と、保険等により、リスクを第三者に移転させる対応がある。

[16] リスクを他者と共有すること。例えば、リスクが生じる業務やサービスを他社に委託する、保険等によりリスクを移転することなどが含まれる。

[17] 情報に基づいた意思決定により、リスクを低減するための管理策を実施せず、リスクを受容すること。例えば、リスクを生じさせる脅威の発生頻度が低い、リスクによる影響及び損害が小さい、又は、情報セキュリティ管理策の実施に要する費用及び労力と管理策による効果のバランスが取れないなどの情報に基づき、管理策を実施せず、リスクを受容するなど。

[18] この場合、できる限り複数の選択肢の中から適切なものを選ぶようにし、管理策が無効化された場合の代替策や、環境の変化に伴う改善策の立案などに役立てることを考慮する。

・費用・労力、制約

・後日の報告、監視に必要な要求事項

・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、責任及び権限をもつリスク所有者が、責任及び権限をもつ。

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、どのような責任をも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、管理層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 [27001-8]

### 4.5.1 資源管理 [27001-7.1 / 5.1]

**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 [27001-7.2 / 7.3 / 5.1]

**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、必要な力量を身につ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)]**

必要な力量を身につ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、業務上のリスクや、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の取組を実施する。取組の例を以下に示す。

・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、力量の証拠として、適切な文書化した情報を保持する。[27001-7.2d)]**

教育、訓練については以下の例示を参考に検討し、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［27001-7.4］**

**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
・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方法

b) 内部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、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
・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
・組織内の従業員

c) 外部コミュニケーションでは、以下の例示を参考に、組織の情報セキュリティマネジメントの実施に不可欠な者と、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策定及び管理 [27001-8.1]

**4.5.4.1 組織は、次に示す事項の実施によって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]**

・プロセスに関する基準の設定

・その基準に従った、プロセスの管理の実施

**4.5.4.2 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、利用可能な状態にする。 [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。

**4.5.4.3 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講じる。 [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 [27001-8.2 / 8.3]

**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 [27001-5.1 / 8.2 / 9 / 10.2]

#### 4.6.1 有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]

**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ではなく、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［27001-9］**

**4.6.2.1 組織は、以下を決定し、その結果の証拠として文書化した情報を利用可能な状態とするとともに、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評価する。［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（妥当と考えられる、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
・監視及び測定の実施者
・監視及び測定の結果の、分析及び評価の時期
・監視及び測定の結果の、分析及び評価の実施者

**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並びに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、責任及び計画策定に関する要求事項及び報告を含む、監査プログラムを計画、確立、実施及び維持する。 [27001-9.2.2]**

内部監査プログラムを確立するとき、組織は、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。

**4.6.2.4 組織は、監査基準及び監査範囲を明確にする。[27001-9.2.2a)]**

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。[27001-9.2.2b)]**

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。 [27001-9.2.2c)]**

**4.6.2.7 組織は、監査プログラムの実施及び監査結果の証拠として、文書化した情報を利用可能な状態にする。 [27001-9.2.2]**

監査手順に以下の内容を反映させるとともに、文書化し、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 [27001-9.3]**

**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

基本計画書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。 [27001-9.3.2]**

・前回までのマネジメントレビューの結果講じた処置の状況

・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

・情報セキュリティマネジメントに関連する利害関係者のニーズ及び期待の変化

・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の結果には、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。 [27001-9.3.3]**

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利用可能な状態にする。 [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 [27001-10]

### 4.7.1 是正処置 [27001-10.2]

#### 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。 [27001-10.2]

a) 是正処置[19]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講じる必要性を評価する。 [27001-10.2b)]

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。 [27001-10.2c)]

#### 4.7.1.4 組織は、講じた全ての是正処置の有効性をレビューする。 [27001-10.2d)]

#### 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。 [27001-10.2e)]

#### 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。 [27001-10.2]

#### 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利用可能な状態にする。 [27001-10.2f) / 10.2g)]

・不適合の性質及びそれに対して講じたあらゆる処置

・是正処置の結果

[19] 不適合を是正するための処置を是正処置といい（以下同じ。）、これまでに実施していた管理策に対して検出された不適合に対して処置をする。選択した管理策が管理目的に適していない場合や、期待通りの効果を得られていない場合に適切な処置を実施する。

## 4.8 文書化した情報の管理 [27001-7.5]

### 4.8.1 文書化の指針 [27001-7.5.1]

#### 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[20]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 [27001-7.5.2 / 7.5.3]

#### 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

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、不適切な使用又は完全性の喪失からの保護）。

---

[20] 文書化した情報の程度は、以下の理由によって、異なる場合がある。
・組織の規模、並びに活動、プロセス、製品及びサービスの種類
・プロセス及びその相互作用の複雑さ
・人々の力量

・文書化した情報の配付、アクセス[21]、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策定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、識別し、管理する。

[21] アクセスとは、文書化した情報の閲覧だけの許可に関する決定、文書化した情報の閲覧及び変更の許可及び権限に関する決定、などを意味する。

## Ⅴ．管理策基準

管理策基準に記載される管理策[Xx-X.X]は、情報セキュリティマネジメントの単位毎に、リスク対応のための方針に基づき適切に選択すべき事項である。詳細管理策[Xx-X.X.X]については、管理策を実装するために組織・環境・技術等に応じて必要とする事項を選択するものである。

### 5　組織的管理策

#### 5a　組織的管理

##### 5a-5.1　情報セキュリティのための方針群

管理策：情報セキュリティ方針及びトピック固有の方針[22]は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で、及び重大な変化が発生した場合にレビューする。

目的：　事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。

詳細管理策

5a-5.1.1　組織は、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。

（5a-5.1.1参考）　この情報セキュリティ方針は、トップマネジメントが承認し、情報セキュリティの管理に対する組織の取組を示すものである。

5a-5.1.2　情報セキュリティ方針は、次のものから導き出される要求事項を考慮に入れる。

a）事業上の戦略及び要求事項
b）規制、法令及び契約
c）現在の及び予想される情報セキュリティのリスク及び脅威

5a-5.1.3　情報セキュリティ方針には、次の事項に関する記載を含める。

a）情報セキュリティの定義
b）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み
c）情報セキュリティに関する全ての活動の指針となる原則
d）情報セキュリティに関連する適用される要求事項を満たすことへのコミットメント
e）情報セキュリティマネジメントシステムの継続的な改善へのコミットメント
f）情報セキュリティマネジメントに関する責任の、定められた役割への割当て
g）逸脱及び例外を取り扱う手順

5a-5.1.4　情報セキュリティ方針のいかなる変更もトップマネジメントが承認する。

5a-5.1.5　方針群のより低いレベルでは、情報セキュリティ方針は、情報セキュリティ管理策の実施を更に義務付けるために、必要に応じてトピック固有の方針に

[22] 組織は、これらのトピック固有の方針に、標準、指令、方針又はその他の名称を付けることがある。

よって支持する。

（5a-5.1.5参考）　トピック固有の方針は、一般に、組織内で対象とする特定のグループのニーズに対応するように、又は特定のセキュリティ領域を対象とするように構成される。

5a-5.1.6　トピック固有の方針は、組織の情報セキュリティ方針に沿い、それを補完する。

（5a-5.1.6参考）　このようなトピックの例を、次に示す。

a）アクセス制御
b）物理的及び環境的セキュリティ
c）資産管理
d）情報の転送
e）利用者エンドポイント機器のセキュリティを保った構成及び取扱い
f）ネットワークセキュリティ
g）情報セキュリティインシデント管理
h）バックアップ
i）暗号及び鍵管理
j）情報の分類及び取扱い
k）技術的ぜい弱性の管理
l）セキュリティに配慮した開発

5a-5.1.7　トピック固有の方針の作成、レビュー及び承認に関する責任は、関連する要員に、権限及び技術的力量のレベルに基づいて割り当てる。

5a-5.1.8　レビューには、次のものの変化に応じた、組織の情報セキュリティ方針及びトピック固有の方針並びに情報セキュリティの管理に関する、改善の機会の評価を含める。

a）組織の事業戦略
b）組織の技術環境
c）規制、法令及び契約
d）情報セキュリティリスク
e）現在の及び予想される情報セキュリティの脅威の環境
f）情報セキュリティ事象及びインシデントから学んだ教訓

5a-5.1.9　情報セキュリティ方針及びトピック固有の方針のレビューでは、マネジメントレビュー及び監査の結果を考慮する。

5a-5.1.10　一貫性を維持するため、一つの方針を変更する場合は、他の関連する方針のレビュー及び更新を検討する。

5a-5.1.11　情報セキュリティ方針及びトピック固有の方針は、意図する読者にとって適切で、アクセスでき、かつ、理解しやすい形で、関連する要員及び利害関係者に伝達する。

5a-5.1.12　必要な場合には、方針の受領者に、方針を理解したこと及びその順守に同意することの確認を求める。

（5a-5.1参考1）　組織は、これらの方針文書について、組織のニーズを満たす形式及び名称を

決定することが可能である。

(5a-5.1参考2)　組織によって、情報セキュリティ方針及びトピック固有の方針を単一の文書にすることがある。

(5a-5.1参考3)　組織は、トピック固有の方針に、標準、指令、方針、その他の名称を付けることがある。

5a-5.1.13　情報セキュリティ方針又はトピック固有の方針を組織外に配布する場合には、秘密情報を不適切に開示しないように注意する。

(5a-5.1.13参考)　表1に、情報セキュリティ方針とトピック固有の方針との違いを示す。

**表1－情報セキュリティ方針とトピック固有の方針との違い**

| | 情報セキュリティ方針 | トピック固有の方針 |
|---|---|---|
| **詳細さのレベル** | 一般的又は高いレベル | 固有及び詳細 |
| **文書化し、正式に承認する人** | トップマネジメント | 適切なマネジメントレベル |

## 5a-5.2　情報セキュリティの役割及び責任

管理策：情報セキュリティの役割及び責任は、組織のニーズに従って定め、割り当てる。

目的：　組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

詳細管理策

5a-5.2.1　情報セキュリティの役割及び責任の割当ては、情報セキュリティ方針及びトピック固有の方針※1に従って行う。

※1 5a-5.1参照

5a-5.2.2　組織は、次の事項に関する責任を定義し、管理する。

a) 情報及びその他の関連資産の保護

b) 特定の情報セキュリティプロセスの実施

c) 情報セキュリティのリスクマネジメント活動、特に残留リスクの受容※1

※1 例えば、リスク所有者

d) 組織の情報及びその他の関連資産を使用する全ての要員

5a-5.2.3　必要な場合には、この責任を、個別のサイト及び情報処理施設に対する、より詳細な手引で補完する。

5a-5.2.4　情報セキュリティの責任を割り当てられた個人は、情報セキュリティに関する職務を他者に委任してもよい。しかし、アカウンタビリティは依然としてその個人にあり、委任した職務がいずれも正しく実施されていることを、その個人が確認する。

5a-5.2.5　個人が責任をもつ各セキュリティ領域を定義し、文書化し、伝達する。

5a-5.2.6　承認のレベルを定義し、文書化する。

5a-5.2.7　特定の情報セキュリティの役割をもつ個人は、その役割に必要な知識及び技能において力量をもつ。

5a-5.2.8　その役割に関連し、その役割の責任を果たす上で必要な最新の動向に追随し続けるように支援される。

### 5a-5.3　職務の分離

管理策：相反する職務及び相反する責任範囲は、分離する。

目的：　情報セキュリティ管理策の不正、誤り及び回避のリスクを軽減するため。

詳細管理策

5a-5.3.1　組織は、どの職務及び責任範囲を分離する必要があるかを決定する。

（5a-5.3.1参考）　職務及び責任範囲の分離は、相反する可能性がある職務を一人の個人が自ら実行することを防ぐために、相反する職務を異なる個人に分離することを目的としている。次の事項は、分離が必要になる可能性のある活動の例である。

a）変更の提案、承認及び実行
b）アクセス権の要求、承認及び付与
c）コードの設計、実装及びレビュー
d）ソフトウェアの開発及び本番システムの管理
e）アプリケーションの使用及び管理
f）アプリケーションの使用及びデータベースの管理
g）情報セキュリティ管理策の設計、監査及び保証

5a-5.3.2　分離の管理策の設計においては、共謀のおそれを考慮する。

（5a-5.3.2参考）　小さな組織では、職務の分離を実現するのは難しい場合がある。しかし、この原則は、実施可能な限り適用することが望ましい。

5a-5.3.3　分離が困難である場合には、活動の監視、監査証跡、管理層による監督等の他の管理策を考慮する。

5a-5.3.4　役割に基づくアクセス制御システムを使用する場合に、一人の個人に対して、相反する複数の役割を許可しないことを確実にするように注意する。

5a-5.3.5　多数の役割がある場合、組織は、相反する役割を特定し、その除去を容易にするために自動化ツールの使用を考慮する。

5a-5.3.6　役割を除去又は再割当てする場合のアクセスの問題を最小限にするために、役割は慎重に定義し、付与する。

### 5a-5.4　管理層の責任

管理策：管理層は、組織の確立された情報セキュリティ方針、トピック固有の方針及び手順に従った情報セキュリティの適用を、全ての要員に要求する。

目的：　管理層が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。

詳細管理策

5a-5.4.1　管理層は、情報セキュリティ方針、トピック固有の方針、手順及び情報セキュリティ管理策に対する支援を実証する。

5a-5.4.2　管理層の責任には、要員について、次の事項を確実にすることを含む。

a）組織の情報及びその他の関連資産へのアクセスを許可する前に、情報セキュリティの役割及び責任について、要点を適切に伝える。

b) 組織内で、情報セキュリティについて要員に期待する役割を示す指針を提供する。

c) 組織の情報セキュリティ方針及びトピック固有の方針に従うことを指示する。

d) 組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成させる※1。

※1 6a-6.3参照

e)組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件、契約又は合意を順守させる。

f) 継続的な専門教育を通じて、情報セキュリティに関する適切な技能及び資格を維持させる。

g) 実行可能な場合、情報セキュリティ方針、トピック固有の方針又は情報セキュリティのための手順への違反を報告するための、匿名の報告経路を提供する※1。これによって、匿名の報告を可能にする、又は報告者のアイデンティティに関する知識をその報告を扱う必要のある人だけが知ることを確実にする備えをもつことを可能にする。

※1 例えば、内部通報

h) 組織のセキュリティ関連のプロセス及び管理策を実施するための、適切な資源及びプロジェクトを計画する時間を提供する。

### 5a-5.5 関係当局との連絡

管理策：組織は、関係当局との連絡体制を確立し、維持する。

目的： 組織と、関係する法務、規制及び監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。

詳細管理策

5a-5.5.1 組織は、いつ、誰が関係当局※1に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定する。

※1 例えば、法執行機関、規制当局、監督官庁

5a-5.5.2 関係当局との連絡は、これらの関係当局の現在及び今後の期待※1についての理解を促進するためにも用いる。

※1 例えば、適用される情報セキュリティ規制

### 5a-5.6 専門組織との連絡

管理策：組織は、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・団体との連絡体制を確立し、維持する。

目的： 情報セキュリティに関して適切な情報流通が行われることを確実にするため。

詳細管理策

5a-5.6.1 次の事項を達成する手段として、情報セキュリティに関する研究会又は会議への参加を検討する。

a) 最適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。

b) 情報セキュリティ環境の理解が最新であることを確実にする。

c) 攻撃及びぜい弱性に関する早期警戒警報、勧告及びパッチを受理する。

d) 専門家から情報セキュリティの助言を得る。

e) 新しい技術、製品、サービス、脅威又はぜい弱性に関する情報を共有し、交換する。

f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する※1。

※1 5e-5.24～5e-5.28参照

### 5a-5.7 脅威インテリジェンス

管理策：情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築する。

目的： 適切なリスク低減処置を講じることが可能となるように、組織の脅威環境についての認識をもつため。

詳細管理策

5a-5.7.1 既存の又は新たな脅威に関する情報を、次の目的で収集し、分析する。

a) 脅威が組織に危害を及ぼすことを防止するために、十分な情報に基づく活動を支援する。

b) 脅威の影響を減らす。

5a-5.7.2 脅威インテリジェンスを構成する次の3層全てを考慮する。

a) 戦略的脅威インテリジェンス：脅威の動向に関する大局的な情報の交換※1

※1 例えば、攻撃者の種類又は攻撃の種類

b) 戦術的脅威インテリジェンス：攻撃者が使う手法、ツール及び技術に関する情報の交換

c) 運用上の脅威インテリジェンス：技術的特徴を含む特定の攻撃に関する詳細

5a-5.7.3 脅威インテリジェンスは、次の事項を満たす。

a) 課題に応える（すなわち、組織の保護に関係する。）。

b) 十分な情報を含む（すなわち、脅威の状況に関する正確かつ詳細な理解を組織に提供する。）。

c) 状況認識を与えるような状況情報を含む（すなわち、事象の発生時間、場所、以前の経験及び同様の組織における傾向によって、情報に状況を加える。）。

d) 対応可能である（すなわち、組織が情報に基づいて迅速かつ効果的に対応可能である。）。

5a-5.7.4 脅威インテリジェンス活動は、次の事項を含む。

a) 脅威インテリジェンスの構築の目的を確立する。

b) 脅威インテリジェンスの構築に必要な情報を提供するのに必要かつ適切な内部及び外部の情報源を特定し、吟味し、選択する。

c) 内部及び外部のいずれかによらず、精選した情報源から情報を収集する。

d) 収集した情報を、分析に備えて処理する※1。

※1 例えば、情報を変換、形式化、又は裏付けることによる

e) 情報を、それが組織にどのように関係し、意味をもつかを理解するために分析する。

f) 関係する個人に分析した結果を理解可能な形式で伝達し、共有する。

5a-5.7.5 脅威インテリジェンスを分析し、次のとおりに使用する。

a) 脅威インテリジェンスの情報源から収集した情報を組織の情報セキュリティリスクマネジメントプロセスに含めるプロセスを実施することによって。

b) ファイアウォール、侵入検知システム、マルウェア対策ソリューションなどの技術的な予防及び検知の管理策への追加の入力として。

c) 情報セキュリティテストのプロセス及び手法への入力として。

5a-5.7.6 組織は、脅威インテリジェンス全体を改善するために、脅威インテリジェンスを他の組織と相互に共有する。

## 5a-5.8 プロジェクトマネジメントにおける情報セキュリティ

管理策：情報セキュリティをプロジェクトマネジメントに組み入れる。

目的： プロジェクトのライフサイクル全体を通して、プロジェクトマネジメントにおいて、プロジェクト及び成果物に関連する情報セキュリティリスクに効果的に対処することを確実にするため。

詳細管理策

5a-5.8.1 プロジェクトマネジメントの一部として情報セキュリティリスクに対処することを確実にするために、情報セキュリティをプロジェクトマネジメントに組み入れる。

（5a-5.8.1参考） これは、プロジェクトの複雑さ、規模、期間、分野又は適用領域にかかわらず、あらゆる種類のプロジェクトに適用可能である※1。

※1 例えば、中核事業プロセス、ICT、施設管理又はその他の支援プロセスのプロジェクト

5a-5.8.2 用いるプロジェクトマネジメントでは、次の事項を要求する。

a) 情報セキュリティリスクを、プロジェクトリスクの一部として、プロジェクトのライフサイクル全体を通じて、早い段階で及び定期的にリスクアセスメント及びリスク対応を実施する。

b) 情報セキュリティ要求事項※1には、プロジェクトの早い段階で対処する。

※1 例えば、アプリケーションセキュリティの要求事項（8d-8.26）、知的財産権を順守するための要求事項（5g-5.32）など

c) 内部及び外部への伝達の側面のセキュリティなど、プロジェクトの実行に伴う情報セキュリティリスクを、プロジェクトのライフサイクル全体を通じて考慮し、処理する。

d) 情報セキュリティリスク対応の進捗状況をレビューし、対応の有効性を評価及び試験する。

5a-5.8.3 情報セキュリティの考慮及び活動の適切性は、あらかじめ定めた段階において、適切な人物又はプロジェクト運営委員会などのガバナンス機関がフォローアップする。

5a-5.8.4 プロジェクトに関連する情報セキュリティの責任及び権限を定義し、規定された役割に割り当てる。

5a-5.8.5 プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の方針及び規制から順守すべき要求事項を導出することを含む、様々な方法を用いて決定する。

5a-5.8.6 プロジェクトが提供する製品又はサービスの情報セキュリティ要求事項は、脅威のモデリング、インシデントのレビュー、ぜい弱性の深刻度の使用、緊急時対応計画策定などの活動から導き出すことができ、それによって、情報システムのアーキテクチャ及び設計を運用環境における既知の脅威から保護することを確実にする。

5a-5.8.7 情報セキュリティ要求事項は、ICT開発プロジェクトだけでなく、全ての種類のプロジェクトについて決定する。これらの要求事項を決定する際には、次の事項も考慮する。

a) どのような情報が関係するか（情報の決定）、それに対応する情報セキュリティのニーズは何か※1、及び適切なセキュリティの欠如から生じる可能性のある事業への潜在的な悪影響

※1 分類。5b-5.12参照

b) 特に機密性、完全性及び可用性の観点から、関係する情報及びその他の関連資産に必要な保護のニーズ

c) 認証の要求事項を導き出すための、エンティティが提示する識別情報に求める信頼又は保証のレベル

d) 顧客及びその他の潜在的な業務上の利用者のほか、関係するプロジェクトメンバ、潜在的な運用スタッフ、外部供給者などの特権をもつ、又は技術をもつ利用者に対する、アクセスの提供及び認可のプロセス

e) 利用者に対する、各自の義務及び責任の通知

f) トランザクションのログ取得及び監視、並びに否認防止の要求事項のような、業務プロセスに由来する要求事項

g) 他の情報セキュリティ管理策によって必要になる要求事項※1

※1 例えば、ログ取得及び監視のインタフェース、情報漏えい検知システム

h) 組織の活動に適用される法令、規制及び契約上の条件の順守

i) 第三者との合意又は契約における関連セキュリティ箇条を含む、組織の情報セキュリティ方針及びトピック固有の方針を満たす上で必要な、第三者に求める信頼又は保証のレベル

## 5b 資産管理

### 5b-5.9 情報及びその他の関連資産の目録

管理策：情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。

目的：　組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。

詳細管理策

**【目録】**

5b-5.9.1　組織は、情報及びその他の関連資産を特定し、情報セキュリティの観点からそれらの重要度を決定する。

5b-5.9.2　文書は、必要に応じて専用の目録又は既存の目録として維持する。

5b-5.9.3　情報及びその他の関連資産は、正確で、最新に保たれ、一貫性があり、他の目録と整合している。情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。

a）資産目録に照らして、特定した情報及びその他の関連資産の定期的なレビューを実施する。

b）資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。

5b-5.9.4　資産の場所を、必要に応じて目録に含める。

（5b-5.9参考）　目録は、情報及びその他の関連資産の単一のリストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考えると、情報資産、ハードウェア、ソフトウェア、仮想マシン（VM）、施設、要員、力量、機能及び記録に関する目録などの、動的な目録の集まりとみることが可能である。

5b-5.9.5　各資産は、それに関係する情報の分類に従って分類する※1。

※1 5b-5.12参照

5b-5.9.6　情報及びその他の関連資産の目録の粒度は、組織のニーズに適したレベルである。

（5b-5.9.6参考）　資産の性質上、情報のライフサイクルにおいて資産の特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクルが短いVMインスタンスがある。

**【管理責任】**

5b-5.9.7　特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当て、その上で分類を特定する※1。

※1 5b-5.12及び5b-5.13参照

5b-5.9.8　資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスを実施する。

5b-5.9.9　資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。

5b-5.9.10　現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てする。

**【管理責任者の義務】**

5b-5.9.11　資産の管理責任者は、次の事項を確実にして、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。

a) 情報及びその他の関連資産の目録を作成する。

b) 情報及びその他の関連資産を適切に分類し、保護する。

c) 分類を定期的にレビューする。

d) データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、技術資産の構成要素を一覧表示し、ひも（紐）付ける。

e) 情報及びその他の関連資産の許容される利用に関する要求事項※1を確立する。

※1 5b-5.10参照

f) アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。

g) 情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。

h) 資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。

i) 資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。

### 5b-5.10 情報及びその他の関連資産の許容される利用

管理策：情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。

目的： 情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。

詳細管理策

5b-5.10.1 組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。

5b-5.10.2 要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。

5b-5.10.3 組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。

5b-5.10.4 許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法について、明確に指示をする。

5b-5.10.5 トピック固有の方針には、次の事項を記載する。

a) 情報セキュリティの観点から見た、個人に期待する行動及び許容できない行動

b) 情報及びその他の関連資産について許可する利用及び禁止する利用

c) 組織が実行している監視活動

5b-5.10.6 許容される利用の手順は、情報の分類※1及び特定したリスクに従って、情報のライフサイクル全体にわたって立案する。

※1 5b-5.12参照

5b-5.10.7　許容される利用の手順の立案においては、次の項目を考慮する。

a) 分類のレベルに応じた保護の要求事項に対応するアクセス制限

b) 情報及びその他の関連資産の認可された利用者についての、記録の維持

c) 情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護

d) 情報に関連する資産の、製造業者の仕様に従った保管※1

※1 7b-7.8参照

e) 記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示※1

※1 7b-7.10参照

f) 情報及びその他の関連資産の破棄、並びにサポートされている削除方法の認可※1

※1 8b-8.10参照

## 5b-5.11　資産の返却

管理策：要員及び必要に応じてその他の利害関係者は、雇用、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却する。

目的：　雇用、契約、又は合意を変更又は終了するプロセスの一環として、組織の資産を保護するため。

詳細管理策

5b-5.11.1　雇用の変更及び終了時のプロセスは、前もって支給された物理的及び電子的な資産（組織が所有するもの又は組織に預託されたもの）の全ての返却を含めて制定する。

5b-5.11.2　要員及びその他の利害関係者が組織の装置・機器を購入する場合、又は個人所有の機器を用いる場合には、手順に従って、全ての関連する情報を追跡し、組織に返却し、装置・機器からセキュリティを保って削除することを確実にする※1。

※1 7b-7.14参照

5b-5.11.3　要員及びその他の利害関係者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。

5b-5.11.4　雇用の終了の予告期間中及びそれ以降、組織は、予告を受けた要員が認可を得ずに関連情報※1を複製することを防止する。

※1 例えば、知的財産

5b-5.11.5　組織は、返却する全ての情報及びその他の関連資産を明確に特定し、文書化する。

（5b-5.11.5参考）　これには、次のものが含まれ得る。

a) 利用者エンドポイント機器

b) 可搬記憶装置

c) 専門機器

d) 情報システム、サイト及び物理的アーカイブ用の認証ハードウェア※1

※1 例えば、機械式鍵、物理トークン及びスマートカード

e) 情報の物理的な複製

## 5b-5.12　情報の分類

管理策：情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って分類する。

目的：　組織における情報の重要度に従って、情報の保護のニーズを特定し、理解することを確実にするため。

詳細管理策

| | |
|---|---|
| 5b-5.12.1 | 組織は、情報の分類に関するトピック固有の方針を確立し、それを全ての関連する利害関係者に伝達する。 |
| 5b-5.12.2 | 組織は、分類体系において、機密性、完全性及び可用性の要求事項を考慮する。 |
| 5b-5.12.3 | 情報の分類及び関連する保護管理策では、情報を共有又は制限するため、情報の完全性を保護するため、及び可用性を保証するための事業上のニーズ、並びに情報の機密性、完全性及び可用性に関する法的要求事項を考慮する。 |
| （5b-5.12参考） | 情報以外の資産も、その資産に保管する情報、その資産で処理する情報、又は他の形で取り扱う若しくは保護する情報の分類に合わせて分類することが可能である。 |
| 5b-5.12.4 | 情報の管理責任者は、その情報の分類に対してアカウンタビリティを負う。 |
| 5b-5.12.5 | 分類体系には、分類の規則及びその分類を後にレビューするための基準を含める。 |
| 5b-5.12.6 | 分類の結果は、ライフサイクルを通じた情報の価値、取扱いに慎重を要する度合い、及び重要度の変化に従って更新する。 |
| 5b-5.12.7 | 分類体系は、アクセス制御に関するトピック固有の方針※1と整合していて、組織のそれぞれの事業上のニーズに対応できる。<br>※1 5a-5.1参照 |
| 5b-5.12.8 | 分類は、情報の侵害が組織に与える影響のレベルによって決定することが可能である。分類体系で定義したそれぞれのレベルには、分類体系の適用において意味をもつ名称を付ける。 |
| 5b-5.12.9 | 分類体系は、全員が情報及び該当するその他の関連資産を同じ方法で分類できるよう、組織全体にわたって一貫し、組織の手順に含まれている。 |
| （5b-5.12.9参考） | これによって、全員が保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようになる。 |
| 5b-5.12.10 | 情報共有を含む他の組織との合意は、他の組織から共有された情報の分類を特定し、分類レベルを解釈するための手順を含む。 |
| （5b-5.12.10参考） | 組織内で使用する分類体系は、レベルの名称が類似している場合でも、他の組織で使用する体系と異なる可能性がある。さらに、組織間で移動する情報は、分類体系が同じであっても、各組織の状況に依存して分類が異なる場合がある。異なる体系間の対応は、情報について同等の取扱い及び保護方法を探すことによって決定することが可能である。 |

### 5b-5.13　情報のラベル付け

管理策：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。

目的：　情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。

詳細管理策

5b-5.13.1　情報のラベル付けに関する手順は、あらゆる形式の情報及びその他の関連資産に適用できるものである。

5b-5.13.2　情報のラベル付けは、5.12で確立した分類体系を反映している。

5b-5.13.3　情報のラベルは、容易に認識できる。

5b-5.13.4　情報のラベル付けに関する手順では、記憶媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。

(5b-5.13参考1)　手順では、次の事項を定めることも可能である。

a) ラベル付けを省略する場合※1

※1 例えば、作業負荷を減らすための、秘密でない情報のラベル付け

b) 電子的若しくは物理的手段、又はその他の形式で送信又は保存される情報のラベル付けの方法

c) ラベル付けが不可能な場合※1の取扱いの方法

※1 例えば、技術的制約のため

(5b-5.13参考2)　ラベル付け手法の例は次のものを含む。

a) 物理的ラベル

b) ヘッダ及びフッタ

c) メタデータ

d) 透かし

e) ゴムスタンプ

5b-5.13.5　ディジタル情報は、特に機密性に関して、情報を特定し、管理し、制御するために、メタデータを活用する。

5b-5.13.6　メタデータは、情報の効率的かつ正確な検索を可能にする。

5b-5.13.7　メタデータは、付加した分類ラベルに基づいて、複数のシステムが連携し、決定を下すことを容易にする。

5b-5.13.8　手順には、組織の情報モデル及びICTアーキテクチャに沿って、情報にメタデータをどのように付けるか、どのラベルを使用するか、及びデータをどのように取り扱うことが望ましいかを記載する。

5b-5.13.9　システムが情報をその情報セキュリティ特性に応じて処理するときに、関係する追加のメタデータをシステムで付加する。

5b-5.13.10　要員及びその他の利害関係者に、ラベル付けに関する手順を認識させる。

5b-5.13.11　情報に正しくラベルを付け、それに応じて取り扱うことを確実にするために、全ての要員に必要な訓練を提供する。

5b-5.13.12　取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付ける。

## 5b-5.14　情報の転送

管理策：情報の転送の規則、手順又は合意を、組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備える。

目的：　組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。

詳細管理策

**【情報の転送全般】**

5b-5.14.1　組織は、情報の転送に関するトピック固有の方針を確立し、それを関連する全ての関係者に伝達する。

5b-5.14.2　転送中の情報を保護するための規則、手順及び合意は、関連する情報の分類を反映する。

5b-5.14.3　組織と第三者との間で情報を転送する場合、転送中の全ての形式の情報を保護するために、転送の合意（受信者の認証を含む。）を確立し、維持する※1。

※1 5b-5.10参照

（5b-5.14.3参考）　情報の転送は、電子的転送、物理的記憶媒体の輸送及び口頭での伝達によって行われる場合がある。

5b-5.14.4　全ての種類の情報の転送について、規則、手順及び合意には、次の事項を含める。

a) 転送する情報を、盗聴、認可されていないアクセス、複製、改ざん、誤った経路での通信、破壊及びサービス拒否から保護するために設計された管理策。これは、情報の分類に合ったそれぞれのレベルのアクセス制御、及び暗号技術の利用※1など取扱いに慎重を要する情報を保護するために必要な管理策を含む。

※1 8c-8.24参照

b) 転送中の情報の受渡記録を維持することを含む、追跡可能性及び否認防止を確実にするための管理策

c) 該当する場合には、情報の管理責任者、リスク所有者、セキュリティ担当者及び情報管理者など、転送に関連する適切な連絡先の特定

d) 物理的記憶媒体の紛失又はデータの消失などの情報セキュリティインシデントが発生した場合の責任及び賠償義務

e) 取扱いに慎重を要する又は重要な情報に対する、合意したラベル付けシステム（ラベルの意味を直ちに理解できること、及び情報を適切に保護することを確実にするもの）の使用※1

※1 5b-5.13参照

f) 転送サービスの信頼性及び可用性

g) 情報転送手段の許容される利用に関するトピック固有の方針又は指針※1

※1 5b-5.10参照

h) メッセージを含む全ての業務記録の保持及び破棄[23]の指針

i) 情報の転送に関連するその他の関連する法令、規制及び契約上の要求事項※1の考慮※2

[23] 業務記録の保持及び破棄に関しては、地域の法令及び規制が存在する場合がある。

※1 5g-5.31、5g-5.32、5g-5.33、5g-5.34参照
※2 例えば、電子署名の要求事項

**【電子的転送】**

5b-5.14.5 情報の転送に電子通信手段を使用する場合、規則、手順及び合意では、次の項目も考慮する。

a) 電子通信の利用を通じて伝送される可能性のあるマルウェアの検知及びそれに対する保護※1
※1 8b-8.7参照

b) 添付して通信する、取扱いに慎重を要する電子情報の保護

c) 通信において文書及びメッセージを誤った宛先又は番号に送信することの防止

d) 誰でも使える外部サービス※1を利用する際の、事前承認の取得
※1 例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有又はクラウドストレージ

e) 公開されているアクセス可能なネットワークを通じて情報を転送するときの、より強固な認証レベル

f) 電子通信手段に関連する制限※1
※1 例えば、外部のメールアドレスへの電子メールの自動転送の防止

g) ショートメッセージサービス（SMS）又はインスタントメッセージで重要な情報を送信しないように要員及びその他の利害関係者に助言する。これは、これらが公共の場所で（したがって、認可されていない人に）読まれたり、又は適切に保護されていない装置・機器に保存されたりする可能性があるためである。

h) ファクシミリ又はそのサービスの利用に伴う、次の問題に関わる要員及びその他の利害関係者への助言

1) 組み込まれている記憶装置から受信文を取り出す、認可されていないアクセス

2) 特定の番号にメッセージを送る故意又は偶然のプログラミング

**【物理的記憶媒体の輸送】**

5b-5.14.6 物理的記憶媒体（紙を含む。）を輸送する場合、規則、手順及び合意には、次の事項も含める。

a) 輸送、受渡し及び受領を管理し、通知する責任

b) 伝票の正しい送付先及び送付を確実にすること

c) 輸送中に発生する可能性が高い物理的損傷から、製造業者の仕様に従って内容物を保護するこん（梱）包。例えば、熱、湿気又は電磁界への露出など、記録媒体の再生を妨げる可能性のある環境要因からの保護。こん（梱）包及び送付のための最小限の技術標準の使用※1。
※1 例えば、不透明な封筒の使用

d) 管理層が合意した、認可された信頼できる運送業者のリスト

e) 運送業者を確認する規準

f) 輸送する記憶媒体内の情報の分類レベルに応じて、開封を明らかにする又は開封を防止する管理策※1の使用

※1 例えば、バッグ、コンテナ

g) 運送業者の識別情報を検証する手順

h) 情報の分類に応じた、輸送又は運送業者のサービスを提供する第三者の承認された一覧

i) 記憶媒体の内容及び適用した保護方法を特定するためのログを保持し、認可された受領者のリスト、輸送の責任窓口への発送時刻、及び宛先での受領時刻を記録すること

**【口頭での伝達】**

5b-5.14.7 情報の口頭での伝達を保護するために、要員及びその他の利害関係者に対して、次の事項を行うことが望ましいことを留意させる。

a) 公共の場所又は安全でない通信チャネルを通じた口頭での秘密会話は、認可されていない者に聞かれる可能性があるので行わない。

b) 秘密情報を含んだメッセージを留守番電話又は音声メッセージに残さない。留守番電話又は音声メッセージに残したメッセージは、認可されていない者が再生する可能性、共有システムに保管される可能性、又は誤ダイアルの結果、間違って保管される可能性があるからである。

c) 会話を聞く際は、適切なレベルで音を遮断する。

d) 適切な部屋の管理策が実施されることを確実にする※1。

※1 例えば、防音、ドアを閉める。

e) 取扱いに慎重を要する会話においては、始めに注意事項を説明し、出席者に、これから伝える情報の分類レベル及び取扱いの要求事項を知らせる。

## 5c アクセス権管理

### 5c-5.15 アクセス制御

管理策：情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、事業上及び情報セキュリティの要求事項に基づいて確立し、実施する。

目的： 情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。

詳細管理策

5c-5.15.1 情報及びその他の関連資産の管理責任者は、アクセス制御に関連する情報セキュリティ及び事業上の要求事項を決定する。

5c-5.15.2 情報セキュリティ及び事業上の要求事項を考慮したアクセス制御に関するトピック固有の方針を定め、関連する全ての利害関係者に伝達する。

5c-5.15.3 情報セキュリティ、事業上の要求事項及びトピック固有の方針では、次の事項を考慮に入れる。

a) どのエンティティが、情報及びその他の関連資産にどの種類のアクセスを必要とするかの決定

b) アプリケーションセキュリティ※1

※1 8d-8.26参照

c) 物理的アクセス。これは適切な物理的入退管理策※1によって支援する必要がある。

※1 7a-7.2、7a-7.3 及び7a-7.4参照

d) 情報の配布及び認可※1、並びに情報のセキュリティ水準及び情報の分類※2

※1 例えば、知る必要性の原則

※2 5b-5.10、5b-5.12 及び5b-5.13参照

e) 特権的アクセスの制限※1

※1 8a-8.2参照

f) 職務の分離※1

※1 5a-5.3参照

g) データ又はサービスへのアクセスの制限に関連する法令、規制及び契約上の義務※1

※1 5g-5.31、5g-5.32、5g-5.33、5g-5.34 及び8a-8.3参照

h) アクセス制御機能の分離※1

※1 例えば、アクセス要求、アクセス認可、アクセス管理

i) アクセス要求の正式な認可※1

※1 5c-5.16 及び5c-5.18参照

j) アクセス権の管理※1

※1 5c-5.18参照

k) ログ取得※1

※1 8b-8.15参照

5c-5.15.4 アクセス制御規則は、関連するエンティティに対して、適切なアクセス権及び制限を定義し、対応付けすることによって実施する※1。

※1 5c-5.16参照

（5c-5.15.4参考） エンティティは、人間の利用者だけでなく、技術的又は論理的なアイテム※1の場合もある。アクセス制御の管理を簡潔にするために、役割をエンティティのグループに割り当てることが可能である。

※1 例えば、機械、装置・機器又はサービス

5c-5.15.5 アクセス制御規則を定義し、実施するときは、次の事項を考慮に入れる。

a) アクセス権と情報分類との整合性

b) アクセス権と物理的境界のセキュリティのニーズ及び要求事項との整合性

c) エンティティに、使用が認められているネットワーク及びネットワークサービスを含む、情報及びその他の関連資産へのアクセスだけを提供するために、分散環境で利用可能な全ての種類の接続を考慮すること

d) 動的アクセス制御に関連する要素又は要因をどのように反映できるかを検討すること

### 5c-5.16 識別情報の管理

管理策：識別情報のライフサイクル全体を管理する。

目的： 組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。

詳細管理策

5c-5.16.1 識別情報の管理におけるプロセスは、次の事項を確実にする。

a) 個人に割り当てられる識別情報の場合、特定の識別情報を使って実行した処理に関してその個人にアカウンタビリティを負わせることができるように、一つの識別情報は一人の個人にだけひも（紐）付ける。

b) 複数の人に割り当てられる識別情報※1は、業務上又は運用上の理由で必要であり、そのための承認及び文書化をする場合にだけ許可する。

※1 例えば、共有の識別情報

c) 人間以外のエンティティに割り当てられる識別情報は、適切に権限を分離した承認及び独立した継続的な監視の対象とする。

d) 識別情報が不要になった場合※1、識別情報を時機を失せずに無効化又は削除する。

※1 例えば、関連するエンティティが削除された若しくは使用されなくなった場合、又は識別情報にひも（紐）付けされた人が組織を去った若しくは役割を変えた場合

e) 特定の領域では、一つだけの識別情報を一つのエンティティに対応付ける※1。

※1 すなわち、同じ環境下で一つのエンティティに複数の識別情報を対応付けること（複数識別情報）は避ける。

f) 利用者識別情報及び認証情報の使用及び管理に関する全ての重要な事象の記録を保持する。

5c-5.16.2 組織は、利用者識別情報に関連する情報の変更を取り扱う支援プロセスをもつ。

（5c-5.16.2参考） このプロセスは、個人に関連する信頼する文書の再検証を含む場合がある。

5c-5.16.3 第三者が提供し又は発行した識別情報※1を使用する場合、組織は、必要な信頼レベルが第三者の識別情報にあり、関連するリスクを知り、十分に対応する。

※1 例えば、ソーシャルメディアのクレデンシャル

（5c-5.16.3参考） この対応には、第三者に関連する管理策※1、及び認証情報に関連する管理策※2を含む場合がある。

※1 5d-5.19参照
※2 5c-5.17参照

## 5c-5.17 認証情報

管理策：認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。

目的： 適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。

詳細管理策

**【認証情報の割当て】**

5c-5.17.1 認証情報の割当て及び管理のプロセスは、次の事項を確実にする。

a) 仮の秘密認証情報として登録プロセス中に自動的に生成される個人パスワード又は個人識別番号（PIN）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。

b) 新規、更新又は仮の認証情報を発行する前に、利用者の本人確認の手順を確立する。

c) 仮の認証情報を含む認証情報は、セキュリティを保った方法※1で利用者に渡し、保護されていない（平文の）電子メールのメッセージをこの目的で利用することは避ける。

※1 例えば、信頼できる保護された経路を通じて

d) 利用者は、認証情報の受領を知らせる。

e) 業者があらかじめ定めた又は提供した初期設定の認証情報は、システム又はソフトウェアのインストール直後に変更する。

f) 認証情報の割当て及び管理に関する重要な事象の記録を保持し、記録に機密性を付与する。記録保持方法は、承認を受ける※1。

※1 例えば、承認されたパスワード管理ツール（password vault tool）を使用

**【利用者の責任】**

5c-5.17.2 認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。

a) パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された人とだけ共有する。

b) 影響を受けた又は侵害された認証情報は、侵害の知らせ又はその他の兆候があれば、直ちに変更する。

c) パスワードを認証情報として使用する場合、例えば、次のような最適な慣行の推奨事項に従った強力なパスワードを選択する。

1) パスワードは、当人に関する情報※1から、他の者が容易に推測できる又は得られる事項に基づかない。

※1 例えば、名前、電話番号、誕生日

2) パスワードは辞書の単語又はそれらの組合せに基づかない。

3) 覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。

4) パスワードに最小限必要とする長さを定める。

d) 異なるサービス及びシステム間で同じパスワードを使用しない。

e) a)～d)の規則に従う義務が、雇用条件にも含まれている※1。

※1 6a-6.2 参照

**【パスワード管理システム】**

5c-5.17.3 パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。

a) 利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。

b) 優良な慣行の推奨事項※1に従って強固なパスワードを使用させる。

※1 “利用者の責任”のc)参照

c) パスワードは、最初のログイン時に利用者に変更させる。

d) 必要に応じて、例えば、セキュリティインシデントの後に、又は有効な識別情報※1のパスワードを知っている利用者の雇用の終了若しくは変更の時に、パスワードを変更させる。

※1 例えば、共有識別情報

e) 以前のパスワードの再利用を防止する。

f) 一般的に使われるパスワード、並びにハッキングされたシステムで侵害

された利用者名及びパスワードの組合せの使用を防止する。

g) パスワードは、入力時に、画面上に表示しない。

h) パスワードは、保護した形態で保存し、伝達する。

5c-5.17.4　パスワードの暗号化及びハッシュ化は、パスワードに関する承認された暗号技術に従って実行する※1。

※1 8c-8.24参照

## 5c-5.18　アクセス権

管理策：情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。

目的：　情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。

詳細管理策

**【アクセス権の提供及び無効化】**

5c-5.18.1　エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。

a) 情報及びその他の関連資産の利用についての、その情報及びその他の関連資産の管理責任者からの認可の取得※1,※2

※1 5b-5.9参照

※2 アクセス権について、管理層による承認も受けることが適切な場合もある。

b) 事業上の要求事項及び組織のアクセス制御に関するトピック固有の方針並びに規則の考慮

c) アクセス権の承認及び実施の役割の分離、並びに相反する役割の分離を含む、職務の分離の考慮

d) ある者が情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織を去った利用者のアクセス権を時機を失せずに削除する。

e) 臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の日に取り消すことの考慮

f) 許可したアクセスのレベルが、アクセス制御に関するトピック固有の方針に適していること※1、及び職務の分離※2などのその他の情報セキュリティ要求事項と整合していることの検証

※1 5c-5.15参照

※2 5a-5.3参照

g) 認可手順が問題なく完了した後にだけ、アクセス権を有効にする※1

※1 例えば、サービス提供者がアクセス権を有効にする

h) 情報及びその他の関連資産にアクセスするために利用者識別子（ID、論理的又は物理的）に与えられたアクセス権の、一元的な記録の維持

i) 役割又は職務を変更した利用者のアクセス権の変更

j) 物理的及び論理的アクセス権の削除又は調整※1

※1 鍵、認証情報、識別カード又は利用資格の削除、無効化又は交換によって行うことが可能である。

k）利用者の論理的及び物理的アクセス権の変更の記録の維持

**【アクセス権のレビュー】**

5c-5.18.2　物理的及び論理的なアクセス権の定期的なレビューでは、次の事項を考慮する。

a）同じ組織内での何らかの変更後※1又は退職後の利用者のアクセス権※2

※1 例えば、異動、昇進、降格

※2 6a-6.1～6a-6.5参照

b）特権的アクセス権の認可

**【雇用の変更又は終了前の考慮事項】**

5c-5.18.3　情報及びその他の関連資産への利用者のアクセス権は、雇用の変更又は終了の前に、次に示すリスク因子の評価に基づいて、レビューし、調整又は削除する。

a）雇用の終了又は変更が、利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由

b）利用者の現時点の責任

c）現在アクセス可能な資産の価値

## 5d　供給者管理

### 5d-5.19　供給者関係における情報セキュリティ

管理策：供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め、実施する。

目的：　供給者関係において合意したレベルの情報セキュリティを維持するため。

詳細管理策

5d-5.19.1　組織は、供給者関係に関するトピック固有の方針を確立し、関連する全ての利害関係者に伝達する。

5d-5.19.2　組織は、供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順を特定し、実施する。

5d-5.19.3　供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順は、組織によるクラウドサービスプロバイダの資源の利用にも適用する。

5d-5.19.4　供給者が提供する製品及びサービスの利用に関連するセキュリティリスクに対処するためのプロセス及び手順は、組織が実施するもの、並びに供給者の製品若しくはサービスの利用の開始又は供給者の製品及びサービスの利用の終了に関して供給者が実施することを組織が要求するものを含む。

（5d-5.19.4参考）　プロセス及び手順に含まれる内容の例として、次がある。

a）組織の情報の機密性、完全性及び可用性に影響を与える可能性のある供給者の種類※1の特定及び文書化

※1 例えば、ICTサービス、物流、公益事業、金融サービス、ICT基盤の構成要素

b）情報、製品及びサービスの取扱いに慎重を要する度合いに従って供給者を評価及び選択する方法の確立※1

※1例えば、市場分析、顧客への照会、文書のレビュー、オンサイト評価、取得している認証を用いて

c) 適切な情報セキュリティ管理策を備えた供給者の製品又はサービスの評価及び選択、並びにそれらのレビュー。特に、供給者が実施する管理策の正確性及び完全性、それによって供給者の情報及び情報処理の完全性を確実にし、ひいては組織の情報セキュリティを確実にすること。

d) 供給者がアクセス、監視、管理又は使用する可能性のある組織の情報、ICTサービス及び物理的インフラストラクチャの定義

e) 組織の情報の機密性、完全性及び可用性に影響を与える可能性のある、供給者が提供するICT基盤の構成要素及びサービスの種類の定義

f) 次の事項に関連する情報セキュリティリスクの評価及び管理

1) 潜在的な悪意のある供給者の要員に起因するリスクを含む、組織の情報及びその他の関連資産の供給者による使用

2) 供給者が提供する製品（これらの製品で使用されるソフトウェア構成要素及びサブ構成要素を含む。）又はサービスの誤動作又はぜい弱性

g) 第三者のレビュー及び製品の妥当性確認を含む、供給者の種類ごと及びアクセスの種類ごとに確立した情報セキュリティ要求事項の順守の監視

h) 供給者の不順守の低減。これは監視を通じて検知されたか、又は他の手段によって検知されたかによらない。

i) 供給者の製品及びサービスに関連するインシデント及び不測の事態への対処。これには、組織及び供給者の両方の責任を含める。

j) 供給者の情報及び情報処理の可用性、並びにそれによって組織の情報の可用性を確実にするための、レジリエンスに関する対策、並びに必要な場合には、回復及び不測の事態に関する対策

k) 供給者の要員とやり取りする組織の要員を対象とした、職務に関する適切な規則、トピック固有の方針、プロセス、手順及び行動についての、供給者の種類並びに供給者による組織のシステム及び情報へのアクセスのレベルに基づく、意識向上及び訓練

l) 情報、その他の関連資産及び移動が必要なその他のものの転送の管理、並びにその転送期間全体にわたって情報セキュリティの維持を確実にすること

m) 次の事項を含む供給者関係のセキュリティに配慮した終了を確実にするための要求事項

1) アクセス権の回収

2) 情報の取扱い

3) 契約中に開発された知的財産の帰属の決定

4) 供給者又は内部委託の変更における情報の移行性

5) 記録管理

6) 資産の返却

7）情報及びその他の関連資産のセキュリティに配慮した処分

8）機密保持の要求の継続

n）供給者の要員及び設備に期待する要員セキュリティ及び物理的セキュリティのレベル

5d-5.19.5　代替の製品又はサービスの手配の遅延を回避するため、供給者がその製品又はサービスを提供できなくなった場合※1に情報処理を継続するための手順※2を検討する。

※1 例えば、インシデントのため、供給者が事業を行わなくなったため、又は技術の進歩によって一部の構成要素を供給しなくなったため。

※2 例えば、事前に代替の供給者を特定しておく、又は常に代替の供給者も利用する。

## 5d-5.20　供給者との合意における情報セキュリティの取扱い

管理策：供給者関係の種類に応じて、関連する情報セキュリティ要求事項を確立し、各供給者と合意する。

目的：　供給者関係において合意したレベルの情報セキュリティを維持するため。

詳細管理策

5d-5.20.1　関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し、組織と供給者との間に明確な理解が得られることを確実にするために、供給者との合意を確立し、これを文書化する。

(5d-5.20.1参考)　特定された情報セキュリティ要求事項を満たすために、合意には、次の事項を含めることを考慮することが可能である。

a）提供し又はアクセスされる情報の記載、及び提供方法又はアクセス方法の記載

b）組織の分類体系に従った情報の分類※1

※1 5b-5.10、5b-5.12 及び5b-5.13参照

c）組織の分類体系と供給者の分類体系との間の対応付け

d）法令、規制及び契約上の要求事項※1、並びにこれらの要求事項を満たすことを確実にする方法についての記載

※1 データ保護、個人識別可能情報（PII）の取扱い、知的財産権及び著作権に関する要求事項を含む。

e）契約の各当事者に対する、合意した一連の管理策※1の実施の義務、及び供給者に対する、組織の情報セキュリティ要求事項の順守の義務

※1 アクセス制御、パフォーマンスのレビュー、監視、報告及び監査を含む。

f）情報及びその他の関連資産の許容される利用に関する規則。必要な場合、許容されない利用についての規則も含める。

g）供給者の要員による組織の情報及びその他の関連資産の使用を認可する場合及びその認可を解除する場合の手順又は条件※1

※1 例えば、組織の情報及びその他の関連資産を使用することが認可されている供給者の要員を明示するリスト

h）供給者のICT基盤に関する情報セキュリティ要求事項。特に、組織の事業上のニーズ及びリスク基準に基づき、個々の供給者との合意の基礎とな

る、情報の種類及びアクセスの種類それぞれについての最小限の情報セキュリティ要求事項

i) 請負業者が要求事項を満たさなかった場合の補償及び是正

j) インシデント管理の要求事項及び手順（特に、インシデントからの回復中の通知及び協力）

k) 特定の手順及び情報セキュリティ要求事項についての訓練及び意識向上に関する要求事項※1

※1 例えば、インシデント対応手順、認可手順

l) 下請負供給者の使用に関する合意など、実施する必要のある管理策を含む、下請負契約に関する該当する規定※1

※1 例えば、下請負供給者に対して供給者と同じ義務を負わせることの要求、下請負供給者のリストをもつこと及び変更前の通知の要求

m) 情報セキュリティに関する連絡先担当者も含む、関連する連絡先

n) 法的に許容される場合、供給者の要員の選考に関する要求事項。この要求事項には、選考を実施する責任、及び選考が完了しなかった場合又は選考の結果、疑い若しくは懸念が生じた場合に行う通知の手順も含める。

o) 供給者のプロセスに関連する情報セキュリティ要求事項についての第三者立証の証拠及び保証の仕組み、並びに管理策の有効性に関する独立した報告書

p) 合意に関わる、供給者のプロセス及び管理策を監査する権利

q) 管理策の有効性について、報告書を定期的に提出する供給者の義務、及び報告書で提起された問題を適時に修正することに関する合意

r) 合意上の問題点の解決及び紛争解決のプロセス

s) 組織のニーズに合わせたバックアップの提供（頻度及び種類並びに保管場所の点で）

t) 主要設備と同じ脅威にはさらされない代替設備（すなわち、災害回復サイト）の可用性を確実にすること、及び主要管理策が失敗した場合のフォールバック管理策（代替管理策）の考慮

u) 組織への事前通知を確実にする変更管理プロセスをもつこと、及び組織が変更を受け入れない可能性

v) 情報の分類に合った物理的セキュリティ管理策

w) 物理的輸送又は論理的送信中に情報を保護するための情報の転送の管理策

x) 記録管理、資産の返却、情報及びその他の関連資産のセキュリティに配慮した処分、並びに継続的な機密保持義務を含む、合意締結時に定める終了条項

y) 供給者が保存している組織の情報を、不要になり次第、セキュリティに配慮して破壊する方法の規定

z) 契約の終了時に、別の供給者又は組織自らへの引継ぎの支援を確実にすること

5d-5.20.2　組織は、自らの情報がどこへ渡っているかを追跡するために、外部関係者との合意※1の登録簿を作成し、維持する。

※1 例えば、契約、覚書、情報共有契約

5d-5.20.3 組織はまた、外部関係者との合意を定期的にレビューし、妥当性を確認し、更新して、それらが依然として必要であり、関連する情報セキュリティ条項によって目的に適合することを確実にする。

## 5d-5.21 ICTサプライチェーンにおける情報セキュリティの管理

管理策：ICT製品及びサービス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を管理するためのプロセス及び手順を定め、実施する。

目的： 供給者関係において合意したレベルの情報セキュリティを維持するため。

詳細管理策

5d-5.21.1 供給者関係に関する一般的な情報セキュリティ要求事項に加えて、ICTサプライチェーンセキュリティにおける情報セキュリティに対処するために、次の事項を考慮する。

a) ICT製品又はサービスの取得に適用する情報セキュリティ要求事項を定める。

b) 供給者が組織に提供するICTサービスの一部を下請負契約に出す場合には、そのサプライチェーン全体に組織のセキュリティ要求事項を伝達するようICTサービスの供給者に要求する。

c) ICT製品に関して、その製品に他の供給者又は他のエンティティ※1から購入又は取得した構成要素が含まれる場合には、そのサプライチェーン全体に適切なセキュリティ慣行を伝達するようICT製品の供給者に要求する。

※1 例えば、下請負ソフトウェア開発者、ハードウェア構成要素供給者

d) ICT製品の供給者に、製品で使用しているソフトウェア構成要素を記載した情報を提供するよう要求する。

e) ICT製品の供給者に、自らの製品が実装するセキュリティ機能及びそのセキュリティに配慮した運用に必要な構成を説明する情報を提供するよう要求する。

f) 提供されたICT製品及びサービスが規定のセキュリティ要求事項を順守していることを確認するための、監視プロセス及び許容可能な監視方法を実施する。このような供給者レビュー方法の例に、侵入テスト、及び供給者の情報セキュリティ運用に関する第三者立証の検証又は妥当性確認がある。

g) 製品又はサービスの機能を維持するために重要な構成要素を特定し、文書化するプロセスを実施する。重要な構成要素に対しては、組織の外で作られる場合に必要とされる注意、精査及び更なるフォローアップの強化が求められる（特に、供給者が製品又はサービスの構成要素を他の供給者に外部委託する場合。）。

h) 重要な構成要素及びその供給元が、サプライチェーン全体を通じて追跡可能であるという保証を得る。

i) 提供されるICT製品が期待どおりに機能し、予期しない又は好ましくない

特性をもたないという保証を得る。

j) 供給者からの構成要素が真正のものであり、その仕様から変更されていないことを確実にするためのプロセスを実施する。対策の例に、改ざん防止ラベル、暗号ハッシュ検証又はディジタル署名がある。仕様外の動作を監視することが、改ざん又は偽造を見つける手掛りとなる可能性がある。改ざんの防止及び検知は、設計、開発、統合、運用及び保守を含むシステム開発ライフサイクルの複数の段階で実施する。

k) ICT製品が、例えば、正式な認証又は共通基準承認アレンジメント（Common Criteria Recognition Arrangement）などの評価体系を通じて、必要なセキュリティレベルを達成していることの保証を得る。

l) サプライチェーンについての情報、並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定める。

m) ICT構成要素のライフサイクル及び継続的な使用、並びにこれに関連するセキュリティリスクを管理するための具体的なプロセスを実施する。このプロセスには、その構成要素が入手できなくなる（供給者が事業を営まなくなる、又は技術進歩によって供給者がその構成要素を提供しなくなる）というリスクを管理することも含まれる。代替供給者の特定、並びにソフトウェア及び力量を代替供給者に移転するプロセスを検討する。

### 5d-5.22　供給者のサービス提供の監視、レビュー及び変更管理

管理策：組織は、供給者の情報セキュリティの活動及びサービス提供を定常的に監視し、レビューし、評価し、変更を管理する。

目的：　供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。

詳細管理策

5d-5.22.1　供給者のサービスを監視し、レビューし、変更管理することによって、次の点を確実にする。

a) 合意における情報セキュリティの条件の順守

b) 情報セキュリティのインシデント及び問題の適切な管理

c) 供給者のサービスの変更又は事業状況の変化がサービス提供に影響を与えないこと

5d-5.22.2　供給者のサービスの監視、レビュー及び変更管理は、次のために、組織と供給者との間の関係を管理するプロセスを含む。

a) 合意の順守を検証するために、サービスのパフォーマンスレベルを監視する。

b) 次の事項を含む供給者による変更を監視する。

1) 現在提供されているサービスの強化

2) 新しいアプリケーション及びシステムの開発

3) 組織の諸方針及び諸手順の、変更又は更新

4) 情報セキュリティインシデントの解決及び情報セキュリティの改善のための、新たな又は変更した管理策

c) 次の事項を含む供給者サービスの変更を監視する。

1) ネットワークの変更及び強化
2) 新技術の利用
3) 新製品又は新しい版若しくはリリースの採用
4) 新たな開発ツール及び開発環境
5) サービス設備の物理的設置場所の変更
6) 下請負供給者の変更
7) 他の供給者への下請負契約

d) 供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定する。

e) 独立した監査人の報告書が入手できれば、これのレビューと併せて供給者及び下請負供給者の監査を実施し、特定された問題の追跡調査を行う。

f) 合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューする。

g) 供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する事業の中断・阻害の記録をレビューする。

h) 特定された情報セキュリティ事象又はインシデントに対応し、管理する。

i) 情報セキュリティのぜい弱性を特定し、管理する。

j) 供給者とその供給者との間の供給者関係における情報セキュリティの側面をレビューする。

k) 供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の後においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持する※1。

※1 5f-5.29、5f-5.30、5g-5.35、5g-5.36及び8b-8.14参照

l) 供給者が、順守をレビューし、合意の要求事項を実施する責任を割り当てる。

m) 供給者が適切な情報セキュリティレベルを維持していることを定期的に評価する。

5d-5.22.3 供給者関係を管理する責任は、指定された個人又はチームに割り当てる。

5d-5.22.4 合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。

5d-5.22.5 サービスの提供において不完全な点があった場合は、適切な処置をとる。

### 5d-5.23 クラウドサービスの利用における情報セキュリティ

管理策：クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立する。

目的： クラウドサービスの利用における情報セキュリティを規定し、管理するため。

詳細管理策

5d-5.23.1　組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。

5d-5.23.2　組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。

(5d-5.23.2参考)　これは、外部関係者が提供するサービスを、組織が管理する方法の既存の取組の拡張又はその一部である可能性がある※1。

※1 5d-5.21及び5d-5.22参照

(5d-5.23参考)　クラウドサービスの利用は、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である組織との間の、情報セキュリティに関する責任の共有及び分担、並びに共同作業を伴う可能性がある。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である組織との両方の責任を適切に定義し、実践することが不可欠である。

5d-5.23.3　組織は次の事項を定義する。

a) クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項
b) クラウドサービスの選定基準及びクラウドサービス利用の範囲
c) クラウドサービスの利用及び管理に関する役割及び責任
d) どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスタマとしての組織が管理するか。
e) クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法
f) クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して保証を得る方法
g) 組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法
h) クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順
i) 情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用を監視し、レビューし、評価する組織の取組
j) クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法

(5d-5.23参考)　クラウドサービスの合意は、多くの場合、事前に定義されており、交渉の余地はないことを踏まえ、全てのクラウドサービスについて、組織は、クラウドサービスプロバイダとのクラウドサービスの合意をレビューする。

5d-5.23.4　クラウドサービスの合意は、機密性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。

5d-5.23.5　組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントも実施する。

5d-5.23.6　クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。

5d-5.23.7　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である組織との間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。

a) アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。

b) 組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。

c) マルウェア監視及び保護ソリューションを実装する。

d) 組織の取扱いに慎重を要する情報を、承認されている場所※1、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。

※1 例えば、特定の国又は地域

e) クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。

f) クラウドサービスが、更に外部の供給者へ下請負契約されている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。

g) 異なる法域にわたるディジタル証拠に関する法令及び規制を考慮して、ディジタル証拠を収集する際に組織を支援する。

h) 組織がクラウドサービスの利用を終了したいときに、適切な期間にわたって、適切な支援及びサービスを提供する。

i) クラウドサービスカスタマである組織が利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の必要なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。

j) サービスの提供中又はサービスの終了時に組織が要求する場合、クラウドサービスカスタマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。

5d-5.23.8　クラウドサービスカスタマである組織は、組織へのサービス提供方法に対して、実質的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダが事前に通知することを合意において要求することが望ましいかどうかを、次の事項を含めて考慮する。

a) クラウドサービスの提供に影響する又はそれを変更するような技術インフラストラクチャの変更※1

※1 例えば、再配置、再構成、又はハードウェア若しくはソフトウェアの変更

b) 新しい地理的又は法的区域での情報の処理又は保存

c) ピアクラウドサービスプロバイダ又はその他の下請負業者の利用（既存

の業者の変更又は新しい業者の利用を含む。）

5d-5.23.9　クラウドサービスを利用する組織は、クラウドサービスプロバイダと緊密な連絡を維持する。

（5d-5.23.9参考）　こうした連絡によって、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である組織との両方が各サービスの特性を監視し、合意に含まれるコミットメントの不履行を報告する仕組みを含む、クラウドサービスの利用についての情報セキュリティに関する情報の相互交換が可能になる。

## 5e　インシデント管理

### 5e-5.24　情報セキュリティインシデント管理の計画策定及び準備

管理策：組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。

目的：　情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ、秩序のある対応を確実にするため。

詳細管理策

**【役割及び責任】**

5e-5.24.1　組織は、適切な情報セキュリティインシデント管理プロセスを確立する。

5e-5.24.2　インシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に効果的に伝達する。

5e-5.24.3　情報セキュリティインシデント管理プロセスを確立する際には、次の事項を考慮する。

a）連絡先を含む、情報セキュリティ事象を報告するための共通の方法を確立する※1。

※1 6a-6.8参照

b）管理、文書化、検知、トリアージ、優先順位付け、分析、伝達及び利害関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。

c）情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。

d）組織内で、情報セキュリティインシデントに関連する事項は、力量のある要員だけが取り扱えるようにする。そうした要員には、文書化した手順及び定期的な訓練を提供する。

e）インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。

**【インシデント管理手順】**

5e-5.24.4　情報セキュリティインシデント管理の目的について、経営陣が同意している。

5e-5.24.5　情報セキュリティインシデント管理について責任ある人々が、潜在的な結果及び重大度に基づく解決の時間枠を含む、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。

5e-5.24.6　これらの目的及び優先順位を満たすようにインシデント管理手順を実施する。

5e-5.24.7 経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。

a) 何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価

b) 情報セキュリティ事象及び情報セキュリティインシデントの監視※1、検知※2、分類※3、分析及び報告※4,※5

※1 8b-8.15及び8b-8.16参照
※2 8b-8.16参照
※3 5e-5.25参照
※4 6a-6.8参照
※5 人間又は自動的手段によって

c) インシデントの種類及びカテゴリに従った、対応及びエスカレーション※1、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理

※1 5e-5.26参照

d) 関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整※1

※1 5a-5.5及び5a-5.6参照

e) インシデント管理活動のログ取得

f) 証拠の取扱い※1

※1 5e-5.28参照

g) 根本原因分析又は事後分析手順

h) 学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定

**【報告手順】**

5e-5.24.8 情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。

a) 情報セキュリティ事象が発生した場合にとる処置※1

※1 例えば、生じた誤動作、画面上の表示など関連する詳細全てを直ちに記録し、直ちに連絡先に報告し、協調した処置だけをとる。

b) 情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するためのインシデント書式の使用

c) 情報セキュリティ事象の報告者に、その件が対処され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続

d) インシデント報告書の作成

5e-5.24.9 インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項※1を考慮する。

※1 例えば、規制当局への侵害通知の要求事項

### 5e-5.25 情報セキュリティ事象の評価及び決定

管理策：組織は情報セキュリティ事象を評価し、それらを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。

目的：　情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。

詳細管理策

5e-5.25.1　インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。

5e-5.25.2　体系には、事象を情報セキュリティインシデントに分類する基準を含める。

5e-5.25.3　連絡の窓口は、合意した体系を使用して、各情報セキュリティ事象を評価する。

5e-5.25.4　情報セキュリティインシデントの調整及び対応に責任を負う要員は、評価を実行し、情報セキュリティ事象に関する決定をする。

5e-5.25.5　評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。

## 5e-5.26　情報セキュリティインシデントへの対応

管理策：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。

目的：　情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。

詳細管理策

5e-5.26.1　組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。

5e-5.26.2　情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する※1。

※1 5e-5.24参照

5e-5.26.3　情報セキュリティインシデントへの対応策には、次の事項を含める。

a) インシデントの結果が拡がる可能性がある場合は、インシデントの影響を受けるシステムを含める。

b) 情報セキュリティインシデントの発生後、できるだけ速やかに証拠※1を収集する。

※1 5e-5.28参照

c) 必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う※1。

※1 5f-5.29及び5f-5.30参照

d) 後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。

e) 知る必要性の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。

f) 対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。

g) インシデントへの対処が滞りなく済んだ後、正式にそれを終了し、記録する。

h) 必要に応じて、情報セキュリティのフォレンジック分析を実施する※1。

※1 5e-5.28参照

i) 根本原因を特定するために、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする※1。

※1 5e-5.27参照

j) インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するものを含む、情報セキュリティのぜい弱性及び弱点を特定し、管理する。

### 5e-5.27 情報セキュリティインシデントからの学習

管理策：情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。

目的： 将来のインシデントの起こりやすさ又は影響を減らすため。

詳細管理策

5e-5.27.1 組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。

5e-5.27.2 情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。

a) インシデントのシナリオ及び手順を含むインシデント管理計画を強化する※1。

※1 5e-5.24参照

b) 組織の情報セキュリティリスクアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。

c) 発生し得るインシデントの事例、こうしたインシデントへの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練※1を強化する。

※1 6a-6.3参照

### 5e-5.28 証拠の収集

管理策：組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。

目的： 懲戒処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。

詳細管理策

5e-5.28.1 懲戒処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合は、内部の手順を定めてそれに従う。

5e-5.28.2 法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容される可能性を最大にするために、異なる幾つかの法域の要求事項を考慮する。

5e-5.28.3 情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための

証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っているか、切れているか）に従って、証拠の特定、収集、取得及び保存の指示を規定する。

5e-5.28.4　証拠は原則として、適切な国内法廷又は別の懲戒会議において受容される方法で収集し、次の事項を示す。

a）記録は完全で、いかなる方法でも改ざんされていない。

b）電子証拠の複製は原本と同一であることが推定される。

c）証拠の収集元である情報システムは、証拠を記録した時点で正しく機能していた。

5e-5.28.5　保存した証拠の価値を強化するために、入手可能であれば、要員及びツールの適格性を示す証明書又はその他適切な手段を追求する。

5e-5.28.6　ディジタル証拠が組織の枠又は法域を越える場合、組織は必要とされる情報をディジタル証拠として収集することが法的に認められていることを確認する。

## 5f　事業継続における情報セキュリティ管理

### 5f-5.29　事業の中断・阻害時の情報セキュリティ

管理策：組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画する。

目的：　事業の中断・阻害時に情報及びその他の関連資産を保護するため。

詳細管理策

5f-5.29.1　組織は、事業の中断・阻害時に情報セキュリティ管理策を適応させるための自らの要求事項を決定する。

5f-5.29.2　情報セキュリティ要求事項は、事業継続マネジメントプロセスに含める。

5f-5.29.3　中断又は障害後に重要な事業プロセスにおける情報のセキュリティを維持又は復旧するために、計画を策定し、実施し、試験し、レビューし、評価する。

5f-5.29.4　情報のセキュリティは、必要なレベル及び必要な時間内に復旧する。

5f-5.29.5　組織は次の事項を実施し、維持する。

a）事業継続計画及びICT継続計画における情報セキュリティ管理策、支援システム及びツール

b）事業の中断・阻害時に既存の情報セキュリティ管理策を維持するためのプロセス

c）事業の中断・阻害時に維持できない情報セキュリティ管理策を補う管理策

### 5f-5.30　事業継続のためのICTの備え

管理策：事業継続の目的及びICT継続の要求事項に基づいて、ICTの備えを計画し、実施し、維持し、試験する。

目的：　事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。

詳細管理策

（5f-5.30参考）　事業継続に関するICTの備えは、事業の中断・阻害時にも組織の目的が継続して満たされることを確実にするための、事業継続マネジメント及び情報セキュリティマネジメントの重要な構成要素である。

5f-5.30.1　ICT継続の要求事項を、事業影響度分析（BIA）の結果をもとに規定する場合、そのBIAプロセスでは、影響の種類及び評価基準を用いて、製品及びサービスを提供する事業活動の中断・阻害から生じる影響を経時的に評価する。

5f-5.30.2　事業の中断・阻害の結果として生じる影響の大きさ及び期間を用いて優先する活動を特定し、これに目標復旧時間（RTO）を設定した後、BIAでは、優先する活動の支援にどの資源が必要かを決定する。

5f-5.30.3　優先する事業活動を支援する資源にもRTOを定め、これらの資源の一部としてICTサービスを含める。

（5f-5.30参考）　ICTサービスに係るBIAを拡張して、事業の中断・阻害時の活動を支援するために必要な、ICTシステムのパフォーマンス、容量・能力の要求事項、及び情報の目標復旧時点（RPO）を定めることが可能である。

5f-5.30.4　ICTサービスに関わるBIA及びリスクアセスメントの結果に基づいて、組織は、事業の中断・阻害の前、中断・阻害中及び中断・阻害の後の選択肢を考慮したICT継続戦略を特定し、選択する。

5f-5.30.5　ICTサービスに必要な可用性レベルを満たし、重要なプロセスの中断又は失敗後に求められる時間内に回復するために、この戦略に基づいて計画を作成し、実装し、試験する。

（5f-5.30.5参考）　事業継続戦略は、一つ以上のソリューションから成る可能性がある。

5f-5.30.6　組織は、次の事項を確実にする。

a）事業の中断・阻害に備え、それを緩和し、それに対応するために、必要な責任、権限及び力量をもつ要員が支援する適切な組織構造を備えている。

b）組織がICTサービスの中断・阻害を管理する方法を詳述した、対応及び復旧手順を含むICT継続計画について、次を実施する。

1）演習及びテストを通じた定期的な評価

2）経営陣による承認

c）ICT継続計画は、次のICT継続に関する情報を含む。

1）BIAで特定した事業継続の要求事項及び目的を満たすためのパフォーマンス及び容量・能力の仕様

2）優先するICTサービスそれぞれのRTO及びそれらの構成要素を復旧する手順

3）情報として定義された優先するICT資源のRPO及び情報を復旧する手順

## 5g　コンプライアンス管理

### 5g-5.31　法令、規制及び契約上の要求事項

管理策：情報セキュリティに関連する法令、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を特定し、文書化し、また、最新に保つ。

目的：　情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。

詳細管理策

**【コンプライアンス管理全般】**

5g-5.31.1　法令、規制又は契約上の要求事項を含む外部の要求事項は、次の場合に考慮

に入れる。

a) 情報セキュリティの方針群及び手順の策定
b) 情報セキュリティ管理策の設計、実施又は変更
c) 内部のニーズ又は供給者との合意のために情報セキュリティ要求事項を設定するプロセスの一部としての、情報及びその他の関連資産の分類
d) 情報セキュリティリスクアセスメントの実施、及び情報セキュリティリスク対応活動の決定
e) 情報セキュリティに関連する役割及び責任に従ったプロセスの決定
f) 組織、並びに供給を受ける製品及びサービスの範囲に関係する、供給者の契約上の要求事項の特定

**【法令及び規制】**

5g-5.31.2 組織は、次の事項を行う。

a) 自らの事業の種類に対する要求事項を認識するために、組織の情報セキュリティに関連する全ての法令及び規制を特定する。
b) 組織が次のとおりである場合に、関連する全ての国における順守を考慮する。
  - 他国で事業を行っている。
  - 法令及び規制が組織に影響を与える可能性がある、他国の製品及びサービスを利用している。
  - 法令及び規制が組織に影響を与える可能性がある、法域との境界を越えて情報の移転を行う。
c) 変更に追随し、新しい法令を特定するために、特定した法令及び規制を定期的にレビューする。
d) これらの要求事項を満たすためのプロセス及び個々の責任を定義し、文書化する。

**【暗号化】**

5g-5.31.3 暗号化は、次の項目に関連する合意、法令及び規制の順守を考慮に入れる。

a) 暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制
b) 暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制
c) 暗号利用に関する規制
d) 暗号化された情報への、国の当局による強制的又は任意的アクセス方法
e) ディジタル署名、eシール及びディジタル証明書の有効性

(5g-5.31.3参考1) 暗号化は、多くの場合、固有の法的要求事項をもつ分野である。

(5g-5.31.3参考2) 関連する法令及び規制の順守を確実にするために、特に暗号化された情報又は暗号化ツールを法域の境界を越えて転送する場合、法的な助言を求めることが推奨される。

**【契約】**

5g-5.31.4 情報セキュリティに関する契約上の要求事項には、次のものに記載されてい

る要求事項を含む。

a) 顧客との契約

b) 供給者との契約※1

※1 5d-5.20参照

c) 保険契約

### 5g-5.32 知的財産権

管理策：組織は知的財産権を保護するための適切な手順を実施する。

目的： 知的財産権及び権利関係のある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。

詳細管理策

5g-5.32.1 知的財産となり得るものを保護するために、次の事項を考慮する。

a) 知的財産権の保護に関するトピック固有の方針を定め、伝達する。

b) ソフトウェア製品及び情報製品のコンプライアンスにのっとった利用を定めた、知的財産権の順守の手順を発行する。

c) 著作権を侵害しないことを確実にするために、ソフトウェアは、知名度の高い、かつ、定評のある供給元だけを通して取得する。

d) 適切な資産登録簿を維持管理し、知的財産権の保護が求められている全ての資産を特定する。

e) 使用許諾を得ていることの証明及び証拠、手引などを維持・管理する。

f) 使用許諾で許可された最大利用者数又は資源数※1を超過しないことを確実にする。

※1 例えば、中央処理装置（CPU）

g) 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確実にするためのレビューを行う。

h) 適切な使用許諾条件を維持・管理するための手順を定める。

i) ソフトウェアの処分又は他人への譲渡についての手順を定める。

j) 公衆ネットワーク及び外部供給元から入手するソフトウェア及び情報の使用条件を順守する。

k) 著作権法又は適用される使用許諾が認めている場合を除いて、商用記録（ビデオ、録音）を複製、他形式に変換、又は抜粋しない。

l) 著作権法又は適用される使用許諾が認めている場合を除いて、規格※1、書籍、記事、報告書又はその他文書の全部又は一部を複写しない。

※1 例えば、ISO/IEC規格

### 5g-5.33 記録の保護

管理策：記録は、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。

目的： 記録の保護及び可用性に関連する、法令、規制及び契約上の要求事項の順守、並びにコミュニティ又は社会の期待に応えることを確実にするため。

詳細管理策

5g-5.33.1 組織は、自らの事業の状況及び自らの管理の要求事項が時間の経過とともに

変化するため、記録の真正性、信頼性、完全性及び使用可能性を保護するために次の段階を踏む。

a) 記録の改変の防止を含む、記録の保存、受渡記録の取扱い及び記録の処分に関する指針を発行する。これらの指針は、記録管理及びその他の記録の要求事項に関する組織のトピック固有の方針に沿っている。

b) 記録及びそれらの記録の保持することが望ましい期間を明確にした保持計画を作成する。

5g-5.33.2 記録を保存し、取り扱うシステムは、国又は地域の法令又は規制、及び該当する場合には、コミュニティ又は社会の期待も考慮に入れて、記録及びその保持期間の特定を確実にする。

5g-5.33.3 記録の保持期間が終了した後、組織にとって必要ない場合には、そのシステムは、記録を適切に破棄できるようにする。

5g-5.33.4 具体的な組織の記録の保護について決定する場合は、組織の分類体系に基づき、その情報に適用されている情報セキュリティ分類を考慮する。

5g-5.33.5 記録類は、記録の種類※1によって、また、それぞれの種類を更に詳細に、保持期間、及び許容される物理的又は電子的な記憶媒体の種類によって分類する。

※1 例えば、会計記録、事業のトランザクション記録、人事記録、法務記録

5g-5.33.6 満たすべき要求に応じて、許容される時間枠内及び書式で、要求された記録を取り出すことができるような、データ保存システムを選択する。

5g-5.33.7 電子記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じて記録にアクセスできること（記憶媒体及び書式の読取り可能性）を確実にする手順を確立する。

5g-5.33.8 記録を保持している期間中、記録の復号を可能にするために、暗号化したアーカイブ又はディジタル署名に用いた暗号鍵及び暗号プログラムも保持する※1。

※1 8c-8.24参照

5g-5.33.9 記録媒体の保存及び取扱いの手順は、記憶媒体の製造業者が示す推奨の仕様に従って実施する。

5g-5.33.10 記録の保存に用いる媒体が劣化する可能性を考慮する。

## 5g-5.34 プライバシー及びPIIの保護

管理策：組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシー及びPIIの保護に関する要求事項を特定し、満たす。

目的： PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。

詳細管理策

5g-5.34.1 組織は、プライバシー及びPIIの保護に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。

5g-5.34.2 組織は、プライバシー及びPIIの保護のための手順を策定し、実施する。

5g-5.34.3 組織は、プライバシー及びPIIの保護のために策定した手順を、PIIの処理に関わる全ての利害関係者に伝達する。

5g-5.34.4　組織は、プライバシー及びPIIの保護のために策定した手順の順守、並びにプライバシー及びPIIの保護に関する全ての法令及び規制の順守のために、適切な役割、責任及び管理策を整備する。

5g-5.34.5　プライバシー及びPIIの保護に関する責任者は、要員、サービス提供者及びその他の利害関係者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。

（5g-5.34.5参考）　多くの場合、例えば、プライバシー担当役員のような一人の責任者を任命することによって最も達成される。

5g-5.34.6　PIIの取扱いについての責任は、関連する法令及び規制を考慮に入れて処置する。

5g-5.34.7　PIIを保護するための適切な技術的及び組織的対策を実施する。

### 5g-5.35　情報セキュリティの独立したレビュー

管理策：人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、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。

目的：　組織における情報セキュリティ管理の取組の、継続的な適切性、十分性及び有効性を確実にするため。

詳細管理策

5g-5.35.1　組織は、情報セキュリティの独立したレビューを実施するためのプロセスをもつ。

5g-5.35.2　管理層は、情報セキュリティの定期的な独立したレビューを計画し、発議する。

5g-5.35.3　情報セキュリティの独立したレビューは、情報セキュリティ方針、トピック固有の方針、及びその他の管理策を含む、情報セキュリティの取組の改善の機会及び変更の必要性の評価を含む。

5g-5.35.4　情報セキュリティの独立したレビューは、レビューの対象となる領域から独立した個人・組織※1が実施する。

※1 例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者

5g-5.35.5　情報セキュリティの独立したレビューを実施する個人・組織は、適切な力量をもつ。

5g-5.35.6　情報セキュリティの独立したレビューを実施する個人は、評価を行う上で独立性をもつことを確実にするため、権限をもつ系統に属さない。

5g-5.35.7　情報セキュリティの独立したレビューの結果は、レビューを発議した管理層、及び、適切な場合には、トップマネジメントに報告する。

5g-5.35.8　情報セキュリティの独立したレビューの記録は、維持する。

5g-5.35.9　情報セキュリティの独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組及び実施が十分でない※1ことが明確になった場合には、管理層は是正処置を発議する。

※1 例えば、文書化した目的及び要求事項が、情報セキュリティ方針及び

トピック固有の方針（5a-5.1参照）に記載された情報セキュリティに関する方向付けを満たしていない、又はこれを順守していない。

5g-5.35.10　情報セキュリティの定期的な独立したレビューに加えて、組織は次の場合にも、独立したレビューの実施を検討する。

a）組織に影響する法令及び規制が変わる。

b）重大なインシデントが生じる。

c）組織が新しい事業を開始する、又は現在の事業を変更する。

d）組織が新しい製品若しくはサービスの利用を開始する、又は現在の製品若しくはサービスの利用を変更する。

e）組織が情報セキュリティの管理策及び手順を大幅に変更する。

### 5g-5.36　情報セキュリティのための方針群、規則及び標準の順守

管理策：組織の情報セキュリティ方針、トピック固有の方針、規則及び標準を順守していることを定期的にレビューする。

目的：　情報セキュリティを、組織の情報セキュリティ方針、トピック固有の方針、規則及び標準に従って実施し、運用することを確実にするため。

詳細管理策

5g-5.36.1　管理者及びサービス、製品又は情報の管理責任者は、情報セキュリティ方針、トピック固有の方針、規則、標準及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューする方法を特定する。

5g-5.36.2　定めに従って効率的に情報セキュリティのレビューを行うため、自動的な測定ツール及び報告ツールの使用を考慮する。

5g-5.36.3　情報セキュリティのレビューの結果、何らかの不順守を検出した場合、管理者は、次の事項を行う。

a）不順守の原因を特定する。

b）順守を達成するための是正処置の必要性を評価する。

c）適切な是正処置を実施する。

d）是正処置の有効性を検証し、不備又は弱点を特定するために、講じた是正処置をレビューする。

5g-5.36.4　管理者及びサービス、製品又は情報の管理責任者が実施した情報セキュリティのレビュー及び是正処置の結果を記録し、また、その記録を維持管理する。

5g-5.36.5　管理者の責任範囲に対して、情報セキュリティの独立したレビュー※1が実施されるときは、管理者は、独立したレビュー実施者に対して、その結果を報告する。

※1 5g-5.35参照

5g-5.36.6　情報セキュリティ要求事項の不順守に対する是正処置は、リスクに対して適切に、時機を失せずに完了する。

5g-5.36.7　次に予定している情報セキュリティのレビューまでに完了しない場合、そのレビュー時に少なくとも進捗状況を取り上げる。

### 5g-5.37　操作手順書

管理策：情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能にする。

目的：　情報処理設備の正確で、かつ、セキュリティに配慮した操作を確実にするため。

詳細管理策

5g-5.37.1　次の場合には、情報セキュリティに関連する組織の操作活動の手順書を作成する。

a) 多くの人が同じ活動を行う必要がある場合

b) まれにしか行わない活動で、次に実行するときに手順を忘れている可能性が高い場合

c) 新たな活動で、正しく実行しないとリスクが生じる場合

d) 新しい要員に活動を引き継ぐ前

5g-5.37.2　情報処理設備の操作手順には、次の事項を明記する。

a) 責任者

b) システムのセキュリティに配慮した導入及び構成

c) 情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。）

d) バックアップ※1及びレジリエンス

※1 8b-8.13参照

e) スケジュールに関する要求事項。これには、他のシステムとの依存関係を含む。

f) 作業中に発生し得る、誤り又はその他の例外状況の処理についての指示※1

※1 例えば、ユーティリティプログラムの利用の制限（8b-8.18参照）

g) 操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及びエスカレーション用の連絡先

h) 記憶媒体の取扱いに関する指示※1

※1 7b-7.10及び7b-7.14参照

i) システムが故障した場合の再起動及び回復の手順

j) 監査証跡及びシステムログ情報※1並びにビデオ監視システム※2の管理

※1 8b-8.15及び8b-8.17参照

※2 7a-7.4参照

k) 容量・能力、パフォーマンス及びセキュリティなどの監視手順※1

※1 8a-8.6 及び8b-8.16参照

l) 保守手順

5g-5.37.3　情報処理設備の操作手順書は必要に応じてレビューし、更新する。

5g-5.37.4　情報処理設備の操作手順書の変更は認可のもとで行う。

5g-5.37.5　技術的に可能であれば、情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。

## 6　人的管理策

### 6a　人的管理

#### 6a-6.1　選考

管理策：要員になる全ての候補者についての経歴などの確認は、適用される法令、規制及び倫理を考

慮に入れて、組織に加わる前に、及びその後継続的に行う。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。

目的： 全ての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。

詳細管理策

6a-6.1.1 選考プロセスは、フルタイム、パートタイム及び臨時スタッフを含む全ての要員に対して実行する。

6a-6.1.2 サービス供給者を通じて選考される個人に関して契約をする場合には、選考の要求事項を組織と供給者との間の合意に含める。

6a-6.1.3 組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令を考慮して収集し、扱う。

（6a-6.1.3参考） 法域によっては、選考活動について、組織が候補者に事前に通知することが法的に必要な場合がある。

6a-6.1.4 要員になる候補者の確認は、関連があるプライバシー、PII保護及び雇用に関する法令の全てを考慮に入れ、許容される場合には、次の事項を含む。

a) 満足のいく推薦状※1の入手の可否

※1 例えば、業務及び人物に関する推薦状

b) 応募者の履歴書の確認（完全であるか及び正確であるかの確認）

c) 提示された学術上及び職業上の資格の確認

d) 公的証明書※1の確認

※1 例えば、パスポート又は適切な当局が発行したその他の許容可能な文書

e) 候補者が重要な役割を担う場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認

6a-6.1.5 情報セキュリティに関する特定の役割のために雇用する場合、組織は、次の事項を確認する。

a) 候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えている。

b) 特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物である。

6a-6.1.6 最初の発令で就く業務であるか、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報※1を扱っているときには、組織は、より詳細な確認も検討する。

※1 例えば、財務情報、個人情報又は医療情報

6a-6.1.7 選考手順には、要員になる候補者の確認のためのレビューの基準及び制約を定める※1。

※1 例えば、誰が選考するのか。また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。

6a-6.1.8 時機を失せずに要員になる候補者の確認を完了できない状況では、レビューが終了するまで、例えば、次のようなリスク低減のための管理策を実施する。

a) 実務研修の開始時期を遅らせる。

b) 企業資産の利用を遅らせる。

c) アクセスを限定した実務研修を実施する。

d) 雇用を終了する。

6a-6.1.9 個人の役割の重要性に応じて、要員が適切であり続けることを確実にするための確認を定期的に繰り返す。

### 6a-6.2 雇用条件

管理策：雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載する。

目的： 要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。

詳細管理策

6a-6.2.1 要員の契約上の義務は、組織の情報セキュリティ方針及びその他の関連するトピック固有の方針を考慮に入れる。

6a-6.2.2 場合に応じて、次の事項について明確にし、言及する。

a) 秘密情報へのアクセスが与えられる全ての要員が情報及びその他の関連資産へのアクセスが与えられる前に署名することが望ましい秘密保持契約書又は守秘義務契約書※1

※1 6a-6.6参照

b) 法的な責任及び権利※1

※1 例えば、著作権法、データ保護に関連して制定された法令（5g-5.32及び5g-5.34参照）に関するもの

c) 要員によって扱われる、情報の分類、組織の情報及びその他の関連資産の管理、並びに情報処理施設及び情報サービスの管理に関する責任※1

※1 5b-5.9及び5b-5.13参照

d) 利害関係者から受け取った情報の扱いに関する責任

e) 要員が組織の情報セキュリティ要求事項に従わない場合にとる処置※1

※1 6a-6.4参照

6a-6.2.3 情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝達する。

6a-6.2.4 組織は、要員が情報セキュリティに関する雇用条件に同意することを確実にする。

6a-6.2.5 情報セキュリティに関する雇用条件は、情報システム及びサービスに関連する組織の資産に対する要員によるアクセスの特性及び範囲に応じて、適切なものとする。

6a-6.2.6 法令、規制、情報セキュリティ方針又はトピック固有の方針が変更された場合は、情報セキュリティに関する雇用条件をレビューする。

6a-6.2.7 適切であれば、雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を継続させる※1。

※1 6a-6.5参照

### 6a-6.3 情報セキュリティの意識向上、教育及び訓練

管理策：組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピ

ック固有の方針及び手順についての、適切な、情報セキュリティに関する意識向上プログラム、教育及び訓練を受け、また、定常的な更新を受ける。

目的：　要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。

詳細管理策

**【情報セキュリティの意識向上、教育及び訓練全般】**

6a-6.3.1　情報セキュリティの意識向上、教育及び訓練プログラムは、保護すべき組織の情報及び情報を保護するために実施されている情報セキュリティ管理策を考慮に入れて、組織の情報セキュリティ方針、トピック固有の方針及び情報セキュリティの関連する手順に沿って確立する。

6a-6.3.2　情報セキュリティの意識向上、教育及び訓練は、定期的に実施する。

6a-6.3.3　可能な場合、開始時の意識向上、教育及び訓練を、新しい要員、及び情報セキュリティに関する要求事項が大幅に異なる新たな職位又は役割に異動した者にも適用する。

6a-6.3.4　知識が伝わったこと、並びに意識向上、教育及び訓練プログラムの有効性を確認するため、意識向上、教育及び訓練の活動終了時に、要員の理解の評価を行う。

**【意識向上】**

6a-6.3.5　情報セキュリティの意識向上プログラムは、要員に対し、情報セキュリティに関する各自の責任及びその責任を果たす方法について、認識させることを狙いとする。

6a-6.3.6　意識向上プログラムは、内部及び外部の要員※1を含む、組織における要員の役割を考慮に入れて、計画する。

※1 例えば、外部のコンサルタント、供給者の要員

6a-6.3.7　意識向上プログラムの活動は、長期にわたり、できれば定期的に実施する。

（6a-6.3.7参考）　これによって、活動が繰り返され、新しい要員も対象となる。

6a-6.3.8　意識向上プログラムの活動では、情報セキュリティインシデントから学んだ教訓を生かす。

6a-6.3.9　意識向上プログラムには、キャンペーン、パンフレット、ポスター、会報、ウェブサイト、説明会、ブリーフィング、eラーニングモジュール、電子メールなど、適切な物理的又は仮想的な手段を通じた多くの意識向上活動を含める。

6a-6.3.10　情報セキュリティの意識向上には、例えば、次のような一般的な側面を含める。

a) 組織全体にわたる情報セキュリティに対する経営陣のコミットメント

b) 情報セキュリティ方針及びトピック固有の方針、基準、法令、規制、契約及び合意を考慮に入れた、適用される情報セキュリティの規則及び義務に関する精通度及び順守のニーズ

c) 自身が行動したこと及び行動しなかったことに対する個人のアカウンタビリティ、並びに組織及び利害関係者に属する情報のセキュリティを保

ち、これを保護することに対する一般的な責任

d) 情報セキュリティに関する基本的な手順※1

※1 例えば、情報セキュリティ事象の報告（6a-6.8）及び基本的な管理策（例えば、パスワードのセキュリティ（5c-5.17））

e) 情報セキュリティに関連する事項についての追加の情報及び助言（情報セキュリティの意識向上に関する追加の資料も含む。）を得るための連絡先及び情報源

**【教育及び訓練】**

6a-6.3.11 組織は、特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、適切な訓練計画を特定し、準備し、実施する。

6a-6.3.12 技術チームは、装置・機器、システム、アプリケーション及びサービスに必要なセキュリティレベルを構成し、維持する技能をもつ。

6a-6.3.13 技術チームに不足している技能がある場合、組織は処置をとり、それを取得させる。

6a-6.3.14 教育及び訓練プログラムは、様々な形式※1を検討する。

※1 例えば、講義又は自己学習、専門スタッフ又はコンサルタントによる指導（オンザジョブトレーニング）、スタッフを異なる活動に従事させるローテーション、既に熟練している人材の採用及びコンサルタントの雇用

（6a-6.3.14参考） 教室、遠隔教育、ウェブ利用、自習式、及びその他異なる提供手段が利用可能である。

6a-6.3.15 技術要員は、会報及び雑誌を購読する、又は技術的及び専門的な向上を目的とした会議及びイベントに参加することによって、自らの知識を最新の状態に保つ。

### 6a-6.4 懲戒手続

管理策：情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。

目的： 要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を抑止すること、及びそれを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。

詳細管理策

6a-6.4.1 懲戒手続は、情報セキュリティ方針違反が生じたことの事前の確認を待って開始する※1。

※1 5e-5.28参照

6a-6.4.2 正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。

a) 違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果

b)違反が意図的である（悪意がある）か、又は意図的でない（偶発的）か。

c) 最初の違反か又は繰り返されたものか。

d) 違反者は、適切に教育・訓練されていたかどうか。

6a-6.4.3 懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並び

に必要に応じてその他の要素を考慮に入れる。

6a-6.4.4　懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使う。

（6a-6.4.4参考）　意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。

### 6a-6.5　雇用の終了又は変更後の責任

管理策：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、施行し、関連する要員及びその他の利害関係者に伝達する。

目的：　雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。

詳細管理策

6a-6.5.1　雇用の終了又は変更を管理する手続では、終了又は変更後にどの情報セキュリティの責任及び義務を引き続き有効とすることが望ましいかを定める。

6a-6.5.2　雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取得したその他の知識、並びにその他の秘密保持契約に含まれる責任を含める※1。

※1 6a-6.6参照

6a-6.5.3　雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件※1、契約又は合意に含める。

※1 6a-6.2参照

（6a-6.5.3参考）　個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。

6a-6.5.4　責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。

6a-6.5.5　職務を去る又は職務が変わる個人がもつ情報セキュリティの役割及び責任を特定し、別の個人に移す。

6a-6.5.6　変更及び運用の手順を要員、その他の利害関係者及び関連する連絡先担当者に※1伝達するための手続を確立する。

※1 例えば、顧客及び供給者への伝達

6a-6.5.7　雇用の終了又は変更の手続は、供給者の要員、供給者との契約若しくは組織との仕事の終了が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。

### 6a-6.6　秘密保持契約又は守秘義務契約

管理策：情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定常的にレビューし、要員及びその他の関連する利害関係者が署名する。

目的：　要員又は外部の関係者がアクセスできる情報の秘密保持のため。

詳細管理策

6a-6.6.1　秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。

6a-6.6.2　秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。

6a-6.6.3　組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。

6a-6.6.4　秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。

a) 保護する情報の定義※1

※1 例えば、秘密情報

b) 秘密を無期限に又は情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間

c) 契約終了時に要求する処置

d) 認可されていない情報開示を避けるための、署名者の責任及び行為

e) 情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係

f) 秘密情報の許可された利用範囲、及び情報を利用する署名者の権利

g) 高度に取扱いに慎重を要する状況における、秘密情報に関わる行為の監査及び監視の権利

h) 認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス

i) 契約終了時における情報の返却又は破棄に関する条件

j) 契約の不順守が発生した場合に講じるべき処置

6a-6.6.5　組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる※1。

※1 5g-5.31、5g-5.32、5g-5.33及び5g-5.34参照

6a-6.6.6　秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。

## 6a-6.7　リモートワーク

管理策：組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。

目的：　要員が遠隔で作業をする場合の情報セキュリティを確実にするため。

詳細管理策[24]

(6a-6.7参考)　リモートワークは、組織の構外から組織の要員が作業し、ハードコピーで又はICT機器を通じて電子的に情報にアクセスするときに常に行われる。リモートワーク環境は、“テレワーキング”、“コンピュータ端末を用いた在宅勤務（telecommuting）”、“柔軟な作業場（flexible workplace）”、“仮想的な作業環境”、及び“遠隔保守”と呼ばれる環境を含んでいる。

6a-6.7.1　リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関するトピック固有の方針を発行する。

[24] 法域によって異なる、地域の法令及び規制のため、本項の全ての詳細管理策が適用できるとは限らない。

6a-6.7.2 適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。

a) 要員が配置されている法域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ

b) 施錠可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告に関する規則など、遠隔物理環境のための規則及びセキュリティの仕組み※1

※1 6a-6.8参照

c) 期待される物理的なリモートワーク環境

d) 次を考慮した、通信のセキュリティに関する要求事項

- 組織のシステムへのリモートアクセスの必要性
- 通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い
- システム及びアプリケーションの取扱いに慎重を要する度合い

e) 個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップアクセスなどリモートアクセスの使用

f) リモートワークの場所における、他者※1による情報又は資源への認可されていないアクセスの脅威

※1 例えば、家族、友人

g) 公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威

h) 家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限

i) ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用

j) システムを遠隔で展開し、初期化するためのセキュリティに配慮した仕組み

k) 組織のネットワークへのリモートアクセスを許可する場合に、単一要素認証の仕組みのぜい弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み

6a-6.7.3 リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。

a) 組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供

b) 許可した作業、保持することができる情報の分類、並びにリモートワークを行う者にアクセスを認可する内部システム及びサービスの定義

c) 遠隔で作業する者及び支援を提供する者のための訓練の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。

d) 機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有

効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したリモートアクセス方法を含む、適切な通信機器の提供

e) 物理的セキュリティ

f) 家族及び訪問者による機器及び情報へのアクセスに関する規則及び手引

g) ハードウェア及びソフトウェアのサポート及び保守の提供

h) 保険の提供

i) バックアップ及び事業継続のための手順

j) 監査及びセキュリティの監視

k) リモートワークが終了したときの、権限及びアクセス権の失効並びに機器の返却

### 6a-6.8 情報セキュリティ事象の報告

管理策：組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。

目的： 要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。

詳細管理策

6a-6.8.1 情報セキュリティインシデントの影響を防止又は最小化するために、全ての要員及び利用者に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させておく。

6a-6.8.2 全ての要員及び利用者に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。

6a-6.8.3 報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるものとする。

6a-6.8.4 情報セキュリティ事象には、インシデント、違反及びぜい弱性を含める。

6a-6.8.5 情報セキュリティ事象の報告を検討する状況には、次を含める。

a) 効果のない情報セキュリティ管理策

b) 情報の機密性、完全性又は可用性に関する期待に対する違反

c) ヒューマンエラー

d) 情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守

e) 物理的セキュリティ対策に対する違反

f) 変更管理プロセスを経ないシステム変更

g) ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動

h) アクセス違反

i) ぜい弱性

j) マルウェア感染の疑い

6a-6.8.6 要員及び利用者に、疑いをもった情報セキュリティのぜい弱性の立証を試み

ないように要求する。

（6a-6.8.6参考）　ぜい弱性を検査することは、システムの不正使用の企てと見られる可能性があり、情報システム又はサービスに損傷を与える可能性もあり、それはディジタル証拠を破損又は不明瞭にする可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。

## 7　物理的管理策

### 7a　物理的領域の管理

#### 7a-7.1　物理的セキュリティ境界

管理策：情報及びその他の関連資産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。

目的：　組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。

詳細管理策

7a-7.1.1　物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。

a）境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。

b）情報処理設備を収容した建物又は敷地が物理的に頑丈な境界をもつ（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない。）。敷地内の屋根、壁、天井及び床は、堅固な構造物とし、外部に接する全ての扉を、開閉制御の仕組み※1によって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。換気口の位置も考慮する。

※1 例えば、かんぬき、警報装置、錠

c）セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警告、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。

#### 7a-7.2　物理的入退

管理策：セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。

目的：　組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。

詳細管理策

**【物理的入退全般】**

7a-7.2.1　荷物の受渡場所などのアクセス場所（受付など）、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。

7a-7.2.2　可能な場合には、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。

7a-7.2.3　物理的入退の管理策の実施については、次の事項を考慮する。

a) 敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、更新及び失効を含める※1。

※1 5c-5.18参照

b) 全てのアクセスについて、物理的な記録簿又は電子形式の監査証跡を、セキュリティを保って維持及び監視し、全ての記録※1及び取扱いに慎重を要する認証情報を保護する。

※1 5g-5.33参照

c) 情報を処理する又は保管する領域へのアクセスを管理するためのプロセス及び技術的な仕組みを確立し、実装する。認証の仕組みには、アクセスカード、生体認証、又はアクセスカード及び秘密の個人識別番号のような二要素認証の仕組みの使用を含む。慎重を要する領域へのアクセスには、二重のセキュリティドアの採用を検討する。

d) 要員が監視している受付エリア、又は敷地若しくは建物への物理的なアクセスを管理するその他の手段を設定する。

e) 入退の際に要員及び利害関係者の持ち物を検査[25]し、確認する。

f) 全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。常勤の従業員、供給者及び訪問者を識別しやすくするために、容易に区別できるバッジの使用を検討する。

g) セキュリティを保つべき領域又は情報処理施設への、供給者の要員によるアクセスは、限定的かつ必要なときにだけ許可する。このアクセスは、認可を必要とし、監視する。

h) 複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。

i) 物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。

j) 非常口などの他の入退場所を、認可されていないアクセスから保護する。

k) 物理的な鍵又は認証情報※1の管理を確実にし、記録簿又は毎年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する※2。

※1 例えば、ロックコード、オフィス、部屋及び鍵キャビネットなどの設備のコンビネーションロック

※2 認証情報の詳細については5c-5.17参照

**【訪問者】**

7a-7.2.4　物理的入退の訪問者に関する管理策では、次の事項を考慮する。

[25] 持ち物の検査が可能か否かに関して、地域の法令及び規制が存在する可能性がある。

a) 適切な手段によって訪問者のアイデンティティを認証する。

b) 訪問者の出入りの日時を記録する。

c) 特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下でだけ、訪問者にアクセスを許可する。

d) 明示的に例外が許可されない限り、全ての訪問者を監視する。

**【荷物の受渡場所及び入荷資材】**

7a-7.2.5 荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。

a) 建物外部からの受渡場所へのアクセスは、特定の認可された要員に制限する。

b) 受渡場所は、配達要員が建物の他の場所に認可されていないアクセスをすることなく荷積み及び荷降ろしできるように設計する。

c) 受渡場所の外部扉は、制限領域への扉が開いているときにはセキュリティを保つ。

d) 入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。

e) 入荷物は、事業所へ持ち込むときに資産の管理手順※1に従って登録する。

※1 5b-5.9 及び7b-7.10 参照

f) 可能な場合には、入荷と出荷とは、物理的に分離した場所で扱う。

g) 入荷物は、輸送中に開封された痕跡がないかを検査する。開封の痕跡が見つかった場合には、直ちにセキュリティ要員に報告する。

## 7a-7.3 オフィス、部屋及び施設のセキュリティ

管理策：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、実装する。

目的： オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、及び干渉を防ぐため。

詳細管理策

7a-7.3.1 オフィス、部屋及び施設のセキュリティを保つために、次の事項を考慮する。

a) 重要な施設は、一般の人のアクセスが避けられる場所に設置する。

b) 適用可能な場合、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないことを確実にする。

c) 施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する。該当する場合、電磁遮蔽も考慮する。

d) 秘密情報処理施設の場所を示す案内板、内線電話帳及びオンラインでアクセス可能な地図は、認可されていない者に容易に利用可能とならないようにする。

## 7a-7.4 物理的セキュリティの監視

管理策：施設は、認可していない物理的アクセスについて継続的に監視する。

目的：　認可されていない物理的アクセスを検知し、抑止するため。

詳細管理策

7a-7.4.1　物理的な施設は、監視システムによって監視する。

（7a-7.4.1参考）　これには、内部で又は監視サービス提供者が管理する、警備員、侵入者警報、監視カメラなどのビデオ監視システム、及び物理的セキュリティ情報管理ソフトウェアを含む場合がある。

7a-7.4.2　重要なシステムを収容している建物へのアクセスは、認可されていないアクセス又は疑わしい行動を検知するために、次の手段によって継続的に監視する。

a）組織の施設の内部及び外部の慎重を要する領域へのアクセスを目視し、記録するために、監視カメラなどのビデオ監視システムを設置する。

b）関連する適用される標準に従って、侵入者警報を起動する次のような接触、音又は動きの検知器を設置し、それらを定期的に試験する。

1）パニック警報装置として使用するために、接触が発生又は遮断される可能性のある場所（窓及びドア並びに物体の下など）に、接触が発生又は遮断されたときに警報を起動する接触検知器

2）物体が視野を通過したときに警報を起動する、赤外線技術に基づく動きの検知器

3）ガラスが割れる音に敏感に反応し、それを使用して警報を発し、セキュリティ要員に警告することができるセンサー

c）全ての外部扉及びアクセス可能な窓を対象として、これらの警報を使用する。無人の領域は常に警報器を稼働させる。その他の領域※1も対象とする。

※1 例えば、コンピュータ室又は通信室

7a-7.4.3　監視システムの設計は機密性を維持する。

（7a-7.4.3参考）　これは、漏えいすると、検知されずに侵入することが容易になるためである。

7a-7.4.4　監視システムは、動画などの監視情報が、認可されていない人によってアクセスされることを防止するため、又はシステムが遠隔から無効にされることを防止するために、認可されていないアクセスから保護する。

7a-7.4.5　警報システムの制御盤は警報付きの領域に配置する。

7a-7.4.6　安全警報の場合は、警報を設定した人が簡単に出られるような場所に配置する。

7a-7.4.7　制御盤及び検知器は不正防止（tamperproof）の仕組みをもつ。

7a-7.4.8　システムは、意図したとおり作動していることを確実にするため定期的に試験する※1。

※1 システムの構成要素がバッテリ駆動の場合は特に試験が重要である。

7a-7.4.9　監視及び記録の仕組みは、特に要員の監視及び記録された映像の保持期間に関して、データ保護及びPII保護の法令を含む地域の法規制を考慮して使用する。

### 7a-7.5　物理的及び環境的脅威からの保護

管理策：自然災害及びその他の意図的又は意図的でない、インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し、実装する。

目的：　物理的及び環境的脅威に起因する事象の結果を防止又は低減するため。

詳細管理策

7a-7.5.1　物理的及び環境的脅威がもたらす潜在的な結果を特定するためのリスクアセスメントは、物理的な場所で重要な運用を開始する前に、及び定期的に実施する。

7a-7.5.2　必要な物理的及び環境的脅威からの保護策を実施し、また、物理的及び環境的脅威の変化を監視する。

7a-7.5.3　火災、洪水、地震、爆発、暴力行為、有毒廃棄物、環境排出物、その他の自然災害又は人的災害などの物理的及び環境的脅威から生じるリスクを管理する方法について、専門家の助言を得る。

7a-7.5.4　物理的施設の場所及び建造物では、次のことを考慮に入れる。

a) 適切な標高、水域、構造断層線など、現地の地形

b) 政治不安、犯罪活動又はテロ攻撃を誘発する可能性が高い場所など、都市の脅威

7a-7.5.5　リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の採用を考慮する。

a) 火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知し、警報を送信する又は消火システムを起動することができるシステムを設置し、構成する。消火は、周囲の環境に対して最も適切な物質を使用して実施する※1。

※1 例えば、閉鎖空間におけるガス

b) 洪水：記憶媒体又は情報処理システムを含む領域の床の下に、洪水を早期に検知できるシステムを設置する。洪水が発生した場合に水ポンプ又は同等の手段をすぐに利用できるようにする。

c) 電気サージ：サーバ及びクライアントの両方の情報システムを電気サージ又は同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。

d) 爆発物及び武器：取扱いに慎重を要する情報処理施設に入る要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。

### 7a-7.6　セキュリティを保つべき領域での作業

管理策：セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施する。

目的：　セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び認可されていない干渉から保護するため。

詳細管理策

7a-7.6.1　セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。

7a-7.6.2 セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。

a) 要員には、セキュリティを保つべき領域の存在又はその領域内での活動を、知る必要性の原則に基づく範囲でだけ認識させる。

b) 安全面の理由のため及び悪意のある活動の機会を低減するための両面から、セキュリティを保つべき領域での監督されていない作業は、回避する。

c) セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に検査する。

d) 画像、映像、音声又はその他の記録装置※1は、認可されたもの以外は許可しない。

※1 例えば、利用者エンドポイント機器に付いたカメラ

e) セキュリティを保つべき領域での利用者エンドポイント機器の携行及び使用を適切に管理する。

f) 見やすいように又はアクセスできるように緊急手順を掲示する。

## 7a-7.7 クリアデスク・クリアスクリーン

管理策：書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。

目的： 通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。

詳細管理策

7a-7.7.1 組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。

7a-7.7.2 クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。

a) 取扱いに慎重を要する業務情報又は重要な業務情報※1は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管しておく。

※1 例えば、紙又は電子記憶媒体上の業務情報

b) 使用していないとき又は離席時には、施錠又はその他のセキュリティ手段によって利用者エンドポイント機器を保護する。

c) 利用者エンドポイント機器は、離席時には、ログオフ状態にしておくか、又は利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をもつ構成とする。

d) 印刷を実行した人に、プリンタ又は複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの横に立ったときにだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。

e) 取扱いに慎重を要する情報を含む文書及び取外し可能な記憶媒体をセキ

ュリティを保って保管し、不要になった場合はセキュリティを保った処分の仕組みを使用してそれらを破棄する。

f) 画面上のポップアップの設定に関する規則及び手引を確立し、伝達する※1。

※1 例えば、プレゼンテーション、画面共有の際、又は公共の場所においては、可能であれば新しい電子メール及びメッセージングのポップアップを抑止する。

g) 不要になった場合には、ホワイトボード上及びその他の種類の掲示上の取扱いに慎重を要する情報又は重要な情報を消去する。

7a-7.7.3 組織は、組織の資産※1を後に残さないことを確実にするために、退出する前に最後の清掃を行うことを含む、施設から退去する際の適切な手順をもつ。

※1 例えば、引き出し又は収納用具の後ろに落ちた文書など

## 7b 装置の管理

### 7b-7.8 装置の設置及び保護

管理策：装置は、セキュリティを保って設置し、保護する。

目的： 物理的及び環境的脅威、並びに認可されていないアクセス及び損傷によるリスクを低減するため。

詳細管理策

7b-7.8.1 装置を保護するために、次の事項を考慮する。

a) 装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。

b) 取扱いに慎重を要するデータを扱う情報処理設備は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するために、その位置を慎重に定める。

c) 潜在的な物理的及び環境的脅威※1のリスクを最小限に抑えるための管理策を採用する。

※1例えば、盗難、火災、爆発、ばい（煤）煙、水（又は給水の不具合）、じんあい（塵埃）、振動、化学的汚染、電力供給の妨害、通信妨害、電磁波放射、破壊

d) 情報処理施設・設備の周辺での飲食及び喫煙に関する指針を確立する。

e) 情報処理施設・設備の運用に悪影響を与える可能性がある環境条件※1を監視する。

※1 例えば、温度、湿度

f) 全ての建物に、落雷からの保護を適用する。全ての電力及び通信の引込線に避雷器を装着する。

g) 作業現場などの環境にある装置には、特別な保護方法※1の使用を考慮する。

※1 例えば、キーボードカバー

h) 電磁波の放射による情報漏えいのリスクを最小限にするため、秘密情報を処理する装置を保護する。

i) 組織が管理する情報処理施設・設備を、組織が管理していない情報処理施設・設備から物理的に分離する。

## 7b-7.9　構外にある資産のセキュリティ

管理策：構外にある資産を保護する。

目的：構外にある装置・機器の紛失、損傷、盗難又は侵害、及び組織の業務の中断を防止するため。

詳細管理策

（7b-7.9参考）　組織が所有する装置・機器、及び個人が所有し組織のために用いる機器［私物機器の業務利用（BYOD）］を含む、情報を保管又は処理する、組織の構外で使用する装置・機器※1は全て保護する必要がある。

※1 例えば、モバイル機器

7b-7.9.1　構外にある装置・機器の使用は、管理者によって認可される。

7b-7.9.2　組織の構外で情報を保管又は処理する装置・機器の保護のために、次の事項を考慮する。

a）構外に持ち出した装置・機器及び記憶媒体は、公共の場所で、かつ、セキュリティが保たれない場所に無人状態で放置しない。

b）装置・機器の保護※1に関する製造業者の指示を常に守る。

※1 例えば、強力な電磁場、水、熱、湿度、ほこり（埃）にさらすことに対する保護

c）構外にある装置・機器を、複数の個人又は利害関係者の間で移動する場合には、その装置・機器の受渡記録を明記した記録（少なくとも、その装置・機器に対して責任を負う者の氏名及び組織を含むもの）を維持する。資産とともに移動する必要のない情報は、移動前にセキュリティを保って削除する。

d）必要かつ実施可能な場合には、組織の構内から装置・機器及び媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する※1。

※1 5b-5.14参照

e）公共交通機関において機器※1上の情報を見ること、及びのぞき見に関連するリスクに対して保護する。

※1 例えば、モバイル又はラップトップ

f）機器の位置追跡及び遠隔データ消去機能を実装する。

（7b-7.9.2参考）　組織の構外に装置※1を恒久的に設置すると、損傷、盗難又は傍受のリスクが高くなる可能性がある。これらのリスクは、場所によってかなり異なる可能性がある。

※1 アンテナ、現金自動預け払い機（ATM）など

7b-7.9.3　装置を恒久的に設置する構外のそれぞれの場所に応じた最も適切な対策の決定には、リスクを考慮する。

7b-7.9.4　装置を組織の構外に恒久的に設置する場合、次の事項を考慮する。

a）物理的セキュリティの監視※1

※1 7a-7.4参照

b）物理的及び環境的脅威からの保護※1

※1 7a-7.5参照

c）物理的アクセス制御及び不正防止（tamper proofing）の管理策

d）論理的アクセス制御

## 7b-7.10　記憶媒体

管理策：記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、その取得、使用、移送及び廃棄のライフサイクルを通して管理する。

目的：　記憶媒体上の情報に対して認可された開示、変更、移動又は破棄だけがなされることを確実にするため。

詳細管理策

**【取外し可能な記憶媒体】**

7b-7.10.1　取外し可能な記憶媒体の管理において、次の事項を考慮する。

a) 取外し可能な記憶媒体の管理に関するトピック固有の方針を確立し、取外し可能な記憶媒体を使用する又は取り扱う全ての人にトピック固有の方針を伝達する。

b) 必要かつ実施可能な場合には、組織から記憶媒体を搬出する場合に認可を要求し、監査証跡を残すために搬出の記録を保持する。

c) 全ての記憶媒体は、情報の分類に従って安全でセキュリティが保たれた環境に保管し、製造業者の仕様に従って、環境の脅威（熱、水分、湿度、電場、経年劣化など）から保護する。

d) 情報の機密性又は完全性が重要な考慮事項である場合は、取外し可能な記憶媒体上の情報を保護するために、暗号技術を用いる。

e) 保管した情報がまだ必要な間に記憶媒体が劣化するリスクを軽減するため、読み出せなくなる前に情報を新しい記憶媒体に移し替える。

f) 価値の高い情報は、一斉に損傷又は消失するリスクをより低減するために、複数の複製を別の記憶媒体に保管する。

g) 情報を失う危険性を小さくするために、取外し可能な記憶媒体の登録を検討する。

h) 取外し可能な記憶媒体のポート※1は、組織にその利用について理由があるときにだけ有効とする。

※1 例えば、セキュアディジタル（SD）カードスロット及びユニバーサルシリアルバス（USB）ポート

i) 取外し可能な記憶媒体を用いる必要がある場合、そのような記憶媒体への情報の転送を監視する。

j) 情報は、物理的な輸送中、例えば、郵便サービス又は宅配便で記憶媒体を送る場合に、認可されていないアクセス、不正使用又は破損に関してぜい弱である可能性がある。

（7b-7.10.1参考）　この管理策では、媒体は紙の文書を含んでいる。物理的記憶媒体を輸送する場合には、5b-5.14のセキュリティ対策を適用する。

**【セキュリティを保った再利用又は処分】**

7b-7.10.2　認可されていない者に秘密情報が漏えいするリスクを最小化するために、記憶媒体のセキュリティを保った再利用又は処分の手順を確立する。

7b-7.10.3　秘密情報を格納した記憶媒体の、セキュリティを保った再利用又は処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。

7b-7.10.4　記憶媒体のセキュリティを保った再利用又は処分の管理策の実施については、次の事項を考慮する。

a) 秘密情報を含む記憶媒体を組織内で再利用する必要がある場合には、セキュリティを保ってデータを消去するか、又は再利用する前に記憶媒体をフォーマットする※1。

※1 8b-8.10参照

b) 秘密情報を含む記憶媒体は、必要でなくなったときはセキュリティを保って処分する※1。

※1 例えば、内容を破壊、細断又はセキュリティを保って消去することによって

c) セキュリティを保った処分を必要とする可能性のある品目を特定する手順をもつ。

d) 多くの業者が、記憶媒体の収集及び処分のサービスを提供している。十分な管理策及び経験をもつ適切な外部の供給者を選定することに、注意を払う。

e) 監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録しておく。

f) 処分のために記憶媒体を集める場合、集積することによる影響に配慮する。取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に変わる場合がある。

7b-7.10.5　取扱いに慎重を要するデータを含んだ装置・機器が損傷した場合には、リスクアセスメントを実施し、修理又は廃棄に出すよりも物理的に破壊する方が望ましいか否かを決定する※1。

※1 7b-7.14参照

## 7b-7.11　サポートユーティリティ

管理策：情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護する。

目的：　サポートユーティリティの故障及び中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、又は組織の運用の中断を防止するため。

詳細管理策

7b-7.11. 1　組織は、情報処理施設・設備をサポートするユーティリティ※1に依存している。そのため、組織は次の事項を行う。

※1 例えば、電気、通信サービス、給水、ガス、下水、換気、空調

a) ユーティリティを支援する装置を、関連する製造業者の仕様に従って構成し、操作し、保守することを確実にする。

b) ユーティリティが事業の成長及び他のサポートユーティリティとの相互作用に対応する能力を、定期的に評価することを確実にする。

c) ユーティリティを支援する装置が適切に機能することを確実にするために、定期的に検査し、試験することを確実にする。

d) 必要であれば、ユーティリティの不具合を検知するための警報装置を取

り付ける。

e) 必要であれば、物理的な経路が異なる複数の供給元をユーティリティに備えることを確実にする。

f) ユーティリティを支援する装置がネットワークに接続されている場合、情報処理施設・設備から分離したネットワーク上にあることを確実にする。

g) ユーティリティを支援する装置を、必要な場合だけ、かつ、セキュリティを保った方法でだけインターネットに接続することを確実にする。

7b-7.11.2 サポートユーティリティのための非常用の照明及び通信手段を備える。

7b-7.11.3 非常口又は設備室の近くに、電源、給水、ガス又はその他のユーティリティを遮断するための緊急スイッチ及び緊急バルブを設置する。

7b-7.11.4 緊急連絡先の詳細を記録し、停止した場合に要員が利用できるようにする。

## 7b-7.12 ケーブル配線のセキュリティ

管理策：電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護する。

目的： 電源ケーブル及び通信ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。

詳細管理策

7b-7.12.1 ケーブル配線のセキュリティのために、次の事項を考慮する。

a) 情報処理施設・設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設するか、又は床ケーブル保護装置、電柱など、これに代わる十分な保護手段を施す。ケーブルが地下にある場合は、偶発的な切断から保護する※1。

※1 例えば、外装電線管又はケーブルの存在を示す表示を利用して

b) 干渉を防止するために、電源ケーブルは、通信ケーブルから隔離する。

c) 取扱いに慎重を要するシステム又は重要なシステムのために、次の追加の管理策の採用を検討する。

1) 外装電線管の導入。点検箇所・終端箇所の施錠可能な部屋又は箱への設置及び警報装置の設置

2) ケーブルを保護するための電磁遮蔽の利用

3) ケーブルに取り付けられた認可されていない装置・機器を検知するための定期的な技術的探索及び物理的検査

4) 配線盤、端子盤及びケーブル室への管理されたアクセス※1

※1 例えば、物理鍵又はPINを用いる。

5) 光ファイバーケーブルの使用

d) ケーブル配線の物理的識別及び検査を可能にするために、ケーブルの各端に始点及び終点に関する十分な詳細情報をラベル付けする。

7b-7.12.2 ケーブルに関するインシデント又は不具合から生じるリスクを管理する方法について、専門家の助言を求める。

### 7b-7.13　装置の保守

管理策：装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守する。

目的：　不十分な保守による、情報及びその他の関連資産の消失、損傷、盗難又は侵害、並びに組織の運用の中断を防止するため。

詳細管理策

7b-7.13.1　装置の保守のために、次の事項を考慮する。

a) 装置は、供給者の推奨するサービスの頻度及び仕様に従って保守する。

b) 組織の保守プログラムを実施し、監視する。

c) 認可された保守要員だけが、装置の修理及び保守を実施する。

d) 故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。

e) 装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。

f) 構内で保守を実施する場合は保守要員を監督する。

g) 遠隔保守のためのアクセスを認可し、管理する。

h) 情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティ※1の対策を適用する。

※1 7b-7.9参照

i) 保険において課される全ての保守要求事項を順守する。

j) 保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。

k) 装置を処分することに決定した場合、装置のセキュリティを保った処分又は再利用※1の対策を適用する。

※1 7b-7.14参照

### 7b-7.14　装置のセキュリティを保った処分又は再利用

管理策：記憶媒体を内蔵した装置は、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てるよう上書きしていることを確実にするために、検証する。

目的：　処分又は再利用する装置からの情報漏えいを防止するため。

詳細管理策

7b-7.14.1　装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。

7b-7.14.2　秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。

7b-7.14.3　秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。

（7b-7.14.3参考）　記憶媒体のセキュリティを保った処分に関する詳細な手引については7b-7.10を、情報の削除に関する手引については8b-8.10を参照。

7b-7.14.4　組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は慈善団体への寄付を含む処分を行う前に除去する。

7b-7.14.5　組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。

（7b-7.14.5参考）　これは、次のような要因に依存する。

a）施設を元の状態に戻すリース合意

b）次のテナントに対して、取扱いに慎重を要する情報を含むシステムが残されるリスクの最小化※1

※1 例えば、利用者アクセスのリスト、映像又は画像ファイル

c）移転先の施設で管理策を再利用できること

# 8　技術的管理策

## 8a　情報アクセスの管理

### 8a-8.1　利用者エンドポイント機器

管理策：利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護する。

目的：　利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。

詳細管理策

**【技術的管理策全般】**

8a-8.1.1　組織は、利用者エンドポイント機器のセキュリティを保った構成及び取扱いに関するトピック固有の方針を確立する。

8a-8.1.2　利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。

a）利用者エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル

b）利用者エンドポイント機器の登録

c）物理的保護についての要求事項

d）ソフトウェアのインストールの制限※1

※1 例えば、システムの実務管理者が遠隔で管理する。

e）利用者エンドポイント機器のソフトウェア（ソフトウェアの版を含む。）の要求事項及び更新の適用の要求事項※1

※1 例えば、動的自動更新

f）情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則※1

※1 例えば、パーソナルファイアウォールの使用を求める。

g）アクセス制御

h）記憶装置の暗号化

i) マルウェアからの保護

j) 遠隔操作による機器の無効化、データの消去又はロック

k) バックアップ

l) ウェブサービス及びウェブアプリケーションの使用

m) エンドユーザーの行動の分析※1

※1 8b-8.16参照

n) 取外し可能なメモリ装置を含む取外し可能な機器の使用、及び物理ポート※1を無効化できる可能性

※1 例えば、USBポート

o) 利用者エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産※1を、機器上の他の情報及びその他の関連資産からセキュリティを保って分離することが可能である。

※1 例えば、ソフトウェア

8a-8.1.3 ある情報が特に慎重な取扱いを要する場合に、利用者エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。

(8a-8.1.3参考) その場合、機器に追加の技術的保護手段が必要になる可能性がある。例としては、オフライン作業のためのファイルのダウンロードの無効化、及びSDカードなどのローカルストレージの無効化を確実にすることがある。

8a-8.1.4 可能な限り、利用者エンドポイント機の管理策に関する推奨事項を、構成管理※1又は自動化されたツールによって強制する。

※1 8b-8.9参照

**【利用者の責任】**

8a-8.1.5 利用者エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する自らの責任について、全ての利用者に認識させる。

8a-8.1.6 利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように助言する。

a) 利用者エンドポイント機器を利用する必要がなくなったら、実行していたセッションからログオフし、サービスを終了する。

b) 利用者エンドポイント機器は、利用していない場合、物理的管理策※1及び論理的管理策※2を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。

※1 例えば、キーロック又は特殊ロック

※2 例えば、パスワードアクセス

c) 公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する※1。

※1 例えば、他人が背後から読むことが可能な場合に秘密情報を読むことは避ける、また、プライバシースクリーンフィルタを使用する。

d) 利用者エンドポイント機器を盗難から物理的に保護する※1。

※1 例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所において

8a-8.1.7　利用者エンドポイント機器の盗難又は紛失に備えて、法令、規制、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。

**【個人所有の機器の使用】**

8a-8.1.8　個人所有の機器※1の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。

※1 BYODとしても知られる。

a) 機器の個人使用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。

b) 利用者が自らの義務（物理的保護、ソフトウェアの更新など）を受け入れた場合にだけ、業務情報にアクセスできるようにする。業務データについて帰属を主張しないこと、及び機器の盗難若しくは紛失があった場合又はサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。こうした場合、PII保護に関する法令を考慮する。

c) 個人所有の機器で開発された知的財産権に関する紛争を防止するためのトピック固有の方針及び手順

d) 個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）。これは法令で禁止されている場合がある。

e) 要員又は外部組織の利用者が個人で所有する利用者エンドポイント機器上のクライアントソフトウェアについて、ライセンスを受ける責任を組織が負うことになる可能性があるソフトウェアライセンス契約

**【無線接続】**

8a-8.1.9　組織は、利用者エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。

a) 機器の無線接続の構成※1

※1 例えば、ぜい弱なプロトコルを無効化する。

b) 関連するトピック固有の方針に従って適切な帯域幅の無線又は有線接続を使用すること※1

※1 例えば、バックアップ又はソフトウェア更新が必要であるため。

### 8a-8.2　特権的アクセス権

管理策：特権的アクセス権の割当て及び利用は、制限し、管理する。

目的：　認可された利用者、ソフトウェア構成要素及びサービスだけに特権的アクセス権が与えられることを確実にするため。

詳細管理策

8a-8.2.1　特権的アクセス権の割当ては、アクセス制御に関するトピック固有の方針※1に従って、認可プロセスによって管理する。

※1 5c-5.15参照

8a-8.2.2　この管理策の実施については、次の事項を考慮する。

a) 各々のシステム又はプロセス※1の特権的アクセス権を必要とする利用者を特定する。

※1 例えば、オペレーティングシステム、データベース管理システム、アプリケーション

b) 特権的アクセス権を、アクセス制御に関するトピック固有の方針※1に沿って、必要に応じて、かつ、事象ごとに、利用者に割り当てる（すなわち、特権的アクセスを必要とする活動を実行するために必要な力量をもつ個人に対してだけ、かつその個人の職務上の役割のための最小限の要求に基づいて）。

※1 5c-5.15参照

c) 特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない。）及び割り当てた全ての特権の記録を維持する。

d) 特権的アクセス権の終了に関する要求事項を定め、実施する。

e) 利用者が、自らが特権的アクセス権をもっていること、及び自らがいつ特権的アクセスモードになっているかを認識することを確実にするための対策を講じる。考えられる対策としては、特別の利用者識別情報、利用者インタフェース設定、又は特別の装置の使用が含まれる。

f) 特権的アクセス権における認証の要求事項は、通常のアクセス権における要求事項よりも要求が高くなる場合がある。特権的アクセス権を用いて作業を行う前に、再認証又は認証の格上げが必要になる場合がある。

g) 定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任及び力量の点で今も適格であるかどうかを検証する※1。

※1 5c-5.18参照

h) 汎用の実務管理者ID※1の使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのようなID の認証情報を管理し、保護する※2。

※1 “root”など

※2 5c-5.17参照

i) 特権的アクセス権を永続的に許可するのではなく、承認された変更又は活動※1を実施するのに必要な時間枠だけ一時的な特権的アクセスを許可する。これはしばしばブレークグラス手順（break glass procedure）と呼ばれ、しばしば特権的アクセス管理技術において自動化されている。

※1 例えば、保守活動又は一部の重要な変更

j) 監査の目的で、システムへの全ての特権的アクセスのログを記録する。

k) 特権的アクセス権をもつ識別情報を複数の人で共有又は連携することはせず、特定の特権的アクセス権の割当てが許可された個別の識別情報を各人に割り当てる。特権的アクセス権の管理を簡素化するために、識別情報をグループ化することが可能である※1。

※1 例えば、実務管理者グループを定義することによって

l）特権的アクセス権をもつ識別情報は、管理作業を実行するためだけに使用し、日常の一般的な職務（すなわち、電子メールの確認、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ。）。

### 8a-8.3　情報へのアクセス制限

管理策：情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限する。

目的：　情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。

詳細管理策

8a-8.3.1　情報及びその他の関連資産へのアクセスは、確立されたトピック固有の方針に従って制限する。

8a-8.3.2　アクセス制限の要求事項を満たすために、次の事項を考慮する。

a）未知の利用者識別情報又は匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。公開アクセス又は匿名アクセスは、取扱いに慎重を要する情報を含まない保管場所にだけ許可する。

b）システム、アプリケーション及びサービスにもつ情報へのアクセスを制御するための構成の仕組みを提供する。

c）利用者がアクセスできるデータを制御する。

d）どの識別情報又は識別情報のグループがどのアクセス権※1をもつかを制御する。

※1 読出し、書込み、削除、実行など

e）取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。

8a-8.3.3　次の場合には、組織にとって高い価値をもつ取扱いに慎重を要する情報を保護するための動的アクセス管理手法及びプロセスの採用を検討する。

a）誰がどの期間、どのように情報にアクセスできるかを細かく制御する必要がある。

b）情報を組織外の人々と共有し、誰がそれにアクセスできるかを制御する。

c）情報の使用及び配布をリアルタイムで動的に管理する。

d）認可されていない変更、複製及び配布（印刷を含む。）から情報を保護する。

e）情報の使用を監視する。

f）将来、調査が必要になった場合に備えて、情報の変更を記録する。

8a-8.3.4　動的アクセス管理手法は、次の事項を含め、情報をそのライフサイクル（すなわち、作成、処理、保存、送信及び処分）を通じて保護する。

a）次の事項を考慮して、個別の事例に基づき動的アクセス管理に関する規則を確立する。

1) 識別情報、装置・機器、場所又はアプリケーションに基づいてアクセス許可を与える。

2) 動的アクセス管理手法を用いてどの情報を保護する必要があるかを決定するために分類体系を活用する。

b) 運用、監視及び報告のプロセスを確立し、技術基盤を支援する。

8a-8.3.5 動的アクセス管理システムは、次の方法によって情報を保護する。

a) 情報にアクセスする際に、認証、適切な資格情報又は証明書を要求する。

b) アクセスを、例えば、規定された時間枠※1に制限する。

※1 所定の日付以後、特定の日付までなど

c) 情報を保護するために暗号化を利用する。

d) 情報の印刷許可を定義する。

e) 誰が情報にアクセスし、その情報がどのように使用されたかを記録する。

f) 情報の悪用の試みが検知された場合に警報を上げる。

## 8a-8.4 ソースコードへのアクセス

管理策：ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理する。

目的： 認可されていない機能が入り込むことを防止し、意図しない又は悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。

詳細管理策

8a-8.4.1 ソースコード、関連書類※1及び開発ツール※2へのアクセスは、厳重に管理する。

※1 例えば、設計書、仕様書、検証計画書、妥当性確認計画書

※2 例えば、コンパイラ、ビルダ、統合ツール、テストプラットフォーム及びテスト環境

(8a-8.4.1参考) ソースコードについては、できればソースコード管理システムにおいて、コードを集中保管して管理することによってこれを達成することが可能である。

8a-8.4.2 ソースコードへの読取りアクセス及び書込みアクセスは、必要に応じて要員の役割に基づいて制限する。

(8a-8.4.2参考) 例えば、ソースコードへの読取りアクセスは組織内で広く提供することはできるが、ソースコードへの書込みアクセスは、特権をもつ要員又は指定された管理責任者だけに認める。

8a-8.4.3 コード部品を組織内の複数の開発者が使用する場合には、一元化したコードリポジトリへの読取りアクセスを提供する。

8a-8.4.4 オープンソースコード又は第三者のコード部品の一元化した外部コードリポジトリへの書込みアクセスは制限する。

8a-8.4.5 コンピュータプログラムが破壊される危険性の低減を目的として、プログラムソースライブラリへのアクセスを管理するために、次の事項を考慮する。

a) プログラムソースコード及びプログラムソースライブラリへのアクセス

は、確立した手順に従って管理する。

b) ソースコードへの読取り及び書込みアクセスの許可は、業務上のニーズに基づき、変更又は悪用のリスクに対処するために管理し、かつ、確立された手順に従って行う。

c) ソースコード及び関連情報の更新、並びにソースコードへのアクセスの許可は、変更管理手順※1に従って行い、かつ、適切な認可を得た後にだけ実施する。

※1 8d-8.32参照

d) 開発者にソースコードリポジトリへの直接アクセスは許可せず、ソースコードに関する活動及び認可を管理する開発者ツールを通じて許可する。

e) プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。

f) ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。

8a-8.4.6 プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策※1の使用を考慮する。

※1 例えば、ディジタル署名

## 8a-8.5 セキュリティを保った認証

管理策：セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。

目的： システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。

詳細管理策

8a-8.5.1 利用者、ソフトウェア、メッセージ、及びその他のエンティティが提示する識別情報を検証するために、適切な認証技術を選択する。

8a-8.5.2 認証の強度は、アクセスする情報の分類に適したものを選択する。

8a-8.5.3 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、ディジタル証明書、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。

8a-8.5.4 重要な情報システムにアクセスするために、認証情報に追加の認証要素を加える※1。

※1 多要素認証とも呼ばれる。

(8a-8.5.4参考1) 知識、所持物、生体情報など、複数の認証要素を組み合わせて使用することで、認可されていないアクセスの可能性を減らすことが可能である。

(8a-8.5.4参考2) 特定の状況下においては、多要素認証に他の手法も組み合わせて、あらかじめ定義したルール及びパターンに基づく追加の要素も条件として要求することが可能である。このルール及びパターンには、通常と異なる場所からのアクセス、通常と異なる装置・機器からのアクセス、通常と異なる時間でのアクセスなどがある。

8a-8.5.5 生体認証情報は、機密性が損なわれた場合は無効化する。

8a-8.5.6 使用の条件※1によっては、生体認証が利用できないことに備えるため、生体認証は少なくとも一つの代替の認証手法をもつ。

※1 例えば、湿気又は加齢

8a-8.5.7 システム又はアプリケーションにログオンする手順は、認可されていないアクセスのリスクを最小限に抑えるように設計する。

8a-8.5.8 ログオンの手順及び技術は、次の事項を考慮して実装する。

a) 認可されていない利用者に不必要な手助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。

b) “システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定する”という一般的な警告を表示する。

c) ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない※1。

※1 例えば、エラー状態が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを示すことは望ましくない。

d) ログオン情報の妥当性確認は、全ての入力データが完了した時点でだけ行う。

e) 利用者名及びパスワードに関する総当たり攻撃でログオンしようとする試みから保護する※1。

※1 例えば、コンピュータと人間とを区別する完全に自動化された公開チューリングテスト（CAPTCHA）を使用する、あらかじめ定義した回数の試行失敗の後にパスワードリセットを要求する、又は最大と定めた回数のエラーの後に利用者をブロックする。

f) 失敗した試み及び成功した試みのログをとる。

g) ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる※1。

※1 例えば、誤ったパスワードの試行が特定の回数に達したときに利用者及び組織のシステム実務管理者に警告を送信する。

h) ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。

1) 前回成功裏にログオンできた日時

2) 前回のログオン以降、失敗したログオンの試みがある場合は、その詳細

i) 入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある※1。

※1 例えば、アクセシビリティのために、又はエラーの繰返しによって利用者がブロックされないようにするために

j) ネットワーク“スニファ”プログラムで捕捉されることを避けるため、ネットワークを介してパスワードを平文で通信しない。

k) リスクの高い場所※1では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。

※1 例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、利用者エンドポイント機器

l) リスクの高いアプリケーションのセキュリティを高め、認可されていな

いアクセスの危険性を低減するために、接続の継続時間を制限する。

### 8a-8.6　容量・能力の管理

管理策：現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。

目的：　情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。

詳細管理策

8a-8.6.1　事業におけるシステム及びプロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。

8a-8.6.2　システムの可用性及び効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び監視を適用する。

8a-8.6.3　組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及びサービスの負荷テストを実施する。

8a-8.6.4　適切な時点で問題を知らせるために、検知のための管理策を備える。

8a-8.6.5　将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。

8a-8.6.6　入手に長い期間又は高額な費用がかかる資源については、特別な注意を払うため、管理者、及びサービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。

8a-8.6.7　システムセキュリティ又はサービスに脅威をもたらす可能性のある、潜在的な資源の制限及び主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する情報を用い、また、適切な処置を立案する。

（8a-8.6参考）　十分な容量・能力の提供は、容量・能力の増強又は需要の低減によって達成することが可能である。

8a-8.6.8　容量・能力を増強するには、次の事項を考慮する。

a）新しい要員を雇用する。

b）新しい施設又は場所を取得する。

c）より強力な処理システム、メモリ及びストレージを取得する。

d）容量・能力の課題に直接に応えるという特性があるクラウドコンピューティングを利用する。クラウドコンピューティングは、特定のアプリケーション及びサービスで利用できる資源を要求に応じて迅速に拡張し、削減することを可能とする、弾力性及びスケーラビリティをもっている。

8a-8.6.9　組織の資源に関する需要を減らすために、次の事項を考慮する。

a）古いデータの削除（ディスクスペース）

b）保持期間を満了したハードコピー記録の処分（棚スペースを空ける。）

c）アプリケーション、システム、データベース又は環境の廃止

d）バッチのプロセス及びスケジュールの最適化

e) アプリケーションコード及びデータベースへの問合せの最適化

f) 重要でない場合、大量の帯域を必要とするサービス※1に対する帯域割当ての拒否又は制限

※1 例えば、動画のストリーミング

8a-8.6.10 業務上必須のシステムについては、容量・能力の管理計画を文書化することを検討する。

## 8b 情報資産運用に関する管理

### 8b-8.7 マルウェアに対する保護

管理策：マルウェアに対する保護を実施し、利用者の適切な認識によって支援する。

目的： 情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。

詳細管理策

8b-8.7.1 マルウェアに対する保護は、マルウェアの検出・修復ソフトウェア、情報セキュリティに対する認識、及びシステムへの適切なアクセス・変更管理についての管理策に基づく。

（8b-8.7.1参考） 通常、マルウェアの検出・修復ソフトウェアを単独で使用することは十分ではない。

8b-8.7.2 マルウェアに対する保護については、次の手引を考慮する。

a) 認可されていないソフトウェアの使用を防止又は検出するための規則及び管理策の実施※1

※1 例えば、アプリケーションの許可リスト（すなわち、許可されたアプリケーションを示すリストの使用）（8b-8.19及び8d-8.32参照）

b) 悪意のあるウェブサイトであると知られている又は疑われるウェブサイトの使用を、防止又は検出するための管理策の実施※1

※1 例えば、ブロックリスト

c) マルウェアに付け込まれる可能性のあるぜい弱性を減らす※1。

※1 例えば、技術的ぜい弱性管理によって（8b-8.8及び8b-8.19参照）

d) システム、特に重要な業務プロセスを支えるシステムのソフトウェア及びデータについて、定常的な自動化された妥当性確認の実施。承認されていないファイル又は認可されていない変更の存在を調査する。

e) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクに対する保護対策を確立する。

f) コンピュータ及び電子記憶媒体をスキャンするための、マルウェアの検出・修復ソフトウェアの導入及び定常的な更新。次の事項を含む定常的なスキャンを実施する。

1) ネットワーク経由又は何らかの形式の電子記憶媒体を通じて入手した全てのデータに対する、マルウェア検出のための使用前のスキャン

2) 電子メール及びインスタントメッセージングの添付ファイル及びダウンロードしたファイルに対する、マルウェア検出のための使用前のスキャン。このスキャンは、様々な場所※1で、及び組織のネット

ワークの入口で実施する。

※1 例えば、電子メールサーバ、デスクトップコンピュータ

3) ウェブページに対するアクセスの際のマルウェア検出のためのスキャン

g) リスクアセスメントの結果に基づき、かつ、次の事項を考慮して、マルウェアの検出・修復ツールの配置及び構成を決定する。

1) 特に効果的である場合には、多層防御の原則。例えば、これはネットワークゲートウェイ※1、並びに利用者エンドポイント機器及びサーバにおいて、マルウェアの検出につながる可能性がある。

※1 電子メール、ファイル転送、ウェブなどの様々なアプリケーションプロトコルにおけるネットワークゲートウェイ

2) 攻撃者がマルウェアを送り込むための回避技術※1、又はマルウェアの送信における暗号化プロトコルの使用

※1 例えば、暗号化されたファイルの使用

h) マルウェアに対する通常の管理策をう（迂）回する可能性がある、保守及び緊急時の手順中におけるマルウェアの入り込みの防止に注意を払う。

i) 例外承認権限、文書化した正当性の提示、及びレビューの日付を含む、マルウェアに対する一部又は全ての対策の一時的又は恒久的な無効化を認可するプロセスを実装する。これは、マルウェアに対する保護によって通常の運用が中断・阻害される場合に必要になる可能性がある。

j) マルウェアの攻撃から回復するための適切な事業継続計画の策定。これには、必要な全てのデータ及びソフトウェアのバックアップ（オンラインとオフラインとの両方のバックアップを含む。）並びに回復の対策を含める※1。

※1 8b-8.13参照

k) 壊滅的な影響が生じる可能性のある環境の隔離

l) システム上でマルウェアに対する保護を扱う手順及び責任の定義。これには、手順の使用、報告及びマルウェア攻撃からの回復に関する訓練を含む。

m) マルウェアに感染した電子メール、ファイル又はプログラムの受信、送信又はインストールを特定し、可能ならば軽減する方法について、全ての利用者に意識向上又は訓練※1を提供する※2。

※1 6a-6.3参照

※2 n)及びo)で収集された情報を、意識向上及び訓練を最新状態に保つことを確実にするために使用することが可能である。

n) 定常的に新種のマルウェアに関する情報を収集するための手順の実施※1

※1 例えば、メーリングリストへの登録又は関連するウェブサイトの確認

o) 警告情報などマルウェアに関する情報が適格で定評のある情報源※1から来ており、正確かつ役立つことを検証する。

※1 例えば、信頼できるインターネットサイト、マルウェア検出ソフトウェアの供給者

### 8b-8.8 技術的ぜい弱性の管理

管理策：利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。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し、適切な手段をとる。

目的：　技術的ぜい弱性の悪用を防止するため。

詳細管理策

**【技術的ぜい弱性の特定】**

8b-8.8.1　組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録※1をもつ。

※1 5b-5.9～5b-5.14参照

8b-8.8.2　資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況※1、及びそのソフトウェアに責任のある組織内の担当者を含める。

※1 例えば、どのソフトウェアがどのシステム上に導入されているか。

8b-8.8.3　技術的ぜい弱性を特定するために、組織は次の事項を考慮する。

a) 技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、更新、資産移動の追跡、及び要求される全ての調整責務が含まれる。

b) ソフトウェア及びその他の技術※1に関して、関連する技術的ぜい弱性を特定し、また、ぜい弱性を継続して認識するために用いる情報源を特定する。情報源のリストは、この目録を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。

※1 組織の資産目録リストに基づく。5b-5.9 参照

c) 情報システム（その構成要素を含む。）の供給者に、適用される契約に要求事項を含め、ぜい弱性の報告、取扱い及び開示を確実にすることを要求する※1。

※1 5d-5.20参照

d) ぜい弱性を特定し、ぜい弱性のパッチ適用が成功したかどうかを検証するために、使用している技術に適したぜい弱性スキャンツールを使用する。

e) ぜい弱性の特定を支援するために、力量があり認可された者が、計画され、文書化された、再現可能な侵入テスト又はぜい弱性アセスメントを実施する。この活動はシステムのセキュリティを危うくする可能性があるため、注意を払う。

f) 第三者のライブラリ及びソースコードの使用について、ぜい弱性を追跡する。これはセキュリティに配慮したコーディングに含める※1。

※1 8d-8.28参照

8b-8.8.4　組織は、次の事項のための手順及び能力を開発する。

a) 自らの製品及びサービス並びにこれらで使用している外部の構成要素について、ぜい弱性の存在を検知する。

b) 内部又は外部の供給元からぜい弱性報告を受け取る。

8b-8.8.5　組織は、調査者及び他の人が問題を報告できるように、ぜい弱性の開示に関するトピック固有の方針の一部として公開連絡先を示す。

8b-8.8.6　組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な脅威イ

ンテリジェンス又は情報共有の場を利用する。

8b-8.8.7　組織は、ぜい弱性を適切に修復するために、組織におけるぜい弱性の特定を支援する動機付けとして、報酬を提供するバグ報奨金プログラムの採用を検討する。

8b-8.8.8　組織が力量のある業界団体又は他の利害関係者と情報を共有する。

**【技術的ぜい弱性の評価】**

8b-8.8.9　特定した技術的ぜい弱性を評価するために、次の手引を考慮する。

a) どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。

b) 潜在的な技術的ぜい弱性を特定したときは、それに伴うリスク及び講じるべき処置を特定する。

（8b-8.8.9参考）　この処置は、ぜい弱性のあるシステムの更新又は他の管理策の適用を含む可能性がある。

**【技術的ぜい弱性に対処するための適切な対策の実施】**

8b-8.8.10　認可された全てのソフトウェアに、最新の承認済みパッチ及びアプリケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。

8b-8.8.11　変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。

8b-8.8.12　全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。

8b-8.8.13　必要に応じて、独立した評価機関がソフトウェアの変更を試験し、妥当性を確認する。

8b-8.8.14　技術的ぜい弱性に対処するために、次の手引を考慮する。

a) 潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムラインを定義する。

b) 技術的ぜい弱性への対処の緊急性に応じて、変更管理に関する管理策※1又は情報セキュリティインシデント対応手順※2に従って、処置を実行する。

※1 8d-8.32参照
※2 5e-5.26参照

c) 正当な供給元（組織の内部又は外部の可能性がある）からの更新だけを使用する。

d) 更新を適用する前に、それが有効であること及び耐えられない副作用をもたらさないことを確実にするために、更新を試験し、評価する※1。

※1 すなわち、更新が利用可能な場合、更新の適用に伴うリスクを評価する（ぜい弱性が引き起こすリスクを、更新を適用することのリスクと比較する。）。

e) リスクの高いシステムには最初に対処する。

f) 修復（一般にはソフトウェアの更新又はパッチ）を開発する。

g) 修復又は低減策が効果的であるかどうかを確認するために試験する。

h) 修復の真正性を検証する仕組みを提供する。

i) 利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。

1) ソフトウェア業者又はその他の関連供給元が提案する回避策を適用する。

2) そのぜい弱性に関係するサービス又は機能を停止する。

3) ネットワーク境界におけるアクセス制御※1を調整又は追加する※2。

※1 例えば、ファイアウォール

※2 8c-8.20～8c-8.22参照

4) ぜい弱なシステム、装置・機器又はアプリケーションを、適切なトラフィックフィルタ（ときに仮想パッチと呼ばれる。）を導入して攻撃から保護する。

5) 実際の攻撃を検知するために、監視を強化する。

6) そのぜい弱性に対する認識を高める。

8b-8.8.15 取得したソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリースし、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。

**【その他の考慮事項】**

8b-8.8.16 監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。

8b-8.8.17 技術的ぜい弱性の管理プロセスは、その有効性及び効率性を確実にするために、定常的に監視し、評価する。

8b-8.8.18 技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。

（8b-8.8.18参考） これは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を提供するためである。

8b-8.8.19 組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがその実施を確実に行うことを確認する。

8b-8.8.20 クラウドサービスの利用に関する合意には、次を含める。

a) 技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任

b) 技術的ぜい弱性に関するクラウドサービスプロバイダの対応を報告するプロセス※1

※1 5d-5.23参照

（8b-8.8.20参考） 一部のクラウドサービスの場合には、クラウドサービスプロバイダ及びクラウドサービスカスタマにそれぞれの責任が存在する。例えば、クラウドサービスカスタマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。

### 8b-8.9　構成管理

管理策：ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューする。

目的：　ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。

詳細管理策

**【構成管理全般】**

8b-8.9.1　組織は、ハードウェア、ソフトウェア、サービス※1及びネットワークに関して、新しく導入したシステム及び運用システムの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し、実装する。

※1 例えば、クラウドサービス

8b-8.9.2　全ての構成変更を良好に管理することを確実にするために、役割、責任及び手順を定める。

**【標準テンプレート】**

8b-8.9.3　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成のための標準テンプレートを次のように定義する。

a）公開され、入手できる手引※1を使用する。

※1 例えば、業者及び独立したセキュリティ組織による既定のテンプレート

b）十分なセキュリティレベルを決定するために、必要な保護のレベルを考慮する。

c）組織の情報セキュリティ方針、トピック固有の方針、標準及びその他のセキュリティ要求事項を支援する。

d）組織の状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。

8b-8.9.4　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートは、定期的にレビューすることに加えて、新しい脅威又はぜい弱性に対処する必要がある場合、又は新版のソフトウェア若しくはハードウェアを導入した場合に更新する。

8b-8.9.5　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートの策定に当たって、次の事項を考慮する。

a）特権的又は実務管理者レベルのアクセス権をもつ識別情報の数を最小限にする。

b）不必要な、使用されていない又はセキュリティが保たれていない識別情報を無効化する。

c）不必要な機能及びサービスを無効化又は制限する。

d）強力なユーティリティプログラム及びホストパラメータ設定へのアクセスを制限する。

e）クロックを同期させる。

f) 初期パスワードなどの業者による初期認証情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態をレビューする。

g) 既定の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。

h) 使用許諾の要求事項が満たされていることを検証する※1。

※1 5g-5.32参照

**【構成の管理】**

8b-8.9.6 ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録し、全ての構成変更のログを維持する。これらの記録はセキュリティを保って保管する。

(8b-8.9.6参考1) これは、構成データベース又は構成テンプレートなど様々な方法で達成することが可能である。

(8b-8.9.6参考2) 構成の変更は、変更管理プロセスに従う※1。

※1 8d-8.32参照

(8b-8.9.6参考3) 構成記録には、次の事項を含み得る。

a) 資産の最新の管理責任者又は連絡先情報

b) 構成の最終変更日

c) 構成テンプレートの版

d) その他の資産の構成との関係

**【構成の監視】**

8b-8.9.7 構成は、包括的なシステム管理ツール群※1を用いて監視する。

※1 例えば、保守ユーティリティ、遠隔サポート、エンタープライズ管理ツール、バックアップ及び復元ソフトウェア

8b-8.9.8 構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。

8b-8.9.9 実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。

## 8b-8.10 情報の削除

管理策：情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった時点で削除する。

目的： 取扱いに慎重を要する情報の不用意な漏えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を順守するため。

詳細管理策

**【情報の削除全般】**

8b-8.10.1 取扱いに慎重を要する情報は、望ましくない開示のリスクを減らすために、必要な期間より長く保持しない。

8b-8.10.2 システム、アプリケーション及びサービスに関する情報を削除する場合は、次の事項を考慮する。

a) 業務の要求事項に従い、また、関連する法令及び規制を考慮して、削除

手法※1を選択する。

※1 例えば、電子的な上書き又は暗号化消去

b) 削除の結果を証拠として記録する※1。

※1 情報の削除の正式記録は、生じ得る情報漏えい事象の原因を分析するときに役立つ。

c) 情報の削除を行うサービス提供者を利用する場合、サービス提供者から情報の削除の証拠を得る。

8b-8.10.3 第三者が組織に代わってその情報を保存する場合、組織は、情報の削除に関する要求事項を第三者との合意に含め、サービスの実施中及び終了時に実行させることを検討する。

**【削除手法】**

8b-8.10.4 組織のデータ保持に関するトピック固有の方針に従い、また、関連する法令及び規制を考慮して、取扱いに慎重を要する情報は、必要がなくなったとき、次の方法で削除する。

a) 必要でなくなったとき、情報をセキュリティを保って破壊するようにシステムを構成する※1。

※1 例えば、データ保持に関するトピック固有の方針に従って定義した期間の後に、又は対象のアクセス要求に応じて

b) 古い版、複製及び一時ファイルは、それらがどこにあっても削除する。

c) 情報を恒久的に削除し、専門家が使う復旧ツール又はフォレンジックツールを使用しても情報が復旧できないことを確実にする助けとするために、広く認められた、セキュリティを保った削除ソフトウェアを使用する。

d) 広く認められ、認定された、セキュリティを保った廃棄サービス提供者を利用する。

e) 処分する記憶媒体の種類に適した処分の仕組みを使用する※1。

※1 例えば、ハードディスクドライブ及びその他の磁気記憶媒体の消磁

8b-8.10.5 クラウドサービスを利用する場合、組織はクラウドサービスプロバイダが提供する削除手法が許容できるかどうかを検証し、許容できるならばそれを利用し、又はクラウドサービスプロバイダに情報の削除を要請する。

8b-8.10.6 削除プロセスは、利用可能かつ適用可能な場合には、トピック固有の方針に従って自動化する。

（8b-8.10.6参考） 削除する情報の、取扱いに慎重を要する度合いに応じて、ログによって、削除プロセスが実行されたことを追跡又は検証することが可能である。

8b-8.10.7 装置・機器を業者に返送するとき、取扱いに慎重を要する情報が意図せず漏えいすることを防止するために、装置・機器を組織の施設から出す前に、補助記憶媒体※1及びメモリを取り除くことによって、取扱いに慎重を要する情報を保護する。

※1 例えば、ハードディスクドライブ

8b-8.10.8 組織はその装置・機器で取り扱う情報の分類に従って適切な手法を選択する※1。

※1 一部の装置・機器（例えば、スマートフォン）では、セキュリティを保った情報の削除は、装置・機器の破壊又は装置・機器に組み込まれ

ている機能（例えば、“工場出荷時の設定の復元”）の使用によってだけ実施可能である。

8b-8.10.9　記憶装置を物理的に破壊し、同時にそこに含む情報を消去するために、7b-7.14にある対策を適用する。

## 8b-8.11　データマスキング

管理策：データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用する。

目的：　PIIを含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。

詳細管理策

8b-8.11.1　取扱いに慎重を要するデータ※1の保護が必要である場合、組織は仮名化、匿名化などを含むデータマスキングの手法※2を利用してそのデータを隠すことを検討する。

※1 例えば、PII
※2 データマスキング手法という。

（8b-8.11.1参考）　仮名化又は匿名化の手法では、次のことが可能である。

a）PIIのデータを隠す。
b）PII主体の真のアイデンティティ又はその他の取扱いに慎重を要する情報を偽装する。
c）PIIとPII主体のアイデンティティとの間のひも（紐）付け又は他の取扱いに慎重を要する情報との間のひも（紐）付けを切る。

8b-8.11.2　仮名化又は匿名化の手法を利用する場合、データが十分に仮名化又は匿名化されていることを検証する。

8b-8.11.3　データの匿名化では、取扱いに慎重を要する情報の全ての要素に対して有効とするように考慮する。

（8b-8.11.3参考）　データの匿名化が適切に考慮されていない場合、ある人物が直接識別できるデータが匿名化されていても、間接的に識別を可能とする別のデータが存在して、その人物が識別できる場合がある。

8b-8.11.4　データマスキング手法には、仮名化、匿名化のほかに、次を含む手法を考慮する。

a）データを暗号化する。
b）文字をヌル化又は消去する。
c）数及び日付を変える。
d）取扱いに慎重を要するデータのうち特定の値を別の値に置き換える。
e）値をそのハッシュ値に置き換える。

8b-8.11.5　データマスキング手法を実装する場合、次の事項を考慮する。

a）利用者に必要最小限のデータだけを示すように問合せ（クエリ）及びマスクを設計する。
b）データセットの一部の記録に関して、利用者に一部のデータを見せない

ことが望ましい場合、データを難読化する仕組みを設計し、実装する※1。

※1 例えば、緊急の場合であっても、患者が自らの記録の全てを病院スタッフが見ることができることを望まない場合、病院スタッフには部分的に難読化したデータを提示し、そのデータが適切な治療に有用な情報を含む場合は、特定の役割をもつスタッフだけがアクセスできるようにする。

c) データを難読化する場合、データを難読化しているかどうかを利用者が知ることができないことを、PII主体が要求できるようにする※1。

※1 難読化の難読化。これは医療施設で利用され、例えば、血液検査の結果など取扱いに慎重を要する情報が難読化されていることを、患者が要員に知られたくない場合などである。

d) 法令又は規制上の要求事項※1。

※1 例えば、処理中又は保管中に、支払いカードの情報をマスキングすることを要求する。

8b-8.11.6 データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。

a) 処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル

b) 処理するデータへのアクセス制御

c) 処理するデータの使用法に関する合意又は制限

d) PII主体を識別するために、処理するデータを他の情報と照合することの禁止

e) 処理するデータの提供及び受領の追跡

## 8b-8.12 データ漏えい防止

管理策：データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用する。

目的： 個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。

詳細管理策

8b-8.12.1 組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。

a) 漏えいから保護する情報※1の特定及び分類

※1 例えば、個人情報、価格設定モデル、製品設計

b) データ漏えいの経路・手段の監視※1

※1 例えば、電子メール、ファイル転送、モバイル機器及び可搬記憶装置

c) 情報の漏えいを防止するための処置※1

※1 例えば、取扱いに慎重を要する情報を含むメールの検疫

8b-8.12.2 データ漏えい防止ツールを、次の目的で使用する。

a) 認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する※1。

※1 例えば、利用者のシステム上の整理されていない情報

b) 取扱いに慎重を要する情報の開示を検出する※1。

※1 例えば、信頼できない第三者のクラウドサービスに情報がアップロードされた場合、又は電子メールで送信された場合にこれらを検出する。

c) 取扱いに慎重を要する情報を漏えいする利用者の行為又はネットワーク送信を阻止する※1。

※1 例えば、データベースエントリのスプレッドシートへのコピーを防止する。

8b-8.12.3　組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する必要があるかどうかを判断する。

8b-8.12.4　組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。

8b-8.12.5　データの取り出しが必要な場合、利用者による取り出しを許可し、利用者に自らの行動にアカウンタビリティをもたせる役割を、データの管理責任者に与える。

8b-8.12.6　画面のスクリーンショット又は写真を撮ることには、利用条件、訓練及び監査によって対応する。

8b-8.12.7　データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。

8b-8.12.8　データ漏えい防止は、ちょう報活動の対象となる可能性がある、又はコミュニティにとって重要な可能性がある秘密情報※1を敵対者が情報収集活動によって取得することに対する保護も考慮する。

※1 地政学、人、財務、商取引、科学又はその他に関する秘密情報

8b-8.12.9　データ漏えい防止活動は、独立の活動又は敵対者の情報収集活動への対応のいずれかとして、敵対者の決定を混乱させる方策※1を講じる。

※1 真正の情報を偽の情報に置き換えるような、リバースソーシャルエンジニアリング又は攻撃者を引き付けるハニーポットの使用がある。

### 8b-8.13　情報のバックアップ

管理策：合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。

目的：　データ又はシステムの損失からの回復を可能にするため。

詳細管理策

8b-8.13.1　組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。

8b-8.13.2　インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。

8b-8.13.3　バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステムをバックアップする方法について計画を作成し、実装する。

8b-8.13.4　バックアップ計画を策定するときは、次の事項を考慮に入れる。

a) バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。

b) バックアップの範囲※1、及びバックアップの頻度は、組織の事業上の要求事項※2、関係する情報のセキュリティ要求事項、及びその情報の組織の継続的な運用に対する重要度を考慮して決定する。

※1 例えば、フルバックアップ、差分バックアップ
※2 例えば、目標復旧時点（5f-5.30参照）

c) バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。

d) バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護※1を実施する。

※1 箇条7及び8a-8.1参照

e) バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないように、テストシステム上で行い、原本の記憶媒体に上書きしない。

f) 特定したリスクに応じて、暗号化によってバックアップ情報を保護する※1。

※1 例えば、機密性が重要な状況において

g) バックアップを作成する前に、不注意によるデータ損失の検出を確実にするように注意する。

8b-8.13.5 バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。

8b-8.13.6 個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の目的を満たすことを確実にするために、定期的に試験する※1。

※1 5f-5.30参照

8b-8.13.7 定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。

8b-8.13.8 重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。

8b-8.13.9 組織がクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。

8b-8.13.10 組織は、クラウドサービスの一部として提供されるバックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。

8b-8.13.11 重要な業務情報の保持期間は、複製の保存に関するあらゆる要求事項を考慮に入れて、決定する。

8b-8.13.12 組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の削除※1、また、法令及び規制を考慮する。

※1 8b-8.10参照

### 8b-8.14 情報処理施設・設備の冗長性

管理策：情報処理施設・設備は、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。

目的：　情報処理施設・設備の継続的な運用を確実にするため。

詳細管理策

8b-8.14.1　組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。

8b-8.14.2　組織は、可用性の要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。

8b-8.14.3　組織は、冗長な構成要素及び情報処理施設・設備を作動させる手順を計画し、実装する。

（8b-8.14.3参考）　冗長性は、情報処理施設・設備の一部又は全体を二重化させる※1ことによって導入することが可能である。

※1 予備の構成要素をもつか、又は二つの全ての要素をもつ。

8b-8.14.4　冗長な構成要素及び情報処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておくか、又は緊急の場合に自動若しくは手動で作動させるかを定める。

8b-8.14.5　冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。

8b-8.14.6　情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるようにし、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とする仕組みを設ける。

8b-8.14.7　組織は、冗長システムを実装する場合、次の事項を考慮する。

a) インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二者以上と契約する。

b) 冗長性のあるネットワークを使用する。

c) 冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。

d) 物理的に冗長性のある電力供給装置又は電源を使用する。

e) ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散して使用する。

f) システムにおいて二重化した構成要素※1をもつ、又はネットワークにおいて二重化した構成要素※2をもつ。

※1 例えば、CPU、ハードディスク、メモリ

※2 例えば、ファイアウォール、ルーター、スイッチ

8b-8.14.8　実施できる場合、できれば本番モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。

### 8b-8.15　ログ取得

管理策：活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。

目的：　事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを

防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。

詳細管理策

**【ログ取得全般】**

8b-8.15.1　組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。

8b-8.15.2　ログ特有の要求事項は、ログ取得に関するトピック固有の方針に文書化する。

8b-8.15.3　活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。

a) 利用者ID

b) システムの動作

c) 関係する事象の日時及び内容※1

※1 例えば、ログオン、ログオフ

d) 装置・機器の識別情報、システムの識別子及び所在地

e) ネットワークアドレス及びプロトコル

8b-8.15.4　次の事象について、ログ取得を考慮する。

a) システムへのアクセスの、成功及び失敗した試み

b) データ及び他の資源へのアクセスの、成功及び失敗した試み

c) システム構成の変更

d) 特権の利用

e) ユーティリティプログラム及びアプリケーションの利用

f) アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類

g) アクセス制御システムが発した警報

h) セキュリティシステム※1の起動及び停止

※1 例えば、ウイルス対策システム、侵入検知システム

i) 識別情報の作成、変更又は削除

j) アプリケーション※1において利用者が実行したトランザクション

※1 第三者が提供又は実行するサービス又は製品の場合がある。

(8b-8.15.4参考)　インシデントの分析、警告及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源※1をもつことが重要である。

※1 8b-8.17参照

**【ログの保護】**

8b-8.15.5　特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。

8b-8.15.6　特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。

(8b-8.15.6参考)　利用者は、その直接の管理下で、情報処理施設・設備に関するログを改変する可能性がある。

8b-8.15.7　管理策は、次の事項を含む、ログ情報の認可されていない変更及びログ取得機能の運用上の問題から保護することを目指す。

a) 記録されたメッセージ形式の変更

b) ログファイルの編集又は削除

c) ログファイルを保持している記憶媒体の記録容量を超過した場合のイベント記録の不具合又は過去のイベント記録への上書き

8b-8.15.8 ログは保護することとし、その手法として、次の使用を考慮する。

a) 暗号技術によるハッシュ化

b) 追加専用及び読取り専用ファイルへの記録

c) 公開透明性ファイル※1への記録

※1 第三者が確認できるようにすることで運用における透明性を確保することを目的として公開されるファイル

(8b-8.15.8参考) ログは、データ保持に関する要求事項、又は証拠の収集及び保持※1のための要求事項によって、保存が求められる場合がある。

※1 5e-5.28参照

8b-8.15.9 組織がエラーのデバッグ又はトラブルシューティングを支援するために、システム又はアプリケーションのログを業者に送信する必要がある場合、利用者名、インターネットプロトコル、IPアドレス、ホスト名、組織名などの情報について、業者に送信する前に、可能な場合はデータマスキング手法※1を使用してログの非識別化を行う。

※1 8b-8.11参照

8b-8.15.10 イベントログは、取扱いに慎重を要するデータ及びPIIを含む可能性があるため、適切なプライバシー保護対策を講じる※1。

※1 5g-5.34参照

**【ログ分析】**

8b-8.15.11 ログ分析は、侵害の可能性がある通常とは異なる活動又は異常な挙動を特定する助けとなるように、情報セキュリティ事象の分析及び解釈を含む。

8b-8.15.12 事象の分析は、次の事項を考慮して実施する。

a) 分析を実施する専門家に必要な技能

b) ログ分析の手順の決定

c) 各セキュリティ関連事象の必要な属性

d) 既定の規則※1の使用を通じて特定される例外事象

※1 例えば、セキュリティ情報及びイベント管理（SIEM）又はファイアウォールの規則、並びに侵入検知システム（IDS）又はマルウェアのシグネチャ

e) 異常な活動及び挙動と比較する利用者及びエンティティの挙動分析（UEBA）、既知の挙動パターン及び標準ネットワークトラフィック

f) 傾向分析又はパターン分析の結果※1

※1 例えば、データ分析、ビッグデータ技術及び特定の目的の分析ツールを使用した結果

g) 利用可能な脅威インテリジェンス

8b-8.15.13 ログ分析は、次の事項を含む、異常な挙動を特定し、分析する助けとなる監視活動によって支援する。

a) 保護された資源※1への成功及び失敗したアクセスの試みをレビューする。

※1 例えば、ドメインネームシステム（DNS）サーバ、ウェブポータル及び共有ファイル

b) ボットネットのコマンド アンド コントロールサーバ（以下、C&Cサーバと表す。）への接続のような、悪意のあるサーバへのアウトバウンドネットワーク接続を特定するために、DNSログを確認する。

c) システム及びネットワーク内の異常な活動に関するサービス提供者からの使用状況報告※1を調べる※2。

※1 例えば、インボイス又はサービス報告
※2 例えば、活動のパターンをレビューする

d) より正確な検知及びインシデント分析を確実にするために、入口、出口などの物理的監視のイベントログを含める。

e) 効率的で非常に正確な分析を行えるように、ログを相互に関係付ける。

8b-8.15.14 情報セキュリティインシデントの疑い、及び実際の情報セキュリティインシデントを特定し※1、更なる調査を行う※2。

※1 例えば、マルウェア感染又はファイアウォールに対する探査
※2 例えば、情報セキュリティインシデント管理プロセスの一部として調査を行う（5e-5.25参照）。

## 8b-8.16 監視活動

管理策：情報セキュリティインシデントの可能性を評価するために、ネットワーク、システム及びアプリケーションについて異常な挙動がないか監視し、適切な処置を講じる。

目的： 異常な挙動及び情報セキュリティインシデントの可能性を検出するため。

詳細管理策

8b-8.16.1 監視のために、次の事項を行う。

a) 監視の範囲及びレベルは、業務及び情報セキュリティの要求事項に従い、関連する法令及び規制を考慮して決定する。

b) 監視を記録する。

c) 監視記録は、定めた保持期間にわたって維持する。

8b-8.16.2 監視システムに含めるものとして、次の事項を考慮する。

a) アウトバウンド及びインバウンドの、ネットワーク、システム及びアプリケーションのトラフィック

b) システム、サーバ、ネットワーク装置、監視システム、重要なアプリケーションなどへのアクセス

c) 重要な又は実務管理者が扱うシステム及びネットワークの構成ファイル

d) セキュリティツールからのログ※1

※1 例えば、ウイルス対策、IDS、不正侵入防止システム（IPS）、ウェブフィルタ、ファイアウォール、データ漏えい防止（DLP）

e) システム及びネットワークの活動に関するイベントログ

f) 実行しているコードがそのシステムでの実行を認可されていること、及びそれが改ざん※1されていないことの確認

※1 例えば、望ましくないコードを追加する再コンパイルによる改ざん

g) 資源※1の使用及びそれらの動作状況

※1 例えば、CPU、ハードディスク、メモリ、帯域幅

8b-8.16.3 組織は、正常な挙動の基準を確立し、この基準に照らして異常を監視する。基準を確立する場合、次の事項を考慮する。

a) 通常時及びピーク時のシステムの使用率

b) 各利用者又は利用者グループの通常のアクセス時間、アクセスの場所、アクセスの頻度

8b-8.16.4 監視システムは、次のような異常な挙動を特定するために、確立した基準に照らして構成する。

a) プロセス又はアプリケーションの計画外の終了

b) 既知の悪意のあるIP アドレス又はネットワークドメイン※1から送信されるマルウェア又はトラフィックに典型的に伴う挙動

※1 例えば、ボットネットのC&Cサーバに関係するもの

c) 既知の攻撃の特性※1

※1 例えば、サービス妨害及びバッファオーバーフロー

d) 異常なシステム動作※1

※1 例えば、キー入力のログ、プロセスインジェクション、及び標準プロトコルの使用における逸脱

e) ボトルネック及び過負荷※1

※1 例えば、ネットワークの待ち行列、遅延レベル及びネットワーク上の通信の乱れ

f) システム又は情報への認可されていないアクセス又はその試み

g) 業務アプリケーション、システム及びネットワークの認可されていないスキャン

h) 保護された資源※1への成功及び失敗したアクセスの試み

※1 例えば、DNS サーバ、ウェブポータル及びファイルシステム

i) 想定される挙動に対して、利用者及びシステムの異常な挙動

8b-8.16.5 監視ツールによる継続的監視を使用し、次の事項を考慮する。

a) 監視は、組織のニーズ及び能力に応じて、リアルタイム又は定期的な間隔で行う。

b) 大量のデータを取り扱い、常に変化する脅威の状況に適応し、リアルタイムで通知することを可能にする機能をもつ監視ツールを利用する。

c) 特定のシグネチャ及びデータ、又はネットワーク若しくはアプリケーションの動作パターンも認識できる監視ツールを利用する。

8b-8.16.6 自動監視ソフトウェアは、あらかじめ定めたしきい値に基づいて警告を発するように構成する※1。

※1 例えば、管理コンソール、電子メールメッセージ又はインスタントメッセージングシステムを通じて構成する。

8b-8.16.7 警告システムは、誤検出を最小限にするために、組織の基準に合わせて調整し、学習させる。

8b-8.16.8 要員は警告への対応に専念させることが望ましく、インシデントの可能性がある事象を正確に判定できるように適切に訓練を受けさせる。

8b-8.16.9 警告通知を受信し、対応するための冗長性のあるシステム及びプロセスを備える。

8b-8.16.10 監査、セキュリティ評価、ぜい弱性スキャン及び監視※1を改善するために、異常な事象を関係者に伝達する。

※1 5e-5.25参照

8b-8.16.11　情報セキュリティに対する有害な事象の影響を最小にするために、その存在を示す監視システムからの通知に時機を失せず対応する手順を確立する※1。

※1 5e-5.26参照

8b-8.16.12　将来の誤検出の数を減らすために監視ソフトウェアを調整するなど、誤検出を特定し、対処する手順も確立する。

### 8b-8.17　クロックの同期

管理策：組織が使用する情報処理システムのクロックは、組織が採用した時刻源と同期させる。

目的：　セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。

詳細管理策

8b-8.17.1　時刻の表現、信頼できる同期及び正確さに関する、外部及び内部の要求事項は、文書化し、実装する。

（8b-8.17.1参考）　この要求事項は、法令、規制、契約、標準及び内部監視のニーズに由来する可能性がある。

8b-8.17.2　ビル管理システム、入退出システム、及び調査を支援するために使用できるその他のシステムを含む全てのシステムに対して、組織内で基準とする時刻源を考慮して定める。

8b-8.17.3　国の原子時計又は全地球測位システム（GPS）から配信される時刻に基づくクロックを、ログ取得システムの基準クロック、すなわち、正確なタイムスタンプを確実にする一貫性のある信頼できる日付及び時刻源として使用する。

8b-8.17.4　ネットワークで接続された全てのシステムを基準クロックと同期させるために、ネットワークタイムプロトコル（NTP）又は高精度タイムプロトコル（PTP）などのプロトコルを使用する。

（8b-8.17.4参考）　組織は、外部クロックの信頼性を改善し、変動を適切に管理するために、二つの外部時刻源を同時に使用することが可能である。

8b-8.17.5　クラウドサービスの利用によりクロックの同期が困難となる場合、不一致から生じるリスクを軽減するために、各サービスのクロックを監視し、差を記録する。

（8b-8.17.5参考）　複数のクラウドサービスを使用する場合、又はクラウドサービス及びオンプレミスサービスの両方を使用する場合には、クロックの同期が困難なことがある。

### 8b-8.18　特権的なユーティリティプログラムの使用

管理策：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。

目的：　ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。

詳細管理策

8b-8.18.1　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においては、次の事項を考慮する。

a) 可能な限り少人数の信頼できる認可された利用者だけに限定した、ユーティリティプログラムの使用制限※1

※1 8a-8.2参照

b) ユーティリティプログラムを使用する要員の一意の識別を含む、ユーティリティプログラムの識別、認証及び認可手順の使用

c) ユーティリティプログラムの認可レベルの明確化及び文書化

d) ユーティリティプログラムを臨時に用いる場合の認可

e) 権限の分離が必要な場合に、システム上のアプリケーションにアクセスする利用者に、ユーティリティプログラムの使用を不可とする

f) 全ての不要なユーティリティプログラムの除去又は無効化

g) 少なくとも、アプリケーションソフトウェアからのユーティリティプログラムの論理的分離。実施できる場合、ユーティリティプログラムのネットワーク通信をアプリケーショントラフィックから分離

h) ユーティリティプログラムの使用の制限※1

※1 例えば、認可されたシステム変更のための期間での利用

i) ユーティリティプログラムの全ての使用に関するログ

### 8b-8.19 運用システムへのソフトウェアの導入

管理策：運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施する。

目的： 運用システムの完全性の維持を確実にし、技術的ぜい弱性の悪用を防止するため。

詳細管理策

8b-8.19.1 運用システムで使用するソフトウェアの変更及び導入において、セキュリティを保つために、次の事項を考慮する。

a) 運用ソフトウェアの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する※1。

※1 8a-8.5参照

b) 運用システムには、承認された実行可能なコードだけを導入し、開発用コード又はコンパイラは一切導入しないことを確実にする。

c) ソフトウェアは、十分なテストに成功した後に導入し、更新する※1。

※1 8d-8.29及び8d-8.31参照

d) 対応する全てのプログラムソースライブラリを更新する。

e) 全ての運用ソフトウェアの管理を維持するために、システム文書の管理と同様に、構成管理システムを利用する。

f) 変更を実装する前に、ロールバック計画を定める。

g) 運用ソフトウェアの更新の全てについて、監査ログを維持する。

h) ソフトウェアの旧版は、緊急時対応の手段として、及び保管しているデータをそのソフトウェアで読み込む又は処理する必要がある間は、全ての必要な情報及びパラメータ、手順、設定の詳細並びにサポートソフトウェアとともに保管しておく。

8b-8.19.2　新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティ※1を考慮に入れる。

※1 例えば、新しい情報セキュリティ機能の導入、既存の版に影響を及ぼす情報セキュリティのぜい弱性の数及び深刻度

8b-8.19.3　情報セキュリティ上のぜい弱性を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する※1。

※1 8b-8.8及び8b-8.19参照

8b-8.19.4　外部から供給されるソフトウェア及びパッケージ※1に依存するソフトウェアは、情報セキュリティのぜい弱性をもたらす可能性があるため、認可されていない変更を回避するために監視し、管理する。

※1 例えば、外部サイトが提供しているモジュールを使用するソフトウェアプログラム

8b-8.19.5　運用システムで利用するソフトウェアの版を、ソフトウェア業者（供給者）がサポートする版に維持する。

8b-8.19.6　組織は、サポートのないソフトウェアに依存することのリスクを考慮する。

（8b-8.19.6参考）　ソフトウェア業者は、徐々に古い版のソフトウェアのサポートを中止する。

8b-8.19.7　運用システムで使用するオープンソースソフトウェアは、最新で適切なリリースの使用を維持する。

（8b-8.19.7参考）　時間の経過とともに、オープンソースコードが維持されなくなるにもかかわらず、オープンソースソフトウェアリポジトリで引き続き利用できる場合がある。

8b-8.19.8　組織は、運用システムで使用する場合、保守がなされないオープンソースソフトウェアに依存するリスクも考慮する。

8b-8.19.9　供給者がソフトウェアの導入又は更新に関与する場合、物理的又は論理的アクセスは、必要なときに、適切な認可を得た場合にだけ許可する。

8b-8.19.10　供給者の活動を監視する※1。

※1 5d-5.22参照

8b-8.19.11　組織は、利用者が導入できるソフトウェアの種類について、厳密な規則を定め、施行する。

8b-8.19.12　特権の許可は最小限にするという原則を、運用システムへのソフトウェアの導入に適用する。

8b-8.19.13　組織は、ソフトウェアのインストールの種類のうち、許可するもの※1、及び禁止するもの※2を特定する。

※1 例えば、既存のソフトウェアの更新及びセキュリティパッチの適用
※2 例えば、個人利用のためだけのソフトウェア、その由来から悪意のある可能性が不明な又は疑わしいソフトウェア

8b-8.19.14　特権は、利用者の役割に基づいて付与する。

## 8c　情報システムの適正利用の管理

### 8c-8.20　ネットワークセキュリティ

管理策：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、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御する。

目的：　ネットワーク及びそれを支援する情報処理設備において、情報をネットワークを通じた侵害

から保護するため。

詳細管理策

8c-8.20.1　ネットワークにおける情報のセキュリティを確実にし、接続したネットワークサービスを認可されていないアクセスから保護するために、管理策を実施する。

8c-8.20.2　ネットワークセキュリティの管理策では、特に、次の事項を考慮する。

a) ネットワークごとに、扱ってよい情報の種類及び分類レベル

b) ネットワーク装置及び機器の管理に関する責任及び手順を確立する。

c) ネットワーク図及び装置・機器※1の構成ファイルを含む最新の文書を維持する。

※1 例えば、ルーター、スイッチ

d) 適切な場合には、ネットワークの運用責任は、ICTシステムの運用から分離する※1。

※1 5a-5.3参照

e) 公衆ネットワーク、第三者ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、管理策を確立する※1。

※1 ネットワークサービスの可用性及びネットワークに接続したコンピュータの可用性を維持するためには、追加の管理策が要求される場合もある（5d-5.22、8c-8.24、5b-5.14及び6a-6.6参照）。

f) 情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関係のある行動の記録及び検知ができるように、適切なログを取得し、監視する※1。

※1 8b-8.16及び8b-8.15参照

g) 組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするために、様々なネットワーク管理作業を綿密に調整する。

h) ネットワーク上のシステムを認証する。

i) ネットワークへのシステムの接続を制限し、フィルタリングする※1。

※1 例えば、ファイアウォールを使用する。

j) ネットワークへの装置及び機器の接続を検出し、制限し、認証する。

k) ネットワーク装置・機器の要塞化（hardening）

l) ネットワーク管理の経路を他のネットワークトラフィックから分離する。

m) ネットワークが攻撃を受けた場合、重要なサブネットワークを一時的に分離する※1。

※1 例えば、ドローブリッジ（跳ね橋）を用いて分離する。

n) ぜい弱なネットワークプロトコルを無効化する。

8c-8.20.3　組織は、仮想化ネットワークの使用に、適切なセキュリティ管理策を適用することを確実にする。

（8c-8.20.3参考1）　仮想化ネットワークには、ソフトウェア定義ネットワーク（SDN、SD-WAN）も含む。

（8c-8.20.3参考2）　仮想化ネットワークは、物理的ネットワーク上での通信の論理的分離を可能

にすることから、セキュリティの観点で望ましい場合があり、特に分散型コンピューティングを用いて実装したシステム及びアプリケーションにおいてこのことが該当する。

### 8c-8.21　ネットワークサービスのセキュリティ

管理策：ネットワークサービスのセキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視する。

目的：　ネットワークサービスの利用におけるセキュリティを確実にするため。

詳細管理策

8c-8.21.1　それぞれのネットワークサービスに必要なセキュリティ対策※1を、内部又は外部のネットワークサービス提供者が特定し、実装する。

※1 例えば、セキュリティ機能、サービスレベル及びサービスの要求事項

8c-8.21.2　組織は、ネットワークサービス提供者による、ネットワークサービスに必要なセキュリティの対策の実施を確実にする。

8c-8.21.3　合意したサービスをセキュリティを保って管理できる、ネットワークサービス提供者の能力を定め、定常的に監視する。

8c-8.21.4　監査の権利について組織と提供者との間で合意する。

8c-8.21.5　組織は、サービス提供者が適切なセキュリティ対策を維持していることを実証するために、サービス提供者が提示する第三者認証も考慮する。

8c-8.21.6　ネットワーク及びネットワークサービスの利用に関する規則は、次の事項を対象として策定し、実施する。

a) アクセスが許可されているネットワーク及びネットワークサービス

b) 様々なネットワークサービスにアクセスするための認証の要求事項

c) 誰にどのネットワーク及びネットワークサービスにアクセスすることを許すかを決定する認可手順

d) ネットワーク接続及びネットワークサービスへのアクセスを保護するためのネットワーク管理並びに技術的管理策及び手順

e) ネットワーク及びネットワークサービスにアクセスするために利用する手段※1

※1 例えば、仮想プライベートネットワーク（VPN）又は無線ネットワークの利用

f) アクセス時の利用者の時刻、場所及びその他の属性

g) ネットワークサービスの利用の監視

8c-8.21.7　ネットワークサービスは次のセキュリティ機能を考慮する。

a) ネットワークサービスのセキュリティに適用する技術※1

※1 例えば、認証、暗号化、ネットワーク接続管理

b) セキュリティ規則及びネットワーク接続規則に従った、ネットワークサービスへのセキュリティを確保した接続のために要求される技術的パラメータ

c) 利用者が性能、可用性及び機密性の要求事項に従ってキャッシングの利用を選択できる、キャッシング※1及びそのパラメータ

※1 例えば、コンテンツ配信ネットワークにおけるキャッシング

d) 必要な場合、ネットワークサービス又はアプリケーションへのアクセスを制限するための、ネットワークサービス利用の手順

## 8c-8.22 ネットワークの分離

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

目的： 業務のニーズに基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。

詳細管理策

8c-8.22.1 組織は、大規模なネットワークを幾つかのネットワーク領域に分離し、公衆ネットワーク（すなわち、インターネット）から分離することによって、大規模なネットワークのセキュリティを管理する。

8c-8.22.2 ネットワーク領域は、可能であれば組織の単位※1又は特定の組合せ※2に従い、信頼性、重要性及び取扱いに慎重を要する度合い※3に基づいて選択する。

※1 例えば、人事、財務、マーケティング
※2 例えば、複数の組織の単位に接続しているサーバ領域
※3 例えば、公開されている領域、デスクトップ領域、サーバ領域、低リスクシステム及び高リスクシステム

8c-8.22.3 ネットワークの分離は、可能であれば物理的に異なるネットワーク又は論理的に異なるネットワークを用いて行う。

8c-8.22.4 それぞれのネットワーク領域の境界は、明確に定める。

8c-8.22.5 ネットワーク領域間のアクセスを認める場合、アクセスは境界にゲートウェイ※1を設けて制御する。

※1 例えば、ファイアウォール、フィルタリングルーター

8c-8.22.6 ネットワーク領域を分離する際の基準及びゲートウェイを通じて認められるアクセスの基準は、それぞれの領域のセキュリティ要求事項のアセスメントに基づく。

8c-8.22.7 それぞれのネットワーク領域のセキュリティ要求事項のアセスメントでは、次の事項を評価する。

a) アクセス制御に関するトピック固有の方針※1、アクセス要求事項、並びに処理する情報の価値及び分類に従っているか。

※1 5c-5.15参照

b) 適切なゲートウェイ技術を組み込むための費用対効果を考慮しているか。

8c-8.22.8 無線ネットワークの分離のために、電波の届く範囲の調整を考慮する。

（8c-8.22.8参考） 無線ネットワークは、ネットワークの境界が十分に定められていないため、特別な取扱いを要する。

8c-8.22.9 取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策※1に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離するように配慮する。

※1 8c-8.20参照

8c-8.22.10 要員が組織のトピック固有の方針に適合する管理された利用者エンドポイン

ト機器だけを使用する場合、ゲスト用の無線アクセスネットワークを要員用の無線アクセスネットワークから分離する。

8c-8.22.11　ゲスト用のWiFiは、要員によるゲストWiFiの利用を防ぐために、少なくとも要員用のWiFiと同じ制限をもつ。

## 8c-8.23　ウェブフィルタリング

管理策：悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理する。

目的：　システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。

詳細管理策

8c-8.23.1　組織は、違法な情報があるウェブサイト、又はウイルス若しくはフィッシングの材料があることが知られているウェブサイトに組織の要員がアクセスするリスクを減らす。

（8c-8.23.1参考）　リスクを減らす手法として、関係するウェブサイトのIPアドレス又はドメインへのアクセスを阻止することがある。一部のブラウザ及びマルウェア対策技術は、アクセスすることが望ましくないウェブサイトへのアクセスを自動的に阻止、又は阻止するように構成することが可能である。

8c-8.23.2　組織は、要員がアクセスすることが望ましい又は望ましくないウェブサイトの種類を特定する。

8c-8.23.3　組織は次の種類のウェブサイトへのアクセスを塞ぐことを考慮する。

a）情報アップロード機能をもつウェブサイト。ただし、正当な業務上の理由のため許可されている場合を除く。

b）悪意のある、又はその疑いのあるウェブサイト※1

※1 例えば、マルウェア又はフィッシングコンテンツを配布しているウェブサイト

c）C&Cサーバ

d）脅威インテリジェンスで認識した悪意のあるウェブサイト※1

※1 5a-5.7 参照

e）違法なコンテンツを供給しているウェブサイト

8c-8.23.4　ウェブフィルタリングに関する管理策を導入する前に、組織は、望ましくない又は不適切なウェブサイト及びウェブベースのアプリケーションに対する制限を含め、オンライン資源を安全かつ適切に使用するための規則を確立する。

8c-8.23.5　オンライン資源を安全かつ適切に使用するための規則は最新の状態に保つ。

8c-8.23.6　ウェブへのアクセスを含む、オンライン資源のセキュリティを保った適切な使用について、要員を訓練する。

8c-8.23.7　オンライン資源のセキュリティを保った適切な使用についての訓練には、組織の規則、セキュリティ上の懸念を報告するための連絡先、及び制限されたウェブ資源に正当な業務上の理由によってアクセスする必要がある場合の例外プロセスを含める。

8c-8.23.8　ウェブサイトで、セキュリティが保たれないことを通知するブラウザアドバ

イザリを利用者が無効にしないことを確実にするように、要員を訓練する。

### 8c-8.24　暗号の利用

管理策：暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施する。

目的：　事業上及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性又は完全性を保護するための暗号の適切かつ効果的な利用を確実にするため。

詳細管理策

**【暗号の利用全般】**

8c-8.24.1　暗号化を利用する場合、次の事項を考慮する。

a) 情報を保護する上での一般原則も含む、組織で定義した暗号に関するトピック固有の方針。暗号技術の利用の便益を最大化し、リスクを最小化し、不適切又は誤った利用を回避するには、暗号の利用に関するトピック固有の方針が必要である。

b) 要求された保護レベル及び情報の分類を特定し、その結果によって、要求される暗号アルゴリズムの種別、強度及び品質を確立する。

c) 持ち運び可能な利用者エンドポイント機器又は記憶媒体に保持され、ネットワークを通じてその機器又は記憶媒体に伝送される情報を保護するための暗号の利用

d) 鍵管理に対する取組。これには、暗号鍵の生成及び保護手法、並びに鍵が紛失した場合、危たい（殆）化した場合又は損傷した場合の暗号化された情報の復元手法を含む。

e) 次の事項に関する役割及び責任

1) 暗号を効果的に利用するための規則の実施

2) 鍵生成を含めた鍵管理※1

※1 8c-8.24の“鍵管理”参照

f) 採用する標準類、並びに組織での利用が承認又は要求されている暗号アルゴリズム、暗号強度、暗号ソリューション及び利用方法

g) 暗号化した情報を用いることの、コンテンツ検査※1に依存する管理策への影響

※1 例えば、マルウェアの検出又はコンテンツフィルタリング

8c-8.24.2　暗号を効果的に利用するための組織の規則を実施するときには、世界の様々な地域における暗号技術の利用、及び国境を越える暗号化された情報の流れに関する問題に適用される、規制及び国内の制約を考慮する※1。

※1 5g-5.31参照

8c-8.24.3　暗号サービスの外部供給者※1とのサービスレベルに関する合意又は契約の内容は、賠償責任、サービスの信頼性及びサービス提供の応答時間を扱う※2。

※1 例えば、認証局

※2 5d-5.22参照

**【鍵管理】**

8c-8.24.4　鍵管理システムは、次に関する一連の合意された標準類、手順及びセキュリ

ティを保った手法に基づくことを考慮する。

a) 種々の暗号システム及び種々のアプリケーションのために鍵[26]を生成する。

b) 公開鍵証明書を発行し、入手する。

c) 意図するエンティティに鍵を配布する。これには、受領時に、鍵をどのような方法で活性化するか（使える状態にするか）も含む。

d) 鍵を保管する。これには、認可されている利用者がどのような方法で鍵にアクセスするかも含む。

e) 鍵を変更又は更新する。これには、鍵をいつ、どのような方法で変更するかの規則も含む。

f) 危たい（殆）化した鍵に対処する。

g) 鍵を無効にする※1。これには、鍵をどのような方法で取消し又は非活性化するかも含む。

※1 例えば、鍵が危たい（殆）化した場合、又は利用者が組織を離脱した場合（後者の場合には、鍵は保存する。）

h) 紛失した鍵又は破損した鍵を回復する。

i) 鍵をバックアップ又は保存する。

j) 鍵を破壊する。

k) 鍵管理に関連する活動を記録し、監査する。

l) 鍵管理に関する組織の規則に従って鍵を一定期間だけ利用できるように、鍵の活性化及び非活性化の日付を設定する。

m) 暗号鍵へのアクセスに関する法的要求※1の取扱い

※1 例えば、裁判での証拠として、暗号化された情報を平文で求められた場合

(8c-8.24.4参考) 適切な鍵管理には、暗号鍵を生成、保管、保存、読出し、配布、利用停止及び破壊するための、セキュリティを保ったプロセスが必要となる。

8c-8.24.5 全ての暗号鍵は、改変及び紛失から保護する。

8c-8.24.6 秘密鍵及びプライベート鍵は、認可されていない利用及び開示から保護する。

8c-8.24.7 鍵の生成、保管及び保存のために用いる装置は、物理的に保護する。

8c-8.24.8 暗号鍵の完全性に加え、多くの事例では、公開鍵の真正性も考慮する。

## 8d 情報システム開発／導入の管理

### 8d-8.25 セキュリティに配慮した開発のライフサイクル

管理策：ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。

目的： 情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。

詳細管理策

(8d-8.25参考) セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシス

[26] この基準における“プライベート鍵”及び“公開鍵”の用語は、JIS Q 27002:2024と同様、公開鍵（非対称暗号）方式における一対の鍵のうち、それぞれ“private key”及び“public key”に対応している。また、“秘密鍵”は、共通鍵（対称暗号）方式における“secret key”に対応している。

テムを構築するには、セキュリティに配慮した開発が必要となる。

8d-8.25.1　セキュリティに配慮した開発を達成するために、次の側面を考慮する。

a) 開発環境、テスト環境及び本番環境の分離※1
※1 8d-8.31参照

b) ソフトウェア開発のライフサイクルにおける、次に関わるセキュリティに関する手引

1) ソフトウェア開発の方法論におけるセキュリティ※1
※1 8d-8.28及び8d-8.27参照

2) 用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針※1
※1 8d-8.28参照

c) 仕様策定及び設計段階におけるセキュリティ要求事項※1
※1 5a-5.8参照

d) プロジェクトにおけるセキュリティの確認項目※1
※1 5a-5.8参照

e) 回帰テスト、コードスキャン、侵入テストなどのシステム及びセキュリティのテスト※1
※1 8d-8.29参照

f) ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ※1
※1 8a-8.4及び8b-8.9参照

g) 版の管理におけるセキュリティ※1
※1 8d-8.32参照

h) アプリケーションセキュリティに関して必要な知識及び訓練※1
※1 8d-8.28参照

i) ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力※1
※1 8d-8.28参照

j) ライセンスに関する将来の問題を回避しつつ、費用対効果の高いソリューションを確実にするための、ライセンスの要求事項及び代替案※1
※1 5g-5.32参照

8d-8.25.2　開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの保証を得る※1。
※1 8d-8.30参照

## 8d-8.26　アプリケーションセキュリティの要求事項

管理策：アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。

目的：　アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。

詳細管理策

**【アプリケーションセキュリティの要求事項全般】**

8d-8.26.1　アプリケーションセキュリティの要求事項をリスクアセスメントを通じて特定し、規定する。

8d-8.26.2　アプリケーションセキュリティの要求事項は、情報セキュリティの専門家の

支援を受けて作成することを考慮する。

(8d-8.26.2参考) アプリケーションセキュリティの要求事項は、アプリケーションの目的に応じて、幅広いトピックにわたることがある。

8d-8.26.3 アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。

a) エンティティの識別情報の信頼のレベル※1

※1 例えば、認証を通じて（5c-5.17、8a-8.2及び8a-8.5参照）

b) アプリケーションで処理する情報の種類及び分類レベルの特定

c) アプリケーション内のデータ及び機能へのアクセス及びアクセスのレベルを分離することの必要性

d) 悪意のある攻撃又は意図しない事業の中断・阻害に対するレジリエンス※1

※1 例えば、バッファオーバーフロー又はSQLインジェクションからの保護

e) トランザクションが生成、処理、完結又は保管される法域における法令及び規制上の要求事項

f) 関与する全ての当事者のプライバシーの必要性

g) 秘密情報の保護に関する要求事項

h) 処理、転送及び保持するデータの保護

i) 関与する全ての当事者間の通信をセキュリティを保って暗号化する必要性

j) 完全性の確認及び入力の妥当性確認を含む入力の管理策

k) 自動化した管理策※1

※1 例えば、承認の回数制限又は二重承認の要求

l) 出力にアクセスできる人及びその認可も考慮した出力の管理策

m) “自由記述”欄の内容に関する制限、これは、機密データ※1を管理されずに保存することにつながり得るため。

※1 例えば、個人データ

n) トランザクションのログ取得及び監視、否認防止の要求事項など、業務プロセスに由来する要求事項

o) 他のセキュリティ管理策によって必要となる要求事項※1

※1 例えば、ログ取得及び監視システム並びに情報漏えい検知システムとのインタフェース

p) エラーメッセージの取扱い

**【トランザクションサービス】**

8d-8.26.4 組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。

a) 各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼のレベル

b) 交換又は処理する情報の完全性に必要な信頼のレベル、及び完全性の欠如を特定するための仕組み※1

※1 例えば、巡回冗長検査、ハッシュ化、ディジタル署名

c) 重要な取引文書の内容の承認、その発行、又はその文書への署名を誰が行えるかについての認可プロセス

d) 重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止※1

※1 例えば、入札手続、契約手続に関連する契約

e) トランザクションの機密性及び完全性※1

※1 例えば、注文、納入先の宛名情報及び受領確認

f) トランザクションの機密性を維持する期間に関する要求事項

g) 保険及びその他の契約上の要求事項

**【電子注文及び支払いアプリケーション】**

8d-8.26.5 電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。

a) 注文情報の機密性及び完全性を維持するための要求事項

b) 顧客から提供された支払い情報を検証するための、適切な検査の度合い

c) トランザクション情報の紛失又は重複の防止

d) トランザクションの詳細を、公開している環境の外で保管すること※1

※1 例えば、組織のイントラネット内に設置しているデータ保存環境とすること、及びインターネットから直接アクセス可能な電子記憶媒体上にそれらを保持して危険にさらさないこと

e) 信頼できる専門機関を利用※1する場合、エンド ツー エンドの証明書又は署名管理プロセスを通じたセキュリティの統合及び組込み

※1 例えば、ディジタル署名又はディジタル証明書の発行・維持の目的で利用

(8d-8.26参考) これらの考慮事項の幾つかは、法的要求事項を考慮に入れながら、暗号※1を適用することによって対応することが可能である※2。

※1 8c-8.24参照

※2 5g-5.31～5g-5.36を参照。特に、暗号に関連する法令については、5g-5.31を参照。

## 8d-8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

管理策：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開発活動に対して適用する。

目的： 情報システムを、開発のライフサイクルにおいてセキュリティに配慮して設計し、実装し、運用することを確実にするため。

詳細管理策

8d-8.27.1 セキュリティに配慮したシステム構築の原則を確立し、文書化し、情報システム構築活動に適用する。

8d-8.27.2 セキュリティは、全てのアーキテクチャ層（業務、データ、アプリケーション及び技術）において設計する。新技術は、セキュリティのリスクを分析し、その設計を既知の攻撃パターンに照らしてレビューする。

(8d-8.27参考) セキュリティに配慮したシステム構築の原則は、利用者認証技術、セキュリティを保ったセッション管理及びデータの妥当性確認並びにサニタイジングに関する詳細管理策となる。

8d-8.27.3 セキュリティに配慮したシステム構築の原則には、次の分析を含める。

a) 特定した脅威から情報及びシステムを保護するために必要なあらゆるセキュリティ管理策

b) セキュリティ事象を防止し、検知し又はそれに対応するセキュリティ管

理策の機能

c) 特定の業務プロセスに必要な特定のセキュリティ管理策※1

※1 例えば、取扱いに慎重を要する情報の暗号化、完全性の確認及び情報のディジタル署名

d) セキュリティ管理策をどこでどのように適用するか※1。

※1 例えば、セキュリティアーキテクチャ及び技術基盤と統合することによって

e) 個々のセキュリティ管理策（手動及び自動）を連携し、統合した管理策群を作る方法

8d-8.27.4 セキュリティに配慮したシステム構築の原則では、次の事項を考慮に入れる。

a) セキュリティアーキテクチャと統合する必要性

b) 技術的なセキュリティ基盤※1

※1 例えば、公開鍵基盤（PKI）、識別情報及びアクセスの管理（IAM）、データ漏えい防止、動的アクセス管理

c) 選択した技術を開発し、サポートする組織の能力

d) セキュリティ要求事項を満たすための費用、時間及び複雑さ

e) 最新の優れた慣行

8d-8.27.5 セキュリティに配慮したシステム構築には、次の事項を含める。

a) “設計によるセキュリティ（セキュリティバイデザイン）”、“多層防御”、“デフォルトでのセキュリティ”、“デフォルト拒否”、“故障時のセキュリティ”、“外部アプリケーションからの入力を信用しない”、“導入時のセキュリティ”、“違反の想定”、“最小特権”、“利便性及び管理性”、“最小機能”などの、セキュリティアーキテクチャの原則の使用

b) 情報セキュリティのぜい弱性を特定し、セキュリティ管理策を規定することを確実にし、セキュリティ要求事項を満たす助けとなる、セキュリティ指向の設計レビュー

c) 要求事項を完全には満たしていない※1セキュリティ管理策の文書化及び正式な承認

※1 例えば、安全に関する要求事項を優先するため

d) システムの要塞化（hardening）

8d-8.27.6 組織は、次のような“ゼロトラスト（zero trust）”の原則を考慮する。

a) 組織の情報システムは既に侵害されていることを想定し、ネットワーク境界のセキュリティだけに依存しない。

b) 情報システムへのアクセスにおいて“決して信頼せず、常に検証する”取組を採用する。

c) 情報システムへの要求がエンド ツー エンドで暗号化されることを確実にする。

d) 情報システムへの各要求を、組織の内部からのものであっても、公開の外部ネットワークから来たかのように検証する（すなわち、組織の境界の内側又は外側のいずれであれ、自動的に信頼することはしない。）。

e) “最小特権”及び動的アクセス制御手法を使用する※1。これは、情報又

はシステムへの要求の認証及び認可を、認証情報※2、利用者識別情報※3、利用者エンドポイント機器に関するデータ、データ分類※4などの、状況に関する情報に基づいて行うことを含む。

※1 5c-5.15、5c-5.18及び8a-8.2参照
※2 5c-5.17参照
※3 5c-5.16参照
※4 5b-5.12参照

f) 認証情報※1及び利用者識別情報※2、利用者エンドポイント機器に関するデータ、並びにデータ分類※3を含めた情報に基づいて、例えば、強力な認証※4を実行することによって、情報システムへの要求を常に認証し、認可要求の妥当性を常に確認する。

※1 5c-5.17参照
※2 5c-5.16参照
※3 5b-5.12参照
※4 多要素認証（8a-8.5参照）など

8d-8.27.7 確立したセキュリティに配慮したシステム構築の原則は、該当する場合には、組織と組織が外部委託した供給者との間の、契約及び拘束力をもつその他の合意を通じて、外部委託した情報システムの開発にも適用する。

8d-8.27.8 組織は、供給者のセキュリティに配慮したシステム構築の行為が組織のニーズと一致することを確実にする。

8d-8.27.9 セキュリティに配慮したシステム構築の原則及び確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするために、定期的にレビューする。

8d-8.27.10 セキュリティに配慮したシステム構築の原則及び確立した構築手順が、新規の潜在的な脅威に対抗するという点で常に最新であること、及び適用される技術及びソリューションの進展に継続して適用可能であることを確実にするために、定期的にレビューする。

## 8d-8.28 セキュリティに配慮したコーディング

管理策：セキュリティに配慮したコーディングの原則をソフトウェア開発に適用する。

目的： ソフトウェアをセキュリティに配慮して作成し、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。

詳細管理策

**【セキュリティに配慮したコーディング全般】**

8d-8.28.1 組織は、セキュリティに配慮したコーディングに関して優れたガバナンスを実現する、組織全体のプロセスを確立する。

8d-8.28.2 最低限のセキュリティに配慮したコーディングのベースラインを確立し、適用する。

8d-8.28.3 セキュリティに配慮したコーディングのためのプロセス及びガバナンスを、第三者から入手したソフトウェア構成要素及びオープンソースソフトウェアも対象とするように拡張する。

8d-8.28.4 組織は、組織のセキュリティに配慮したコーディングの原則を下記により方向付ける。

a) 現実世界の脅威、並びにソフトウェアのぜい弱性に関する最新の助言及び情報を監視する

b) 組織のセキュリティに配慮したコーディングの原則を継続的に改善する

c) 組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に施す

(8d-8.28.4参考) これは、急速に変化する脅威の状況に対抗するために、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。

**【計画及びコーディング前】**

8d-8.28.5 セキュリティに配慮したコーディングの原則を、新規の開発及び再利用の両方で使用する。

8d-8.28.6 セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及びサービスの両方に適用する。

8d-8.28.7 コーディング前の計画及び前提条件は、次の事項を含む。

a) 組織内及び外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び広く認められた原則

b) 情報セキュリティのぜい弱性につながる一般的及び歴史的なコーディング慣行及び欠陥

c) セキュリティに配慮したコードの作成を実施させるために、統合開発環境（IDE）などの開発ツールを構成する。

d) 該当する場合には、開発ツール及び実行環境の提供者が示す手引に従う。

e) 更新された開発ツール※1の維持及び使用

※1 例えば、コンパイラ

f) セキュリティに配慮したコードを作成する際の開発者の資格

g) 脅威モデリングを含むセキュリティに配慮した設計及びアーキテクチャ

h) セキュリティに配慮したコーディング標準、及び関係する場合はその使用を義務付けること

i) 開発のための管理された環境の使用

**【コーディング中】**

8d-8.28.8 コーディング中の考慮事項は、次の事項を含む。

a) 使用するプログラム言語及び手法に特有の、セキュリティに配慮したコーディング慣行

b) ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。

c) 構造化プログラミング手法を使用する。

d) コードを文書化し、情報セキュリティのぜい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。

e) セキュリティに配慮しない設計手法の使用を禁止する※1。

※1 例えば、ハードコード（決め打ち）されたパスワード、承認されていないコードサンプル及び認可されていないウェブサービスの使用

8d-8.28.9 セキュリティに配慮して作成するソフトウェアのテストは開発中及び開発後

に実施する※1。

※1 8d-8.29参照

（8d-8.28.9参考） 静的アプリケーションセキュリティテスト（SAST）プロセスで、ソフトウェアのセキュリティのぜい弱性を特定することが可能である。

8d-8.28.10 ソフトウェアの運用を開始する前に、次の事項を評価する。

a) 攻撃対象領域（attack surface）及び最小特権の原則

b) 最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。

**【レビュー及び保守】**

8d-8.28.11 コードの運用が開始された後、次のことを行う。

a) 更新はセキュリティに配慮してパッケージ化し、適用する。

b) 報告された情報セキュリティのぜい弱性に対処する※1。

※1 8b-8.8参照

c) エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。

d) ソースコードを、認可されていないアクセス及び改ざんから保護する※1。

※1 例えば、アクセス制御、版管理などの機能を提供する構成管理ツールを使用する

8d-8.28.12 外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。

a) 外部ライブラリを管理し※1、リリースサイクルに合わせて規則正しく更新することを確実にする。

※1 例えば、使用するライブラリ及びそれらの版の目録を維持することによる

b) 十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用

c) 外部の構成要素の使用許諾、セキュリティ及び履歴

d) ソフトウェアが保守可能で、追跡することができ、実証された定評のある供給元に由来することを確実にする。

e) 開発資源及び成果物の十分に長期的な可用性

8d-8.28.13 ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。

a) 組み込まれた管理策及び完全性プロセスが危険にさらされるリスク

b) 業者の同意を得るかどうか。

c) 標準のプログラム更新として業者から必要な変更を得る可能性

d) 変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響

e) 使用中の他のソフトウェアとの互換性

### 8d-8.29 開発及び受入れにおけるセキュリティテスト

管理策：セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。

目的： アプリケーション又はコードを本番環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの妥当性確認をするため。

詳細管理策

8d-8.29.1　新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて綿密に試験し、検証する。

8d-8.29.2　セキュリティテストは、システム又は構成要素のテストに統合し、その一部とする。

8d-8.29.3　セキュリティテストは、機能的又は非機能的に表現することができる一連の要求事項に照らして実施する。

8d-8.29.4　セキュリティテストは、次の事項のテストを含む。

a) セキュリティ機能※1

※1 例えば、利用者認証（8a-8.5参照）、アクセス制限（8a-8.3参照）及び暗号の利用（8c-8.24参照）

b) セキュリティに配慮したコーディング※1

※1 8d-8.28参照

c) オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成※1

※1 8b-8.9、8c-8.20及び8c-8.22参照

8d-8.29.5　セキュリティテスト計画は、一連の判定基準を使用して決定する。

8d-8.29.6　セキュリティテストの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。

8d-8.29.7　セキュリティテスト計画には次の事項を含める。

a) 活動及びテストの詳細スケジュール

b) 一連の条件の下での入力及び予想される出力

c) 結果を評価する基準

d) 必要な場合、更なる処置の決定

8d-8.29.8　組織は、セキュリティに関係する欠陥の修正を検証する。

（8d-8.29.8参考）　検証には、コード分析ツール又はぜい弱性スキャナなどの自動化ツールを利用することができる。

8d-8.29.9　組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。

a) 最初に開発チームが実施する。

b) その次に、システムが期待どおりに、かつ、期待した形でだけ動作することを確実にするために、独立した受入れテストを実施する※1。

※1 5a-5.8参照

8d-8.29.10　セキュリティのテストにおいて、次の事項を考慮する。

a) セキュリティの欠陥のテストに関連して、予期しない入力及び条件を含め、コードのレビュー活動を実施する。

b) セキュリティに配慮していない構成及びシステムのぜい弱性を特定するために、ぜい弱性スキャンを実施する。

c) セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。

8d-8.29.11　外部委託した開発、及び購入した構成要素については、取得プロセスに従う。

8d-8.29.12　供給者との契約では、特定したセキュリティ要求事項に言及する※1。

※1 5d-5.20参照

8d-8.29.13　外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づく判定基準に照らして評価する。

8d-8.29.14　セキュリティテストは、システムが組織の環境にぜい弱性をもたらさないこと及びテストが信頼できるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する※1。

※1 8d-8.31参照

## 8d-8.30　外部委託による開発

管理策：組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。

目的：　組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。

詳細管理策

8d-8.30.1　システム開発を外部委託する場合には、次の事項を行う。

a) 要求事項及び期待を伝達する。

b) 要求事項を満たし、期待に応えることを合意する。

c) 外部委託から提供された作業及び成果物がこの期待を満たすかどうかを継続的に監視する。

d) 開発されたシステムをレビューする。

8d-8.30.2　組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。

a) 外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権※1

※1 5g-5.32参照

b) セキュリティに配慮した設計、コーディング及びテストの実施についての契約上の要求事項※1

※1 8d-8.25～8d-8.29参照

c) 外部の開発者が考慮すべき脅威モデルの提供

d) 成果物の質及び正確さに関する受入れテスト※1

※1 8d-8.29参照

e) 受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出※1

※1 例えば、保証報告書

f) 引渡しに当たって、悪意のある内容（意図的なもの及び意図しないもの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出

g) 既知のぜい弱性が含まれないよう、十分なテストを実施していることを示す証拠の提出

h) ソフトウェアソースコードの預託契約※1

※1 例えば、供給者が事業を終了する場合

i) 開発のプロセス及び管理策を監査する、契約に基づく権利

j) 開発環境のセキュリティ要求事項※1

※1 8d-8.31参照

k) 適用される法令※1の考慮

※1 例えば、個人データの保護に関する法令

### 8d-8.31　開発環境、テスト環境及び本番環境の分離

管理策：開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。

目的：　開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。

詳細管理策

8d-8.31.1　本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。

8d-8.31.2　開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。

a) 開発システムと本番システムとを適切に分離し、それらを異なる領域で※1運用する。

※1 例えば、別々の仮想環境又は物理環境で

b) 開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。

c) 本番システム及びアプリケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする※1。

※1 8d-8.29参照

d) 特定し、承認された状況を除いて、本番環境ではテストを行わない。

e) コンパイラ、エディタ、及びその他の開発ツール又はユーティリティプログラムは、必要がないときには、本番システムからアクセス可能としない。

f) 誤りのリスクを減らすために、メニューに適切な環境識別ラベルを表示する。

g) 取扱いに慎重を要する情報は、開発システム及びテストシステムに同等の管理策が備わっていない限り、その開発システム環境及びテストシステム環境にはコピーしない。

8d-8.31.3　全ての場合において、開発環境及びテスト環境は、次の事項を考慮して保護する。

a) 全ての開発、統合及びテストツール（ビルダ、インテグレータ、コンパイラ、構成システム及びライブラリを含む。）のパッチ適用及び更新

b) システム及びソフトウェアのセキュリティに配慮した構成

c) 環境へのアクセスの制御

d) 環境の変更及びそこに保存されているコードの監視

e) 環境の、セキュリティに配慮した監視

f) 環境のバックアップをとること

8d-8.31.4　一人の人間が、事前のレビュー及び承認なしに、開発環境及び本番環境の両方に変更を加えることができないようにする。

（8d-8.31.4参考）　これは、例えばアクセス権の分離又は監視を伴う規則によって達成可能である。

8d-8.31.5　通常と異なる状況では、認可されていない変更を検出し、対処するために、

詳細なログ取得、リアルタイム監視などの追加の対策を実施する。

### 8d-8.32　変更管理

管理策：情報処理設備及び情報システムの変更は、変更管理手順に従う。

目的：　変更を実行するときに情報セキュリティを維持するため。

詳細管理策

8d-8.32.1　新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、テスト、品質管理及び管理された実装についての合意された規則及び正式な手続に従う。

8d-8.32.2　情報処理設備及び情報システムの全ての変更を良好に管理することを確実にするように、管理責任及び手順を設ける。

8d-8.32.3　変更管理手順は、情報処理設備及び情報システムにおける情報の機密性、完全性及び可用性を確実にするために、設計の初期段階からその後の全ての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装する。

8d-8.32.4　実施可能な場合には、ICT基盤及びソフトウェアの変更管理手順を統合する。

8d-8.32.5　変更管理手順には、次の事項を含む。

a）全ての依存関係を考慮した、変更の潜在的影響に関する計画策定及び評価

b）変更の認可

c）関連する利害関係者への変更の伝達

d）変更のテスト及びテストの受入れ※1

※1 8d-8.29参照

e）導入計画を含む変更の実施

f）フォールバック手順（代替手順）を含む緊急時及び不測の事態の考慮

g）上記の全てを含む変更の記録の維持

h）運用文書類※1及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすること

※1 5g-5.37参照

i）ICT継続計画並びに対応及び復旧手順※1が、適切な状態であるように、必要に応じて変更することを確実にすること

※1 5f-5.30参照

### 8d-8.33　テスト用情報

管理策：テスト用情報は、適切に選定し、保護し、管理する。

目的：　テストの適切な実施、及びテストに使用する運用情報の保護を確実にするため。

詳細管理策

8d-8.33.1　テスト結果の信頼性及び関連する運用情報の機密性を確実にするように、テスト用情報を選択する。

8d-8.33.2　取扱いに慎重を要する情報（PIIを含む。）を、開発環境及びテスト環境へ複製しない※1。

※1 8d-8.31参照

8d-8.33.3　運用情報の複製をテスト目的で用いる場合は、その保護のために、テスト環境を組織内又はクラウドサービス上のいずれに構築しているかにかかわらず、次の事項を適用する。

a) 運用環境に適用するものと同じアクセス制御手順をテスト環境に適用する。

b) 運用情報の複製をテスト環境に置く場合は、その都度認可を受ける。

c) 運用情報の複製及び利用は、監査証跡とするためにログをとる。

d) テストに使用する場合、取扱いに慎重を要する情報は、削除又はマスキング※1によって保護する。

※1 8b-8.11参照

e) テスト用情報の認可されていない使用を防止するために、テストの完了直後にテスト環境から運用情報を適切に削除※1する。

※1 8b-8.10参照

8d-8.33.4　テスト用情報は、セキュリティに配慮して保存し（結果を無効にする可能性がある改ざんを防止するため）、テスト目的でだけ使用する。

## 8d-8.34　監査におけるテスト中の情報システムの保護

管理策：運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意する。

目的：　監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。

詳細管理策

8d-8.34.1　監査におけるテスト中の情報システムの保護のための管理策の実施については、次の事項を守る。

a) システム及びデータへのアクセスに関する監査要求は、適切な管理層の同意を得る。

b) 技術監査におけるテストの範囲を、合意し、管理する。

c) 監査におけるテストは、ソフトウェア及びデータの読出し専用のアクセスに限定する。必要な情報を取得するために参照専用のアクセスを利用できない場合、監査人に代わって必要なアクセス権をもつ経験豊かな実務管理者がテストを実行する。

d) アクセスを許可する場合、許可する前にシステムへのアクセスに使用する装置・機器※1のセキュリティ要求事項※2を確立し、検証する。

※1 例えば、ラップトップ又はタブレット

※2 例えば、ウイルス対策及びパッチ適用

e) 読出し専用以外のアクセスは、システムファイルの隔離された複製に対してだけ許可し、それらの複製は、監査が完了した時点で削除するか、又は監査の文書化の要求によってそのようなファイルを保存する義務があるときは、適切に保護する。

f) 監査ツールの実行など、特別又は追加の処理に関する要求を特定し、合意する。

g) 監査におけるテストがシステムの可用性に影響する可能性がある場合、こうしたテストは営業時間外に実施する。
h) 監査及びテストを目的とする全てのアクセスを監視し、ログをとる。

## VI. 用語集

本管理基準で用いている用語の定義は次表の通りである。原則としてJIS Q 27002:2024における定義に準拠しているが、同規格にて定義されていないものについてはJIS Q 27000:2019又は独自の定義を用いている。

| | | 用語 | 意味 | 出典規格 |
|---|---|---|---|---|
| あ | 1 | アクセス制御（access control） | 資産への物理的及び論理的アクセスが、事業上及び情報セキュリティの要求事項に基づいて認可及び制限されることを確実にする手段。 | JIS Q 27002:2024 |
| | 2 | 受渡記録（chain of custody） | ある時点から別の時点までの資料の実証可能な所持、移動、取扱い、及び場所。 | JIS Q 27002:2024 |
| | 3 | エンティティ（entity） | ある領域の運用に関与する、他と区別して認識できる存在であるアイテム。 | JIS Q 27002:2024 |
| | 4 | エンドポイント機器（endpoint device） | ネットワーク接続された情報通信技術（ICT）ハードウェア機器。 | JIS Q 27002:2024 |
| | 5 | 起こりやすさ（likelihood） | 何かが起こる可能性。 | JIS Q 27000:2019 |
| か | 6 | 外部委託する（outsource） | ある組織の機能又はプロセスの一部を外部の組織が実施するという取決めを行う。 | JIS Q 27000:2019 |
| | 7 | 外部状況（external context） | 組織が自らの目的を達成しようとする場合の外部環境。 | JIS Q 27000:2019 |
| | 8 | ガバナンス主体 | 情報セキュリティガバナンスの目的の設定及びプロセスの定義に関する責任を担う主体。 | 本管理基準にて定義 |
| | 9 | 可用性（availability） | 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。 | JIS Q 27000:2019 |
| | 10 | 監査（audit） | 監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセス。 | JIS Q 27000:2019 |
| | 11 | 監査範囲（audit scope） | 監査の及ぶ領域及び境界。 | JIS Q 27000:2019 |
| | 12 | 監視（monitoring） | システム、プロセス又は活動の状況を明確にすること。 | JIS Q 27000:2019 |
| | 13 | 完全性（integrity） | 正確さ及び完全さの特性。 | JIS Q 27000:2019 |
| | 14 | 管理策（control） | リスクを維持及び／又は修正する対策。 | JIS Q 27002:2024 |
| | 15 | 管理層（management） | 組織のそれぞれの階層にある部署の責任者。 | 本管理基準にて定義 |
| | 16 | 規則（rule） | 何をすることが求められるか、何が許されるか又は許されないかについて組織の期待を述べている、組織が認めた原則又は指示。 | JIS Q 27002:2024 |
| | 17 | 機密性（confidentiality） | 認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。 | JIS Q 27000:2019 |
| | 18 | 脅威（threat） | システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。 | JIS Q 27002:2024 |
| | 19 | 記録（record） | 法的な義務の遂行において又は業務の処理において、組織又は個人によって証拠及び資産として作成、受領及び維持された情報。 | JIS Q 27002:2024 |
| | 20 | 経営陣（governing body） | 組織のパフォーマンス及び適合性について説明責任を負う個人又はグループ。 | JIS Q 27000:2019 |
| | 21 | 継続的改善（continual improvement） | パフォーマンスを向上するために繰り返し行われる活動。 | JIS Q 27000:2019 |
| | 22 | 結果（consequence） | 目的に影響を与える事象の結末（outcome）。 | JIS Q 27000:2019 |
| | 23 | 公開透明性ファイル（public | 第三者が確認できるようにすることで運用における透明性を確保することを目的として公開されるファイル。 | 本管理基準にて定義 |

| | | 用語 | 意味 | 出典規格 |
|---|---|---|---|---|
| | | transparency file） | | |
| | 24 | 攻撃（attack） | 成功した又は不成功の、資産の認可されていない破壊、改ざん、無効化、アクセスの試み、又は資産の暴露、盗用、若しくは認可されていない使用の試み。 | JIS Q 27002:2024 |
| | 25 | 個人識別可能情報（PII: personally identifiable information） | （a）情報と、これに関連する自然人との間のひも（紐）付けを確立するために利用され得る情報、又は（b）自然人に直接若しくは間接にひも（紐）付けられるか又はその可能性がある情報 | JIS Q 27002:2024 |
| さ | 26 | 残留リスク（residual risk） | リスク対応後に残っているリスク。 | JIS Q 27000:2019 |
| | 27 | 事業の中断・阻害（disruption） | 予見されたか、されなかったかにかかわらず、組織の目的に従って想定される製品及びサービスの提供では計画されておらず、好ましくない逸脱を引き起こすインシデント。 | JIS Q 27002:2024 |
| | 28 | 資産（asset） | 組織にとって価値のある全てのもの。 | JIS Q 27002:2024 |
| | 29 | 事象（event） | ある一連の周辺状況の出現又は変化。 | JIS Q 27000:2019 |
| | 30 | 指標（indicator） | 見積り又は評価を示す測定量。 | JIS Q 27000:2019 |
| | 31 | 修正（correction） | 検出された不適合を除去するための処置。 | JIS Q 27000:2019 |
| | 32 | 情報システム（information system） | アプリケーション、サービス、IT 資産、又は情報を取り扱う他の構成要素などの組合せ。 | JIS Q 27002:2024 |
| | 33 | 情報処理施設・設備（information processing facilities） | あらゆる情報処理のシステム、サービス若しくは基盤、又はこれらを収納する物理的場所。 | JIS Q 27002:2024 |
| | 34 | 情報セキュリティ（information security） | 情報の機密性、完全性及び可用性を維持すること。 | JIS Q 27000:2019 |
| | 35 | 情報セキュリティインシデント（information security incident） | 組織の資産に害を及ぼす又はその運用を危うくする可能性のある一つ以上の関連する特定された情報セキュリティ事象。 | JIS Q 27002:2024 |
| | 36 | 情報セキュリティインシデント管理（information security incident management） | 情報セキュリティインシデントの取扱いに対する一貫した有効な取組の実行。 | JIS Q 27002:2024 |
| | 37 | 情報セキュリティガバナンス（governance of information security） | 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。 | JIS Q 27000:2019 |
| | 38 | 情報セキュリティ事象（information security event） | 情報セキュリティ侵害又は管理策の不具合の可能性を示す事象。 | JIS Q 27000:2019 |
| | 39 | 情報セキュリティ侵害（information security breach） | 送信、保存又はその他の処理がなされる保護された情報の望ましくない破壊、損失、改ざん、開示、又はそうした情報へのアクセスにつながる情報セキュリティの毀損。 | JIS Q 27002:2024 |
| | 40 | 真正性（authenticity） | エンティティは、それが主張するとおりのものであるという特性。 | JIS Q 27002:2024 |

| | | 用語 | 意味 | 出典規格 |
|---|---|---|---|---|
| | 41 | 信頼性（reliability） | 意図する行動と結果とが一貫しているという特性。 | JIS Q 27002:2024 |
| | 42 | ステークホルダ（stakeholder） | （「利害関係者」（推奨用語）と同意（許容用語）） | JIS Q 27000:2019 |
| | 43 | ぜい弱性（vulnerability） | 一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。 | JIS Q 27002:2024 |
| | 44 | 是正処置（corrective action） | 不適合の原因を除去し、再発を防止するための処置。 | JIS Q 27000:2019 |
| | 45 | 測定（measurement） | 値を決定するプロセス。 | JIS Q 27000:2019 |
| | 46 | 測定方法（measurement method） | 特定の尺度に関して属性を定量化するために使う一連の操作の論理的な順序を一般的に記述したもの。 | JIS Q 27000:2019 |
| | 47 | 組織（organization） | 自らの目的を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。 | JIS Q 27000:2019 |
| た | 48 | 適合（conformity） | 要求事項を満たしていること。 | JIS Q 27000:2019 |
| | 49 | 手順（procedure） | 活動又はプロセスを実行するために規定された方法。 | JIS Q 27002:2024 |
| | 50 | データマスキング（data masking） | データのうち取扱いに慎重を要するものについて、具体的な内容が明らかにならないようにするための加工。仮名化や匿名化を含む。 | 本管理基準にて定義 |
| | 51 | トップマネジメント（top management） | 最高位で組織を指揮し、管理する個人又は人々の集まり。 | JIS Q 27000:2019 |
| | | | 情報セキュリティマネジメントを行う組織の長（または責任者）。<br>（注）「情報セキュリティマネジメントを行う組織」は部門単位であることがあり、複数の組織が一つの企業や機関の中に存在することがある。 | 本管理基準にて定義 |
| | 52 | トピック固有の方針（topic-specific policy） | 適切なマネジメントレベルで正式に表明された、固有の主題又はトピックに関する意図及び方向付け。 | JIS Q 27002:2024 |
| | 53 | 取扱いに慎重を要する情報（sensitive information） | 個人、組織、国家安全保障又は公共安全に悪影響を与える可能性があるため、利用不能、認可されていないアクセス、変更又は開示から保護する必要がある情報。 | JIS Q 27002:2024 |
| な | 54 | 内部状況（internal context） | 組織が自らの目的を達成しようとする場合の内部環境。 | JIS Q 27000:2019 |
| | 55 | 認証（authentication） | エンティティの主張する特性が正しいという保証の提供。 | JIS Q 27002:2024 |
| は | 56 | パフォーマンス（performance） | 測定可能な結果。 | JIS Q 27000:2019 |
| | 57 | PII 主体（PII principal） | PII に関連する自然人。 | JIS Q 27002:2024 |
| | 58 | 否認防止（non-repudiation） | 主張された事象又は処置の発生、及びそれらを引き起こしたエンティティを証明する能力。 | JIS Q 27002:2024 |
| | 59 | 秘密情報（confidential information） | 認可されていない個人、エンティティ又はプロセスに対して、使用させる又は開示することを意図していない情報。 | JIS Q 27002:2024 |
| | 60 | 不適合（non-conformity） | 要求事項を満たしていないこと。 | JIS Q 27000:2019 |
| | 61 | プロセス（process） | インプットを使用又は変換して結果を生み出す、相互に関連する又は相互に作用する一連の活動。 | JIS Q 27002:2024 |
| | 62 | 文書化した情報（documented | 組織が管理し、維持するよう要求されている情報、及びそれが含まれている媒体。 | JIS Q 27000:2019 |

| | | 用語 | 意味 | 出典規格 |
|---|---|---|---|---|
| | | information) | | |
| | 63 | 方針（policy） | トップマネジメントによって正式に表明された組織の意図及び方向付け。 | JIS Q 27002:2024 |
| ま | 64 | マネジメントシステム（management system） | 方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素。 | JIS Q 27000:2019 |
| | 65 | 目的（objective） | 達成する結果。 | JIS Q 27000:2019 |
| | 66 | 目標復旧時間（RTO: recovery time objective） | 事業の中断・阻害が発生した後、最小限のサービス及び／又は製品並びにサポートシステム、アプリケーション、又は機能をその中で復旧すべき期間。 | JIS Q 27002:2024 |
| | 67 | 目標復旧時点（RPO: recovery point objective） | 事業の中断・阻害が発生した後にデータを復旧すべき時点。 | JIS Q 27002:2024 |
| や | 68 | 有効性（effectiveness） | 計画した活動を実行し、計画した結果を達成した程度。 | JIS Q 27000:2019 |
| | 69 | 要員（personnel） | 組織の指示の下で仕事をしている人々。 | JIS Q 27002:2024 |
| | 70 | 要求事項（requirement） | 明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待。 | JIS Q 27000:2019 |
| ら | 71 | 利害関係者（interested party） | ある決定事項若しくは活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している、個人又は組織。 | JIS Q 27002:2024 |
| | 72 | 力量（competence） | 意図した結果を達成するために、知識及び技能を適用する能力。 | JIS Q 27000:2019 |
| | 73 | リスク（risk） | 目的に対する不確かさの影響。 | JIS Q 27000:2019 |
| | 74 | リスクアセスメント（risk assessment） | リスク特定、リスク分析及びリスク評価のプロセス全体。 | JIS Q 27000:2019 |
| | 75 | リスク基準（risk criteria） | リスクの重大性を評価するための目安とする条件。 | JIS Q 27000:2019 |
| | 76 | リスク受容（risk acceptance） | ある特定のリスクをとるという情報に基づいた意思決定。 | JIS Q 27000:2019 |
| | 77 | リスク所有者（risk owner） | リスクを運用管理することについて、アカウンタビリティ及び権限をもつ人又は主体。 | JIS Q 27000:2019 |
| | 78 | リスク対応（risk treatment） | リスクを修正するプロセス。 | JIS Q 27000:2019 |
| | 79 | リスク認識（risk awareness） | リスク（目的に対する不確かさの影響）の存在を単に知るだけでなく、より一歩進めて組織としてリスクに対してどのような対策をしなければならないかまで含めて認識すること。 | 情報セキュリティ管理基準活用ガイドラインにて定義 |
| | 80 | リスク評価（risk evaluation） | リスク及び／又はその大きさが受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。 | JIS Q 27000:2019 |
| | 81 | リスク分析（risk analysis） | リスクの特質を理解し、リスクレベルを決定するプロセス。 | JIS Q 27000:2019 |
| | 82 | リスクマネジメント（risk management） | リスクについて、組織を指揮統制するための調整された活動。 | JIS Q 27000:2019 |
| | 83 | リスクマネジメントプロセス（risk management process） | コミュニケーション、協議及び組織の状況の確定の活動、並びにリスクの特定、分析、評価、対応、監視及びレビューの活動に対する、運用管理方針、手順及び実務の体系的な適用。 | JIS Q 27000:2019 |

| | | 用語 | 意味 | 出典規格 |
|---|---|---|---|---|
| | 84 | リスクレベル（level of risk） | 結果とその起こりやすさの組合せとして表現される、リスクの大きさ。 | JIS Q 27000:2019 |
| | 85 | 利用者（user） | 組織の情報システムにアクセスする利害関係者。 | JIS Q 27002:2024 |
| | 86 | 利用者エンドポイント機器（user endpoint device） | 利用者が情報処理サービスにアクセスするために使用するエンドポイント機器。 | JIS Q 27002:2024 |
| | 87 | レビュー（review） | 確定された目的を達成するため、対象となる事柄の適切性、妥当性及び有効性を決定するために実行される活動。 | JIS Q 27000:2019 |

## Ⅶ. 属性一覧

Ⅴで示した管理策基準の各管理策について、JIS Q 27002:2024で定義されている属性の一覧を示す。

＜記号凡例＞

| | | | | | |
|---|---|---|---|---|---|
| 管理策タイプ | P | #予防 | 運用機能 | G | #ガバナンス |
| | D | #検知(Detective) | | As | #資産管理 |
| | C | #是正 | | IP | #情報保護 |
| 情報セキュリティ特性 | C | #機密性 | | H | #人的資源のセキュリティ |
| | I | #完全性 | | P | #物理的セキュリティ |
| | A | #可用性 | | Sy | #システム及びネットワークのセキュリティ |
| サイバーセキュリティ概念 | I | #識別 | | Ap | #アプリケーションセキュリティ |
| | P | #防御(Protect) | | Se | #セキュリティを保った構成 |
| | D | #検知(Detect) | | Id | #識別情報及びアクセスの管理 |
| | Rs | #対応 | | T | #脅威及びぜい弱性の管理 |
| | Rc | #復旧 | | C | #継続 |
| セキュリティドメイン | G | #ガバナンス及びエコシステム | | Su | #供給者関係のセキュリティ |
| | P | #保護 | | L | #法令及び順守 |
| | D | #防御(Defence) | | IE | #情報セキュリティ事象管理 |
| | R | #レジリエンス | | IA | #情報セキュリティ保証 |

| 識別子 | 管理策名 | 管理策タイプ | 情報セキュリティ特性 | サイバーセキュリティ概念 | 運用機能 | セキュリティドメイン |
|---|---|---|---|---|---|---|
| 5a-5.1 | 情報セキュリティのための方針群 | P | C, I, A | I | G | G, R |
| 5a-5.2 | 情報セキュリティの役割及び責任 | P | C, I, A | I | G | G, P, R |
| 5a-5.3 | 職務の分離 | P | C, I, A | P | G, Id | G |
| 5a-5.4 | 管理層の責任 | P | C, I, A | I | G | G |
| 5a-5.5 | 関係当局との連絡 | P, C | C, I, A | I, P, Rs, Rc | G | D, R |
| 5a-5.6 | 専門組織との連絡 | P, C | C, I, A | P, Rs, Rc | G | D |
| 5a-5.7 | 脅威インテリジェンス | P, D, C | C, I, A | I, D, Rs | T | D, R |
| 5a-5.8 | プロジェクトマネジメントにおける情報セキュリティ | P | C, I, A | I, P | G | G, P |
| 5b-5.9 | 情報及びその他の関連資産の目録 | P | C, I, A | I | As | G, P |
| 5b-5.10 | 情報及びその他の関連資産の許容される利用 | P | C, I, A | P | As, IP | G, P |
| 5b-5.11 | 資産の返却 | P | C, I, A | P | As | P |
| 5b-5.12 | 情報の分類 | P | C, I, A | I | IP | P, D |
| 5b-5.13 | 情報のラベル付け | P | C, I, A | P | IP | P, D |
| 5b-5.14 | 情報の転送 | P | C, I, A | P | As, IP | P |
| 5c-5.15 | アクセス制御 | P | C, I, A | P | Id | P |
| 5c-5.16 | 識別情報の管理 | P | C, I, A | P | Id | P |
| 5c-5.17 | 認証情報 | P | C, I, A | P | Id | P |
| 5c-5.18 | アクセス権 | P | C, I, A | P | Id | P |
| 5d-5.19 | 供給者関係における情報セキュリティ | P | C, I, A | I | Su | G, P |

| 識別子 | 管理策名 | 管理策タイプ | 情報セキュリティ特性 | サイバーセキュリティ概念 | 運用機能 | セキュリティドメイン |
|---|---|---|---|---|---|---|
| 5d-5.20 | 供給者との合意における情報セキュリティの取扱い | P | C, I, A | I | Su | G, P |
| 5d-5.21 | ICT サプライチェーンにおける情報セキュリティの管理 | P | C, I, A | I | Su | G, P |
| 5d-5.22 | 供給者のサービス提供の監視、レビュー及び変更管理 | P | C, I, A | I | Su, IA | G, P, D |
| 5d-5.23 | クラウドサービスの利用における情報セキュリティ | P | C, I, A | P | Su | G, P |
| 5e-5.24 | 情報セキュリティインシデント管理の計画策定及び準備 | C | C, I, A | Rs, Rc | G, IE | D |
| 5e-5.25 | 情報セキュリティ事象の評価及び決定 | D | C, I, A | D, Rs | IE | D |
| 5e-5.26 | 情報セキュリティインシデントへの対応 | C | C, I, A | Rs, Rc | IE | D |
| 5e-5.27 | 情報セキュリティインシデントからの学習 | P | C, I, A | I, P | IE | D |
| 5e-5.28 | 証拠の収集 | C | C, I, A | D, Rs | IE | D |
| 5f-5.29 | 事業の中断・阻害時の情報セキュリティ | P, C | C, I, A | P, Rs | C | P, R |
| 5f-5.30 | 事業継続のための ICT の備え | C | A | Rs | C | R |
| 5g-5.31 | 法令、規制及び契約上の要求事項 | P | C, I, A | I | L | G, P |
| 5g-5.32 | 知的財産権 | P | C, I, A | I | L | G |
| 5g-5.33 | 記録の保護 | P | C, I, A | I, P | L, As, IP | D |
| 5g-5.34 | プライバシー及び PII の保護 | P | C, I, A | I, P | IP, L | P |
| 5g-5.35 | 情報セキュリティの独立したレビュー | P, C | C, I, A | I, P | IA | G |
| 5g-5.36 | 情報セキュリティのための方針群、規則及び標準の順守 | P | C, I, A | I, P | L, IA | G |
| 5g-5.37 | 操作手順書 | P, C | C, I, A | P, Rc | As, P, Sy, Ap, Se, Id, T, C, IE | G, P, D |
| 6a-6.1 | 選考 | P | C, I, A | P | H | G |
| 6a-6.2 | 雇用条件 | P | C, I, A | P | H | G |
| 6a-6.3 | 情報セキュリティの意識向上、教育及び訓練 | P | C, I, A | P | H | G |
| 6a-6.4 | 懲戒手続 | P, C | C, I, A | P, Rs | H | G |
| 6a-6.5 | 雇用の終了又は変更後の責任 | P | C, I, A | P | H, As | G |
| 6a-6.6 | 秘密保持契約又は守秘義務契約 | P | C | P | H, IP, Su | G |
| 6a-6.7 | リモートワーク | P | C, I, A | P | As, IP, P, Sy | P |
| 6a-6.8 | 情報セキュリティ事象の報告 | D | C, I, A | D | IE | D |
| 7a-7.1 | 物理的セキュリティ境界 | P | C, I, A | P | P | P |
| 7a-7.2 | 物理的入退 | P | C, I, A | P | P, Id | P |
| 7a-7.3 | オフィス、部屋及び施設のセキュリティ | P | C, I, A | P | P, As | P |
| 7a-7.4 | 物理的セキュリティの監視 | P, D | C, I, A | P, D | P | P, D |
| 7a-7.5 | 物理的及び環境的脅威からの保護 | P | C, I, A | P | P | P |
| 7a-7.6 | セキュリティを保つべき領域での作業 | P | C, I, A | P | P | P |
| 7a-7.7 | クリアデスク・クリアスクリーン | P | C | P | P | P |
| 7b-7.8 | 装置の設置及び保護 | P | C, I, A | P | P, As | P |
| 7b-7.9 | 構外にある資産のセキュリティ | P | C, I, A | P | P, As | P |
| 7b-7.10 | 記憶媒体 | P | C, I, A | P | P, As | P |

| 識別子 | 管理策名 | 管理策タイプ | 情報セキュリティ特性 | サイバーセキュリティ概念 | 運用機能 | セキュリティドメイン |
|---|---|---|---|---|---|---|
| 7b-7.11 | サポートユーティリティ | P, D | I, A | P, D | P | P |
| 7b-7.12 | ケーブル配線のセキュリティ | P | C, A | P | P | P |
| 7b-7.13 | 装置の保守 | P | C, I, A | P | P, As | P, R |
| 7b-7.14 | 装置のセキュリティを保った処分又は再利用 | P | C | P | P, As | P |
| 8a-8.1 | 利用者エンドポイント機器 | P | C, I, A | P | As, IP | P |
| 8a-8.2 | 特権的アクセス権 | P | C, I, A | P | Id | P |
| 8a-8.3 | 情報へのアクセス制限 | P | C, I, A | P | Id | P |
| 8a-8.4 | ソースコードへのアクセス | P | C, I, A | P | Id, Ap, Se | P |
| 8a-8.5 | セキュリティを保った認証 | P | C, I, A | P | Id | P |
| 8a-8.6 | 容量・能力の管理 | P, D | I, A | I, P, D | C | G, P |
| 8b-8.7 | マルウェアに対する保護 | P, D, C | C, I, A | P, D | Sy, IP | P, D |
| 8b-8.8 | 技術的ぜい弱性の管理 | P | C, I, A | I, P | T | G, P, D |
| 8b-8.9 | 構成管理 | P | C, I, A | P | Se | P |
| 8b-8.10 | 情報の削除 | P | C | P | IP, L | P |
| 8b-8.11 | データマスキング | P | C | P | IP | P |
| 8b-8.12 | データ漏えい防止 | P, D | C | P, D | IP | P, D |
| 8b-8.13 | 情報のバックアップ | C | I, A | Rc | C | P |
| 8b-8.14 | 情報処理施設・設備の冗長性 | P | A | P | C, As | P, R |
| 8b-8.15 | ログ取得 | D | C, I, A | D | IE | P, D |
| 8b-8.16 | 監視活動 | D, C | C, I, A | D, Rs | IE | D |
| 8b-8.17 | クロックの同期 | D | I | P, D | IE | P, D |
| 8b-8.18 | 特権的なユーティリティプログラムの使用 | P | C, I, A | P | Sy, Se, Ap | P |
| 8b-8.19 | 運用システムへのソフトウェアの導入 | P | C, I, A | P | Se, Ap | P |
| 8c-8.20 | ネットワークセキュリティ | P, D | C, I, A | P, D | Sy | P |
| 8c-8.21 | ネットワークサービスのセキュリティ | P | C, I, A | P | Sy | P |
| 8c-8.22 | ネットワークの分離 | P | C, I, A | P | Sy | P |
| 8c-8.23 | ウェブフィルタリング | P | C, I, A | P | Sy | P |
| 8c-8.24 | 暗号の利用 | P | C, I, A | P | Se | P |
| 8d-8.25 | セキュリティに配慮した開発のライフサイクル | P | C, I, A | P | Ap, Sy | P |
| 8d-8.26 | アプリケーションセキュリティの要求事項 | P | C, I, A | P | Ap, Sy | P, D |
| 8d-8.27 | セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 | P | C, I, A | P | Ap, Sy | P |
| 8d-8.28 | セキュリティに配慮したコーディング | P | C, I, A | P | Ap, Sy | P |
| 8d-8.29 | 開発及び受入れにおけるセキュリティテスト | P | C, I, A | I | Ap, IA, Sy | P |
| 8d-8.30 | 外部委託による開発 | P, D | C, I, A | I, P, D | Sy, Ap, Su | G, P |
| 8d-8.31 | 開発環境、テスト環境及び本番環境の分離 | P | C, I, A | P | Ap, Sy | P |
| 8d-8.32 | 変更管理 | P | C, I, A | P | Ap, Sy | P |

| 識別子 | 管理策名 | 管理策タイプ | 情報セキュリティ特性 | サイバーセキュリティ概念 | 運用機能 | セキュリティドメイン |
|---|---|---|---|---|---|---|
| 8d-8.33 | テスト用情報 | P | C, I | P | IP | P |
| 8d-8.34 | 監査におけるテスト中の情報システムの保護 | P | C, I, A | P | Sy, IP | G, P |