情報セキュリティ管理基準

（平成２８年改正版）

Ⅰ．主旨

(1) 情報セキュリティ管理基準の策定

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。当該基準は、情報セキュリティマネジメントにおける管理策のための国際標準規格であるISO/IEC 17799:2000（JIS X 5080:2002）を基にしており、組織体の業種及び規模等を問わず汎用的に適用できるように、情報資産を保護するための最適な実践慣行を帰納要約し、情報セキュリティに関するコントロールの目的、コントロールの項目を規定したものである。

(2) 情報セキュリティ管理基準（平成20年改正版）

その後、平成17年には、情報セキュリティマネジメントに関わる重要な国際規格として、ISO/IEC 27001:2005　ISMS要求事項（JIS Q 27001:2006[1]）及びISO/IEC 27002:2005（旧ISO/IEC 17799:2000）情報セキュリティマネジメントのための実践規範（JIS Q 27002:2006）が策定された。

このようなISO/IECにおける国際規格化の動きを受け、平成20年に「情報セキュリティ管理基準」をより効果的に活用できるように、国際規格と整合を取る形で見直しを行った。見直しにおいては、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て、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定することによって、組織体が効率的に情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行えるように規定した。

(3) 情報セキュリティ管理基準（平成28年改正版）

さらに、平成25年には、ISO/IEC 27001及び27002は、ISO/IEC 27001:2013（JIS Q 27001:2014）及び、ISO/IEC 27002:2013（JIS Q 27002:2014）に改訂され、マネジメントシステムの共通化、構成の変更、IT環境の変化等に伴う管理策の新規追加、削除、統合など、大幅な変更が加えられたところである。

「情報セキュリティ管理基準（平成28年改正版）」（以下「本管理基準」という。）は、このように大幅な変更が加えられたJIS Q 27001:2014及びJIS Q 27002:2014と整合を取り、旧版に引き続き、多くの利用者がISOに則った情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行えるよう、構成の変更も含め、情報セキュリティ管理基準（平成20年改正版）を大幅に改正し、実施すべき管理策の見直しも行ったものである。

Ⅱ．本管理基準の位置づけ

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

[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。

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。当然のことではあるが、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、本管理基準の項目等を取捨選択、追加又は統合することにより、該当する関係機関において独自の管理基準を策定し活用することが望ましい。

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」（平成15年経済産業省告示第114号）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。また、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。

Ⅲ．構成

本管理基準は、マネジメント基準と管理策基準から構成される。

「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 27001:2014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 27001:2014における構成順序を一部変更する。その際、JIS Q 27001:2014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 27001:2014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［27001-10.1］

4.8 文書化した情報の管理［27001-7.5］

4.8.1 文書化［27001-7.5.1］

4.8.2 文書管理［27001-7.5.2 / 7.5.3］

「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 27001:2014附属書A「管理目的及び管理策」、JIS Q 27002:2014をもとに専門家の知見を加えて作成しており、管理目的と管理策で構成される。また、既存のISMS認証などとの整合性にも配慮している。

「管理策基準」の内容は次のとおりである。

5 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

6 情報セキュリティのための組織

6.1 内部組織

6.2 モバイル機器及びテレワーキング

7 人的資源のセキュリティ

7.1 雇用前

7.2 雇用期間中

7.3 雇用の終了又は変更

8 資産の管理

8.1 資産に対する責任

8.2 情報分類

8.3 媒体の取扱い

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

9.2 利用者アクセスの管理

9.3 利用者の責任

9.4 システム及びアプリケーションのアクセス制御

10 暗号

10.1 暗号による管理策

11 物理及び環境的セキュリティ

11.1 セキュリティを保つべき領域

11.2 装置

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 27001:2014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 Q27001:2014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確立 [27001-4]**
>
> **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 27001:2014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、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[2]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以下により確認する。

---

[2] JIS Q 27001:2014では、ISO/IEC27001：2013で用いられるManagementについて、「トップマネジメント」、「経営陣」、「管理層」の3つの用語を用いている。「トップマネジメント」と「経営陣」は同じ意味と考えられるが、本文では「トップマネジメント」、附属書では「経営陣」と記載されている（本管理基準でもマネジメント基準では「トップマネジメント」を、管理策基準では「経営陣」を用いている。）。なお、「管理層」は、管理責任のある者の意味であり、「トップマネジメント（経営陣）」とその他の管理者の総称である。

・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。
・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。
・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。
・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。
・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。
・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。

4.4.1.2 トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。[27001-5.3]

・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。
・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。

また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。

・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限
・リスクアセスメントにおいて、リスクを運用管理する責任･権限を持つリスク所有者[3]
・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限
・セキュリティ要求事項を満たしているか監査する責任・権限
・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限
・各プロセスの結果及び効果を組織内に周知する責任・権限

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

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

4.4.2 組織及びその状況の理解 [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

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

a) 外部状況

[3] リスク所有者とは、リスクを運用管理することについて、責任及び権限を持つ人を指す（以下同じ。）。

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

b)　内部状況

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

4.4.3 利害関係者のニーズ及び期待の理解 [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
・利害関係者の情報セキュリティに関連する要求事項

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

・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。
　－情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等)
　－セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等)
　－情報セキュリティ監査を行う人又は組織(監査室等)
　－組織内の情報セキュリティ専門家
・取引先、パートナー、サプライチェーン上の関係者
・親会社、グループ会社
・当該組織のセキュリティを監督する省庁、政府機関
・所属するセキュリティ団体、協会

4.4.4 適用範囲の決定 [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、以下のようなものが含まれる。
－国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
－組織の目的に影響を与える主要な原動力及び傾向
－外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観

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

4.4.5 方針の確立 [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、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。

・実施事項
・必要な資源
・責任者
・達成期限
・結果の評価方法

4.4.5.3 トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1a)]

・情報セキュリティ方針及び情報セキュリティ目的を確立すること。
・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。

また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。

・文書化された情報セキュリティ方針への署名
・情報セキュリティ方針が議論された会議の議事録

これらはトップマネジメントの責任を明確にするために実施する。

4.4.6 リスク及び機会に対処する活動 [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) 情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。

・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。

・情報セキュリティリスクアセスメントの結果が比較可能であること。

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

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

a) 情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。

b) リスクを特定する過程において、リスク所有者を特定する。

c) リスクを特定する際には、以下について考慮する。

・リスク源[4]が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。

・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。

・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ

・全ての重大な原因及び結果

・以下を特定すること。

－リスク源

－影響を受ける領域、事象

－原因及び起こり得る結果

この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。

[4] 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持っているものを指す（以下同じ。）。

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[5]

・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[6]

・リスク源の除去[7]

・発生頻度の変更[8]

・結果の変更[9]

---

[5] 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など。

[6] 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、リスクを引受ける又は負担すること。例えば、市場拡大するために、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。

[7] 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。

[8] 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。

[9] 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。

・（契約及びリスクファイナンス[10]を含む。）他者とのリスクの共有[11]

・情報に基づいた意思決定によるリスクの保有[12]

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[13]。

4.4.8.3 組織は、管理策が見落とされていないことを検証する。[27001-6.1.3c)]

必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。

4.4.8.4 組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)]

a)情報セキュリティリスク対応計画には、以下を含む。

・期待される効果を含む、対応選択肢選定の理由

・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者

・対応内容

・必要な資源

・費用・労力、制約

・後日の報告、監視に必要な要求事項

・対応時期及び日程

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

---

[10] 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する対応がある。

[11] 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。

[12] 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。

[13] 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。

いることがほとんどであり、責任がトップマネジメントに集中している。

一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。

リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。

4.4.8.5 組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3f)]

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

・技術的に対応可能になる時期

・コスト的に対応可能になる時期

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

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

4.5 情報セキュリティマネジメントの運用 [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、以下のような資源を割り当てる。[27001-5.1c)]

・情報セキュリティマネジメントの各プロセスに必要な人又は組織

・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム

・上記に必要な費用

4.5.2 力量、認識 [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)］

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

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

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

実施結果については記録し、要員選択の客観性を確保する。

4.5.2.5 組織は、力量の証拠として、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を検討し、定期的に実施する。

・教育・訓練基本計画
・教育・訓練実施計画
・確認テスト又は評価報告

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

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

情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリ

ティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。

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

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

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

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

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

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

・トップマネジメント
・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者
・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者
・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、以下に示すような者と、必要に応じて、コミュニケーションを実施する。

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

4.5.4 情報セキュリティマネジメントの運用の計画及び管理 [27001-8.1]

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

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

4.5.4.3 組織は、計画通りに実施されたことを確信するために、文書化した情報を、保持する。 [2

7001-8.1]

文書化した情報に、以下の情報が集められているかどうかを確認する。

・管理策の実施状況

・管理策の有効性

・管理策を取り巻く環境の変化

また、これらの情報を把握し判断する体制を構築する。

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

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

4.5.5 情報セキュリティリスクアセスメントの実施 [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、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し、以下を決定する。 [27001-9.1]

・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。）
・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。）
・監視及び測定の実施時期
・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及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。

c) 適合性の監査においては、以下の項目を対象に含む。

・関連する法令又は規制の要求事項
・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項

d) 情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。

・管理策の有効性及び維持
・管理策が期待通りに実施されていること。

4.6.2.3 組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。 [27001-9.2c)]

監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。

監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。

・監査の目的と重点目標
・対象となる監査プロセスの状況と重要性

・対象となる領域の状況と重要性

・前回までの監査結果

4.6.2.4 組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)]

監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。

・監査の基準（以下の内容も含む。）

－目的、権限と責任

－独立性、客観性と職業倫理

－専門能力

－業務上の義務

－品質管理

－監査の実施方法

－監査報告書の形式

・監査の範囲

・監査の頻度又は時期

・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）

4.6.2.5 組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2e)]

監査人の選定においては監査基準に従い、以下の点を考慮する。

・外観上の独立性

・精神上の独立性

・職業倫理と誠実性

なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。

4.6.2.6 組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2f)]

4.6.2.7 組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2g)]

監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。

・監査の計画・実施に関する責任及び要求事項

・結果報告・記録維持に関する責任と要求事項

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]

・前回までのマネジメントレビューの結果とった処置の状況

・情報セキュリティマネジメントに関連する外部及び内部の課題の変化

・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック

－不適合及び是正処置

－監視及び測定の結果

－監査結果

－情報セキュリティ目的の達成

・利害関係者からのフィードバック

・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況

・継続的改善の機会

また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。

4.6.3.3 マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。 [27001-9.3]

マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。

・情報セキュリティマネジメントの有効性の改善

・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新

・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正

・必要となる経営資源の特定

・パフォーマンス測定方法の改善

なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。

4.6.3.4 組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。 [27001-9.3]

マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。

4.7 情報セキュリティマネジメントの維持及び改善 [27001-10]

4.7.1 是正処置 [27001-10.1]

4.7.1.1 組織は、不適合が発生した場合、不適合の是正のための処置を取る。 [27001-10.1a)]

a) 是正措置[14]を取る際は、以下を実施する。

・その不適合を管理し、是正するための処置

・その不適合によって起こった結果への対処

・是正処置を手順どおりに実施するために、以下について文書化する。

－不適合の再発防止を確実にするために選択した処置の必要性の評価

－必要な是正処置の決定

－必要な是正処置の実施

－実施した処置の記録

－実施した是正処置のレビュー

b) 不適合は以下の活動によって検出される。

・定期的な情報セキュリティリスクアセスメント

・定期的な情報セキュリティ内部監査

・定期的なマネジメントレビュー

・不適合を手順どおりに検出するために、以下について文書化する。

－情報セキュリティマネジメントに対する不適合の特定

－情報セキュリティマネジメントに対する不適合の原因の決定

なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。

4.7.1.2 組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。 [27001-10.1b)]

必要性を評価する際は、以下を実施する。

・その不適合のレビュー

・その不適合の原因の明確化

・類似の不適合の有無、又はそれが発生する可能性の明確化

4.7.1.3 組織は、必要な処置を実施する。 [27001-10.1c)]

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

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

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

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

・不適合の性質及びとった処置

・是正処置の結果

---

[14] 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[15]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

---

[15] 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

及び完全性の喪失からの保護）。

・文書化した情報の配付、アクセス[16]、検索及び利用

・文書化した情報の読みやすさが保たれることを含む、保管及び保存

・文書化した情報の変更の管理（例えば、版の管理）

・文書化した情報の保持及び廃棄

また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。

[16] 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[X.X.X]は、情報セキュリティリスクアセスメントの結果に基づき、適切に選択すべき事項である。詳細管理策[X.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 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

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

5.1.1 情報セキュリティのための方針群は、これを定義し、管理層[17]が承認し、発行し、従業員及び関連する外部関係者に通知する。

5.1.1.1 組織は、経営陣によって承認され、組織の情報セキュリティ目的の管理に対する取組みを示すものとして、方針群の最も高いレベルに、一つの情報セキュリティ方針を定める。

5.1.1.2 情報セキュリティ方針は、事業戦略によって生じる要求事項を取り扱う。

5.1.1.3 情報セキュリティ方針は、規制、法令及び契約によって生じる要求事項を取り扱う。

5.1.1.4 情報セキュリティ方針は、現在の及び予想される情報セキュリティの脅威環境によって生じる要求事項を取り扱う。

5.1.1.5 情報セキュリティ方針には、情報セキュリティに関する全ての活動の指針となる、情報セキュリティの定義、目的及び原則に関する記載を含める。

5.1.1.6 情報セキュリティ方針には、情報セキュリティマネジメントに関する一般的な責任及び特定の責任の、定められた役割への割当てに関する記載を含める。

5.1.1.7 情報セキュリティ方針には、逸脱及び例外を取り扱うプロセスに関する記載を含める。

5.1.1.8 方針群のより低いレベルでは、情報セキュリティ方針は、トピックに応じて定める個別方針[18]によって支持されるようにする。

5.1.1.9 個別方針のトピックとして、アクセス制御を含める。

5.1.1.10 個別方針のトピックとして、情報分類（及び取扱い）を含める。

5.1.1.11 個別方針のトピックとして、物理的及び環境的セキュリティを含める。

5.1.1.12 個別方針のトピックとして、エンドユーザ関連のトピック（資産利用の許容範囲、クリアデスク・クリアスクリーン、情報転送、モバイル機器及びテレワーキング、ソフトウェアのインストール及び使用の制限）を含める。

5.1.1.13 個別方針のトピックとして、バックアップを含める。

5.1.1.14 個別方針のトピックとして、情報の転送を含める。

5.1.1.15 個別方針のトピックとして、マルウェアからの保護を含める。

5.1.1.16 個別方針のトピックとして、技術的ぜい弱性の管理を含める。

5.1.1.17 個別方針のトピックとして、暗号による管理策を含める。

5.1.1.18 個別方針のトピックとして、通信のセキュリティを含める。

5.1.1.19 個別方針のトピックとして、プライバシー及び個人を特定できる情報（以下「PII」 とい

---

[17] 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。

[18] 個別方針は、情報セキュリティ管理策の実施を更に求めるもので、一般に組織内の対象となる特定のグループの要求に対処するように、又は特定のトピックを対象とするように構成される。

う。）の保護を含める。

5.1.1.20　個別方針のトピックとして、供給者関係を含める。

5.1.1.21　トピック別の個別方針は、従業員及び関係する外部関係者にとって適切で、アクセス可能かつ理解可能な形式で伝達する（例えば、情報セキュリティの意識向上、教育及び訓練のプログラムに従う。）。

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

5.1.2.1　各々の情報セキュリティのための方針には、その方針の作成、レビュー及び評価についての管理責任を与えられた責任者を置く。

5.1.2.2　情報セキュリティのための方針群のレビューには、組織環境、業務環境、法的状況又は技術環境の変化に応じた、組織の情報セキュリティのための方針群及び情報セキュリティの管理への取組みに関する、改善の機会の評価を含める。

5.1.2.3　情報セキュリティのための方針群のレビューでは、マネジメントレビューの結果を考慮し、反映する。

5.1.2.4　改訂された情報セキュリティのための方針は、管理層から承認を得る。

6　情報セキュリティのための組織

6.1　内部組織

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

6.1.1　全ての情報セキュリティの責任を定め、割り当てる。

6.1.1.1　情報セキュリティの責任の割当ては、情報セキュリティのための方針群によって行う。

6.1.1.2　個々の資産の保護に対する責任及び特定の情報セキュリティプロセスの実施に対する責任を定める。

6.1.1.3　情報セキュリティのリスクマネジメント活動に関する責任、特に残留リスクの受容に関する責任を定める。

6.1.1.4　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。

6.1.1.5　資産の保護及び特定の情報セキュリティプロセスの実行に関する局所的(local)な責任を定める。

6.1.1.6　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が、責任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。

6.1.1.7　個人が責任をもつ領域を規定する。

6.1.1.8　個人が責任をもつ領域を規定するために、資産及び情報セキュリティプロセスの識別及び規定を実施する。

6.1.1.9　個人が責任をもつ領域を規定するために、各資産又は情報セキュリティプロセスに対する責任主体の指定、及びその責任の詳細の文書化を実施する。

6.1.1.10　個人が責任をもつ領域を規定するために、承認レベルの規定及び文書化を実施する。

6.1.1.11　個人が責任をもつ領域を規定するために、情報セキュリティ分野における責任を果たせるよう、任命された個人が当該分野の力量をもつこと、及び最新の状況を把握するための機

会が与えられるようにする。

6.1.1.12　個人が責任をもつ領域を規定するために、供給者関係における情報セキュリティの側面の調整及び管理に関する事項の特定及び文書化を実施する。

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

6.1.2.1　認可されていない状態又は検知されない状態で、一人で資産に対してアクセス、修正又は使用ができないように注意する。

6.1.2.2　ある作業を始めることと、その作業を認可することとを分離する。

6.1.2.3　管理策は、共謀のおそれを考慮して設計する。

6.1.2.4　職務の分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理層による監督）を実施する。

6.1.3　関係当局との適切な連絡体制を維持する。

6.1.3.1　組織は、いつ、誰が関係当局（例えば、法の執行機関、規制当局、監督官庁）に連絡するかの手順を備える。

6.1.3.2　法が破られたと疑われる場合に、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の手順を備える。

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

6.1.4.1　最適な慣行に関する認識を改善し、関係するセキュリティ情報を最新に保つ手段として、情報セキュリティに関する研究会又は会議へ参加する。

6.1.4.2　情報セキュリティ環境の理解が最新かつ完全であることを確実にする手段として、情報セキュリティに関する研究会又は会議へ参加する。

6.1.4.3　攻撃及びぜい弱性に関連する早期警戒警報、勧告及びパッチを受理する手段として、情報セキュリティに関する研究会又は会議へ参加する。

6.1.4.4　専門家から情報セキュリティの助言を得る手段として、情報セキュリティに関する研究会又は会議へ参加する。

6.1.4.5　新しい技術、製品、脅威又はぜい弱性に関する情報を共用し、交換する手段として、情報セキュリティに関する研究会又は会議へ参加する。

6.1.4.6　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参加する。

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

6.1.5.1　情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするために、情報セキュリティを組織のプロジェクトマネジメント手法に組み入れ、プロジェクトの特性にかかわらず、一般にあらゆるプロジェクト（例えば、中核事業プロセス、IT、施設管理、その他のサポートプロセスのためのプロジェクト）に適用されるようにする。

6.1.5.2　プロジェクトマネジメント手法においては、情報セキュリティ目的をプロジェクトの目的に含める。

6.1.5.3　プロジェクトマネジメント手法においては、必要な管理策を特定するため、プロジェクトの早い段階で情報セキュリティリスクアセスメントを実施する。

6.1.5.4　プロジェクトマネジメント手法においては、適用するプロジェクトマネジメントの方法論の全ての局面において、情報セキュリティを含める。

6.1.5.5　全てのプロジェクトにおいて、情報セキュリティの組織への影響を明確にし、これを定期的にレビューする。

6.1.5.6　プロジェクトマネジメント手法で定められた役割を明確にするため、情報セキュリティに関する責任を定め、割り当てる。

6.2　モバイル機器及びテレワーキング

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

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

6.2.1.1　モバイル機器を用いる場合、業務情報が危険にさらされないことを確実にするために、特別な注意を払う。

6.2.1.2　モバイル機器の情報セキュリティ方針は、保護されていない環境におけるモバイル機器を用いた作業のリスクを考慮して定める。

6.2.1.3　モバイル機器の情報セキュリティ方針には、モバイル機器の登録を含める。

6.2.1.4　モバイル機器の情報セキュリティ方針には、物理的保護についての要求事項を含める。

6.2.1.5　モバイル機器の情報セキュリティ方針には、ソフトウェアのインストールの制限を含める。

6.2.1.6　モバイル機器の情報セキュリティ方針には、モバイル機器のソフトウェアのバージョン及びパッチ適用に対する要求事項を含める。

6.2.1.7　モバイル機器の情報セキュリティ方針には、情報サービスへの接続の制限を含める。

6.2.1.8　モバイル機器の情報セキュリティ方針には、アクセス制御を含める。

6.2.1.9　モバイル機器の情報セキュリティ方針には、暗号技術を含める。

6.2.1.10　モバイル機器の情報セキュリティ方針には、マルウェアからの保護を含める。

6.2.1.11　モバイル機器の情報セキュリティ方針には、遠隔操作による機器の無効化、データの消去又はロックを含める。

6.2.1.12　モバイル機器の情報セキュリティ方針には、バックアップを含める。

6.2.1.13　モバイル機器の情報セキュリティ方針には、ウェブサービス及びウェブアプリケーションの使用を含める。

6.2.1.14　公共の場所、会議室、その他保護されていない場所でモバイル機器を用いるときは、注意を払う。

6.2.1.15　モバイル機器に保管され、処理される情報について、認可されていないアクセス又は漏えいを防止するため、例えば、暗号技術の使用、秘密認証情報の使用の強制などの保護を実施する。

6.2.1.16　モバイル機器は、盗難、特にどこか（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所）に置き忘れたときの盗難から、物理的に保護する。

6.2.1.17　モバイル機器の盗難又は紛失の場合の対策のために、法規制、保険及び組織の他のセキュリティ要求事項を考慮した特定の手順を確立する。

6.2.1.18　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モバイル機器は、無人の状態で放置しない。

6.2.1.19　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モバイル機

器は、可能な場合には、物理的に施錠するか、又はモバイル機器のセキュリティを確保するために特別な錠を用いる。

6.2.1.20　作業形態に起因する追加のリスク及び実施すべき管理策についての意識向上のために、モバイル機器を用いる要員に対する教育・訓練を計画・準備・実施する。

6.2.1.21　モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、機器の私的な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。）。

6.2.1.22　モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、エンドユーザ合意書に利用者が署名した場合にだけ、業務情報にアクセスできるようにする（エンドユーザ合意書には、利用者の義務（物理的な保護、ソフトウェアの更新など）についての確認、業務データに対する所有権を主張しないこと、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。この方針では、プライバシーに関する法令を考慮する。）。

6.2.2　テレワーキング[19]の場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。

6.2.2.1　テレワーキング活動を許可する組織は、テレワーキングを行う場合の条件及び制限を定めた方針を発行する。

6.2.2.2　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、建物及び周辺環境の物理的セキュリティを考慮に入れた、テレワーキングの場所の既存の物理的セキュリティの状況を考慮して定める。

6.2.2.3　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、提案された物理的なテレワーキングの環境を考慮して定める。

6.2.2.4　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、組織の内部システムへの遠隔アクセスの必要性、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慎重度及び内部システムの取扱いに関する慎重度を考慮した、通信のセキュリティに関する要求事項を考慮して定める。

6.2.2.5　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置で情報を処理及び保管できないようにする仮想デスクトップへのアクセスを考慮して定める。

6.2.2.6　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、住環境を共有する者（例えば、家族、友人）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を考慮して定める。

6.2.2.7　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、家庭のネットワークの使用及び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を考慮して定める。

---

[19] テレワーキングとは、オフィス以外で行うあらゆる作業形態をいう。これには、“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）”、“遠隔作業”及び“仮想的な作業”の環境のような、従来とは異なる作業環境を含む。

6.2.2.8　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置の上で開発した知的財産の権利に関する論争を防ぐための方針及び手順を考慮して定める。

6.2.2.9　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置へのアクセス（装置のセキュリティ検証のためのもの、又は調査期間中に行うもの）を考慮して定める。なお、このアクセスは、法令が禁じている場合がある。

6.2.2.10　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、従業員又は外部の利用者が個人的に所有するワークステーション上のクライアントソフトウェアの使用許諾について、組織が責任をもつことになる場合の、ソフトウェアの使用許諾契約を考慮して定める。

6.2.2.11　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、マルウェアに対する保護及びファイアウォールの要件を考慮して定める。

6.2.2.12　テレワーキングを行う場合に考慮すべき指針及び取決めには、組織の管理下にない個人所有の装置の使用を許さない場合には、テレワーキング活動のための適切な装置及び保管用具の用意に関する事項を含める。

6.2.2.13　テレワーキングを行う場合に考慮すべき指針及び取決めには、許可した作業、作業時間、保持してもよい情報の分類、並びにテレワーキング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に関する事項を含める。

6.2.2.14　テレワーキングを行う場合に考慮すべき指針及び取決めには、安全な遠隔アクセス方法を含め、適切な通信装置の用意に関する事項を含める。

6.2.2.15　テレワーキングを行う場合に考慮すべき指針及び取決めには、 物理的セキュリティに関する事項を含める。

6.2.2.16　テレワーキングを行う場合に考慮すべき指針及び取決めには、家族及び訪問者による装置及び情報へのアクセスに関する規則及び手引を含める。

6.2.2.17　テレワーキングを行う場合に考慮すべき指針及び取決めには、ハードウェア及びソフトウェアのサポート及び保守の用意を含める。

6.2.2.18　テレワーキングを行う場合に考慮すべき指針及び取決めには、保険の用意を含める。

6.2.2.19　テレワーキングを行う場合に考慮すべき指針及び取決めには、バックアップ及び事業継続のための手順を含める。

6.2.2.20　テレワーキングを行う場合に考慮すべき指針及び取決めには、監査及びセキュリティの監視に関する事項を含める。

6.2.2.21　テレワーキングを行う場合に考慮すべき指針及び取決めには、テレワーキングが終了したときの、権限及びアクセス権の失効並びに装置の返却に関する事項を含める。

7　人的資源のセキュリティ

7.1　雇用前

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

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

7.1.1.1　関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、満足のいく推薦状（例えば、業務についてのもの、人物についてのもの）の入手の可否の確認を行う。

7.1.1.2　関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、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）を行う。

7.1.1.3　関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、提示された学術上及び職業上の資格の確認を行う。

7.1.1.4　関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、公的証明書（パスポート又は同種の文書）の確認を行う。

7.1.1.5　関連があるプライバシー、PIIの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認を行う。

7.1.1.6　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、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ことを確認する。

7.1.1.7　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、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ことを確認する。

7.1.1.8　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（例えば、財務情報、極秘情報）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。

7.1.1.9　手順には、確認のためのレビューの基準及び制約を定める（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。）。

7.1.1.10　選考プロセスは、契約相手に対しても確実に実施する。

7.1.1.11　契約相手に対して選考プロセスを実施する場合、組織と契約相手との間の合意では、選考の実施に関する責任、及びその選考が完了していないとき又はその結果に疑念若しくは懸念があるときに従う必要がある告知手順を定める。

7.1.1.12　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に従って収集し、扱う。

7.1.1.13　適用される法令によっては、選考活動について候補者へ、事前に通知する。

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

7.1.2.1　従業員又は契約相手の契約上の義務には、組織の情報セキュリティのための方針群を反映する。

7.1.2.2　従業員又は契約相手の契約には、秘密情報へのアクセスが与えられる全ての従業員及び契約相手による、情報処理施設へのアクセスが与えられる前の、秘密保持契約書又は守秘義務契約書への署名を行う。

7.1.2.3　従業員又は契約相手の契約には、従業員又は契約相手の法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法律に関するもの）を明確にする。

7.1.2.4　従業員又は契約相手の契約には、従業員又は契約相手によって扱われる情報の分類に関する責任、並びに従業員又は契約相手によって扱われる組織の情報、情報に関連するその他

の資産、情報処理施設及び情報サービスの管理に関する責任を明確にする。

7.1.2.5　従業員又は契約相手の契約には、他社又は外部関係者から受け取った情報の扱いに関する従業員又は契約相手の責任を明確にする。

7.1.2.6　従業員又は契約相手の契約には、従業員又は契約相手が組織のセキュリティ要求事項に従わない場合にとる処置を含める。

7.1.2.7　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える。

7.1.2.8　組織は、従業員及び契約相手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仕組みを整備する。

7.1.2.9　雇用条件は、情報システム及びサービスと関連する組織の資産に対する、従業員及び契約相手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。

7.1.2.10　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。

7.2　雇用期間中

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

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

7.2.1.1　経営陣の責任には、従業員及び契約相手に、秘密情報又は情報システムへのアクセスが許可される前に、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仕組みを整備することを含める。

7.2.1.2　経営陣の責任には、従業員及び契約相手に、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備することを含める。

7.2.1.3　経営陣の責任には、従業員及び契約相手に、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備することを含める。

7.2.1.4　経営陣の責任には、従業員及び契約相手に、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、一定の水準を達成する仕組みを整備することを含める。

7.2.1.5　経営陣の責任には、従業員及び契約相手に、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、雇用条件に従うようにする仕組みを整備することを含める。

7.2.1.6　経営陣の責任には、従業員及び契約相手に、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備することを含める。

7.2.1.7　経営陣の責任には、従業員及び契約相手に、情報セキュリティのための方針群又は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（例えば、内部告発）仕組みを整備することを含める。

7.2.1.8　経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動する。

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

7.2.2.1　情報セキュリティの意識向上プログラムは、従業員、及び関係する場合は契約相手に対し、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。

7.2.2.2 情報セキュリティの意識向上プログラムは、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管理策を考慮に入れて、組織の情報セキュリティのための方針群及び関連する手順に沿って確立する。

7.2.2.3 情報セキュリティの意識向上プログラムには、キャンペーン（例えば、情報セキュリティの日）、及びパンフレット又は会報の発行のような、複数の意識向上活動を含める。

7.2.2.4 情報セキュリティの意識向上プログラムは、組織における従業員の役割、及び関係する場合には契約相手の認識に対する組織の期待を考慮に入れて、計画する。

7.2.2.5 情報セキュリティの意識向上プログラムの活動は、新しい従業員及び契約相手も対象とされるよう、長期にわたり、できれば定期的に計画する。

7.2.2.6 情報セキュリティの意識向上プログラムは、定期的に更新して組織の方針及び手順に沿って、情報セキュリティインシデントから学んだ教訓が生かされるようにする。

7.2.2.7 意識向上のための訓練は、（例えば、教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他を含む、多様な手段を用いて、）組織の情報セキュリティの意識向上プログラムで必要とされた場合に実施する。

7.2.2.8 情報セキュリティの教育及び訓練には、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の提示を含める。

7.2.2.9 情報セキュリティの教育及び訓練には、方針、規格、法令、規制、契約及び合意で定められた、適用される情報セキュリティの規則及び義務を熟知し、これを順守する必要性を含める。

7.2.2.10 情報セキュリティの教育及び訓練には、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責任、並びに組織及び外部関係者に属する情報のセキュリティを保つか、これを保護することに対する一般的な責任を含める。

7.2.2.11 情報セキュリティの教育及び訓練には、情報セキュリティに関する基本的な手順（例えば、情報セキュリティインシデントの報告）及び基本的な管理策（例えば、パスワードのセキュリティ、マルウェアの制御、クリアデスク）を含める。

7.2.2.12 情報セキュリティの教育及び訓練には、情報セキュリティに関連する事項についての追加的な情報及び助言（情報セキュリティの教育及び訓練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を含める。

7.2.2.13 情報セキュリティの教育及び訓練は、定期的に実施する。

7.2.2.14 最初の教育及び訓練は、新入社員だけでなく、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し、その役割が始まる前に実施する。

7.2.2.15 組織は、教育及び訓練を効果的に実施するためのプログラムを開発する。

7.2.2.16 教育及び訓練を効果的に実施するためのプログラムは、保護する必要のある組織の情報及び情報を保護するために実施されている管理策を考慮に入れるプロセスを含める。

7.2.2.17 教育及び訓練を効果的に実施するためのプログラムは、組織の情報セキュリティのための方針群及び関連手順に沿っている。

7.2.2.18 教育及び訓練を効果的に実施するためのプログラムでは、講義又は自己学習のように、多様な教育及び訓練の形式を考慮して、定める。

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

続を備える。

7.2.3.1　懲戒手続は、情報セキュリティ違反が生じたことの事前の確認を待って開始する。

7.2.3.2　正式な懲戒手続には、情報セキュリティ違反を犯したという疑いがかけられた従業員に対する正確かつ公平な取扱いを含める。

7.2.3.3　正式な懲戒手続は、違反の内容及び重大さ並びにその業務上の影響、最初の違反か又は繰り返されたものか、違反者は、適切に教育・訓練されていたかどうか、関連する法令、取引契約、その他の必要な要素を考慮した段階別の対応を定める。

7.2.3.4　懲戒手続を、従業員が情報セキュリティ違反（従業員による組織の情報セキュリティのための方針群及び手順への違反並びに他の全ての情報セキュリティ違反）を起こすことを防ぐための抑止力として使う[20]。

7.3　雇用の終了及び変更

目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。

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

7.3.1.1　雇用の終了に関する責任の伝達には、実施中の情報セキュリティ要求事項及び法的責任、並びに適切であれば、従業員又は契約相手の、雇用の終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任を含める。

7.3.1.2　雇用の終了後も引き続き有効な責任及び義務は、従業員又は契約相手の雇用条件に含める。

7.3.1.3　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み合わせとして管理する。

8　資産の管理

8.1　資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため。

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

8.1.1.1　組織は、情報のライフサイクルに関連した資産を特定し、その重要度を文書化する。

8.1.1.2　情報のライフサイクルには、作成、処理、保管、送信、削除及び破棄を含める。

8.1.1.3　文書は、専用の目録又は既存の目録として維持する。

8.1.1.4　資産目録は、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ことを確実にする仕組みを整備する。

8.1.1.5　特定された各資産について、管理責任者を割り当て、分類する。

8.1.2　目録の中で維持される資産は、管理する。

8.1.2.1　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において、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。

8.1.2.2　資産の管理責任者は、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。

8.1.2.3　資産の管理責任者は、資産の目録を作成する仕組みを整備する。

---

[20] 意図的な違反には、緊急の処置が求められる場合がある。

8.1.2.4　資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。

8.1.2.5　資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。

8.1.2.6　資産の管理責任者は、 資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。

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

8.1.3.1　組織の資産を利用する又はアクセスできる従業員及び外部の利用者に対し、組織における情報や情報処理施設に関連する資産あるいは資源に関する情報セキュリティ要求事項について、認識させる。

8.1.3.2　従業員及び外部の利用者は、どのような情報処理資源の利用に対しても、また、利用者自身の責任の下で行ったいかなる利用に対しても、責任をもつ。

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

8.1.4.1　雇用の終了時の手続は、前もって支給された物理的及び電子的な資産（組織が管理責任をもつ又は組織に委託されたもの）の全ての返却を含める。

8.1.4.2　従業員及び外部の利用者が組織の設備を購入する場合、又は個人所有の設備を用いる場合には、手順に従って、全ての関連する情報を組織に返却し、設備からセキュリティを保って確実に消去する。

8.1.4.3　従業員及び外部の利用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。

8.1.4.4　雇用の終了の予告期間中は、雇用が終了する従業員及び契約相手が認可を得ずに関連情報（例えば、知的財産）を複製することのないよう、組織が管理する。

8.2　情報分類

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

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

8.2.1.1　情報の分類及び関連する保護管理策には、情報を共有又は制限する業務上の要求、及び法的要求事項を含める。

8.2.1.2　情報資産の管理責任者は、その情報の分類に対して責任を負う。

8.2.1.3　分類体系には、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。

8.2.1.4　分類体系における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価する。

8.2.1.5　分類体系は、アクセス制御方針と整合させる。

8.2.1.6　それぞれのレベルには、分類体系の適用において意味をなすような名称を付ける。

8.2.1.7　分類体系は、組織全体にわたって一貫させ、全員が情報及び関連する資産を同じ方法で分類[21]し、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する。

---

[21] 情報以外の資産も、その資産に保管される情報、処理される情報、又は他の形で取り扱われる若しくは保護される情報の分類に従って分類できる。

8.2.1.8　分類は、組織のプロセスに含め、組織全体にわたって一貫した論理的なものとする。

8.2.1.9　分類の結果は、組織にとっての取扱いに慎重を要する度合い及び重要性（例えば、機密性、完全性、可用性）に応じた資産の価値を含める。

8.2.1.10　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性の変化に応じて、更新する。

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

8.2.2.1　情報のラベル付けに関する手順は、物理的形式及び電子的形式の情報及び関連する資産に適用できるようにする。

8.2.2.2　ラベル付けは、8.2.1 で確立した分類体系を反映する。

8.2.2.3　ラベルは、容易に認識できるようにする。

8.2.2.4　情報のラベル付けに関する手順では、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[22]を示す。

8.2.2.5　従業員及び契約相手に、ラベル付けに関する手順を認識させる。

8.2.2.6　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。

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

8.2.3.1　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順を作成する。

8.2.3.2　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、各レベルの分類に応じた保護の要求事項に対応するアクセス制限に関する手順を含める。

8.2.3.3　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、資産の認可された受領者について、正式な記録を維持するための手順を含める。

8.2.3.4　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、情報の一時的又は恒久的な複製は、情報の原本と同等のレベルで保護するための手順を含める。

8.2.3.5　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、IT 資産は、製造業者の仕様に従って保管するための手順を含める。

8.2.3.6　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、媒体の全ての複製には、認可された受領者の注意をひくように明確な印を付けるための手順を含める。

8.2.3.7　他組織との情報共有を含む合意には、その情報の分類を特定し、他組織からの分類ラベルを解釈するための手順を含める[23]。

8.3　媒体の取扱い

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

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

8.3.1.1　取外し可能な媒体の管理のために、再利用可能な媒体を組織から移動する場合に、その内容が以後不要であるならば、これを復元不能とする。

8.3.1.2　取外し可能な媒体の管理のために、必要かつ実際的な場合には、組織から移動する媒体に

---

[22] 作業負荷を減らすために、ラベル付けを省略する場合（例えば、秘密でない情報のラベル付け）を定めることもできる。

[23] 組織で用いる分類体系は、レベルの名称が似ていても、他の組織が用いる分類体系と同等とは限らない。また，複数の組織間を移動する情報は、分類体系が同一であっても、各組織の状況に応じて分類が異なる場合がある。

ついて、認可を要求する。

8.3.1.3　取外し可能な媒体の管理のために、組織から移動する媒体について、監査証跡の維持のために記録を保管する。

8.3.1.4　取外し可能な媒体の管理のために、全ての媒体は、製造業者の仕様に従って、安全でセキュリティが保たれた環境に保管する。

8.3.1.5　取外し可能な媒体の管理のために、データの機密性又は完全性が重要な考慮事項である場合は、取外し可能な媒体上のデータを保護するために、暗号技術を用いる。

8.3.1.6　取外し可能な媒体の管理のために、保管されたデータがまだ必要な間に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データを新しい媒体に移動する。

8.3.1.7　取外し可能な媒体の管理のために、価値の高いデータは、一斉に損傷又は消失するリスクをより低減するために、複数の複製を別の媒体に保管する。

8.3.1.8　取外し可能な媒体の管理のために、データ消失の危険性を小さくするために、取外し可能な媒体の登録を含める。

8.3.1.9　取外し可能な媒体の管理のために、取外し可能な媒体のドライブは、その利用のための業務上の理由があるときにだけ有効とする。

8.3.1.10　取外し可能な媒体の管理のために、取外し可能な媒体を用いる必要がある場合、媒体への情報の転送を監視する。

8.3.1.11　取外し可能な媒体の管理のための手順及び認可のレベルは、文書化する。

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

8.3.2.1　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、媒体のセキュリティを保った処分のための正式な手順を確立する。

8.3.2.2　秘密情報を格納した媒体の、セキュリティを保った処分の手順は、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。

8.3.2.3　秘密情報を格納した媒体は、セキュリティを保って、保管し、処分する（例えば、焼却、シュレッダーの利用、組織内の他のアプリケーションでの媒体の再利用のためのデータ消去）。

8.3.2.4　セキュリティを保った処分を必要とする品目を特定するための手順を定める。

8.3.2.5　取扱いに慎重を要する媒体類を選び出すことが困難な場合には、セキュリティを保って全ての媒体を処分する。

8.3.2.6　媒体の収集並びに処分のサービスを提供する外部業者は、十分な管理策及び経験を持つ適切な契約相手を選択する。

8.3.2.7　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する。

8.3.2.8　処分のために情報を含む媒体を集める場合、それらの情報が集積されることによる影響に配慮し、手順に含める。

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

8.3.3.1　輸送される情報を格納した媒体を保護するために、信頼できる輸送機関又は運送業者を用いる。

8.3.3.2　輸送される情報を格納した媒体を保護するために、認可された運送業者の一覧について、管理者の合意を得る。

8.3.3.3　輸送される情報を格納した媒体を保護するために、運送業者を確認する手順を導入する。

8.3.3.4　輸送される情報を格納した媒体を保護するために、輸送途中に生じるかもしれない物理的損傷から内容を保護（例えば、媒体の復旧効果を低減させる場合のある、熱、湿気又は電磁気にさらすといった環境要因からの保護）するために、こん（梱）包を十分な強度とし、また、製造業者の仕様にも従う。

8.3.3.5　輸送される情報を格納した媒体を保護するために、媒体の内容、適用された保護、並びに輸送の責任窓口への受渡時刻及び目的地での受取り時刻の記録を特定するログを保持する。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため。

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

9.1.1.1　資産の管理責任者は、資産に対する利用者のそれぞれの役割に対して、適切なアクセス制御規則、アクセス権及び制限を、アクセスに伴う情報セキュリティリスクを反映した制御の詳細さ及び厳密さで、決定する。

9.1.1.2　アクセス制御は、論理的アクセス制御と物理的アクセス制御の両面を考慮して決定する。

9.1.1.3　利用者及びサービス提供者には、アクセス制御によって達成する業務上の要求事項を明確に規定して提供する。

9.1.1.4　アクセス制御方針に、業務用アプリケーションのセキュリティ要求事項を反映する。

9.1.1.5　アクセス制御方針には、情報の伝達及び認可に対する方針（例えば、知る必要性の原則、情報のセキュリティ水準、情報の分類）を含める。

9.1.1.6　アクセス制御方針は、システム及びネットワークにおける、アクセス権と情報分類の方針との整合性を考慮して定める。

9.1.1.7　アクセス制御方針には、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及び契約上の義務を反映する。

9.1.1.8　アクセス制御方針に、利用可能な全ての種類の接続を認識する分散ネットワーク環境におけるアクセス権の管理を含める。

9.1.1.9　アクセス制御方針に、アクセス制御における役割の分離（例えば、アクセス要求、アクセス認可、アクセス管理）の方針を含める。

9.1.1.10　アクセス制御方針に、アクセス要求の正式な認可に対する要求事項を含める。

9.1.1.11　アクセス制御方針に、アクセス権の定期的なレビューに対する要求事項を含める。

9.1.1.12　アクセス制御方針に、アクセス権の削除の方針を含める。

9.1.1.13　アクセス制御方針に、利用者の識別情報及び秘密認証情報の利用及び管理に関する、全ての重要な事象の記録の保管を含める。

9.1.1.14　アクセス制御方針に、特権的アクセスを認められた役割を含める。

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

9.1.2.1　ネットワーク及びネットワークサービスの利用に関し、方針を設定する。

9.1.2.2　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方針は、アクセスが許されるネットワーク及びネットワークサービスを対象にする。

9.1.2.3　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方針は、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にする。

9.1.2.4　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方針は、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運用管理面からの管理策及び管理手順を対象にする。

9.1.2.5　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方針は、ネットワーク及びネットワークサービスへのアクセスに利用される手段（例えば、VPN、無線ネットワーク）を対象にする。

9.1.2.6　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方針は、様々なネットワークサービスへのアクセスに対する利用者認証の要求事項を対象にする。

9.1.2.7　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方針は、ネットワークサービスの利用の監視を対象にする。

9.1.2.8　ネットワークサービスの利用に関する方針は、組織のアクセス制御方針と整合させる。

9.2　利用者アクセスの管理

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

9.2.1　アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。

9.2.1.1　利用者ID を管理するプロセスに、利用者と利用者自身の行動とを対応付けすること、及び利用者がその行動に責任をもつことを可能にする、一意な利用者ID の利用を含める。

9.2.1.2　利用者ID を管理するプロセスに、共有ID の利用は、業務上又は運用上の理由で必要な場合にだけ許可し、承認し、記録することを含める。

9.2.1.3　利用者ID を管理するプロセスに、組織を離れた利用者の利用者IDの、即座の無効化又は削除を含める。

9.2.1.4　利用者ID を管理するプロセスに、必要のない利用者ID の定期的な特定、及び削除又は無効化することを含める。

9.2.1.5　利用者ID を管理するプロセスに、別の利用者に重複する利用者ID を発行しないことを確実にするよう定める。

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

9.2.2.1　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスの利用についての、その情報システム又はサービスの管理責任者からの認可を得ていることの点検を含める（アクセス権について、管理層から別の承認を受けることが適切な場合もある。）。

9.2.2.2　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、許可したアクセスのレベルが、アクセス制御方針に適していることの点検を含める。

9.2.2.3　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、 許可したアクセスのレベルが、職務の分離などのその他の要求事項と整合していることの検証を含める。

9.2.2.4　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、認可手順が完了するまで、（例えば、サービス提供者が）アクセス権を有効にしないことが確実になるよう定める。

9.2.2.5　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスにアクセスするために利用者ID に与えられたアクセス権の、一元的な記録の維持を含める。

9.2.2.6　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、役割又は職務を変更した利用者のアクセス権の変更、及び組織を離れた利用者のアクセス権の即座の解除又は停止することを含める。

9.2.2.7　利用者ID に対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスの管理責任者による、アクセス権の定期的なレビューを含める。

9.2.3　特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.1　特権的アクセス権の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理する。

9.2.3.2　特権の割当ての正式な認可プロセスでは、各々のシステム又はプロセス（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、各アプリケーション）に関連した特権的アクセス権、及び特権的アクセス権を割り当てる必要がある利用者を特定する。

9.2.3.3　特権の割当ての正式な認可プロセスでは、特権的アクセス権を、アクセス制御方針に沿って、使用の必要性に応じて、かつ、事象に応じて、利用者に割り当てる。すなわち、利用者の職務上の役割のための最小限の要求事項に基づいて割り当てる。

9.2.3.4　特権の割当ての正式な認可プロセスでは、割り当てた全ての特権の認可プロセス及び記録を維持する。

9.2.3.5　特権の割当ての正式な認可プロセスでは、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。

9.2.3.6　特権の割当ての正式な認可プロセスでは、特権的アクセス権の終了に関する要求事項を定める。

9.2.3.7　特権の割当ての正式な認可プロセスでは、特権的アクセス権は、通常業務に用いている利用者ID とは別の利用者ID に割り当てる。特権を与えられたID からは、通常業務を行わない。

9.2.3.8　特権の割当ての正式な認可プロセスでは、特権的アクセス権を与えられた利用者の力量がその職務に見合っていることを検証するために、その力量を定期的にレビューする。

9.2.3.9　特権の割当ての正式な認可プロセスでは、汎用の実務管理者ID の認可されていない使用を避けるため、システムの構成管理機能に応じて、具体的な手順を確立及び維持する。

9.2.3.10　特権の割当ての正式な認可プロセスでは、汎用の実務管理者ID に関しては、共有する場合に秘密認証情報の機密性を維持する（例えば、頻繁にパスワードを変更する、特権を与えられた利用者が離職する又は職務を変更する場合はできるだけ早くパスワードを変更する、特権を与えられた利用者の間で適切な方法でパスワードを伝達する。）。

9.2.4　秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.1　秘密認証情報の割当ての正式な管理プロセスでは、個人の秘密認証情報を秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合もある。

9.2.4.2　秘密認証情報の割当ての正式な管理プロセスでは、グループの（すなわち、共用の）秘密認証情報はグループのメンバ内だけの秘密に保つ旨の文書への署名を、利用者に要求する。

この署名文書は、雇用契約の条件に含める場合もある。

9.2.4.3 秘密認証情報の割当ての正式な管理プロセスでは、利用者に各自の秘密認証情報を保持することを求める場合、最初に、セキュリティが保たれた仮の秘密認証情報を発行し、最初の使用時にこれを変更させる。

9.2.4.4 秘密認証情報の割当ての正式な管理プロセスでは、新規、更新又は仮の秘密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。

9.2.4.5 秘密認証情報の割当ての正式な管理プロセスでは、仮の秘密認証情報は、セキュリティを保った方法で利用者に渡す。外部関係者を通して渡すこと又は保護されていない（暗号化していない）電子メールのメッセージを利用することは避ける。

9.2.4.6 秘密認証情報の割当ての正式な管理プロセスでは、仮の秘密認証情報は、一人一人に対して一意とし、推測されないものとする。

9.2.4.7 秘密認証情報の割当ての正式な管理プロセスでは、利用者は、秘密認証情報の受領を知らせる。

9.2.4.8 秘密認証情報の割当ての正式な管理プロセスでは、業者があらかじめ設定した秘密認証情報は、システム又はソフトウェアのインストール後に変更する。

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

9.2.5.1 利用者のアクセス権は、定められた間隔で見直す。

9.2.5.2 利用者のアクセス権は、何らかの変更（例えば、昇進、降格、雇用の終了）があった後に見直す。

9.2.5.3 利用者のアクセス権は、利用者の役割が同一組織内で変更された場合、そのアクセス権についてレビューし、割当てをし直す。

9.2.5.4 特権的アクセス権の認可は、利用者のアクセス権より頻繁な間隔でレビューする。

9.2.5.5 特権の割当てを定められた間隔で点検して、認可されていない特権が取得されていないことを確認する。

9.2.5.6 特権アカウントを変更する際は、定期的なレビューのために変更ログをとる。

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

9.2.6.1 雇用の終了時に、アクセス権を削除する必要があるかどうかを決定し、情報並びに情報処理施設及びサービスに関連する資産に対する個人のアクセス権を削除又は一時停止を行う。

9.2.6.2 雇用を変更した場合、新規の業務において承認されていない全てのアクセス権を削除する。

9.2.6.3 削除又は修正が望ましいアクセス権には、物理的な及び論理的なアクセスに関するものを含める。

9.2.6.4 従業員及び契約相手のアクセス権を特定するあらゆる文書に、アクセス権の削除又は修正[24]を反映する。

9.2.6.5 辞めていく従業員又は外部の利用者が引き続き有効な利用者ID のパスワードを知っている場合、雇用・契約・合意の終了又は変更に当たって、これらのパスワードを変更する。

9.2.6.6 情報及び情報処理施設に関連する資産へのアクセス権は、雇用の終了又は変更の前に、雇用の終了又は変更が、従業員若しくは外部の利用者の側によるものか又は経営側によるも

[24] アクセス権の削除又は修正は、鍵、身分証明書、情報処理機器又は利用登録の、削除、失効又は差替えによって行うことができる。

のかどうか、及び雇用の終了の理由、従業員、外部の利用者、又は他の利用者の現時点の責任、現在アクセス可能な資産の価値のリスク因子の評価に応じて、縮小又は削除する。

9.3 利用者の責任

目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

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

9.3.1.1 全ての利用者に、秘密認証情報を秘密にしておき、関係当局の者を含む他者に秘密認証情報が漏えいしないよう助言する。

9.3.1.2 全ての利用者に、秘密認証情報を、例えば、紙、ソフトウェアのファイル、携帯用の機器に、記録して保管しなように助言する。ただし、記録がセキュリティを確保して保管され、その保管方法が承認されている場合には、この限りではない（例えば、パスワード保管システム(password vault)）。

9.3.1.3 全ての利用者に、秘密認証情報に対する危険の兆候が見られる場合には、その秘密認証情報を変更するよう助言する。

9.3.1.4 全ての利用者に、秘密認証情報としてパスワードを用いる場合は、十分な最短文字数をもつ質の良いパスワードを選定するよう助言する（質の良いパスワードとは、次の条件を満たすものとする。①覚えやすい。②当人の関連情報（例えば、名前、電話番号、誕生日）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。③辞書攻撃にぜい弱でない（すなわち、辞書に含まれる語から成り立っていない。）。④同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではない。⑤仮パスワードを発行する場合、最初のログオン時点で変更する。）。

9.3.1.5 全ての利用者に、個人用の秘密認証情報を共有しないよう助言する。

9.3.1.6 全ての利用者に、自動ログオン手順において、秘密認証情報としてパスワードを用い、かつ、そのパスワードを保管する場合、パスワードの適切な保護を確実にするよう助言する。

9.3.1.7 全ての利用者に、業務目的のものと業務目的でないものとに、同じ秘密認証情報を用いないよう助言する。

9.4 システム及びアプリケーションのアクセス制御

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

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

9.4.1.1 アクセスへの制限は、個々の業務用アプリケーションの要求事項に基づき、定められたアクセス制御方針に従う。

9.4.1.2 アクセス制限の要求事項を満たすために、アプリケーションシステム機能へのアクセスを制御するためのメニューを提供する。

9.4.1.3 アクセス制限の要求事項を満たすために、利用者がアクセスできるデータを制御する。

9.4.1.4 アクセス制限の要求事項を満たすために、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御する。

9.4.1.5 アクセス制限の要求事項を満たすために、他のアプリケーションのアクセス権を制御する。

9.4.1.6 アクセス制限の要求事項を満たすために、出力に含まれる情報を制限する。

9.4.1.7 アクセス制限の要求事項を満たすために、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。

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

9.4.2.1　利用者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。

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

9.4.2.3　システム又はアプリケーションへログオンするための手順は、認可されていないアクセスの機会を最小限に抑えるように設計する。

9.4.2.4　ログオン手順では、認可されていない利用者に無用な助けを与えないために、システム又はアプリケーションについての情報の開示は、最小限にする。

9.4.2.5　システム又はアプリケーションの識別子を、ログオン手順が正常に終了するまで表示しない。

9.4.2.6　ログオン手順では、「コンピュータへのアクセスは、認可されている利用者に限定する」という警告を表示する。

9.4.2.7　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。

9.4.2.8　ログオン手順では、 ログオン情報の妥当性検証は、全ての入力データが完了した時点でだけ行う。誤り条件が発生しても、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指摘しない。

9.4.2.9　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。

9.4.2.10　ログオン手順では、失敗した試み及び成功した試みのログをとる。

9.4.2.11　ログオン制御への違反又は違反が試みられた可能性が検知された場合には、セキュリティ事象として取り上げる。

9.4.2.12　ログオンが成功裏に終了した時点で、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、その詳細を表示する。

9.4.2.13　ログオン手順では、入力したパスワードは表示しない。

9.4.2.14　ログオン手順では、ネットワークを介してパスワードを平文で通信しない。

9.4.2.15　ログオン手順では、リスクの高い場所（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、モバイル機器）では特に、あらかじめ定めた使用中断時間が経過したセッションは終了する。

9.4.2.16　ログオン手順では、リスクの高いアプリケーションのセキュリティを高めるために接続時間を制限し、認可されていないアクセスの危険性を低減する。

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

9.4.3.1　パスワードの管理システムでは、責任追跡性を維持するために、それぞれの利用者ID及びパスワードを使用させるようにする。

9.4.3.2　パスワードの管理システムでは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。

9.4.3.3　パスワードの管理システムでは、質の良いパスワードを選択させるようにする。

9.4.3.4　パスワードの管理システムでは、パスワードは、最初のログオン時に利用者に変更させるようにする。

9.4.3.5　パスワードの管理システムでは、パスワードは、定期的に及び必要に応じて変更させるようにする。

9.4.3.6　パスワードの管理システムでは、以前に用いられたパスワードの記録を維持し、再使用を防止する。

9.4.3.7　パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにする。

9.4.3.8　パスワードの管理システムでは、パスワードのファイルは、アプリケーションシステムのデータとは別に保存する。

9.4.3.9　パスワードの管理システムでは、パスワードは、保護した形態で保存し、伝達する。

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

9.4.4.1　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のための識別、認証及び認可手順を整備し、使用する。

9.4.4.2　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は、アプリケーションソフトウェアから分離する。

9.4.4.3　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、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する。

9.4.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムを臨時に用いる場合の認可手順を整備する。

9.4.4.5　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を制限する（例えば、認可されたシステム変更のための期間での利用）。

9.4.4.6　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全ての使用に関するログを取得する。

9.4.4.7　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認可レベルを明確にし、文書化する。

9.4.4.8　不要な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は全て除去又は無効化する。

9.4.4.9　権限の分離が必要な場合には、システム上のアプリケーションへのアクセス権をもつ利用者に対して、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を禁止する。

9.4.5　プログラムソースコードへのアクセスは、制限する。

9.4.5.1　プログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスは、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に、厳重に管理する。

9.4.5.2　可能な限り、プログラムソースライブラリは、運用システムの中に保持しない。

9.4.5.3　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は、確立した手順に従って管理する。

9.4.5.4　サポート要員による、プログラムソースライブラリへの無制限のアクセスを許さない。

9.4.5.5　プログラムソースライブラリ及び関連情報の更新、並びにプログラマへのプログラムソースの発行は、適切な認可を得た後にだけ実施する。

9.4.5.6　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。

9.4.5.7　プログラムソースライブラリへの全てのアクセスについて、監査ログを維持する。

9.4.5.8　プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従う。

9.4.5.9　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、その完全性を保証するために役立つ追加的な管理策（例えば、ディジタル署名）を実施する。

10　暗号

10.1　暗号による管理策

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

10.1.1　情報を保護するための暗号による管理策の利用[25]に関する方針は、策定し、実施する。

10.1.1.1　暗号の利用に関する方針は、業務情報を保護する上での一般原則も含め、暗号による管理策の組織全体での使用に関する管理の取組みを考慮して定める。

10.1.1.2　暗号の利用に関する方針は、リスクアセスメントに基づく、要求される暗号アルゴリズムの種別、強度及び品質を考慮に入れた、要求された保護レベルの識別を考慮して定める。

10.1.1.3　暗号の利用に関する方針は、持ち運び可能な若しくは取外し可能な媒体装置又は通信によって伝送される情報を、保護するための暗号の利用を考慮して定める。

10.1.1.4　暗号の利用に関する方針は、暗号鍵の保護手法、及び鍵が紛失、危険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、鍵管理に対する取組み方を考慮して定める。

10.1.1.5　暗号の利用に関する方針は、この方針の実施の責任や鍵生成を含めた鍵管理に対する責任など、役割及び責任を考慮して定める。

10.1.1.6　暗号の利用に関する方針は、組織全体にわたって効果的に実施するために採用する標準類（業務プロセスに用いるソリューションの選択）を考慮して定める。

10.1.1.7　暗号の利用に関する方針は、暗号化した情報を用いることの、情報内容の検査（例えば、マルウェアの検出）に依存する管理策への影響を考慮して定める。

10.1.1.8　暗号に関わる組織の方針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含める。

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

10.1.2.1　方針には、暗号鍵の生成、保管、保存、読出し、配布、使用停止及び破壊を含むライフサイクル全体にわたって必要となる、セキュリティを保ったプロセスにおいて、暗号鍵を管理するための要求事項を含める。

10.1.2.2　最適な慣行に従って、暗号アルゴリズム、鍵の長さ及び使用法を選定する。

10.1.2.3　全ての暗号鍵は、改変及び紛失から保護する。

---

[25] 暗号による管理策は、様々な情報セキュリティ目的を達成するために、例えば次のように利用できる。
a）**機密性**　保管又は伝送される、取扱いに慎重を要する情報又は重要な情報を守るための、情報の暗号化の利用
b）**完全性・真正性**　保管又は伝送される、取扱いに慎重を要する情報又は重要な情報の完全性・真正性を検証するための、ディジタル署名又はメッセージ認証コードの利用
c）**否認防止**　ある事象又は活動が、起こったこと又は起こらなかったことの証拠を提供するための、暗号技術の利用
d）**認証**　システム利用者、システムエンティティ及びシステム資源へのアクセスを要求している、又はこれらとやり取りしている、利用者及びその他のシステムエンティティを認証するための、暗号技術の利用

10.1.2.4　鍵の生成、保管及び保存のために用いられる装置は、物理的に保護する。

10.1.2.5　鍵管理システムは、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き、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の鍵を生成する。

10.1.2.6　鍵管理システムは、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き、公開鍵証明書を発行し、入手する。

10.1.2.7　鍵管理システムは、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き、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。）についても含める。

10.1.2.8　鍵管理システムは、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き、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める。

10.1.2.9　鍵管理システムは、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き、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める。

10.1.2.10　鍵管理システムは、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き、危険になった鍵に対処する。

10.1.2.11　鍵管理システムは、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き、鍵を無効にする（例えば、鍵が危険になった場合、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。）。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める。

10.1.2.12　鍵管理システムは、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き、紛失した鍵又は破損した鍵を回復する。

10.1.2.13　鍵管理システムは、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き、鍵をバックアップ又は保存する。

10.1.2.14　鍵管理システムは、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き、鍵を破壊する。

10.1.2.15　鍵管理システムは、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き、鍵管理に関連する活動を記録し、監査する。

10.1.2.16　不適切な使用を起こりにくくするために、鍵の活性化及び非活性化の期日を定め、これによって、鍵管理の方針で定めた期間内でだけ鍵を使用できるようにする。

10.1.2.17　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ためセキュリティを保って管理し、公開鍵は、真正性を保つ[26]。

10.1.2.18　公開鍵証明書を発行する認証局は、要求された信頼度を提供するために適切な管理策及び手順を備え、認知された組織であることを確認する。

10.1.2.19　暗号サービスの外部供給者（例えば、認証局）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ための応答時間に関する事項を含める。

---

[26] 管理策基準において、公開鍵（非対称暗号）方式における一対の鍵のうち、“private key”を“プライベート鍵”とし、“public key”を“公開鍵”とした。また、共通鍵（対称暗号）方式における“secret key”を“秘密鍵”とした。

11　物理的及び環境的セキュリティ

11.1　セキュリティを保つべき領域

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

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

11.1.1.1　情報及び情報処理施設のある領域を保護するために、境界内に設置している資産のセキュリティ要求事項及びリスクアセスメントの結果に基づいて、それぞれの物理的セキュリティ境界の位置及び強度を定める。

11.1.1.2　情報及び情報処理施設のある領域を保護するために、情報処理施設を収容した建物又は敷地の境界は、物理的に頑丈にする（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。）。具体的には、以下の4点を行う。

1. 敷地内の屋根、壁及び床は、堅固な構造物とする。
2. 外部に接する全ての扉を、開閉制御の仕組み（例えば、かんぬき、警報装置、錠）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。
3. 要員が不在のときには、扉及び窓を施錠する。
4. 窓（特に一階の窓）については外部から保護する。

11.1.1.3　情報及び情報処理施設のある領域を保護するために、敷地又は建物への物理的アクセスを管理する。具体的には、以下の2点を行う。

1. 有人の受付又はその他の手段を備える。
2. 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。

11.1.1.4　情報及び情報処理施設のある領域を保護するために、認可されていない物理的アクセス及び周囲への悪影響を防止するために、物理的な障壁を設置する。

11.1.1.5　情報及び情報処理施設のある領域を保護するために、以下の2点を行う。

1. セキュリティ境界上にある全ての防火扉は、該当する地域標準、国内標準及び国際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、警報機能を備え、監視し、試験する。
2. 防火扉は、その地域の消防規則に従って、不具合が発生しても安全側に作動するように運用する。

11.1.1.6　情報及び情報処理施設のある領域を保護するために、以下の4点を行う。

1. 全ての外部に接する扉及びアクセス可能な窓を保護するために、侵入者を検知する適切なシステムを、地域標準、国内標準又は国際標準に沿って導入する。
2. 定めに従って試験を実施する。
3. 無人の領域では、常に警報装置を作動させる。
4. セキュリティ上重要な他の領域（例えば、コンピュータ室、通信機器室）にも、常に警報装置を作動させる。

11.1.1.7　情報及び情報処理施設のある領域を保護するために、組織が自ら管理する情報処理施設は、外部関係者が管理する施設から物理的に分離する。

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

11.1.2.1　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者の入退の日付及び時刻を記録する。

11.1.2.2　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、アクセスが事前に承認されている場合を除いて、全ての訪問者を監督する。

11.1.2.3　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者には、特定され、認可された目的のためのアクセスだけを許可し、その領域のセキュリティ要求事項及び緊急時の手順についての指示を与える。

11.1.2.4　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切な手段によって、訪問者の識別情報を認証する。

11.1.2.5　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切なアクセス制御（例えば、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導入）を実施する。

11.1.2.6　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、秘密情報を処理又は保管する領域へのアクセスを、認可された者だけに制限する。

11.1.2.7　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全てのアクセスについて、物理的な記録日誌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する。

11.1.2.8　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全ての従業員、契約相手及び外部関係者に、何らかの形式の、目に見える証明書の着用を要求する。

11.1.2.9　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、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。

11.1.2.10　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス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。

11.1.2.11　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス要員によるアクセスは認可を必要とし、監視する。

11.1.2.12　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域へのアクセス権は、定期的にレビューし、更新し、必要なときには無効にする。

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

11.1.3.1　オフィス、部屋及び施設のセキュリティを保つために、主要な施設は、一般の人のアクセスが避けられる場所に設置する。

11.1.3.2　オフィス、部屋及び施設のセキュリティを保つために、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、一切表示しないように設計する。

11.1.3.3　オフィス、部屋及び施設のセキュリティを保つために、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、電磁遮蔽も含める。）。

11.1.3.4　オフィス、部屋及び施設のセキュリティを保つために、秘密情報処理施設の場所を示す案内板及び内線電話帳は、認可されていない者が容易にアクセスできないようにする。

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

11.1.4.1　火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害からの損傷を回避する方法について、専門家の助言を得る。

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

11.1.5.1　セキュリティを保つべき領域での作業に関する手順の設計においては、要員は、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は、業務上知る必要のある要員にのみ知らせることを含める。

11.1.5.2　セキュリティを保つべき領域での作業に関する手順の設計に、安全面の理由のため及び悪意ある活動の機会を防止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、回避することを含める。

11.1.5.3　セキュリティを保つべき領域での作業に関する手順の設計に、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、定期的に点検することを含める。

11.1.5.4　セキュリティを保つべき領域での作業に関する手順の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯端末に付いたカメラ）は、認可されたもの以外は許可しないことを含める。

11.1.5.5　セキュリティを保つべき領域での作業に関する取決めには、その領域で作業する従業員及び外部の利用者に対する管理策を含める。

11.1.5.6　セキュリティを保つべき領域での作業に関する取決めは、セキュリティを保つべき領域で行われる全ての活動に適用する。

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

11.1.6.1　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、建物外部からの受渡場所へのアクセスは、識別及び認可された要員に制限する。

11.1.6.2　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所は、配達要員が建物の他の場所にアクセス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。

11.1.6.3　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所の外部扉は、内部の扉が開いているときにはセキュリティを保つ。

11.1.6.4　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、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。

11.1.6.5　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。

11.1.6.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもある

その他の場所を管理するため、入荷と出荷とは、物理的に分離した場所で扱う。

11.1.6.7　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、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。

11.2　装置

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

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

11.2.1.1　装置を保護するために、装置は、作業領域への不必要なアクセスが最小限になるように設置する。

11.2.1.2　装置を保護するために、取扱いに慎重を要するデータを扱う情報処理施設は、施設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よう、その位置を慎重に定める。

11.2.1.3　装置を保護するために、認可されていないアクセスを回避するよう、保管設備のセキュリティを保つ。

11.2.1.4　装置を保護するために、特別な保護を必要とする装置は、それ以外の装置を分離するか、若しくは装置間に障壁を設ける。

11.2.1.5　装置を保護するために、潜在的な物理的及び環境的脅威（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）のリスクを最小限に抑えるよう管理策を採用する。

11.2.1.6　装置を保護するために、情報処理施設の周辺での飲食及び喫煙に関する指針を確立する。

11.2.1.7　装置を保護するために、情報処理施設の運用に悪影響を与えることがある環境条件（例えば、温度、湿度）を監視する。

11.2.1.8　装置を保護するために、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。

11.2.1.9　装置を保護するために、作業現場などの環境にある装置には、特別な保護方法（例えば、キーボードカバー）を使用する。

11.2.1.10　装置を保護するために、秘密情報を処理する装置は、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。

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

11.2.2.1　サポートユーティリティ（例えば、電気、通信サービス、給水、ガス、下水、換気、空調）は、装置の製造業者の仕様及び地域の法的要求事項に適合しているものを採用する。

11.2.2.2　サポートユーティリティは、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。

11.2.2.3　サポートユーティリティは、適切に機能することを確実にするために、定期的に検査及び試験する。

11.2.2.4　サポートユーティリティは、必要であれば、不具合を検知するための警報装置を取り付ける。

11.2.2.5　サポートユーティリティは、必要であれば、物理的な経路が異なる複数の供給元を確保する。

11.2.2.6　非常用の照明及び通信手段を備える。

11.2.2.7　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。

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

11.2.3.1　情報処理施設に接続する電源ケーブル及び通信回線は、地下に埋設するか、又はこれに代わる十分な保護手段を施す。

11.2.3.2　ケーブル間の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。

11.2.3.3　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、以下の4点を行う。

1. 外装電線管を導入し、点検箇所・終端箇所の施錠可能な部屋又は箱へ設置する。
2. ケーブルを保護するための電磁遮蔽を利用する。
3. ケーブルに取り付けられた認可されていない装置の技術的探索及び物理的検査を実施する。
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を実施する。

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

11.2.4.1　可用性及び完全性を継続的に維持することを確実とするために、装置は、供給者の推奨する間隔及び仕様に従って保守する。

11.2.4.2　可用性及び完全性を継続的に維持することを確実とするために、認可された保守要員だけが、装置の修理及び手入れを実施する。

11.2.4.3　可用性及び完全性を継続的に維持することを確実とするために、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。

11.2.4.4　可用性及び完全性を継続的に維持することを確実とするために、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。その装置から秘密情報を消去するか、又は保守要員が十分に信頼できる者であることを確かめる。

11.2.4.5　可用性及び完全性を継続的に維持することを確実とするために、保険約款で定められた、保守に関する全ての要求事項を順守する。

11.2.4.6　可用性及び完全性を継続的に維持することを確実とするために、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不具合を起こさないことを確実にするために検査する。

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

11.2.5.1　資産を構外に持ち出すことを許す権限をもつ従業員及び外部の利用者を特定する。

11.2.5.2　資産の持出し期限を設定し、また、返却がそのとおりであったか検証する。

11.2.5.3　資産が構外に持ち出されていることを記録し、また、返却時に記録する。

11.2.5.4　資産を扱う又は利用する者について、その識別情報、役割及び所属を文書化し、構外へ持ち出した装置、情報又はソフトウェアとともに返却させる。

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

11.2.6.1　情報を保管及び処理する装置（組織が所有する装置、及び個人が所有し組織のために用いる装置）を組織の構外で用いる場合は、管理層の認可を得る。

11.2.6.2　構外に持ち出した装置及び媒体は、公共の場所に無人状態で放置しない。

11.2.6.3　構外にある装置の保護のために、装置の保護（例えば、強力な電磁場にさらすことに対する保護）に関する製造業者の指示を常に守る。

11.2.6.4　構外にある装置の保護のために、在宅勤務、テレワーキング及び一時的サイトのような構外の場所についての管理策を、リスクアセスメントに基づいて決定し、状況に応じた管理策（例えば、施錠可能な文書保管庫、クリアデスク方針、コンピュータのアクセス制御、セキュリティを保ったオフィスとの通信）を適切に適用する。

11.2.6.5　構外にある装置の保護のために、構外にある装置を、複数の個人又は外部関係者の間で移動する場合には、その装置の受渡記録を明記した記録（少なくとも、その装置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。

11.2.6.6　リスク（例えば、損傷、盗難、傍受）は、場所によってかなり異なる場合があるため、それぞれの場所に応じた最も適切な管理策は、リスクを考慮して決定する。

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

11.2.7.1　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。

11.2.7.2　秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊すること、又はその情報を破壊、消去若しくは上書きする。

11.2.7.3　秘密情報又は著作権のある情報を格納した記憶媒体の消去又は上書きには、標準的な消去又は初期化の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。

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

11.2.8.1　無人状態にある装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、全ての利用者に認識させる。

11.2.8.2　利用者に、実行していた処理が終わった時点で、接続を切るよう助言する（ただし、例えば、パスワードによって保護されたスクリーンセーバなどの適切なロック機能によって保護されている場合は、その限りではない。）。

11.2.8.3　利用者に、必要がなくなったら、アプリケーション又はネットワークサービスからログオフするよう助言する。

11.2.8.4　利用者に、コンピュータ又はモバイル機器は、利用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって、認可されていない利用から保護するよう助言する。

11.2.9　書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。[27]

11.2.9.1　クリアデスク・クリアスクリーン方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応するリスク及び文化的側面を含める。

---

[27] クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。

11.2.9.2　取扱いに慎重を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）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）保管する。

11.2.9.3　コンピュータ及び端末は、離席時には、ログオフ状態にするか、又はパスワード、トークン若しくは類似の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する。

11.2.9.4　コンピュータ及び端末は、利用しないときは、施錠、パスワード又は他の管理策によって保護する。

11.2.9.5　コピー機及びその他の再生技術（例えば、スキャナ、ディジタルカメラ）の認可されていない利用は、防止する。

11.2.9.6　取扱いに慎重を要する情報又は機密扱い情報を含む媒体は、プリンタから直ちに取り出す。

12　運用のセキュリティ

12.1　運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。

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

12.1.1.1　情報処理設備及び通信設備に関連する操作（例えば、コンピュータの起動・停止の手順、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書を作成する。

12.1.1.2　情報処理設備及び通信設備に関連する操作手順には、システムの導入及び構成を含む、操作上の指示を明記する。

12.1.1.3　情報処理設備及び通信設備に関連する操作手順には、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。）を含む、操作上の指示を明記する。

12.1.1.4　情報処理設備及び通信設備に関連する操作手順には、バックアップを含む、操作上の指示を明記する。

12.1.1.5　情報処理設備及び通信設備に関連する操作手順には、スケジュール作成に関する要求事項（他のシステムとの相互依存性、最も早い作業の開始時刻及び最も遅い作業の完了時刻など）を含む、操作上の指示を明記する。

12.1.1.6　情報処理設備及び通信設備に関連する操作手順には、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（システムユーティリティの利用の制限）を含む、操作上の指示を明記する。

12.1.1.7　情報処理設備及び通信設備に関連する操作手順には、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、サポート用及び段階的取扱い（escalation）用の連絡先を含む、操作上の指示を明記する。

12.1.1.8　情報処理設備及び通信設備に関連する操作手順には、特別な出力及び媒体の取扱いに関する指示（特殊な用紙の使用、秘密情報の出力の管理（失敗した作業出力のセキュリティを保った処分手順を含む。））を含む、操作上の指示を明記する。

12.1.1.9　情報処理設備及び通信設備に関連する操作手順には、システムが故障した場合の再起動及び回復の手順を含む、操作上の指示を明記する。

12.1.1.10　情報処理設備及び通信設備に関連する操作手順には、監査証跡及びシステムログ情報の管理を含む、操作上の指示を明記する。

12.1.1.11　情報処理設備及び通信設備に関連する操作手順には、監視手順を含む、操作上の指示を明記する。

12.1.1.12　システムの管理活動のための操作手順及び文書化手順は、正式な文書として取り扱い、その手順書の変更は、管理層が認可する。

12.1.1.13　情報システムは、技術的に可能な場合には、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。

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

12.1.2.1　組織、業務プロセス、情報処理設備及びシステムの変更管理には、重要な変更の特定及び記録を含める。

12.1.2.2　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更作業の計画策定及びテストの実施を含める。

12.1.2.3　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の潜在的な影響（情報セキュリティ上の影響を含む。）のアセスメントを含める。

12.1.2.4　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の申出を正式に承認する手順を含める。

12.1.2.5　組織、業務プロセス、情報処理設備及びシステムの変更管理には、情報セキュリティ要求事項が満たされていることの検証を含める。

12.1.2.6　組織、業務プロセス、情報処理設備及びシステムの変更管理には、全ての関係者への変更に関する詳細事項の通知を含める。

12.1.2.7　組織、業務プロセス、情報処理設備及びシステムの変更管理には、うまくいかない変更及びこれに伴う予期できない事象を取り消し、これらから回復する手順及び責任を含む、代替手順を確立することを含める。

12.1.2.8　組織、業務プロセス、情報処理設備及びシステムの変更管理には、インシデントの解決のために必要な変更を、迅速にかつ管理して実施できるようにするための、緊急時の変更プロセスの提供を含める。

12.1.2.9　組織、業務プロセス、情報処理設備及びシステムに対するあらゆる変更の十分な管理を確実にするために、正式な責任体制及び手順を備える。

12.1.2.10　組織、業務プロセス、情報処理設備及びシステムに対する変更がなされたときには、変更に関わる全ての関連情報を含んだ監査ログを保持する。

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

12.1.3.1　事業におけるシステムの重要度を考慮に入れて、その容量・能力に関する要求事項を特定する。

12.1.3.2　システムの可用性及び効率性を確実にするため、また、改善のために、システム調整及び監視を適用する。

12.1.3.3　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。

12.1.3.4　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含める。

12.1.3.5　管理者は、特別な注意を払う必要のある主要なシステム資源（入手時間がかかるか又は費

用がかかる資源）の使用を監視する。

12.1.3.6　管理者は、使用の傾向、特に業務用アプリケーション又は情報システムの管理ツールに関連した傾向を特定する。

12.1.3.7　システムセキュリティ又はサービスに脅威をもたらすおそれのある、潜在的なあい（隘）路（bottlenecks）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、上記の監視及び傾向を特定した情報を利用して、適切な処置[28]を立案する。

12.1.3.8　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。

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

12.1.4.1　運用上の問題を防ぐために必要な、開発環境、試験環境及び運用環境の間の分離レベルを特定し、それに従って分離する。

12.1.4.2　ソフトウェアの開発から運用の段階への移行についての規則は、明確に定め、文書化する。

12.1.4.3　開発ソフトウェア及び運用ソフトウェアは、異なるシステム又はコンピュータ上で、及び異なる領域又はディレクトリで実行する。

12.1.4.4　運用システム及びアプリケーションに対する変更は、運用システムに適用する前に、試験環境又はステージング環境（運用環境に近い試験環境）で試験する。

12.1.4.5　例外的な状況以外では、運用システムで試験を行わない。

12.1.4.6　コンパイラ、エディタ、及びその他の開発ツール又はシステムユーティリティは、必要でない場合には、運用システムからアクセスできないようにする。

12.1.4.7　利用者は、運用システム及び試験システムに対して、異なるユーザプロファイルを用いる。

12.1.4.8　メニューには、誤操作によるリスクを低減するために、適切な識別メッセージを表示する。

12.1.4.9　取扱いに慎重を要するデータは、試験システムに同等の管理策が備わっていない限り、その試験システム環境には複写を禁止する。

12.2　マルウェアからの保護

目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。

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

12.2.1.1　マルウェアに対する検出・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き、マルウェアから保護する。

12.2.1.2　認可されていないソフトウェアの使用を禁止する正式な方針を確立する。

12.2.1.3　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管理策を実施（例えば、アプリケーションのホワイトリスト化）する。

12.2.1.4　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を実施（例えば、ブラックリスト）する。

---

[28] 容量・能力を増やすか、要求を減らすことによって、十分な容量・能力を提供することができる。容量・能力の要求に関する管理の例には、次を含む。

a）古いデータの削除（ディスクスペース）

b）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

c）バッチのプロセス及びスケジュールの最適化

d）アプリケーションの処理方法及びデータベースへの問合せの最適化

e）事業上重要でない場合，大量の帯域を必要とするサービス（例えば，動画のストリーミング）に対する帯域割当ての拒否又は制限

12.2.1.5　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から保護し、どのような保護対策を行うことが望ましいかを示す組織の正式な方針を確立する。

12.2.1.6　マルウェアに付け込まれる可能性のあるぜい弱性を、技術的ぜい弱性管理などを通じて低減させる。

12.2.1.7　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の、定めに従ったレビューを実施する。未承認のファイル又は認可されていない変更があった場合には、正式に調査する。

12.2.1.8　予防又は定常作業として、コンピュータ及び媒体を走査（scan）するために、マルウェアの検出・修復ソフトウェアの導入及び定めに従った更新として、以下の3点を行う。

1. ネットワーク経由又は何らかの形式の記憶媒体を通じて入手した全てのファイルに対する、マルウェア検出のための使用前の走査
2. 電子メール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走査。この走査は、様々な場所（例えば、電子メールサーバ、デスクトップコンピュータ、組織のネットワークの入口）で実施する。
3. ウェブページに対するマルウェア検出のための走査

12.2.1.9　システムにおけるマルウェアからの保護、保護策の利用方法に関する訓練、マルウェアの攻撃の報告及びマルウェアの攻撃からの回復に関する手順及び責任を明確にする。

12.2.1.10　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を策定する。

12.2.1.11　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、バックアップ及び回復の手順を含める。

12.2.1.12　常に情報を収集するための手順を実施（例えば、新種のマルウェアに関する情報を提供するメーリングリストへの登録又はウェブサイトの確認）する。

12.2.1.13　マルウェアに関する情報を確認し、警告情報が正確かつ役立つことを確実にするための以下の2つの手順を実施する。

1. 管理者は、単なるいたずらと真のマルウェアとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、マルウェアの対策ソフトウェア供給者）の利用を確実にする仕組みを整備する
2. 管理者は、マルウェアではなく、いたずらの問題及びそれらを受け取ったときの対応について、全ての利用者に認識させる仕組みを整備する

12.2.1.14　壊滅的な影響が及ぶ可能性のある環境を隔離する。

12.3　バックアップ

目的：データの消失から保護するため。

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

12.3.1.1　バックアップ方針を確立し、情報、ソフトウェア及びシステムイメージのバックアップに関する組織の要求事項を定める。

12.3.1.2　バックアップ方針では、保管及び保護に関する要求事項を定める。

12.3.1.3　災害又は媒体故障の発生の後に、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。

12.3.1.4　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。

12.3.1.5　バックアップの範囲（例えば、フルバックアップ、差分バックアップ）、及びバックアップの頻度は、組織の業務上の要求事項、関連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事業継続に対しての重要度を考慮して決定する。

12.3.1.6　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、十分離れた場所に保管する。

12.3.1.7　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を実施する。

12.3.1.8　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、定めに従って試験する。

12.3.1.9　バックアップに用いる媒体の試験は、データ復旧手順の試験と併せて行い、必要なデータ復旧時間に照らし合わせて確認する。

12.3.1.10　バックアップデータを復旧させる能力の試験は、バックアップ手順又はデータ復旧プロセスに失敗し、データに修復不能な損傷又は損失が発生した場合に備えて、原本の媒体に上書きするのではなく、専用の試験媒体を用いて行う。

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

12.3.1.12　運用手順では、バックアップ方針に従って、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、計画されたバックアップの失敗に対処する。

12.3.1.13　個々のシステム及びサービスに関するバックアップの取決めは、事業継続計画の要求事項を満たすことを確実にするために、定めに従って試験する。

12.3.1.14　重要なシステム及びサービスに関するバックアップの取決めは、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。

12.3.1.15　永久保存する複製物に関するあらゆる要求事項を考慮に入れて、不可欠な業務情報の保管期間を決定する。

12.4　ログ取得及び監視

目的：イベントを記録し、証拠を作成するため。

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

12.4.1.1　イベントログには、利用者IDを含める。

12.4.1.2　イベントログには、システムの動作を含める。

12.4.1.3　イベントログには、主要なイベントの日時及び内容（例えば、ログオン、ログオフ）を含める。

12.4.1.4　イベントログには、装置のID又は所在地（可能な場合）、及びシステムの識別子を含める。

12.4.1.5　イベントログには、システムへのアクセスの、成功及び失敗した試みの記録を含める。

12.4.1.6　イベントログには、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の記録を含める。

12.4.1.7　イベントログには、システム構成の変更を含める。

12.4.1.8　イベントログには、特権の利用を含める。

12.4.1.9　イベントログには、システムユーティリティ及びアプリケーションの利用を含める。

12.4.1.10　イベントログには、アクセスされたファイル及びアクセスの種類を含める。

12.4.1.11　イベントログには、ネットワークアドレス及びプロトコルを含める。

12.4.1.12　イベントログには、アクセス制御システムが発した警報を含める。

12.4.1.13　イベントログには、保護システム（例えば、ウィルス対策システム、侵入検知システム）の作動及び停止を含める。

12.4.1.14　イベントログには、アプリケーションにおいて利用者が実行したトランザクションの記録を含める。

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

12.4.2.1　記録されたメッセージ形式の変更から保護する。

12.4.2.2　認可されていないログファイルの編集又は削除から保護する。

12.4.2.3　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を引き起こす、ログファイル媒体の記録容量超過の問題から保護する。

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

12.4.3.1　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業を記録する。

12.4.3.2　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その利用者の作業のログを保護する。

12.4.3.3　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業のログを定期的にレビューする。

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

12.4.4.1　時刻の表示、同期及び正確さに関する外部及び内部の要求事項[29]は、文書化する。

12.4.4.2　組織内で用いるための基準となる時刻源を定める。

12.4.4.3　基準となる時刻源を外部から取得するための組織の取組み及び内部のクロックを確実に同期させる方法を文書化し、実施する。

12.5　運用ソフトウェアの管理

目的：運用システムの完全性を確実にするため。

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

12.5.1.1　運用ソフトウェア、アプリケーション及びプログラムライブラリの更新は、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。

12.5.1.2　運用システムは、実行可能なコードだけを保持し、開発用コード又はコンパイラは保持しない。

12.5.1.3　アプリケーション及びオペレーティングシステムソフトウェアは、十分な試験に成功した後に導入する。

12.5.1.4　アプリケーション及びオペレーティングシステムソフトウェアの試験は、使用性、セキュリティ、他システムへの影響及びユーザフレンドリ性の試験を含める。

12.5.1.5　アプリケーション及びオペレーティングシステムソフトウェアの試験は、運用システムと

[29] このような要求事項は、法的、規制及び契約上の要求事項、標準類の順守、又は内部監視に関する要求事項であり得る。

は別のシステムで実行する。

12.5.1.6　アプリケーション及びオペレーティングシステムソフトウェアの試験は、対応するプログラムソースライブラリが更新済みであることを確実にする仕組みを整備する。

12.5.1.7　導入したソフトウェアの管理を維持するために、システムに関する文書化と同様に、構成管理システムを利用する。

12.5.1.8　変更を実施する前に、ロールバック計画を備える。

12.5.1.9　運用プログラムライブラリの更新の全てについて、監査ログを維持する。

12.5.1.10　緊急時対応の手段として、一つ前の版のアプリケーションソフトウェアを保持する。

12.5.1.11　ソフトウェアの旧版は、そのソフトウェアが扱ったデータが保存されている間は、必要とされる情報及びパラメータの全て、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する。

12.5.1.12　運用システムに利用される業者供給ソフトウェアは、供給者によってサポートされるレベルを維持する。

12.5.1.13　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して管理する。

12.5.1.14　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（例えば、新しい情報セキュリティ機能の導入、この版が必要になった情報セキュリティ問題の量及び質）を考慮して行う。

12.5.1.15　情報セキュリティ上の弱点を除去するか、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。

12.5.1.16　供給者による物理的又は論理的アクセスは、サポート目的で必要なときに、管理層の承認を得た場合にだけ許可する。

12.5.1.17　供給者による物理的又は論理的アクセスを許可している間は、供給者の活動を監視する。

12.5.1.18　セキュリティ上の弱点を招く可能性のある認可されていない変更を回避するために、外部から供給されるソフトウェア及びモジュールは、監視し、管理する。

12.6　技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため。

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

12.6.1.1　技術的ぜい弱性の管理をサポートするために必要となる具体的な情報には、ソフトウェア業者、版番号、配置状況（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。）、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。

12.6.1.2　潜在していた技術的ぜい弱性を特定したときは、適切かつ時機を失しない処置をとる。

12.6.1.3　技術的ぜい弱性の管理に関連する役割及び責任を定める。

12.6.1.4　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、パッチの適用、資産移動の追跡、及び要求される全ての調整責務を含める。

12.6.1.5　技術的ぜい弱性を特定し、また、それらぜい弱性を継続して認識させるために用いる情報資源（ぜい弱性検査ツールなど）を、ソフトウェア及びその他の技術（組織の資産目録リストに基づく。）に対応させて特定する。

12.6.1.6　技術的ぜい弱性の情報資源は、資産目録を変更したとき、又は他の新しい若しくは有益な

資源を発見したときに更新を行う。

12.6.1.7　潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める。

12.6.1.8　潜在的な技術的ぜい弱性が特定されたときは、組織は、それと関連するリスク及びとるべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する。

12.6.1.9　技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、とるべき処置を実行する。

12.6.1.10　正当な供給元からパッチを入手できる場合は、そのパッチを適用することに関連したリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。）。

12.6.1.11　パッチの適用前に、それらが有効であること及びそれらが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、パッチを試験及び評価するとともに、利用可能なパッチがない場合は、以下の4点を実施する。

1. そのぜい弱性に関係するサービス又は機能を停止する。
2. ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する。
3. 実際の攻撃を検知するために、監視を強化する。
4. ぜい弱性に対する認識を高める。

12.6.1.12　修正パッチの適用、その他実施した全ての手順について監査ログを保持する。

12.6.1.13　技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する。

12.6.1.14　技術的ぜい弱性は、リスクの高いシステムには最初に対処する。

12.6.1.15　技術的ぜい弱性に対する有効な管理プロセスは、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準備するために、インシデント管理活動と整合させる。

12.6.1.16　ぜい弱性が特定されていながら適切な対応策がない場合には、その状況に対処するための手順を定める。

12.6.1.17　ぜい弱性が特定されていながら適切な対応策がない場合には、組織は、既知のぜい弱性に関するリスクを評価し、適切な検知及び是正処置を定める。

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

12.6.2.1　組織は、利用者がインストールしてもよいソフトウェアの種類について、厳密な方針を定め、施行する。

12.6.2.2　特権の許可は最小限にするという原則を適用する。

12.6.2.3　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（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）、及び禁止するもの（例えば、個人利用のためのソフトウェア、潜在的な悪意の有無が不明又はその疑いがあるソフトウェア）を特定する。

12.6.2.4　特権は、関連する利用者の役割を考慮したうえで付与する。

12.7　情報システムの監査に対する考慮事項

目的：運用システムに対する監査活動の影響を最小限にするため。

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

12.7.1.1　システム及びデータへのアクセスに関する監査要求事項は、適切な管理層の同意を得る。

12.7.1.2　技術監査における試験の範囲を、合意し、管理する。

12.7.1.3　監査における試験は、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。

12.7.1.4　監査における試験では、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消去するか、又は監査の文書化の要求の下で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。

12.7.1.5　監査における試験を実施するための、 特別又は追加の処理に関する要求事項を特定し、合意する。

12.7.1.6　監査における試験がシステムの可用性に影響する可能性がある場合、こうした試験は営業時間外に実施する。

12.7.1.7　監査における試験を実施する際には、参照用の証跡を残すために、全てのアクセスを監視し、ログをとる。

13　通信のセキュリティ

13.1　ネットワークセキュリティ管理

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

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

13.1.1.1　ネットワークにおける情報のセキュリティ、及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にするために、管理策を実施する。

13.1.1.2　ネットワーク設備の管理に関する責任及び手順を確立する。

13.1.1.3　ネットワークの運用責任は、コンピュータの運用から、分離する。

13.1.1.4　公衆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、特別な管理策を確立する。

13.1.1.5　ネットワークサービスの可用性及びネットワークを介して接続したコンピュータの可用性を維持するために、特別な管理策を確立する。

13.1.1.6　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連した行動を記録及び検知できるように、適切なログ取得及び監視を適用する。

13.1.1.7　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、様々な管理作業を綿密に調整する。

13.1.1.8　ネットワーク上のシステムを認証する。

13.1.1.9　ネットワークへのシステムの接続を制限する。

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

13.1.2.1　ネットワークサービスの提供者と合意したサービスをセキュリティを保って管理するために必要なネットワークサービス提供者の能力を定め、常に監視し、監査の権利についてネ

ットワークサービス提供者と合意する。

13.1.2.2　それぞれのサービスに必要なセキュリティについての取決め（例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、組織は、ネットワークサービス提供者によるこれらの対策の実施を確実にする仕組みを整備する。

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

13.1.3.1　大規模なネットワークのセキュリティを管理するために、必要に応じてネットワークを幾つかのネットワーク領域に分離する。

13.1.3.2　ネットワーク領域は、組織の単位（例えば、人的資源、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、信頼性のレベル（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）に基づいて選択する。

13.1.3.3　ネットワーク領域の分離は、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（例えば、仮想私設網）を用いることによって行う。

13.1.3.4　各ネットワーク領域の境界は、明確に定める。

13.1.3.5　ネットワーク領域間のアクセスは、境界にゲートウェイ（例えば、ファイアウォール、フィルタリングルータ）を設けて制御する。

13.1.3.6　各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に基づき、ネットワークを領域に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を定める。

13.1.3.7　各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は、アクセス制御方針、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い、また、費用対効果を考慮して適切なゲートウェイ技術を組み込む。

13.1.3.8　ネットワークの境界が十分に定められていない無線ネットワークでは、ネットワーク領域の分離のための特別な取扱いを定める。

13.1.3.9　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の方針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[30]されるまでは、内部ネットワークから分離する。

13.2　情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

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

13.2.1.1　情報転送のために通信設備を利用するときに従う手順及び管理策には、転送する情報を、盗聴、複製、改ざん、誤った経路での通信及び破壊から保護するために設計された手順を反映する。

13.2.1.2　情報転送のために通信設備を利用するときに従う手順及び管理策には、電子的メッセージ通信を通じて伝送される可能性のあるマルウェアを検出し、これらから保護するための手順を反映する。

13.2.1.3　情報転送のために通信設備を利用するときに従う手順及び管理策には、添付形式として通信される、取扱いに慎重を要する電子情報の保護に関する手順を反映する。

13.2.1.4　情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の許容で

[30] 認証、暗号化及び利用者レベルでのアクセス制御技術が適切に実施された場合、最新かつ標準に基づく無線ネットワークは、組織の内部ネットワークへ直接接続するために十分な場合がある。

きる利用について規定した方針又は指針を反映する。

13.2.1.5　情報転送のために通信設備を利用するときに従う手順及び管理策には、要員、外部関係者及びその他の利用者の、組織を危うくするような行為（例えば、名誉き（毀）損、嫌がらせ、成りすまし、チェーンメールの転送、架空購入）をしないことの責任を含める。

13.2.1.6　情報転送のために通信設備を利用するときに従う手順及び管理策には、暗号技術の利用（例えば、情報の機密性、完全性及び真正性を保護するための暗号の利用）を含める。

13.2.1.7　情報転送のために通信設備を利用するときに従う手順及び管理策には、関連する国及び地域の法令及び規制に従った、全ての業務通信文（メッセージを含む。）の保持及び処分に関する指針を反映する。

13.2.1.8　情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の利用（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）に関する管理策及び制限を反映する。

13.2.1.9　情報転送のために通信設備を利用するときに従う手順及び管理策には、秘密情報を漏えいしないように適切な予防策を講じることの、要員への助言を含める。

13.2.1.10　情報転送のために通信設備を利用するときに従う手順及び管理策には、留守番電話に残したメッセージの、認可されていない者による再生、共有システムに保管、又は誤ダイアルによる間違った先へ保管されることを防止するため、秘密情報を含んだメッセージを留守番電話に残さないことを含める。

13.2.1.11　情報転送のために通信設備を利用するときに従う手順及び管理策には、ファクシミリ又はそのサービスの利用に伴う問題（ファクシミリの受信文の取出し装置への認可されていないアクセス、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、誤ダイアル、又は間違って記憶した番号を用いることによる、誤った番号への文書及びメッセージの送付）について要員に意識させることを含める。

13.2.1.12　公共の場所、並びにセキュリティが確保されていない通信経路、出入りが自由なオフィス及び会議室では、秘密の会話はしないほうがよいことを要員に意識させる。

13.2.1.13　情報転送サービスは、関連するいかなる法的要求事項についても順守する。

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

13.2.2.1　情報転送に関する合意に、送信、発送及び受領についての管理及び通知を行う責任を含める。

13.2.2.2　情報転送に関する合意に、追跡可能性及び否認防止を確実にするための手順を含める。

13.2.2.3　情報転送に関する合意に、こん（梱）包及び送信に関する必要最小限の技術標準を含める。

13.2.2.4　情報転送に関する合意に、預託条項を含める。

13.2.2.5　情報転送に関する合意に、運送業者を確認する規準を含める。

13.2.2.6　情報転送に関する合意に、情報セキュリティインシデントが発生した場合（例えば、データの紛失）の責任及び賠償義務を含める。

13.2.2.7　情報転送に関する合意に、取扱いに慎重を要する又は重要な情報に対する、合意されたラベル付けシステム（ラベルの意味を直ちに理解すること、及び情報を適切に保護することを確実にするもの）の使用を含める。

13.2.2.8　情報転送に関する合意に、情報及びソフトウェアの記録及び読出しに関する技術標準を含

める。

13.2.2.9　情報転送に関する合意に、取扱いに慎重を要するもの（例えば、暗号鍵）を保護するために必要とされる、特別な管理策を含める。

13.2.2.10　情報転送に関する合意に、転送中の情報についての、管理状況の履歴の維持を含める。

13.2.2.11　情報転送に関する合意に、容認できるアクセス制御のレベルを含める。

13.2.2.12　情報転送に関する合意においては、転送中の情報及び物理的媒体を保護するための方針、手順及び標準類を確立及び維持し、参照する。

13.2.2.13　情報交換に関する、いかなる合意における情報セキュリティの事項も、関連する業務情報の取扱いに慎重を要する度合いを反映する。

13.2.3　電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.3.1　電子的メッセージ通信のための情報セキュリティでは、組織が採用している分類体系に従った、認可されていないアクセス、改ざん又はサービス妨害からのメッセージを保護する。

13.2.3.2　電子的メッセージ通信のための情報セキュリティでは、正しい送付先及びメッセージ送信を確実にする仕組みを整備する。

13.2.3.3　電子的メッセージ通信のための情報セキュリティでは、サービスの信頼性及び可用性を確保する。

13.2.3.4　電子的メッセージ通信のための情報セキュリティでは、法的考慮（例えば、電子署名のための要求事項）を含める。

13.2.3.5　電子的メッセージ通信のための情報セキュリティでは、誰でも使える外部サービス（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）を利用する際の、事前承認を取得する。

13.2.3.6　電子的メッセージ通信のための情報セキュリティでは、公開されているネットワークからのアクセスを制御する、より強固な認証レベルを決定する。

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

13.2.4.1　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。

13.2.4.2　秘密保持契約又は守秘義務契約は、外部関係者又は組織の従業員に適用する。

13.2.4.3　秘密保持契約又は守秘義務契約の当事者の種類、並びに当事者に許可される秘密情報のアクセス及び取扱いを考慮して、契約の要素を選定又は追加する。

13.2.4.4　秘密保持契約又は守秘義務契約には、保護される情報の定義（例えば、秘密情報）を含める。

13.2.4.5　秘密保持契約又は守秘義務契約には、秘密を無期限に保持する場合も含めた、契約の有効期間を含める。

13.2.4.6　秘密保持契約又は守秘義務契約には、契約終了時に要求する処置を含める。

13.2.4.7　秘密保持契約又は守秘義務契約には、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を含める。

13.2.4.8　秘密保持契約又は守秘義務契約には、情報、企業秘密及び知的財産の所有権、並びにこれらの秘密情報の保護との関連を含める。

13.2.4.9　秘密保持契約又は守秘義務契約には、秘密情報の許可された利用範囲、及び情報を利用す

る署名者の権利を含める。

13.2.4.10　秘密保持契約又は守秘義務契約には、秘密情報に関する行為の監査及び監視の権利を含める。

13.2.4.11　秘密保持契約又は守秘義務契約には、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を含める。

13.2.4.12　秘密保持契約又は守秘義務契約には、契約終了時における情報の返却又は破棄に関する条件を含める。

13.2.4.13　秘密保持契約又は守秘義務契約には、契約違反が発生した場合にとるべき処置を含める。

13.2.4.14　組織の情報セキュリティ要求事項に応じて、秘密保持契約又は守秘義務契約に必要な要素を含める。

13.2.4.15　秘密保持契約又は守秘義務契約は、その法域において適用される法令及び規制の全てに従う。

13.2.4.16　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。

14　システムの取得、開発及び保守

14.1　情報システムのセキュリティ要求事項

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

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

14.1.1.1　情報セキュリティ要求事項は、方針及び規則に由来する順守の要求事項、脅威のモデリング、インシデントのレビュー、又はぜい弱性の限界の使用のような、様々な方法を用いて特定する。

14.1.1.2　情報セキュリティ要求事項の特定作業の結果は、文書化し、全ての利害関係者によってレビューする。

14.1.1.3　情報セキュリティ要求事項及び情報セキュリティ管理策には、関連する情報の業務上の価値、及びセキュリティが不十分だった場合に業務に及ぶ可能性のある悪影響を反映する。

14.1.1.4　情報セキュリティ要求事項及び関連するプロセスの特定及び管理は、情報システムプロジェクトにその初期段階で統合する。

14.1.1.5　情報セキュリティ要求事項においては、利用者認証の要求事項を導き出すために、利用者が提示する識別情報に対して求める信頼のレベルを定める。

14.1.1.6　情報セキュリティ要求事項においては、業務上の利用者のほか、特権を与えられた利用者及び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を定める。

14.1.1.7　情報セキュリティ要求事項においては、利用者及び運用担当者に対する、各自の義務及び責任の通知を明確にする。

14.1.1.8　情報セキュリティ要求事項においては、関連する資産の保護の要求、特に、可用性、機密性及び完全性に関する保護の要求を明確にする。

14.1.1.9　情報セキュリティ要求事項においては、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を定める。

14.1.1.10　情報セキュリティ要求事項においては、他のセキュリティ管理策によって義務付けられる要求事項を定める（例えば、ログ取得及び監視のインターフェース、情報漏えい検知システム）。

14.1.1.11　公衆ネットワークを介してサービスを提供するアプリケーション、又はトランザクションを実施するアプリケーションについては、14.1.2 及び14.1.3の管理策を考慮して決定する。

14.1.1.12　製品を入手する際には、正式な試験及び調達プロセスに従う。

14.1.1.13　製品の供給者との契約は、明確にされたセキュリティ要求事項を規定する。

14.1.1.14　提案された製品のセキュリティの機能性が指定された要求を満たさない場合は、発生するリスク及び関連する管理策を、製品を購入する前に再考する。

14.1.1.15　当該システムにおいて稼働するソフトウェア及びサービスと整合する製品のセキュリティ構成に関して、入手可能な手引を用いて、これを評価し、実施する。

14.1.1.16　製品を受け入れる基準は、特定したセキュリティ要求事項を満たすことの確証を与える機能の観点で定める。

14.1.1.17　製品は、入手する前に製品を受け入れる基準に照らして評価する。

14.1.1.18　機能の追加によって、許容できない追加のリスクを取り込まないことを確実にするために、レビューする。

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

14.1.2.1　公衆ネットワークを経由するアプリケーションサービスは、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（例えば、認証）のレベルを定める。

14.1.2.2　公衆ネットワークを経由するアプリケーションサービスは、重要な取引文書の内容の承認、その発行、及びその文書への署名を誰が行うかについての認可プロセスを明確にする。

14.1.2.3　公衆ネットワークを経由するアプリケーションサービスは、サービスの提供又は利用が認可されていることを通信業者に十分に通知していることを確実にする仕組みを整備する。

14.1.2.4　公衆ネットワークを経由するアプリケーションサービスは、入札手続、契約手続などにおいて、重要な文書の機密性、完全性及び発送・受領の証明、並びに契約の否認防止に関する要求事項を決定し、それを達成する。

14.1.2.5　公衆ネットワークを経由するアプリケーションサービスは、重要な文書の完全性についての、信頼のレベルを定める。

14.1.2.6　公衆ネットワークを経由するアプリケーションサービスは、秘密情報の保護に関する要求事項を定める。

14.1.2.7　公衆ネットワークを経由するアプリケーションサービスは、注文のトランザクション、支払い情報、納入先の宛名情報及び受領確認の機密性及び完全性を維持する。

14.1.2.8　公衆ネットワークを経由するアプリケーションサービスは、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を定める。

14.1.2.9　公衆ネットワークを経由するアプリケーションサービスは、不正行為を防ぐための、最も適切な支払いの決済形式を選択する。

14.1.2.10　公衆ネットワークを経由するアプリケーションサービスは、注文情報の機密性及び完全性を維持するために要求される保護のレベルを定める。

14.1.2.11　公衆ネットワークを経由するアプリケーションサービスは、トランザクション情報の紛失又は重複を防止する。

14.1.2.12　公衆ネットワークを経由するアプリケーションサービスは、不正なトランザクションに関する賠償義務を明確にする。

14.1.2.13　公衆ネットワークを経由するアプリケーションサービスは、保険の要件を決定する。

14.1.2.14　アプリケーションサービスに関する当事者間の取決めは、権限の詳細も含め、合意したサービス条件を両当事者に義務付ける合意書によって裏付ける。

14.1.2.15　攻撃に対する対応力（resilience）の要求事項（関連するアプリケーションサーバを保護するための要求事項、及びサービスの提供に必要となるネットワーク相互接続の可用性を確実にするための要求事項を含む。）を定める。

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

・不完全な通信

・誤った通信経路設定

・認可されていないメッセージの変更

・認可されていない開示

・認可されていないメッセージの複製又は再生

14.1.3.1　アプリケーションサービスのトランザクションでは、トランザクションに関わる各当事者による電子署名を利用する。

14.1.3.2　アプリケーションサービスのトランザクションでは、トランザクションの種々の面において、以下を確実にする仕組みを整備する。

1.全ての当事者の秘密認証情報は、有効であり、かつ、検証を経ている。

2.トランザクションが秘密に保たれている。

3.全ての当事者に関係するプライバシーを守っている。

14.1.3.3　アプリケーションサービスのトランザクションでは、関わる全ての当事者間の通信経路を暗号化する。

14.1.3.4　アプリケーションサービスのトランザクションでは、関わる全ての当事者間で使われる通信プロトコルのセキュリティを維持する。

14.1.3.5　アプリケーションサービスのトランザクションでは、その詳細情報を、公開している環境の外（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）で保管すること、及びインターネットから直接アクセス可能な記憶媒体上にそれらを保持して危険にさらさないことを確実にする仕組みを整備する。

14.1.3.6　アプリケーションサービスのトランザクションでは、信頼できる専門機関を利用（例えば、ディジタル署名又はディジタル証明書の発行・維持の目的での利用）する場合、エンドツーエンドの証明書及び／又は署名管理プロセスを通じたセキュリティを統合し、組み込む。

14.2　開発及びサポートプロセスにおけるセキュリティ

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

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

14.2.1.1　セキュリティに配慮した開発のための方針には、開発環境のセキュリティを含める。

14.2.1.2　セキュリティに配慮した開発のための方針には、ソフトウェア開発のライフサイクルにおける、以下の2点の手引きを含める。

1. ソフトウェア開発の方法論におけるセキュリティ
2. 用いる各プログラミング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

14.2.1.3　セキュリティに配慮した開発のための方針には、設計段階におけるセキュリティ要求事項を含める。

14.2.1.4　セキュリティに配慮した開発のための方針には、プロジェクトの開発の節目ごとにおけるセキュリティの確認項目を含める。

14.2.1.5　セキュリティに配慮した開発のための方針には、セキュリティが保たれたリポジトリを含める。

14.2.1.6　セキュリティに配慮した開発のための方針には、版の管理におけるセキュリティを含める。

14.2.1.7　セキュリティに配慮した開発のための方針には、アプリケーションのセキュリティに関して必要な知識を含める。

14.2.1.8　セキュリティに配慮した開発のための方針には、ぜい弱性を回避、発見及び修正するに当たっての開発者の能力を含める。

14.2.1.9　開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合には、新規開発する場合及びコードを再利用する場合の両方に、セキュアプログラミング技術を用いる。

14.2.1.10　セキュリティに配慮したコーディングに関する標準類を確認し、その使用を義務付ける。

14.2.1.11　開発者は、開発に適用する標準類の使用及び試験について訓練を受け、また、コードレビューによって標準類の使用を検証する。

14.2.1.12　開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの保証を得る。

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

14.2.2.1　初期設計段階からその後の全ての保守業務に至るまで、システム、アプリケーション及び製品の完全性を確実にするため、正式な変更管理手順を文書化し、実施する。

14.2.2.2　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、試験、品質管理及び管理された実装からなる正式な手続に従う。

14.2.2.3　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の際の手続には、リスクアセスメント、変更の影響分析及び必要なセキュリティ管理策の仕様化を含める。

14.2.2.4　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の際の手続は、既存のセキュリティ及び管理手順が損なわれないこと、サポートプログラマによるシステムへのアクセスはその作業に必要な部分に限定されること、並びにいかなる変更に対しても正式な合意及び承認が得られていることを確実にする仕組みを整備する。

14.2.2.5　変更管理手順には、実施可能な範囲でアプリケーション及びその運用に関する変更管理手順を統合する。

14.2.2.6　変更管理手順には、合意された認可レベルの記録を維持することを含める。

14.2.2.7　変更管理手順には、変更は、認可されている利用者によって提出されることを確実にすることを含める。

14.2.2.8　変更管理手順には、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするために、管理策及び手順をレビューすることを含める。

14.2.2.9　変更管理手順には、修正を必要とする全てのソフトウェア、情報、データベース及びハードウェアを特定することを含める。

14.2.2.10　変更管理手順には、セキュリティ上の既知の弱点を最少化するために、セキュリティが特に重要とされるコードを特定し、これを点検することを含める。

14.2.2.11　変更管理手順には、作業を開始する前に、提案の詳細について正式な承認を得ることを含める。

14.2.2.12　変更管理手順には、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすることを含める。

14.2.2.13　変更管理手順には、システムに関する一式の文書が各変更の完了時点で更新されること、及び古い文書類は記録・保管されるか又は処分されることを確実にすることを含める。

14.2.2.14　変更管理手順には、全てのソフトウェアの更新について、版数の管理を維持することを含める。

14.2.2.15　変更管理手順には、全ての変更要求の監査証跡を維持・管理することを含める。

14.2.2.16　変更管理手順には、操作手順書などの運用文書類及び利用者手順が、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を含める。

14.2.2.17　変更管理手順には、変更の実施は最も適切な時期に行い、関係する業務処理を妨げないことを確実にすることを含める。

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

14.2.3.1　オペレーティングプラットフォームの変更によって、アプリケーションの機能及び処理の完全性が損なわれていないことを確実にするために、これらに関係する手続きをレビューする。

14.2.3.2　オペレーティングプラットフォームの変更の実施前に適切な試験及びレビューを行っても間に合うように、オペレーティングプラットフォームの変更を通知することを確実にする仕組みを整備する。

14.2.3.3　事業継続計画に対して、適切な変更がなされることを確実にする仕組みを整備する。

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

14.2.4.1　可能な限り、そして実行可能な場合には、業者が供給するパッケージソフトウェアは、変更しないで用いる。

14.2.4.2　パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれるリスクへの対応を行う。

14.2.4.3　パッケージソフトウェアの変更が必要な場合は、業者の同意を取得する。

14.2.4.4　パッケージソフトウェアの変更が必要な場合は、標準的なプログラム更新として、業者から必要とする変更が得られる可能性について確認を行う。

14.2.4.5　パッケージソフトウェアの変更が必要な場合は、変更の結果として、将来のソフトウェアの保守に対して、組織が責任を負うようになるかどうかの確認を行う。

14.2.4.6　パッケージソフトウェアの変更が必要な場合は、用いている他のソフトウェアとの互換性

について確認を行う。

14.2.4.7　パッケージソフトウェアの変更が必要な場合、原本のソフトウェアは保管し、指定された複製に対して変更を適用する。

14.2.4.8　全ての認可されたソフトウェアに対して最新の承認したパッチ及びアプリケーションの更新を導入していることを確実にするために、ソフトウェアの更新管理手続を実施する。

14.2.4.9　将来のソフトウェア更新において、パッケージソフトウェアの変更を再び適用できるように、全ての変更は、十分に試験し、文書化する。

14.2.4.10　パッケージソフトウェアの変更が必要な場合には、変更は、独立した評価機関による試験を受け、正当性を証明する。

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

14.2.5.1　セキュリティに配慮したシステム構築の原則に基づき、情報システムの構築手順を確立し、文書化し、組織の情報システム構築活動に適用する。

14.2.5.2　セキュリティは、情報セキュリティの必要性とアクセス性の必要性との均衡を保ちながら、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。

14.2.5.3　新技術は、セキュリティ上のリスクについて分析し、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。

14.2.5.4　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。

14.2.5.5　セキュリティに配慮したシステム構築の原則及び手順が、新規の潜在的な脅威に対抗するという点で最新であり続けていること、及び適用される技術及びソリューションの進展に適用可能であり続けていることを確実にするために、定期的にレビューする。

14.2.5.6　セキュリティに配慮したシステム構築の原則は、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にも適用する。

14.2.5.7　組織は、供給者の設計のセキュリティに関する原則が、自身の原則と同様に厳密なものであることを確認する。

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

14.2.6.1　セキュリティに配慮した開発環境には、システムの開発及び統合に関連する要員、プロセス及び技術を含める。

14.2.6.2　組織は、個々のシステム開発業務に伴うリスクを評価し、システムによって処理、保管及び伝送されるデータの取扱いに慎重を要する度合いを考慮して、セキュリティに配慮した開発環境を確立する。

14.2.6.3　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、適用される外部及び内部の要求事項（例えば、規制又は方針によるもの）を定める。

14.2.6.4　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、組織によって既に実施されており、システム開発を支えるようなセキ

ュリティ管理策を定める。

14.2.6.5　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、その環境で作業する要員の信頼性を考慮して要員を決定する。

14.2.6.6　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、システム開発に関連した外部委託の程度を考慮して委託先を決定する。

14.2.6.7　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、異なる開発環境の分離の必要性を考慮して環境を構築する。

14.2.6.8　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境へのアクセスの制御を実施する。

14.2.6.9　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境の変更及びそこに保管されたコードに対する変更を監視する。

14.2.6.10　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、セキュリティに配慮した遠隔地でのバックアップを保管する。

14.2.6.11　組織は、個々のシステム開発業務に伴うリスクを評価し、セキュリティに配慮した開発環境を確立するため、開発環境からの、及び開発環境への、データの移動を管理する。

14.2.6.12　特定の開発環境の保護レベルを決定した後、組織は、セキュリティに配慮した開発手順の中の該当するプロセスを文書化し、必要とする全ての要員にこれらを提供する。

14.2.7　組織は、外部委託したシステム開発活動を監督し、監視する。

14.2.7.1　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部委託した内容に関連する使用許諾に関する取決め、コードの所有権及び知的財産権に関わる事項を契約に含める。

14.2.7.2　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティに配慮した設計、コーディング及び試験の実施についての要求事項を契約に含める。

14.2.7.3　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、外部の開発者への、承認済みの脅威モデルの提供を契約に含める。

14.2.7.4　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の質及び正確さに関する受入れ試験を契約に含める。

14.2.7.5　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、セキュリティ及びプライバシーについて、容認可能な最低限のレベルを定めるためにセキュリティしきい（閾）値を用いていることを示す証拠の提出を契約に含める。

14.2.7.6　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、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）が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。

14.2.7.7　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、既知のぜい弱性が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。

14.2.7.8　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、預託契約に関する取決め（例えば、ソースコードが利用できなくなった場合）を契約に含める。

14.2.7.9　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、開発のプロセス及び管理策を監査するための契約上の権利を契約に含める。

14.2.7.10　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の作成に用いたビルド環境の有効な文書化を契約に含める。

14.2.7.11　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、適用される法令の順守及び管理の効率の検証については、組織が責任を負うことを契約に含める。

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

14.2.8.1　組織内でシステムを新規に開発、更新するプロセスにおいては、詳細な活動計画及び一定範囲の条件下での入出力試験の準備を含めた綿密な試験及び検証は、最初に開発チームが実施する。

14.2.8.2　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、組織内で開発するもの及び外部委託したものの両方について、開発チームから独立した受入れ試験を実施する。

14.2.8.3　試験は、そのシステムの重要性及び性質に見合った程度で実施する。

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

14.2.9.1　システムの受入れ試験は、情報セキュリティ要求事項の試験及びセキュリティに配慮したシステム開発の慣行の順守を含める。

14.2.9.2　受け入れた構成部品及び統合されたシステムに対して、試験を実施する。

14.2.9.3　組織は、コード分析ツール又はぜい弱性スキャナのような自動化ツールを利用してセキュリティに関連する欠陥を修正した場合は、この修正を検証する。

14.2.9.4　試験は、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試験が信頼できるものであることを確実にするために、現実に即した試験環境で実施する。

14.3　試験データ

目的：試験に用いるデータの保護を確実にするため。

14.3.1　試験データは、注意深く選定し、保護し、管理する。

14.3.1.1　PII 又はその他の秘密情報を含んだ運用データは、試験目的に用いない。

14.3.1.2　PII 又はその他の秘密情報を試験目的で用いる場合には、取扱いに慎重を要する詳細な記述及び内容の全てを、消去又は改変することによって保護する。

14.3.1.3　運用データを試験目的で用いる場合は、運用アプリケーションシステムに適用されるアクセス制御手順を、試験アプリケーションシステムにも適用する。

14.3.1.4　運用情報を試験環境にコピーする場合は、その都度認可を受ける。

14.3.1.5　運用データを試験目的で用いる場合は、運用情報は、試験が完了した後直ちに試験環境から消去する。

14.3.1.6　運用データを試験目的で用いる場合は、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取得する。

15　供給者関係

15.1　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため。

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

15.1.1.1　組織は、供給者による組織の情報へのアクセスに具体的に対処するため、方針において情報セキュリティ管理策を特定し、義務付ける。

15.1.1.2　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織が、自らの情報へのアクセスを許可する供給者の種類（例えば、IT サービス、物流サービス、金融サービス、IT 基盤の構成要素などの供給者）の特定及び文書化を含める。

15.1.1.3　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者関係を管理するための標準化されたプロセス及びライフサイクルを含める。

15.1.1.4　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理を含める。

15.1.1.5　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるものを含める。

15.1.1.6　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセス及び手順（これには第三者のレビュー及び製品の妥当性確認も含まれる。）を含める。

15.1.1.7　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の完全性を確実にするための、正確さ及び完全さの管理を含める。

15.1.1.8　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織の情報を保護するために供給者に適用する義務の種類を含める。

15.1.1.9　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者によるアクセスに伴うインシデント及び不測の事態への対処（これには、組織及び供給者の責任も含める。）を含める。

15.1.1.10　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の可用性を確実にするための、対応力に関する取決め、並びに必要な場合には、回復及び不測の事態に関する取決めを含める。

15.1.1.11　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、調達に関与する組織の要員を対象とした、適用される方針、プロセス及び手順についての意識向上訓練を含める。

15.1.1.12　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者の要員とやり取りする組織の要員を対象とした、関与及び行動に関する適切な規則（これは、供給者の種類、並びに組織のシステム及び情報への供給者によるアクセスのレベルに基づく。）についての意識向上訓練を含める。

15.1.1.13　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報セキュリティに関する要求事項及び管理策を、両当事者が署名する合意書の中に記載

する条件を含める。

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

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

15.1.2.1　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誤解が生じない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。

15.1.2.2　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、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を含める。

15.1.2.3　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の分類体系に従った情報の分類（必要な場合、組織の分類体系と供給者の分類体系との間の対応付け）を含める。

15.1.2.4　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、法的及び規制の要求事項（データ保護、知的財産権及び著作権に関する要求事項を含む。）、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を含める。

15.1.2.5　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、契約の各当事者に対する、合意した一連の管理策（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。）の実施の義務を含める。

15.1.2.6　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報の許容可能な利用に関する規則（必要な場合、許容できない利用についての規則も）を含める。

15.1.2.7　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織の情報にアクセスする若しくは組織の情報を受領することが認可されている供給者の要員の明確なリスト、又は供給者の要員による組織の情報へのアクセス若しくはその受領を認可する場合及びその認可を解除する場合の手順・条件を含める。

15.1.2.8　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、それぞれの契約に関連する情報セキュリティのための方針群を含める。

15.1.2.9　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、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）を含める。

15.1.2.10　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、インシデント対応手順、認可手順などの、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を含める。

15.1.2.11　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、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制を含める。

15.1.2.12　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、情報セキュリティに関する連絡先担当者も含む、合意における相手方の担当者を含める。

15.1.2.13　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、必要に応じて、供給者の要員の選考に関する要求事項を含める（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を実施する責任も含める。）。

15.1.2.14　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、供給者が実施する、合意に関わるプロセス及び管理策を監査する権利を含める。

15.1.2.15　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、合意上の問題点の解決及び紛争解決のプロセスを含める。

15.1.2.16　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、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管理策及び合意の有効性について、独立した報告書を定期的に提出する供給者の義務を含める。

15.1.2.17　特定された情報セキュリティ要求事項を満たすために、供給者との合意には、組織のセキュリティ要求事項を順守するという供給者の義務を含める。

15.1.3　供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.1.3.1　供給者との合意には、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のほかに、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ことを含める。

15.1.3.2　供給者との合意には、ICT サービスに関して、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供給者に要求することを含める。

15.1.3.3　供給者との合意には、ICT 製品に関して、その製品に他の供給者から購入した構成部品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供給者に要求することを含める。

15.1.3.4　供給者との合意には、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とを含める。

15.1.3.5　特に、直接の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（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に対しては、組織の外で作られる場合に注意及び精査の強化が求められるため）、供給者との合意には、重要な構成要素を特定するためのプロセスを実施することを含める。

15.1.3.6　供給者との合意には、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ことを含める。

15.1.3.7　供給者との合意には、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ことを含める。

15.1.3.8　供給者との合意には、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ことを含める。

15.1.3.9　供給者との合意には、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とを含める。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める。

15.2 供給者のサービス提供の管理

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

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

15.2.1.1 供給者のサービスを監視及びレビューすることによって、その合意における情報セキュリティの条件の順守、並びに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を確実にする仕組みを整備する。

15.2.1.2 供給者のサービスの監視及びレビューは、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ことを含める。

15.2.1.3 供給者のサービスの監視及びレビューは、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ことを含める。

15.2.1.4 供給者のサービスの監視及びレビューは、独立した監査人の報告書が入手できれば、供給者の作成したサービスの報告のレビューと併せて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ことを含める。

15.2.1.5 供給者のサービスの監視及びレビューは、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ことを含める。

15.2.1.6 供給者のサービスの監視及びレビューは、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中断記録をレビューすることを含める。

15.2.1.7 供給者のサービスの監視及びレビューは、特定された問題の解決及び管理を実施することを含める。

15.2.1.8 供給者のサービスの監視及びレビューは、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ことを含める。

15.2.1.9 供給者のサービスの監視及びレビューは、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とともに、供給者が十分なサービス提供能力を維持することを確実にすることを含める。

15.2.1.10 供給者関係を管理する責任は、指定された個人又はサービス管理チームに割り当てる。

15.2.1.11 組織は、供給者が、順守状況のレビュー及び合意書における要求事項の実施についての責任を割り当てる。

15.2.1.12 組織は、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する。

15.2.1.13 組織は、サービスの提供において不完全な点があった場合に適切な処置をとる。

15.2.1.14 組織は、供給者がアクセス、処理又は管理する、取扱いに慎重を要する又は重要な情報・情報処理設備に対して、全てのセキュリティの側面についての十分かつ包括的な管理及び可視性を維持する。

15.2.1.15 組織は、報告プロセスを規定することで、セキュリティに関連した活動（例えば、変更管理、ぜい弱性識別、情報セキュリティインシデントの報告及び対応）の可視性を維持する。

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

15.2.2.1　供給者のサービス提供の変更に対する管理は、供給者との合意に対する変更を考慮して実施する。

15.2.2.2　供給者のサービス提供の変更に対する管理は、以下の4点を実施するために組織が行う変更を考慮して実施する。

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

15.2.2.3　供給者のサービス提供の変更に対する管理は、以下の7点を実施するための供給者サービスにおける変更を考慮して実施する。

1. ネットワークに対する変更及び強化
2. 新技術の利用
3. 新製品又は新しい版・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. 供給者の変更
7. 他の供給者への下請負契約

16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

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

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

16.1.1.1　情報セキュリティインシデント管理に関する管理層の責任及び手順について、組織において、以下の6点の手順が策定され、十分に伝達されることを確実にするために、管理層の責任を確立する。

1. インシデント対応の計画及び準備のための手順
2. 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を監視、検知、分析及び報告するための手順
3. インシデント管理活動のログを取得するための手順
4. 法的証拠を扱うための手順
5. 情報セキュリティ事象の評価及び決定のための手順、並びに情報セキュリティ弱点の評価のための手順
6. 対応手順（段階的取扱い、インシデントからの回復の管理、並びに内部及び外部の要員又は組織への伝達のための手順を含む。）

16.1.1.2　情報セキュリティインシデント管理に関する管理層の責任及び手順について、確立する手

順においては、以下の3点を確実にする。

1. 組織内の情報セキュリティインシデントに関連する事項は、力量のある要員が取り扱う。
2. セキュリティインシデントを検知及び報告する場合の連絡先を定める。
3. 情報セキュリティインシデントに関連した事項を取り扱う関係当局、外部の利益団体又は会議との適切な連絡を保つ。

16.1.1.3　情報セキュリティインシデント管理に関する管理層の責任及び手順について、報告手順においては、以下の4点を含める。

1. 情報セキュリティ事象が発生した場合に、報告作業を助け、報告する者が必要な全ての処置を忘れないよう手助けするための情報セキュリティ事象の報告書式の作成
2. 情報セキュリティ事象が発生した場合にとる手順。例えば、詳細全て（不順守又は違反の形態、生じた誤動作、画面上の表示など）の記録を直ちにとる、直ちに連絡先に報告し、協調した処置だけをとる。
3. セキュリティ違反を犯した従業員を処罰するために確立された正式な懲戒手続への言及
4. 情報セキュリティ事象の報告者に、その件の処理が終結した後で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

16.1.1.4　情報セキュリティインシデント管理の目的について、経営陣の同意を得る。

16.1.1.5　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に対し、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確実に理解させる。

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

16.1.2.1　全ての従業員及び契約相手に、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る。

16.1.2.2　全ての従業員及び契約相手に、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。

16.1.2.3　情報セキュリティ事象の報告には、効果のないセキュリティ管理策を含める。

16.1.2.4　情報セキュリティ事象の報告には、情報の完全性、機密性又は可用性に関する期待に対する違反を含める。

16.1.2.5　情報セキュリティ事象の報告には、人による誤りを含める。

16.1.2.6　情報セキュリティ事象の報告には、個別方針又は指針の不順守を含める。

16.1.2.7　情報セキュリティ事象の報告には、物理的セキュリティの取決めに対する違反を含める。

16.1.2.8　情報セキュリティ事象の報告には、管理されていないシステム変更を含める。

16.1.2.9　情報セキュリティ事象の報告には、ソフトウェア又はハードウェアの誤動作を含める。

16.1.2.10　情報セキュリティ事象の報告には、アクセス違反を含める。

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

16.1.3.1　全ての従業員及び契約相手は、情報セキュリティインシデントを防止するため、情報セキュリティ弱点をできるだけ速やかに連絡先に報告する。

16.1.3.2　情報セキュリティ弱点の報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるようにする。

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

16.1.4.1　連絡先の者は、合意された情報セキュリティ事象・情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価し、その事象を情報セキュリティインシデントに分類する[31]か否かを決定する。

16.1.4.2　評価及び決定の結果[32]は、以後の参照及び検証のために詳細に記録する。

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

16.1.5.1　情報セキュリティインシデントには、指定された連絡先、及び組織又は外部関係者の他の関係する要員が対応する。

16.1.5.2　対応策には、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を収集することを含める。

16.1.5.3　対応策には、必要に応じて、情報セキュリティの法的分析を実施することを含める。

16.1.5.4　対応策には、必要に応じて、段階的取扱い（escalation）を行うことを含める。

16.1.5.5　対応策には、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ことを含める。

16.1.5.6　対応策には、知る必要性を認められている内部・外部の他の要員又は組織に対し、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ことを含める。

16.1.5.7　対応策には、インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処することを含める。

16.1.5.8　対応策には、インシデントへの対応が滞りなく済んだ後、正式にそれを終了し、記録することを含める。

16.1.5.9　インシデントの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。

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

16.1.6.1　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及び監視できるようにする仕組みを備える。

16.1.6.2　情報セキュリティインシデントの評価から得た情報は、再発する又は影響の大きいインシデントを特定するために利用する。

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

16.1.7.1　懲戒処置及び法的処置のために証拠を取り扱う場合は、内部の手順を定め、それに従う。

16.1.7.2　懲戒処置及び法的処置のために証拠を取り扱う手順では、各種の媒体、装置及び装置の状態（例えば、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、取得及び保存のプロセスを規定する。

16.1.7.3　懲戒処置及び法的処置のために証拠を取り扱う手順では、管理状況の一連の履歴を取得するプロセスを規定する。

16.1.7.4　懲戒処置及び法的処置のために証拠を取り扱う手順では、証拠の保全を行うプロセスを規定する。

---

[31] インシデントの分類及び優先順位付けは、インシデントの影響及び程度の特定に役立てることができる。

[32] 組織内に情報セキュリティインシデント対応チームがある場合は、確認又は再評価のために、評価及び決定の結果をこの対応チームに転送してもよい。

16.1.7.5　懲戒処置及び法的処置のために証拠を取り扱う手順では、要員の安全を確保するプロセスを規定する。

16.1.7.6　懲戒処置及び法的処置のために証拠を取り扱う手順では、関与する要員の役割及び責任を定める。

16.1.7.7　懲戒処置及び法的処置のために証拠を取り扱う手順では、要員の力量を定める。

16.1.7.8　懲戒処置及び法的処置のために証拠を取り扱う手順では、文書化することを定める。

16.1.7.9　懲戒処置及び法的処置のために証拠を取り扱う手順では、要点説明を行うことを定める。

16.1.7.10　保存された証拠の価値を強化するために、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及する。

16.1.7.11　懲戒処置及び法的処置に必要な法的証拠が、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法的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。

16.1.7.12　懲戒処置及び法的処置に関連する幾つかの法域にまたがる証拠の利用の可能性を最大にするために、それらの異なる法域の要求事項を確認する。

17　事業継続マネジメントにおける情報セキュリティの側面

17.1　情報セキュリティ継続

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

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

17.1.1.1　組織は、情報セキュリティの継続が事業継続マネジメント（以下「BCM」という。）プロセス又は災害復旧管理（以下「DRM」という。）プロセスに織り込まれているか否かを判断する。

17.1.1.2　組織は、事業継続及び災害復旧に関する計画を立てる場合に、情報セキュリティ要求事項を定める。

17.1.1.3　事業継続及び災害復旧に関する正式な計画が策定されていない場合に、通常の業務状況とは異なる困難な状況においても、情報セキュリティ要求事項は変わらず存続するよう定める。

17.1.1.4　事業継続及び災害復旧に関する正式な計画が策定されていない場合において、情報セキュリティ要求事項が変わらず存続すると定められない場合には、情報セキュリティの側面について事業影響度分析を実施し、通常の業務状況とは異なる困難な状況に適用できる情報セキュリティ要求事項を定める。

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

17.1.2.1　組織は、必要な権限、経験及び力量を備えた要員を用い、中断・阻害を引き起こす事象に備え、これを軽減し、これに対処するための十分な管理構造を確実に設ける。

17.1.2.2　組織は、インシデントを管理し、情報セキュリティを維持するための責任、権限及び力量を備えたインシデント対応要員を確実に任命する。

17.1.2.3　組織は、経営陣が承認した情報セキュリティ継続の目的に基づいて、組織が中断・阻害を引き起こす事象を管理し、その情報セキュリティを既定のレベルに維持する場合の方法を計画及び手順に詳細に記して、計画、対応及び回復の文書化した手順を確実に策定し、これらを承認する。

17.1.2.4　組織は、情報セキュリティ継続に関する要求事項に従って、事業継続又は災害復旧のためのプロセス及び手順、並びにこれらを支援するシステム及びツールにおける情報セキュリティ管理策を確立し、文書化し、実施し、維持する。

17.1.2.5　組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において既存の情報セキュリティ管理策を維持するための、プロセス及び手順の変更並びにそれらの実施の変更を確立し、文書化し、実施し、維持する。

17.1.2.6　組織は、情報セキュリティ継続に関する要求事項に従って、困難な状況において維持することが不可能な情報セキュリティ管理策を補うための管理策を確立し、文書化し、実施し、維持する。

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

17.1.3.1　運用に関するものか、継続に関するものかを問わず、組織、技術、手順及びプロセスの変更が、情報セキュリティ継続に関する要求事項の変更につながる場合、変更後の要求事項に照らして、情報セキュリティのためのプロセス、手順及び管理策の継続性をレビューする。

17.1.3.2　組織は、情報セキュリティ継続のためのプロセス、手順及び管理策の機能が情報セキュリティ継続の目的と整合していることを確実にするために、これらの機能を実行し、試験する。

17.1.3.3　組織は、情報セキュリティ継続のためのプロセス、手順及び管理策を機能させる知識及びルーチンを実行及び試験し、そのパフォーマンスが情報セキュリティ継続の目的に整合していることを確実にする仕組みを整備する。

17.1.3.4　組織は、情報システム、情報セキュリティのプロセス、手順及び管理策、又はBCM・DRMのプロセス及びソリューションが変更された場合には、情報セキュリティ継続のための手段の妥当性及び有効性をレビューする。

17.2　冗長性

目的：情報処理施設の可用性を確実にするため。

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

17.2.1.1　組織は、情報システムの可用性に関する業務上の要求事項を特定する。

17.2.1.2　組織は、既存のシステムアーキテクチャを利用しても可用性を保証できない場合には、冗長な構成要素又はアーキテクチャを構築する。

17.2.1.3　組織は、一つの構成要素から別の構成要素への切替え（failover）による冗長の場合、それ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。

18　順守

18.1　法的及び契約上の要求事項の順守

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

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

18.1.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項を満

たすための具体的な管理策及び具体的な責任について定め、文書化する。

18.1.1.2　管理者は、事業の種類に関連した要求事項を満たすために、各自の組織に適用される全ての法令を特定する。

18.1.1.3　組織が他の国で事業を営む場合には、管理者は、関連する全ての国における法令、規制及び契約上の要求事項を順守する。

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

18.1.2.1　ソフトウェア製品及び情報製品の合法利用を明確に定めた知的財産権順守方針を公表する。

18.1.2.2　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。

18.1.2.3　知的財産権を保護するための方針に対する認識を持続させ、それらの方針に違反した要員に対して懲罰処置をとる意思を通知する。

18.1.2.4　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。

18.1.2.5　使用許諾を得ていることの証明及び証拠、マスタディスク、手引などを維持・管理する。

18.1.2.6　使用許諾で許可された最大利用者数を超過しないことを確実にするための管理策を実施する。

18.1.2.7　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のレビューを行う。

18.1.2.8　適切な使用許諾条件を維持・管理するための方針を定める。

18.1.2.9　ソフトウェアの処分又は他人への譲渡についての方針を定める。

18.1.2.10　公衆ネットワークから入手するソフトウェア及び情報の使用条件に従う。

18.1.2.11　著作権法が認めている場合を除いて、商用記録（フィルム、録音）を複製、他形式に変換、又は抜粋しない。

18.1.2.12　著作権法が認めている場合を除いて、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。

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

18.1.3.1　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分類を考慮して決定する。

18.1.3.2　記録類は、記録の種類（例えば、会計記録、データベース記録、トランザクションログ、監査ログ、運用手順）によって、また、更にそれぞれの種類での保持期間及び許容される記憶媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光媒体）の詳細によって分類する。

18.1.3.3　保存した記録の暗号化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は、その記録類を保存している期間中に記録の復号が可能なように、保管する。

18.1.3.4　記録の保存に用いる媒体が劣化する可能性を考慮して記録の保存及び取扱いの手順を定める。

18.1.3.5　記録の保存及び取扱いの手順は、媒体の製造業者の推奨の仕様に従って実施する。

18.1.3.6　電子的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、保持期間を通じてデータにアクセスできること（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。

18.1.3.7　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、要求されたデータ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。

18.1.3.8　データ保存及びデータ処理システムは、記録を確実に特定し、国又は地域の法令又は規制が適用される場合に定められている記録の保持期間を確実に特定する。

18.1.3.9　保持期間が終了した後、組織にとって必要ない場合には、データ保存及びデータ処理システムは、記録を適切に破棄できるようにする。

18.1.3.10　記録保護の目的を満たすため、組織内では、記録及び情報の保持、保存、取扱い及び処分に関する指針を発行する。

18.1.3.11　記録保護の目的を満たすため、組織内では、記録及びそれらの記録の保持期間を明確にした保持計画を作成する。

18.1.3.12　記録保護の目的を満たすため、組織内では、主要な情報の出典一覧を維持・管理する。

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

18.1.4.1　プライバシー及びPIIの保護に関する組織の方針を確立して実施する。

18.1.4.2　プライバシー及びPIIの保護に関する組織の方針は、PIIの処理に関与する全ての者に伝達する。

18.1.4.3　プライバシー及びPIIの保護に関する組織の方針の順守、並びに人々のプライバシーの保護及びPIIの保護に関する全ての法令及び規制の順守のために、適切な管理構造及び管理策を確立する。

18.1.4.4　プライバシー及びPIIの保護の責任者（例えば、プライバシー担当役員）は、管理者、利用者及びサービス提供者に対して、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。

18.1.4.5　PII の取扱い、及びプライバシーの原則の認識を確実にすることについての責任は、関連する法令及び規制に従って処置する。

18.1.4.6　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。

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

18.1.5.1　関連する協定、法令及び規制を順守するため、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を順守する。

18.1.5.2　関連する協定、法令及び規制を順守するため、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を順守する。

18.1.5.3　関連する協定、法令及び規制を順守するため、暗号利用に関する規制を順守する。

18.1.5.4　関連する協定、法令及び規制を順守するため、内容の機密性を守るためにハードウェア又はソフトウェアによって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を定める。

18.1.5.5　関連する法令及び規制の順守を確実にするために、法的な助言を求める。

18.1.5.6　暗号化された情報又は暗号制御機能を、法域を越えて持ち出す前に、法的な助言を受ける。

18.2　情報セキュリティのレビュー

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

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

18.2.1.1　経営陣は、情報セキュリティをマネジメントする組織の取組みが、引き続き適切、妥当及び有効であることを確実にするために、独立したレビューを発議し、実施させる。

18.2.1.2　独立したレビューには、改善の機会のアセスメントを含める。

18.2.1.3　独立したレビューには、方針及び管理目的を含むセキュリティの取組みの変更について、その必要性の評価を含める。

18.2.1.4　独立したレビューは、レビューが行われる領域から独立した個人・組織（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）が実施する。

18.2.1.5　独立したレビューは、適切な技能及び経験をもつ個人・組織が実施する。

18.2.1.6　独立したレビューの結果は、記録し、レビューを発議した経営陣に報告する。

18.2.1.7　独立したレビューの結果の記録は、維持する。

18.2.1.8　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み及び実施が十分でない（例えば、文書化した目的及び要求事項が、情報セキュリティのための方針群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、又はこれと適合していない）ことが明確になった場合には、経営陣は是正処置の検討を指示する。

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

18.2.2.1　管理者は、方針、標準類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ための方法を特定する。

18.2.2.2　管理者は定めに従って効率的に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を使用する。

18.2.2.3　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、不順守の原因を特定する。

18.2.2.4　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、順守を達成するための処置の必要性を評価する。

18.2.2.5　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、適切な是正処置を実施する。

18.2.2.6　管理者によるレビューの結果、何らかの是正処置を実施した場合、管理者は、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、とった是正処置をレビューする。

18.2.2.7　管理者が実施したレビュー及び是正処置の結果を記録する、また、その記録を維持・管理する。

18.2.2.8　管理者の責任範囲に対して、独立したレビュー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、レビュー及び是正処置の結果を報告する。

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

18.2.3.1　技術的順守は、技術専門家が後に解釈するための技術レポートを生成する自動ツールを活

用してレビューする。

18.2.3.2　技術的順守は、自動ツールの活用に代わるものとして、経験をもつシステムエンジニアが手動で（必要な場合には、適切なソフトウェアツールの助けを得て）レビューする。

18.2.3.3　侵入テスト又はぜい弱性アセスメントを用いる場合、このような作業は、システムのセキュリティを危うくするかもしれないことに注意する。

18.2.3.4　侵入テスト又はぜい弱性アセスメントは、計画し、文書化し、また、繰り返し実施する。

18.2.3.5　いかなる技術的順守のレビューも、力量があり、認可されている者によって、又はその者の監督の下でだけ、実施する。