情報セキュリティ管理基準

（平成２０年改正版）

Ⅰ．主旨

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

このような状況を踏まえ、経済産業省では、平成15年に、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール（管理策）を整備・運用するための実践的な規範として、「情報セキュリティ管理基準」（平成15年経済産業省告示第112号）を策定した。「情報セキュリティ管理基準」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。

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、「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策定した。「情報セキュリティ管理基準（平成20年改正版）」は、組織体における情報セキュリティマネジメントの円滑で効果的な確立を目指して、マネジメントサイクル構築の出発点から具体的な管理策に至るまで、包括的な適用範囲を有する基準となっている。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のっとって、本管理基準の項目等を取捨選択、追加することにより、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、「情報セキュリティ管理基準（平成20年改正版）」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と整合するように配慮している。

---

*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。

Ⅱ．構成

情報セキュリティ管理基準（平成20年改正版）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 27001:2006を基にして策定しているが、抽出に当たっては次の２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」の内容は以下のとおりである。

1 情報セキュリティマネジメントの確立
- 1.1 適用範囲の定義
- 1.2 基本方針の策定
- 1.3 リスクアセスメント
- 1.4 管理策の選択

2 情報セキュリティマネジメントの導入と運用
- 2.1 リスク対応計画
- 2.2 管理策の実施
- 2.3 情報セキュリティマネジメントの運用管理
- 2.4 教育、訓練、意識向上および力量

3 情報セキュリティマネジメントの監視およびレビュー
- 3.1 有効性の継続的改善
- 3.2 監視及びレビューの準備
- 3.3 管理策の有効性評価
- 3.4 情報セキュリティマネジメントの継続性評価

4 情報セキュリティマネジメントの維持および改善
- 4.1 改善策の導入
- 4.2 是正処置
- 4.3 予防処置

5 文書管理および記録の管理
- 5.1 文書化
- 5.2 文書管理
- 5.3 記録の管理

「管理策基準」は、組織に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 27001:2006附属書Ａ「管理目的及び管理策」、JIS Q 27002:2006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。

1 セキュリティ基本方針

Ⅲ．マネジメント基準

1 情報セキュリティマネジメントの確立

情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を定義し、基本方針を策定する。これらをもとに、リスクアセスメントを実施し、管理目的、管理策の選択を実施する。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。

1.1 適用範囲の定義

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。

1.1.1 情報セキュリティマネジメントの適用範囲及び境界を定義する

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

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。

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、社会的な要求（法令、業界の慣習、顧客満足など）、内部的な要求（事業継続、内部統制）の双方があり、これらを考慮して適用範囲を定義する。

1.2 基本方針の策定

1.2.1 情報セキュリティ基本方針を策定する

情報セキュリティ基本方針の策定においては、適用範囲の定義と同様に以下の点について考慮する。

・自らの事業
・体制
・所在地
・資産
・技術の特徴

また、文書化の際には以下の項目が定義されているかどうかを確認する。

・目的を設定するための枠組

・情報セキュリティに関係する活動の方向性
・事業における要求事項
・法令または規制による要求事項
・契約上のセキュリティ義務
・情報セキュリティマネジメントの確立及び維持体制（役割及び責任を含む）
・リスクアセスメントの方針（基準や取り組み方など）

基本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されなければならない。

1.2.2 経営陣は情報セキュリティ基本方針にコミットする

経営陣が情報セキュリティ基本方針にコミットした証拠を以下の記録などをもって示す。
・文書化された情報セキュリティ基本方針への署名
・情報セキュリティ基本方針が議論された会議の議事録

これらは経営陣の責任を明確にするために実施する。コミットした情報セキュリティ基本方針は組織に伝えられるように文書化され、しかるべき方法で通達する。

1.3 リスクアセスメント

1.3.1 リスクアセスメントに対する組織の取り組み方を定義する

リスクアセスメントの実施に当たって以下の内容について議論し、定義する。
・リスクアセスメントを実施するための体制（責任、役割）
・リスクアセスメントの実施計画
・リスクアセスメントの手法（リスク受容基準を含む）
・リスク受容可能レベル

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。リスクアセスメント手法は以下の条件を満たすようなものを選択する。

ここで設定するリスク受容可能レベルはリスクアセスメント作業全般における判断基準として利用され、その結果を反映し、情報セキュリティマネジメント全般におけるリスク受容基準及びリスク受容可能レベルを経営陣の承認のもとに決定する。（1.3.4参照）
・リスクアセスメントの結果が比較可能である
・リスクアセスメントの結果が再現可能である

必要に応じてツールを利用するなどが必要になる。

1.3.2 リスクを特定する

情報セキュリティマネジメントの範囲内におけるリスクを特定するには、それぞれの情報資産において以下の点について考慮する。
・情報資産の管理責任者
・情報資産に対する脅威
・脅威に対応したぜい弱性
・機密性、完全性、可用性が損なわれた場合の影響

情報資産一覧を作成しているのであれば、これらの項目を追加し、リスクを特定するためのチェックリストとしてもよい。特定した範囲内のすべての情報資産についてリスクを特定するためには、保管されている情報資産だけではなく、一時的に作成された情報など

を考慮する必要がある。

1.3.3 リスクを分析し、評価する

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

リスクを特定するためのチェックリストに以下の項目を加え、評価方法を定型化するとよい。

・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

リスク評価の結果は今後の改善に利用するため保管しておく。

1.3.4 経営陣はリスク受容基準及びリスクの受容可能レベルを決定する

リスクを明確にするために、リスク受容基準を決定する。リスク受容基準はリスクを測るための基準であり、リスクアセスメント手法をより効果的にするために以下の点について考慮する。

・リスクアセスメントの結果が比較可能である

・リスクアセスメントの結果が再現可能である

また、リスク受容基準にしたがって、どのレベルのリスクまでを受け入れるのかを明確にするために、リスクの受容可能レベルを決定する。

決定したリスク受容基準及びリスクの受容可能レベルについては、経営陣の責任を明確にするための証拠として、以下を残す。

・リスク受容基準及びリスク受容可能レベルが承認された会議の議事録

1.4 管理策の選択

リスクアセスメントの結果に応じて適切な管理策を選択する。管理策の選択には「管理策基準」を活用する。

1.4.1 リスク対応のための選択肢を特定し、評価する

リスク対応には以下の選択肢があり、対応が必要だとされたすべてのものについていずれかの措置を採る。

・適切な管理策の適用

・方針またはリスクの受容可能レベルに応じた、リスクの受容

・リスクの回避（資産の廃棄もしくは業務の停止など）

・リスクの移転

どの選択肢を選んだ場合も、その理由を明確にし、記載しておく。これによってリスク対応の評価や改善に役立つことになる。

1.4.2 リスク対応のための管理目的及び管理策を選択する

リスク対応のための方針が決まったら、管理策の目的（管理目的）及び管理策について検討する。検討の際には以下について考慮する。

・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

具体的な管理策の選択においては、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。ただし、「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。

対策の選択においては、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ようにするのが望ましい。

1.4.3 残留リスクについて経営陣の承認を得る

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

経営陣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。

1.4.4 情報セキュリティマネジメントを導入し運用することについて経営陣の許可を得る

残留リスクについて承認を得たうえで、情報セキュリティマネジメントを導入し運用することについて、経営陣の許可を得る。

経営陣は許可を行うことによって責任を負うことになるため、その責任を全うするためにもマネジメントレビューを実施し、情報セキュリティマネジメントが適切に実施されているかどうかを判断するための情報収集を行う。

2 情報セキュリティマネジメントの導入と運用

組織が特定したリスクに対応するための管理を実施する。管理策が目的に沿って、期待通りに実施されるための運用基盤を策定し、見直しを行うことでより効果的な対応を可能とする。組織全体が情報セキュリティマネジメントに協力する体制として教育・訓練、意識向上プログラムなども実施する。

2.1 リスク対応計画

2.1.1 リスク対応計画を策定する

リスク対応計画の策定では、情報セキュリティリスクの運営管理のために、以下の内容について特定し、文書化する。

・経営陣の適切な活動

・経営資源

・責任体制

・優先順位

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経営陣が行っていることがほとんどであり、責任が経営陣に集中している。これは経営陣が責任を放棄してしまえば、情報セキュリティについての取り組みは行わないとするのと同義であり、経営陣がどのように行動し、どのような責任を持つかについて明確にする必要がある。

2.1.2 リスク対応計画を実施する

特定した管理目的を達成するためにリスク対応計画を実施する。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ておく必要がある。

2.1.3 経営陣はリスク対応計画の実施のために十分な経営資源を提供する

リスク対応計画には相応の経営資源が必要になる。以下の点について考慮する。

・管理策の導入にかかる費用、人員、作業工数、技術
・管理策の運用にかかる費用、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、予算化しておくことが重要になる。また、セキュリティインシデントが発生した場合の一時対応についても検討し、予算化する。

2.2 管理策の実施

2.2.1 管理目的を満たすために管理策を実施する

管理策はその管理目的を満たすために、以下の点を考慮して実施する。

・管理目的を決定した際のリスク
・その他の管理策との関係

管理策の関連性については、管理策の実施だけではなく改善においても考慮する。

2.2.2 選択した管理策または一連の管理策の有効性をどのように評価するか、また評価の結果をどのように活用するかを定義する

管理目的を満たしているかどうかを評価するためにも、管理策の有効性について測定をする。具体的な測定方法については管理目的の種類によって異なるが、以下の点を考慮する。

・結果の比較ができること
・繰り返し測定できる方法であること

評価の結果、有効性が損なわれたと判断した場合の対応についてもあらかじめ決めておくことで、迅速な対応が可能になる。

2.3 情報セキュリティマネジメントの運用管理

2.3.1 情報セキュリティマネジメントの運用を管理する

情報セキュリティマネジメントの運用を管理するために、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。

2.3.2 情報セキュリティマネジメントのための経営資源を管理する

管理目的を満たすためには、継続的に管理策を実施していかなければならない。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は、適切な時期に適切に提供できるように、経営資源を確保する。

2.3.3 迅速にセキュリティイベントを検知でき、セキュリティインシデントに対応できるための手順及びそのための管理策を実施する

セキュリティイベントの連鎖によって重大なセキュリティインシデントが発生しないために、以下の項目についてあらかじめ検討し、定義しておく。

・セキュリティイベント及びセキュリティインシデントの定義
・セキュリティインシデントの特定

・セキュリティイベントを発見した際の情報伝達
・セキュリティインシデントを特定した場合の情報伝達
・セキュリティインシデントの影響度及び重大さに応じた対応手順

システムを利用して検知できないイベントについては、従業者を十分に教育するなどして、異常を速やかに検知できるような体制を構築する。

2.4 教育、訓練、意識向上及び力量

2.4.1 経営陣は情報セキュリティ基本方針に適合することの重要性を組織に伝える

経営陣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、情報セキュリティ基本方針と共に伝える必要がある。情報セキュリティ基本方針に適合することと同様に以下の点についても伝える。

・情報セキュリティの適用範囲
・情報セキュリティの目的
・情報セキュリティにおける法の下での責任
・情報セキュリティの継続的改善の必要性

また、組織が同じ規定に従って同じ判断ができるように基準を策定しておく必要がある。これには情報分類などが挙げられる。個人情報のように組織によって一部解釈が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、伝える必要がある。

2.4.2 情報セキュリティマネジメントに影響がある業務に従事する要員に必要な力量を決定する

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見直しが必要になる。

2.4.3 必要な力量が持てるように教育・訓練するか、的確な要員の雇用など他の処置をとる

情報セキュリティにかかわる業務に携わるために必要な力量がない場合、教育または訓練を実施する。必要な知識を得るためには教育を、必要なスキル及び経験を得るためには訓練を実施する。

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、確認テストなどを実施する。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。

教育や訓練が間に合わないと判断される場合は相応の力量を有した要員を雇用したり、社内業務との関連が少ない業務においては外部委託を検討する。

2.4.4 教育・訓練、意識向上に関して有効性を評価する

教育、訓練、意識向上が正しく行われているかについて、判断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

テスト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心掛ける。

2.4.5 教育、訓練、技能、経験及び資格についての記録を維持する

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

・確認テストまたは評価報告

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、一覧とする。資格については有効期限などを明確にし、更新することも重要である。

2.4.6 関連する要員すべてが、情報セキュリティについての活動が持つ意味と重要性とを認識する

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、情報セキュリティ基本方針の通達や教育の一環として周知徹底する必要がある。管理策がなぜ実施されているのかについての理解を深めることによって、それぞれの担当する情報セキュリティに直接関係のない業務においても、意識を持って取り組むことができる。

2.4.7 関連する要員すべてが、情報セキュリティマネジメントの目的の達成に向けて自分はどのように貢献できるかを認識する

情報セキュリティマネジメントはトップダウンで行われることが多いが、実際にそれらを実行するのは組織内のすべての従業者となる。従業者すべてが役割を理解することで、円滑な情報セキュリティマネジメントを導入・運用することができる。

役割が明確になるように以下の点について従業者に伝える。

・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

・これらが記載された文書の所在

また、セキュリティイベントやセキュリティインシデントに迅速に対応するためにすべての従業者には、異常を検知した場合の報告手順について徹底しておくことも重要である。

3 情報セキュリティマネジメントの監視及びレビュー

情報セキュリティマネジメントは環境の変化などに対応して見直されなければならない。管理策の有効性、情報セキュリティマネジメントの継続性などを測るために、監視、監査、レビューなどを実施する。

3.1 有効性の継続的改善

3.1.1 情報セキュリティマネジメントの有効性を継続的に改善する

情報セキュリティマネジメントの有効性を継続的に改善するために、以下の活動を実施する。

・定期的なリスクアセスメント

・定期的な監視

・情報セキュリティ監査

・マネジメントレビュー

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

3.2 監視及びレビューの準備

3.2.1 監視及びレビューの手続きやその他の管理策を実施する

管理策にはシステムで実施しているものと人力にゆだねているものがある。どちらも正しく管理策が実施されているかどうかを調査するために情報を収集する。これらの収集した情報を基に経営陣は管理策の効果が期待通りかどうかを判断する。収集した情報を比較、再現ができるように取得するために以下を検討し、文書化する。

・通常の処理の誤りを検知する方法

・セキュリティ違反及びセキュリティインシデントの迅速な特定方法

・経営陣が判断するための情報収集方法及び期待値

・セキュリティインシデント対応の妥当性の確認方法

また、セキュリティインシデントの防止のために、セキュリティイベントとセキュリティインシデントの関連についても検討し、文書化されているとよい。

3.2.2 経営陣は情報セキュリティマネジメントの内部監査の実施を確実にする

情報セキュリティマネジメントの有効性や準拠性を評価するために内部監査を実施する。内部監査の実施を確実にするために経営陣は以下の点について考慮し、経営資源を提供する。

・内部監査基本計画

・内部監査を実施するための経営資源

・内部監査によって検出されるだろう不適合を処置するための予算

内部監査は、実施すること自体が目的ではなく、不適合に対する改善処置を実施し、情報セキュリティマネジメントに対する不適合をなくすことが本来の目的である。そのため、不適合を処置するための予算を確保しておくことが重要である。

3.2.3 経営陣は情報セキュリティマネジメントのマネジメントレビューを実施する

情報セキュリティマネジメントの継続性を評価するためにマネジメントレビューを実施する。マネジメントレビューの実施を確実にするために経営陣は以下の点について考慮し、経営資源を提供する。

・マネジメントレビュー基本計画

・マネジメントレビューを実施するための経営資源

・マネジメントレビューによって検出されるであろう不適合を処置するための予算

マネジメントレビューは、実施すること自体が目的ではなく、不適合に対する改善処置を実施し、情報セキュリティマネジメントに対する不適合をなくすことが本来の目的である。そのため、不適合を処置するための予算を確保しておくことが重要である。

また、マネジメントレビューは情報セキュリティマネジメント全体に対して実施するため、効率を良くするために、監視や監査との連携を視野に入れた基本計画を構築するのが望ましい。

3.3 管理策の有効性評価

3.3.1 情報セキュリティマネジメントの有効性について定期的にレビューする

情報セキュリティマネジメントの有効性については以下の2点について定期的にレビューする。

・情報セキュリティ基本方針及び目的を満たしているか

・セキュリティ管理策が管理目的を満たしているか

総合的なレビューにおいては、システムや業務上の情報収集だけではなく、セキュリティ監査の結果、イベントやインシデントの状況、有効性測定の結果、提案及びすべての利害関係者からのフィードバックを考慮する。

事業目標の変更など、経営的な変更が行われた場合などについても、事業影響度が変化するなど情報セキュリティマネジメントに関連する場合もあるので、さまざまな方面からの情報収集及び判断が必要となる。

3.3.2 管理策の有効性を測定する

あらかじめ計画した間隔で、管理策の有効性を測定する。管理策の有効性を測定する際には以下の点について考慮する。

・管理目的と管理策の目標

・管理策の背景となるリスク

・関連する管理策

管理策によっては監視が常に必要になるものもあるので、それぞれの管理策に適切な測定方法を検討し、実施する必要がある。

3.3.3 あらかじめ定めた間隔で内部監査を実施する

内部監査は管理策の有効性を総合的に確認するために、定期的に実施する。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ておく。予定通り実施されたことを証明するためにも、実施報告書が作成されているとよい。

また、適合性の監査においては以下の項目を対象として実施する。

・関連する法令または規制の要求事項

・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

・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

3.3.4 監査の対象となるプロセス及び領域の状況及び重要性、並びに前回までの監査結果を考慮して監査プログラムを作成する

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る。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。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

3.3.5 監査の基準、範囲、頻度及び方法を定義する

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
・監査の範囲
・監査の頻度または時期
・監査の方法

特に監査の方法においては、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。監査基準には以下の内容を含める。

・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

3.3.6 監査員の選定及び監査の実施においては、監査プロセスの客観性及び公平性を確実にする

監査人の選定においては監査基準に記載し、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

また、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。

3.3.7 監査の計画、実施、結果に関する責任及び要求事項を、文書化した手順の中で定義する

監査手順に以下の内容を反映させる。

・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ためになくてはならない。監査手順は文書化し、お互いのコミュニケーションのために活用する。

3.3.8 監査された領域に責任をもつ管理者は、発見された不適合及び原因を除去するために遅延なく処置がとられることを確実にする

監査の目的は不適合の発見とその原因の除去である。発見した不適合はそれらが大きな影響を与える前に除去しなければならない。不適合の一覧には以下の内容が含む。

・不適合の種類
・不適合の内容
・不適合の原因（ぜい弱性、脅威、影響など）
・処置の緊急度

記載された内容をもとに、処置の優先順位を決め、対応する。

3.3.9 フォローアップには、とった処置の検証及び検証結果の報告を含める

緊急度の高い不適合に対しては応急処置がとられたり、他の管理策との関連性がとられないまま処置されたりしてしまうものがある。新たな不適合を発生させないためにも、以下の内容ついて検証し、その結果を報告する。

・処置の妥当性
・他の管理策との関連性
・処置の実施に伴う新たなリスク

また、処置を実施することによって新たなリスクが発生する場合がある。これらの内容も検証報告に含めることを忘れてはならない。

3.4 情報セキュリティマネジメントの継続性評価

3.4.1 変化に対応するために、定期的にリスクアセスメントを実施する

あらかじめ決めた計画に沿って、定期的にリスクアセスメントを実施する。以下の変化に伴うリスクの特定及びリスク受容レベルの決定を実施する。

・組織
・技術
・事業の目的及びプロセス
・特定した脅威
・導入した管理策の有効性
・法令、規制、契約上の義務、社会的風潮などの外部事情

少なくとも年に1回は実施されていることを、計画及び実施報告書などから確認できるようにしておく。これらのリスクアセスメントの内容については、情報セキュリティ監査において重要な判断基準にもなるので、わかりやすく文書化しておくことが重要である。

3.4.2 マネジメントレビューを定期的に実施する

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。

・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報告書

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ておく。予定通り実施されたことを証明するためにも、実施報告書が作成されているとよい。

3.4.3 監視及びレビューによって判明した事実を反映するために、情報セキュリティマネジメント計画を更新する

情報セキュリティマネジメント計画の更新は以下の活動から得られた結果をもとに実施される。

・日常行われている監視
・定期的に実施されるマネジメントレビュー

日常行われている監視においては、重大な障害が発生したか、発生する可能性を検知した場合に管理策の見直しを実施する。しかし、管理策の選択そのものに問題がある場合に

は計画そのものを変更する場合もある。

変更の緊急性などについては、リスク受容基準やリスク受容レベルを定義した文書などとともに管理するとよい。

3.4.4 情報セキュリティマネジメントの有効性及びパフォーマンスに影響を及ぼす可能性のある活動及び事象を記録する

マネジメントレビューには以下の項目を提供する。

- 情報セキュリティ監査及びレビューの結果
- 従業者を含む利害関係者からのフィードバック
- 情報セキュリティマネジメントの有効性及びパフォーマンスを改善するために組織の中で利用可能な技術、製品、または手順
- 予防処置及び是正処置の状況
- 前回までのリスクアセスメントが十分に取り上げていなかったぜい弱性または脅威
- 有効性測定の結果
- 前回までのマネジメントレビューの結果に対するフォローアップ
- 情報セキュリティマネジメントに影響を及ぼす可能性のある、あらゆる変化
- 改善のための提案

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。

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ておくのが望ましい。

3.4.5 レビューの結果は明確に文書化し、記録を維持する

レビューの結果は次回の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記録しておかなければならない。レビューの担当者が変更になった場合でも、内容が分かるようにしておくことが重要である。

3.4.6 レビューの結果を反映して改善策を検討する

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を改善する
- リスクアセスメント及びリスク対応計画を更新する
- 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して、手順及び管理策を修正する
- 必要となる経営資源を特定する
- 管理策の有効性測定方法を改善する

改善策の立案においては、管理策を選択した際の記録を参考にするとよい。

4 情報セキュリティマネジメントの維持及び改善

情報セキュリティマネジメントを効果的に運用するために、定期的な見直しを実施する。監視、監査、レビューによって洗い出された不適合や新たなリスクに対しての改善策を導入することで、環境に対応した情報セキュリティマネジメントを運用できる。

4.1 改善策の導入

4.1.1 特定した改善策を情報セキュリティマネジメントに導入する

特定した改善策については、従来の管理策に及ぼす影響を十分に考慮した上で情報セキ

ュリティマネジメントに導入する。以下の項目について考慮すること。

・管理目的を満たすために有効であること

・すでに導入済みの管理策に影響を及ぼさないこと

改善策の導入においても、管理策同様に経営陣の許可を得てから実施する。

4.1.2 自他の組織が経験したことから学んだ内容を考慮し、適切な是正処置及び予防処置を実施する

これまでの管理策の不備については是正処置を、新たなリスクについては予防処置を実施する。是正処置及び予防処置については以下の点について考慮する。

・自組織で発生している障害及びその対応策

・他組織で発生している障害及びその対応策

組織の内外にかかわらず、情報を収集して適宜対応できるような体制を構築しておくこと。

4.1.3 すべての利害関係者に状況に見合った適切な内容で、処置及び改善策を伝えると共に、必要に応じて対応の進め方について合意を得る

管理策の変更による影響について十分に考慮した上で、処置及び改善策を伝える。過去の対策と改善策が混在した状況ではリスクが改善されたとは言えないため、以下の点について確認をし、変更を確実なものとする。

・処置及び改善策における変更点を文書化する

・あらかじめ決められた連絡方法ですべての利害関係者に伝える

・必要に応じて、処置及び改善策を受け入れたことを確認する

もしも変更が受け入れられなかった場合はその背景などを説明し、お互いの利益を損なわないように調整する。

4.1.4 改善策が意図した目的を達成することを確実にする

改善策においても、通常の管理策同様に管理目的を達成するために測定方法を明確にし、管理策が適切に実施されていることを確実にする。改善策が目的を達成していない場合は同様に新たな改善策を検討し、導入する。

4.2 是正処置

4.2.1 情報セキュリティマネジメントの要求事項に対する不適合の原因を除去する処置を、その再発防止のためにとる

不適合を是正するための処置を是正処置といい、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かったり、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。

不適合は以下の活動によって検出される。

・定期的なリスクアセスメント

・定期的な監視

・情報セキュリティ監査

・マネジメントレビュー

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必要がある。

4.2.2 是正処置のために手順を策定し、文書化する

是正処置の手順には以下の活動を含める。

・情報セキュリティマネジメントに対する不適合を特定する
・情報セキュリティマネジメントに対する不適合の原因を決定する
・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を評価する
・必要な是正処置の決定をする
・必要な是正処置を実施する
・実施した処置を記録する
・実施した是正処置をレビューする

これらの活動を手順どおりに実施するために文書化する。

4.3 予防処置

4.3.1 情報セキュリティマネジメントの要求事項に対する不適合の発生を防止するために、起こりうる不適合の原因を除去する処置を決定する

不適合を予防するための処置を予防処置といい、これまでに実施していなかった新たな管理策を実施することが多い。これは組織の戦略の変更や、組織を取り巻く環境の変化に伴って新たな脅威やぜい弱性が対象となるためであり、以下の活動の結果として反映される。

・定期的なリスクアセスメント
・定期的な監視
・情報セキュリティ監査
・マネジメントレビュー

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必要がある。予防処置は是正処置に比べて多くの場合、費用対効果が大きいことから、緊急度に応じて迅速に対応することが望ましい。

4.3.2 予防処置のために手順を策定し、文書化する

予防処置のための手順には以下の活動を含める。

・情報セキュリティマネジメントに対する不適合を特定する
・情報セキュリティマネジメントに対する不適合の原因を決定する
・不適合の発生を予防するために選択した処置の必要性を評価する
・リスクアセスメントの結果に基づいて必要な予防処置の決定をする
・必要な予防処置を実施する
・実施した処置を記録する
・実施した予防処置をレビューする
・変化したリスクを特定し、大きく変化したリスクに注意を向けて予防処置に対する要求事項を特定する

これらの活動を手順どおりに実施するために文書化する。

5 文書管理及び記録の管理

情報セキュリティマネジメントの確立、導入と運用、監視・監査・レビュー、維持・改善のそれぞれのフェーズに共通の内容として文書管理及び記録の管理が挙げられる。情報セキュリティマネジメントにおける様々な活動が効果的に連携していることを説明するために、文書及び記録を管理する。

5.1 文書化

5.1.1 情報セキュリティマネジメント文書は、とった処置から、経営陣の決定及び方針にたどれることを確実にする

情報セキュリティマネジメントに関連する文書には以下の内容を含める。

・情報セキュリティ基本方針及び目的
・情報セキュリティマネジメントの適用範囲
・情報セキュリティマネジメントを支えている手順及び管理策
・リスクアセスメントの方法
・リスクアセスメント報告
・リスク対応計画
・情報セキュリティを有効に計画、運用、管理するための手順
・管理策の有効性を測定するための手順
・記録

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されていなければならない。また、知る必要性のないものがそれを閲覧できるようにならないことを確実にしなければならない。

5.1.2 手順は正しく実行できるように文書化する

正しく実行できるように手順を文書化するためには以下を実施する。

・手順を確立する
・手順を文書化する
・手順を実施した結果を反映する
・手順が正しく実行できるように改善し、維持する

すべての関係者が同じ判断で同じ手順を実施できるように、必要に応じて判断基準を含めることを忘れてはならない。

5.2 文書管理

5.2.1 情報セキュリティマネジメントに関連する文書は保護し、管理する

情報セキュリティマネジメントに関連する文書は以下の点について考慮し、維持・改善に役立てるために保護し、管理する。

・選択した管理策がリスクアセスメント及びリスク対応のプロセスまでたどれること
・選択した管理策が情報セキュリティ基本方針及び目的までつながること

これらの連携が途切れてしまった場合、管理策が適切に運用・管理されているか、また有効性を満たしているかなどの判断ができなくなるばかりか、そもそもの目的を反映しているのかさえもわからなくなってしまう。正しい文書管理のもと、構成や変更を管理する必要がある。

5.2.2 管理活動を定義した手順を作成する

文書管理には以下の活動を含む。これらを適切に実施できるような手順を作成する。

・文書を発行する前に、適切かどうかを承認する
・文書をレビューする
・必要に応じて、文書を更新し、再承認する
・文書の改編を特定するための記載をする
・文書の現在の改版状況を特定するための記載をする

・必要に応じて、文書に関連する版を参照できるようにする
・文書を読みやすくし、かつ容易に識別可能であるようにする
・文書のアクセス管理を実施する
・文書ライフサイクルを定義し、それに応じた処理ができるように手順を定める
・外部で作成された文書であることを識別できるようにする
・文書の配布管理手順を定め、実施する
・廃止文書の誤使用を防止する
・廃止文書を何らかの目的で保持する場合には、適切な識別を施す

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。

5.3 記録の管理

5.3.1 情報セキュリティマネジメントの運用に関する有効な証拠を提供するために、記録を作成する

情報セキュリティマネジメントが実施されていることをすべての利害関係者に説明するために記録及び、記録をまとめた報告書を作成する。記録の取得については以下の目的についてそれぞれ作成する。

・管理策の有効性を判断するため
・情報セキュリティマネジメントの実施を説明するため
・事故が発生した際の原因調査のため

管理策の有効性や情報セキュリティマネジメントの実施を説明するための記録はその取得だけではなく、定期的に報告書としてまとめていくことが必要になる。記録を取っているだけでは十分ではない。

5.3.2 記録した結果が再現可能であることを確実にする

情報セキュリティマネジメントの維持・改善のために、記録した結果から行動した内容が推測できるなど、再現可能であることを確実にするために、以下の点を考慮する。

・記録に十分な内容が含まれているか
・記録が漏れなく取得されているか
・記録が信頼できるか

十分な記録の内容には以下のものが含まれているのが望ましい。

・活動が記録された日時
・活動をした主体
・活動をした場所
・活動内容

活動主体は従業者以外にも、コンピュータやネットワーク機器の場合もある。主体を正しく識別できるように、それぞれに個別のIDを割り当てるなど、記録に反映できるようにする。

また、記録の漏れがないよう、記録を取得する体制及びシステムなどを構築する。

5.3.3 記録は関連する法令又は規制の要求事項及び契約上の義務を考慮して保護し、管理する

記録には機密情報や個人情報などを含む場合がある。含まれる内容に応じて適切なアクセス権を設定し、管理する。また、法令によっては記録の保管年数を規定しているものが

ある。これらの要求に応じるために、以下を考慮して記録を保護、管理する。

・記録に含まれる情報と法令、規制、契約の関係

・記録を保存したメディアの耐性（耐用年数など）

・記録を保存したメディアの改ざんの可能性（書き込み制限など）

記録を複製した場合にはそのバージョンと複製の数を管理するなど、正式な文書がどれになるかを明確にできるように管理する。記録は情報資産の一部として管理する。

5.3.4 記録は読みやすく、容易に識別可能で、検索可能にする

記録は再現性を損なわない程度に正規化し、活用しやすいようにしておく。場合によっては報告書などの形式にするなどして、その記録の利用者が適切に活用できるような状態にしておく。記録を編集する際には以下の点について考慮する。

・利用者が読みやすいように編集する

・利用者が識別しやすいように編集する

・利用者が利用したい時にいつでも検索できるように検索用の分類を付与する

記録はその保存期間に応じて適切な編集をする。

5.3.5 記録の識別、保管、保護、検索、保存期間及び廃棄のために必要な管理策を文書化し、実施する

記録も通常の文書と同様に情報資産として扱われる。したがって、情報資産と同様にライフサイクルに応じて適切な管理を実施する。記録の管理においては、特に以下について考慮する。

・記録の真正性

・記録の関連性

・記録の保管方法

・記録の保存期間

記録の種別によっては、その他の記録との関連性を位置づける内容（データベースにおける外部キーなど）を削除するなどして、関係が損なわれることで意味をなさない場合もあるため、編集保存する際に特に気をつける必要がある。

5.3.6 プロセスのパフォーマンスの記録及び情報セキュリティマネジメントに関係する重大なセキュリティインシデントすべての発生記録を保持する

記録は説明責任を果たすためだけに活用するのではなく、管理策のパフォーマンス測定や、改善策の提案にも活用される。プロセスのパフォーマンスを測るための記録及び、インシデントの発生記録については、相当期間すべての情報を保持しておく。

改善策の妥当性を測ったり、長期的なパフォーマンスの測定などに利用したりするには、生の記録ではなく、統計データで十分な場合もある。記録を保管しておく書庫の大きさやストレージの容量に従って適切な管理を実施できるように、あらかじめ手順を作成し、それに従って作業を実施する。

Ⅳ．管理策基準

1 セキュリティ基本方針

1.1 情報セキュリティ基本方針

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、関連する法令及び

規制に従って規定するため

1.1.1 情報セキュリティ基本方針文書は、経営陣が承認し、また、全従業員及び関連する外部関係者に公表し、通知する

1.1.1.1 情報セキュリティ基本方針文書に、経営陣の責任を明記し、情報セキュリティの管理に対する組織の取組み方を示す

1.1.1.2 情報セキュリティ基本方針文書に、情報セキュリティの定義、その目的及び適用範囲、並びに情報共有を可能にする基盤としてのセキュリティの重要性に関する記述を含める

1.1.1.3 情報セキュリティ基本方針文書に、事業戦略及び事業目的に沿った情報セキュリティの目標及び原則を支持する経営陣の意向を含める

1.1.1.4 情報セキュリティ基本方針文書に、リスクアセスメント及びリスクマネジメントの構造を含む、管理目的及び管理策を設定するための枠組みを含める

1.1.1.5 情報セキュリティ基本方針文書に、組織にとって特に重要な、セキュリティの個別方針、原則、標準類及び順守の要求事項（法令、規則及び契約上の要求事項の順守、セキュリティ教育・訓練及び意識向上に関する要求事項、事業継続管理、情報セキュリティ基本方針違反に対する処置など）の簡潔な説明を含める

1.1.1.6 情報セキュリティ基本方針文書に、情報セキュリティインシデントを報告することも含んだ、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義を含める

1.1.1.7 情報セキュリティ基本方針文書は、情報セキュリティ基本方針を支持する文書（例えば、特定の情報システムのためのより詳細なセキュリティ方針及び手順、又は利用者が順守することが望ましいセキュリティ規則）への参照情報を含める

1.1.1.8 情報セキュリティ基本方針は、想定する読者にとって、適切で、利用可能で、かつ、理解しやすい形で、組織全体にわたって利用者に知らせる

1.1.2 情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当及び有効であることを確実にするためにレビューする

1.1.2.1 情報セキュリティ基本方針の作成、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

1.1.2.2 情報セキュリティ基本方針のレビューに、組織の情報セキュリティ基本方針を改善する機会の評価、及び組織環境、業務環境、法的状況又は技術環境の変化に応じた情報セキュリティの管理への取組みの評価を含める

1.1.2.3 情報セキュリティ基本方針のレビューに、マネジメントレビューの結果を考慮し、反映する

1.1.2.4 改訂された情報セキュリティ基本方針は、経営陣から承認を得る

2 情報セキュリティのための組織

2.1 内部組織

目的：組織内の情報セキュリティを管理するため

2.1.1 経営陣は、情報セキュリティの責任に関する明りょうな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持する

2.1.1.1 経営陣は、組織の要求事項を満たす情報セキュリティ目標を共有し、関連するプロセスに統合することを確実にする

2.1.1.2　経営陣は、情報セキュリティ基本方針を明確に表現し、レビューし、承認する

2.1.1.3　経営陣は、情報セキュリティ基本方針の実施の有効性をレビューする

2.1.1.4　経営陣は、セキュリティを主導するための明りょうな方向付け及び目に見える形での経営陣の支持を提供する

2.1.1.5　経営陣は、情報セキュリティに必要とされる資源（人的資源、予算、情報システムなど）を提供する

2.1.1.6　経営陣は、組織全体にわたる情報セキュリティのための明確な役割及び責任の割当てを承認する

2.1.1.7　経営陣は、情報セキュリティに関する意識を維持するための計画及びプログラムを開始する

2.1.1.8　経営陣は、情報セキュリティの実施を組織全体にわたって調整が確実に行われる仕組みを整備する

2.1.1.9　経営陣は、内部又は外部の専門的な情報セキュリティの助言の必要性を特定し、レビューし、助言の結果を組織内で調整する

2.1.2　情報セキュリティ活動は、組織の中の、関連する役割及び職務機能をもつ様々な部署の代表が、調整する

2.1.2.1　情報セキュリティの調整には、管理者、利用者、実務管理者、業務用ソフトウェアの設計者、監査者及びセキュリティ担当職員の協力及び協調並びに保険、法的問題、人的資源、IT又はリスクマネジメントのような分野の専門家の技能を含める

2.1.2.2　情報セキュリティの調整では、情報セキュリティ基本方針を順守したセキュリティ活動を確実に実行する

2.1.2.3　情報セキュリティの調整では、情報セキュリティ基本方針に対する非順守の事項の扱い方を特定する

2.1.2.4　情報セキュリティの調整では、情報セキュリティのための方法及びプロセス（例えば、リスクアセスメント、情報分類）を承認する

2.1.2.5　情報セキュリティの調整では、重要な脅威の変化の特定並びに情報及び情報処理施設がさらされる脅威を特定する

2.1.2.6　情報セキュリティの調整では、情報セキュリティの管理策の妥当性の評価及びその実施を調整する

2.1.2.7　情報セキュリティの調整では、組織全体にわたる情報セキュリティの教育、訓練及び意識向上の効果的な促進のための調整を行う

2.1.2.8　情報セキュリティの調整では、情報セキュリティインシデントの監視及びレビューによって得た情報の評価、並びに特定された情報セキュリティインシデントに応じた適切な処置を推奨する

2.1.3　すべての情報セキュリティ責任を明確に定める

2.1.3.1　情報セキュリティ責任の割当ては、情報セキュリティ基本方針に従って行う

2.1.3.2　個々の資産の保護に対する責任及び特定のセキュリティプロセスの実施に対する責任を、明確に定める

2.1.3.3　必要な場合には、この責任は、個別のサイト及び情報処理施設に関する、より詳細な手引で補う

2.1.3.4　資産の保護及び事業継続計画のような特定のセキュリティプロセスの実行に限定される責任を明確に定める

2.1.3.5　セキュリティに関する職務を他者に委任する場合は、いずれの委任した職務も正しく実行されていることを確認する

2.1.3.6　個人が責任をもつ領域を明確にするために、個々の特定のシステムに関連した資産及びセキュリティのプロセスを識別し、明確に規定する

2.1.3.7　個人が責任をもつ領域を明確にするために、各資産又はセキュリティのプロセスに対する責任主体（例えば、個人、職位）の指名及びその責任の詳細の文書化を行う

2.1.3.8　個人が責任をもつ領域を明確にするために、承認の権限の明確な規定及び文書化を行う

2.1.4　新しい情報処理設備に対する経営陣による認可プロセスを定め実施する

2.1.4.1　認可プロセスでは、新しい設備の目的及び用途について、適切な利用部門の経営陣の承認に加え、すべての関連するセキュリティ方針及び要求事項を確実に満たすために、その情報システムセキュリティ環境の維持に責任をもつ管理者の承認を得る

2.1.4.2　認可プロセスでは、ハードウェア及びソフトウェアが、他のシステム構成要素と両立できることを確実にするために、検査する

2.1.4.3　認可プロセスでは、業務情報の処理のための、個人の又は私的に所有する情報処理設備（例えば、ラップトップコンピュータ、家庭用コンピュータ、携帯端末）の利用が、新しいぜい弱性をもち込むことにならないよう、管理策を特定し、実施する

2.1.5　情報保護に対する組織の必要とすること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する

2.1.5.1　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盛り込む

2.1.5.2　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

2.1.5.3　秘密保持契約又は守秘義務契約には、契約の有効期間を含める

2.1.5.4　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

2.1.5.5　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（例えば、知る必要がある要員だけに知らせる。）ための、署名者の責任及び行為を含める

2.1.5.6　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、並びにこれの秘密情報の保護との関連を含める

2.1.5.7　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

2.1.5.8　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

2.1.5.9　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

2.1.5.10　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

2.1.5.11　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取られる処置を含める

2.1.5.12　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則のすべて

に従うようにする

2.1.5.13 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

2.1.6 関係当局との適切な連絡体制を維持する

2.1.6.1 法が破られたと疑われる場合に、いつ、だれが関係当局（例えば、法の執行機関、監督官庁）に連絡するか、また、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

2.1.6.2 インターネットからの攻撃下にある組織は、外部の第三者（例えば、インターネットサービス提供者、通信事業者）が攻撃元に対して対策を取ることを必要とする場合も考慮した連絡体制を維持する

2.1.7 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

2.1.7.1 新しい技術、製品、脅威又はぜい弱性に関する情報の共用、交換及び入手などと、情報セキュリティインシデントを扱う場合の、適切な連絡窓口の提供などを目的として、情報セキュリティに関する研究会又は会議に参加する

2.1.7.2 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ことを目的として、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

2.1.8 情報セキュリティ及びその実施のマネジメントに対する組織の取組み（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）について、あらかじめ計画した間隔で、又はセキュリティの実施に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

2.1.8.1 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り組みが、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する

2.1.8.2 独立したレビューには、改善の機会のアセスメントを含む

2.1.8.3 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方の変更の必要性の評価を含む

2.1.8.4 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、適切な技能及び経験を持った個人・組織（例えば、内部監査の担当部署、独立した管理者、そのようなレビューを専門に行う第三者組織）が実施する

2.1.8.5 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し、その内容を記録として維持する

2.1.8.6 独立したレビューにより、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こと、又は情報セキュリティ基本方針文書に記載された情報セキュリティに関する方向付けを順守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

2.2 外部組織

目的：外部組織によってアクセス、処理、通信又は管理される組織の情報及び情報処理施設のセキュリティを維持するため

2.2.1 外部組織がかかわる業務プロセスからの、組織の情報及び情報処理施設に対するリスクを識別する。また、外部組織にアクセスを許可する前に適切な管理策を実施する

2.2.1.1 外部組織からのアクセスに関連するリスクの識別の対象には、外部組織がアクセスする必要がある情報処理施設を含める

2.2.1.2 外部組織からのアクセスに関連するリスクの識別の観点に、外部組織による情報及び情報処理施設へのアクセスの種類（物理的アクセス、論理的アクセス、組織のネットワークと外部組織のネットワークとの間の接続、アクセスの実施場所の区別など）を含める

2.2.1.3 外部組織からのアクセスに関連するリスクの識別の観点に、関連する情報の、価値及び取扱いに慎重を要する度合い、並びに業務運用における重要度を含める

2.2.1.4 外部組織からのアクセスに関連するリスクの識別の観点に、外部組織によるアクセスを想定していない情報を保護するために必要な管理策を含める

2.2.1.5 外部組織からのアクセスに関連するリスクの識別の観点に、組織の情報を取り扱う外部組織の要員を含める

2.2.1.6 外部組織からのアクセスに関連するリスクの識別の観点に、アクセスを認可された組織又は要員を識別する方法、その認可を確認する方法及び再確認を行う頻度を含める

2.2.1.7 外部組織からのアクセスに関連するリスクの識別の観点に、情報の格納、処理、通信、共有及び交換に外部組織が用いる種々の手段及び管理策を含める

2.2.1.8 外部組織からのアクセスに関連するリスクの識別の観点に、外部組織が必要としたときに利用できないアクセスの影響及び外部組織が不正確な情報又は誤った情報を入力又は受領することの影響を含める

2.2.1.9 外部組織からのアクセスに関連するリスクの識別の観点に、情報セキュリティインシデント及び潜在的な損傷を処理する慣行及び手順並びに情報セキュリティインシデントが発生した場合に外部組織のアクセスを継続する条件を含める

2.2.1.10 外部組織からのアクセスに関連するリスクの識別の観点に、外部組織との関連で考慮することが望ましい、法令及び規則の要求事項並びに契約上の義務を含める

2.2.1.11 外部組織からのアクセスに関連するリスクの識別の観点に、契約が他の関係者の利害に及ぼす影響を含める

2.2.1.12 外部組織による組織の情報へのアクセスは、適切な管理策を実施するまで提供しない

2.2.1.13 外部組織による組織の情報へのアクセスは、接続又はアクセスの条件、及び業務に関する取決めを明示した契約書を締結するまで提供しない

2.2.1.14 外部組織との業務から生じるすべてのセキュリティ要求事項は、外部組織との契約に反映する

2.2.1.15 外部組織が自らの責務を認識し、組織の情報及び情報処理施設に関するアクセス、処理、通信又は管理についての責任及び義務を受け入れることを確実にする

2.2.2 顧客に組織の情報又は資産へのアクセスを許す前に、明確にしたすべてのセキュリティ要求事項を満たすように対処する

2.2.2.1 顧客が組織の資産にアクセスする際のセキュリティの要求事項には、情報・ソフトウェアを含む組織の資産を保護するための手順及び既知のぜい弱性の管理、資産を危うくする事態を判断するための手順、完全性の確保、情報の複製及び開示の制限を含む資産の保護を含める

2.2.2.2 顧客が組織の資産にアクセスする際のセキュリティの要求事項には、提供する製品又はサービスを記載する

2.2.2.3 顧客が組織の資産にアクセスする際のセキュリティの要求事項には、顧客のアクセスの様々な理由、要求事項及び利便を記載する

2.2.2.4 顧客に組織の情報又は資産へのアクセスを許す前に、アクセス制御方針を策定する。このアクセス制御方針には、承認されたアクセス方法、並びに固有の識別子（例えば、利用者IDとパスワードとの組合せ）の管理及び使用、利用者のアクセス及び特権の認可プロセス、明示的に認可されていないすべてのアクセスを禁止することの表明、アクセス権を失効させる、又はシステム間の接続を阻止する手続を含める

2.2.2.5 顧客に組織の情報又は資産へのアクセスを許す前に、情報（例えば、個人情報）の誤り、情報セキュリティインシデント及びセキュリティ違反の報告、通知及び調査に関する取決めを明確にする

2.2.2.6 顧客が組織の資産にアクセスする際のセキュリティ要求事項には、顧客に組織の情報又は資産へのアクセスを許す前に、利用できる各サービスを記載する

2.2.2.7 顧客に組織の情報又は資産へのアクセスを許す前に、サービスの目標レベル及び受け入れられないレベルを明確にする

2.2.2.8 顧客に組織の情報又は資産へのアクセスを許す前に、組織の資産に関係する活動を監視し、中止させる権利を明確にする

2.2.2.9 顧客に組織の情報又は資産へのアクセスを許す前に、組織及び顧客のそれぞれの義務を明確にする

2.2.2.10 顧客に組織の情報又は資産へのアクセスを許す前に、法的な問題に関する責任及び法的要求事項を満たすことを確実にする。特に、契約が他国の顧客との協力にかかわるものである場合、その国の法制度を考慮に入れる

2.2.2.11 顧客に組織の情報又は資産へのアクセスを許す前に、知的財産権（IPR）及び著作権の取扱い、並びに共同作業の成果の保護のあり方を明確にする

2.2.3 組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げる

2.2.3.1 組織と第三者との間に誤解がないことを確実にするために契約の確認を行う

2.2.3.2 組織は、第三者の補償の内容（損害賠償など）が納得できる内容であることを確認する

2.2.3.3 特定されたセキュリティ要求事項を満たすために、第三者との契約に、情報セキュリティ基本方針を含める

2.2.3.4 特定されたセキュリティ要求事項を満たすために、第三者との契約に、資産保護を確実にするための管理策を含める。この管理策には、次の事項を含める

1.情報、ソフトウェア及びハードウェアを含む組織の資産を保護する手順
2.要求する物理的保護に関する管理策及び手段
3.悪意のあるソフトウェアからの保護を確実にするための管理策
4.資産を危うくする事態を判断するための手順
5.契約の終了時又は契約期間中の合意時点における情報及び資産の返却又は破棄を確実にするための管理策
6.資産に関連する特性（例えば、機密性、完全性、可用性）
7.情報の複製及び開示の制限、並びに秘密保持契約の利用

2.2.3.5 特定されたセキュリティ要求事項を満たすために、第三者との契約に、利用者及び実務管理者に対する、方法、手順及びセキュリティについての教育・訓練を含める

2.2.3.6 特定されたセキュリティ要求事項を満たすために、第三者との契約に、情報セキュリティの責任及び課題に対する利用者の認識の確実化を含める

2.2.3.7 特定されたセキュリティ要求事項を満たすために、第三者との契約に、適切ならば、要員の異動に関する規定を含める

2.2.3.8 特定されたセキュリティ要求事項を満たすために、第三者との契約に、ハードウェア及びソフトウェアの導入及び保守に関する責任を含める

2.2.3.9 特定されたセキュリティ要求事項を満たすために、第三者との契約に、明確な報告項目及び合意された報告の書式を含める

2.2.3.10 特定されたセキュリティ要求事項を満たすために、第三者との契約に、変更管理の明確で具体的なプロセスを含める

2.2.3.11 特定されたセキュリティ要求事項を満たすために、第三者との契約に、アクセス制御の方針を含める。この方針には、第三者のアクセスを必要とする様々な理由、要求事項及び利便、許可されたアクセス方法、並びに固有の識別子（例えば、利用者IDとパスワードとの組合せ）の管理及び使用、利用者のアクセス及び特権の認可プロセス、利用可能なサービスの利用を認可されている個人、並びにその利用におけるそれぞれの権限及び特権の一覧を維持するための要求事項、明示的に認可されていないすべてのアクセスを禁止することの表明、アクセス権を失効させる、又はシステム間の接続を阻止する手続がある

2.2.3.12 特定されたセキュリティ要求事項を満たすために、第三者との契約に、契約に記載された要求事項への違反と同様に、情報セキュリティインシデント及びセキュリティ違反の報告、通知及び調査に関する取決めを含める

2.2.3.13 特定されたセキュリティ要求事項を満たすために、第三者との契約に、提供する製品又はサービスの記載、及びセキュリティの分類に従って利用可能となる情報の規定を含める

2.2.3.14 特定されたセキュリティ要求事項を満たすために、第三者との契約に、サービスの目標レベル及び受け入れられないレベルを含める

2.2.3.15 特定されたセキュリティ要求事項を満たすために、第三者との契約に、検証可能な実施状況を測る基準、その監視及び報告の定義を含める

2.2.3.16 特定されたセキュリティ要求事項を満たすために、第三者との契約に、組織の資産に関連する活動を監視し、中止させる権利を含める

2.2.3.17 特定されたセキュリティ要求事項を満たすために、第三者との契約に、契約で規定した責任を対象に監査する権利、そのような監査を第三者に実施させる権利、及び監査人の法的資格を掲げる権利を含める

2.2.3.18 特定されたセキュリティ要求事項を満たすために、第三者との契約に、問題解決のための段階的処理プロセス（escalation process）の確立を含める

2.2.3.19 特定されたセキュリティ要求事項を満たすために、第三者との契約に、可用性及び信頼性の測定を含み、組織の事業における優先度に従ったサービス継続に関する要求事項を含める

2.2.3.20 特定されたセキュリティ要求事項を満たすために、第三者との契約に、契約当事者それぞれの義務を含める

2.2.3.21 特定されたセキュリティ要求事項を満たすために、第三者との契約に、法的な問題に関する責任及び法的要求事項（契約が他国の顧客との協力にかかわるものである場合、その国の法制度）を満たすことを確実にする方法を含める

2.2.3.22 特定されたセキュリティ要求事項を満たすために、第三者との契約に、知的財産権（IPR）及び著作権の取扱い、並びに共同作業の成果の保護を含める

2.2.3.23 特定されたセキュリティ要求事項を満たすために、第三者との契約に、第三者による下請負業者の利用の有無、及びこれらの下請負業者が実施する必要のあるセキュリティ管理策を含める

2.2.3.24 特定されたセキュリティ要求事項を満たすために、第三者との契約に、契約の見直し又は打切りのための条件（契約当事者が契約の期限前に関係の打切りを希望する場合に備えた対応計画、組織のセキュリティ要求事項が変化となった場合の契約の見直し、資産目録、ライセンス、契約又はそれらに関係する権利についてのその時点での文書）を含める

3 資産の管理

3.1 資産に対する責任

目的：組織の資産を適切に保護し、維持するため

3.1.1 すべての資産は、明確に識別する。また、重要な資産すべての目録を、作成し、維持する

3.1.1.1 資産目録には、重要度を記録する

3.1.1.2 資産目録には、資産の種類、形式、所在、バックアップ情報、ライセンス情報及び業務上の価値を含め、災害から復旧するために必要なすべての情報を記載する

3.1.1.3 資産目録は、他の目録と不必要に重複することなく、その記載内容が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

3.1.1.4 資産目録を作成し維持する場合には、各々の資産の管理責任者及び情報の分類について合意し文書化する

3.1.1.5 資産の重要度に応じた保護のレベルは、資産の重要度、業務上の価値及びセキュリティ上の分類に基づいて決める

3.1.2 情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定する

3.1.2.1 資産の管理責任者は、情報及び情報処理施設と関連する資産を適切な方法で分類することを確実にすることに責任を持つ

3.1.2.2 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して、アクセスの制限及び分類を定め、定期的に見直す責任を持つ

3.1.2.3 業務プロセス、定められた一連の活動、業務用ソフトウェア、定義された一連のデータなどについて、管理責任者を設置する

3.1.3 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

3.1.3.1 すべての従業員、契約相手及び第三者の利用者に対し、情報及び情報処理施設と関連する資産の利用（電子メール及びインターネットの利用、モバイル装置、特に組織の構外

での利用を含む）の許容範囲に関する規則を周知徹底する

3.1.3.2 従業員、契約相手及び第三者の利用者に対して、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もとで行ったいかなる利用に対しても、責任があることを認識させる

3.2 情報の分類

目的：情報の適切なレベルでの保護を確実にするため

3.2.1 情報は、組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から、分類する

3.2.1.1 情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮し、情報の分類及び関連する保護管理策を策定する

3.2.1.2 分類の指針には、あらかじめ決められたアクセス制御方針に従った最初の分類及び時間が経ってからの再分類に関する取扱いを含める

3.2.1.3 資産の管理責任者の責任で、資産の分類を定め、定期的にそれをレビューし、それを最新の状態で、かつ、適切なレベルで維持することを確実にする仕組みを整備する

3.2.1.4 分類項目の数及びそれらの利用で得られる効用（経済性又は実用性など）を考慮し、情報を分類する

3.2.2 情報に対するラベル付け及び取扱いに関する適切な一連の手順は、組織が採用した分類体系に従って策定し、実施する

3.2.2.1 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資産に適用できるようにする

3.2.2.2 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（出力に）付ける

3.2.2.3 印刷された文書、スクリーン表示、記録媒体（例えば、テープ、ディスク、CD、DVD）、電子的なメッセージ及び転送ファイルなどの項目を考慮し、分類の指針に従ったラベル付けを実施する

3.2.2.4 各分類レベルについて、安全な処理、保存、伝達、秘密解除及び破棄を含む取扱い手順を定める

3.2.2.5 各分類レベルについての取扱い手順には、情報資産受け渡し及び保管の記録の管理及びセキュリティ関連事象のログの取得に関する手順を含める

3.2.2.6 他の組織との情報共有を含む契約には、自分の組織における分類への置き換えや関連付けなど、その情報の分類を特定し、他の組織の分類ラベルを解釈するための手順を含める

4 人的資源のセキュリティ[*2]

4.1 雇用前

目的：従業員、契約相手及び第三者の利用者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とともに、盗難、不正行為、又は施設の不正使用のリスクを低減するため

4.1.1 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任は、組織の情報セキュリティ基本方針に従って定め、文書化する

4.1.1.1 従業員のセキュリティ上の役割及び責任には、組織の情報セキュリティ基本方針に従って実施し、行動することを含める

4.1.1.2 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、認可されていないアクセス、認可されていない開示、改ざん、破壊又は妨害から資産を保護することを含める

4.1.1.3 従業員、契約相手のセキュリティ上の役割及び責任には、特定のセキュリティのプロセス又は活動を実施することを含める

4.1.1.4 従業員、契約相手及び第三者の利用者の取るべき行動に関するセキュリティ上の役割及び責任を、個人に割り当てることを確実にする仕組みを整備する

4.1.1.5 従業員、契約相手及び第三者の利用者のセキュリティ上の役割及び責任には、セキュリティ事象、その可能性のある事象又は組織に対するその他のセキュリティリスクを報告することを含める

4.1.1.6 セキュリティ上の役割及び責任を定め、雇用前のプロセスにおいて、採用候補者に明確に伝える

4.1.1.7 組織の雇用プロセスを通して採用していない者（例えば、外部組織から派遣された者）のセキュリティの役割及び責任も、明確に定め、伝える

4.1.2 従業員、契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は、関連のある法令、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

4.1.2.1 従業員、契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は、関連がある個人情報及び個人データの保護に関する法令及び／又は雇用に関する法令のすべてを考慮に入れる

---

*2 「4 人的資源のセキュリティ」では、組織の情報セキュリティに影響を与え得る者を、従業員、契約相手及び第三者の利用者の三群に大別し、また、組織とそれらの者とのかかわりの経過を、関係の開始、継続及び終了の三段階に大別して、人的資源のセキュリティを取り扱う。このことから「4 人的資源のセキュリティ」では、従業員、契約相手又は第三者の利用者のいずれに関しても、組織が関係を開始することを雇用（4.1 参照）、この関係が継続している期間を雇用期間（4.2 参照）、この関係が終了することを雇用の終了と総称する（4.3 参照）。また、雇用期間中における職務内容の変更を、旧職務の雇用が終了し、新職務の雇用が開始するととらえ、これを雇用の変更と総称する（4.3 参照）。

また、「4 人的資源のセキュリティ」では、組織と従業員、契約相手及び第三者の利用者との情報セキュリティ側面での関係を規定したもの（文書化しているかどうかを問わない）を、職務定義書、雇用条件又は雇用契約書と総称し（4.1、4.2 参照）、必要に応じて、組織と従業員、契約相手又は第三者の利用者との雇用の関係を、それぞれ、雇用、契約又は合意と称する（4.3 参照）。このことから、例えば、雇用の終了を、従業員については雇用の終了、契約相手については契約の終了、また第三者の利用者については合意の終了として、それぞれを区別することがある。

「4 人的資源のセキュリティ」において従業員とは、常勤・非常勤、常用・臨時、又は長期・短期などの雇用の形態を問わない。契約相手には、組織が契約を締結したサービス提供業者、下請負業者、人材派遣業者などのほかに、これら業者の従業員であって、組織と締結した契約の履行のために組織に派遣された者なども含む（派遣された者が、組織とは直接に契約を締結していないことに留意）。第三者の利用者には、組織への一般来訪者、組織が開設するウェブサイト（ネットバンキングなど）の閲覧者などが含まれる。ただし、ウエブサイトの完全公開情報の閲覧については、除外する。

4.1.2.2 採用の選考では、関係する法令上許される場合には、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、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）の入手を行う

4.1.2.3 採用の選考では、関係する法令上許される場合には、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、応募者の履歴書の点検（完全であるか、正確であるかの点検）を行う

4.1.2.4 採用の選考では、関係する法令上許される場合には、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、提示された学術上及び職業上の資格の確認を行う

4.1.2.5 採用の選考では、関係する法令上許される場合には、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、公的証明書（パスポート又は同種の文書）の点検を行う

4.1.2.6 採用の選考では、関係する法令上許される場合には、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、信用調査又は犯罪記録の点検のような、より詳細な点検を行う

4.1.2.7 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取扱いに慎重を要する情報（例えば、財務情報、極秘情報）を扱っているときには、組織は、更に、より詳細な点検も検討する

4.1.2.8 選考の手順には、経歴などの確認のための基準及び制約を定める（例えば、だれが選考するのか。また、この確認は、どのように、いつ、なぜ行うのか。）

4.1.2.9 選考手続は契約相手及び第三者の利用者に対しても実施する

4.1.2.10 契約相手を通して要員が提供される場合は、契約相手との契約書に、要員選考に対する契約相手の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義若しくは懸念があるときに契約相手が守る必要がある告知手順を明確に記載する

4.1.2.11 第三者との契約書にも、要員選考に対する責任及び告知手順のすべてを明確に記載する

4.1.2.12 組織内での地位を得ようと考えているすべ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

4.1.2.13 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

4.1.3 従業員、契約相手及び第三者の利用者は、契約上の義務の一部として、情報セキュリティに関する、これらの者の責任及び組織の責任を記載した雇用契約書に同意し、署名する

4.1.3.1 雇用条件には、組織の情報セキュリティ基本方針を反映する

4.1.3.2 雇用条件には、取扱いに慎重を要する情報へのアクセスが与えられる、すべての従業員、契約相手及び第三者の利用者による、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含める

4.1.3.3 雇用条件には、従業員、契約相手及びその他利用者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ついてのもの）を含める

4.1.3.4 雇用条件では、従業員、契約相手及び第三者の利用者によって扱われる情報システム及びサービスに関連する、情報の分類及び組織の資産の管理に関する責任を明確にする

4.1.3.5 雇用条件では、他社又は外部組織から受け取った情報の扱いに関する従業員、契約相手

及び第三者の利用者の責任を明確にする

4.1.3.6 雇用条件には、組織での雇用の結果として、又は雇用の過程で作成された個人情報を含む、個人情報の扱いに関する組織の責任を含める

4.1.3.7 雇用条件には、組織の構外及び通常の勤務時間外に及ぶ責任（例えば、在宅勤務における責任）を含める

4.1.3.8 雇用条件には、従業員、契約相手及び第三者の利用者が組織のセキュリティ要求事項に従わない場合に取る処置を含める

4.1.3.9 従業員、契約相手及び第三者の利用者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

4.1.3.10 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、契約相手及び第三者の利用者によるアクセスの特性及び範囲に応じて、雇用条件を適切なものとする

4.1.3.11 雇用終了後も、定められた期間は雇用条件に含まれる責任を継続する

4.2 雇用期間中

目的：従業員、契約相手及び第三者の利用者の、情報セキュリティの脅威及び諸問題並びに責任及び義務に対する認識を確実なものとし、通常の業務の中で組織の情報セキュリティ基本方針を維持し、人による誤りのリスクを低減できるようにすることを確実にするため

4.2.1 経営陣は、組織の確立された方針及び手順に従ったセキュリティの適用を従業員、契約相手及び第三者の利用者に要求する

4.2.1.1 経営陣の責任には、従業員、契約相手及び第三者の利用者に、取扱いに慎重を要する情報又は情報システムへのアクセスを許可する前に、情報セキュリティの役割及び責任についての正確な伝達が確実になされる仕組みを整備することを含める

4.2.1.2 経営陣の責任には、従業員、契約相手及び第三者の利用者に、組織内での役割において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確実に提供する仕組みを整備することを含める

4.2.1.3 経営陣の責任には、従業員、契約相手及び第三者の利用者に、組織のセキュリティ方針に従うように確実に動機づけする仕組みを整備することを含める

4.2.1.4 経営陣の責任には、従業員、契約相手及び第三者の利用者が、組織内の役割及び責任に関連するセキュリティについての一定レベルの認識を確実に達成する仕組みを整備することを含める

4.2.1.5 経営陣の責任には、従業員、契約相手及び第三者の利用者が、組織の情報セキュリティ基本方針及び適切な仕事のやり方を含め、確実に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

4.2.1.6 経営陣の責任には、従業員、契約相手及び第三者の利用者が、適切な技能及び資格を確実に保持するようにする仕組みを整備することを含める

4.2.2 組織のすべての従業員並びに、関係するならば、契約相手及び第三者の利用者は、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・訓練を受け、また、定めに従ってそれを更新する

4.2.2.1 組織の方針や手順、職務の機能が変更になった場合には、組織のすべての従業員、関係する場合は契約相手及び第三者の利用者に対して、更新教育・訓練を行う

4.2.2.2 セキュリティの意識向上、教育及び訓練は、情報又はサービスへのアクセスを認可する

前に実施する

4.2.2.3 セキュリティの意識向上、教育及び訓練は、組織のセキュリティ方針及びねらいを紹介するために設計された正式な研修プロセスから開始する

4.2.2.4 セキュリティの意識向上、教育及び訓練には、情報処理設備の正しい利用（例えば、ログオン手順）、パッケージソフトウェアの利用及び懲戒手続に関する情報、セキュリティ要求事項、法的責任並びに実務管理を含める

4.2.2.5 セキュリティの意識向上、教育及び訓練には、既知の脅威、セキュリティに関する更なる助言を得るための窓口及び情報セキュリティインシデントのための適切な報告経路に関する情報を含める

4.2.3 セキュリティ違反を犯した従業員に対する正式な懲戒手続を備える

4.2.3.1 懲戒手続は、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

4.2.3.2 正式な懲戒手続は、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確実にするよう定める

4.2.3.3 正式な懲戒手続では、違反の内容及び重大さ並びにその業務上の影響、最初の違反か繰り返されたものか、違反者の教育・訓練の状況、関連法令、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

4.2.3.4 懲戒手続には、違法行為が重大な場合には、職権、アクセス権及び特権を直ちにはく（剥）奪できること、必要ならば、その現場から速やかに連れ出すことができることを盛り込む

4.3 雇用の終了又は変更

目的：従業員、契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため

4.3.1 雇用の終了又は変更の実施に対する責任は、明確に定め、割り当てる

4.3.1.1 雇用の終了に関する責任の伝達事項には、実施中のセキュリティ要求事項及び法的責任並びに、適切ならば、従業員、契約相手及び第三者の利用者の、雇用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

4.3.1.2 雇用終了後もなお有効な責任及び義務を、従業員、契約相手及び第三者の利用者の契約に含める

4.3.1.3 責任又は雇用の変更は、変更前の責任又は雇用の終了と、変更後の責任又は雇用の開始として管理する

4.3.2 すべての従業員、契約相手及び第三者の利用者は、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すべてを返却する

4.3.2.1 雇用終了時の手続には、前もって支給されたソフトウェア、会社のすべての書類及びすべての設備、その他の組織の資産（例えば、モバイルコンピューティング装置、クレジットカード、アクセスカード、ソフトウェア、手引書及び電子媒体）の返却を含める

4.3.2.2 雇用終了時の手続には、従業員、契約相手及び第三者の利用者が組織の設備を購入する場合には、すべての関連する情報を組織に返却し、設備から確実に消去することを含める

4.3.2.3 雇用終了時の手続には、個人所有の設備を業務に使用した場合には、すべての関連する情報を組織に返却し、設備から確実に消去することを含める

4.3.2.4　雇用終了時の手続には、従業員、契約相手及び第三者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、組織に引き継ぐことを含める

4.3.3　すべての従業員、契約相手及び第三者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

4.3.3.1　雇用終了時の手続には、情報システム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の見直しを行い、アクセス権を削除する必要性を判断することを含める

4.3.3.2　雇用の変更時には、変更後の業務では承認されていないすべてのアクセス権の削除を行う

4.3.3.3　雇用終了時の手続には、物理的又は論理的なアクセス権の削除に加えて、かぎ、身分証明書、情報処理設備及び署名及び組織の現行の一員であると認定する書類などの認証手段の返却若しくは削除を含める

4.3.3.4　辞めていく従業員、契約相手又は第三者の利用者が稼動中のアカウントのパスワードを知っている場合、雇用、契約若しくは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

4.3.3.5　情報資産及び情報処理施設へのアクセス権は、雇用の終了又は変更の前に、自己都合か経営陣側の都合か、雇用終了の理由、現時点での責任、アクセス可能な資産の価値などのリスク因子の評価に応じて、縮小又は削除する

5 物理的及び環境的セキュリティ

5.1 セキュリティを保つべき領域

目的：組織の施設及び情報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

5.1.1　情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いる

5.1.1.1　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とリスクアセスメントの結果に基づいて、それぞれの物理的境界の位置及び強度を定める

5.1.1.2　情報及び情報処理施設のある領域を保護するために、情報処理設備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、境界にはすき間がなく、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.敷地の外周壁を堅固な構造物とする

2.開閉制御の仕組み（例えば、かんぬき、警報装置、錠）によって、すべての外部に接する扉を、認可されていないアクセスから適切に保護する

3.要員が不在のときは扉及び窓に施錠する

4.窓（特に一階の窓）については、外部の脅威からの保護策を講ずる

5.1.1.3　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

5.1.1.4　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、物理的な障壁を設置する

5.1.1.5　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すべての防火扉を壁と関連させて、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の、警報機能を備え、監視し、試験を実施する

2.その防火扉が、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

5.1.1.6 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.すべ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の、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）では常に警報装置を作動させる

5.1.1.7 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設備を、第三者が管理する設備から物理的に分離する

5.1.1.8 情報及び情報処理施設のある領域を保護するために、セキュリティ境界内において、セキュリティ要求事項が異なる領域が存在する場合には、物理的アクセスを管理するための障壁及び境界を追加する

5.1.2 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

5.1.2.1 セキュリティを保つべき領域が認可されたもの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・時刻を記録する

5.1.2.2 セキュリティを保つべき領域が認可されたもの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、すべての訪問者を監督する

5.1.2.3 セキュリティを保つべき領域が認可されたものだけにアクセスを許すことを確実にするため、訪問者に、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、更に、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

5.1.2.4 セキュリティを保つべき領域が認可されたものだけにアクセスを許すことを確実にするため、取扱いに慎重を要する情報を処理又は保管する領域へのアクセスを管理し、認可された者だけに制限する

5.1.2.5 セキュリティを保つべき領域が認可されたものだけにアクセスを許すことを確実にするため、すべてのアクセスを認可し、その妥当性を確認するために、認証のための管理策（例えば、個人識別番号付のアクセス制御カード）を用いる

5.1.2.6 セキュリティを保つべき領域が認可されたものだけにアクセスを許すことを確実にするため、すべてのアクセスの監査証跡を、セキュリティを保って維持する

5.1.2.7 セキュリティを保つべき領域が認可されたものだけにアクセスを許すことを確実にするため、すべての従業員、契約相手及び第三者の利用者並びにすべての訪問者に、何らかの形式の、目に見える証明書の着用を求める

5.1.2.8 セキュリティを保つべき領域が認可されたもの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

かけた場合には、セキュリティ要員への迅速な連絡をさせる

5.1.2.9 セキュリティを保つべき領域が認可されたもの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、又は取扱いに慎重を要する情報処理施設への第三者のサポートサービス要員によるアクセスを、限定的に、必要時にだけ許可する

5.1.2.10 セキュリティを保つべき領域が認可されたもの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、又は取扱いに慎重を要する情報処理施設への第三者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、監視される

5.1.2.11 セキュリティを保つべき領域が認可されたもの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を定期的にレビューし、更新し、必要な時は無効にする

5.1.3 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

5.1.3.1 オフィス、部屋及び施設のセキュリティを保つための設計には、関連する安全衛生の規則及び標準に準拠する

5.1.3.2 オフィス、部屋及び施設の物理的な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ように設計する

5.1.3.3 オフィス、部屋及び施設のセキュリティを保つために、適用可能ならば、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

5.1.3.4 オフィス、部屋及び施設のセキュリティを保つために、取扱いに慎重を要する情報を処理する情報処理施設の場所を示す案内板及び内線電話帳は、一般の人が容易にアクセスできないように設計する

5.1.4 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による被害から物理的に保護する設計を行い、適用する

5.1.4.1 隣接する施設からもたらされるセキュリティ脅威（例えば、隣接建物の火災、屋根からの漏水、地下室の浸水、街路での爆発）から保護する

5.1.4.2 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ため、防災対策の設計において、危険な又は燃えやすい材料は、セキュリティを保つべき領域から安全な距離をおいて保管するようにする

5.1.4.3 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ため、防災対策の設計において、防災活動の障害となるおそれのある物若しくは災害を誘発又は拡大させる恐れのあるもの、例えば文房具のようなかさ張る在庫若しくは廃棄物などは、セキュリティを保つべき領域内に保管しないようにする

5.1.4.4 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ため、防災対策の設計において、緊急時のための予備装置及びバックアップ媒体は、主事業所の災害からの損傷を回避するために、安全な距離をおいて設置するようにする

5.1.4.5 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ため、防災対策の設計において、法令や条例などに定められた、適切な消火器具を備え、適切に配置するようにする

5.1.5 セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用する

5.1.5.1 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、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

5.1.5.2 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、安全面の理由のためと、悪意ある活動の機会を防止するためとの両面から、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を回避することを含める

5.1.5.3 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、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

5.1.5.4 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、セキュリティを保つべき領域への物品の持込、持ち出しを管理することを含める

5.1.5.5 セキュリティを保つべき領域での作業に関する物理的な保護及び指針の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯音楽端末やICレコーダ、カメラ付き携帯電話）の使用及び持込みについて、認可されたもの以外は、許可しないことを含める

5.1.6 一般の人が立ち寄る場所（例えば、荷物などの受渡場所）及び敷地内の認可されていない者が立ち入ることもある場所は、管理する。また、可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す

5.1.6.1 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある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を、識別・認可された要員に制限する

5.1.6.2 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある場所を管理するため、受渡場所で、配達要員が建物の他の場所にアクセスすることなく荷降ろしできるようにする

5.1.6.3 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある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でもセキュリティを保つ

5.1.6.4 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある場所を管理するため、入荷物について、受渡場所から使用場所へ移動する前に、潜在的な脅威を検査する

5.1.6.5 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある場所を管理するため、入荷物を、事業所へ持ち込むときに資産管理手順に従って登録する

5.1.6.6 一般の人が立ち寄る場所及び敷地内の認可されていない者が立ち入ることもある場所を管理するため、可能な場合には、入荷と出荷とは、物理的に分離した場所で扱う

5.2 装置のセキュリティ

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

5.2.1 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、又は保護する

5.2.1.1 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

5.2.1.2 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設備は、設備の使

用中に認可されていない者が情報をのぞき見るリスクを低減するように設置し、また、その視角を制限する

5.2.1.3 装置を保護するために、記憶装置に、認可されていないアクセスを回避するための物理的なセキュリティを確保する

5.2.1.4 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

5.2.1.5 装置を保護するために、潜在的な物理的脅威（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ための管理策を採用する

5.2.1.6 装置を保護するために、情報処理設備の周辺での飲食及び喫煙を制限する

5.2.1.7 装置を保護するために、情報処理設備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

5.2.1.8 装置を保護するために、すべての建物に、落雷からの保護手段を適用する。すべての電力及び通信の引込線に避雷器を装着する

5.2.1.9 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）の使用を採用する

5.2.1.10 装置を保護するために、電磁波などの放射による情報漏えいのリスクが最小限になるように、取扱いに慎重を要する情報を処理する装置を保護する

5.2.2 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

5.2.2.1 すべてのサポートユーティリティ（例えば、電気、給水、下水、暖房及び換気、空調）は、システムに十分なサポートを与えるよう、管理する

5.2.2.2 サポートユーティリティは、正しく機能することを確実にするため、及び不具合又は故障によるいかなるリスクをも低減するために、定期的に検査し、適切に試験する

5.2.2.3 サポートユーティリティに、装置の製造者の仕様に適合する適切な電力を供給する

5.2.2.4 重要な業務の運用をサポートする装置には、定められた手順での運転停止又は連続運転をサポートする、無停電電源装置（UPS）を設置する

5.2.2.5 電力についての緊急時対応計画には、無停電電源装置（UPS）が故障した場合のとるべき処置についても含める

5.2.2.6 長時間にわたる停電の場合でも処理の継続が要求される場合には、非常用発電機を導入する。また、非常用発電機の長時間運転を確実にするために、十分な燃料供給を確保する

5.2.2.7 無停電電源装置（UPS）及び非常用発電機を、十分な能力を保有していることを確実にするために定期的に点検し、装置の製造者の推奨に従って試験する

5.2.2.8 複数の電源又は事業所の規模が大きい場合には、別の変電設備を利用する

5.2.2.9 非常時に即座に電源を切ることができるように、電源を切るための緊急スイッチは、設備室の非常口近くに設置する。さらに、主電源の停電に備えて非常用照明を備える

5.2.2.10 主電源の停電に備えて非常用照明を備える

5.2.2.11 給水は、空調、加湿装置及び消防設備（使用している場合）に供給するために、安定的に十分に実施する

5.2.2.12 給水システムの不具合が、装置に損傷を与え又は消防設備を有効に作動させなくするた

め、サポートユーティリティの不具合を検知するための警報システムを、評価し、導入する

5.2.2.13 サポートユーティリティの提供業者との電話設備は、一つの接続経路の障害が音声サービスの途絶につながることのないように、少なくとも二つの異なった経路を保有する。音声サービスは、緊急連絡のための地域の法令の要求事項を満たすのに十分なものとする

5.2.3 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、傍受又は損傷から保護する

5.2.3.1 情報処理設備に接続する電源ケーブル及び通信回線は、可能な場合には、地下に埋設するか、又はそれに代わる十分な保護手段を施す

5.2.3.2 ネットワーク用ケーブル配線は、電線管の使用、又は公共の場所を経由する経路の回避などによって、認可されていない傍受又は損傷から保護する

5.2.3.3 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

5.2.3.4 取扱いの誤り（例えば、違うネットワークケーブルを不注意で接続する。）を最小限にするために、ケーブル及び装置を明確に識別するラベル付けを行う

5.2.3.5 ケーブル配線の間違いの可能性を減少させるために、文書化した配線表を使用する

5.2.3.6 取扱いに慎重を要する、又は重要なシステムは、外装電線管を導入し、点検箇所・終端箇所は施錠可能な部屋又は箱へ設置する

5.2.3.7 取扱いに慎重を要する、又は重要なシステムは、適切なセキュリティを提供する代替経路及び／又は伝送媒体を利用する

5.2.3.8 取扱いに慎重を要する、又は重要なシステムは、光ファイバケーブルを使用する

5.2.3.9 取扱いに慎重を要する、又は重要なシステムはケーブルを保護するため電磁遮へい（蔽）を利用する

5.2.3.10 取扱いに慎重を要する、又は重要なシステムは、ケーブルに取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

5.2.3.11 取扱いに慎重を要する、又は重要なシステムは、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

5.2.4 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とするために、正しく保守する

5.2.4.1 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、供給者の推奨する保守間隔及び仕様に従って保守する

5.2.4.2 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

5.2.4.3 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又は実際の故障のすべて、並びに予防及び是正のための保守のすべてについての記録を保持する

5.2.4.4 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によって、適切な管理策を実施する。必要な場合には、その装置から取扱いに慎重を要する情報を消去するか、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

5.2.4.5 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

すべての要求事項を順守する

5.2.5　構外にある装置に対しては、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

5.2.5.1　情報処理装置を組織の構外で使用する場合は、所有者がだれであるかに関係なく、経営陣の認可を得る

5.2.5.2　構外にも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

5.2.5.3　ポータブルコンピュータは、外出時には、手荷物として持ち運び、可能ならば外部からわからないようにする

5.2.5.4　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）に関する製造者の指示を常に守る

5.2.5.5　構外にある装置の保護のために、在宅作業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する。具体的には、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

5.2.5.6　構外の装置を保護するために、保険による十分な保証を備える

5.2.6　記憶媒体を内蔵した装置は、処分する前に、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、又は問題が起きないように上書きしていることを確実にするために、すべてを点検する

5.2.6.1　取扱いに慎重を要する情報を格納した装置は、物理的に破壊し、又はその情報を破壊、消去若しくは上書きする。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、元の情報を取り戻せなくなるようにする技術を利用する

5.2.7　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

5.2.7.1　資産を構外にもち出すことを許す権限をもつ従業員、契約相手及び第三者の利用者を、明確に特定する

5.2.7.2　装置のもち出し期限を設定し、また、返却がそのとおりであったか点検する

5.2.7.3　必要、かつ、適切な場合は、装置が構外にもち出されていることを記録し、また、返却時に記録する

6 通信及び運用管理

6.1 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

6.1.1　操作手順は、文書化し、維持する。また、その手順は、必要とするすべての利用者に対して利用可能にする

6.1.1.1　情報処理設備及び通信設備に関連するシステムの管理活動（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

6.1.1.2　情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記する

6.1.1.3　情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、バックアップを含む、各作業の詳細な実施に関する指示を明記する

6.1.1.4　情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、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、最早作業開始時刻と最遅作業完了時刻など）を含む、各作業の詳細な実施に関する指示を明記する

6.1.1.5 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、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、各作業の詳細な実施に関する指示を明記する

6.1.1.6 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記する

6.1.1.7 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、特別な出力及び媒体の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記する

6.1.1.8 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、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、各作業の詳細な実施に関する指示を明記する

6.1.1.9 情報処理設備及び通信設備に関連するシステムの管理活動の手順書には、監査証跡及びシステムログ情報の管理を含む、各作業の詳細な実施に関する指示を明記する

6.1.1.10 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扱い、その手順書の変更は、経営陣が認可する

6.1.1.11 情報システムは、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う

6.1.2 情報処理設備及びシステムの変更は、管理する

6.1.2.1 運用システム及び業務用ソフトウェアの変更を、厳格に管理する

6.1.2.2 運用システム及び業務用ソフトウェアの変更管理に、重要な変更の特定及び記録を含める

6.1.2.3 運用システム及び業務用ソフトウェアの変更管理に、変更作業の計画策定及びテスト実施を含める

6.1.2.4 運用システム及び業務用ソフトウェアの変更管理に、変更における潜在的な影響（セキュリティ上の影響を含む）のアセスメントを含める

6.1.2.5 運用システム及び業務用ソフトウェアの変更管理に、変更の申出を正式に承認する手順を含める

6.1.2.6 運用システム及び業務用ソフトウェアの変更管理に、すべての関係者への変更に関する詳細事項の通知を含める

6.1.2.7 運用システム及び業務用ソフトウェアの変更管理に、うまくいかない変更及び予期できない変更を、中止すること及び復旧させることに対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

6.1.2.8 装置、ソフトウェア又は手順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確立する

6.1.2.9 装置、ソフトウェア又は手順に対する変更がなされたときには、変更にかかわるすべての関連情報を含んだ監査ログを保持する

6.1.2.10 運用環境の変更は、その変更を実行するための正当な事業上の理由（システムへのリスク増加など）があるときだけ実施する

6.1.3　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、分割する

6.1.3.1　認可されていない状態又は気づかれない状態で、一人の利用者が資産に対してアクセス、修正又は使用ができないようにする

6.1.3.2　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割する

6.1.3.3　共謀のおそれがある場合は、共謀を防ぐ管理策（例えば、二人以上のかかわりを持たせる）の設計を行う

6.1.3.4　職務の分割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、経営陣による監督）を実施する

6.1.4　開発施設、試験施設及び運用施設は、運用システム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

6.1.4.1　運用上の問題を回避するために、運用環境、試験環境及び開発環境の間で分離のレベルを特定し、適切な管理策を導入する

6.1.4.2　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を明確に定め、文書化する

6.1.4.3　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の、異なる領域又はディレクトリで実行する

6.1.4.4　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

6.1.4.5　試験システム環境は、運用システム環境と可能な限り同等にする

6.1.4.6　運用システムと試験システムとでは、異なるユーザプロファイル（例えば、異なるユーザIDやパスワード）を用いる

6.1.4.7　誤操作によるリスクを低減するために、運用システムと試験システムを識別するための適切なメッセージをシステムのメニューなどに表示する

6.1.4.8　取扱いに慎重を要するデータの試験システム環境への複写を禁止する

6.1.4.9　開発システム、試験システム及び運用システムがネットワークで接続されている場合、その境界で適切なアクセス制限を実施する

6.2 第三者が提供するサービスの管理

目的：第三者の提供するサービスに関する合意に沿った、情報セキュリティ及びサービスの適切なレベルを実現し、維持するため

6.2.1　第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義、及び提供サービスレベルが、第三者によって実施、運用、及び維持されることを確実にする

6.2.1.1　第三者によるサービスの提供には、合意されたセキュリティの取決め、サービスの定義、及びサービスの管理を含める

6.2.1.2　外部委託契約の場合、組織は必要な外部委託先への移行内容（情報移行、情報処理施設の移行又はその他移行すべきもの）を計画する

6.2.1.3　外部委託契約の場合、移行期間を通してセキュリティの維持を確実にする仕組みを整備する

6.2.1.4　組織は、重大なサービス不具合又は災害の後においても、合意されたサービス継続レベルを維持す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、第三者が十分なサービス提供機能を維持することを確実にする仕組みを整備する

6.2.2　第三者が提供するサービス、報告及び記録は、常に監視し、レビューする。また、監査も定期的に実施する

6.2.2.1　合意における情報セキュリティの条件の順守を確実にするために、第三者が提供するサービスの監視及びレビューを実施する

6.2.2.2　第三者が提供するサービスの監視及びレビューにおいては、情報セキュリティのインシデント及び問題点の適切な管理を確実にする仕組みを整備する

6.2.2.3　合意の順守を点検するために、第三者が提供するサービスの実施レベルを監視する

6.2.2.4　第三者の作成したサービスの報告をレビューし、合意によって必要とされている定期進ちょく（捗）会合を設定する

6.2.2.5　第三者及び組織は、合意並びにすべての業務支援指針及び手順書で要求されるように、情報セキュリティインシデントの情報及びその情報のレビュー結果を提供する

6.2.2.6　第三者監査証跡並びにセキュリティ事象記録、運用上の問題点の記録、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

6.2.2.7　第三者が提供するサービスの監視及びレビューにおいては、識別された問題の解決及び管理を実施する

6.2.2.8　指定された個人又はサービス管理チームに、第三者との関係を管理する責任を割り当てる

6.2.2.9　組織は、順守状況の点検及び契約における要求事項の施行に対する責任を第三者に割り当てることを確実にする仕組みを整備する

6.2.2.10　契約における要求事項、特に情報セキュリティに関する要求事項を満足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

6.2.2.11　サービスの提供において不完全な点があった場合は、適切な処置をする

6.2.2.12　組織は、第三者が利用、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若しくは情報処理設備に対して、すべてのセキュリティの側面についての十分で包括的な管理及び可視性を維持する

6.2.2.13　組織は、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・対応）の可視性を維持することを確実にするために、報告プロセス、様式及び構成を明確に規定する

6.2.3　関連する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、サービス提供の変更（現行の情報セキュリティ方針、手順及び管理策の保守・改善を含む。）を管理する

6.2.3.1　第三者の提供するサービスに対する変更管理プロセスでは、現在提供されているサービスの強化のために、組織が行う変更を含める

6.2.3.2　第三者の提供するサービスに対する変更管理プロセスでは、新しい業務用ソフトウェア及びシステムの開発のために、組織が行う変更を含める

6.2.3.3　第三者の提供するサービスに対する変更管理プロセスでは、組織の諸方針及び諸手順の変更又は更新のために、組織が行う変更を含める

6.2.3.4　第三者の提供するサービスに対する変更管理プロセスでは、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管理策のために、組織が行う変更を含める

6.2.3.5 第三者の提供するサービスに対する変更管理プロセスでは、ネットワークに対する変更及び強化のために実施される第三者サービスにおける変更を含める

6.2.3.6 第三者の提供するサービスに対する変更管理プロセスでは、新技術の利用のために実施される第三者サービスにおける変更を含める

6.2.3.7 第三者の提供するサービスに対する変更管理プロセスでは、新製品又は新しい版及びリリースの採用のために実施される第三者サービスにおける変更を含める

6.2.3.8 第三者の提供するサービスに対する変更管理プロセスでは、新たな開発ツール及び開発環境を導入のために実施される第三者サービスにおける変更を含める

6.2.3.9 第三者の提供するサービスに対する変更管理プロセスでは、サービス設備の物理的設置場所の変更のために実施される第三者サービスにおける変更を含める

6.2.3.10 第三者の提供するサービスに対する変更管理プロセスでは、ベンダの変更のために実施される第三者サービスにおける変更を含める

6.3 システムの計画作成及び受入れ

目的：システム故障のリスクを最小限に抑えるため

6.3.1 要求されたシステム性能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

6.3.1.1 新規及び現在進行中の活動のために、容量・能力に関する要求事項を特定する

6.3.1.2 システムの可用性及び効率性を確実にするため、また、必要な場合には、改善のために、システム調整及び監視を適用する

6.3.1.3 適切な時点で問題を知らせるために、探知のための管理策を備える

6.3.1.4 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側される傾向を考慮し、将来必要とされる容量・能力を予測する

6.3.1.5 入手に時間又は費用がかかる資源については、特別な注意を要するため、管理者は、主要なシステム資源の使用を監視する

6.3.1.6 管理者は、使用の傾向、特に業務用ソフトウェア又は情報システムの管理ツールに関連した傾向を識別する

6.3.1.7 管理者は、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、潜在的な障害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、上記の監視及び識別の情報を利用して、適切な処置を立案する

6.3.1.8 容量及び能力が設計時の想定を超えた場合の対応手順を作成する

6.3.2 新しい情報システム及びその改訂版・更新版の受入れ基準を確立する。また、開発中及びその受入れ前に適切なシステム試験を実施する

6.3.2.1 新しいシステムを受け入れるための要求事項及び基準を明確に定義し、合意し、文書化し、試験することを確実にする仕組みを整備する

6.3.2.2 新しい情報システム、改訂版及び更新版は、正式な受入れの後、システムに組み込む

6.3.2.3 正式な受入れの決定前に、性能及びコンピュータの容量・能力の要求事項を確認する

6.3.2.4 正式な受入れの決定前に、誤りからの回復及び再起動の手順並びに障害対策計画を策定する

6.3.2.5 正式な受入れの決定前に、定められた標準類にのっとった通常の操作手順を準備し、確認する

6.3.2.6 正式な受入れの決定前に、合意された、備えているセキュリティ管理策群を確認する

6.3.2.7 正式な受入れの決定前に、手動による有効な手順を確認する

6.3.2.8 正式な受入れの決定前に、事業継続の取り決めを確認する

6.3.2.9 正式な受入れの決定前に、新しいシステムの導入が、既存のシステムに対して、特に処理が頂点に達したとき（例えば、月末）でも、悪影響を及ぼさないという証拠を確認する

6.3.2.10 正式な受入れの決定前に、新しいシステムが組織のセキュリティ全般に及ぼす影響について検討したという証拠を確認する

6.3.2.11 正式な受入れの決定前に、新しいシステムの操作又は利用に関する訓練を実施する

6.3.2.12 正式な受入れの決定前に、利用者の遂行能力に影響し、人間による誤りの回避につながる使い勝手を確認する

6.3.2.13 主要な新しいシステム開発においては、提案されているシステムの運用効率を確実にするために、開発プロセスのあらゆる段階で運用にかかわる関係者及び利用者から意見を聞く

6.3.2.14 すべての受入れ基準が完全に満たされていることを確認するために、適切な試験を実施する

6.3.2.15 セキュリティ要求事項に適切に対処していることを検証するため、受入れには正式な認証プロセス及び認定プロセスを導入する

6.4 悪意のあるコード及びモバイルコード[*3]からの保護

目的：ソフトウェア及び情報の完全性を保護するため

6.4.1 悪意のあるコードから保護するために、検出、予防及び回復のための管理策並びに利用者に適切に意識させるための手順を実施する

6.4.1.1 悪意のあるコードに対する検知・修復ソフトウェア、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、悪意のあるコードから保護する

6.4.1.2 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

6.4.1.3 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

6.4.1.4 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を、定めに従いレビューし、未承認のファイル又は認可されていない変更の存在に対しては、正式に調査する

6.4.1.5 電子的又は光学的媒体上のファイル及びネットワーク経由で入手したファイルに対する、悪意のあるコード検出のための使用前点検を実施する

6.4.1.6 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、悪意のあるコード検出のための使用前点検を、必要な場所（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 モバイルコードとは、あるコンピュータから別のコンピュータへ移動するソフトウェアであって、利用者とのやり取りがほとんどない、又はまったくない状態で自動的に起動し、特定の機能を実行するものをいう。

6.4.1.7 ウェブページに対する悪意のあるコード検出のための点検を実施する

6.4.1.8 保護内容が最新のものであることを確実にするために、定義ファイル及びスキャンエンジンの自動更新を行うよう、悪意のあるコードの対策ソフトウェアを設定する

6.4.1.9 システムにおける悪意のあるコードからの保護、保護策の利用方法に関する訓練、悪意のあるコード感染の報告、及び感染からの回復に関する管理の手順及び責任を明確にする

6.4.1.10 悪意のあるコード感染からの回復のための適切な事業継続計画を策定する

6.4.1.11 悪意のあるコード感染からの回復のための事業継続計画には、すべての必要なデータ及びソフトウェアのバックアップ並びに回復の手順を含める

6.4.1.12 常に情報を収集するための手順（例えば、新種の悪意のあるコードに関する情報を提供するメーリングリストへの登録及び／又はウェブサイトの確認）を定め、実施する

6.4.1.13 悪意のあるコード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手順を定め、実施する

6.4.1.14 管理者は、単なるいたずらと真の悪意のあるコード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又は悪意のあるコードの対策ソフトウェア供給業者）の利用を確実にする仕組みを整備する

6.4.1.15 管理者は、悪意のあるコードではなく、単なる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、すべての利用者に認識させる

6.4.2 モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行う。また、認可されていないモバイルコードを実行できないようにする

6.4.2.1 モバイルコードが許可されていない動作を実行することから保護するため、論理的に隔離された環境でモバイルコードを実行する

6.4.2.2 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードのいかなる利用も阻止する（例えば、電子メールソフトウェアにて、HTMLメールの表示、モバイルコードの使用又はメールのプレビューを禁止する。あるいはマクロ機能のある文書作成ソフトウェアにて、マクロの実行をデフォルトで禁止する又はマクロ実行時に警告を表示する）

6.4.2.3 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードの受取りを阻止する（例えば、WEBブラウザの設定で、認可されていないサイトのモバイルコードを実行できない設定を行う、認可されたWEBサイトのモバイルコードだけを実行する設定を行う）

6.4.2.4 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードが管理されていることを確実にする仕組みとして、特定のシステム上で利用可能なように、技術的な手段を作動させる

6.4.2.5 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードが利用可能な資源を管理する

6.4.2.6 モバイルコードが許可されていない動作を実行することから保護するため、モバイルコードを一意に認証するための暗号による管理策を利用する

6.4.2.7 自社で開発するモバイルコードには電子署名を付与する

6.5 バックアップ

目的：情報及び情報処理設備の完全性及び可用性を維持するため

6.5.1 情報及びソフトウェアのバックアップは、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

6.5.1.1 災害又は媒体故障の発生の後に、すべ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

6.5.1.2 情報のバックアップの必要なレベルを明確化する

6.5.1.3 バックアップ情報の正確で完全な記録及び文書化したデータ復旧手順を作成する

6.5.1.4 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

6.5.1.5 定期的なバックアップの取得について、仕様書、運用手順書などに含める

6.5.1.6 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

6.5.1.7 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

6.5.1.8 主事業所で媒体に適用している管理策は、バックアップ情報の保管場所にも適用する

6.5.1.9 バックアップファイルは、不正なアクセスによる改ざん、破壊、盗難などの脅威から、保護する

6.5.1.10 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

6.5.1.11 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

6.5.1.12 バックアップからの復旧手順は、有効であること、及び回復のための運用手順で定められた時間内に完了できることを確実にするために、定めに従って点検し試験する

6.5.1.13 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、個々のシステムにおけるバックアップの取決めを、定めに従って検査する

6.5.1.14 重要なシステムにおけ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すべてを対象とする

6.5.1.15 事業に不可欠な情報の保管期間及び永久保存する複製物に対する要求事項を決定する

6.5.1.16 バックアップ取得プロセス及び復元プロセスが自動化されている場合、それぞれのプロセスを導入前に試験し、導入後には定期的な間隔で試験する

6.6 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基盤の保護を確実にするため

6.6.1 ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御する

6.6.1.1 ネットワーク管理者は、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仕組みを整備する

6.6.1.2 適切と判断される場合には、ネットワークの運用責任を、コンピュータの運用から分離

する

6.6.1.3 遠隔地に所在する設備（利用者の領域に設置した設備を含む。）の管理に関する責任及び手順を確立する

6.6.1.4 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業務用ソフトウェアを保護するために、特別な管理策を確立する

6.6.1.5 セキュリティに関連した活動を記録できるように、適切なログ取得及び監視を適用する

6.6.1.6 サービスの最大限の活用及び管理策の情報処理基盤全体への一貫した適用の確実化のために、様々な管理作業を綿密に調整する

6.6.1.7 ネットワーク上の機器では、アクセス制御方針に基づき、すべてのネットワークインタフェースでアクセス制御を実施する

6.6.1.8 ネットワーク上の機器では、業務に使用していない空きポートへの接続を制限する

6.6.1.9 無線ネットワークを使用する場合、接続時認証には、安全とされている方式を使用する

6.6.1.10 ネットワーク上の不正なイベントを監視するため、侵入検知システムを導入する

6.6.1.11 侵入検知システムが、常に最新の攻撃・不正アクセスに対応可能なように、定義ファイル、検知ルールなどの更新を実施する

6.6.1.12 停止が許容できないシステムの場合、ネットワークを冗長化する

6.6.2 すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について、セキュリティ特性、サービスレベル及び管理上の要求事項を特定し、また、いかなるネットワークサービス合意書にもこれらを盛り込む

6.6.2.1 ネットワークサービス提供者が合意したサービスを、セキュリティを保って管理する能力を見定め、また、常に監視する

6.6.2.2 ネットワークサービスに対する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

6.6.2.3 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、ネットワークサービス提供者による対策の実施を確実にする仕組みを整備する

6.7 媒体の取扱い

目的：資産の認可されていない開示、改ざん、除去又は破壊及びビジネス活動の中断を防止するため

6.7.1 取外し可能な媒体の管理のための手順を備える

6.7.1.1 不要となることで組織の管理外となる媒体が再利用可能なものであるときは、格納している内容を回復不能とする

6.7.1.2 組織の管理外とする媒体のすべてについて、認可を要求する

6.7.1.3 媒体を組織の管理外とする措置のすべてについて、監査証跡の維持のために記録を保管する

6.7.1.4 すべての媒体を、製造者の仕様に従って、安全でセキュリティが保たれた環境に保管する

6.7.1.5 情報を媒体の寿命（製造者の仕様に従う。）よりも長く保管することが必要な場合、媒体の劣化による情報の消失を避けるために、その媒体に保管された情報を他の媒体に記録・保管する

6.7.1.6　データ消失の危険性を小さくするために、取外し可能な媒体を登録する

6.7.1.7　取外し可能な媒体のドライバは、その実行のための業務上の理由があるときにだけ有効とする

6.7.1.8　認可されない媒体の接続を防止するために、管理者以外がドライバのインストールやアンインストールをできない設定にする

6.7.1.9　取外し可能な媒体の管理に関わるすべての手順及び認可のレベルを、明確に文書化する

6.7.1.10　媒体への不必要なアクセスによる開示を防止するために、媒体内のデータをパスワードや暗号化により保護する

6.7.2　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ちかつ安全に処分する

6.7.2.1　取扱いに慎重を要する情報を格納した媒体のセキュリティを保ち、かつ、安全に保管し、処分する（例えば、焼却、消磁、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利用のためのデータ消去）

6.7.2.2　リース機器の返却や媒体の廃棄において、復元できないように情報の消去を確実にする仕組みを整備する（例えば、専用の消去ツールを用いる）

6.7.2.3　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

6.7.2.4　書類、装置及び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

6.7.2.5　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

6.7.2.6　処分のために媒体を集める場合、集積することによる影響に配慮し、手順に含める

6.7.2.7　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すべての媒体を処分する

6.7.3　情報の取扱い及び保管についての手順は、その情報を認可されていない開示又は不正使用から保護するために、確立する

6.7.3.1　情報の取扱い（すなわち、その情報の分類に応じた処理、保管及び通信）のための手順を策定する

6.7.3.2　情報の取扱いのための手順に、すべての媒体の、示された分類レベルによる取扱い及びラベル付けを含める

6.7.3.3　情報の取扱いのための手順に、認可されていない者のアクセスを防止するためのアクセス制限を含める

6.7.3.4　情報の取扱いのための手順に、認可されたデータ受領者の正式な記録の維持を含める

6.7.3.5　情報の取扱いのための手順に、入力データが完全であること、処理が適切に完了していること、及び出力の妥当性確認を行うことの確実化を含める

6.7.3.6　情報の取扱いのための手順に、出力待ちのために一時的に蓄積されたデータに対する、その取扱いの慎重度に応じた保護を含める

6.7.3.7　情報の取扱いのための手順に、製造者の仕様に従った、媒体の保管を含める

6.7.3.8　情報の取扱いのための手順に、データの配布先を最小範囲に限定することを含める

6.7.3.9　情報の取扱いのための手順に、認可された受領者の注意を求めるため、媒体の複製すべてに明確な表示を行うことを含める

6.7.3.10　情報の取扱いのための手順に、配布先及び認可された受領者の一覧表の定期的なレビューを含める

6.7.4 システム文書を認可されていないアクセスから保護する

6.7.4.1 セキュリティを保って、システム文書を保管する

6.7.4.2 システム文書へのアクセスを最小限に抑え、当該業務の管理者が認可する

6.7.4.3 関係者以外がシステム文書へアクセスできないように、パスワードによる制限や暗号化を行う

6.7.4.4 公衆ネットワーク上に保持されている、又は公衆ネットワークを経由して供給されるシステム文書を適切に保護する

6.8 情報の交換

目的：組織内部で交換した及び外部と交換した、情報及びソフトウェアのセキュリティを維持するため

6.8.1 あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備える

6.8.1.1 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、交換する情報を盗聴、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

6.8.1.2 情報交換のために電子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場合がある悪意のあるコードの検知及びそのコードからの保護における手順を反映する

6.8.1.3 情報交換のために電子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おける手順を反映する

6.8.1.4 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、通信設備の許容できる利用について規定した方針又は指針を反映する

6.8.1.5 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、特別なリスクが伴うことを考慮した、無線通信の利用における手順を反映する

6.8.1.6 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、従業員、契約相手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

6.8.1.7 情報交換のために電子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

6.8.1.8 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、関連する国家及び地域の法令及び規則に従った、すべての業務通信文（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

6.8.1.9 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、認可されていない者によるアクセスを防止する対策として、取扱いに慎重を要する又は重要な情報の印刷装置（例えば、複写機、プリンタ、ファクシミリ装置）上での放置禁止を含める

6.8.1.10 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、通信設備による転送（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

6.8.1.11 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、要員に、取扱いに慎重を要する情報の立ち聞き又は傍受を避けるための適切な予防策の実施が望ましいことの意識付けを行うことを含める。この予防策には、例えば、すぐ近くにいる人々、受話器若しくは電話回線への物理的なアクセス又は盗聴器の使用による盗聴、及び他の形式による傍受、電話を受けている人のそばの人々による立ち聞き又は傍受を避けることを含む

6.8.1.12 情報交換のために電子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、共有システムへの保管及び誤ダイアルによる間違った先への保管などを防止するため、取扱いに慎重を要する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

6.8.1.13 情報交換のために電子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

6.8.1.14 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、認可されていない利用のための収集を避けるために、個人を特定できるデータ（例えば、電子メールアドレス、その他の個人情報）を、いかなるソフトウェアにも登録しないように、要員に意識させることを含める

6.8.1.15 情報交換のために電子通信設備を利用するときに従う手順及び管理策には、ファクシミリ装置及びコピー機のデータ蓄積機能により、印刷紙又は通信に障害が起きた場合、その障害が回復したときに印刷可能にするためにデータを蓄えることを要員に意識させることを含める

6.8.1.16 公共の場所、又は出入りが自由なオフィス及び防音性のない壁で囲われた会議室では、機密の会話はしない方がよいことを要員に意識付ける

6.8.2 組織と外部組織との間の情報及びソフトウェアの交換について、両者間で合意を成立させる

6.8.2.1 情報交換に関する合意に、送信、発送及び受領についての管理並びにそれらの通知を行う責任を含める

6.8.2.2 情報交換に関する合意に、発信者、発送及び受領の通知における手順を含める

6.8.2.3 情報交換に関する合意に、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

6.8.2.4 情報交換に関する合意に、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

6.8.2.5 情報交換に関する合意に、預託条項を含める

6.8.2.6 情報交換に関する合意に、配達者の身元を確認する標準を含める

6.8.2.7 情報交換に関する合意に、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

6.8.2.8 情報交換に関する合意に、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

6.8.2.9 情報交換に関する合意に、個人データ、著作権及びソフトウェアライセンスの帰属を含

める

6.8.2.10 情報交換に関する合意に、個人データの保護、著作権及びソフトウェアのライセンスの順守並びに同様の考慮事項に対する責任を含める

6.8.2.11 情報交換に関する合意に、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

6.8.2.12 情報交換に関する合意に、取扱いに慎重を要するもの（例えば、暗号かぎ）を保護するために必要とされる場合、特別な管理策を含める

6.8.2.13 配送中の情報及び物理的な媒体を保護するための方針、手順及び標準類を確立し、維持する

6.8.2.14 情報交換による合意は、配送中の情報及び物理的な媒体を保護するための方針、手順並びに標準類を参照する

6.8.2.15 情報交換に関する、いかなる合意におけるセキュリティの事項も、関連する業務情報の取扱いの慎重度を反映する

6.8.3 情報を格納した媒体は、組織の物理的境界を越えた配送の途中における、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

6.8.3.1 事業所間で配送される情報媒体を保護するために、信頼できる輸送機関又は宅配業者を用いる

6.8.3.2 事業所間で配送される情報媒体を保護するために、認可されたすべての宅配業者について、管理者の合意を得る

6.8.3.3 事業所間で配送される情報媒体を保護するために、配達者の身元を確認する手順を導入する

6.8.3.4 事業所間で配送される情報媒体を保護するために、配送途中に生じるかも知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）を目的として、こん（梱）包を十分な強度とし、また、製造者の仕様（例えば、ソフトウェア向けの仕様）にも従う

6.8.3.5 事業所間で配送される情報媒体を保護するために、取扱いに慎重を要する情報を、認可されていない開示又は改ざんからの保護を目的として、施錠したコンテナを使用する

6.8.3.6 事業所間で配送される情報媒体を保護するために、取扱いに慎重を要する情報を、認可されていない開示又は改ざんからの保護を目的として、手渡しにて配送する

6.8.3.7 事業所間で配送される情報媒体を保護するために、取扱いに慎重を要する情報を、認可されていない開示又は改ざんからの保護を目的として、開封防止包装（開封を試みた場合、その証拠が残るもの）を利用する

6.8.3.8 事業所間で配送される情報媒体を保護するために、取扱いに慎重を要する情報を、認可されていない開示又は改ざんからの保護を目的として、特別な場合には貨物を複数に分割し、異なる経路で配送する

6.8.3.9 事業所間で配送される情報媒体を保護するために、取扱いに慎重を要する情報を媒体に格納する場合は、パスワードによるアクセス制限若しくは暗号化を行う

6.8.4 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

6.8.4.1 電子的メッセージ通信のためのセキュリティでは、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保護する

6.8.4.2　電子的メッセージ通信のためのセキュリティでは、正しい送付先及び送付手段（添付ファイルの暗号化、パスワードを設定するなど）を確実にする仕組みを整備する

6.8.4.3　電子的メッセージ通信のためのセキュリティでは、サービスの一般的な信頼性及び可用性を確保する

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

6.8.4.5　電子的メッセージ通信のためのセキュリティでは、だれ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、ファイル共有）の利用について、事前承認を得る

6.8.4.6　電子的メッセージ通信のためのセキュリティでは、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

6.8.4.7　重要な情報のやり取りに電子メールを使用する場合、暗号や電子署名の仕組みを導入する

6.8.5　業務用情報システムの相互接続と関連がある情報を保護するために、個別方針及び手順を策定し、実施する

6.8.5.1　業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、組織内の他の部門と情報を共有している管理システム及び会計システムにおける既知のぜい弱性を含める

6.8.5.2　業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、業務通信システムにおける情報のぜい弱性（例えば、通話又は電話会議の録音、通話の機密性、ファクシミリの保管、メールの開封、メールの配信）を考慮点として含める

6.8.5.3　業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、情報の共有を管理するための方針及び適切な管理策を考慮点として含める

6.8.5.4　業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムが適切なレベルの保護を提供しない場合の、取扱いに慎重を要する業務情報及び秘密文書の相互接続からの除外を考慮点として含める

6.8.5.5　業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別な者（例えば、重要な業務計画に従事している要員）が関係する業務日誌へのアクセスの制限を考慮点として含める

6.8.5.6　業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、システムの使用が許された要員、契約相手又は提携業者の区分、そこからシステムがアクセスされる場合がある場所を考慮点として含める

6.8.5.7　業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、特別の設備に対するアクセスの、特定の区分に属する利用者だけへの限定を考慮点として含める

6.8.5.8　業務用情報システムを相互接続することのセキュリティ及び業務への影響の識別には、利用者の地位の識別（例えば、他の利用者のために、組織又は契約相手の従業員として名簿に載っている者）を考慮点として含める

6.8.5.9　業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を

策定するためのリスクの分析には、システム内の情報の保持及びバックアップを考慮点として含める

6.8.5.10 業務用情報システムの相互接続と関連がある情報を保護するための個別方針及び手順を策定するためのリスクの分析には、緊急時に用いる代替手段についての要求事項及び取決めを考慮点として含める

6.9 電子商取引サービス

目的：電子商取引サービスのセキュリティ及びそれらサービスのセキュリティを保った利用を確実にするため

6.9.1 公衆ネットワークを経由する電子商取引に含まれる情報は、不正行為、契約紛争、認可されていない開示及び改ざんから保護する

6.9.1.1 電子商取引に関するセキュリティとして、各組織が主張する自らの身元についての、それぞれが要求する信頼（例えば、認証）のレベルを定める

6.9.1.2 電子商取引に関するセキュリティとして、価格の設定、重要な取引文書の発行又は重要な取引文書への署名をだれが行うかについての認可プロセスを明確にする

6.9.1.3 電子商取引に関するセキュリティとして、認可していることを取引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

6.9.1.4 電子商取引に関するセキュリティとして、重要な文書の機密性、完全性及び発送・受領の証明と、契約の否認防止とに関する要求事項及び対応手続（例えば、申込み手続、契約手続）を定める

6.9.1.5 電子商取引に関するセキュリティとして、公表された価格表の完全性（改ざんされていないこと）についての、信頼のレベルを定める

6.9.1.6 電子商取引に関するセキュリティとして、取扱いに慎重を要するデータ又は情報の機密性を確保する

6.9.1.7 電子商取引に関するセキュリティとして、注文取引、支払い情報、納入先のあて名情報並びに受領確認の機密性及び完全性を維持する

6.9.1.8 電子商取引に関するセキュリティとして、顧客から提供された支払い情報を確認するための適切な検査のレベルを定める

6.9.1.9 電子商取引に関するセキュリティとして、最も適切な支払いの決済形式を選択する

6.9.1.10 電子商取引に関するセキュリティとして、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

6.9.1.11 電子商取引に関するセキュリティとして、受注情報の紛失又は重複を防止する

6.9.1.12 電子商取引に関するセキュリティとして、不正な取引に関する賠償義務を明確にする

6.9.1.13 電子商取引に関するセキュリティとして、保険の要件を決定する

6.9.1.14 電子商取引に関する当事者間の合意は、権限（価格の設定、重要な取引文書の発行又は重要な取引文書への署名をだれが行うかについての認可プロセス）の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けする

6.9.1.15 情報サービス事業者と付加価値ネットワーク事業者との間に、合意を交わす

6.9.1.16 公開している電子商取引システムでは、その取引条件を顧客に公表する

6.9.1.17 電子商取引に用いる基幹コンピュータが持つ攻撃に対する耐性について、及び電子商取引の実施に必要とされるネットワーク相互接続のセキュリティ上の影響について確認す

る

6.9.1.18 電子商取引におけるすべての取引に関するログを取得し保存する

6.9.1.19 電子商取引において、リスクを低減するために、公開かぎ暗号及びディジタル署名を利用したセキュリティを保つ認証方法を利用するときは、信頼される第三者を利用する

6.9.2 オンライン取引に含まれる情報は、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

・認可されていない複製又は再生

6.9.2.1 オンライン取引のためのセキュリティとして、取引にかかわる各当事者は電子署名を利用する

6.9.2.2 オンライン取引のためのセキュリティとして、取引の種々の面で、すべての当事者の信任状は有効であり、かつ、検査を経ていることを確実にする仕組みを整備する

6.9.2.3 オンライン取引のためのセキュリティとして、取引の種々の面で、すべての当事者の信任状は有効であり、取引の種々の面での取引が機密性を保っていることを確実にする仕組みを整備する

6.9.2.4 オンライン取引のためのセキュリティとして、取引の種々の面で、すべての当事者に関係する個人情報を守っていることを確実にする仕組みを整備する

6.9.2.5 オンライン取引のためのセキュリティとして、かかわるすべての当事者間の通信経路を暗号化する

6.9.2.6 オンライン取引に含まれる情報を保護するために、かかわるすべ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

6.9.2.7 オンライン取引のためのセキュリティとして、取引の詳細情報を、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

6.9.2.8 オンライン取引のためのセキュリティとして、信頼できる専門機関を利用（例えば、ディジタル署名及び／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並びに／又は署名管理プロセスを通じてセキュリティを統合し、組み込む

6.9.2.9 採用される管理策の程度は、オンライン取引の形態それぞれに関係したリスクのレベルに相応させる

6.9.2.10 オンライン取引は、その取引の発生地、処理経由地、完了地及び／又は保管地の法域における、法令、規則、及び規制を順守する

6.9.3 認可されていない変更を防止するために、公開システム上で利用可能な情報の完全性を保護する

6.9.3.1 公開システム上で利用できるようにする、高いレベルでの完全性を要求するソフトウェア、データ及び関連情報は、適切な手段（例えば、ディジタル署名）で保護する

6.9.3.2 公開システムは、情報を利用できるようにする前及び定期的に、セキュリティ上の弱点

及び不具合について、試験する

6.9.3.3 情報を公開する前に、正式な承認の手続きをとる

6.9.3.4 外部からシステムに供給されるすべての入力を検証し、承認する

6.9.3.5 電子的情報公開システムについては、特に、それが情報のフィードバック及び直接入力を許すものである場合には、個人データ保護に関連するあらゆる法令を順守して、情報を収集する

6.9.3.6 電子的情報公開システムについては、特に、それが情報のフィードバック及び直接入力を許すものである場合には、情報公開システムに入力され、また、そこで処理される情報は、時機を失することなく、完全、かつ、正確に処理する

6.9.3.7 電子的情報公開システムについては、特に、それが情報のフィードバック及び直接入力を許すものである場合には、取扱いに慎重を要する情報は、収集、処理及び保管している間、保護する

6.9.3.8 電子的情報公開システムについては、特に、それが情報のフィードバック及び直接入力を許すものである場合には、情報公開システムにアクセスできても、そのシステムが接続しているネットワークへの意図しないアクセスは、許可しない

6.9.3.9 公開されているシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された法域、取引が行われている法域又はシステムの管理者が居住する法域の法令、規制及び規則を順守する

6.10 監視

目的：認可されていない情報処理活動を検知するため

6.10.1 利用者の活動、例外処理及びセキュリティ事象を記録した監査ログを取得し、また、将来の調査及びアクセス制御の監視を補うために、合意された期間、保持する

6.10.1.1 監査ログには、利用者IDを含める

6.10.1.2 監査ログには、主要な事象の日時及び内容（例えば、ログオン、ログオフ）を含める

6.10.1.3 監査ログには、可能な場合には、端末装置のID又は所在地を含める

6.10.1.4 監査ログには、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

6.10.1.5 監査ログには、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

6.10.1.6 監査ログには、システム構成の変更を含める

6.10.1.7 監査ログには、特権の利用を含める

6.10.1.8 監査ログには、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

6.10.1.9 監査ログには、アクセスされたファイル及びアクセスの種類を含める

6.10.1.10 監査ログには、ネットワークアドレス及びプロトコルを含める

6.10.1.11 監査ログには、アクセス制御システムが発した警報を含める

6.10.1.12 監査ログには、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

6.10.1.13 機密性の高い個人情報を含む監査ログに対して、適切な個人情報保護対策（例えば、暗号化やアクセス管理）を実施する

6.10.1.14 システムの実務管理者には、管理者自身の活動のログを編集、削除、又は停止する権限を付与しない

6.10.2 情報処理設備の使用状況を監視する手順を確立し、また、監視活動の結果を定めに従ってレビューする

6.10.2.1 個々の設備に対して要求される監視のレベルを、リスクアセスメントによって決定する

6.10.2.2 監視活動に適用できるすべての関連した法的要求事項を順守する

6.10.2.3 認可されているアクセスに関して、利用者IDを監視する

6.10.2.4 認可されているアクセスに関して、重要な事象の日時を監視する

6.10.2.5 認可されているアクセスに関して、事象の種類を監視する

6.10.2.6 認可されているアクセスに関して、アクセスされたファイルを監視する

6.10.2.7 認可されているアクセスに関して、使用されたプログラム・ユーティリティを監視する

6.10.2.8 すべての特権操作に関して、特権アカウント（例えば、スーパーバイザ、ルート、実務管理者）の使用を監視する

6.10.2.9 すべての特権操作に関して、システムの起動及び停止を監視する

6.10.2.10すべての特権操作に関して、入出力装置の取付け・取外しを監視する

6.10.2.11認可されていないアクセスの試みに関して、失敗した又は拒否した利用者による試みを監視する

6.10.2.12認可されていないアクセスの試みに関して、失敗した又は拒否した、データ及び他の資源に関連する試みを監視する

6.10.2.13認可されていないアクセスの試みに関して、ネットワークのゲートウェイ及びファイアウォールにおけるアクセス方針違反及びその通知を監視する

6.10.2.14認可されていないアクセスの試みに関して、自己の侵入検知システムが発する警告を監視する

6.10.2.15システムの警告又は不具合に関して、コンソールの警告又はメッセージを監視する

6.10.2.16システムの警告又は不具合に関して、システムログの例外処理を監視する

6.10.2.17システムの警告又は不具合に関して、ネットワーク管理の警報を監視する

6.10.2.18システムの警告又は不具合に関して、アクセス制御システムが発した警報を監視する

6.10.2.19システムの警告又は不具合に関して、システムセキュリティの設定及び管理策への変更又は変更の試みを監視する

6.10.2.20監視結果のレビュー頻度は、関係するリスクに応じて決定する

6.10.2.21監視結果のレビュー頻度決定時に考慮するリスク要因として、業務手続の重要度を含める

6.10.2.22監視結果のレビュー頻度決定時に考慮するリスク要因として、関係する情報の価値、取扱いに慎重を要する度合い又は重要度を含める

6.10.2.23監視結果のレビュー頻度決定時に考慮するリスク要因として、システムへの侵入及び不正使用の過去の経験並びに悪用されたぜい弱性の頻度を含める

6.10.2.24監視結果のレビュー頻度決定時に考慮するリスク要因として、システムの相互接続の範囲（特に公衆ネットワーク）を含める

6.10.2.25監視結果のレビュー頻度決定時に考慮するリスク要因として、停止させたログ機能を含める

6.10.3 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

6.10.3.1 記録されたメッセージ形式の認可されていない変更から保護する

6.10.3.2 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

6.10.3.3 事象記録の不具合又は過去の事象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

6.10.3.4 ログ情報は、専用のログサーバに保存し、他のサーバや機器とは論理的又は物理的に分離する

6.10.3.5 セキュリティ監視を目的として重要事象の識別を補助するために、ログファイルの調査や正当性確認を実施する適切なシステムユーティリティ又は監査ツールを使用する

6.10.4 システムの実務管理者及び運用担当者の作業を記録する

6.10.4.1 作業ログには、事象（成功又は失敗したもの）の発生時刻を記録する

6.10.4.2 作業ログには、事象に関する情報（例えば、扱ったファイル）又は不具合に関する情報（例えば、発生した誤り、とった是正処置）を記録する

6.10.4.3 作業ログには、関与したアカウント及び実務管理者又は運用担当者を記録する

6.10.4.4 作業ログには、関与したプロセスを記録する

6.10.4.5 システムの実務管理者及び運用担当者の作業ログを、定めに従ってレビューする

6.10.4.6 システム及びネットワークの実務管理者が規則を順守して活動していることを監視するために、システム及びネットワークの実務管理者の管理外にある侵入検知システムを利用する

6.10.5 障害のログを取得し、分析し、また、障害に対する適切な処置をとる

6.10.5.1 利用者又はシステムプログラムから報告された、情報処理又は通信システムの問題に関連する障害は、ログを取得する

6.10.5.2 報告された障害の取扱いについて、障害が完全に解決したことを確実にするための障害ログのレビューに関する明確な規則を策定する

6.10.5.3 報告された障害の取扱いについて、管理策が意味を失っていないこと及び実施する処置が完全に認可を得ることを確実にするための是正手段のレビューに関する明確な規則を策定する

6.10.5.4 システム機能が利用可能な場合には、エラーログ取得の機能を作動させる

6.10.5.5 個々のシステムに要求された記録のレベルは、パフォーマンスが低下することを考慮した上で、リスクアセスメントに基づいて決定する

6.10.6 組織又はセキュリティ領域内のすべての情報処理システム内のクロックは、合意された正確な時刻源と同期させる

6.10.6.1 コンピュータ又は通信装置に実時刻を表すクロック機能がある場合には、そのクロックは、合意された標準時（例えば、万国標準時（UTC）又は現地の標準時）に合わせる

6.10.6.2 クロックの有意な変化があるかどうかを点検し、それを修正する手順を策定する

6.10.6.3 タイムスタンプを実際の日時に反映することを確実にするため、地域の特性（例えば、夏時間）を考慮に入れ、日時についての記法に基づく正確な解釈を行う

6.10.6.4 記録システムのマスタクロックとして、国家の原子時計に基づく時報と同期したクロックを利用する

6.10.6.5 すべてのサーバをマスタクロックに同期させておくために、時刻同期プロトコル（Network time protocol:NTP）を利用する

7 アクセス制御

7.1 アクセス制御に対する業務上の要求事項

目的：情報へのアクセスを制御するため

7.1.1 アクセス制御方針は、アクセスについての業務上及び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

7.1.1.1 利用者ごと又は利用者のグループごとに対するアクセス制御規則及びアクセス権を、アクセス方針の中に明確に規定する

7.1.1.2 アクセス制御方針は、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立てる

7.1.1.3 利用者及びサービス提供者には、アクセス制御に適合する業務上の要求事項を明確に規定して提示する

7.1.1.4 アクセス制御方針に、個々の業務用ソフトウェアのセキュリティ要求事項を反映する

7.1.1.5 アクセス制御方針は、業務用ソフトウェアにかかわるすべての情報及びその情報が直面するリスクの識別を考慮して定める

7.1.1.6 アクセス制御方針には、情報の伝達及びアクセスの認可に対する方針（例えば、知る必要がある要員だけに知らせるとの原則、情報のセキュリティ水準、情報の分類）を含める

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

7.1.1.8 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保護に関連する法令及び契約上の義務を反映する

7.1.1.9 アクセス制御方針に、組織内の一般的な職務に対する標準的な利用者のアクセス権限プロファイルを含める

7.1.1.10 アクセス制御方針に、分散ネットワーク環境（例えばブランチ環境など、利用可能なすべての接続を認識しているネットワーク）におけるアクセス権の管理を含める

7.1.1.11 アクセス制御方針に、アクセス制御における役割の分割（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

7.1.1.12 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

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

7.1.1.14 アクセス制御方針に、アクセス権の削除の方針を含める

7.2 利用者アクセスの管理

目的：情報システムへの、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

7.2.1 すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備える

7.2.1.1 利用者の登録・登録削除のためのアクセス制御手順に、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

7.2.1.2 利用者の登録・登録削除のためのアクセス制御手順に、グループ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

7.2.1.3 利用者の登録・登録削除のためのアクセス制御手順に、利用者が情報システム又はサー

ビスの利用について、そのシステムの管理者から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経営陣から別の承認を受けることが適切な場合もある。）

7.2.1.4 利用者の登録・登録削除のためのアクセス制御手順に、許可したアクセスのレベルが、業務の目的に適していることの点検を含める

7.2.1.5 利用者の登録・登録削除のためのアクセス制御手順に、許可したアクセスのレベルが、組織のセキュリティ基本方針と整合していること（例えば、職務権限の分割に矛盾するおそれはないか。）の点検を含める

7.2.1.6 利用者の登録・登録削除のためのアクセス制御手順に、利用者に各自のアクセス権について記述した文書を発行することを含める

7.2.1.7 利用者の登録・登録削除のためのアクセス制御手順に、利用者に各自がアクセス条件を理解していることを示す文書に、署名を要求することを含める

7.2.1.8 利用者の登録・登録削除のためのアクセス制御手順は、認可手順が完了するまでサービス提供者が利用者にアクセスさせないようにすることが確実になるよう定める

7.2.1.9 利用者の登録・登録削除のためのアクセス制御手順に、サービスを利用するために登録されているすべての人の正式な記録の維持を含める

7.2.1.10 利用者の登録・登録削除のためのアクセス制御手順に、役割又は職務を変更した利用者、又は組織から離れた利用者のアクセス権の即座の解除、若しくは停止することを含める

7.2.1.11 利用者の登録・登録削除のためのアクセス制御手順に、必要のない利用者ID及びアカウントがないかの定期的な、点検、及び、削除又は停止することを含める

7.2.1.12 利用者の登録・登録削除のためのアクセス制御手順は、重複する利用者IDを別の利用者に発行しないことを確実にするよう定める

7.2.1.13 利用者のアクセス役割を、業務上の要求事項に基づいて確立する（利用者のアクセス役割とは、多くのアクセス権を典型的な利用者アクセス権限プロファイルとして要約したものである。）

7.2.2 特権の割当て及び利用は、制限し、管理する

7.2.2.1 認可されていないアクセスからの保護が必要な、利用者が複数のシステムでは、正式な認可プロセスによって特権の割当てを管理する

7.2.2.2 特権の割当ての正式な認可プロセスでは、各システム製品（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、各業務用ソフトウェア）に関連させた特権及び特権を割り当てる必要がある利用者を特定する

7.2.2.3 特権の割当ての正式な認可プロセスでは、特権は、アクセス制御方針に沿って、利用の必要性原則に則って（すなわち、利用者の機能上の役割が必要になった場合に限って、そのための最小限の要求事項に従い）割り当てる

7.2.2.4 特権の割当ての正式な認可プロセスでは、割り当てたすべての特権の認可プロセスを維持する

7.2.2.5 特権の割当ての正式な認可プロセスでは、割り当てたすべての特権の記録を維持する

7.2.2.6 特権の割当ての正式な認可プロセスでは、特権は、認可プロセスが完了するまで許可しない

7.2.2.7 利用者に対する特権の許可が必要ないように、システムルーチンの開発及び利用を促進する

7.2.2.8　特権での動作を必要としないプログラムの開発及び利用を推進する

7.2.2.9　特権は、通常の業務用途に利用される利用者IDとは別の利用者IDに割り当てる

7.2.3　パスワードの割当ては、正式な管理プロセスによって管理する

7.2.3.1　パスワードの割当ての正式な管理プロセスでは、パスワードの割当ては、個人のパスワード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、雇用契約書の中に含めてもよい）

7.2.3.2　パスワードの割当ての正式な管理プロセスでは、グループのパスワード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、雇用契約書の中に含めてもよい）

7.2.3.3　パスワードの割当ての正式な管理プロセスでは、利用者に自分で作ったパスワードを保持することを求める場合、最初に、直ちに変更しなければならないセキュリティを保った仮パスワードを発行する

7.2.3.4　パスワードの割当ての正式な管理プロセスでは、新規、更新又は仮のパスワードを発行する前に利用者の身元を確認する手順を確立する

7.2.3.5　パスワードの割当ての正式な管理プロセスでは、仮パスワードはセキュリティを保った方法で利用者に渡し、第三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）電子メールメッセージを利用することは避ける

7.2.3.6　パスワードの割当ての正式な管理プロセスでは、仮パスワードは一人一人に対して一意とし、推測されないものとする

7.2.3.7　パスワードの割当ての正式な管理プロセスでは、利用者に、パスワードの受領を報告させる

7.2.3.8　パスワードの割当ての正式な管理プロセスでは、パスワードは、保護されていない状態では決してコンピュータシステム上に保管しない

7.2.3.9　パスワードの割当ての正式な管理プロセスでは、ベンダがあらかじめ設定したパスワードは、システム又はソフトウェアエアのインストール後に変更する

7.2.3.10　パスワードを割当てる際に、パスワードの品質を確保する仕組みを導入する

7.2.3.11　パスワードの有効期限を設定する

7.2.4　管理者は、正式なプロセスを使用して、利用者のアクセス権を定められた間隔でレビューする

7.2.4.1　利用者のアクセス権は、定期的な間隔（例えば、6か月間隔）で見直す

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

7.2.4.3　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（例えば、3か月間隔）でレビューする

7.2.4.4　特権の割当てを定期的に点検して、認可されていない特権が取得されてないことを確実にする

7.2.4.5　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取る

7.3 利用者の責任

目的：認可されていない利用者のアクセス並びに情報及び情報処理設備の損傷又は盗難を防止するため

7.3.1　パスワードの選択及び利用時に、正しいセキュリティ慣行に従うことを、利用者に要求する

7.3.1.1　すべての利用者に、パスワードを秘密にしておくよう助言する

7.3.1.2　すべての利用者に、パスワードを記録して保管しないよう助言する（例えば、紙、ソフトウェアのファイル又は携帯用のデバイスへの記録。ただし、記録がセキュリティを確保して保管され、保管方法が承認されている場合には、その限りではない。）

7.3.1.3　すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合には、パスワードを変更するよう助言する

7.3.1.4　すべての利用者に、十分な最短文字数をもつ質の良いパスワードを選択するよう助言する（質の良いパスワードとは、次の条件を満たすものである。①覚えやすい、②例えば、名前、電話番号、誕生日など、当人の関連情報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辞書に含まれる語から成り立っておらず、辞書攻撃にぜい弱でない、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ない）

7.3.1.5　すべての利用者に、パスワードは、定期的な間隔で、又はアクセス回数に基づいて変更するよう助言する

7.3.1.6　特権を許可した利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するよう助言する

7.3.1.7　すべての利用者に、古いパスワードを再利用したり、循環させて利用したりしないよう助言する

7.3.1.8　仮パスワードを発行する場合、すべての利用者に、最初のログオン時点で変更するよう助言する

7.3.1.9　すべての利用者に、自動ログオンプロセスにパスワードを含めない（例えばマクロ又は機能キーにパスワードを記憶させない）よう助言する

7.3.1.10　すべての利用者に、個人用のパスワードを共有しないよう助言する

7.3.1.11　すべての利用者に、業務目的の認証と業務目的以外の認証に同じパスワードを使用しないよう助言する

7.3.1.12　紛失又は失念したパスワードを扱うヘルプデスクシステムは、パスワードシステムへの攻撃の手段になる可能性もあるため、利用権限や承認手続きなどの管理には特別な注意を払う

7.3.1.13　利用者が複数のサービス、システム又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、それぞれのサービス、システム又はプラットフォームの中で保管したパスワードに対する適切な保護が確立していることを利用者に保証しているときは、一つの質の良いパスワードを用いてもよいことを利用者に提示する

7.3.2　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

7.3.2.1　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、すべての利用者に認識させる

7.3.2.2　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構によって保護されている場合はその限りではない）

7.3.2.3 利用者に、処理が終了したら、はん用大型コンピュータ、サーバ及びオフィスのパーソナルコンピュータをログオフするよう助言する（パーソナルコンピュータ画面又は端末の電源を切るだけで済ませない。）

7.3.2.4 利用者に、パーソナルコンピュータ又は端末を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

7.3.3 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[*4]

7.3.3.1 クリアデスク・クリアスクリーン方針は、情報の分類、法令及び契約上の要求事項並びに組織の抱えるそれらに対応するリスク及び文化的側面を考慮して定める

7.3.3.2 取扱いに慎重を要する又は重要な業務情報を含む電子記憶媒体及び紙媒体は、必要のない場合、特にオフィスにだれもいないときには、施錠して（理想的には金庫若しくは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

7.3.3.3 コンピュータ及び端末は、離席時には、ログオフ状態にしておく、又はパスワード、トークン若しくは類似の利用者認証機構で管理されたスクリーン及びキーボードのロック機構によって保護する

7.3.3.4 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

7.3.3.5 郵便物の受渡場所及び無人状態のファクシミリ装置を保護する

7.3.3.6 コピー機及びスキャナやデジタルカメラなどその他の記録再生技術の利用は認可されている場合を除き、防止する

7.3.3.7 取扱いに慎重を要する情報又は機密扱い情報を含む文書を印刷した場合は、プリンタから即刻取り出す

7.4 ネットワークのアクセス制御

目的： ネットワークを利用したサービスへの認可されていないアクセスを防止するため

7.4.1 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供する

7.4.1.1 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

7.4.1.2 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、だれ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

7.4.1.3 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、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

7.4.1.4 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、インターネットサービス提

---

*4 クリアデスクは、机上に書類を放置しないことである。また、クリアスクリーンは、情報をスクリーンに残したまま離席しないことである。

供者又は遠隔システムへのダイヤルアップ接続を許可するための条件）を対象にする

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

7.4.2　遠隔利用者のアクセスを管理するために、適切な認証方法を利用する

7.4.2.1　遠隔利用者の認証は、暗号に基づく技術、ハードウェアトークン、チャレンジ－レスポンス・プロトコルなどのパスワードよりもなりすましに強い方法を用いて達成する（このような技術を利用した実現可能な導入は、種々の仮想私設網（VPN）ソリューションに見ることができる。専用私設回線も、接続元の確認に使うことができる。）

7.4.2.2　公衆回線網を用いる場合、認可されていない接続及び好ましくない接続から、組織の情報処理設備を保護するためコールバックの手順及び制御（例えば、コールバックモデムの利用、発信者番号での認証）を整備する

7.4.2.3　コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いない。もし、転送機能をもつネットワークサービスの手順及び制御を用いる場合は、転送にかかわる弱点を避けるために、この機能の利用を禁止する

7.4.2.4　コールバックの手順及び制御を用いるとき、コールバックプロセスでは、実際の回線切断を組織側で確実に行う

7.4.2.5　コールバックの手順及び制御を用いるとき、コールバックプロセスにおいて組織側の回線切断が確実に実行されるよう、手順及び制御を徹底的に試験する

7.4.2.6　無線ネットワークを使用する場合は、ネットワークトラフィックの探知されない傍受及び挿入の機会が増大するので、追加の認証管理策を導入する

7.4.2.7　遠隔利用者からの接続のログ（認証ログ及び接続ログ）を取得する

7.4.2.8　遠隔利用者のグループがセキュリティを保った共有コンピュータ設備に接続するとき、そのグループを認証するための代替手段としてノード認証を利用する場合は、暗号技術（例えば、機器証明書に基づくもの）を用いた認証手段を用いる

7.4.3　特定の場所及び装置からの接続を認証するための手段として、自動の装置識別を考慮する

7.4.3.1　一つ以上のネットワークが存在して、特にそれらのネットワークの取扱い慎重度が異なる場合には、装置に内蔵された又は附属した識別子により、その装置がどのネットワークへの接続を許可されているかを明確にする

7.4.3.2　装置識別子のセキュリティを維持するために、必要に応じて装置の物理的な保護策を導入する

7.4.3.3　必要に応じて、利用者の認証に追加して、装置の自動識別を導入する

7.4.4　診断用及び環境設定用ポートへの物理的及び論理的なアクセスは、制御する

7.4.4.1　遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、施錠を利用する

7.4.4.2　遠隔診断用及び環境設定用のポートへのアクセスに対する管理策として、ポートへの物理的なアクセスを制御するサポート手順を利用する

7.4.4.3　コンピュータ又はネットワーク設備上に導入されたサービス、ポート及び類似の設備で、業務機能に特に必要でないものは、動作しないようにするか、又は除去する

7.4.4.4　ハードウェア及びソフトウェアのサポート手順には、保守要員との間で合意できた場合にだけ、遠隔診断用及び環境設定用のポートへのアクセスを可能にすることを確実にすることを含める

7.4.5　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、グループごとに分割する

7.4.5.1　大規模なネットワークのセキュリティを制御するために、必要に応じてネットワークを幾つかの論理的ネットワーク領域（例えば、組織の内部ネットワーク領域及び外部ネットワーク領域）に分割し、分割した個々の領域を、明確に定められたセキュリティ境界によって保護する

7.4.5.2　異なる論理的ネットワーク領域は、リスクアセスメント結果及びそれぞれの領域内の異なるセキュリティ要求事項に基づき、セキュリティレベル別の管理策群を適用して、ネットワークセキュリティ環境を更に分割（例えば、公開されているシステム、内部ネットワーク、重要な資産のように分割）する

7.4.5.3　異なる論理的ネットワーク領域の境界には、相互に接続する二つの領域間のアクセス及び情報の流れを制御するために、セキュリティゲートウェイを導入する

7.4.5.4　異なる論理的ネットワーク領域間に導入するゲートウェイは、領域間の通信をフィルタにかけ、また、認可されていないアクセスを組織のアクセス制御方針に従って阻止するように構成する（この種のゲートウェイの一例としては、一般にファイアウォールと呼ばれるものがある。論理的領域を分割する他の方法としては、組織内の利用者グループに対して仮想私設網を使ってネットワークアクセスを制限するものがある。）

7.4.5.5　無線ネットワークは、内部ネットワーク及び私設のネットワークから分割する

7.4.5.6　無線ネットワークを使用する場合は、ネットワーク境界を明確にすることは容易ではないため、リスクアセスメントを実施し、ネットワーク分割を維持する管理策（例えば、強い認証、暗号方式、周波数選択）を特定する

7.4.6　共有ネットワーク、特に、組織の境界を越えて広がっているネットワークについて、アクセス制御方針及び業務用ソフトウェアの要求事項に沿って、利用者のネットワーク接続能力を制限する

7.4.6.1　利用者のネットワークへのアクセス権は、アクセス制御方針の要求に従って、維持し更新する

7.4.6.2　利用者の接続（例えば電子メールのようなメッセージ通信、ファイル転送、対話型アクセス、業務用ソフトウェアによるアクセス）は、事前に定められた表又は規則によって通信をフィルタにかける、ネットワークゲートウェイによって制限する

7.4.6.3　ネットワークへのアクセスを一日の中の一定の時間又は一定の日に制限する

7.4.7　コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、ルーティング制御の管理策をネットワークに対して実施する

7.4.7.1　経路指定の制御は、通してよい発信元及びあて先のアドレスを点検する機構（ポジティブリスト方式）に基づいて実施する

7.4.7.2　プロキシ及び／又はネットワークアドレス変換を採用する場合には、内部及び外部のネットワーク制御を行う箇所において、発信元及びあて先のアドレスが正当であることを確認するために、セキュリティゲートウェイを利用する

7.4.7.3　セキュリティゲートを利用してネットワーク制御を行う場合は、配置された機構の強度及び欠点を識別する

7.4.7.4　ネットワーク経路を指定した制御に対する要求事項は、アクセス制御方針に基づいて定める

7.5 オペレーティングシステムのアクセス制御

目的：オペレーティングシステムへの、認可されていないアクセスを防止するため

7.5.1 オペレーティングシステムへのアクセスは、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

7.5.1.1 オペレーティングシステム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危険性を最小限に抑えるように設計する

7.5.1.2 適切なログオン手順として、システム又は業務用ソフトウェアの識別子を、ログオン手順が正常に終了するまで表示しない

7.5.1.3 適切なログオン手順として、「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

7.5.1.4 適切なログオン手順として、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

7.5.1.5 適切なログオン手順として、ログオン情報の妥当性検証は、利用者ＩＤ、パスワードなどのすべてのデータの入力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

7.5.1.6 適切なログオン手順として、許容できるログオンの試みの失敗回数（例えば、3回）を制限する

7.5.1.7 適切なログオン手順として、ログオンの失敗した試み及び成功した試みを記録する

7.5.1.8 適切なログオン手順として、ログオンの試みが許容回数に達した場合に、次のログオンの試みが可能となるまでの間隔の設定、又は特別な認可なしで引き続き行われる試みを拒否する

7.5.1.9 適切なログオン手順として、ログオン失敗時にデータリンク接続の切断をする

7.5.1.10 適切なログオン手順として、ログオンの試みが許容回数に達した場合は、警告メッセージをシステムコンソールに送信する

7.5.1.11 適切なログオン手順として、パスワードの最小文字数及び防御されるシステムの価値によってパスワードの再試行できる回数を設定する

7.5.1.12 適切なログオン手順として、ログオン手順のために許容される最長時間及び最短時間を制限する

7.5.1.13 適切なログオン手順として、ログオン手順のために許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了する

7.5.1.14 適切なログオン手順として、ログオンが正常にできた時点で、前回の正常にログオンできた日時を表示する

7.5.1.15 適切なログオン手順として、ログオンが正常にできた時点で、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

7.5.1.16 適切なログオン手順として、入力したパスワードは表示しない、又は記号でパスワードの文字を隠す

7.5.1.17 適切なログオン手順として、チャレンジ－レスポンス方式などの、パスワードが平文で通信されないような認証方式を用いる

7.5.2 すべての利用者は、各個人の利用ごとに一意な識別子（利用者ID）を保有する。また、利用者が主張する同一性を検証するために、適切な認証技術を選択する

7.5.2.1 利用者の識別及び認証の管理策は、利用者のすべてのタイプ（例えば、技術サポート要員、操作員、ネットワーク実務管理者、システムプログラマ、データベース実務管理者）に適用する

7.5.2.2 利用者IDは、責任をもつ個人の活動を追跡するために用いる

7.5.2.3 一般権限の利用者の活動は、特権権限のアカウントからでなく、一般権限のアカウントから実施する

7.5.2.4 明らかに業務上の利点がある例外的状況においては、利用者のグループ又は特定の業務に対して共有利用者IDを用いる場合、管理者の承認を文書で得る

7.5.2.5 利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、責任の追跡性を維持するための追加の管理策を導入する

7.5.2.6 個人によるジェネリックID（使用が特定の利用者に限定されない識別子）の使用は、そのIDによって利用可能な機能又は実行された行動を追跡する必要がない（例えば、読出し専用アクセス）か、又は他の適切な管理策（例えば、ジェネリックIDのためのパスワードを一度に一人の要員だけに発行し、その使用事例のログを取る。）がある場合に限って、許可する

7.5.2.7 高度な認証及び識別が必要な場合には、パスワードに代わる認証手段（例えば、暗号による手段、ICカード、トークン、生体認証による手段）を使用する

7.5.3 パスワードを管理するシステムは対話式にし、また、良質なパスワードを確実とするものにする

7.5.3.1 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とパスワードとを使用させるようにする

7.5.3.2 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又は変更を許可し、さらに、入力誤りを考慮した確認手順を組み入れる

7.5.3.3 パスワードの管理システムでは、質のよいパスワードを選択させるようにする

7.5.3.4 パスワードの管理システムでは、パスワードを変更させるようにする

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

7.5.3.6 パスワードの管理システムでは、以前の利用者パスワードの記録を維持し再使用を防止する

7.5.3.7 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

7.5.3.8 パスワードの管理システムでは、パスワードファイルを、業務用ソフトウェアシステムのデータとは別に保存する

7.5.3.9 パスワードは保護した形態（例えば、暗号化、ハッシュ値）で保存し、伝達する

7.5.4 システム及び業務用ソフトウェア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

7.5.4.1 システムユーティリティ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

7.5.4.2 システムユーティリティは、業務用ソフトウェアと分離する

7.5.4.3 システムユーティリティの使用は、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制限する

7.5.4.4　システムユーティリティを臨時に使用する場合の認可手順を整備する

7.5.4.5　システムユーティリティの使用を制限する（例えば、認可されたシステム変更のための期間での利用）

7.5.4.6　システムユーティリティのすべての使用のログを取得する

7.5.4.7　システムユーティリティの認可レベルを明確にし、文書化する

7.5.4.8　不要なユーティリティソフトウェア及びシステムソフトウェアはすべて除去又は無効化する

7.5.4.9　職務の分割が必要な場合には、システム上の業務用ソフトウェアへのアクセス権をもつ利用者に対して、システムユーティリティの使用を禁止する

7.5.5　一定の使用中断時間が経過したときは、使用が中断しているセッションを遮断する

7.5.5.1　セッションのタイムアウト機能は、一定の使用中断時間の経過後にセッションの画面を閉じ、さらに（おそらくは間隔をおいて）、業務用ソフトウェアとネットワーク接続を共に閉じる

7.5.5.2　セッションのタイムアウトまでの時間は、領域のセキュリティリスク、取り扱っている情報及び使用している業務用ソフトウェアの重要性並びに装置の利用者に関連するリスクを反映する

7.5.6　リスクの高い業務用ソフトウェアに対しては、更なるセキュリティを提供するために、接続時間の制限を利用する

7.5.6.1　取扱いに慎重を要する業務用ソフトウェアに対して、特にリスクの高い場所（例えば、組織のセキュリティマネジメントの及ばない一般の人が立ち入る場所又は外部の領域）からの利用を考慮して、接続時間の制御方針を定める

7.5.6.2　接続時間の制御は、予め時間帯（例えば、バッチファイル伝送のための時間帯）を定めておく、通常の対話型接続を短時間を行う、接続時間を通常の就業時間内とする（残業時間又は延長時間の運転の要求がない場合）、時間間隔をおいて再認証を要求するなどの方法で行う

7.6 業務用ソフトウェア及び情報のアクセス制御

目的：業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため

7.6.1　利用者及びサポート要員による情報及び業務用ソフトウェアシステム機能へのアクセスは、既定のアクセス制御方針に従って、制限する

7.6.1.1　情報及び業務用ソフトウェアシステム機能へのアクセスは、組織のアクセス制御方針と、個々の業務用ソフトウェアの要求事項に基づいて、制限する

7.6.1.2　アクセス制限の要求事項を満たすために、業務用ソフトウェア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

7.6.1.3　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

7.6.1.4　アクセス制限の要求事項を満たすために、他の業務用ソフトウェアからのアクセスを制御する

7.6.1.5　取扱いに慎重を要する情報を処理する業務用ソフトウェアシステムからの出力は、その出力の使用に関連した情報だけを含めることを確実にする仕組みを整備する

7.6.1.6　取扱いに慎重を要する情報を処理する業務用ソフトウェアシステムからの出力は、その

出力を認可されている端末装置及び場所だけに送ることを確実にする仕組みを整備する

7.6.1.7 取扱いに慎重を要する情報を処理する業務用ソフトウェアシステムからの出力は、冗長な情報を取り除くことを確実にするために、定期的にレビューする

7.6.2 取扱いに慎重を要するシステムは、専用の（隔離された）コンピュータ環境をもつ

7.6.2.1 取扱いに慎重を要するシステムの隔離のため、業務用ソフトウェアシステムの取扱い慎重度は、業務用ソフトウェアの責任者が明確に特定し、文書化する

7.6.2.2 取扱いに慎重を要する業務用ソフトウェアを共有環境で用いる場合、そのシステムの管理者は、資源とリスクを共有する業務用ソフトウェアシステムを認識した上で、そのリスクの受容を判断する

7.7 モバイルコンピューティング及びテレワーキング[*5]

目的：モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため

7.7.1 モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するために、正式な方針を備えなければならず、また、適切なセキュリティ対策を採用する

7.7.1.1 モバイルコンピューティング方針は、保護されていない環境におけるモバイルコンピューティング装置を用いた作業のリスクを考慮して定める

7.7.1.2 モバイルコンピューティング方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウィルス対策についての要求事項などを含める

7.7.1.3 モバイルコンピューティング方針には、モバイル設備をネットワークに接続する場合の規則及び助言並びに公共の場所でモバイル設備を使用する場合の手引を含める

7.7.1.4 公共の場所でモバイル設備を使用する場合の手引には、認可されていない者による盗み見のリスクを避けるように注意し、防止することを含める

7.7.1.5 モバイルコンピューティング設備では、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、物理的に保護するよう教育し、重要度の高い、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないよう助言する

7.7.1.6 モバイルコンピューティング設備に保管され、処理される情報について、認可されていないアクセス及び漏えいを防止するため、例えば、暗号技術のような保護を備える

7.7.1.7 モバイルコンピューティングでは、悪意のあるソフトウェアに対抗する手順を最新のものに保ち、備える

7.7.1.8 モバイルコンピューティングでは、重要性の高い業務情報のバックアップを定期的に取る

7.7.1.9 モバイルコンピューティングでは、情報を素早く容易にバックアップできる装置を利用可能にする

7.7.1.10 モバイルコンピューティングのバックアップは、情報の盗難、喪失などから、十分な保護をする

---

*5 モバイルコンピューティングとは、移動中又は外出先でコンピュータを利用することであり、テレワーキングとは、要員が、自分の所属する組織の外の決まった場所で、通信技術を用いて作業することである。

7.7.1.11 モバイルコンピューティングの設備を用いた、公衆ネットワークを経由しての業務情報への遠隔アクセスのために、識別及び認証と適切なアクセス制御機構を備える

7.7.1.12 モバイルコンピューティング設備の盗難又は紛失の場合の対策のために、法規定、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

7.7.1.13 モバイルコンピューティング設備で、重要度の高い、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、可能な場合には、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いる

7.7.1.14 モバイルコンピューティングを用いる要員に対する、その作業形態に起因するリスク及び実施すべき管理策についての教育・訓練を計画し、実施する

7.7.1.15 モバイルネットワークの無線接続に関する管理手順を定める

7.7.2 テレワーキングのための方針、運用計画及び手順を策定し、実施する

7.7.2.1 テレワーキング活動は、適切なセキュリティの取決め及び管理策を備え、かつ、これらが組織のセキュリティ基本方針に適合している場合にのみ認可する

7.7.2.2 テレワーキングの場所に適切な保護（例えば、装置及び情報の盗難、情報の認可されていない開示、遠隔地から組織の内部システムへの認可されていないアクセス、設備の不正使用に対するもの）を備える

7.7.2.3 テレワーキングの活動は、経営陣が認可し管理する

7.7.2.4 テレワーキングのための方針、運用計画及び手順に、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物理的なセキュリティの状況の確認を含める

7.7.2.5 テレワーキングのための方針、運用計画及び手順に、提案された物理的なテレワーキングの環境の確認を含める

7.7.2.6 テレワーキングのための方針、運用計画及び手順に、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の確認を含める

7.7.2.7 テレワーキングのための方針、運用計画及び手順は、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

7.7.2.8 テレワーキングのための方針、運用計画及び手順は、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

7.7.2.9 テレワーキングのための方針、運用計画及び手順は、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個別方針及び手順を考慮して定める

7.7.2.10 テレワーキングのための方針、運用計画及び手順は、個人所有の装置へのアクセス（装置のセキュリティ点検のためのもの、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、法律が禁じている場合がある

7.7.2.11 テレワーキングのための方針、運用計画及び手順は、ソフトウェアの使用許諾に関する取決め（例えば、従業員、契約相手又は第三者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）を考慮して定める

7.7.2.12 テレワーキングのための方針、運用計画及び手順は、ウィルス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

7.7.2.13 テレワーキングの指針及び取決めに、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

7.7.2.14 テレワーキングの指針及び取決めに、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

7.7.2.15 テレワーキングの指針及び取決めに、遠隔アクセスを安全にする方法も含め、適切な通信装置の用意に関する事項を含める

7.7.2.16 テレワーキングの指針及び取決めに、物理的なセキュリティに関する事項を含める

7.7.2.17 テレワーキングの指針及び取決めに、家族及び来訪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

7.7.2.18 テレワーキングの指針及び取決めに、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

7.7.2.19 テレワーキングの指針及び取決めに、保険の用意を含める

7.7.2.20 テレワーキングの指針及び取決めに、バックアップ及び事業継続のための手順を含める

7.7.2.21 テレワーキングの指針及び取決めに、監査及びセキュリティの監視に関する事項を含める

7.7.2.22 テレワーキングの指針及び取決めに、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

7.7.2.23 テレワーキング用コンピュータからの接続を受けるネットワーク接続機器（VPN装置、RAS装置など）では、同一の利用者による複数接続を排除する設定を行う

8 情報システムの取得、開発及び保守

8.1 情報システムのセキュリティ要求事項

目的：セキュリティは情報システムの欠くことのできない部分であることを確実にするため

8.1.1 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業務上の要求事項を記述した文書では、セキュリティの管理策についての要求事項を仕様化する

8.1.1.1 セキュリティ管理策についての要求事項の仕様は、情報システムに組み込まれるべき自動化された制御と、補助的な手動による制御の必要性を考慮して仕様化を行う

8.1.1.2 業務用ソフトウェアのために開発又は購入されたソフトウェアのパッケージのセキュリティの評価では、ソフトウェアに組み込まれている自動化された制御の評価と、必要となる補助的な手動による制御の評価を行う

8.1.1.3 セキュリティ要求事項及び管理策は、関係する情報資産の業務上の価値を考慮して定める

8.1.1.4 セキュリティ要求事項及び管理策は、セキュリティの不具合又はセキュリティが確保されていない場合に起こると思われる業務上の損傷の可能性を考慮して定める

8.1.1.5 情報システムの開発及び試験環境におけるセキュリティ管理策についても同様にセキュリティの要求事項を定める

8.1.1.6 製品を購入する際には、正式な試験及び調達プロセスに従う

8.1.1.7　製品の供給者との契約の中で、必要とされる要求事項を規定する

8.1.1.8　供給者から提案された製品のセキュリティ機能が、指定した要求を満たさない場合は、製品購入前に発生するリスクの評価及び関連する管理策の策定を行う

8.1.1.9　購入した製品の付加機能がセキュリティリスクを引き起こす場合は、これを無効にする。ただし、このリスクに対応する管理策の提案があれば、これをレビューして、付加機能の優位性の判定を行う

8.2 業務用ソフトウェアでの正確な処理

目的：業務用ソフトウェアにおける情報の誤り、消失、認可されていない変更又は不正使用を防止するため

8.2.1　業務用ソフトウェアに入力するデータは、正確で適切であることを確実にするために、その妥当性を確認する

8.2.1.1　入力に使用される業務取引処理（transaction）、常備データ（例えば、名前、住所、信用限度額、顧客参照番号）及びパラメタ表（例えば、売価、通貨交換レート、税率）の妥当性を点検する

8.2.1.2　範囲外の値の入力データを検出するため、二重入力又はその他の入力検査を実施する

8.2.1.3　入力データフィールド中の無効文字を検出するため、二重入力又はその他の入力検査を実施する

8.2.1.4　入力漏れデータ又は不完全なデータを検出するため、二重入力又はその他の入力検査を実施する

8.2.1.5　データ量の上限及び下限からの超過を検出するため、二重入力又はその他の入力検査を実施する

8.2.1.6　認可されていない又は一貫しない制御データを検出するため、二重入力又はその他の入力検査を実施する

8.2.1.7　入力データの妥当性及び完全性を確認するため、重要なフィールド又はデータファイルの内容は、定期的にレビューを行う

8.2.1.8　入力データに認可されていない変更があるかどうかについて、紙に印刷した入力文書の点検を行う

8.2.1.9　利用者によるパスワードの指定時などで伏せ文字を使用する場合、二重入力の検査を行い、誤りを検出する機構を導入する

8.2.1.10　入力データの妥当性確認の誤り検出時の対応手続を作成する

8.2.1.11　入力データのもっともらしさ（形式的な正しさ）を試験する手続を作成する

8.2.1.12　データ入力処理に携わっているすべての要員の責任を明確に定義する

8.2.1.13　データの入力処理に携わっている作業のログを作成する

8.2.1.14　業務用ソフトウェアに入力するデータは、悪意のあるものであることを想定し、自動的な検査及び妥当性確認を行う

8.2.2　処理の誤り又は故意の行為によって発生する情報の破壊を検出するために、妥当性確認の機能を業務用ソフトウェアに組み込む

8.2.2.1　業務用ソフトウェアの設計及び実装において、完全性の喪失につながる処理の不具合のリスクを最小化することを確実にする仕組みを整備する

8.2.2.2　業務用ソフトウェアの設計及び実装に際しては、データの追加、修正及び削除を行うデ

ータ変更機能を導入する

8.2.2.3 業務用ソフトウェアの設計及び実装に際しては、プログラムが間違った順序で実行されること、又はそれ以前の処理の不具合の後でプログラムが実行されることを防止する手続を定める

8.2.2.4 業務用ソフトウェアの設計及び実装に際しては、データの正しい処理を確実にするための、不具合から回復する適切なプログラムを使用する

8.2.2.5 取引処理の更新後のデータファイルのバランスをチェックする処理（逐次処理又は一括処理）を導入する

8.2.2.6 処理開始時のファイル内容と前回終了時のファイル内容との整合を取るための制御（各実行処理の間の制御、ファイルの更新の合計値、各プログラム間の制御）を組み込む

8.2.2.7 システム生成データの妥当性確認の仕組みを組み込む

8.2.2.8 中央のコンピュータと遠隔のコンピュータとの間で、ダウンロード又はアップロードがある場合、そのデータ又はソフトウェアの、完全性、真正性又は他のセキュリティ特性の点検を組み込む

8.2.2.9 レコード及びファイルの全体のハッシュ合計の点検を組み込む

8.2.2.10 業務用ソフトウェアプログラムが正しい時刻に実行されることを確実にするための点検を組み込む

8.2.2.11 プログラムが正しい順序で実行され、不具合の場合は終了すること、及び問題が解決するまでは処理が停止することを確実に実施しているかの点検を組み込む

8.2.2.12 妥当性確認の誤り検出時の対応手続を作成する

8.2.2.13 妥当性確認の作業結果を作業ログとして作成し、安全に保管する

8.2.2.14 データ変更のログには、その変更を行った者若しくはプロセス及び変更内容を特定できる情報を含める

8.2.2.15 データ変更のログ管理には、改ざん及び可用性に対する管理策を導入する

8.2.3 業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し、また、適切な管理策を特定し、実施する

8.2.3.1 業務用ソフトウェアの真正性を確実にするため、ハッシュ値などによる改ざん検知を行う

8.2.3.2 業務用ソフトウェアの真正性を確実にするため、ソフトウェアを読み込み専用媒体に格納する

8.2.3.3 業務用ソフトウェアの真正性を確実にするため、ソフトウェアの更新は認可された管理者のみが行う

8.2.3.4 完全性の保護が必要なメッセージの送信の際には、電子署名などのメッセージ認証機能を使用する

8.2.3.5 メッセージ認証機構に使用される署名機能には、安全とされる暗号アルゴリズムと鍵長を用いる

8.2.3.6 メッセージの完全性確認の誤り検出時の対応手続を作成する

8.2.4 業務用ソフトウェアからの出力データは、保存する情報の処理が正しく、かつ、状況に対して適切であることを確実にするために、その妥当性を確認する

8.2.4.1 業務用ソフトウェアからの出力データの妥当性確認には、業務用ソフトウェアからの出

力データが適正であるかどうかを試験するためのもっともらしさ（形式的な正しさ）の検査を含める

8.2.4.2 業務用ソフトウェアからの出力データの妥当性確認には、すべてのデータの処理を確実にするための調整（reconciliation）の回数を含める

8.2.4.3 業務用ソフトウェアからの出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を決めるために、読取り装置又はその後の処理システムにとっての十分な情報の提供を含める

8.2.4.4 出力データの妥当性確認の誤り検出時の対応手続を作成する

8.2.4.5 データ出力処理に携わっているすべての要員の責任を明確に定義する

8.2.4.6 データの出力処理に携わっている作業のログを作成する

8.2.4.7 業務用ソフトウェアが、利用者による入力データをそのままの形で含んだ出力を行う場合、悪意のあるものが含まれることを想定し、自動的な検査及び妥当性確認を行う

8.3 暗号による管理策

目的：暗号手段によって、情報の機密性、真正性又は完全性を保護するため

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

8.3.1.1 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、組織全体で暗号による管理策を用いることに向けた管理の取組み方を考慮して定める

8.3.1.2 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

8.3.1.3 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、取扱いに慎重を要する情報を保護するための暗号の利用を考慮して定める

8.3.1.4 暗号の利用に関する方針は、暗号かぎの保護手法、及びかぎが紛失、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、かぎ管理に対する取組み方を考慮して定める

8.3.1.5 暗号の利用に関する方針は、この方針の実施の責任やかぎ生成を含めたかぎ管理に対する責任など、役割及び責任を考慮して定める

8.3.1.6 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べき標準類（業務プロセスに用いる解決策の選択）を考慮して定める

8.3.1.7 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、ウィルスの検出）に依存する管理策への影響を考慮して定める

8.3.1.8 暗号にかか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、規則及び国内の制約を考慮し、個別の対応方法を定める

8.3.1.9 ディジタル署名を利用する場合には、関連する法令、特に、ディジタル署名を付すことが法的に要求される条件について規定した法令を考慮する

8.3.1.10 暗号モジュールの生成（コンパイルなど）は、スタンドアロンのコンピュータなど安全な環境で行う

8.3.1.11 暗号モジュールが、組織外のソースコードやライブラリから生成する場合、モジュール

を生成する前にハッシュ値などによりそれらの真正性を検証する

8.3.2 組織における暗号技術の利用を支持するために、かぎ管理を実施する

8.3.2.1 すべての暗号かぎは、改変、紛失、及び破壊から保護する

8.3.2.2 秘密かぎ及びプライベートかぎは、認可されていない開示から保護する

8.3.2.3 かぎの生成、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

8.3.2.4 暗号かぎの生成は、アクセス管理された安全な環境で実施する

8.3.2.5 暗号かぎをバックアップとして保存する場合、物理的にアクセス管理された環境にオフラインの状態で保管する

8.3.2.6 かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアのためのかぎ生成のために、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を定める

8.3.2.7 かぎ管理システムでは、公開かぎ証明書の生成及び入手のために、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を定める

8.3.2.8 かぎ管理システムでは、意図する利用者へのかぎ配布のために、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を定める。ここには、受領時に、かぎ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

8.3.2.9 かぎ管理システムでは、かぎの蓄積のために、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を定める。ここには、かぎをいつ、どのような方法で変更するかの規則も含める

8.3.2.10 かぎ管理システムでは、かぎの変更又は更新のために、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を定める。ここには、かぎをいつ、どのような方法で変更するかの規則も含める

8.3.2.11 かぎ管理システムでは、危険になったかぎの対処のために、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を定める

8.3.2.12 かぎ管理システムでは、かぎを無効にするために、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を定める。ここには、かぎの取消し又は非活性化する方法も含める

8.3.2.13 かぎ管理システムでは、事業継続管理の一環として、紛失したかぎ又は破損したかぎを復旧するために、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を定める

8.3.2.14 かぎ管理システムでは、かぎの保管のために、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を定める

8.3.2.15 かぎ管理システムでは、かぎの破壊のために、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を定める

8.3.2.16 かぎ管理システムでは、かぎ管理に関連する活動の記録と監査のために、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を定める

8.3.2.17 セキュリティが損なわれる可能性を低減するために、かぎが限定された期間内だけで用いられるように、かぎの活性化及び非活性化の期日を定める

8.3.2.18 かぎが用いられる限定された期間は、暗号による管理策を利用している環境及び認識しているリスクに基づいて定める

8.3.2.19 公開かぎは、真正性を保証するため、公開かぎ証明書を付ける

8.3.2.20 公開かぎ証明書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ている、認知された組織によって発行する

8.3.2.21 暗号サービスの外部供給者（例えば、証明機関）とのサービスレベルに関する合意又は契約の内容には、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

8.3.2.22 公開している公開かぎや公開かぎ証明書は、改ざんによる攻撃から守るために、適切なアクセス管理をする

8.4 システムファイルのセキュリティ

目的：システムファイルのセキュリティを確実にするため

8.4.1 運用システムにかかわるソフトウェアの導入を管理する手順を備える

8.4.1.1 運用ソフトウェア、業務用ソフトウェア及びプログラムライブラリの更新は、適切な経営陣の認可に基づき、訓練された実務責任者だけが実施する

8.4.1.2 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

8.4.1.3 業務用ソフトウェア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

8.4.1.4 業務用ソフトウェア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

8.4.1.5 業務用ソフトウェア及びオペレーティングシステムソフトウェアの試験は、運用システムとは別のシステムで実行する

8.4.1.6 業務用ソフトウェア及びオペレーティングシステムソフトウェアの試験を行う際は、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

8.4.1.7 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

8.4.1.8 変更を実施する前に、ロールバック計画を定める

8.4.1.9 運用プログラムライブラリの更新のすべてについて、監査ログを維持する

8.4.1.10 緊急時対応の手段として、一つ前の版の業務用ソフトウェアを保持する

8.4.1.11 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タのすべて、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

8.4.1.12 運用システムに利用されるベンダ供給ソフトウェアは、供給者によってサポートされるバージョンレベルを維持する

8.4.1.13 旧版のソフトウェアを継続して使用するかどうかの決定には、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行う

8.4.1.14 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（新しいセキュリティ機能の導入、この版が必要になったセキュリティ問題の量及び質）を考慮して行う

8.4.1.15 セキュリティ上の弱点を除去する又は低減するのに役立つ場合には、ソフトウェアパッ

チを適用する

8.4.1.16 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、経営陣の承認を得た場合にだけ許可する

8.4.1.17 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

8.4.1.18 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を、監視し管理する

8.4.1.19 オペレーティングシステムのアップグレードは、安定性やセキュリティが劣化するリスクを考慮した上で、必要がある場合のみ行う

8.4.2 試験データは、注意深く選択し、保護し、管理する

8.4.2.1 個人情報又はその他の取扱に慎重を要する情報を含んだ運用データベースは、試験の用途には用いない

8.4.2.2 個人情報又はその他の取扱いに慎重を要する情報を試験の用途に用いる場合には、使用の前に、取扱いに慎重を要する詳細な記述及び内容のすべてを消去するか、又は改変する

8.4.2.3 運用データを試験目的で使用する場合、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は、試験アプリケーションシステムにも適用する

8.4.2.4 運用情報を試験アプリケーションシステムにコピーする場合は、その都度認可を受ける

8.4.2.5 運用データを試験目的で使用する場合、運用情報は、試験が完了した後直ちに試験アプリケーションシステムから消去する

8.4.2.6 運用データを試験目的で使用する場合、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

8.4.3 プログラムソースコードへのアクセスは、制限する

8.4.3.1 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）は、認可されていない機能が入り込むことを防止し、また、意図しない変更を回避するために、厳重に管理する

8.4.3.2 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

8.4.3.3 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

8.4.3.4 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

8.4.3.5 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

8.4.3.6 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

8.4.3.7 プログラムソースライブラリへのすべてのアクセスについて、監査ログを維持する

8.4.3.8 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

8.5 開発及びサポートプロセスにおけるセキュリティ

目的：業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため

8.5.1 変更の実施は、正式な変更管理手順の使用によって、管理する

8.5.1.1 情報システムに対する破壊の危険性を最小限に抑えるために、正式な変更管理手順を文書化し、確実に実行させる仕組みを整備する

8.5.1.2 新しいシステム導入及び既存システムに対する大規模の変更は、文書化、仕様化、試験、

品質管理及び管理された実装から成る正式な手続に従う

8.5.1.3 新しいシステム導入及び既存システムに対する大規模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

8.5.1.4 新しいシステム導入及び既存システムに対する大規模な変更の際の手続には、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含める

8.5.1.5 実現可能ならば、業務用ソフトウェア及び運用の変更管理手順を統合する

8.5.1.6 変更手順には、合意された認可レベルの記録の維持を含める

8.5.1.7 変更手順には、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仕組みを含める

8.5.1.8 変更手順には、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

8.5.1.9 変更手順には、修正を必要とするすべてのソフトウェア、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

8.5.1.10 変更手順には、作業を開始する前に詳細な作業項目の提案について正式な承認を得ることを含める

8.5.1.11 変更手順には、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仕組みを含める

8.5.1.12 変更手順には、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仕組みを含める

8.5.1.13 変更手順には、システムに関する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仕組みを含める

8.5.1.14 変更手順には、すべ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

8.5.1.15 変更手順には、すべての変更要求の監査証跡を維持管理することを含める

8.5.1.16 変更手順には、運用文書類及び利用者手順を、適切な状態にあるように、必要に応じて変更することを確実にする仕組みを含める

8.5.1.17 変更手順には、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仕組みを含める

8.5.2 オペレーティングシステ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、重要な業務用ソフトウェアをレビューし、試験する

8.5.2.1 オペレーティングシステムの変更によって業務用ソフトウェアの管理策及び完全性に関する手順が損なわれなかったことを確実にするために、その管理策及び手順をレビューする

8.5.2.2 年間サポート計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含める

8.5.2.3 実施前に行う適切な試験及びレビューをしても間に合うように、オペレーティングシステ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

8.5.2.4 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

8.5.3　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、すべての変更は、厳重に管理する

8.5.3.1　パッケージソフトウェアの変更を行う場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクへの対応を行う

8.5.3.2　パッケージソフトウェアの変更を行う場合は、ベンダの同意を得る

8.5.3.3　パッケージソフトウェアの変更を行う場合は、標準的なプログラム更新として、ベンダから必要とされる変更が得られる可能性について確認を行う

8.5.3.4　パッケージソフトウェアの変更を行う場合は、変更の結果として、将来のソフトウェア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

8.5.3.5　変更が必要な場合、原本のソフトウェアは保管し、明確に識別された複製に対して変更を適用する

8.5.3.6　ソフトウェア更新管理手続は、最新の承認したパッチ及び業務用ソフトウェアの更新が、すべての認可されたソフトウェアのために導入していることを確実にするために実施する

8.5.3.7　将来のソフトウェア更新において、必要な場合には、再び適用できるように、すべての変更は、十分に試験し、文書化する

8.5.3.8　必要な場合には、変更は、独立した評価組織による試験を受け、正当性を証明する

8.5.4　情報漏えいの可能性を抑止する

8.5.4.1　外向けに公開された媒体及びコミュニケーションの中に、隠された情報がないか詳しく調べる

8.5.4.2　システム及び通信の振舞いから、第三者が情報を導き出せる可能性を低減させるため、こうした振舞いを隠ぺいする

8.5.4.3　高い完全性を考慮されているシステム及びソフトウェアを利用する（例えば、独立した機関に評価された製品の使用）

8.5.4.4　既存の法規定の下で許されている場合には、要員及びシステムのアクティビティを常に監視する

8.5.4.5　コンピュータシステムにおけるリソース使用状況を監視する

8.5.5　組織は、外部委託したソフトウェア開発を監督し、監視する

8.5.5.1　ソフトウェア開発を外部委託する場合、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契約を締結する

8.5.5.2　ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を確認する

8.5.5.3　ソフトウェア開発を外部委託する場合、第三者による不具合の場合の預託（escrow）契約に関する取決めを契約に含める

8.5.5.4　ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権を契約に含める

8.5.5.5　ソフトウェア開発を外部委託する場合、コードの品質及びセキュリティの機能性についての要求事項を契約に含める

8.5.5.6　ソフトウェア開発を外部委託する場合、納品されたソフトウェアに対する検収試験に、悪意のあるコード及びトロイの木馬の検出を含める

8.5.5.7　ソフトウェア開発を外部委託する場合、納品されたソフトウェアに対する検収試験に、ぜい弱性検出を含める

8.6 技術的ぜい弱性管理

目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため

8.6.1　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

8.6.1.1　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

8.6.1.2　技術的ぜい弱性の管理に関連する役割と責任とを定める

8.6.1.3　技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性にかか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すべての調整責務を含む

8.6.1.4　ソフトウェア及びその他の技術に関する技術的ぜい弱性の情報資源を特定し、管理する

8.6.1.5　技術的ぜい弱性の情報資源は、資産目録が更新された場合、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

8.6.1.6　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

8.6.1.7　潜在的な技術的ぜい弱性が特定されたときは、それと関連するリスク及び取るべき処置（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

8.6.1.8　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、取るべき処置を実行する

8.6.1.9　技術的ぜい弱性が特定されたときは、リスクの高いシステムから順に取るべき処置を実行する

8.6.1.10　パッチが利用可能ならば、そのパッチを適用することに関連するリスクを評価する（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。）

8.6.1.11　パッチの適用前に、パッチが正しいものであることを検証する

8.6.1.12　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

8.6.1.13　利用可能なパッチがない場合は、そのぜい弱性に関係するサービス又は機能を停止する

8.6.1.14　利用可能なパッチがない場合は、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

8.6.1.15　利用可能なパッチがない場合は、実際の攻撃を検知又は防止するために、監視を強化する

8.6.1.16　利用可能なパッチがない場合は、ぜい弱性に対する意識を高める

8.6.1.17　修正パッチの適用、その他実施したすべての手順について監査ログを保持する

8.6.1.18　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

9 情報セキュリティインシデントの管理

9.1 情報セキュリティの事象及び弱点の報告

目的：情報システムに関連する情報セキュリティの事象及び弱点を、時機を失しない是正処置をとることができるやり方で連絡することを確実にするため

9.1.1　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

9.1.1.1　情報セキュリティ事象の正式な報告手順と、その報告を受けた場合に取る処置を定めた、インシデントの対応及び段階的取扱いの手順を定める

9.1.1.2　情報セキュリティ事象報告の連絡先を明確にする

9.1.1.3　情報セキュリティ事象報告の連絡先は、いつでも利用でき、また、適切で時機を失しない対応を提供できることを確実にする仕組みを整備する

9.1.1.4　すべての従業員、契約相手及び第三者の利用者に、いかなる情報セキュリティの事象もできるだけ速やかに報告する責任があることを認識させておく

9.1.1.5　すべての従業員、契約相手及び第三者の利用者に、情報セキュリティ事象の報告手順及びその連絡先を認識させる

9.1.1.6　報告手順には、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、適切なフィードバックの手続を含める

9.1.1.7　報告手順には、報告作業を助け、報告者が情報セキュリティ事象に直面した場合にすべての必要な作業を忘れないようにする、情報セキュリティ事象の報告書式を含める

9.1.1.8　報告手順には、情報セキュリティ事象に直面した場合に重要な詳細すべて（例えば、非順守又は違反の形態、起きた誤動作、画面上の表示、奇妙な挙動）を直ちに記録をすることを含める

9.1.1.9　報告手順には、情報セキュリティ事象に直面した場合には、どのような独断の行動も取らずに、直ちに連絡先に報告することを含める

9.1.1.10　報告手順には、セキュリティ違反を犯した従業員、契約相手又は第三者の利用者を処罰する、確立された正式な懲戒手続への言及を含める

9.1.1.11　危険性の高い環境では脅迫警報機能（ある行為が脅迫を受けてなされていることを密かに伝える手段）を備える

9.1.1.12　脅迫警報への対応手順は、その警報が示す高い危険の状況を反映する

9.1.1.13　システムの誤動作又はその他の異常な挙動についても、情報セキュリティ事象として常に報告する

9.1.2　すべての従業員、契約相手並びに第三者の情報システム及びサービスの利用者に、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セキュリティ弱点は、どのようなものでも記録し、また、報告するように要求する

9.1.2.1　すべての従業員、契約相手及び第三者の利用者に対して、情報セキュリティインシデントを防止するため、システム又はサービスの中で発見した又は疑いを持ったセキュリティ弱点を管理者又は直接にサービス提供者に、できるだけ速やかに報告することを要求する

9.1.2.2　セキュリティ弱点を管理者又は直接にサービス提供者に報告するための仕組みは、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

9.1.2.3　すべての従業員、契約相手及び第三者の利用者に、いかなる場合でも疑いをもった弱点を自分で立証しようと試みるべきではないことを周知する

9.2 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：情報セキュリティインシデントの管理に、一貫性のある効果的な取組み方法を用いることを確

実にするため

9.2.1 情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、責任体制及び手順を確立する

9.2.1.1 情報セキュリティの事象及び弱点の報告に加えて、情報セキュリティインシデントを検知するために、システム、警告及びぜい弱性の監視を利用する

9.2.1.2 情報セキュリティインシデントの管理手順には、情報システムの不具合発生及びサービスの停止時の扱いを含める

9.2.1.3 情報セキュリティインシデントの管理手順には、悪意のあるコード検出、発生時の扱いを含める

9.2.1.4 情報セキュリティインシデントの管理手順には、サービス妨害発生時の扱いを含める

9.2.1.5 情報セキュリティインシデントの管理手順には、不完全又は不正確な業務データに起因する誤り発生時の扱いを含める

9.2.1.6 情報セキュリティインシデントの管理手順には、機密性及び完全性の侵害発生時の扱いを含める

9.2.1.7 情報セキュリティインシデントの管理手順には、情報システムの不正使用発生時の扱いを含める

9.2.1.8 情報セキュリティインシデントの管理手順には、インシデントの原因の分析及び特定を含める

9.2.1.9 情報セキュリティインシデントの管理手順には、インシデントの抑制策を含める

9.2.1.10 情報セキュリティインシデントの管理手順には、必要な場合には、再発防止のための是正処置の計画作成及び実施を含める

9.2.1.11 情報セキュリティインシデントの管理手順には、インシデントからの回復によって影響を受ける人々、又はインシデントからの回復にかかわる人々との情報交換を含める

9.2.1.12 情報セキュリティインシデントの管理手順には、とった処置についての関連当局への報告を含める

9.2.1.13 内部の問題の分析のために、監査証跡及びこれに類する証拠を適切に収集及び保全する

9.2.1.14 契約若しくは規制の要求に対する違反の疑いに関連する法的証拠又は民事若しくは刑事訴訟（例えば、コンピュータの不正使用又はデータ保護に関して制定された法律を根拠とする訴訟）での法的証拠として使用するために、監査証跡及びこれに類する証拠を適切に収集及び保全する

9.2.1.15 ソフトウェア及びサービスの提供者からの補償についての交渉のために、監査証跡及びこれに類する証拠を適切に収集及び保全する

9.2.1.16 セキュリティ違反からの回復処置及びシステムの不具合の修復処置は、慎重に、かつ、正式に管理する

9.2.1.17 明確に特定され認可された要員だけに、作動中のシステム及びデータに対するアクセスを許すことを確実にする仕組みを整備する

9.2.1.18 実施したすべての緊急処置について、文書に詳細を記録することを確実にする仕組みを整備する

9.2.1.19 経営陣に緊急処置を報告し、定められているやり方でレビューを受けることを確実にする仕組みを整備する

9.2.1.20 業務システム及び管理策の完全性を最短で確認することを確実にする仕組みを整備する

9.2.1.21 情報セキュリティインシデントを管理する目的について経営陣による同意を得る

9.2.1.22 情報セキュリティインシデントの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周知する

9.2.2 情報セキュリティインシデントの形態、規模及び費用を定量化し監視できるようにする仕組みを備える

9.2.2.1 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

9.2.3 情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には、関係する法域で定めている証拠に関する規則に従うために、証拠を収集、保全及び提出する

9.2.3.1 組織内で扱う懲戒処置のための証拠を収集するための内部手順を定める

9.2.3.2 証拠が紙文書の場合には、文書の発見者及び立ち会った者、発見場所及び日時の記録を行い、原本とともにセキュリティを保って保管する

9.2.3.3 証拠が紙文書の場合には、いかなる調査でも、原本を損なわないことを確実にする仕組みを整備する

9.2.3.4 証拠がコンピュータ媒体上の情報の場合には、取外し可能な媒体及びハードディスク又は記憶装置の中の情報を（適用される要求事項に応じて）複製又は複写する

9.2.3.5 証拠がコンピュータ媒体上の情報の場合には、複写プロセスでのすべての作業のログを保管し、そのプロセスには立会人を置く

9.2.3.6 証拠がコンピュータ媒体上の情報の場合には、原本とする媒体及びログ（それが困難な場合は、少なくとも一つの複製物又は複写物）は、だれも触れないようにセキュリティを保って保管する

9.2.3.7 訴訟に関連したどのような作業も、証拠物件の複写物だけを利用して行う

9.2.3.8 証拠物件の複写は信頼できる要員の監督下で行い、いつどこでその複写プロセスを実行したか、だれが複写作業を担当したか、並びにどのツール及びプログラムを利用したかのログを取る

10 事業継続管理

10.1 事業継続管理における情報セキュリティの側面

目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに、それらから重要な業務プロセスを保護し、また、事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため

10.1.1 組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う、管理された手続を策定し、維持する

10.1.1.1 事業継続管理手続には、重要な業務プロセスの識別及び優先順位付けも含め、組織が直面しているリスクを、可能性及び影響の面から理解することを組み込む

10.1.1.2 事業継続管理手続には、重要な業務プロセスにかかわるすべての資産を識別することを組み込む

10.1.1.3 事業継続管理手続には、情報セキュリティインシデントによって発生する業務プロセスの中断が事業に及ぼすと思われる影響を理解し、情報処理施設の事業目的を確立するこ

とを組み込む

10.1.1.4 事業継続管理手続には、適切な保険への加入の是非の判断を組み込む

10.1.1.5 事業継続管理手続には、予防及び緩和のための追加管理策を特定し、それらの実施の検討を組み込む

10.1.1.6 事業継続管理手続には、識別された情報セキュリティの要求事項を取り扱うのに十分な、財政上、組織上、技術上及び環境上の経営資源を特定することを組み込む

10.1.1.7 事業継続管理手続には、要員の安全並びに情報処理設備及び組織の資産の保護を確実にする仕組みを組み込む

10.1.1.8 事業継続管理手続には、合意された事業継続戦略に沿って情報セキュリティの要求事項を取り扱った事業継続計画を策定し、文書化することを組み込む

10.1.1.9 事業継続管理手続には、策定した計画及び手続を定めに従って試験し、更新することを組み込む

10.1.1.10 事業継続管理手続には、事業継続管理を組織のプロセス及び機構に組み込むことを確実にする仕組みを含める

10.1.1.11 事業継続管理手続には、この手続の責任を、組織内の適切な階層に割り当てることを組み込む

10.1.2 業務プロセスの中断を引き起こし得る事象は、そのような中断の発生確率及び影響並びに中断が情報セキュリティに及ぼす結果とともに、特定する

10.1.2.1 情報セキュリティの側面からの事業継続の策定に当たっては、組織の業務プロセスの中断を引き起こし得る事象（又は一連の事象。例えば、装置の故障、人による誤り、盗難、火災、自然災害、テロ行為）を特定し、またこのような業務プロセス中断の発生確率及び影響を、時間、損傷規模及び回復期間の面から判断するために、リスクアセスメントを行う

10.1.2.2 事業継続に関するリスクアセスメントは、事業資源及び業務プロセスの管理者の全面的な関与の下で実施する

10.1.2.3 事業継続に関するリスクアセスメントでは、情報処理施設のみならず、すべての業務プロセスを対象とする

10.1.2.4 事業継続に関するリスクアセスメントでは、情報セキュリティ特有の結果の観点（すなわち、機密性、完全性、可用性）も含める

10.1.2.5 事業継続に関するリスクアセスメントでは、組織に関連した基準及び目的（重要な資源、中断の影響、受容可能な停止時間及び回復の優先順位を含む）に対して、リスクの特定、定量化及び優先順位付けを行う

10.1.2.6 リスクアセスメントの結果に応じて、事業継続に対する包括的な取組方法を決定するため、事業継続戦略を策定する

10.1.2.7 事業継続戦略及びこの戦略を実施に移すための計画は、経営陣の承認を得る

10.1.3 重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施する

10.1.3.1 事業継続計画の策定プロセスでは、すべての責任及び事業継続手順を特定し、合意する

10.1.3.2 事業継続計画の策定プロセスでは、受容可能な情報の損失及びサービスの停止を特定する

10.1.3.3 事業継続計画の策定プロセスでは、業務の運用並びに情報の可用性の回復及び復旧を、要求された時間内で可能にする手順を定める

10.1.3.4 事業継続計画の策定プロセスでは、内部の事業間及び外部の事業との事業上の依存関係並びに締結済の契約を評価する

10.1.3.5 事業継続計画の策定プロセスでは、損傷を受けたプロセスが回復及び復旧するまでの、損傷を受けなかったプロセスにおける運用手順を定める

10.1.3.6 事業継続計画の策定プロセスでは、合意された手順及び手続の文書化を行う

10.1.3.7 事業継続計画の策定プロセスでは、危機管理を含む、合意された手順及び手続についての、適切な要員教育について定める

10.1.3.8 事業継続計画の策定プロセスでは、計画の試験及び更新について定める

10.1.3.9 事業継続計画の策定プロセスでは、計画の実行を支持するサービス及び経営資源を特定する（情報処理設備の代替手段と同様に、要員配置及び情報処理設備以外の経営資源も含む）

10.1.3.10事業継続計画の策定プロセスでは、代替手段として、無償の協定又は有償の契約という形での、第三者との取決めも考慮して特定する

10.1.3.11主事業所に起きた災害による被害を免れるのに十分な遠隔地に、事業継続計画の複製を保管する

10.1.3.12事業継続計画の複製は最新に保ち、主事業所と同等のセキュリティレベルで保護することを確実にする

10.1.3.13事業継続計画の複製を保管する場所には、事業継続計画を実行するために必要な他のものも保管する

10.1.3.14一時的な代替場所を利用する場合、この場所で実施されるセキュリティ管理策は主事業所と同等のレベルにする

10.1.4 すべての計画が整合したものになることを確実にするため、情報セキュリティ上の要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持する

10.1.4.1 各事業継続計画では、事業継続の取組み方（例えば、情報又は情報システムの可用性及びセキュリティを確実にするための取組み方）を記述する

10.1.4.2 各事業継続計画では、計画の各要素の実行について責任を負う各個人だけでなく、その段階的計画及びその発動条件も定める

10.1.4.3 新しい要求事項が明確になった場合は、既存のいかなる緊急時手順（例えば、避難計画、代替手段利用計画）も、適切に修正する

10.1.4.4 事業継続上の問題を常に適切に取り扱うことを確実にするための手順を、組織の変更管理プログラムに組み込む

10.1.4.5 各事業継続計画では、それぞれの管理者を明確にする

10.1.4.6 緊急時手順、手動による代替手段利用計画及び再開計画は、該当する事業資源又は関連するプロセスの管理者の責任範囲で策定する

10.1.4.7 情報処理施設及び通信施設のような選択可能な技術サービスに対する代替手段の手配は、サービス提供者の責任とする契約を締結する

10.1.4.8 事業継続計画策定の枠組みには、各計画の実施前に従うべき手続（例えば、状況をどの

ように評価するか、だれがかかわるべきか）を記載した計画発動条件の策定を組み入れる

10.1.4.9 事業継続計画策定の枠組みには、業務の運用を危険にさらすインシデントが発生した場合に取るべき処置について記載した緊急時手順の策定を組み入れる

10.1.4.10事業継続計画策定の枠組みには、主要な事業活動又はその活動を支持するサービスの拠点を一時的な代替場所に移動するため、及び業務プロセスを要求された時間内に回復するために取るべき処置について記載した代替手段利用手順の策定を組み入れる

10.1.4.11事業継続計画策定の枠組みには、損傷を受けたプロセスが回復及び復旧するまでの間の、損傷を受けなかったプロセスにおける臨時の運用手順の策定を組み入れる

10.1.4.12事業継続計画策定の枠組みには、正常操業に復帰するために取るべき処置について記載した再開手順の策定を組み入れる

10.1.4.13事業継続計画策定の枠組みには、事業継続計画をいつどのように試験するかを定めた維持計画予定表及びその計画を維持するための手続の策定を組み入れる

10.1.4.14事業継続計画策定の枠組みには、事業継続手続を理解させ、手続が継続して有効であることを確実にするために設計される意識向上活動、教育活動及び訓練活動の策定を組み入れる

10.1.4.15事業継続計画策定の枠組みには、計画の要素の実施責任者の明確化（代理者の任命を含む）を組み入れる

10.1.4.16事業継続計画策定の枠組みには、緊急時手順、代替手段利用手順及び再開手順を実施するために必要な、重要な資産及び資源の特定を組み入れる

10.1.5 事業継続計画は、最新で効果的なものであることを確実にするために、定めに従って試験・更新する

10.1.5.1 事業継続計画の試験では、回復チームのすべてのメンバー及び他の関連要員に対し、事業継続計画、事業継続及び情報セキュリティに対する自身の責任並びに計画が発動された場合の自身の役割を確実に認識させる仕組みを整備する

10.1.5.2 事業継続計画の試験予定表で、計画の各要素をいつどのようにして試験するかを示す

10.1.5.3 計画の個々の要素は、頻繁に試験する

10.1.5.4 事業継続計画が実際に役立つことを保証するために、様々な状況の机上試験を実施する（障害例を用いて事業回復対策を検討する。）

10.1.5.5 事業継続計画が実際に役立つことを保証するために、模擬試験を実施する（特に、インシデント・危機の発生後の管理上の役割について、要員を教育・訓練する。）

10.1.5.6 事業継続計画が実際に役立つことを保証するために、技術的回復試験を実施する（情報システムを有効に復旧できることを確実にする。）

10.1.5.7 事業継続計画が実際に役立つことを保証するために、代替の事業場所における回復試験を実施する（回復運転と並行して、主事業所から離れた場所で業務プロセスを実施する。）

10.1.5.8 事業継続計画が実際に役立つことを保証するために、供給者の設備及び供給サービスの試験を実施する（外部から供給されるサービス及び製品が契約事項を満たすことを確実にする。）

10.1.5.9 事業継続計画が実際に役立つことを保証するために、全体的な模擬回復試験を実施する

（組織、要員、装置、施設及び手続が障害に対処できることを試験する。）

10.1.5.10各試験の手法は、個別の回復計画に関連したやり方で適用する

10.1.5.11試験の結果を記録すること、及び必要な場合には計画を改善するための処置をとる

10.1.5.12各事業継続計画の定めに従ったレビューに対する責任を割り当てる

10.1.5.13レビュー又は試験において、事業継続計画にいまだ反映されていない事業上の取決めの変更を識別した場合には、事業継続計画を適切に更新する

10.1.5.14事業継続計画の変更管理手続は、更新された計画を配付し、強化されていることを定期的見直しによって確認する

10.1.5.15新しい装置の取得、運用システムのアップグレード及び次の変更があった場合には、事業継続計画の更新の是非を判断する

1．要員

2．あて名又は電話番号

3．事業戦略

4．所在地、施設及び資源

5．法規制

6．契約相手、供給業者及び主要な顧客

7．手続又は手続の新規設定若しくは廃止

8．（運用上及び財務上の）リスク

11 順守

11.1 法的要求事項の順守[*6]

目的：法令、規制又は契約上のあらゆる義務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

11.1.1 各情報システム及び組織について、すべての関連する法令、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方を、明確に定め、文書化し、また、最新に保つ

11.1.1.1 各情報システム及び組織について、すべての関連する法令、規則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責任を同様に定め、文書化する

11.1.2 知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、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導入する

11.1.2.1 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

11.1.2.2 著作権を侵害しないことを確実にするために、ソフトウェアは知られた定評のある供給元（企業規模を問わない）だけを通して取得する

11.1.2.3 知的財産権を保護するための方針に対する意識を持続させ、それらの方針に違反した要員に対して懲罰処置を取る意思を通知する

11.1.2.4 適切な財産登録簿を維持管理し、知的財産権保護が要求事項となっているすべての資産

---

*6 法的順守は、しばしば、コンプライアンスといわれることがある。

を識別する

11.1.2.5 使用許諾を得ていることの証明及び証拠並びにマスタディスク、手引などを維持管理する

11.1.2.6 許諾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

11.1.2.7 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点検を行う

11.1.2.8 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

11.1.2.9 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

11.1.2.10 知的財産を考慮すべき可能性があるものを保護するために、適切な監査ツールを用いる

11.1.2.11 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管理方針を定め、また、提示される使用条件に従う

11.1.2.12 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

11.1.2.13 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

11.1.3 重要な記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊及び改ざんから保護する

11.1.3.1 記録類は、記録の種類（例えば、会計記録、データベース記録、取引ログ、監査ログ）によって、また、さらにそれぞれの種類の中でも保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光媒体）によって分類して保管する

11.1.3.2 暗号化して保存した記録又は電子署名と関連する暗号かぎに関する情報及びプログラム（暗号、署名用のプログラムなど）は、その記録類が保存されている期間中であればその復号が可能なように保管する

11.1.3.3 記録の保存に用いる媒体は、劣化する可能性を考慮して選択する

11.1.3.4 保存及び取扱いの手順は、製造業者の推奨の仕様に従って実施する

11.1.3.5 電子的記録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取り入れる

11.1.3.6 満たすべき要求に応じて、許容される時間枠内及び書式で、要求された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

11.1.3.7 保存及び取扱いシステムでは、適切な属性情報などにより、記録の明確な特定を確実にするための仕組みを導入する

11.1.3.8 記録の種類により、国家又は地域の法律又は規則が適用される場合には、定められている保持期間を明確にする

11.1.3.9 記録の保持期間が、契約及び事業上の要求事項から定められる場合には、その保持期間の明確化を確実にする

11.1.3.10 保持期間が終了した後、組織にとって必要ない場合には、保存及び取扱いシステムは、記録を適切に破棄できるようにする

11.1.3.11 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し、保持計画（保持期間を明確にしたもの）を作成し、主要な情報の目録（inventory）を維持管理し、記録

及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実施する

11.1.4 個人データ及び個人情報の保護は、関連する法令、規制、及び適用がある場合には、契約条項の中の要求に従って確実にする

11.1.4.1 個人データ及び個人情報の保護に関する組織の方針を確立して実施する

11.1.4.2 個人データ及び個人情報の保護に関する組織の方針は、個人情報の処理に関与するすべての者に伝達する

11.1.4.3 個人データ及び個人情報の保護の体制を構築し、経営陣の中から責任者を選出する

11.1.4.4 個人データ及び個人情報の保護の責任者は、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

11.1.4.5 個人情報の取扱いに関する、及びデータ保護原則の認識の確実化に関する責任は、関連する法令及び規則に従って処置する

11.1.4.6 個人情報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

11.1.5 認可されていない目的のための情報処理施設の利用は、阻止する

11.1.5.1 情報処理施設の利用は、経営陣による承認を必要とする

11.1.5.2 情報処理施設の認可されていない利用が、監視又は他の手段で明らかになった場合、この利用を適切な懲戒処置及び／又は法的処置の検討にかかわる管理者に通知する

11.1.5.3 監視手順を導入する前に、法的助言を受ける

11.1.5.4 情報処理施設のすべての利用者に対し、自分に許可されたアクセスの正確な範囲と、認可されていない利用を検知するための適切な監視の導入を認識させる

11.1.5.5 組織の従業員、契約者及び第三者の利用者に、認可された使用以外の情報処理施設の使用は、すべて許されていないことを知らせる

11.1.5.6 情報システムへのログオン時には、利用しようとしている情報処理施設が組織の所有である旨、及び認可されていないアクセスは許されない旨の警告文を表示する

11.1.6 暗号化機能は、関連するすべての協定、法令及び規制を順守して用いる

11.1.6.1 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及び／又は輸出に関する規制を順守する

11.1.6.2 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及び／又は輸出に関する規制を順守する

11.1.6.3 暗号利用に関する規制を順守する

11.1.6.4 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が行われる場合の手順を定める

11.1.6.5 暗号に関連する国の法令及び規則の順守を確実にするために、法的な助言を求める

11.1.6.6 暗号化された情報又は暗号制御機能を他国にもち出す前に、法的な助言を受ける

11.2 セキュリティ方針及び標準の順守並びに技術的順守

目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため

11.2.1 管理者は、セキュリティ方針及び標準類への順守を達成するために、自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にする

11.2.1.1 管理者は自分の責任範囲内にある情報処理が、適切なセキュリティ方針、標準類及びその他のセキュリティ要求事項すべてに対して、順守していることを定めに従ってレビューする

11.2.1.2 管理者によるレビューの結果、何らかの非順守を見出した場合、管理者は非順守の原因を特定し、再発しないことを確実にするための処置の必要性を評価し、適切な是正処置を確定して実施する

11.2.1.3 管理者は、是正処置を実施した場合、その効果をレビューする

11.2.1.4 管理者が実施したレビュー及び是正処置の結果を記録し、維持管理する

11.2.1.5 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

11.2.2 情報システムを、セキュリティ実施標準の順守に関して、定めに従って点検する

11.2.2.1 技術的順守点検は、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による助けを得て）行うか、及び／又は技術専門家が後に解釈するための技術報告書を生成する自動ツールのサポートを受けて実施する

11.2.2.2 情報システムの侵入テスト又はぜい弱性アセスメントを計画し、文書化し、また繰り返し実施する

11.2.2.3 いかなる技術的順守点検も、力量があり組織によって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

11.3 情報システムの監査に対する考慮事項

目的：情報システムに対する監査手続の有効性を最大限にするため、及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため

11.3.1 運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意する

11.3.1.1 監査要求事項は、担当経営陣の同意を得る

11.3.1.2 運用システムの点検の範囲を、合意し管理する

11.3.1.3 運用システムの点検は、ソフトウェア及びデータを読み出し専用のアクセスに限定する

11.3.1.4 運用システムの点検における、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もと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

11.3.1.5 運用システムの点検を実施するための資源を、明確に識別し、利用可能にする

11.3.1.6 運用システムの点検を実施するための、特別又は追加の処理に対する要求事項を、識別し、合意する

11.3.1.7 運用システムの点検の行う際には、参照用の証跡を残すために、すべてのアクセスを監視しログを取る

11.3.1.8 重要データ又はシステムを点検する場合、タイムスタンプを付した参照用の証跡を利用する

11.3.1.9 運用システムの点検は、すべての手順、要求事項及び責任について、文書化する

11.3.1.10監査の実施者は被監査活動と独立とする

11.3.2 情報システムを監査するツールの不正使用又は悪用を防止するために、それらのツールへのアクセスは、抑制する

11.3.2.1 情報システムを監査するツール（例えば、ソフトウェア又はデータファイル）は、適切なレベルの保護を追加する場合を除いて、開発及び運用システムから分離しておく

11.3.2.2 情報システムを監査するツール（例えば、ソフトウェア又はデータファイル）は、適切なレベルの保護を追加する場合を除いて、テープ保管場所又は利用者領域に保持しない