情報セキュリティ管理基準

Ver1.0

前文

インターネットを中核とする情報技術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前提条件となり、また安全な社会生活を支える基盤条件となっている。国際社会においても情報セキュリティ確保の要請は喫緊の課題とされている。

情報セキュリティ管理基準は、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を整備、運用するための実践規範である。情報セキュリティマネジメントは、第一義的には、組織体における必要性と組織体の責任において果たされるべきものである。本管理基準は、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、組織体が情報セキュリティマネジメント体制の構築と、適切なコントロールの整備と運用を効果的に導入できるように支援することを目的としている。

情報セキュリティ管理基準は、情報セキュリティに係るマネジメントサイクル確立のための国際標準規格である ISO/IEC 17799:2000（JIS X 5080:2002）をもとにしており、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、マネジメント及びコントロールの項目を規定したものである。本管理基準は、組織体の業種及び規模等を問わず適用できるよう汎用的なものとなっている。組織体においては、本管理基準を基礎として、リスクアセスメントの結果等に基づき、独自に必要とする項目を追加、あるいは削除して活用することができる。ただし、情報セキュリティは、個々のマネジメント及びコントロールの項目が相互に結びつき合ってはじめて有効に機能するものであり、また、計画、実施、評価、是正を通じたマネジメントサイクルとして機能するように留意しなければならない。

情報セキュリティ管理基準は、主要な管理項目ごとにその目的を示し、次いで管理の目的を達成するために必要とされるコントロール目標と具体的なコントロール手続を規定している。本管理基準は、管理項目ごとにその目的から具体的なコントロール手続に至るまでを関連づけて、末広がりとなる体系性をもたせている。効果的な情報セキュリティ管理を実現するためには、マネジメントサイクル構築の出発点となるべき管理の目的を明確にした上で、リスクアセスメントに基づいた最適な管理資源の配分が行えるよう、必要とされるコントロールを対応づけてゆくことが重要となるからである。

情報セキュリティ管理基準は、本管理基準と姉妹編をなす情報セキュリティ監査基準に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。また、本管理基準は、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。

なお、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の趣旨及び体系に則って、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。

注

〇コントロールについて

本管理基準中、各目的の下位に存在し、「〇.〇.〇　……」と記述される部分を「コントロール」と呼ぶ。

例）1.1.1　経営人は、組織にまたがる情報セキュリティ基本方針の発行及び維持を通じて、明確な基本方針の方向性を定めること

〇サブコントロールについて

本管理基準中、コントロールの下位に存在し、「〇.〇.〇.〇　……」と記述される部分を「サブコントロール」と呼ぶ。

例）1.1.1.1 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること

目次

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指針及び支持を規定するため

1.1.1 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること

1.1.1.1 基本方針文書には、経営陣の責任を明記すること

1.1.1.2 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること

1.1.1.3 基本方針文書には、情報セキュリティの定義を含めること

1.1.1.4 基本方針文書には、その目的を含めること

1.1.1.5 基本方針文書には、適用範囲を含めること

1.1.1.6 基本方針文書には、情報共有を可能にするための機構としてのセキュリティの重要性を含めること

1.1.1.7 基本方針文書には、情報セキュリティの目標を支持する経営陣の意向声明書を含めること

1.1.1.8 基本方針文書には、原則を支持する経営陣の意向声明書を含めること

1.1.1.9 基本方針文書には、法律上及び契約上の要求事項への適合を含めること

1.1.1.10 基本方針文書には、セキュリティ教育の要求事項を含めること

1.1.1.11 基本方針文書には、ウイルス及び他の悪意のあるソフトウェアの予防及び検出を含めること

1.1.1.12 基本方針文書には、事業継続管理を含めること

1.1.1.13 基本方針文書には、セキュリティ基本方針違反に対する措置を含めること

1.1.1.14 基本方針文書には、セキュリティの事件・事故を報告することを含めること

1.1.1.15 基本方針文書には、情報セキュリティマネジメントの一般的責任の定義を含めること

1.1.1.16 基本方針文書には、特定責任の定義を含めること

1.1.1.17 基本方針文書には、基本方針を支持する文書（例えば、特定の情報システムについてのより詳細なセキュリティ個別方針及び手順又は利用者が従うことが望ましいセキュリティ規則）の参照情報を含めること

1.1.1.18 基本方針文書には、この基本方針が、想定した読者にとって、適切で、利用可能で、かつ理解し易い形で、組織全体にわたって利用者に知らせること

1.1.2 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること

1.1.2.1 見直し手続によって、当初のリスクアセスメントの基礎事項に影響を及ぼす変化（例えば、重大なセキュリティの事件・事故、新しいぜい（脆）弱性、又は組織基盤若しくは技術基盤の変化）に対応して確実

に見直しを実施すること

1.1.2.2 記録されたセキュリティの事件・事故の性質、回数及び影響によって示される、基本方針の有効性について、日程を定め、定期的に見直しを実施すること

1.1.2.3 事業効率における管理策の費用及び影響について、日程を定め、定期的に見直しを実施すること

1.1.2.4 技術変更による効果について、日程を定め、定期的に見直しを実施すること

2 組織のセキュリティ

2.1 情報セキュリティ基盤

目的：組織内の情報セキュリティを管理するため

2.1.1 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経営者による目に見える形での支持を確実にするために、運営委員会を設置すること

2.1.2 運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること

- 2.1.2.1 運営委員会は、適切な責任及び資源配分によって、組織内におけるセキュリティを促進すること
- 2.1.2.2 運営委員会は、情報セキュリティ基本方針並びに全体的な責任の見直し及び承認をすること
- 2.1.2.3 運営委員会は、情報資産が重大な脅威にさらされていることを示す変化を監視すること
- 2.1.2.4 運営委員会は、情報セキュリティの事件・事故の見直し及び監視をすること
- 2.1.2.5 運営委員会は、情報セキュリティを強化するための主要な発議の承認をすること
- 2.1.2.6 運営委員会は、一人の管理者が、すべてのセキュリティ関連活動に責任をもつこと

2.1.3 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を設置すること

- 2.1.3.1 管理者の代表を集めた委員会では、組織全体の情報セキュリティのそれぞれの役割及び責任への同意を得ること
- 2.1.3.2 管理者の代表を集めた委員会では、情報セキュリティのための個別の方法及び手順（例えば、リスクアセスメント、セキュリティの分類体系）への同意を得ること
- 2.1.3.3 管理者の代表を集めた委員会では、組織全体の情報セキュリティの発議（例えば、セキュリティの意識向上プログラム）への同意及び支持を得ること
- 2.1.3.4 管理者の代表を集めた委員会では、セキュリティを、情報化計画の作成過程の一部にすることを確実にすること
- 2.1.3.5 管理者の代表を集めた委員会では、新しいシステム又は新しいサービスのためのそれぞれの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の調整をすること
- 2.1.3.6 管理者の代表を集めた委員会では、情報セキュリティの事件・事故の見直しをすること
- 2.1.3.7 管理者の代表を集めた委員会では、組織全体への情報セキュリティに対する目に見える形での業務上の支援の促進をすること

2.1.4 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手続の実施に対する責任を、明確に定めること

2.1.4.1 情報セキュリティ基本方針には、組織内のセキュリティの役割及び責任の割当てに関する全般的な手引を規定すること

2.1.4.2 情報セキュリティ基本方針に、個別のサイト、システム又はサービスに関するより詳細な手引を追加すること

2.1.4.3 個々の物理的資産及び情報資産に限定した責任、並びに事業継続計画のようなセキュリティ手順を、明確に定義すること

2.1.4.4 一人の情報セキュリティ管理者を任命すること

2.1.4.5 情報資産の責任者は、その資産のセキュリティに対して最終的な責任をもつこと

2.1.4.6 情報資産の責任者は、委任された責任が正しく果たされたかを判断できること

2.1.4.7 各管理者が責任を負う範囲は明確に規定すること

2.1.4.8 個々のシステムに関連したいろいろな資産及びセキュリティ手順は、識別され、及び明確に定義されること

2.1.4.9 各資産又はセキュリティ手順に対する管理者の責任は、協議の下で決め、その責任の詳細は、文書化されること

2.1.4.10 承認の権限の範囲は、明確に定義され、文書化されること

2.1.5 新しい情報処理設備に対する経営者による認可手続を確立すること

2.1.5.1 新しい設備は、そ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を得ること

2.1.5.2 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からも承認を得ること

2.1.5.3 ハードウェア及びソフトウェアは、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こと

2.1.5.4 個人が所有する情報処理設備を業務情報の処理に用いる場合、その使用及びそれに伴って必要となる管理策は、認可を得ること

2.1.5.5 職場での個人用情報処理設備の使用は、評価を受け、認可を得ること

2.1.6 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること

2.1.6.1 専門家によるセキュリティの助言は、経験を積んだ社内の情報セキュリティ助言者が行うこと

2.1.6.2 専門家を雇わないならば、特定の個人を指名して、社内の知識及び経験を一貫性を保つように調整させ、セキュリティの方針決定を支援させること

2.1.6.3 このような任に当たる者は、自分自身の経験を超えた専門的な助言を与えるためには、適切な社外の助言者との接触をもつこと

2.1.6.4 情報セキュリティ助言者又は同等の担当者は、自らの経験又は外部の助言を用いて、情報セキュリティのあらゆる面について助言を与えることを業務とすること

2.1.6.5 助言者は、組織内のあらゆる経営陣と直接接触できること
2.1.6.6 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに速やかに相談を受け付けること
2.1.6.7 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに専門家の指導に関する情報又は調査手段を提供すること

2.1.7 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること
2.1.7.1 セキュリティのグループ及び業界の委員会の一員となることも考慮すること
2.1.7.2 組織の機密情報が認可されていない人々に絶対に渡らないように、セキュリティ情報の交換を制限すること

2.1.8 情報セキュリティ基本方針の実施を、他者が見直すこと
2.1.8.1 情報セキュリティ基本方針文書には、情報セキュリティの基本方針及び責任を記述すること

2.2 第三者によるアクセスのセキュリティ
目的：第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため

2.2.1 組織の情報処理施設への第三者のアクセスに関連づけてリスクを評価し、適切な管理策を実施すること
2.2.1.1 物理的アクセス、例えば、事務所、コンピュータ室及びファイルキャビネットへのアクセスを考慮すること
2.2.1.2 論理的アクセス、例えば、組織のデータベース、情報システムへのアクセスを考慮すること
2.2.1.3 第三者に接続する業務上の必要がある場合には、その管理策の要求事項を明らかにするために、リスクアセスメントを実施すること
2.2.1.4 リスクアセスメントにおいては、要求されるアクセスの種類、情報の価値、第三者が採用する管理策、及び組織の情報のセキュリティに対するこのアクセスの影響を考慮すること
2.2.1.5 第三者アクセスにかかわるすべてのセキュリティ要求事項又は内部管理策は、第三者との契約書に反映させること
2.2.1.6 情報及び情報処理施設への第三者によるアクセスは、適切な管理策を実施すること
2.2.1.7 第三者によるアクセスは、接続又はアクセスについての条件を明示した契約書を締結するまで、開始させないこと

2.2.2 組織の情報処理施設への第三者アクセスにかかわる取決めは、正式な契約に基づくこと
2.2.2.1 第三者アクセスに関する契約には、組織のセキュリティ基本方針及び

標準類に適合することを確実にするために、すべてのセキュリティ要求事項を含めるか又は引用すること

2.2.2.2 第三者アクセスに関する契約書は、組織と第三者との間に誤解が全くないことを確実にするものであること

2.2.2.3 組織は、その供給業者の損失補償について納得していること

2.2.2.4 契約書には、情報セキュリティに関する一般方針を含めることを考慮すること

2.2.2.5 契約書には、情報及びソフトウェアを含む、組織の資産を保護する手順を含むことを考慮すること

2.2.2.6 契約書には、資産が危険にさらされているか、例えば、データの喪失又は変更が生じているかどうかを判定するための手順を含めることを考慮すること

2.2.2.7 契約書には、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を確実に返還又は破棄するための管理策を含めることを考慮すること

2.2.2.8 契約書には、完全性及び可用性を含めることを考慮すること

2.2.2.9 契約書には、情報の複製及び開示の制限を含めることを考慮すること

2.2.2.10 契約書には、利用できる各サービスの記述を含めることを考慮すること

2.2.2.11 契約書には、サービスの目標となるレベル及びサービスの受け入れられないレベルを含めることを考慮すること

2.2.2.12 契約書には、必要ならば、要員の異動に関する規定を含めることを考慮すること

2.2.2.13 契約書には、契約当事者それぞれの義務を含めることを考慮すること

2.2.2.14 契約書には、法律関連事項を含めることを考慮すること（例えば、データ保護に関連して制定された法律における責任。特に、契約が他国の組織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する）

2.2.2.15 契約書には、知的所有権（IPR）及び著作権の取扱い、並びに共同作業に伴う保護の条項を含めることを考慮すること

2.2.2.16 契約書には、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 及びパスワード）の管理及び使用を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.17 契約書には、利用者によるアクセス及び利用者特権の認可手続を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.18 契約書には、利用可能サービスを認可されている個人、並びにその利用者が持っている権限及び特権の内容の一覧表を維持管理するための要求事項を含むアクセス制御の合意事項を含めることを考慮すること

2.2.2.19 契約書には、検証可能な性能基準、それらの監視及び報告の定義を含めることを考慮すること

2.2.2.20 契約書には、利用者の活動を監視し、無効にする権利を含めることを考慮すること
2.2.2.21 契約上の責任を監査する権利又はそのような監査を第三者に実施させる権利を含めることを考慮すること
2.2.2.22 契約書には、問題解決のための段階的処理手順の確立を含めることを考慮すること
2.2.2.23 契約書には、障害対策の取決めを含めることを考慮すること
2.2.2.24 契約書には、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ことを考慮すること
2.2.2.25 契約書には、明確な報告の構成及び合意された報告の形式を含めることを考慮すること
2.2.2.26 契約書には、変更管理の明確な、設定された手続を含めることを考慮すること
2.2.2.27 契約書には、要求される物理的保護の管理策、及びそれらの管理策の実施を確実にするための仕組みを含めることを考慮すること
2.2.2.28 契約書には、利用者及び管理者に対する、方法、手順及びセキュリティについての訓練を含めることを考慮すること
2.2.2.29 契約書には、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を含めることを考慮すること
2.2.2.30 契約書には、セキュリティ事件・事故及びセキュリティ違反についての報告、通知及び調査に関する取決めを含めることを考慮すること
2.2.2.31 契約書には、第三者と下請け業者とのかかわりを含めることを考慮すること

2.3 外部委託

目的：情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため

2.3.1 情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述すること
2.3.1.1 外部委託契約書には、法的な要求事項（例えば、データ保護に関連して制定された法律）をどのように満たすかを取り扱うこと
2.3.1.2 外部委託契約書には、請負業者を含め、外部委託にかかわるすべての当事者がそれぞれのセキュリティの責任についての認識を確実にするためにどのような取決めが適切であるかを取り扱うこと
2.3.1.3 外部委託契約書には、組織の事業資産の完全性及び機密性をどのように維持し、それを検証するかを取り扱うこと
2.3.1.4 外部委託契約書には、慎重な取扱いを要する組織の業務情報への認可された利用者によるアクセスを制約及び制限するために、どのような物理的及び論理的管理策を用いるかを取り扱うこと
2.3.1.5 外部委託契約書には、災害の際に、サービスの可用性をどのように維持するかを取り扱うこと

2.3.1.6 外部委託契約書には、外部委託した装置については、どのようなレベルの物理的セキュリティを施すかを取り扱うこと

2.3.1.7 外部委託契約書には、監査する権利を取り扱うこと

2.3.1.8 2.2.2 に列挙した事項も、この契約の一部として考慮すること

2.3.1.9 契約では、両当事者間の合意によるセキュリティマネジメント計画において、追加されたセキュリティ要求事項及び手順を認めること

3 資産の分類及び管理

3.1 資産に対する責任

目的：組織の資産の適切な保護を維持するため

3.1.1 情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持すること

3.1.1.1 組織は、その資産並びにそれらの相対価値及び重要度を明確に把握できるようにすること

3.1.1.2 情報システムそれぞれに関連づけて重要な資産について目録を作成すること

3.1.1.3 各資産を、その現在の所在とともに、明確に識別すること

3.1.1.4 各資産を、その現在の所在とともに、セキュリティの分類について合意すること

3.1.1.5 各資産を、その現在の所在とともに、文書化すること

3.1.1.6 各資産を、その現在の所在とともに、その管理責任及びセキュリティの分類について合意すること

3.2 情報の分類

目的：情報資産の適切なレベルでの保護を確実にするため

3.2.1 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響（例えば、情報への認可されていないアクセス又は情報の損傷）を考慮に入れること

3.2.1.1 情報及び重要なデータを取り扱うシステムからの出力は、それが組織に対してもつ価値及び取扱い慎重度によってラベル付けすること

3.2.1.2 過度の分類によって無駄な出費を生じないようにすること

3.2.1.3 分類の指針には、前もって決められた個別方針に従って変わることもある、という事実を予期し考慮しておくこと

3.2.1.4 分類区分の数及びそれらの区分を用いる効用を考慮すること

3.2.1.5 他の組織からの文書に付いている分類ラベルは、同じか又は類似した名称のラベルでも、定義が異なることがあるので、その解釈には注意すること

3.2.1.6 情報（例えば、文書、データ記録、データファイル又はディスケット）の分類を定める責任、及びその分類を定期的に見直す責任は、その情報の作成者又は指定された管理者にあること

3.2.2 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること

3.2.2.1 各分類について、複製に適用する取扱い手順を定めること

3.2.2.2 各分類について、保存に適用する取扱い手順を定めること

3.2.2.3 各分類について、郵便による伝達に適用する取扱い手順を定めること

3.2.2.4 各分類について、ファクシミリによる伝達に適用する取扱い手順を定めること
3.2.2.5 各分類について、電子メールによる伝達に適用する取扱い手順を定めること
3.2.2.6 各分類について、移動電話による伝達に適用する取扱い手順を定めること
3.2.2.7 各分類について、音声メールによる伝達に適用する取扱い手順を定めること
3.2.2.8 各分類について、留守番電話による伝達に適用する取扱い手順を定めること
3.2.2.9 各分類について、言葉による伝達に適用する取扱い手順を定めること
3.2.2.10 各分類について、破棄に適用する取扱い手順を定めること
3.2.2.11 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）付けること
3.2.2.12 ラベル付けは、分類の指針に定める規則に従った分類を反映すること

4 人的セキュリティ

4.1 職務定義及び雇用におけるセキュリティ

目的：人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため

4.1.1 セキュリティの役割及び責任は、組織の情報セキュリティ基本方針で定められたとおりに、適切に文書化すること

4.1.1.1 セキュリティの役割及び責任を文書化したものには、セキュリティ基本方針を実行又は維持するための一般的な責任のすべてを含めること

4.1.1.2 セキュリティの役割及び責任を文書化したものには、特定の資産を保護するための具体的な責任を含めること

4.1.1.3 セキュリティの役割及び責任を文書化したものには、特定のセキュリティの手続を含めること

4.1.1.4 セキュリティの役割及び責任を文書化したものには、特定のセキュリティ活動を進めるための具体的な責任を含めること

4.1.2 常勤職員を採用するときは、提出された応募資料の内容を検査すること

4.1.2.1 かなりの権限をもつ地位に就く職員については、この調査を定期的に繰り返すこと

4.1.2.2 経営者は新入職員及び経験の浅い職員に取扱いに慎重を要するシステムにアクセスすることを認めたときは、それらに対する管理監督についての評価を行うこと

4.1.2.3 すべての職員の仕事は、上級の職員による定期的見直し及び承認手順のもとに置くこと

4.1.2.4 職員の個人的事情がその仕事に影響を及ぼす可能性を、管理者は認識していること

4.1.2.5 不正行為、盗難、誤り又はその他のセキュリティにかかわる問題は、当該裁判管轄で施行されている適切な法令に従って取り扱うこと

4.1.2.6 常勤職員を採用するときは、提出された応募資料の内容を検査すること

4.1.2.7 応募資料の検査において、提出された人物推薦状は役にたつかを考慮すること

4.1.2.8 応募資料の検査において、履歴書の検査をすること

4.1.2.9 応募資料の検査において、提示された学術上及び職業上の資格の確認をすること

4.1.2.10 応募資料の検査において、公的証明書（パスポート又は同種の文書）の検査をすること

4.1.2.11 組織は、その者に対して信用調査を行うこと

4.1.2.12 請負業者及び臨時職員に対しても同様の審査手続を実施すること

4.1.2.13 派遣会社が従う必要のある審査の責任及び通知の手順を、派遣会社

との契約に明記すること

4.1.3 従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること

4.1.3.1 既存の契約（機密保持条項を含むもの）の効力が及ばない臨時職員及び外部利用者に対しては、情報処理設備へのアクセスを認める前に、機密保持契約書への署名を要求すること

4.1.3.2 機密保持契約は、雇用条件又は請負契約に変更がある場合、特に従業員がその組織を離れることになるとき又は請負契約が終了するときには、見直しを行うこと

4.1.4 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること

4.1.4.1 適切ならば、これらの責任を、雇用終了後の定められた期間継続すること

4.1.4.2 従業員がセキュリティ要求事項を無視した場合に採る措置についても雇用条件に含めること

4.1.4.3 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を明確にすること

4.1.4.4 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を雇用条件に含めること

4.1.4.5 雇用条件には、雇用者側データについての重要度の分類及びその管理に対しての義務を含めること

4.1.4.6 雇用条件には、通常の勤務場所及び勤務時間からは外れた状況においても、これらの責任が適用されることの記述があること

4.2 利用者の訓練

目的：情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティ基本方針を維持していくことを確実にするため

4.2.1 組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと

4.2.1.1 教育には、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施する、情報処理設備の正しい使用方法（例えば、ログオン手順、パッケージソフトウェアの使用方法）に関する訓練を含むこと

4.3 セキュリティ事件・事故及び誤動作への対処

目的：セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため

4.3.1 セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やか

に報告すること

4.3.1.1 事件・事故の正式な報告手順を、事件・事故への対処手順とともに確立すること

4.3.1.2 事件･事故の正式な報告を受けたならば直ちに取るべき措置に着手できるようにすること

4.3.1.3 すべての従業員及び請負業者に、セキュリティ事件･事故の報告手順を認識させておくこと

4.3.1.4 すべての従業員及び請負業者に、セキュリティ事件･事故をできるだけ速やかに報告するよう要求すること

4.3.1.5 適切なフィードバックの手続を構築していること

4.3.2 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること

4.3.2.1 利用者は、全ての従業員及び請負業者に、事件・事故の発生を知った場合又はその疑いを持った場合は、できるだけ速やかに、自分の管理者又はサービス提供者に対し直接報告すること

4.3.2.2 利用者には、弱点ではないかと疑われる事柄の証明を、いかなる場合でも自ら試みるべきでないと知らせておくこと

4.3.3 ソフトウェアの誤動作を報告する手順を確立すること

4.3.3.1 ソフトウェア誤動作を報告する手順の確立において､問題の兆候及び画面に現れるメッセージへの注意を考慮すること

4.3.3.2 ソフトウェア誤動作を報告する手順の確立において､コンピュータの隔離を考慮すること

4.3.3.3 ソフトウェア誤動作を報告する手順の確立において､コンピュータの使用停止を考慮すること

4.3.3.4 ソフトウェア誤動作を報告する手順の確立において､適切な関係先に対する警報を考慮すること

4.3.3.5 ソフトウェア誤動作を報告する手順の確立において､装置の検査の前に組織のすべてのネットワークを切断することを考慮すること

4.3.3.6 ソフトウェア誤動作を報告する手順の確立において､ディスケットを別のコンピュータに移さないことを考慮すること

4.3.3.7 ソフトウェア誤動作を報告する手順の確立において､情報セキュリティ管理者への速やかな報告を考慮すること

4.3.3.8 利用者は､疑いのあるソフトウェアの除去を認可なしに試みないこと

4.3.3.9 回復処置は、適切に訓練されること

4.3.3.10 回復処置は、経験を積んだ職員が実施すること

4.3.4 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること

4.3.4.1 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みから得られる情報を、事件・事故の再発若しくは影響

の大きい事件・事故又は誤動作を識別するために用いること

4.3.5 組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること

4.3.5.1 違反した従業員に対する、正式な懲戒手続は、重大な又は度重なるセキュリティ違反を犯した疑いのある従業員に対して、正しく、かつ、公平な取扱いを確実にするものであること

5 物理的及び環境的セキュリティ

5.1 セキュリティが保たれた領域

目的：業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため

5.1.1 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること

5.1.1.1 セキュリティ境界を明確に定義すること

5.1.1.2 情報処理設備を収容した建物又は敷地の境界は、物理的に頑丈であること

5.1.1.3 敷地の外周壁を堅固な構造物とすること、及びすべての外部扉を認可されていないアクセスから開閉制御の仕組み（かんぬき、警報装置、錠など）で適切に保護すること

5.1.1.4 敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること

5.1.1.5 敷地及び建物へのアクセスは、認可された職員だけに制限すること

5.1.1.6 物理的な壁は、床から天井にわたる構造で設けること

5.1.1.7 セキュリティ境界上にあるすべての防火扉は、警報装置付き及び密閉式であること

5.1.2 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セキュリティの保たれた領域を保護すること

5.1.2.1 セキュリティが保たれた領域への訪問者を監視すること

5.1.2.2 セキュリティが保たれた領域への訪問者に立ち入り許可を求めさせること

5.1.2.3 セキュリティが保たれた領域への入退の日付・時間を記録すること

5.1.2.4 セキュリティが保たれた領域への訪問者には、認可された特定の目的に限ってのアクセスを認めること

5.1.2.5 セキュリティが保たれた領域への訪問者には、その領域のセキュリティ要求事項及び非常時の手順を説明した文書を渡すこと

5.1.2.6 取扱いに慎重を要する情報及び情報処理設備へのアクセスを管理すること

5.1.2.7 取扱いに慎重を要する情報及び情報処理設備へのアクセスは認可された者だけに制限すること

5.1.2.8 アクセスをすべて認可して妥当性を確認するために、暗証番号付きの磁気カードといった認証管理策を用いること

5.1.2.9 すべてのアクセスの監査証跡は、安全に保管しておくこと

5.1.2.10 すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること

5.1.2.11 付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること

5.1.2.12 セキュリティが保たれた領域へのアクセス権は、定期的に見直し及び更新すること

5.1.3 セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること

5.1.3.1 関連する健康及び安全に関する規制並びに標準類も考慮に入れること

5.1.3.2 隣接場所から及んでくるセキュリティ上のいかなる脅威についても考慮すること

5.1.3.3 主要な設備は、一般の人のアクセスが避けられる場所に設置すること

5.1.3.4 建物は目立たせず、その用途を示す表示は最小限とすること

5.1.3.5 情報処理作業の存在を示すものは建物の内外を問わず一切表示しないこと

5.1.3.6 複写機、ファクシミリといった支援機能及び装置は、セキュリティの保たれた領域内の適切な場所に設置すること

5.1.3.7 要員が不在のときは扉及び窓に施錠すること

5.1.3.8 一階の窓については、外部に対する防御を考慮すること

5.1.3.9 すべての外部扉及びアクセス可能な窓には、適切な侵入者の検知システムを設置すること

5.1.3.10 侵入者の検知システムは、専門の標準類に従って取り付けられること

5.1.3.11 侵入者の検知システムは、定期的に点検すること

5.1.3.12 無人の領域には常に警報装置を稼働させること

5.1.3.13 コンピュータ室又は通信室といった他の領域においても、警報装置を設置すること

5.1.3.14 組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと

5.1.3.15 取扱いに慎重を要する情報処理設備の所在を掲げた職員録及び社内電話帳は、一般の人に容易に見られないようにすること

5.1.3.16 危険物又は可燃物は、セキュリティが保たれた領域から十分に離れた場所に、安全に保管すること

5.1.3.17 セキュリティが保たれた領域には、事務用品などを、必要もないのに大量に保管しないこと

5.1.3.18 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと

5.1.4 セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること

5.1.4.1 セキュリティが保たれた領域の存在又はそこでの作業は、その必要がある要員だけが知っていること

5.1.4.2 セキュリティが保たれた領域において監視もなく作業することは、避けること

5.1.4.3 セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと

5.1.4.4 セキュリティが保たれた領域を無人にするときは、定期的に検査すること

5.1.4.5 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること

5.1.4.6 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは認可のもとにおくこと

5.1.4.7 セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは監視下におくこと

5.1.4.8 あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、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こと

5.1.4.9 認可なしの、写真機、ビデオカメラ、録音機、又はその他の記録装置の使用は、許さないこと

5.1.5 品物を受け渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること

5.1.5.1 品物を受け渡しする場所についてのセキュリティ要求事項は、リスクアセスメントに基づいて決定すること

5.1.5.2 建物の外から一時保管場所へのアクセスは、本人の確認及び認可を受けた要員に限定すること

5.1.5.3 一時保管場所については、建物内の他の場所にアクセスすることなく受渡しの要員が荷おろしできるように、設計を行うこと

5.1.5.4 一時保管場所の内部扉を開いているときは、外部扉を締めること

5.1.5.5 一時保管場所から使用場所に搬入品を移送する前に、危険の可能性がないかどうか、その品物を検査すること

5.1.5.6 敷地内に搬入するときには、搬入品の登録を行うこと

5.2 装置のセキュリティ

目的：資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため

5.2.1 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること

5.2.1.1 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること

5.2.1.2 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること

5.2.1.3 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること

5.2.1.4 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の

策定を考慮すること

5.2.1.5 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること

5.2.1.6 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること

5.2.1.7 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること

5.2.2 装置は、停電、その他の電源異常から保護すること

5.2.2.1 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること

5.2.2.2 電源の多重化をすること

5.2.2.3 無停電電源装置（UPS)を設置すること

5.2.2.4 非常用発電機の設置をすること

5.2.2.5 障害対策計画では、UPS が故障した場合に取るべき措置についても計画しておくこと

5.2.2.6 UPS は、容量が十分であることを定期的に確認すること

5.2.2.7 UPS は、製造者の推奨に従って点検すること

5.2.2.8 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること

5.2.2.9 発電機を使用する場合、製造者の推奨に従って定期的に点検すること

5.2.2.10 発電機を長時間運転できるように、燃料の十分な供給を確保すること

5.2.2.11 電源の緊急スイッチは、機械室の非常口近くに設置すること

5.2.2.12 主電源の停電時用として非常用照明を備えること

5.2.2.13 落雷防護はすべての建物に備えること

5.2.2.14 すべての外部通信回線に落雷防護フィルタを付けること

5.2.3 データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること

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、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと

5.2.3.2 ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること

5.2.3.3 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こと

5.2.3.4 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること

5.2.3.5 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること

5.2.3.6 取扱に慎重を要するシステム又は重要なシステムに対しては、データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、代替経路又は伝送媒体を使用すること

5.2.3.7 取扱に慎重を要するシステム又は重要なシステムに対しては、データ伝送又は情報サービスに使用する通信ケーブルの配線は光ファイバケーブルを使用すること

5.2.3.8 取扱に慎重を要するシステム又は重要なシステムに対しては、認可されていない装置がケーブルに取り付けられているかどうかについての調査すること

5.2.4 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること

5.2.4.1 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること

5.2.4.2 認可された保守担当者だけが装置の修理及び手入れを実施すること

5.2.4.3 すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること

5.2.4.4 すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること

5.2.4.5 装置を保守するために搬出する場合、適切な管理策を施すこと

5.2.4.6 保険約款によって定められたすべての要求事項に従うこと

5.2.5 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること

5.2.5.1 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること

5.2.5.2 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと

5.2.5.3 ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること

5.2.5.4 装置の保護に関しては、製造者の指示に常に従うこと

5.2.5.5 在宅作業についての管理策は、リスクアセスメントによって決定すること

5.2.5.6 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること

5.2.5.7 事業所外の装置を保護するために、十分な保険が付保されていること

5.2.5.8 セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること

5.2.6 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること

5.2.6.1 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること

5.2.6.2 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が、消去又は上書きされているか確認すること

5.3 その他の管理策

目的：情報及び情報処理設備の損傷又は盗難を防止するため

5.3.1 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、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の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること

5.3.1.1 クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること

5.3.1.2 クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること

5.3.1.3 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管すること

5.3.1.4 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと

5.3.1.5 パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと

5.3.1.6 パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること

5.3.1.7 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること

5.3.1.8 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと

5.3.1.9 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと

5.3.2 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできないこと

5.3.2.1 持出し時及び返却時に記録を残すこと

5.3.2.2 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること

5.3.2.3 現場検査があることを各人が認識していること

6 通信及び運用管理

6.1 運用手順及び責任

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 セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと

6.1.1.1 操作手順は、正式な文書として取り扱うこと

6.1.1.2 操作手順が変更の場合は管理者によって認可されること

6.1.1.3 操作手順には、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こと

6.1.1.4 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.5 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.6 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.7 操作手順には、特別な出力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こと

6.1.1.8 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること

6.1.1.9 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること

6.1.2 情報処理設備及びシステムの変更について管理すること

6.1.2.1 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること

6.1.2.2 運用プログラムは、厳重な変更管理の下に置くこと

6.1.2.3 プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること

6.1.2.4 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合すること

6.1.2.5 重要な変更を識別及び記録すること

6.1.2.6 重要な変更の潜在的な影響の評価をすること

6.1.2.7 変更の申出を正式に承認する手順を確立すること

6.1.2.8 変更の詳細の、全関係者への通知をすること

6.1.2.9 うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること

6.1.3 セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立

すること

6.1.3.1 情報システムの故障及びサービスの停止に対処できるように、手順を定めること

6.1.3.2 サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること

6.1.3.3 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること

6.1.3.4 機密性に対する違反に対処できるように、手順を定めること

6.1.3.5 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を含めること

6.1.3.6 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること

6.1.3.7 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること

6.1.3.8 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること

6.1.3.9 通常の障害対策計画手順には、監督機関に対する措置の報告を含めること

6.1.3.10 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること

6.1.3.11 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での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収集し、安全に保管すること

6.1.3.12 ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること

6.1.3.13 セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理されること

6.1.3.14 事件・事故管理手順では、身分が明らかで、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、許すことを考慮すること

6.1.3.15 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること

6.1.3.16 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること

6.1.3.17 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること

6.1.4 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮すること

6.1.4.1 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による

監督といった他の管理策を考慮すること

6.1.4.2 セキュリティ監査は、独立性を維持すること

6.1.4.3 どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること

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

6.1.4.5 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること

6.1.4.6 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること

6.1.5 開発施設、試験施設及び運用施設を分離するため、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、文書化すること

6.1.5.1 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること

6.1.5.2 同様な分離は、開発と試験との機能間でも実行すること

6.1.5.3 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持すること

6.1.5.4 開発施設、試験施設及び運用施設を分離すること

6.1.5.5 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること

6.1.5.6 開発作業と試験作業とは、可能な限り分離すること

6.1.5.7 コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと

6.1.5.8 運用システム及び試験システムに対しては、異なるログオン手順を用いること

6.1.5.9 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること

6.1.5.10 メニューには、適切な識別メッセージを表示すること

6.1.5.11 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得すること

6.1.5.12 管理用パスワードは、使用後には変更されることを確実にすること

6.1.6 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること

6.1.6.1 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること

6.1.6.2 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること

6.1.6.3 外部委託による施設管理においては、事業継続計画との関連性を考慮すること

6.1.6.4 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮すること

6.1.6.5 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当てを考慮すること

6.1.6.6 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順を考慮すること

6.2 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

6.2.1 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること

6.2.1.1 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること

6.2.1.2 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること

6.2.1.3 管理者は、使用傾向、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と関連した傾向を識別すること

6.2.1.4 システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を用いること

6.2.2 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること

6.2.2.1 管理者は、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、明確に定義すること

6.2.2.2 管理者は、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、文書化すること

6.2.2.3 管理者は、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、合意すること

6.2.2.4 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること

6.2.2.5 管理者は、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、試験することを確実にすること

6.2.2.6 システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること

6.2.2.7 システムの受け入れにおいて、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考慮すること

6.2.2.8 システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮すること

6.2.2.9 システムの受け入れにおいて、合意された適切なセキュリティ管理策

を考慮すること

6.2.2.10 システムの受け入れにおいて、手動による有効な手順を考慮すること

6.2.2.11 システムの受け入れにおいて、事業継続の取決めを考慮すること

6.2.2.12 システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること

6.2.2.13 システムの受け入れにおいて、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について考慮すること

6.2.2.14 システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと

6.2.2.15 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと

6.2.2.16 主要な新しいシステム開発においては、適切な試験を実施し、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こと

6.3 悪意のあるソフトウェアからの保護

目的：ソフトウェア及び情報の完全性を保護するため

6.3.1 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること

6.3.1.1 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと

6.3.1.2 ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること

6.3.1.3 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としての個別方針を考慮すること

6.3.1.4 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期更新を考慮すること

6.3.1.5 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること

6.3.1.6 未承認のファイル又は無認可の変更の存在に対しては、正式に調査すること

6.3.1.7 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること

6.3.1.8 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のすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること

6.3.1.9 システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること

6.3.1.10 ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考慮すること

6.3.1.11 ウイルス感染からの回復のための適切な事業継続計画を考慮すること

6.3.1.12 悪意のあるソフトウェアに関するすべての情報を確認すること

6.3.1.13 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考慮すること

6.3.1.14 管理者は、単なるいたずらと真のウイルス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、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること

6.3.1.15 職員は、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認識していること

6.4 システムの維持管理(Housekeeping)

目的：情報処理及び通信サービスの完全性及び可用性を維持するため

6.4.1 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること

6.4.1.1 災害又は媒体故障が発生した後、極めて重要なすべての業務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こと

6.4.1.2 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた場所に保管すること

6.4.1.3 重要な業務用ソフトウェアについては、少なくとも 3 世代又は 3 サイクル分のバックアップのための情報を保持すること

6.4.1.4 バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと

6.4.1.5 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること

6.4.1.6 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定しておくこと

6.4.1.7 バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること

6.4.1.8 復元手順は、定期的に検査及び試験すること

6.4.2 運用担当者は、自分の作業の記録を継続すること

6.4.2.1 記録には、システムの起動及び終了の時刻を含めること
6.4.2.2 記録には、システム誤り及び実施した是正処置を含めること
6.4.2.3 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること
6.4.2.4 記録には、記録の作成者の名前を含めること

6.4.3 運用担当者の記録は、定期的に独立した検査を受けること

6.4.4 障害については報告を行い、是正処置をとること
6.4.4.1 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること
6.4.4.2 報告された障害の取扱いについては、明確な規定があること
6.4.4.3 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと
6.4.4.4 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを含むこと

6.5 ネットワークの管理

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

6.5.1 ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること
6.5.1.1 ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること
6.5.1.2 ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること
6.5.1.3 ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること
6.5.1.4 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立すること
6.5.1.5 公衆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、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること
6.5.1.6 サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整すること

6.6 媒体の取扱い及びセキュリティ

目的：財産に対する損害及び事業活動に対する妨害を回避するため

6.6.1 コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること

6.6.1.1 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること

6.6.1.2 組織の管理外となる媒体のすべてについて、認可を必要とすること

6.6.1.3 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること

6.6.1.4 すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること

6.6.1.5 コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること

6.6.2 媒体が不要となった場合は、安全、かつ、確実に処分すること

6.6.2.1 媒体の安全な処分のための、正式な手順を確立すること

6.6.2.2 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること

6.6.2.3 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること

6.6.2.4 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと

6.6.2.5 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること

6.6.2.6 処分しようとする媒体を集める場合、集積することによる影響に配慮すること

6.6.3 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること

6.6.3.1 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類に対応させて策定すること

6.6.3.2 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること

6.6.3.3 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮すること

6.6.3.4 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持について考慮すること

6.6.3.5 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを確実にすること

6.6.3.6 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること

6.6.3.7 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮すること

6.6.3.8 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること

6.6.3.9 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて考慮すること

6.6.3.10 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること

6.6.4 認可されていないアクセスからシステムに関する文書を保護すること

6.6.4.1 システムに関する文書は、安全に保管すること

6.6.4.2 システムに関する文書にアクセスできる者は、人数を最小限に抑えること

6.6.4.3 システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること

6.6.4.4 システムに関する文書で、公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること

6.7 情報及びソフトウェアの交換

目的：組織間で交換される情報の紛失、改ざん又は誤用を防止するため

6.7.1 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと

6.7.1.1 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること

6.7.1.2 セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること

6.7.1.3 セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること

6.7.1.4 セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術標準を考慮すること

6.7.1.5 セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること

6.7.1.6 セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること

6.7.1.7 セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考慮すること

6.7.1.8 セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、

及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考慮すること

6.7.1.9 セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること

6.7.1.10 セキュリティ条件にかかわる合意では、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特別な管理策を考慮すること

6.7.2 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること

6.7.2.1 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること

6.7.2.2 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いること

6.7.2.3 媒体の配送においては、宅配業者の身分を確認する手順を導入すること

6.7.2.4 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること

6.7.2.5 媒体の配送においては、施錠されたコンテナの使用を考慮すること

6.7.2.6 媒体の配送においては、手渡しを考慮すること

6.7.2.7 媒体の配送においては、開封防止包装の利用を考慮すること

6.7.2.8 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること

6.7.2.9 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること

6.7.3 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること

6.7.3.1 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求すべきか）について考慮すること

6.7.3.2 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか。取引相手はこれらをどうやって知るか）について考慮すること

6.7.3.3 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること

6.7.3.4 電子商取引のセキュリティにおいては、価格情報について考慮すること

6.7.3.5 電子商取引のセキュリティにおいては、注文取引について考慮すること

6.7.3.6 電子商取引のセキュリティにおいては、審査について考慮すること

6.7.3.7 電子商取引のセキュリティにおいては、決済について考慮すること

6.7.3.8 電子商取引のセキュリティにおいては、注文について考慮すること
6.7.3.9 電子商取引のセキュリティにおいては、責任について考慮すること
6.7.3.10 電子商取引に関する当事者間の合意は、権限の詳細も含め、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ること
6.7.3.11 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も、合意を交わすこと
6.7.3.12 公開している取引システムでは、その取引条件を顧客に公表すること
6.7.3.13 電子商取引に用いる基幹コンピュータのも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なネットワーク相互接続のセキュリティ上のかかわりについて、考慮すること

6.7.4 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること
6.7.4.1 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること
6.7.4.2 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること
6.7.4.3 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること
6.7.4.4 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の責任を含めること
6.7.4.5 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること
6.7.4.6 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること
6.7.4.7 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること

6.7.5 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること
6.7.5.1 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること
6.7.5.2 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること
6.7.5.3 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること
6.7.5.4 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること
6.7.5.5 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについ

て考慮すること

6.7.5.6 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮すること

6.7.5.7 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること

6.7.5.8 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること

6.7.5.9 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること

6.7.5.10 電子オフィスシステムのセキュリティにおいては、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について考慮すること

6.7.6 電子的に公開した情報の完全性を保護するように注意すること

6.7.6.1 公開されたシステム（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地域又は取引が行われている地域に適用される、法律、規則及び規制に適合することを確実にすること

6.7.6.2 情報を公開する前に、正式な認可の手続がとられること

6.7.6.3 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって保護すること

6.7.6.4 公開している電子システムは、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、情報は、あらゆるデータ保護に関連して制定された法律に従って収集すること

6.7.6.5 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること

6.7.6.6 取扱いに慎重を要する情報は、収集の過程及び保管時に保護すること

6.7.6.7 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこと

6.7.7 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策をもつこと

6.7.7.1 音声･画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること

6.7.7.2 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること

6.7.7.3 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせること

6.7.7.4 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残さないようにさせること

6.7.7.5 職員に、ファクシミリを用いる上での問題点を意識させること

7 アクセス制御

7.1 アクセス制御に関する業務上の要求事項

目的：情報へのアクセス制御をするため

7.1.1 アクセス制御についての業務上の要求事項を定義し、文書化すること

7.1.1.1 利用者ごと、または利用者からなるグループごとに対するアクセス制御規則を、アクセス方針宣言書に明確に記述すること

7.1.1.2 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること

7.1.1.3 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること

7.1.1.4 アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること

7.1.1.5 アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること

7.1.1.6 アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮すること

7.1.1.7 アクセス制御に関する個別方針には、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すること

7.1.1.8 アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること

7.1.1.9 アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること

7.1.1.10 アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること

7.1.1.11 アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別すること

7.1.1.12 アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定すること

7.1.1.13 アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をすること

7.1.1.14 アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス許可の変更をすること

7.1.1.15 アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をすること

7.2 利用者のアクセス管理

目的：情報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

7.2.1 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること

7.2.1.1 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること

7.2.1.2 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者 ID を用いること

7.2.1.3 利用者登録手続において、グループ ID の使用は、実施される作業に適切な場合にだけ許可すること

7.2.1.4 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査すること

7.2.1.5 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査すること

7.2.1.6 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査すること

7.2.1.7 利用者登録手続において、重複する利用者 ID が別の利用者に発行されないことを確実にすること

7.2.1.8 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮すること

7.2.1.9 利用者登録手続において、アクセス権の宣言書を利用者に発行すること

7.2.1.10 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること

7.2.1.11 利用者登録手続において、認可手続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

7.2.1.12 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること

7.2.1.13 利用者登録手続において、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を直ちに取り消すこと

7.2.1.14 利用者登録手続において、もはや必要のない利用者 ID 及びアカウントがないか定期的に検査し、あれば削除すること

7.2.2 特権の割り当て及び使用は、制限し、管理すること

7.2.2.1 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること

7.2.2.2 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別すること

7.2.2.3 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること

7.2.2.4 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと

7.2.2.5 特権の割り当てにおいて、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使用を促進すること

7.2.2.6 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者 ID とは別の利用者 ID に、割り当てること

7.2.3 パスワードの割当ては、正規の管理手続によって統制すること

7.2.3.1 パスワード管理手続の取組において、個人のパスワードを秘密に保つこと

7.2.3.2 パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に求めること

7.2.3.3 パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること

7.2.3.4 パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること

7.2.3.5 パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること

7.2.3.6 パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避けること

7.2.3.7 パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること

7.2.3.8 パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと

7.2.3.9 パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びＩＣカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮すること

7.2.4 データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施する

こと

7.2.4.1 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと

7.2.4.2 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと

7.2.4.3 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、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こと

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を防止するため

7.3.1 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと

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に助言すること

7.3.1.2 すべての利用者に、パスワードを紙に記録して保管しないように助言すること

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は、パスワードを変更するように助言すること

7.3.1.4 すべての利用者に、最短 6 文字の質の良いパスワードを選択すること

7.3.1.5 すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること

7.3.1.6 すべての利用者に、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に助言すること

7.3.1.7 すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること

7.3.1.8 すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること

7.3.1.9 すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること

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に助言すること

7.3.1.11 すべての利用者に、利用者が複数のサービス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、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言すること

7.3.2 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること

7.3.2.1 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護をするこ

と

7.3.2.2 無人運転の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、すべての利用者及び請負業者に認識させること

7.3.2.3 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること

7.3.2.4 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること

7.3.2.5 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、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使用からセキュリティを保つように保護するように助言すること

7.4 ネットワークのアクセス制御

目的：ネットワークを介したサービスの保護のため

7.4.1 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること

7.4.1.1 ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること

7.4.1.2 ネットワーク及びネットワークサービスの使用についての個別方針には、アクセスすること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こと

7.4.1.3 ネットワーク及びネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること

7.4.1.4 ネットワーク及びネットワークサービスの使用についての個別方針には、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管理策及び管理手順を対象にすること

7.4.1.5 ネットワーク及びネットワークサービスの使用についての個別方針は、業務上のアクセス制御方針と整合していること

7.4.2 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること

7.4.2.1 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること

7.4.2.2 指定された接続経路には、専用線又は専用電話番号を割り当てること

7.4.2.3 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること

7.4.2.4 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること

7.4.2.5 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること

7.4.2.6 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること

7.4.2.7 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること

7.4.2.8 組織内の利用者グループのために別々の論理領域（例えば、仮想私設網（Virtual Private Network：VPN））を設定することによって、ネットワークアクセスを制限すること

7.4.2.9 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと

7.4.3 遠隔地からの利用者のアクセスには、認証を行うこと

7.4.3.1 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こと

7.4.3.2 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること

7.4.3.3 コールバックの手順及び制御を徹底的に試験すること

7.4.4 遠隔コンピュータシステムへの接続は、認証されること

7.4.5 診断ポートへのアクセスは、セキュリティを保つように制御されること

7.4.5.1 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること

7.4.5.2 ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.4.6 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること

7.4.6.1 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること

7.4.6.2 ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと

7.4.6.3 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮すること

7.4.7 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと

7.4.7.1 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること

7.4.7.2 電子メールには制限を適用すること

7.4.7.3 一方向のファイル転送には制限を適用すること

7.4.7.4 双方向のファイル転送には制限を適用すること

7.4.7.5 対話型アクセスには制限を適用すること

7.4.7.6 時間帯又は日付に対応したネットワークアクセスには制限を適用すること

7.4.8 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、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、経路指定の制御策を組み込むこと

7.4.8.1 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること

7.4.8.2 ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと

7.4.9 ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.4.9.1 ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること

7.5 オペレーティングシステムのアクセス制御

目的：認可されていないコンピュータアクセスを防止するため

7.5.1 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること

7.5.2 情報サービスへのアクセスは、安全なログオン手続を経て達成されること

7.5.2.1 コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること

7.5.2.2 システムについての情報の開示は最小限にすること

7.5.2.3 ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しないこと

7.5.2.4 ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示すること

7.5.2.5 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表示をしないこと

7.5.2.6 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こと

7.5.2.7 許容されるログオンの試みの失敗回数を制限すること

7.5.2.8 ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと

7.5.2.9 ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること

7.5.2.10 ログオンの失敗時には、データリンク接続を切ること

7.5.2.11 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こと

7.5.2.12 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こと

7.5.2.13 ログオンの失敗時には、失敗した試みを記録すること

7.5.2.14 ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること

7.5.2.15 ログオンが無事できた時点で、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こと

7.5.3 すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者 ID）を保有すること

7.5.3.1 利用者 ID には、利用者の特権レベル（例えば、管理者(マネージャ)、監督者(スーパーバイザ)）を表示しないこと

7.5.3.2 明らかに業務上の利点がある例外的状況において、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こと

7.5.4 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること

7.5.4.1 パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること

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

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

7.5.4.4 パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること

7.5.4.5 パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること

7.5.4.6 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、一定期間、維持し再使用を防止すること

7.5.4.7 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こと

7.5.4.8 パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること

7.5.4.9 パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること

7.5.4.10 パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること

7.5.5 システムユーティリティのために認証手順を使用すること

7.5.5.1 業務用ソフトウェアからシステムユーティリティを分離すること

7.5.5.2 システムユーティリティの使用を、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こと

7.5.5.3 システムユーティリティを臨時に使用する際には認可をすること

7.5.5.4 システムユーティリティの使用の制限をすること

7.5.5.5 システムユーティリティのすべての使用を記録すること

7.5.5.6 システムユーティリティの認可レベルの明確化及び文書化をすること

7.5.5.7 すべての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の除去をすること

7.5.6 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮すること

7.5.6.1 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと

7.5.6.2 脅迫に対する警報に対応する責任及び手順を明確に定めること

7.5.7 リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末は遮断されること

7.5.7.1 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること

7.5.7.2 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであること

7.5.8 リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供すること

7.5.8.1 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session)を用いること

7.5.8.2 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること

7.6 業務用ソフトウェアのアクセス制御

目的：認可されていないコンピュータアクセスを防止するため

7.6.1 ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限すること

7.6.1.1 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること

7.6.1.2 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮すること

7.6.1.3 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮すること

7.6.1.4 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること

7.6.1.5 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にすること

7.6.1.6 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること

7.6.2 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること

7.6.2.1 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること

7.6.2.2 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること

7.7 システムアクセス及びシステム使用状況の監視

目的：認可されていない活動を検出するため

7.7.1 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること

7.7.1.1 監査記録には、利用者ＩＤを含めること

7.7.1.2 監査記録には、ログオン及びログオフの日時を含めること

7.7.1.3 監査記録には、可能ならば、端末のＩＤ又は所在地を含めること

7.7.1.4 監査記録には、システムへのアクセスを試みて、成功及び失敗した記

録を含めること

7.7.1.5 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること

7.7.2 情報処理設備の使用状況を監視する手順を確立すること

7.7.2.1 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること

7.7.2.2 監視項目には、認可されているアクセスについて、利用者ＩＤを含むこと

7.7.2.3 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと

7.7.2.4 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと

7.7.2.5 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと

7.7.2.6 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと

7.7.2.7 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること

7.7.2.8 監視項目には、すべての特権操作について、システムの起動及び停止を含めること

7.7.2.9 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること

7.7.2.10 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること

7.7.2.11 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること

7.7.2.12 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること

7.7.2.13 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること

7.7.2.14 監視項目には、システム警告又は故障について、システム記録例外事項を含めること

7.7.2.15 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること

7.7.3 監視の結果は、定期的に見直すこと

7.7.3.1 監視結果の見直しの頻度は、関係するリスクによって決めること

7.7.3.2 考慮すべきリスク要因には、業務手続に与える重要性の度合を含めること

7.7.3.3 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること

7.7.3.4 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること

7.7.3.5 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること

7.7.4 システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること

7.7.4.1 セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製すること

7.7.4.2 ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮すること

7.7.4.3 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮すること

7.7.4.4 記録機能のセキュリティに対して注意すること

7.7.4.5 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること

7.7.5 コンピュータの時計は正しく設定すること

7.7.5.1 コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時（例えば、万国標準時に（ＵＣＴ）又は現地の標準時）に合わせること

7.7.5.2 コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること

7.8 移動型計算処理及び遠隔作業

目的：移動型計算処理及び遠隔作業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

7.8.1 ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特別な注意を払うこと

7.8.1.1 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること

7.8.1.2 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること

7.8.1.3 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること

7.8.1.4 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと

7.8.1.5 悪意のあるソフトウェアに対抗する手順を整えること
7.8.1.6 悪意のあるソフトウェアに対抗する手順は最新のものであること
7.8.1.7 移動型計算処理を用いる要員に対する訓練を計画すること
7.8.1.8 情報を素早く、容易にバックアップできる装置が利用可能となっていること
7.8.1.9 これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること
7.8.1.10 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと
7.8.1.11 ネットワークに接続された移動型設備の使用に対して適切な保護がなされること
7.8.1.12 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること
7.8.1.13 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること
7.8.1.14 大切な、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こと（可能ならば、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こと）

7.8.2 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手配されていることを確実にすること
7.8.2.1 遠隔作業の場所に適切な保護が整っていること
7.8.2.2 遠隔作業は、経営陣によって認可され、管理されること
7.8.2.3 遠隔作業は、この作業形態のため適切に手配されていること
7.8.2.4 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること
7.8.2.5 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可すること
7.8.2.6 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮すること
7.8.2.7 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮すること
7.8.2.8 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること
7.8.2.9 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること
7.8.2.10 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報

の取扱いに慎重を要する度合を考慮すること

7.8.2.11 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮すること

7.8.2.12 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの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すること

7.8.2.13 遠隔作業活動のための適切な装置を準備すること

7.8.2.14 遠隔作業活動のための適切な保管棚・庫の準備をすること

7.8.2.15 遠隔作業活動のための許可される作業を明確にすること

7.8.2.16 遠隔作業活動のための作業時間を明確にすること

7.8.2.17 遠隔作業活動のための保持してもよい情報の分類を明確にすること

7.8.2.18 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること

7.8.2.19 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること

7.8.2.20 遠隔作業を行う場所の物理的なセキュリティを確保すること

7.8.2.21 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明確にすること

7.8.2.22 ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること

7.8.2.23 バックアップ及び事業継続のための手順を明確にすること

7.8.2.24 監査及びセキュリティの監視を行うこと

7.8.2.25 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること

8 システムの開発及び保守

8.1 システムのセキュリティ要求事項

目的：情報システムへのセキュリティの組み込みを確実にするため

8.1.1 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には、管理策についての要求事項を明確にすること

8.1.1.1 セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること

8.1.1.2 セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること

8.1.1.3 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考慮すること

8.1.1.4 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること

8.1.1.5 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること

8.1.1.6 セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること

8.1.1.7 セキュリティが確保できなかった場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害の可能性もセキュリティ要求事項及び管理策に反映されること

8.2 業務用システムのセキュリティ

目的：業務用システムにおける利用者データの消失、変更又は誤用を防止するため

8.2.1 業務用システムに入力されるデータは、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こと

8.2.1.1 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること

8.2.1.2 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること

8.2.1.3 データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること

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の二重入力又はその他の入力検査を実施すること

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の二重入力又はその他の入力検査を実施すること

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の二重入力又はその他の入力検査を実施すること

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に重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること

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の紙に印刷した入力文書の点検を考慮すること

8.2.1.9 妥当性確認の誤りに対応する手順について考慮すること

8.2.1.10 入力データのもっともらしさを試験する手順について考慮すること

8.2.1.11 データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること

8.2.2 処理したデータの改変を検出するために、システムに妥当性の検査を組み込むこと

8.2.2.1 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること

8.2.2.2 データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること

8.2.2.3 プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること

8.2.2.4 データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮すること

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とるための処理又はバッチの制御を考慮すること

8.2.2.6 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること

8.2.2.7 システム生成データの妥当性確認を考慮すること

8.2.2.8 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること

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検査を考慮すること

8.2.2.10 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること

8.2.2.11 プログラムが正しい順序で実行されることの検査を考慮すること

8.2.2.12 プログラムが正しい順序で実行されない場合は終了され、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検査を考慮すること

8.2.3 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮すること

8.2.3.1 メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと

8.2.4 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること

8.2.4.1 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと

8.2.4.2 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制御の回数を含むこと

8.2.4.3 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、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供給を含むこと

8.2.4.4 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと

8.2.4.5 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと

8.3 暗号による管理策

目的：情報の機密性、真正性又は完全性を保護するため

8.3.1 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること

8.3.1.1 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること

8.3.1.2 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを考慮すること

8.3.1.3 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを考慮すること

8.3.1.4 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について考慮すること

8.3.1.5 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について考慮すること

8.3.1.6 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを考慮すること

8.3.1.7 暗号による管理策の使用に関する個別方針を定めるとき、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を考慮すること

8.3.2 取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化（Encryption）すること

8.3.2.1 リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること

8.3.2.2 組織における暗号利用の個別方針を実施するとき、世界の異なる地域

における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること

8.3.2.3 暗号技術の輸出入に適用される規制も考慮すること

8.3.2.4 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること

8.3.2.5 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること

8.3.3 電子文書の真正性及び完全性を保護するために、ディジタル署名を用いること

8.3.3.1 秘密かぎの機密性を保護するために注意を払うこと

8.3.3.2 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管すること

8.3.3.3 公開かぎの完全性を保護すること

8.3.3.4 ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること

8.3.3.5 ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること

8.3.3.6 電子商取引の場合、ディジタル署名の法的位置付けを知ること

8.3.3.7 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること

8.3.3.8 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求めること

8.3.4 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には、否認防止サービスを用いること

8.3.5 一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いること

8.3.5.1 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること

8.3.5.2 すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護すること

8.3.5.3 かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いること

8.3.5.4 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を生成する方法を定めること

8.3.5.5 かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること

8.3.5.6 かぎ管理システムでは、予定している利用者にかぎを配付する方法を

定めること

8.3.5.7 かぎ管理システムでは、かぎを保存する方法を定めること

8.3.5.8 かぎ管理システムでは、かぎを変更又は更新する方法を定めること

8.3.5.9 かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること

8.3.5.10 かぎ管理システムでは、かぎを無効にする方法について定めること

8.3.5.11 かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること

8.3.5.12 かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定めること

8.3.5.13 かぎ管理システムでは、かぎを破壊する方法を定めること

8.3.5.14 かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること

8.3.5.15 かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めること

8.3.5.16 かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクによって決めること

8.3.5.17 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること

8.3.5.18 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に関する問題を扱うこと

8.4 システムファイルのセキュリティ

目的：IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため

8.4.1 運用システムでのソフトウェアの実行を管理すること

8.4.1.1 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること

8.4.1.2 運用システムは、実行可能なコードだけを保持すること

8.4.1.3 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しないこと

8.4.1.4 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること

8.4.1.5 古い版のソフトウェアは、事故対策用として保持すること

8.4.1.6 運用システムに使用されるベンダー供給ソフトウェアは、供給者によ

って支援されるレベルで、維持管理されること

8.4.1.7 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること

8.4.1.8 セキュリティ上の欠陥を除去するか又は軽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こと

8.4.1.9 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること

8.4.1.10 供給者の活動は監視されることが望ましい

8.4.2 試験データを保護し、管理すること

8.4.2.1 システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと

8.4.2.2 個人情報が入っている運用データベースは、使用しないようにすること

8.4.2.3 個人情報が入っている情報を使用する場合は、使用する前に、個人的要素を消去すること

8.4.2.4 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用すること

8.4.2.5 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けること

8.4.2.6 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること

8.4.2.7 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること

8.4.3 プログラムソースライブラリへのアクセスに対しては、厳しい管理を維持すること

8.4.3.1 可能な限り、プログラムソースライブラリは、運用システムに含めないこと

8.4.3.2 各アプリケーションごとに、プログラムライブラリ管理責任者を任命すること

8.4.3.3 IT 支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと

8.4.3.4 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと

8.4.3.5 IT 支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること

8.4.3.6 プログラムリストは、セキュリティの保たれた環境に保持されること

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、監査記録を維持管理すること

8.4.3.8 ソースプログラムの旧版は、記録保管しておくこと

8.4.3.9 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと

8.4.3.10 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こと

8.4.3.11 各アプリケーションごとに、プログラムライブラリ管理責任者を任命すること

8.5 開発及び支援過程におけるセキュリティ

目的：業務用システム及び情報のセキュリティを維持するため

8.5.1 情報システムの変更の実施を厳しく管理すること

8.5.1.1 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないように考慮すること

8.5.1.2 支援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

8.5.1.3 変更に対する正式な合意及び承認が得られていることを確実にすること

8.5.1.4 業務用ソフトウェア及び運用の変更管理手順は統合されること

8.5.1.5 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること

8.5.1.6 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること

8.5.1.7 業務用ソフトウェア及び運用の変更過程では、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この手順をレビューすること

8.5.1.8 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識別すること

8.5.1.9 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を得ること

8.5.1.10 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること

8.5.1.11 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること

8.5.1.12 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること

8.5.1.13 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実にすること

8.5.1.14 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェ

アの更新について版数の管理を行うこと

8.5.1.15 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること

8.5.1.16 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること

8.5.1.17 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること

8.5.2 オペレーティングシステムを変更した場合は、業務用システムをレビューし、試験すること

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及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること

8.5.2.2 年間支援計画及び予算には、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ようにすること

8.5.2.3 実施前に行う適切なレビューに間に合うように、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こと

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こと

8.5.3 パッケージソフトウェアの変更は極力行わないようにし、絶対に必要な変更を厳しく管理すること

8.5.3.1 ベンダー供給のパッケージソフトウェアは、変更しないで使用すること

8.5.3.2 パッケージソフトウェアの変更が絶対必要であると判断された場合は、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を考慮すること

8.5.3.3 パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること

8.5.3.4 パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること

8.5.3.5 パッケージソフトウェアの変更が絶対必要であると判断された場合は、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影響を考慮すること

8.5.3.6 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと

8.5.3.7 変更はすべて、完全に試験すること

8.5.3.8 変更はすべて、文書化すること

8.5.3.9 将来更新されたソフトウェアに再び適用できるようにすること

8.5.4 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検

査すること
8.5.4.1 プログラムは定評のある開発元のものだけを購入すること
8.5.4.2 コードの確認ができるようにソースコードでプログラムを購入すること
8.5.4.3 評価された製品を用いること
8.5.4.4 使用前にすべてのソースコードを検査すること
8.5.4.5 一旦導入したコードへのアクセス及びそのコードへの変更を管理すること
8.5.4.6 重要なシステムでの作業には確実に信頼できる要員を用いること
8.5.5 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために、管理策を用いること
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所有権について考慮すること
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考慮すること
8.5.5.3 ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること
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について考慮すること
8.5.5.5 ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること
8.5.5.6 ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること

9 事業継続管理

9.1 事業継続管理の種々の面

目的：事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため

9.1.1 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること

9.1.1.1 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること

9.1.1.2 業務手続の中断が事業に及ぼすと思われる影響を理解し（組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である）、情報処理施設の事業目的を確立すること

9.1.1.3 事業継続の手続の一部をなすこともある適切な保険への加入を考慮すること

9.1.1.4 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること

9.1.1.5 合意された戦略に従って事業継続計画を明確にし、文書化すること

9.1.1.6 実行されている計画及び手続を定期的に試験し、更新すること

9.1.1.7 事業継続管理が組織の手続及び機構に確実に組み込まれるようにすること

9.1.1.8 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること

9.1.2 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること

9.1.2.1 それらの障害の影響（損害規模及び回復期間の両面から）を判断するために、リスクアセスメントを行うこと

9.1.2.2 これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること

9.1.3 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること

9.1.3.1 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること

9.1.4 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること

9.1.4.1 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること

9.1.4.2 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施すること

9.1.4.3 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること

9.1.4.4 事業継続計画の作成過程では、合意された手順及び過程を文書化すること

9.1.4.5 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと

9.1.4.6 事業継続計画の作成過程では、計画の試験及び更新を行うこと

9.1.4.7 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと

9.1.4.8 これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること

9.1.5 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、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること

9.1.5.1 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること

9.1.5.2 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正すること

9.1.5.3 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること

9.1.5.4 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること

9.1.5.5 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと

9.1.5.6 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること

9.1.5.7 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること

9.1.5.8 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること

9.1.5.9 事業継続計画作成の枠組みでは、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保するために計画される認識及び教育活動について考慮すること

9.1.5.10 事業継続計画作成の枠組みでは、個人の責任について考慮すること

9.1.5.11 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するの

に誰が責任をもつかを記述すること

9.1.5.12 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること

9.1.5.13 事業継続計画作成の枠組みでは、各計画には特定の責任者がいること

9.1.5.14 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること

9.1.5.15 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること

9.1.6 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること

9.1.6.1 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること

9.1.6.2 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと

9.1.6.3 計画の個々の構成要素を、頻繁に試験すること

9.1.6.4 計画が実際に役立つことを保証するために、様々な手法を使用すること

9.1.6.5 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）

9.1.6.6 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）

9.1.6.7 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）

9.1.6.8 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施する）

9.1.6.9 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）

9.1.6.10 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験する）

9.1.6.11 いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること

9.1.7 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること

9.1.7.1 事業継続上の問題を適切に対処する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の中に含めること

9.1.7.2 各事業継続計画の定期的見直しに対する責任を割り当てること

9.1.7.3 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること

9.1.7.4 この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること

10 適合性

10.1 法的要求事項への適合

目的：刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため

10.1.1 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること

10.1.1.1 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策､及び個々の責任も同様に明確に定め、文書化すること

10.1.2 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は、法的制限事項に適合するように、適切な手続を実行すること

10.1.2.1 ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること

10.1.2.2 ソフトウェア製品の取得手続に関する標準類を発行すること

10.1.2.3 ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること

10.1.2.4 適切な財産登録簿を維持管理すること

10.1.2.5 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること

10.1.2.6 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること

10.1.2.7 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を確認すること

10.1.2.8 適切な使用許諾条件を維持管理するための個別方針を定めること

10.1.2.9 ソフトウェアの処分又は他人への譲渡についての個別方針を定めること

10.1.2.10 適切な監査ツールを用いるここと

10.1.2.11 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使用条件に従うこと

10.1.3 組織の重要な記録は、消失、破壊及び改ざんから保護されること

10.1.3.1 組織の重要な記録は、消失、破壊及び改ざんから保護されること

10.1.3.2 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について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、光学媒体）の詳細も定めておくこと

10.1.3.3 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること

10.1.3.4 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、

必要なときに、認可されている者が使用できるようにすること
10.1.3.5 記録の保管に用いられる媒体が劣化する可能性を考慮すること
10.1.3.6 保管及び取扱いの手順は、製造業者の推奨に従って実行すること
10.1.3.7 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、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）を確保する手順を含めること
10.1.3.8 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること
10.1.3.9 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にすること
10.1.3.10 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること
10.1.3.11 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行すること
10.1.3.12 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること
10.1.3.13 主要な情報の出典一覧を維持管理すること
10.1.3.14 重要な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行すること

10.1.4 関連する法令に従って個人情報を保護するために、管理策を用いること
10.1.4.1 データ保護の担当役員を任命すること
10.1.4.2 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当役員に報告することは、データ所有者の責任であること
10.1.4.3 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任であること

10.1.5 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いること
10.1.5.1 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること
10.1.5.2 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること
10.1.5.3 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること
10.1.5.4 すべての利用者は、その許可されたアクセスの正確な範囲を認識していること
10.1.5.5 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること

10.1.5.6 ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表示すること

10.1.5.7 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること

10.1.6 暗号による管理策の規制においては、国の法律への適合を確実なものにするために、 法的な助言を求めること

10.1.6.1 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること

10.1.7 人又は組織に対する措置を支援するには、十分な証拠をもつこと

10.1.7.1 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること

10.1.7.2 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとること

10.1.7.3 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること

10.1.7.4 コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっておくこと

10.1.7.5 コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること

10.1.7.6 コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること

10.1.7.7 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得ること

10.2 セキュリティ基本方針及び技術適合のレビュー

目的：組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため

10.2.1 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること

10.2.1.1 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること

10.2.1.2 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること

10.2.2 情報システムは、セキュリティ実行標準と適合していることを定期的に検

査すること

10.2.2.1 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行うこと

10.2.2.2 技術適合の検査では、専門家の技術援助を得ること

10.2.2.3 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されること

10.2.2.4 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること

10.2.2.5 いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施されること

10.3 システム監査の考慮事項

目的：システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため

10.3.1 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意されること

10.3.1.1 監査要求事項は、担当経営陣の同意を得ること

10.3.1.2 検査の範囲は、合意され、管理されること

10.3.1.3 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定すること

10.3.1.4 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること

10.3.1.5 複製ファイルは、監査が完了した時点で消去すること

10.3.1.6 検査を実施するための情報資源は、明確に識別され、利用可能であること

10.3.1.7 特別又は追加処理の要求事項は、識別され、合意されること

10.3.1.8 すべてのアクセスは、照合用の証跡を残すために、監視され、記録されること

10.3.1.9 すべての手順、要求事項及び責任について、文書化すること

10.3.2 システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること

10.3.2.1 システム監査ツールは、開発及び運用システムから分離しておくこと

10.3.2.2 システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
1.1	情報セキュリティ基本方針	情報セキュリティのための経営陣の指針及び支持を規定するため	1) 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること	1) 基本方針文書には、経営陣の責任を明記すること	3.1.1
				2) 基本方針文書には、情報セキュリティの管理に対する組織の取組み方法を明示すること	3.1.1
				3) 基本方針文書には、情報セキュリティの定義を含めること	3.1.1
				4) 基本方針文書には、その目的を含めること	3.1.1
				5) 基本方針文書には、適用範囲を含めること	3.1.1
				6) 基本方針文書には、情報共有を可能にするための機構としてのセキュリティの重要性を含めること	3.1.1
				7) 基本方針文書には、情報セキュリティの目標を支持する経営陣の意向声明書を含めること	3.1.1
				8) 基本方針文書には、原則を支持する経営陣の意向声明書を含めること	3.1.1
				9) 基本方針文書には、法律上及び契約上の要求事項への適合を含めること	3.1.1
				10) 基本方針文書には、セキュリティ教育の要求事項を含めること	3.1.1
				11) 基本方針文書には、ウイルス及び他の悪意のあるソフトウェアの予防及び検出を含めること	3.1.1
				12) 基本方針文書には、事業継続管理を含めること	3.1.1
				13) 基本方針文書には、セキュリティ基本方針違反に対する措置を含めること	3.1.1
				14) 基本方針文書には、セキュリティの事件・事故を報告することを含めること	3.1.1
				15) 基本方針文書には、情報セキュリティマネジメントの一般的責任の定義を含めること	3.1.1
				16) 基本方針文書には、特定責任の定義を含めること	3.1.1
				17) 基本方針文書には、基本方針を支持する文書（例えば、特定の情報システムについてのより詳細なセキュリティ個別方針及び手順又は利用者が従うことが望ましいセキュリティ規則）の参照情報を含めること	3.1.1
				18) 基本方針文書には、この基本方針が、想定した読者にとって、適切で、利用可能で、かつ理解し易い形で、組織全体にわたって利用者に知らせること	3.1.1
			2) 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること	1) 見直し手続によって、当初のリスクアセスメントの基礎事項に影響を及ぼす変化（例えば、重大なセキュリティの事件・事故、新しいぜい（脆）弱性、又は組織基盤若しくは技術基盤の変化）に対応して確実に見直しを実施すること	3.1.2
				2) 記録されたセキュリティの事件・事故の性質、回数及び影響によって示される、基本方針の有効性について、日程を定め、定期的に見直しを実施すること	3.1.2
				3) 事業効率における管理策の費用及び影響について、日程を定め、定期的に見直しを実施すること	3.1.2
				4) 技術変更による効果について、日程を定め、定期的に見直しを実施すること	3.1.2
2.1	情報セキュリティ基盤	組織内の情報セキュリティを管理するため	1) 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経営者による目に見える形での支持を確実にするために、運営委員会を設置すること	（なし）	4.1.1
			2) 運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること	1) 運営委員会は、適切な責任及び資源配分によって、組織内におけるセキュリティを促進すること	4.1.1
				2) 運営委員会は、情報セキュリティ基本方針並びに全体的な責任の見直し及び承認をすること	4.1.1
				3) 運営委員会は、情報資産が重大な脅威にさらされていることを示す変化を監視すること	4.1.1
				4) 運営委員会は、情報セキュリティの事件・事故の見直し及び監視をすること	4.1.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				5) 運営委員会は、情報セキュリティを強化するための主要な発議の承認をすること	4.1.1
				6) 運営委員会は、一人の管理者が、すべてのセキュリティ関連活動に責任をもつこと	4.1.1
			3) 大きな組織では、情報セキュリティの管理策の実施を調整するために、組織の関連部門からの管理者の代表を集めた委員会を設置すること	1) 管理者の代表を集めた委員会では、組織全体の情報セキュリティのそれぞれの役割及び責任への同意を得ること	4.1.2
				2) 管理者の代表を集めた委員会では、情報セキュリティのための個別の方法及び手順（例えば、リスクアセスメント、セキュリティの分類体系）への同意を得ること	4.1.2
				3) 管理者の代表を集めた委員会では、組織全体の情報セキュリティの発議（例えば、セキュリティの意識向上プログラム）への同意及び支持を得ること	4.1.2
				4) 管理者の代表を集めた委員会では、セキュリティを、情報化計画の作成過程の一部にすることを確実にすること	4.1.2
				5) 管理者の代表を集めた委員会では、新しいシステム又は新しいサービスのためのそれぞれの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の調整をすること	4.1.2
				6) 管理者の代表を集めた委員会では、情報セキュリティの事件・事故の見直しをすること	4.1.2
				7) 管理者の代表を集めた委員会では、組織全体への情報セキュリティに対する目に見える形での業務上の支援の促進をすること	4.1.2
			4) 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手続きの実施に対する責任を、明確に定めること	1) 情報セキュリティ基本方針には、組織内のセキュリティの役割及び責任の割当てに関する全般的な手引を規定すること	4.1.3
				2) 情報セキュリティ基本方針に、個別のサイト、システム又はサービスに関するより詳細な手引を追加すること	4.1.3
				3) 個々の物理的資産及び情報資産に限定した責任、並びに事業継続計画のようなセキュリティ手順を、明確に定義すること	4.1.3
				4) 一人の情報セキュリティ管理者を任命すること	4.1.3
				5) 情報資産の責任者は、その資産のセキュリティに対して最終的な責任をもつこと	4.1.3
				6) 情報資産の責任者は、委任された責任が正しく果たされたかを判断できること	4.1.3
				7) 各管理者が責任を負う範囲は明確に規定すること	4.1.3
				8) 個々のシステムに関連したいろいろな資産及びセキュリティ手順は、識別され、及び明確に定義されること	4.1.3
				9) 各資産又はセキュリティ手順に対する管理者の責任は、協議の下で決め、その責任の詳細は、文書化されること	4.1.3
				10) 承認の権限の範囲は、明確に定義され、文書化されること	4.1.3
			5) 新しい情報処理設備に対する経営陣による認可手続を確立すること	1) 新しい設備は、そ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を得ること	4.1.4
				2) 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からも承認を得ること	4.1.4
				3) ハードウェア及びソフトウェアは、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こと	4.1.4
				4) 個人が所有する情報処理設備を業務情報の処理に用いる場合、その使用及びそれに伴って必要となる管理策は、認可を得ること	4.1.4
				5) 職場での個人用情報処理設備の使用は、評価を受け、認可を得ること	4.1.4

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			6) 専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること	1) 専門家によるセキュリティの助言は、経験を積んだ社内の情報セキュリティ助言者が行うこと	4.1.5
				2) 専門家を雇わないならば、特定の個人を指名して、社内の知識及び経験を一貫性を保つように調整させ、セキュリティの方針決定を支援させること	4.1.5
				3) このような任に当たる者は、自分自身の経験を超えた専門的な助言を与えるためには、適切な社外の助言者との接触をもつこと	4.1.5
				4) 情報セキュリティ助言者又は同等の担当者は、自らの経験又は外部の助言を用いて、情報セキュリティのあらゆる面について助言を与えることを業務とすること	4.1.5
				5) 助言者は、組織内のあらゆる経営陣と直接接触できること	4.1.5
				6) 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに速やかに相談を受け付けること	4.1.5
				7) 情報セキュリティ助言者又は同等の担当者は、セキュリティの事件・事故又は違反の疑いがあるときに専門家の指導に関する情報又は調査手段を提供すること	4.1.5
			7) 行政機関、規制機関、情報サービス提供者及び通信事業者との適切な関係を維持すること	1) セキュリティのグループ及び業界の委員会の一員となることも考慮すること	4.1.6
				2) 組織の機密情報が認可されていない人々に絶対に渡らないように、セキュリティ情報の交換を制限すること	4.1.6
			8) 情報セキュリティ基本方針の実施を、他者が見直すこと	1) 情報セキュリティ基本方針文書には、情報セキュリティの基本方針及び責任を記述すること	4.1.7
2.2	第三者によるアクセスのセキュリティ	第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため	1) 組織の情報処理施設への第三者のアクセスに関連づけてリスクを評価し、適切な管理策を実施すること	1) 物理的アクセス、例えば、事務所、コンピュータ室及びファイルキャビネットへのアクセスを考慮すること	4.2.1.1
				2) 論理的アクセス、例えば、組織のデータベース、情報システムへのアクセスを考慮すること	4.2.1.1
				3) 第三者に接続する業務上の必要がある場合には、その管理策の要求事項を明らかにするために、リスクアセスメントを実施すること	4.2.1.2
				4) リスクアセスメントにおいては、要求されるアクセスの種類、情報の価値、第三者が採用する管理策、及び組織の情報のセキュリティに対するこのアクセスの影響を考慮すること	4.2.1.2
				5) 第三者アクセスにかかわるすべてのセキュリティ要求事項又は内部管理策は、第三者との契約書に反映させること	4.2.1.3
				6) 情報及び情報処理施設への第三者によるアクセスは、適切な管理策を実施すること	4.2.1.3
				7) 第三者によるアクセスは、接続又はアクセスについての条件を明示した契約書を締結するまで、開始させないこと	4.2.1.3
			2) 組織の情報処理施設への第三者アクセスにかかわる取決めは、正式な契約に基づくこと	1) 第三者アクセスに関する契約には、組織のセキュリティ基本方針及び標準類に適合することを確実にするために、すべてのセキュリティ要求事項を含めるか又は引用すること	4.2.2
				2) 第三者アクセスに関する契約書は、組織と第三者との間に誤解が全くないことを確実にするものであること	4.2.2
				3) 組織は、その供給業者の損失補償について納得していること	4.2.2
				4) 契約書には、情報セキュリティに関する一般方針を含めることを考慮すること	4.2.2
				5) 契約書には、情報及びソフトウェアを含む、組織の資産を保護する手順を含む資産保護を含めることを考慮すること	4.2.2
				6) 契約書には、資産が危険にさらされているか、例えば、データの喪失又は変更が生じているかどうかを判定するための手順を含めることを考慮すること	4.2.2

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				7) 契約書には、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を確実に返還又は破棄するための管理策を含めることを考慮すること	4.2.2
				8) 契約書には、完全性及び可用性を含めることを考慮すること	4.2.2
				9) 契約書には、情報の複製及び開示の制限を含めることを考慮すること	4.2.2
				10) 契約書には、利用できる各サービスの記述を含めることを考慮すること	4.2.2
				11) 契約書には、サービスの目標となるレベル及びサービスの受け入れられないレベルを含めることを考慮すること	4.2.2
				12) 契約書には、必要ならば、要員の異動に関する規定を含めることを考慮すること	4.2.2
				13) 契約書には、契約当事者それぞれの義務を含めることを考慮すること	4.2.2
				14) 契約書には、法律関連事項を含めることを考慮すること（例えば、データ保護に関連して制定された法律における責任。特に、契約が他国の組織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する）	4.2.2
				15) 契約書には、知的所有権（IPR）及び著作権の取扱い、並びに共同作業に伴う保護の条項を含めることを考慮すること	4.2.2
				16) 契約書には、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及びパスワード）の管理及び使用含むアクセス制御の合意事項を含めることを考慮すること	4.2.2
				17) 契約書には、利用者によるアクセス及び利用者特権の認可手続を含むアクセス制御の合意事項を含めることを考慮すること	4.2.2
				18) 契約書には、利用可能サービスを認可されている個人、並びにその利用者が持っている権限及び特権の内容の一覧表を維持管理するための要求事項を含むアクセス制御の合意事項を含めることを考慮すること	4.2.2
				19) 契約書には、検証可能な性能基準、それらの監視及び報告の定義を含めることを考慮すること	4.2.2
				20) 利用者の活動を監視し、無効にする権利を含めることを考慮すること	4.2.2
				21) 契約上の責任を監査する権利又はそのような監査を第三者に実施させる権利を含めることを考慮すること	4.2.2
				22) 契約書には、問題解決のための段階的処理手順の確立を含めることを考慮すること	4.2.2
				23) 契約書には、障害対策の取決めを含めることを考慮すること	4.2.2
				24) 契約書には、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ことを考慮すること	4.2.2
				25) 契約書には、明確な報告の構成及び合意された報告の形式を含めることを考慮すること	4.2.2
				26) 契約書には、変更管理の明確な、設定された手続を含めることを考慮すること	4.2.2
				27) 契約書には、要求される物理的保護の管理策、及びそれらの管理策の実施を確実にするための仕組みを含めることを考慮すること	4.2.2
				28) 契約書には、利用者及び管理者に対する、方法、手順及びセキュリティについての訓練を含めることを考慮すること	4.2.2
				29) 契約書には、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を含めることを考慮すること	4.2.2
				30) 契約書には、セキュリティ事件・事故及びセキュリティ違反についての報告、通知及び調査に関する取決めを含めることを考慮すること	4.2.2
				31) 契約書には、第三者と下請け業者とのかかわりを含めることを考慮すること	4.2.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
2.3	外部委託	情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため	1) 情報システム、ネットワーク及び/又はデスクトップ環境についての、マネジメント及び統制の全部又は一部を外部委託する組織のセキュリティ要求事項は、当事者間で合意される契約書に記述されること	1) 外部委託契約書には、法的な要求事項（例えば、データ保護に関連して制定された法律）をどのように満たすかを取り扱うこと	4.3.1
				2) 外部委託契約書には、請負業者を含め、外部委託にかかわるすべての当事者がそれぞれのセキュリティの責任についての認識を確実にするためにどのような取決めが適切であるかを取り扱うこと	4.3.1
				3) 外部委託契約書には、組織の事業資産の完全性及び機密性をどのように維持し、それを検証するかを取り扱うこと	4.3.1
				4) 外部委託契約書には慎重な取扱いを要する組織の業務情報への認可された利用者によるアクセスを制約及び制限するために、どのような物理的及び論理的管理策を用いるかを取り扱うこと	4.3.1
				5) 外部委託契約書には災害の際に、サービスの可用性をどのように維持するかを取り扱うこと	4.3.1
				6) 外部委託契約書には外部委託した装置については、どのようなレベルの物理的セキュリティを施すかを取り扱うこと	4.3.1
				7) 外部委託契約書には監査する権利を取り扱うこと	4.3.1
				8) 2.2.2)に列挙した事項も、この契約の一部として考慮すること	4.3.1
				9) 契約では、両当事者間の合意によるセキュリティマネジメント計画において、追加されたセキュリティ要求事項及び手順を認めること	4.3.1
3.1	資産に対する責任	組織の資産の適切な保護を維持するため	1) 情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持すること	1) 組織は、その資産並びにそれらの相対価値及び重要度を明確に把握できるようにすること	5.1.1
				2) 情報システムそれぞれに関連づけて重要な資産について目録を作成すること	5.1.1
				3) 各資産を、その現在の所在とともに、明確に識別すること	5.1.1
				4) 各資産を、その現在の所在とともに、セキュリティの分類について合意すること	5.1.1
				5) 各資産を、その現在の所在とともに、文書化すること	5.1.1
				6) 各資産を、その現在の所在とともに、その管理責任及びセキュリティの分類について合意すること	5.1.1
3.2	情報の分類	情報資産の適切なレベルでの保護を確実にするため	1) 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響（例えば、情報への認可されていないアクセス又は情報の損傷）を考慮に入れておくこと	1) 情報及び重要なデータを取り扱うシステムからの出力は、それが組織に対してもつ価値及び取扱い慎重度によってラベル付けすること	5.2.1
				2) 過度の分類によって無駄な出費を生じないようにすること	5.2.1
				3) 分類の指針には、前もって決められた個別方針に従って変わることもある、という事実を予期し考慮しておくこと	5.2.1
				4) 分類区分の数及びそれらの区分を用いる効用を考慮すること	5.2.1
				5) 他の組織からの文書に付いている分類ラベルは、同じか又は類似した名称のラベルでも、定義が異なることがあるので、その解釈には注意すること	5.2.1
				6) 情報（例えば、文書、データ記録、データファイル又はディスケット）の分類を定める責任、及びその分類を定期的に見直す責任は、その情報の作成者又は指定された管理者にあること	5.2.1
			2) 組織が採用した分類体系に従って情報のラベル付け及び取扱いをするための、一連の手順を定めること	1) 各分類について、複製に適用する取扱い手順を定めること	5.2.2
				2) 各分類について、保存に適用する取扱い手順を定めること	5.2.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				3) 各分類について、郵便による伝達に適用する取扱い手順を定めること	5.2.2
				4) 各分類について、ファクシミリによる伝達に適用する取扱い手順を定めること	5.2.2
				5) 各分類について、電子メールによる伝達に適用する取扱い手順を定めること	5.2.2
				6) 各分類について、移動電話による伝達に適用する取扱い手順を定めること	5.2.2
				7) 各分類について、音声メールによる伝達に適用する取扱い手順を定めること	5.2.2
				8) 各分類について、留守番電話による伝達に適用する取扱い手順を定めること	5.2.2
				9) 各分類について、言葉による伝達に適用する取扱い手順を定めること	5.2.2
				10) 各分類について、破棄に適用する取扱い手順を定めること	5.2.2
				11) 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）付けること	5.2.2
				12) ラベル付けは、分類の指針に定める規則に従った分類を反映すること	5.2.2
4.1	職務定義及び雇用におけるセキュリティ	人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため	1) セキュリティの役割及び責任は、組織の情報セキュリティ基本方針で定められたとおりに、職務定義書のなかに文書化すること	1) セキュリティの役割及び責任を文書化したものには、セキュリティ基本方針を実行又は維持するための一般的な責任のすべてを含めること	6.1.1
				2) セキュリティの役割及び責任を文書化したものには、特定の資産を保護するための具体的な責任を含めること	6.1.1
				3) セキュリティの役割及び責任を文書化したものには、特定のセキュリティの手続を含めること	6.1.1
				4) セキュリティの役割及び責任を文書化したものには、特定のセキュリティ活動を進めるための具体的な責任を含めること	6.1.1
			2) 常勤職員を採用するときは、提出された応募資料の内容を検査すること	1) かなりの権限をもつ地位に就く職員については、この調査を定期的に繰り返すこと	6.1.2
				2) 経営者は新入職員及び経験の浅い職員に取扱いに慎重を要するシステムにアクセスすることを認めたときは、それらに対する管理監督についての評価を行うこと	6.1.2
				3) すべての職員の仕事は、上級の職員による定期的見直し及び承認手順のもとに置くこと	6.1.2
				4) 職員の個人的事情がその仕事に影響を及ぼす可能性を、管理者は認識していること	6.1.2
				5) 不正行為、盗難、誤り又はその他のセキュリティにかかわる問題は、当該裁判管轄で施行されている適切な法令に従って取り扱うこと	6.1.2
				6) 常勤職員を採用するときは、提出された応募資料の内容を検査すること	6.1.2
				7) 応募資料の検査において、提出された人物推薦状は役にたつかを考慮すること	6.1.2
				8) 応募資料の検査において、履歴書の検査をすること	6.1.2
				9) 応募資料の検査において、提示された学術上及び職業上の資格の確認をすること	6.1.2
				10) 応募資料の検査において、公的証明書（パスポート又は同種の文書）の検査をすること	6.1.2
				11) 組織は、その者に対して信用調査を行うこと	6.1.2
				12) 請負業者及び臨時職員に対しても同様の審査手続を実施すること	6.1.2
				13) 派遣会社が従う必要のある、その審査の責任及び通知の手順を、派遣会社との契約に明記すること	6.1.2
			3) 従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること	1) 既存の契約（機密保持条項を含むもの）の効力が及ばない臨時職員及び外部利用者に対しては、情報処理設備へのアクセスを認める前に、機密保持契約書への署名を要求すること	6.1.3

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				2) 機密保持契約は、雇用条件又は請負契約に変更がある場合、特に従業員がその組織を離れることになるとき又は請負契約が終了するときには、見直しを行うこと	6.1.3
			4) 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること	1) 適切ならば、これらの責任を、雇用終了後の定められた期間継続すること	6.1.4
				2) 従業員がセキュリティ要求事項を無視した場合に採る措置についても雇用条件に含めること	6.1.4
				3) 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を明確にすること	6.1.4
				4) 著作権法又はデータ保護に関連して制定された法律といったものに基づく、従業員の責任及び権利を雇用条件に含めること	6.1.4
				5) 雇用条件には、雇用者側データについての重要度の分類及びその管理に対しての義務を含めること	6.1.4
				6) 雇用条件には、通常の勤務場所及び勤務時間からは外れた状況においても、これらの責任が適用されることの記述があること	6.1.4
4.2	利用者の訓練	情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティ基本方針を維持していくことを確実にするため	1) 組織の基本方針及び手順について、組織のすべての従業員及び関係するならば外部利用者を適切に教育し、並びに定期的に更新教育を行うこと	1) 教育には、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施する、情報処理設備の正しい使用方法（例えば、ログオン手順、ソフトウェアパッケージパッケージソフトウェアの使用方法）に関する訓練を含むこと	6.2.1
4.3	セキュリティ事件・事故及び誤動作への対処	セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため	1) セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること	1) 事件・事故の正式な報告手順を、事件・事故への対処手順とともに確立すること	6.3.1
				2) 事件・事故の正式な報告を受けたならば直ちに取るべき措置に着手できるようにすること	6.3.1
				3) すべての従業員及び請負業者に、セキュリティ事件・事故の報告手順を認識させておくこと	6.3.1
				4) すべての従業員及び請負業者に、セキュリティ事件・事故をできるだけ速やかに報告するよう要求すること	6.3.1
				5) 適切なフィードバックの手続を構築していること	6.3.1
			2) 情報サービスの利用者に対して、システム若しくはサービスのセキュリティの弱点、又はそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること	1) 利用者は、全ての従業員及び請負業者に、事件・事故の発生を知った場合又はその疑いを持った場合は、できるだけ速やかに、自分の管理者又はサービス提供者に対し直接報告すること	6.3.2
				2) 利用者には、弱点ではないかと疑われる事柄の証明を、いかなる場合でも自ら試みるべきでないと知らせておくこと	6.3.2
			3) ソフトウェア誤動作を報告する手順を確立すること	1) ソフトウェア誤動作を報告する手順の確立において、問題の兆候及び画面に現れるメッセージへの注意を考慮すること	6.3.3
				2) ソフトウェア誤動作を報告する手順の確立において、コンピュータの隔離を考慮すること	6.3.3
				3) ソフトウェア誤動作を報告する手順の確立において、コンピュータの使用停止を考慮すること	6.3.3
				4) ソフトウェア誤動作を報告する手順の確立において、適切な関係先に対する警報を考慮すること	6.3.3
				5) ソフトウェア誤動作を報告する手順の確立において、装置の検査の前に組織のすべてのネットワークを切断することを考慮すること	6.3.3
				6) ソフトウェア誤動作を報告する手順の確立において、ディスケットを別のコンピュータに移さないことを考慮すること	6.3.3

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				7) ソフトウェア誤動作を報告する手順の確立において、情報セキュリティ管理者への速やかな報告を考慮すること	6.3.3
				8) 利用者は、疑いのあるソフトウェアの除去を認可なしに試みないこと	6.3.3
				9) 回復処置は、適切に訓練されること	6.3.3
				10) 回復処置は、経験を積んだ職員が実施すること	6.3.3
			4) 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みを備えていること	1) 事件・事故及び誤動作の種類、規模並びに費用の定量化及び監視を可能とする仕組みから得られる情報を、事件・事故の再発若しくは影響の大きい事件・事故又は誤動作を識別するために用いること	6.3.4
			5) 組織のセキュリティ基本方針及び手順に違反した従業員に対する、正式な懲戒手続を備えていること	1) 違反した従業員に対する、正式な懲戒手続は、重大な又は度重なるセキュリティ違反を犯した疑いのある従業員に対して、正しく、かつ、公平な取扱いを確実にするものであること	6.3.5
5.1	セキュリティが保たれた領域	業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため	1) 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること	1) セキュリティ境界を明確に定義すること	7.1.1
				2) 情報処理設備を収容した建物又は敷地の境界は、物理的に頑丈であること	7.1.1
				3) 敷地の外周壁を堅固な構造物とすること、及びすべての外部扉を認可されていないアクセスから開閉制御の仕組み（かんぬき、警報装置、錠など）で適切に保護すること	7.1.1
				4) 敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること	7.1.1
				5) 敷地及び建物へのアクセスは、認可された職員だけに制限すること	7.1.1
				6) 物理的な壁は、床から天井にわたる構造で設けること	7.1.1
				7) セキュリティ境界上にあるすべての防火扉は、警報装置付き及び密閉式であること	7.1.1
			2) 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セキュリティの保たれた領域を保護すること	1) セキュリティが保たれた領域への訪問者を監視すること	7.1.2
				2) セキュリティが保たれた領域への訪問者に立ち入り許可を求めさせること	7.1.2
				3) セキュリティが保たれた領域への入退の日付・時間を記録すること	7.1.2
				4) セキュリティが保たれた領域への訪問者には、認可された特定の目的に限ってのアクセスを認めること	7.1.2
				5) セキュリティが保たれた領域への訪問者その領域のセキュリティ要求事項及び非常時の手順を説明した文書を渡すこと	7.1.2
				6) 取扱いに慎重を要する情報及び情報処理設備へのアクセスを管理すること	7.1.2
				7) 取扱いに慎重を要する情報及び情報処理設備へのアクセスは認可された者だけに制限すること	7.1.2
				8) アクセスをすべて認可して、暗証番号付きの磁気カードといった認証管理策を用いること	7.1.2
				9) すべてのアクセスの監査証跡は、安全に保管しておくこと	7.1.2
				10) すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること	7.1.2
				11) 付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること	7.1.2
				12) セキュリティが保たれた領域へのアクセス権は、定期的に見直し及び更新すること	7.1.2
			3) セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること	1) 関連する健康及び安全に関する規制並びに標準類も考慮に入れること	7.1.3

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				2) 隣接場所から及んでくるセキュリティ上のいかなる脅威についても考慮すること	7.1.3
				3) 主要な設備は、一般の人のアクセスが避けられる場所に設置すること	7.1.3
				4) 建物は目立たせず、その用途を示す表示は最小限とすること	7.1.3
				5) 情報処理作業の存在を示すものは建物の内外を問わず一切表示しないこと	7.1.3
				6) 複写機、ファクシミリといった支援機能及び装置は、セキュリティの保たれた領域内の適切な場所に設置すること	7.1.3
				7) 要員が不在のときは扉及び窓に施錠すること	7.1.3
				8) 一階の窓については、外部に対する防御を考慮すること	7.1.3
				9) すべての外部扉及びアクセス可能な窓には、適切な侵入者の検知システムを設置すること	7.1.3
				10) 侵入者の検知システムは、専門の標準類に従って取り付けられること	7.1.3
				11) 侵入者の検知システムは、定期的に点検すること	7.1.3
				12) 無人の領域には常に警報装置を稼働させること	7.1.3
				13) コンピュータ室又は通信室といった他の領域においても、警報装置を設置すること	7.1.3
				14) 組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと	7.1.3
				15) 取扱いに慎重を要する情報処理設備の所在を掲げた職員録及び社内電話帳は、一般の人に容易に見られないようにすること	7.1.3
				16) 危険物又は可燃物は、セキュリティが保たれた領域から十分に離れた場所に、安全に保管すること	7.1.3
				17) セキュリティが保たれた領域には、事務用品などを、必要もないのに大量に保管しないこと	7.1.3
				18) 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと	7.1.3
			4) セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策及び指針を追加すること	1) セキュリティが保たれた領域の存在又はそこでの作業は、その必要がある要員だけが知っていること	7.1.4
				2) セキュリティが保たれた領域において監視もなく作業することは、避けること	7.1.4
				3) セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと	7.1.4
				4) セキュリティが保たれた領域を無人にするときは、定期的に検査すること	7.1.4
				5) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること	7.1.4
				6) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは認可のもとにおくこと	7.1.4
				7) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは監視下におくこと	7.1.4
				8) あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、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こと	7.1.4
				9) 認可なしの、写真機、ビデオカメラ、録音機、又はその他の記録装置の使用は、許さないこと	7.1.4

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
			5) 品物を受け渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること	1) 品物を受け渡しする場所についてのセキュリティ要求事項は、リスクアセスメントに基づいて決定すること	7.1.5
				2) 建物の外から一時保管場所へのアクセスは、本人の確認及び認可を受けた要員に限定すること	7.1.5
				3) 一時保管場所については、建物内の他の場所にアクセスすることなく受渡しの要員が荷おろしできるように、設計を行うこと	7.1.5
				4) 一時保管場所の内部扉を開いているときは、外部扉を締めること	7.1.5
				5) 一時保管場所から使用場所に搬入品を移送する前に、危険の可能性がないかどうか、その品物を検査すること	7.1.5
				6) 敷地内に搬入するときには、搬入品の登録を行うこと	7.1.5
5.2	装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること	1) 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること	7.2.1
				2) 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること	7.2.1
				3) 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること	7.2.1
				4) 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること	7.2.1
				5) 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること	7.2.1
				6) 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること	7.2.1
				7) 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること	7.2.1
			2) 装置は、停電、その他の電源異常から保護すること	1) 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること	7.2.2
				2) 電源の多重化をすること	7.2.2
				3) 無停電電源装置（UPS）を設置すること	7.2.2
				4) 非常用発電機の設置をすること	7.2.2
				5) 障害対策計画では、UPSが故障した場合に取るべき措置についても計画しておくこと	7.2.2
				6) UPSは、容量が十分であることを定期的に確認すること	7.2.2
				7) UPSは、製造者の推奨に従って点検すること	7.2.2
				8) 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること	7.2.2
				9) 発電機を使用する場合、製造者の推奨に従って定期的に点検すること	7.2.2
				10) 発電機を長時間運転できるように、燃料の十分な供給を確保すること	7.2.2
				11) 電源の緊急スイッチは、機械室の非常口近くに設置すること	7.2.2
				12) 主電源の停電時用として非常用照明を備えること	7.2.2
				13) 落雷防護はすべての建物に備えること	7.2.2
				14) すべての外部通信回線に落雷防護フィルタを付けること	7.2.2
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること	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、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと	7.2.3
				2) ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること	7.2.3
				3) 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こと	7.2.3

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				4) 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること	7.2.3
				5) 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること	7.2.3
				6) 取扱いに慎重を要するシステム又は重要なシステムに対しては、代替経路又は伝送媒体を使用すること	7.2.3
				7) 取扱に慎重を要するシステム又は重要なシステムに対しては、光ファイバケーブルを使用すること	7.2.3
				8) 認可されていない装置がケーブルに取り付けられているかどうかについての調査すること	7.2.3
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること	1) 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること	7.2.4
				2) 認可された保守担当者だけが装置の修理及び手入れを実施すること	7.2.4
				3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4
				4) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること	7.2.4
				5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4
				6) 保険約款によって定められたすべての要求事項に従うこと	7.2.4
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること	1) 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること	7.2.5
				2) 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと	7.2.5
				3) ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること	7.2.5
				4) 装置の保護に関しては、製造者の指示に常に従うこと	7.2.5
				5) 在宅作業についての管理策は、リスクアセスメントによって決定すること	7.2.5
				6) 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること	7.2.5
				7) 事業所外の装置を保護するために、十分な保険が付保されていること	7.2.5
				8) セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること	7.2.5
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	1) 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること	7.2.6
				2) 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が、消去又は上書きされているか確認すること	7.2.6
5.3	その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、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の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること	1) クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること	7.3.1
				2) クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること	7.3.1
				3) 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管すること	7.3.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				4) 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと	7.3.1
				5) パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと	7.3.1
				6) パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1
				7) 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること	7.3.1
				8) 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと	7.3.1
				9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできないこと	1) 持出し時及び返却時に記録を残すこと	7.3.2
				2) 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること	7.3.2
				3) 現場検査があることを各人が認識していること	7.3.2
6.1	運用手順及び責任	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	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと	1) 操作手順は、正式な文書として取り扱うこと	8.1.1
				2) 操作手順が変更の場合は管理者によって認可されること	8.1.1
				3) 操作手順には、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こと	8.1.1
				4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1
				5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1
				6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1
				7) 操作手順には、特別な出力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こと	8.1.1
				8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1
				9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1
			2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること	8.1.2
				2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2
				3) プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること	8.1.2
				4) 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合すること	8.1.2
				5) 重要な変更を識別及び記録すること	8.1.2
				6) 重要な変更の潜在的な影響の評価をすること	8.1.2
				7) 変更の申出を正式に承認する手順を確立すること	8.1.2
				8) 変更の詳細の、全関係者への通知をすること	8.1.2
				9) うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立すること	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3
				2) サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること	8.1.3
				3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3
				4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3
				5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を含めること	8.1.3
				6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3
				7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3
				8) 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること	8.1.3
				9) 通常の障害対策計画手順には、監督機関に対する措置の報告を含めること	8.1.3
				10) 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3
				11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での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収集し、安全に保管すること	8.1.3
				12) ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3
				13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理されること	8.1.3
				14) 事件・事故管理手順では、身分が明らかで、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、許すことを考慮すること	8.1.3
				15) 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること	8.1.3
				16) 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3
				17) 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること	8.1.3
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮すること	1) 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること	8.1.4
				2) セキュリティ監査は、独立性を維持すること	8.1.4
				3) どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること	8.1.4
				4) ある作業を始めることと、その作業を認可することとを分離すること	8.1.4
				5) 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること	8.1.4
				6) 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること	8.1.4

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			5) 開発施設、試験施設及び運用施設を分離するため、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、文書化すること	1) 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること	8.1.5
				2) 同様な分離は、開発と試験との機能間でも実行すること	8.1.5
				3) 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持すること	8.1.5
				4) 開発施設、試験施設及び運用施設を分離すること	8.1.5
				5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5
				6) 開発作業と試験作業とは、可能な限り分離すること	8.1.5
				7) コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと	8.1.5
				8) 運用システム及び試験システムに対しては、異なるログオン手順を用いること	8.1.5
				9) 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること	8.1.5
				10) メニューには、適切な識別メッセージを表示すること	8.1.5
				11) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得すること	8.1.5
				12) 管理用パスワードは、使用後には変更されることを確実にすること	8.1.5
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること	8.1.6
				2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6
				3) 外部委託による施設管理においては、事業継続計画との関連性を考慮すること	8.1.6
				4) 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮すること	8.1.6
				5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当てを考慮すること	8.1.6
				6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順を考慮すること	8.1.6
6.2	システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること	1) 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること	8.2.1
				2) 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること	8.2.1
				3) 管理者は、使用傾向、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と関連した傾向を識別すること	8.2.1
				4) システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を用いること	8.2.1
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること	1) 管理者は、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すること	8.2.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				2) 管理者は、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文書化すること	8.2.2
				3) 管理者は、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合意すること	8.2.2
				4) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な評価を実施すること	8.2.2
				5) 管理者は、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、評価することを確実にすること	8.2.2
				6) システムの受け入れにおいて、性能及びコンピュータの容量･能力の要求事項を考慮すること	8.2.2
				7) システムの受け入れにおいて、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考慮すること	8.2.2
				8) システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮すること	8.2.2
				9) システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること	8.2.2
				10) システムの受け入れにおいて、手動による有効な手順を考慮すること	8.2.2
				11) システムの受け入れにおいて、事業継続の取決めを考慮すること	8.2.2
				12) システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること	8.2.2
				13) システムの受け入れにおいて、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得ること	8.2.2
				14) システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと	8.2.2
				15) 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと	8.2.2
				16) 主要な新しいシステム開発においては、適切な試験を実施し、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こと	8.2.2
6.3	悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1
				2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること	8.3.1
				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としての個別方針を考慮すること	8.3.1
				4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期更新を考慮すること	8.3.1
				5) 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること	8.3.1
				6) 未承認のファイル又は無認可の変更の存在に対しては、正式に調査すること	8.3.1
				7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること	8.3.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				8) 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のすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1
				9) システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること	8.3.1
				10) ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考慮すること	8.3.1
				11) ウイルス感染からの回復のための適切な事業継続計画を考慮すること	8.3.1
				12) 悪意のあるソフトウェアに関するすべての情報を確認すること	8.3.1
				13) 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考慮すること	8.3.1
				14) 管理者は、単なるいたずらと真のウイルス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、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること	8.3.1
				15) 職員は、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認識していること	8.3.1
6.4	システムの維持管理(Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること	1) 災害又は媒体故障が発生した後、極めて重要なすべての業務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こと	8.4.1
				2) 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた場所に保管すること	8.4.1
				3) 重要な業務用ソフトウェアについては、少なくとも3世代又は3サイクル分のバックアップのための情報を保持すること	8.4.1
				4) バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと	8.4.1
				5) 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること	8.4.1
				6) 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定しておくこと	8.4.1
				7) バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること	8.4.1
				8) 復元手順は、定期的に検査及び試験すること	8.4.1
			2) 運用担当者は、自分の作業の記録を継続すること	1) 記録には、システムの起動及び終了の時刻を含めること	8.4.1
				2) 記録には、システム誤り及び実施した是正処置を含めること	8.4.2
				3) 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること	8.4.2
				4) 記録には、記録の作成者の名前を含めること	8.4.2
			3) 運用担当者の記録は、定期的に独立した検査を受けること	（なし）	8.4.2
			4) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.3
				2) 報告された障害の取扱いについては、明確な規定があること	8.4.3
				3) 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと	8.4.3
				4) 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを含むこと	8.4.3
6.5	ネットワークの管理	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	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	1) ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること	8.5.1

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること	8.5.1
				3) ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること	8.5.1
				4) 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立すること	8.5.1
				5) 公衆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、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること	8.5.1
				6) サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整すること	8.5.1
6.6	媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること	1) 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること	8.6.1
				2) 組織の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1
				3) 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること	8.6.1
				4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1
				5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること	8.6.1
			2) 媒体が不要となった場合は、安全、かつ、確実に処分すること	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1
				2) 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること	8.6.2
				3) 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること	8.6.2
				4) 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと	8.6.2
				5) 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること	8.6.2
				6) 処分しようとする媒体を集める場合、集積することによる影響に配慮すること	8.6.2
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	1) 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類に対応させて策定すること	8.6.3
				2) 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること	8.6.3
				3) 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮すること	8.6.3
				4) 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持について考慮すること	8.6.3
				5) 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを確実にすること	8.6.3
				6) 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること	8.6.3

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				7) 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮すること	8.6.3
				8) 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること	8.6.3
				9) 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて考慮すること	8.6.3
				10) 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3
			4) 認可されていないアクセスからシステムに関する文書を保護すること	1) システムに関する文書は、安全に保管すること	8.6.4
				2) システムに関する文書にアクセスできる者は、人数を最小限に抑えること	8.6.4
				3) システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること	8.6.4
				4) システムに関する文書で、公衆ネットワークの公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること	8.6.4
6.7	情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと	1) 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること	8.7.1
				2) セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること	8.7.1
				3) セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること	8.7.1
				4) セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術基準標準を考慮すること	8.7.1
				5) セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること	8.7.1
				6) セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること	8.7.1
				7) セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考慮すること	8.7.1
				8) セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考慮すること	8.7.1
				9) セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること	8.7.1
				10) セキュリティ条件にかかわる合意では、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特別な管理策を考慮すること	8.7.1
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2
				2) 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いること	8.7.2
				3) 媒体の配送においては、宅配業者の身分を確認する手順を導入すること	8.7.2
				4) 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること	8.7.2
				5) 媒体の配送においては、施錠されたコンテナの使用を考慮すること	8.7.2

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				6) 媒体の配送においては、手渡しを考慮すること	8.7.2
				7) 媒体の配送においては、開封防止包装の利用を考慮すること	8.7.2
				8) 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること	8.7.2
				9) 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること	8.7.2
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること	1) 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求すべきか）について考慮すること	8.7.3
				2) 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか。取引相手はこれらをどうやって知るか）について考慮すること	8.7.3
				3) 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること	8.7.3
				4) 電子商取引のセキュリティにおいては、価格情報について考慮すること	8.7.3
				5) 電子商取引のセキュリティにおいては、注文取引について考慮すること	8.7.3
				6) 電子商取引のセキュリティにおいては、審査について考慮すること	8.7.3
				7) 電子商取引のセキュリティにおいては、決済について考慮すること	8.7.3
				8) 電子商取引のセキュリティにおいては、注文について考慮すること	8.7.3
				9) 電子商取引のセキュリティにおいては、責任について考慮すること	8.7.3
				10) 電子商取引に関する当事者間の合意は、権限の詳細も含め、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ること	8.7.3
				11) 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も、合意を交わすこと	8.7.3
				12) 公開している取引システムでは、その取引条件を顧客に公表すること	8.7.3
				13) 電子商取引に用いる基幹コンピュータのも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なネットワーク相互接続のセキュリティ上のかかわりについて、考慮すること	8.7.3
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	1) 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること	8.7.4.1
				2) 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること	8.7.4.2
				3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2
				4) 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の責任を含めること	8.7.4.2
				5) 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること	8.7.4.2
				6) 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること	8.7.4.2
				7) 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること	8.7.4.2
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること	1) 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること	8.7.5

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				2) 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること	8.7.5
				3) 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること	8.7.5
				4) 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること	8.7.5
				5) 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて考慮すること	8.7.5
				6) 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮すること	8.7.5
				7) 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること	8.7.5
				8) 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること	8.7.5
				9) 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること	8.7.5
				10) 電子オフィスシステムのセキュリティにおいては、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について考慮すること	8.7.5
			6) 電子的に公開した情報の完全性を保護するように注意すること	1) 公開されたシステム（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地域又は取引が行われている地域に適用される、法律、規則及び規制に適合することを確実にすること	8.7.5
				2) 情報を公開する前に、正式な認可の手続がとられること	8.7.6
				3) 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって保護すること	8.7.6
				4) 公開している電子システムは、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、情報は、あらゆるデータ保護に関連して制定された法律に従って収集すること	8.7.6
				5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6
				6) 取扱いに慎重を要する情報は、収集の過程及び保管時に保護すること	8.7.6
				7) 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこと	8.7.6
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策をもつこと	1) 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること	8.7.7
				2) 電話を使うときには、適切な注意を払うことの必要を、職員に意識させるること	8.7.7
				3) 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせること	8.7.7
				4) 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残さないようにさせること	8.7.7

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7
7.1	アクセス制御に関する業務上の要求事項	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定義し、文書化すること	1) 利用者ごと、または利用者からなるグループごとに対するアクセス制御規則を、アクセス方針宣言書に明確に記述すること	9.1.1.1
				2) 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること	9.1.1.1
				3) 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること	9.1.1.1
				4) アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること	9.1.1.1
				5) アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること	9.1.1.1
				6) アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮すること	9.1.1.1
				7) アクセス制御に関する個別方針には、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すること	9.1.1.1
				8) アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること	9.1.1.1
				9) アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること	9.1.1.1
				10) アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること	9.1.1.1
				11) アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別すること	9.1.1.2
				12) アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定すること	9.1.1.2
				13) アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をすること	9.1.1.2
				14) アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス権の変更をすること	9.1.1.2
				15) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をすること	9.1.1.2
7.2	利用者のアクセス管理	情報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	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1
				2) 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1
				3) 利用者登録手続において、グループIDの使用は、実施される作業に適切な場合にだけ許可すること	9.2.1
				4) 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査すること	9.2.1

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				5) 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査すること	9.2.1
				6) 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査すること	9.2.1
				7) 利用者登録手続において、重複する利用者IDが別の利用者に発行されないことを確実にすること	9.2.1
				8) 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮すること	9.2.1
				9) 利用者登録手続において、アクセス権の宣言書を利用者に発行すること	9.2.1
				10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1
				11) 利用者登録手続において、認可手続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	9.2.1
				12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1
				13) 利用者登録手続において、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を直ちに取り消すこと	9.2.1
				14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1
			2) 特権の割り当て及び使用は、制限し、管理すること	1) 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること	9.2.2
				2) 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別すること	9.2.2
				3) 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2
				4) 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと	9.2.2
				5) 特権の割り当てにおいて、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使用を促進すること	9.2.2
				6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当てること	9.2.2
			3) パスワードの割当ては、正規の管理手続によって統制すること	1) パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	9.2.3
				2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に求めること	9.2.3
				3) パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること	9.2.3
				4) パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	9.2.3
				5) パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること	9.2.3
				6) パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避けること	9.2.3

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3
				8) パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと	9.2.3
				9) パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びICカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮すること	9.2.3
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	1) 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと	9.2.4
				2) 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと	9.2.4
				3) 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、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こと	9.2.4
7.3	利用者の責任	認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1
				2) すべての利用者に、パスワードを紙に記録して保管しないように助言すること	9.3.1
				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は、パスワードを変更するように助言すること	9.3.1
				4) すべての利用者に、最短6文字の質の良いパスワードを選択すること	9.3.1
				5) すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること	9.3.1
				6) すべての利用者に、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に助言すること	9.3.1
				7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1
				8) すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること	9.3.1
				9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1
				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に助言すること	9.3.1
				11) すべての利用者に、利用者が複数のサービス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、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言すること	9.3.1
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護すること	9.3.2
				2) 無人運転の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、すべての利用者及び請負業者に認識させること	9.3.2
				3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること	9.3.2

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
				4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	9.3.2
				5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、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使用からセキュリティを保つように保護するように助言すること	9.3.2
7.4	ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	9.4.1
				2) ネットワークサービスの使用についての個別方針には、アクセスすること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こと	9.4.1
				3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	9.4.1
				4) ネットワークサービスの使用についての個別方針は、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管理策及び管理手順を対象にすること	9.4.1
				5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	9.4.1
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止すること	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	9.4.2
				2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2
				3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	9.4.2
				4) 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること	9.4.2
				5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2
				6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2
				7) 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること	9.4.2
				8) 組織内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2
				9) 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと	9.4.2
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) 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こと	9.4.3
				2) 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること	9.4.3
				3) コールバックの手順及び制御を徹底的に試験すること	9.4.3
			4) 遠隔コンピュータシステムへの接続は、認証されること	（なし）	9.4.4

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること	1) 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること	9.4.5
				2) ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にすること	9.4.5
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	1) 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	9.4.6
				2) ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと	9.4.6
				3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮すること	9.4.6
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	1) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること	9.4.7
				2) 電子メールには制限を適用すること	9.4.7
				3) 一方向のファイル転送には制限を適用すること	9.4.7
				4) 双方向のファイル転送には制限を適用すること	9.4.7
				5) 対話型アクセスには制限を適用すること	9.4.7
				6) 時間帯又は日付に対応したネットワークアクセスには制限を適用すること	9.4.7
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、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、経路指定の制御策を組み込むこと	1) 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること	9.4.8
				2) ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと	9.4.8
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にすること	（なし）	9.4.9
7.5	オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	（なし）	9.5.1
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2
				2) システムについての情報の開示は最小限にすること	9.5.2
				3) ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しないこと	9.5.2
				4) ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示すること	9.5.2
				5) 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表示をしないこと	9.5.2
				6) 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こと	9.5.2
				7) 許容されるログオンの試みの失敗回数を制限すること	9.5.2
				8) ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと	9.5.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				9) ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること	9.5.2
				10) ログオンの失敗時には、データリンク接続を切ること	9.5.2
				11) 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こと	9.5.2
				12) 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こと	9.5.2
				13) ログオンの失敗時には、失敗した試みを記録すること	9.5.2
				14) ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること	9.5.2
				15) ログオンが無事できた時点で、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こと	9.5.2
			3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有すること	1) 利用者IDには、利用者の特権レベル[例えば、管理者(マネージャ)、監督者(スーパーバイザ)]を表示しないこと	9.5.3
				2) 明らかに業務上の利点がある例外的状況において、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こと	9.5.3
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	1) パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること	9.5.4
				2) パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み入れること	9.5.4
				3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4
				4) パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること	9.5.4
				5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4
				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、一定期間、維持し再使用を防止すること	9.5.4
				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こと	9.5.4
				8) パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること	9.5.4
				9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること	9.5.4
				10) パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること	9.5.4
			5) システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからシステムユーティリティを分離すること	9.5.5
				2) システムユーティリティの使用を、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こと	9.5.5
				3) システムユーティリティを臨時に使用する際には認可をすること	9.5.5
				4) システムユーティリティの使用の制限をすること	9.5.5
				5) システムユーティリティのすべての使用を記録すること	9.5.5
				6) システムユーティリティの認可レベルの明確化及び文書化をすること	9.5.5
				7) すべての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の除去をすること	9.5.5

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮すること	1) 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと	9.5.6
				2) 脅迫に対する警報に対応する責任及び手順を明確に定めること	9.5.6
			7) リスクの高い場所(例えば、組織のセキュリティ管理外にある公共又は外部領域)にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末は遮断されること	1) 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	9.5.7
				2) 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであること	9.5.7
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供すること	1) 既定の時間枠(例えば、バッチファイル伝送のための時間枠)を使うか、又は短時間の通常の対話型処理(session)を用いること	9.5.8
				2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8
7.6	業務用ソフトウェアのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	1) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること	9.6.1
				2) 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮すること	9.6.1
				3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮すること	9.6.1
				4) 情報へのアクセス制限では、利用者のアクセス権(例えば、読出し、書込み、削除、実行)を制御することを考慮すること	9.6.1
				5) 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にすること	9.6.1
				6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	1) 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること	9.6.2
				2) 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること	9.6.2
7.7	システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること	1) 監査記録には、利用者IDを含めること	9.7.1
				2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1
				3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1
				4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1
				5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1
			2) 情報処理設備の使用状況を監視する手順を確立すること	1) 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること	9.7.2.1

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				2) 監視項目には、認可されているアクセスについて、利用者IDを含むこと	9.7.2.1
				3) 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと	9.7.2.1
				4) 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと	9.7.2.1
				5) 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと	9.7.2.1
				6) 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと	9.7.2.1
				7) 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること	9.7.2.1
				8) 監視項目には、すべての特権操作について、システムの起動及び停止を含めること	9.7.2.1
				9) 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること	9.7.2.1
				10) 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること	9.7.2.1
				11) 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1
				12) 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること	9.7.2.1
				13) 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること	9.7.2.1
				14) 監視項目には、システム警告又は故障について、システム記録例外事項を含めること	9.7.2.1
				15) 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること	9.7.2.1
			3) 監視の結果は、定期的に見直すこと	1) 監視結果の見直しの頻度は、関係するリスクによって決めること	9.7.2.2
				2) 考慮すべきリスク要因には、業務手続に与える重要性の度合を含めること	9.7.2.2
				3) 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること	9.7.2.2
				4) 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること	9.7.2.2
				5) 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること	9.7.2.2
			4) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること	1) セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製すること	9.7.2.3
				2) ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮すること	9.7.2.3
				3) 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮すること	9.7.2.3
				4) 記録機能のセキュリティに対して注意すること	9.7.2.3
				5) 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること	9.7.2.3
			5) コンピュータの時計は正しく設定すること	1) コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時[例えば、万国標準時に（UCT）又は現地の標準時]に合わせること	9.7.3
				2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
7.8	移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業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	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特別な注意を払うこと	1) 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること	9.8.1
				2) 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること	9.8.1
				3) 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1
				4) 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと	9.8.1
				5) 悪意のあるソフトウェアに対抗する手順を整えること	9.8.1
				6) 悪意のあるソフトウェアに対抗する手順は最新のものであること	9.8.1
				7) 移動型計算処理を用いる要員に対する訓練を計画すること	9.8.1
				8) 情報を素早く、容易にバックアップできる装置が利用可能となっていること	9.8.1
				9) これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること	9.8.1
				10) 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	9.8.1
				11) ネットワークに接続された移動型設備の使用に対して適切な保護がなされること	9.8.1
				12) 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	9.8.1
				13) 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること	9.8.1
				14) 大切な、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こと（可能ならば、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こと）	9.8.1
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手配されていることを確実にすること	1) 遠隔作業の場所に適切な保護が整っていること	9.8.2
				2) 遠隔作業は、経営陣によって認可され、管理されること	9.8.2
				3) 遠隔作業は、この作業形態のため適切に手配されていること	9.8.2
				4) 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること	9.8.2
				5) 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可すること	9.8.2
				6) 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮すること	9.8.2
				7) 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮すること	9.8.2
				8) 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること	9.8.2

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				9) 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること	9.8.2
				10) 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮すること	9.8.2
				11) 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮すること	9.8.2
				12) 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの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すること	9.8.2
				13) 遠隔作業活動のための適切な装置を準備すること	9.8.2
				14) 遠隔作業活動のための適切な保管棚・庫の準備をすること	9.8.2
				15) 遠隔作業活動のための許可される作業を明確にすること	9.8.2
				16) 遠隔作業活動のための作業時間を明確にすること	9.8.2
				17) 遠隔作業活動のための保持してもよい情報の分類を明確にすること	9.8.2
				18) 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること	9.8.2
				19) 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること	9.8.2
				20) 遠隔作業を行う場所の物理的なセキュリティを確保すること	9.8.2
				21) 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明確にすること	9.8.2
				22) ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること	9.8.2
				23) バックアップ及び事業継続のための手順を明確にすること	9.8.2
				24) 監査及びセキュリティの監視を行うこと	9.8.2
				25) 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること	9.8.2
8.1	システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にすること	1) セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1
				2) セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること	10.1.1
				3) 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1
				4) 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること	10.1.1
				5) 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること	10.1.1
				6) セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること	10.1.1
				7) セキュリティが確保できなかった場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害の可能性もセキュリティ要求事項及び管理策に反映されること	10.1.1
8.2	業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、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こと	1) 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること	10.2.1
				2) 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること	10.2.1
				3) データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること	10.2.1
				4) 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること	10.2.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				5) データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること	10.2.1
				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の二重入力又はその他の入力検査を実施すること	10.2.1
				7) 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること	10.2.1
				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の紙に印刷した入力文書の点検を考慮すること	10.2.1
				9) 妥当性確認の誤りに対応する手順について考慮すること	10.2.1
				10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1
				11) データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること	10.2.1
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	1) 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること	10.2.2.1
				2) データ変更を行う追加･削除の機能を持つプログラムの使用及びその位置について考慮すること	10.2.2.1
				3) プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること	10.2.2.1
				4) データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮すること	10.2.2.1
				5) 取引処理の更新後のデータファイルのバランスをとるための処理又はバッチの制御を考慮すること	10.2.2.1
				6) 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること	10.2.2.1
				7) システム生成データの妥当性確認を考慮すること	10.2.2.1
				8) 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること	10.2.2.1
				9) レコード及びファイルの全体のハッシュ合計の検査を考慮すること	10.2.2.1
				10) 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること	10.2.2.1
				11) プログラムが正しい順序で実行されることの検査を考慮すること	10.2.2.1
				12) プログラムが正しい順序で実行されない場合は終了され、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検査を考慮すること	10.2.2.1
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮すること	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をすること	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4
				2) 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制御の回数を含むこと	10.2.4
				3) 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、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供給を含むこと	10.2.4
				4) 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと	10.2.4

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				5) 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと	10.2.4
8.3	暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること	1) 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること	10.3.1
				2) 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを、考慮すること	10.3.1
				3) 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを、考慮すること	10.3.1
				4) 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について、考慮すること	10.3.1
				5) 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について、考慮すること	10.3.1
				6) 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを、考慮すること	10.3.1
				7) 暗号による管理策の使用に関する個別方針を定めるとき、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を考慮すること	10.3.1
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	1) リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること	10.3.2
				2) 組織における暗号利用の個別方針を実施するとき、世界の異なる地域における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること	10.3.2
				3) 暗号技術の輸出入に適用される規制も考慮すること	10.3.2
				4) 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること	10.3.2
				5) 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること	10.3.2
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用いること	1) 秘密かぎの機密性を保護するために注意を払うこと	10.3.3
				2) 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管すること	10.3.3
				3) 公開かぎの完全性を保護すること	10.3.3
				4) ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること	10.3.3
				5) ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること	10.3.3
				6) 電子商取引の場合、ディジタル署名の法的位置付けを知ること	10.3.3
				7) 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること	10.3.3
				8) 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求めること	10.3.3
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いること	（なし）	10.3.4

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			5) 一連の合意された標準類，手順及び方法に基づくかぎ管理システムを，暗号技術の利用を支援するために用いること	1) 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること	10.3.5.1
				2) すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護すること	10.3.5.1
				3) かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いること	10.3.5.1
				4) 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を生成する方法を定めること	10.3.5.1
				5) かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること	10.3.5.1
				6) かぎ管理システムでは、予定している利用者にかぎを配付する方法を定めること	10.3.5.2
				7) かぎ管理システムでは、かぎを保存する方法を定めること	10.3.5.2
				8) かぎ管理システムでは、かぎを変更又は更新する方法を定めること	10.3.5.2
				9) かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること	10.3.5.2
				10) かぎ管理システムでは、かぎを無効にする方法について定めること	10.3.5.2
				11) かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること	10.3.5.2
				12) かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定めること	10.3.5.2
				13) かぎ管理システムでは、かぎを破壊する方法を定めること	10.3.5.2
				14) かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること	10.3.5.2
				15) かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めること	10.3.5.2
				16) かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクによって決めること	10.3.5.2
				17) 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること	10.3.5.2
				18) 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に関する問題を扱うこと	10.3.5.2
8.4	システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため	1) 運用システムでのソフトウェアの実行を管理すること	1) 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること	10.4.1
				2) 運用システムは、実行可能なコードだけを保持すること	10.4.1
				3) 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しないこと	10.4.1
				4) 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること	10.4.1
				5) 古い版のソフトウェアは、事故対策用として保持すること	10.4.1
				6) 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理されること	10.4.1

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				7) 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること	10.4.1
				8) セキュリティ上の欠陥を除去するか又は軽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こと	10.4.1
				9) 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること	10.4.1
				10) 供給者の活動は監視されることが望ましい	10.4.1
			2) 試験データを保護し，管理すること	1) システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2
				2) 個人情報が入っている運用データベースは、使用しないようにすること	10.4.2
				3) 個人情報が入っている情報を使用する場合は，使用する前に，個人的要素を消去すること	10.4.2
				4) 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用すること	10.4.2
				5) 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けること	10.4.2
				6) 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること	10.4.2
				7) 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること	10.4.2
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持すること	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3
				2) 各アプリケーションごとに、プログラムライブラリ管理責任者を任命すること	10.4.3
				3) IT支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと	10.4.3
				4) 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと	10.4.3
				5) その業務用ソフトウェアのためのIT支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること	10.4.3
				6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3
				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、監査記録を維持管理すること	10.4.3
				8) ソースプログラムの旧版は、記録保管しておくこと	10.4.3
				9) 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと	10.4.3
				10) 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こと	10.4.3
8.5	開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	1) 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないこと	10.5.1
				2) 支援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	10.5.1
				3) 変更に対する正式な合意及び承認が得られていることを確実にすること	10.5.1
				4) 業務用ソフトウェア及び運用の変更管理手順は統合されること	10.5.1
				5) 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること	10.5.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				6) 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること	10.5.1
				7) 業務用ソフトウェア及び運用の変更過程では、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この手順をレビューすること	10.5.1
				8) 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識別すること	10.5.1
				9) 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を得ること	10.5.1
				10) 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること	10.5.1
				11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1
				12) 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること	10.5.1
				13) 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実にすること	10.5.1
				14) 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと	10.5.1
				15) 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること	10.5.1
				16) 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること	10.5.1
				17) 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること	10.5.1
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	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及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること	10.5.2
				2) 年間支援計画及び予算には、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ようにすること	10.5.2
				3) 実施前に行う適切なレビューに間に合うように、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こと	10.5.2
				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こと	10.5.2
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	1) ベンダー供給のパッケージソフトウェアは、変更しないで使用すること	10.5.3
				2) パッケージソフトウェアの変更が絶対必要であると判断された場合は、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を考慮すること	10.5.3
				3) パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること	10.5.3
				4) パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること	10.5.3
				5) パッケージソフトウェアの変更が絶対必要であると判断された場合は、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影響を考慮すること	10.5.3

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				6) 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと	10.5.3
				7) 変更はすべて、完全に試験すること	10.5.3
				8) 変更はすべて、文書化すること	10.5.3
				9) 将来更新されたソフトウェアに再び適用できるようにすること	10.5.3
			4) 隠れチャネル (Covert channels) 及びトロイの木馬 (Trojan code) の危険性から保護するために，ソフトウェアの購入，使用及び修正を管理し，検査すること	1) プログラムは定評のある開発元のものだけを購入すること	10.5.4
				2) コードの確認ができるようにソースコードでプログラムを購入すること	10.5.4
				3) 評価された製品を用いること	10.5.4
				4) 使用前にすべてのソースコードを検査すること	10.5.4
				5) 一旦導入したコードへのアクセス及びそのコードへの変更を管理すること	10.5.4
				6) 重要なシステムでの作業には確実に信頼できる要員を用いること	10.5.4
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いること	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所有権について考慮すること	10.5.5
				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考慮すること	10.5.5
				3) ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託 (escrow) 契約に関する取決めについて考慮すること	10.5.5
				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について考慮すること	10.5.5
				5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5
				6) ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること	10.5.5
9.1	事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	1) 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること	11.1.1
				2) 業務手続の中断が事業に及ぼすと思われる影響を理解し (組織の存続性を脅かす可能性のある重大な事件･事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である)、情報処理施設の事業目的を確立すること	11.1.1
				3) 事業継続の手続の一部をなすこともある適切な保険への加入を考慮すること	11.1.1
				4) 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること	11.1.1
				5) 合意された戦略に従って事業継続計画を明確にし、文書化すること	11.1.1
				6) 実行されている計画及び手続を定期的に試験し、更新すること	11.1.1
				7) 事業継続管理が組織の手続及び機構に確実に組み込まれるようにすること	11.1.1
				8) 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること	11.1.1
			2) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること	1) それらの障害の影響 (損害規模及び回復期間の両面から) を判断するために、リスクアセスメントを行うこと	11.1.2
				2) これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること	11.1.2
			3) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること	1) 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること	11.1.2

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
			4) 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること	1) 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること	11.1.3
				2) 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施すること	11.1.3
				3) 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること	11.1.3
				4) 事業継続計画の作成過程では、合意された手順及び過程を文書化すること	11.1.3
				5) 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと	11.1.3
				6) 事業継続計画の作成過程では、計画の試験及び更新を行うこと	11.1.3
				7) 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと	11.1.3
				8) これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること	11.1.3
			5) 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、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること	1) 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること	11.1.4
				2) 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正すること	11.1.4
				3) 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること	11.1.4
				4) 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること	11.1.4
				5) 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと	11.1.4
				6) 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること	11.1.4
				7) 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること	11.1.4
				8) 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること	11.1.4
				9) 事業継続計画作成の枠組みでは、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保するために計画される認識及び教育活動について考慮すること	11.1.4
				10) 事業継続計画作成の枠組みでは、個人の責任について考慮すること	11.1.4
				11) 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること	11.1.4
				12) 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること	11.1.4
				13) 事業継続計画作成の枠組みでは、各計画には特定の責任者がいること	11.1.4

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				14) 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること	11.1.4
				15) 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること	11.1.4
			6) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること	1) 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること	11.1.5.1
				2) 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと	11.1.5.1
				3) 計画の個々の構成要素を、頻繁に試験すること	11.1.5.1
				4) 計画が実際に役立つことを保証するために、様々な手法を使用すること	11.1.5.1
				5) 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）	11.1.5.1
				6) 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）	11.1.5.1
				7) 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）	11.1.5.1
				8) 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施する）	11.1.5.1
				9) 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）	11.1.5.1
				10) 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験する）	11.1.5.1
				11) いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること	11.1.5.1
			7) 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること	1) 事業継続上の問題を適切に対処することを確実にするための手順は、組織の変更管理プログラムの中に含まれること	11.1.5.2
				2) 各事業継続計画の定期的見直しに対する責任を割り当てること	11.1.5.2
				3) 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること	11.1.5.2
				4) この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること	11.1.5.2
10.1	法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること	12.1.1
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するように，適切な手続を実行すること	1) ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること	12.1.2.2
				2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2
				3) ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること	12.1.2.2
				4) 適切な財産登録簿を維持管理すること	12.1.2.2
				5) 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること	12.1.2.2
				6) 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること	12.1.2.2
				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を確認すること	12.1.2.2
				8) 適切な使用許諾条件を維持管理するための個別方針を定めること	12.1.2.2

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				9) ソフトウェアの処分又は他人への譲渡についての個別方針を定めること	12.1.2.2
				10) 適切な監査ツールを用いること	12.1.2.2
				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使用条件に従うこと	12.1.2.2
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	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、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について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、光学媒体）の詳細も定めておくこと	12.1.3
				2) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること	12.1.3
				3) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること	12.1.3
				4) 記録の保管に用いられる媒体が劣化する可能性を考慮すること	12.1.3
				5) 保管及び取扱いの手順は、製造業者の推奨に従って実行すること	12.1.3
				6) 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、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）を確保する手順を含めること	12.1.3
				7) 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること	12.1.3
				8) 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にすること	12.1.3
				9) 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3
				10) 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行すること	12.1.3
				11) 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること	12.1.3
				12) 主要な情報の出典一覧を維持管理すること	12.1.3
				13) 重要な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行すること	12.1.3
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	1) データ保護の担当責任者を任命すること	12.1.4
				2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ所有者の責任であること	12.1.4
				3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任であること	12.1.4
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための管理策を用いること	1) 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること	12.1.5
				2) 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること	12.1.5
				3) 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること	12.1.5
				4) すべての利用者は、その許可されたアクセスの正確な範囲を認識していること	12.1.5
				5) 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること	12.1.5

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				6) ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表示すること	12.1.5
				7) 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること	12.1.5
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために，法的な助言を求めること	1) 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること	12.1.6
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	1) 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること	12.1.7.1
				2) 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとること	12.1.7.1
				3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3
				4) コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっておくこと	12.1.7.3
				5) コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること	12.1.7.3
				6) コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること	12.1.7.3
				7) 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得ること	12.1.7.3
10.2	セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること	1) 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること	12.2.1
				2) 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること	12.2.1
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	1) 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行うこと	12.2.2
				2) 技術適合の検査では、専門家の技術援助を得ること	12.2.2
				3) 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されること	12.2.2
				4) 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること	12.2.2
				5) いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施されること	12.2.2
10.3	システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意されること	1) 監査要求事項は、担当経営陣の同意を得ること	12.3.1
				2) 検査の範囲は、合意され、管理されること	12.3.1
				3) 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定すること	12.3.1
				4) 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること	12.3.1

JIS X 5080:2002と管理基準との対比表

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002
				5) 複製ファイルは、監査が完了した時点で消去すること	12.3.1
				6) 検査を実施するための情報資源は、明確に識別され、利用可能であること	12.3.1
				7) 特別又は追加処理の要求事項は、識別され、合意されること	12.3.1
				8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録されること	12.3.1
				9) すべての手順、要求事項及び責任について、文書化すること	12.3.1
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること	1) システム監査ツールは、開発及び運用システムから分離しておくこと	12.3.2
				2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2