ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(1 / 79)

2002/3/28

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
第4 詳細管理策						
1 セキュリティポリシー						
	(1) 情報セキュリティポリシー			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。	経営陣は，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，情報セキュリティに対する支持及び責任を明示するのが望ましい。	
		①	情報セキュリティポリシーは、経営陣により承認及び制定されること。		3.1.1	情報セキュリティ基本方針文書　基本方針文書は，経営陣によって承認され，適当な手段で，全従業員に公表し，通知することが望ましい。基本方針文書には，経営陣の責任を明記し，情報セキュリティの管理に対する組織の取組み方法を明示することが望ましい。少なくとも，次の指針を含めることが望ましい。 a)情報セキュリティの定義，その目的及び適用範囲，並びに情報共有を可能にするための機構としてのセキュリティの重要性（0.2参照）。 b)情報セキュリティの目標及び原則を支持する経営陣の意向声明書。 c)組織にとって特に重要なセキュリティ基本方針，原則，標準類及び適合する要求事項の簡潔な説明。それらの例を，次に示す。 1)法律上及び契約上の要求事項への適合 2)セキュリティ教育の要求事項 3)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 4)事業継続管理 5)セキュリティ基本方針違反に対する措置 d)セキュリティの事件・事故を報告することも含め，情報セキュリティマネジメントの一般的責任及び特定責任の定義。 e)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。 この基本方針は，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が望ましい。
		②	情報セキュリティポリシーは、必要な関係者全員に公表されること。			同上
		③	情報セキュリティポリシーは、定期的に見直され、必要に応じて変更されること。また、変更された場合にはその変更内容の妥当性が確認されること。		3.1.2	見直し及び評価　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，存在することが望ましい。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が望ましい。また，次の事項について，日程を定め，定期的に見直しを実施することが望ましい。 a)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。 b)事業効率における管理策の費用及び影響。 c)技術変更による効果。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(2 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
2 セキュリティ組織						
	㈠ 情報セキュリティ・インフラストラクチャ			組織内の情報セキュリティを管理するため。	組織内において情報セキュリティを導入し，その実施状態を統制するための管理上の枠組みを確立することが望ましい。 情報セキュリティ基本方針を承認し，セキュリティに対する役割を割り当て，組織全体におけるセキュリティの実施を調整するために，経営陣を指導者とする適切な運営委員会を設置することが望ましい。必要ならば，専門家による情報セキュリティについての助言の情報源を明らかにし，組織内で利用できるようにするのがよい。業界の動向に遅れないようにし，規格及び評価方法に目を配り，セキュリティの事件・事故に対処するときの適切な連絡窓口を確保するために，外部のセキュリティ専門家との連絡網を築くことが望ましい。情報セキュリティは，各専門家（例えば，管理者，利用者，実務管理者，業務用ソフトウェア設計者，監査人及びセキュリティ担当者，並びに，保険及びリスクマネジメントのような分野の専門家）と協力して取り組むことが望ましい。	
		①	経営陣が情報セキュリティについて討論する委員会を設置すること。		4.1.1	情報セキュリティ運営委員会　情報セキュリティは，経営陣全員による事業上の共同責任とする。したがって，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陣による目に見える形での支持を確実にするために，運営委員会の設置を考えることが望ましい。この委員会は，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が望ましい。委員会は，既存の経営組織の一部であってもよい。通常，このような委員会では，次のことを行う。 a)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。 b)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の監視。 c)情報セキュリティの事件・事故の見直し及び監視。 d)情報セキュリティを強化するための主要な発議の承認。 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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(3 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	組織内の情報セキュリティを管理するため、関連する部門を横断的に調整する部門等を設けること。		4.1.2	情報セキュリティの調整　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が必要な場合がある。通常，このような委員会では，次のことを行う。 a)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。 b)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。 c)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。 d)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。 e)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。 f)情報セキュリティの事件・事故の見直し。 g)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。
		③	個々の情報資産に対する保護責任及び特定の業務に関する実施責任を明確にすること。		4.1.3	情報セキュリティ責任の割当て　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，明確に定めることが望ましい。 情報セキュリティ基本方針（3.1参照）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が望ましい。必要ならば，この基本方針に，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してもよい。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が望ましい。 多くの組織では，セキュリティの開発及び実行に対して全般的な責任をもち，管理策の識別を支援するために，一人の情報セキュリティ管理者が任命される。 しかし，管理策の実施及び資源配分に対する責任は，多くの場合，個々の管理者にある。一般的には，各情報資産にそれぞれ一人の責任者を任命し，その者が日々のセキュリティに責任をもつことが普通である。 情報資産の責任者は，そのセキュリティ責任を個々の管理者又はサービス提供者に委任してよい。しかし，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ち，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が望ましい。 各管理者が責任を負う範囲は明確に規定することが必須である。特に，次のことを実施することが望ましい。 a)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が望ましい。 b)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，文書化されることが望ましい。 c)承認の権限の範囲は，明確に定義され，文書化されることが望ましい。

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	情報処理施設及び設備の新規導入に対する経営陣による承認プロセスを定めること。		4.1.4	情報処理設備 の認可手続 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が望ましい。次の管理策を考慮することが望ましい。 a)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が望ましい。また，すべての関連するセキュリティ個別方針及び要求事項を確実に満たすために，その情報システムセキュリティ環境の維持に責任をもつ管理者からも承認を得ることが望ましい。 b)必要ならば，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，検査することが望ましい。 備考　確実な接続のためには，型式承認が必要な場合がある。 c)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，認可を得ることが望ましい。 d)職場での個人用情報処理設備の使用は，新しいぜい 脆）弱性を発生させる可能性があるため，そのような使用は，評価を受け，認可を得ることが望ましい。 これらの管理策は，ネットワーク化された環境では特に重要となる。
		⑤	情報セキュリティに関して、適宜社内または社外の専門家から助言を受け、その内容を組織内に公表すること。		4.1.5	専門家による情報セキュリティの助言 専門家によるセキュリティの助言は，おそらく多くの組織によって要求される。理想的には，このような助言は，経験を積んだ社内の情報セキュリティ助言者が行うのが望ましい。すべての組織が，専門の助言者を雇うことを望んでいるとは限らない。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に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を推奨する。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が望ましい。 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が望ましい。セキュリティ脅威の評価の質及び管理策についての助言の質が，組織の情報セキュリティの有効性を決定する。有効性及び影響力を最大にするために，助言者は，組織内のあらゆる経営者と直接接触できることが望ましい。 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できるだけ速やかに相談を受け付け，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が望ましい。ほとんどの内部的なセキュリティ調査は，通常，経営陣のもとで実施されるが，情報セキュリティ助言者に，調査についての助言，指導又は指揮を依頼してもよい。
		⑥	監督官庁、規制当局及びセキュリティ上重要な役割を担う外部組織への連絡体制を維持すること。		4.1.6	組織間の協力 セキュリティの事件・事故の場合，適切な処置が素早く取られ，助言が得られることを確実にするために，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が望ましい。同様に，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が望ましい。 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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(5 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑦	情報セキュリティポリシーの導入や運用の状況を客観的視点で見直すこと。		4.1.7	情報セキュリティの他者によるレビュー　情報セキュリティ基本方針文書（3.1参照）には，情報セキュリティの基本方針及び責任を記述する。組織の行動が基本方針を適切に反映し，基本方針が実行可能及び有効であることを保証するために，情報セキュリティ基本方針の実施を他者がレビューすることが望ましい（2.2参照）。 このようなレビューは，内部監査部門，他部門の管理者又はそのようなレビューを専門とする第三者組織が実施してもよい。ただし，その場合，レビューを実施する者は，適切な技能及び経験をもつものとする。
	⑵ 第三者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。	第三者による組織の情報処理設備へのアクセスを，管理することが望ましい。 このような第三者のアクセスが業務上必要となる場合は，セキュリティとの関連及び管理要求事項を決めるためにリスクアセスメントを実施することが望ましい。管理策は，その第三者の同意を得て，契約書に明記することが望ましい。 この第三者のアクセスには，他の関係者がかかわることもある。第三者のアクセスを認める契約書には，他の適格な関係者の指名を許可すること及びこれら関係者のアクセス条件も含めることが望ましい。 この規格は，そのような契約の根拠として，また，情報処理の外部委託を考慮する場合に用いることが考えられる。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(6 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、評価されたリスクに基づき必要な措置を講ずること。		4.2.1 4.2.1.1と4.2.1.2と4.2.1.3	第三者のアクセスから生じるリスクの識別 アクセスの種類　第三者に対して許可されるアクセスの種類は，特に重要な意味をもつ。例えば，ネットワーク接続を介した論理的アクセスのリスクは，物理的アクセスに起因するリスクとは異なっている。次のアクセスの種類を考慮することが望ましい。 a)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。 b)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。 アクセスの理由　第三者は，様々な理由によってアクセスを許されることがある。例えば，組織にサービスを提供する，施設内に所在しない第三者が，物理的及び論理的アクセスを許されることがある。そのような第三者の例としては，次のものがある。 a)システムレベル又は個々の適用業務機能にアクセスする必要のある，ハードウェア及びソフトウェアの支援要員。 b)情報の交換，情報システムのアクセス，又はデータベースの共有を許される，取引又は合弁事業の相手。 情報は，セキュリティマネジメントが不十分であると，第三者からのアクセスによって危険にさらされることがある。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が望ましい。そこでは，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が望ましい。 施設内の請負業者 契約書に明記された期間で施設内に所在する第三者も，セキュリティの弱点となることがある。施設内の第三者の例としては，次のものがある。 a)ハードウェア及びソフトウェアの保守及び支援要員。 b)清掃人，配膳人，警備員及びその他の外部組織による支援要員。 c)実習生及びその他の短期の臨時要員。 d)コンサルタント。 情報処理施設への第三者アクセス管理のためにどのような管理策が必要かを理解することは，非常に重要である。一般に，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が望ましい（4.2.2参照）。例えば，情報の機密性が特に必要な場合は，守秘義務契約を用いることになる（6.1.3参照）。 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し，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，開始させないほうがよい。

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	第三者に対し、組織の情報処理施設及び設備へのアクセスを許可する場合、セキュリティ要求事項を明記した正式な契約を締結すること。		4.2.2	第三者との契約書に記載するセキュリティ要求事項　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が望ましい。その契約には，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。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が望ましい。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が望ましい。契約書には，次の事項を含めることを考慮することが望ましい。 a)情報セキュリティに関する一般方針。 b)次の事項を含む資産保護。 1)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。 2)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。 3)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。 4)完全性及び可用性。，5)情報の複製及び開示の制限。 c)利用できる各サービスの記述。 d)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。 e)必要ならば，要員の異動に関する規定。 f)契約当事者それぞれの義務。 g)法律関連事項（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（12.1参照）。 h)知的所有権（IPR）及び著作権（12.1.2参照）の取扱い，並びに共同作業に伴う保護の条項（6.1.3参照）。 i)次の事柄を含むアクセス制御の合意事項。 1)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。 2)利用者によるアクセス及び利用者特権の認可手続。 3)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。 j)検証可能な性能基準，それらの監視及び報告の定義。 k)利用者の活動を監視し，無効にする権利。 l)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。 m)問題解決のための段階的処理手順の確立。必要ならば，障害対策の取決めも考慮することが望ましい。 n)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。 o)明確な報告の構成及び合意された報告の形式。 p)変更管理の明確な，設定された手続。 q)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。 r) 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。 s)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（8.3参照）。 t)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。 u)第三者と下請け業者とのかかわり。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(8 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
	(3) 第三者への委託（アウトソーシングや外部委託）			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。	外部委託に関する取決めは，当事者間の契約において，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対するリスク，セキュリティの管理策及び手順について記述することが望ましい。	
		①	情報システムの管理や制御を委託する場合、セキュリティ要求事項を明記した正式な契約を締結すること。		4.3.1	外部委託契約におけるセキュリティ要求事項　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が望ましい。 例えば，契約書には次の事項を取り扱うことが望ましい。 a)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。 b)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。 c)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。 d)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。 e)災害の際に，サービスの可用性をどのように維持するか。 f)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。 g)監査する権利。 4.2.2に列挙した事項も，この契約の一部として考慮することが望ましい。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が望ましい。 外部委託契約は幾つかの複雑なセキュリティ問題を引き起こすことがあるが，この規格に含まれている管理策は，セキュリティマネジメント計画の構成及び内容に合意するための出発点として役立てることができる。
3. 情報資産の分類及び管理						
	(1) 情報資産に対する責任			組織の資産の適切な保護を維持するため。	すべての主要な情報資産を明らかにし，その管理者を指定することが望ましい。 資産として明確にすることは，適切な保護の維持を確実にすることに役立つ。すべての主要な資産に対して管理者を明確にすること及び適切な管理策を維持する責任を割り当てることが望ましい。管理策の実施責任は委任してもよい。資産に対する責任は，指定されたその管理者にあることが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(9 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	情報資産を適切に管理するため資産台帳を作成し、重要な情報資産のすべてを登録すること。		5.1.1	資産目録　資産目録は，資産保護を効果的に行うことを確実にするために役立ち，また，他の業務上の目的[例えば，健康，安全，保険，財務(資産管理)の理由]のために必要となることもある。資産目録を作成する過程はリスクマネジメントの重要な局面である。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必要がある。この情報に基づいて，組織は資産の価値及び重要度に対応した保護のレベルを設定することができる。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，維持することが望ましい。各資産を，その現在の所在（喪失又は損傷から回復しようとするときに重要）とともに，明確に識別し，その管理責任及びセキュリティの分類（5.2参照）について合意し，文書化することが望ましい。情報システムに関連づけた資産の例を次に示す。 a)情報資産：データベース及びデータファイル，システムに関する文書，ユーザマニュアル，訓練資料，操作又は支援手順，継続計画，代替手段の手配，記録保管された情報。 b)ソフトウェア資産：業務用ソフトウェア，システムソフトウェア，開発用ツール及びユーティリティ。 c)物理的資産：コンピュータ装置（プロセッサ，表示装置，ラップトップ，モデム），通信装置（ルータ，PBX，ファクシミリ，留守番電話），磁気媒体（テープ及びディスク），その他の技術装置（電源，空調装置），什器，収容設備。 d)サービス：計算処理及び通信サービス，一般ユーティリティ（例えば，暖房，照明，電源，空調）。
	(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。	情報は，保護の必要性，優先順位，及び程度を示すために分類することが望ましい。 情報の，取扱いに慎重を要する度合い及び重要性の度合いはさまざまである。情報によっては，保護の度合いの加重又は特別な取扱いが必要なこともある。一連の適切な保護レベルを定め，特別な取扱い方法の必要性を示すために，情報を体系的に分類することが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(10 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	事業における必要性や問題が生じた場合の影響度に応じた情報資産の分類基準を設けること。		5.2.1	分類の指針　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が望ましい。一般的に，情報を分類することは，その情報をどのように取り扱い，保護するかを決めるための近道である。 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が望ましい。また，組織にとってその情報がどれほど重要であるか（例えば，その完全性及び可用性の観点から）によってラベル付けすることが適切な場合もある。情報は，多くの場合，ある期間を過ぎると（例えば，情報が一般に公開された後），慎重な取扱いを必要とせず，また，重要でもなくなる。これらの点も考慮して，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が望ましい。分類の指針には，ある時点での情報の分類は必ずしも恒久的なものではなく，前もって決められた個別方針（9.1参照）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が望ましい。 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が望ましい。複雑すぎる体系は，使用するのが面倒で不経済となるか，又は実用的でなくなる。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が望ましい。 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しする責任は，その情報の作成者又は指定された管理者にあることが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(11 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	情報資産を分類基準に従い分類し、その取扱いに関する手順を定めること。		5.2.2	情報のラベル付け及び取扱い　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，適切な一連の手順を定めることが重要である。これらの手順は，物理的形式及び電子的形式の情報資産に適用できる必要がある。各分類について，次の種類の情報処理活動に適用する取扱い手順を定めることが望ましい。 a)複製 b)保存 c)郵便，ファクシミリ及び電子メールによる伝達 d)移動電話，音声メール，留守番電話を含め，言葉による伝達 e)破棄 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）付けることが望ましい。ラベル付けは，5.2.1に定める規則に従った分類を反映することが望ましい。考慮すべき項目として，印刷された文書，スクリーン表示，記録媒体（テープ，ディスク，CD，カセット），電子的なメッセージ及びファイル転送が含まれる。 一般的に，物理的ラベルは，最も適切なラベル付け形式である。しかし，電子形式の文書のようなある種の情報資産には物理的なラベル付けをすることはできず，電子的手段によるラベル付けが必要となることもある。
4 人的セキュリティ						
	⑴ 職務定義および採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。	要員を採用する段階からセキュリティの責任に言及すること，それを雇用契約に盛り込むこと，及び雇用中はその監視を行うことが望ましい。 採用候補者を十分に審査（6.1.2参照）することが望ましく，慎重を要する業務に就く者については特にそうすることが望ましい。すべての従業員及び情報処理設備の外部利用者は，機密保持（守秘義務）契約書に署名することが望ましい。	
		①	情報セキュリティポリシーに定義した情報セキュリティに関する役割及び責任を職務定義書に明記すること。		6.1.1	セキュリティを職責に含めること　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（3.1参照）で定められたとおりに，適切に文書化することが望ましい。 それには，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とともに，特定の資産を保護するための具体的な責任，又は特定のセキュリティの手続若しくは活動を進めるための具体的な責任をもれなく含めることが望ましい。

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	採用する人員に求める資質や職能を明確にすること。		6.1.2	要員審査及びその個別方針　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が望ましい。これには次の管理策を含むことが望ましい。 a)提出された人物推薦状は役にたつか（例えば，業務ごとに評価の記述があるか）。 b) 履歴書の検査（完全，かつ，正確であるか）。 c) 提示された学術上及び職業上の資格の確認。 d) 公的証明書（パスポート又は同種の文書）の検査。 最初の発令で就く仕事か昇進して就く仕事であるかに拘わらず，情報処理設備にアクセスすることがその担当者にとって必要になる場合，特にそれらの設備が取扱いに慎重を要する情報（例えば，財務情報又は極秘情報）を扱っているときに，組織は，その者に対して信用調査も行うことが望ましい。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が望ましい。 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が望ましい。これら職員が派遣会社から派遣される場合には，派遣会社の審査が完全でなかったとき又は審査の結果に疑義若しくは懸念があるときに，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が望ましい。 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，経営者は，それらに対する管理監督についての評価を行うことが望ましい。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が望ましい。 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が望ましい。個人的又は金銭的問題，行動又は生活様式の変化，度重なる欠勤，及びストレス又は気落ちの現れは，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につながることがある。この情報は，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が望ましい。
		③	人員の採用条件の一部として、被雇用者から機密保持合意書への署名を得ること。		6.1.3	機密保持契約　機密保持契約又は守秘義務契約は，情報が機密又は秘密であることに留意させるために用いられる。従業員は，雇用条件の一部として常に，このような契約書に署名することが望ましい。 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が望ましい。 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，見直しを行うことが望ましい。
		④	人員を採用する際、被雇用者に対し情報セキュリティに関する役割及び責任を明示すること。		6.1.4	雇用条件　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が望ましい。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が望ましい。従業員がセキュリティ要求事項を無視した場合にとる措置についてもここに含めることが望ましい。 例えば，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，並びにそれらを雇用条件に含めることが望ましい。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も，ここに含めることが望ましい。雇用条件には，適切な場合には常に，例えば，自宅での作業（7.2.5及び9.8.1参照）といった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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(13 / 79)

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
	(2) ユーザの教育・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，通常の仕事の中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。	生じ得るセキュリティリスクを最小とするために，セキュリティ手順及び情報処理設備の正しい使用方法を利用者に訓練することが望ましい。	
		① 情報セキュリティポリシーの対象者に対し、情報セキュリティポリシー及び関連する手順等に関する教育・訓練を定期的に実施すること。		6.2.1	情報セキュリティの教育及び訓練　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すること，並びに定期的に更新教育を行うことが望ましい。これには，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）に関する訓練が含まれる。
	(3) セキュリティ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。	セキュリティに影響を及ぼす事件・事故は，適切な連絡経路をとおして，できるだけ速やかに報告することが望ましい。 すべての従業員及び請負業者に，組織の資産のセキュリティに影響を及ぼすおそれのある種々の形態の事件・事故（セキュリティ違反，脅威，弱点又は誤動作）についての報告手順を認識させておくことが望ましい。すべ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もった場合には，指定された連絡先にできるだけ速やかに報告するよう要求することが望ましい。組織は，セキュリティ違反を犯した従業員に適用する正式な懲罰手続を確立することが望ましい。事件・事故を適切に取り扱うためには，事件・事故の発生後できるだけ速やかに証拠を収集する必要があるかもしれない（12.1.7参照）。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(14 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	発見したセキュリティ事故を迅速に報告するため、経営陣を含めた連絡網を設置すること。		6.3.1	セキュリティ事件・事故の報告　セキュリティ事件・事故は，適切な連絡経路をとおして，できるだけ速やかに報告することが望ましい。 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し，その報告を受けたならば直ちに取るべき措置に着手できることが望ましい。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，及びそのような事件・事故をできるだけ速やかに報告するよう要求することが望ましい。事件・事故の処理が落着した後で，その報告された事件・事故の結果を知らせることを確実にするために，適切なフィードバックの手続を構築していることが望ましい。このような事件・事故は，利用者に対する認識訓練（6.2参照）において，何が起こるか，どう対処するか，及び今後の発生をどう回避するかの参考例として使用することが可能である（12.1.7参照）。
		②	セキュリティ事故やそれに準ずる出来事を発見した場合の報告義務を、その義務を有する者に対し周知徹底すること。		6.3.2	セキュリティの弱点の報告　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に，情報サービスの利用者に対して，注意を払い，かつ，報告するよう要求することが望ましい。利用者は，これらの事柄を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が望ましい。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が望ましい。これは，利用者自身を守るためである。というのも，弱点を調査することは，システムの不正使用の企てと見なされることがあり得るからである。
		③	ソフトウェアが誤動作した場合の報告手順を定めること。		6.3.3	ソフトウェアの誤動作の報告　ソフトウェア誤動作を報告する手順を確立することが望ましい。その場合，次の行動を考慮することが望ましい。 a) 問題の兆候及び画面に現れるメッセージに注意することが望ましい。 b) 可能ならばコンピュータを隔離すること，及びその使用を停止することが望ましい。適切な関係先に対して直ちに警報を発することが望ましい。もし装置を検査するつもりならば，電源を再投入する前に，組織のすべてのネットワークとの接続を断つことが望ましい。ディスケットを，別のコンピュータに移さないことが望ましい。 c) このような事柄について，情報セキュリティ管理者に直ちに報告することが望ましい。 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が望ましい。回復処置は，適切に訓練され，かつ，経験を積んだ職員が実施することが望ましい。
		④	発見したセキュリティ事故や誤動作の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にすること。また、その結果を組織の情報セキュリティに反映させる態勢を整えること。		6.3.4	事件・事故からの学習　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が望ましい。この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が望ましい。このことから，将来に発生する頻度，損害及び費用を抑えるための，又はセキュリティ基本方針の見直し過程で当然考慮される，管理策の強化又は追加の必要性が示されることもある（8.1.2参照）。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(15 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	情報セキュリティポリシー及び関連する手順に違反した場合の処置は、正式な懲戒プロセスに従うこと。		6.3.5	懲戒手続　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が望ましい（6.1.4，及び証拠の保存については12.1.7参照）。このような手続は，別の方法ではセキュリティ手順を軽視する傾向のある従業員に対して抑止力として作用することもある。更に，この懲戒手続は，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が望ましい。
5. 物理的及び環境的セキュリティ						
	(1) セキュリティ区画			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。	取扱いに慎重を要する又は重要な業務の情報処理設備は，適切なセキュリティ障壁及び入退の管理を伴う，明確なセキュリティ境界によって保護された領域の中に設置することが望ましい。これら設備を，認可されていないアクセス，損傷及び妨害から，物理的に保護することが望ましい。 講じる保護の程度は，識別されたリスクに対応したものであることが望ましい。書類，媒体及び情報処理設備に対する，認可されていないアクセス又は損傷のリスクを軽減するためには，クリアデスク及びクリアスクリーンの個別方針の設定が推奨される。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(16 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	情報処理施設及び設備は、他の区画と明確に分離したセキュリティ区画に設置され、適切に保護されること。		7.1.1	物理的セキュリティ境界　物理的保護は，業務施設及び情報処理設備の周囲に幾つかの物理的障壁を設けることで達成することができる。障壁はそれぞれが一つのセキュリティ境界となり，それによって全体の保護が強化される。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が望ましい（7.1.3参照）。セキュリティ境界とは，例えば，外壁，カードで制御した入口，又は有人の受付といった障壁を形成するものをいう。各障壁の設置位置及び強度は，リスクアセスメントの結果に依存する。 次の指針及び管理策を検討し，適切に実施することが望ましい。 a) セキュリティ境界を明確に定義することが望ましい。 b) 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が望ましい（すなわち，境界には間げきがない又は容易に侵入できる領域がないことが望ましい）。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が望ましい。 c) 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が望ましい。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が望ましい。 d) 物理的な壁は，認可されていない立入り，並びに火災及び洪水が引き起こす環境への悪影響を防止するために，必要ならば，床から天井にわたる構造で設けることが望ましい。 e) 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が望ましい。
		②	セキュリティ区画は、許可されない者がアクセスできないよう入退管理されること。		7.1.2	物理的入退管理策　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が望ましい。次の管理策を考慮することが望ましい。 a) セキュリティが保たれた領域への訪問者を監視し又は立入り許可を求めさせること，及びその入退の日付・時刻を記録することが望ましい。その訪問者には，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，並びに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が望ましい。 b) 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して，認可された者だけに制限することが望ましい。アクセスをすべて認可して，妥当性を確認するために，例えば，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が望ましい。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が望ましい。 c) 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，並びに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が望ましい。 d) 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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(17 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	セキュリティ区画は、特別な管理を要求される作業場所や施設を保護する目的で建設されること。		7.1.3	オフィス，部屋及び施設のセキュリティ セキュリティが保たれた領域は，施錠されたオフィス，又は物理的セキュリティ境界の内側の幾つかの部屋であってよく，その部屋には施錠することがあり，その内部に施錠可能な保管庫又は金庫を設置することもある。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，騒じょう，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が望ましい。関連する健康及び安全に関する規則並びに標準類も考慮に入れることが望ましい。また，例えば，他の領域からの漏水といった，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が望ましい。 次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 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，さらに，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が望ましい。 c) 例えば，複写機，ファクシミリといった支援機能及び装置は，情報漏えい(洩)などをもたらすおそれがあるアクセスを避けるために，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が望ましい。 d) 要員が不在のときは扉及び窓に施錠することが望ましい。特に一階の窓については，外部に対する防御を考慮することが望ましい。 e) すべての外部扉及びアクセス可能な窓を遮へいするためには，専門の標準類に従って取り付けられ，かつ，定期的に点検する，適切な侵入者の検知システムを設置することが望ましい。無人の領域には常に警報装置を稼働させることが望ましい。例えば，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，このような仕組みを設置することが望ましい。 f) 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が望ましい。 g) 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が望ましい。 h) 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が望ましい。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が望ましい。 i) 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，主事業所で起きた災害によって損傷しないように，主事業所から十分に離れた場所に置くことが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(18 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	セキュリティ区画において作業をするために必要な措置を講じ、ガイドラインを整備すること。		7.1.4	セキュリティが保たれた領域での作業　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，管理策及び指針の追加が必要になることもある。これには，セキュリティが保たれた領域において部外者が行う作業に関するものだけでなく，そこで作業する要員又は部外者そのものについての管理策が含まれる。次の管理策を考慮することが望ましい。 a) 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，知る必要がある要員だけに知らせるという基本に沿って，その必要がある要員だけが知っていることが望ましい。 b) 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，安全のため及び悪意のある行動を防ぐために，避けることが望ましい。 c) 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，及び定期的に検査することが望ましい。 d) 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が望ましい。このアクセスは認可のもとにおくこと，及び監視下におくことが望ましい。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が必要な場合がある。 e) 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，許さないことが望ましい。
		⑤	納品及び積荷場所は、許可されないアクセスを避けるため管理され、情報処理施設及び設備から分離されること。		7.1.5	受渡し場所の隔離　品物を受渡しする場所については管理を行い，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が望ましい。このような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が望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 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，設計を行うことが望ましい。 c) 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が望ましい。 d) 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[7.2.1 d）参照]がないかどうか，その品物を検査することが望ましい。 e) 敷地内に搬入するときには，適切ならば 5.1参照），搬入品の登録を行うことが望ましい。

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
	⑵ 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。	装置は，セキュリティに対する脅威及び環境上の危険から物理的に保護することが望ましい。 装置（この中には，事業施設外で用いられるものも含まれる。）の保護は，データに対する認可されていないアクセスのリスクを軽減し，損失又は損傷を防止するために必要である。装置の保護に関しては，装置の設置場所及び処分についても考慮することが望ましい。危険又は認可されていないアクセスから保護するため，また，補助設備（例えば，電源，及びケーブル配線用施設）を保護するために，特別な管理策が要求されることもある。	
		①	装置の設置場所における環境上の脅威を軽減するための措置を講ずること。		7.2.1	装置の設置及び保護　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又は保護することが望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 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が望ましい。 c) 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が望ましい。 d) 脅威からのリスクを最小限に抑えるための管理策を採用することが望ましい。考えられる脅威には，次のものが含まれる。 1) 窃盗 2) 火災 3) 爆発物 4) 煙 5) 水（又は供給不能） 6) ほこり 7) 振動 8) 化学物質の影響 9) 電源の障害 10) 電磁放射線 e) 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が望ましい。 f) 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が望ましい。 g) 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が望ましい。 h) 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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(20 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	装置を許可されないアクセスから保護すること。			同上
		③	装置を停電やその他の電源異常から保護すること。		7.2.2	電源　装置は，停電，その他の電源異常から保護することが望ましい。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が望ましい。 　電力の供給を途切れさせないための選択には次のものがある。 a) 電力の供給が一つの障害で停止することを避けるための，電源の多重化 b) 無停電電源装置（UPS）の設置 c) 非常用発電機の設置 　連続運転又は定められた手順での運転停止を可能にするために，重要な業務活動を支援する装置に対しては，UPSの設置が推奨される。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が望ましい。UPSは，容量が十分であることを定期的に確認し，製造者の推奨に従って点検することが望ましい。 　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が望ましい。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が望ましい。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が望ましい。さらに，非常時に即座に電源を切ることができるように，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が望ましい。主電源の停電時用として非常用照明を備えることが望ましい。落雷防護はすべての建物に備えることが望ましく，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が望ましい。
		④	データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。		7.2.3	ケーブル配線のセキュリティ　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が望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b)電線管を使用すること又は公衆域を経由する配線経路を避けることなどによって，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が望ましい。 c) 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が望ましい。 d) 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，更に次のような管理策を追加することを考慮する。 1) 外装電線管の導入，及び点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置。 2) 代替経路又は伝送媒体の使用。 3) 光ファイバケーブルの使用。 4) 認可されていない装置がケーブルに取付けられているかどうかについての調査の実施。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(21 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	装置を使用する際、装置製造業者が提供する取扱い説明書や手順書に従い、装置の可用性及び完全性を確実に維持すること。		7.2.4	装置の保守　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が望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 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が望ましい。 c) 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し，保管することが望ましい。 d) 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が望ましい（削除，消去及び上書きされたデータに関しては，7.2.6参照）。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が望ましい。
		⑥	装置を組織の敷地外で利用する際、適切に保護するための手順を定め、必要な措置を講ずること。		7.2.5	事業敷地外における装置のセキュリティ　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が望ましい。実施するセキュリティは，同じ目的のために使用する事業所内の装置に対するものと同等であり，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が望ましい。情報処理装置には，在宅作業のために保有しているか，又は通常の作業場所からもち出した，パーソナルコンピュータ，周辺機器，移動電話，紙，又はその他のあらゆるものが含まれる。次の指針を考慮することが望ましい。 a) 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が望ましい。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が望ましい。 b) 装置の保護に関しては，例えば，強力な電磁場にはさらさないといった，製造者の指示に常に従うことが望ましい。 c) 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が望ましい。状況に応じ，適切な管理策（例えば，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）を適用することが望ましい。 d) 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が望ましい。 セキュリティリスク，例えば，損傷，盗難，傍受は，場所によって異なる。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が望ましい。移動装置を保護するための情報は9.8.1による。
		⑦	装置を処分あるいは再利用する際、装置に格納された情報を事前に消去すること。		7.2.6	装置の安全な処分又は再使用　情報は，装置の不注意な処分又は再使用によって危険にさらされる（8.6.4参照）。取扱いに慎重を要する情報を保持する記憶装置は，標準の削除機能を用いるよりも物理的に破壊するか，又は確実に上書きするほうが望ましい。 例えば，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し，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が望ましい。取扱いに慎重を要するデータを保存した記憶装置が損傷した場合に，それらの装置を破壊，修理，又は廃棄処分のいずれにすべきか判定するためのリスクアセスメントが必要となることもある。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(22 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
	(3) 一般管理策			情報及び情報処理設備の損傷又は盗難を防止するため。	情報及び情報処理設備は，認可されていない者への露呈，それらの者による変更又は盗難から保護することが望ましく，損失又は損害を最小限に抑えるために，管理策を適切に実施することが望ましい。取扱い及び保管の手順は8.6.3でとりあげる。	
		①	離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。		7.3.1	クリアデスク及びクリアスクリーンの個別方針　組織は，通常の勤務時間内及び時間外の情報への認可されていないアクセス，情報の消失及び損傷のリスクを軽減するために，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が望ましい。この個別方針において，情報セキュリティの分類（5.2参照），その分類に対応するリスク，及び組織の文化的側面を考慮することが望ましい。 机上に放置された情報は，火災，洪水又は爆発といった災害時に損傷又は破壊されやすい。 次の管理策を考慮することが望ましい。 a) 適切ならば，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及び/又は他の形式の安全な収納庫内に保管することが望ましい。 b) 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（理想的には耐火金庫又は書庫に）保管しておくことが望ましい。 c) 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が望ましく，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が望ましい。 d) 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が望ましい。 e) 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）ことが望ましい。 f) 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が望ましい。
		②	離席時や帰宅時には、パスワードで保護されたスクリーンセーバの使用やログオフを徹底し、他人による情報システムへのアクセスを防止するための措置を講ずること。			同上
		③	組織が所有する装置や情報、ソフトウェア等を承認なしに組織外へ持ち出さないこと。		7.3.2	資産の移動　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が望ましい。必要，かつ，適切ならば，もち出し時及び返却時に記録を残すことが望ましい。認可されていない資産の移動が行われていないか，現場検査を実施することが望ましい。現場検査があることを各人が認識していることが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(23 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
6. 通信及び運用管理						
	(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。	すべての情報処理設備の管理・運用の責任及び手順を確立することが望ましい。これには，適切な操作指示及び事件・事故の対処手順の策定が含まれる。 不注意又は故意によりシステムを誤用するリスクを軽減するために，適切ならば，職務を分離（8.1.4参照）することが望ましい。	
		①	第3 (1)①(ｳ)にある管理目的及び管理策に従い特定した操作手順を文書化し維持すること。		8.1.1	操作手順書　セキュリティ個別方針によって明確化した操作手順は，文書化し維持していくことが望ましい。操作手順は，正式な文書として取り扱い，変更の場合は管理者によって認可されることが望ましい。 この手順には，次の項目を含む，各作業の詳細な実施に関する指示を明記することが望ましい。 a) 情報の処理及び取扱い。 b) スケジュール作成に関する要求事項。この中には他のシステムとの相互依存，最も早い作業の開始時刻，及び最も遅い作業の完了時刻を含む。 c) 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。この中には，システムユーティリティ（9.5.5参照）の使用の制限を含む。 d) 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。 e)特別な出力の取扱い（例えば，特殊な用紙の使用又は機密情報の出力の管理）に関する指示。この中には，失敗した作業出力の安全な処分手順を含む。 f) システムが故障した場合の再起動及び回復の手順。 情報処理・通信設備に関連するシステムの維持管理活動（例えば，コンピュータの起動・停止の手順，バックアップ，装置の保守，並びにコンピュータ室及びメールの取扱いの管理・安全）の手順書を作成することも望ましい。
		②	情報システムや情報処理施設等に対する変更を管理すること。		8.1.2	運用変更管理　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が望ましい。情報処理設備及びシステムの変更に対する不十分な管理は，システム又はセキュリティ障害の一般的な原因となる。装置，ソフトウェア又は手順に対する変更のすべてに対する十分な管理を確実にするために，正式な管理責任及び手順が定められていることが望ましい。運用プログラムは，厳重な変更管理の下に置くことが望ましい。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が望ましい。運用環境の変更は，業務用ソフトウェアに影響を及ぼすことがある。実行可能ならば，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，統合することが望ましい（10.5.1参照）。次の管理策を考慮することが望ましい。 a) 重要な変更の識別及び記録。 b) そのような変更の潜在的な影響の評価。 c) 変更の申出を正式に承認する手順。 d) 変更の詳細の，全関係者への通知。 e)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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(24 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	セキュリティ事故を管理する責任体制及び手順を定めること。		8.1.3	事件・事故管理手順　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が望ましい（6.3.1参照）。次の管理策を考慮することが望ましい。 a) すべてのタイプの潜在的セキュリティ事件・事故に対処できるように，手順を定めることが望ましい。この事件・事故には次のものを含む。 1) 情報システムの故障及びサービスの停止。 2) サービスの妨害（denial of service: DoS）。 3) 不完全又は不正確な業務データに起因する誤り。 4) 機密性に対する違反。 b) 通常の障害対策計画（システム又はサービスの回復をできるだけ速やかに行うように計画されたもの）に加え，この手順には，次の事項を含めることが望ましい（6.3.4参照）。 1) 事件・事故の原因の分析及び識別。 2) 必要ならば，再発を防止するための対策の計画及び実施。 3) 監査証跡及びこれに類する証拠の収集。 4) 事件・事故からの回復によって影響を受ける，又は事件・事故からの回復にかかわる人々への連絡。 5) 適切な監督機関に対する措置の報告。 c) 適切ならば，次の目的のために，監査証跡及びこれに類する証拠を収集し（12.1.7参照），安全に保管することが望ましい。 1) 内部問題の分析。 2) 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して関連して制定された法律に基づいたもの）での証拠としての使用。 3) ソフトウェア及びサービスの提供者との補償交渉。 d) 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が望ましい。手順は，次の事項を確実にするものであることが望ましい。 1) 身元分が明らかで，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（第三者アクセスについては，4.2.2参照）。 2) 実施したすべての非常措置は，文書に詳細を記録する。 3) 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。 4) 事業システム及び管理策の完全性を，早急に確認する。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(25 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	情報や情報サービスへの許可されない変更や誤用の機会を低減するため、職務の分離及び責任の範囲を明確にすること。		8.1.4	職務の分離　職務の分離は，不注意又は故意によるシステムの誤用のリスクを軽減する一つの手段である。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が望ましい。 　小さな組織では，この管理方法を実施することは難しいかもしれない。しかし，この原則は，実施可能な限り適用することが望ましい。このような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が望ましい。しかしながら，セキュリティ監査だけは，独立性を維持することが重要である。 　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が望ましい。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が望ましい。次の管理策を考慮することが望ましい。 a) 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，分離することが重要である。 b) 共謀のおそれがある場合は，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必要がある。それによって共謀の可能性は減少する。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(26 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	情報システムの開発及びテストの環境を運用施設及び設備から分離すること。		8.1.5	開発施設及び運用施設の分離　開発施設，試験施設及び運用施設を分離することは，それぞれが本来もつ役割を明確に分けるうえで重要である。ソフトウェアの開発から運用の段階への移行についての規則は，明確に定め，文書化することが望ましい。 開発作業及び試験作業は，重大な問題（例えば，ファイル又はシステム環境の好ましくない変更）又はシステム故障の問題を引き起こすことがある。運用上の問題を回避するために，運用環境，試験環境及び開発環境の間で必要となる分離の程度を考慮することが望ましい。同様な分離は，開発と試験との機能間でも実行することが望ましい。この場合，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必要がある。 開発担当者及び試験担当者が運用システム及びその情報にアクセスする場合，これらの担当者は，無認可及び無検査の命令文を挿入すること又は運用データを変更することができるかもしれない。システムによっては，この可能性は，不正行為を働いたり，未試験又は不正な命令文を挿入するために悪用されることもある。無検査又は不正な命令文は，重大な運用上の問題を引き起こすことがある。開発者及び試験者も，運用情報の機密性に脅威をもたらすことがある。 開発作業と試験作業とが，同じコンピュータの運用環境を利用している場合，ソフトウェア及び情報に意図しない変更を引き起こすことがある。したがって，運用ソフトウェア及び業務用データについての不注意による変更のリスク又は無認可のアクセスのリスクを軽減するために，開発施設，試験施設及び運用施設を分離することが望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 開発作業と試験作業とは，可能な限り分離することが望ましい。 c) 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が望ましい。 d) 運用システム及び試験システムに対しては，誤りのリスクを軽減するために，異なるログオン手順を用いることが望ましい。これらの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が望ましい。メニューには，適切な識別メッセージを表示することが望ましい。 e) 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が望ましい。管理策は，そのようなパスワードが使用後には変更されることを確実にすることが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(27 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑥	外部の施設管理サービスを利用する場合、リスクを考慮し適切な措置を決定した上で、この内容を明記した正式な契約を締結すること。		8.1.6	外部委託による施設管理　情報処理施設を管理するために外部の請負業者を利用することは，請負業者の事業所内におけるデータの信用低下，損傷又は喪失といった，セキュリティに影響を与える可能性をもたらすこともある。これらのリスクはあらかじめ識別し，そのうえで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が望ましい（組織の施設へのアクセスにかかわる第三者契約及び外部委託契約に関する指針については4.2.2及び4.3参照）。 　対処することが望ましい問題には，次のものが含まれる。 a) 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。 b) 業務用ソフトウェアの管理者からの承認取得。 c) 事業継続計画との関連性。 d) 指定すべきセキュリティ標準類及び適合性の測定手続。 e) 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。 f) 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（8.1.3参照）。
	(2) システム計画の作成及び受け入れ			システム故障のリスクを最小限に抑えるため。	十分な容量及び資源の可用性を確実にするためには，事前に計画及び準備を行う必要がある。 　システムの過負荷のリスクを軽減するために，将来の容量・能力の要求を予測することが望ましい。新しいシステムの運用上の要求事項を，その受入れ及び使用に先立って，設定し，文書化し，試験することが望ましい。	
		①	情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。		8.2.1	容量・能力の計画作成　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が望ましい。これらの予測では，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側される傾向を考慮することが望ましい。 　新しい容量・能力の確保には，多大の費用及び事前準備の期間が必要となるので，汎用大型コンピュータでは，特に注意が必要である。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が望ましい。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が望ましい。 　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おそ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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(28 / 79)

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
		② 情報システムを新規導入あるいは変更する際の受け入れ基準を確立し、情報システムの本番利用を容認する前に適切なテストを実施すること。		8.2.2	システムの受入れ　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が望ましい。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，明確に定義し，合意し，文書化し，試験することを確実にすることが望ましい。次の管理策を考慮することが望ましい。 a) 性能及びコンピュータの容量 能力の要求事項。 b) 誤りからの回復及び再起動の手順並びに障害対策計画。 c) 定められた標準類にのっとった通常の操作手順の準備及び確認。 d) 合意された適切なセキュリティ管理策。 e) 手動による有効な手順。 f) 11.1が要求する事業継続の取決め。 g)例えば，月末のような最大処理のときに，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。 h) 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。 i) 新しいシステムの運用又は使用に関する訓練。 　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が望ましい。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が望ましい。
	⑶ 不正ソフトウエアからの保護		ソフトウェア及び情報の完全性を保護するため。	悪意のあるソフトウェアの侵入を防止し，検出するために予防の措置を行う必要がある。 　ソフトウェア及び情報処理設備は，コンピュータウイルス，ネットワークワーム，トロイの木馬（10.5.4参照）及びロジック爆弾といった悪意のあるソフトウェアの侵入を受けやすい。利用者には，無認可又は悪意のあるソフトウェアの危険を知らせることが望ましく，管理者は，適切ならば，それらのソフトウェアの侵入を検出し，防止するために，特別な管理策を導入することが望ましい。特に，パーソナルコンピュータのコンピュータウイルスを検出し，防止するための予防の措置は不可欠である。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(29 / 79)

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
		① 情報や情報システムを不正ソフトウェアから保護するための検出及び防止策を講じ、適宜ユーザの教育・訓練を実施すること。		8.3.1	悪意のあるソフトウェアに対する管理策　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が望ましい。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が望ましい。次の管理策を考慮することが望ましい。 a) 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（12.1.2.2参照）。 b) 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（10.5，10.5.4及び10.5.5参照）。 c)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。 d) 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。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が望ましい。 e) 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とお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。 f) 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。この検査は，様々な場所（例えば，電子メールサーバ，デスクトップコンピュータ又は組織のネットワークの入口）において実施してもよい。 g) 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，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（6.3及び8.1.3参照）。 h) ウイルス感染からの回復のための適切な事業継続計画。これには，すべての必要なデータ及びソフトウェアのバックアップ並びに回復の手順を含む（11. 参照）。 i) 悪意のあるソフトウェアに関するすべての情報を確認し，警告情報が正確，かつ，役立つことを確実にするための手順。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が望ましい。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が望ましい。 　これらの管理策は，多数の作業場所をつないでいるネットワークのファイルサーバにとって，特に重要である。
	(4) 情報システム管理		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。	合意されたバックアップ方針（11.1参照）の実施のための，日常作業としての手順を確立することが望ましい。それには，データのバックアップの取得及びそれからの迅速なデータ復元についての実地訓練，事象及び障害の記録，並びに適切ならば，装置環境に対する監視がある。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(30 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	重要な情報及びソフトウエアのバックアップコピーを定期的に取得すること。		8.4.1	情報のバックアップ　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，定期的に取得することが望ましい。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が望ましい。個々のシステムのバックアップ手段は，事業継続計画（11.参照）の要求事項を満たすことを確実にするために，定期的に検査することが望ましい。次の管理策を考慮することが望ましい。 a) 最少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が望ましい。重要な業務用ソフトウェアについては，少なくとも三世代又は三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が望ましい。 b) バックアップには，主事業所で適用される標準に従って，適切なレベルの物理的及び環境的保護（7. 参照）を施すことが望ましい。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が望ましい。 c) 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が望ましい。 d) 復元手順は，その手順が有効であること，及び回復のための運用手順で定められた時間内に完了できることを確実にするために，定期的に検査及び試験することが望ましい。 　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（12.1.3参照）も，また，決定しておくことが望ましい。
		②	情報システムの操作担当者の作業履歴を記録すること。		8.4.2	運用の記録　運用担当者は，自分の作業の記録を継続することが望ましい。記録には，次の事項を状況に応じて含めることが望ましい。 a) システムの起動及び終了の時刻。 b) システム誤り及び実施した是正処置。 c) 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。 d) 記録の作成者の名前。 　運用担当者の記録は，操作手順に照らして，定期的に独立した検査を受けることが望ましい。
		③	障害が報告された情報システムを確実に修正すること。		8.4.3	障害記録　障害については報告を行い，是正処置をとることが望ましい。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，記録することが望ましい。報告された障害の取扱いについては，次のことを含め，明確な規定があることが望ましい。 a) 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。 b) 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。
	⑸ 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。	組織の境界を超えて広がることもあるネットワークのセキュリティ管理には，注意が必要である。 公衆ネットワークを通過するデータで，取扱いに慎重を要するものについては，その保護に，追加の管理策が要求されることもある。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(31 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	ネットワークにおけるセキュリティを確保し維持するための措置を講ずること。		8.5.1	ネットワーク管理策　コンピュータネットワークにおけるセキュリティを実現し，かつ，維持するためには，一連の管理策が要求される。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，及び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ために，管理策を実施することが望ましい。特に，次の管理策を考慮することが望ましい。 a) 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，分離することが望ましい（8.1.4参照）。 b) 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が望ましい。 c) 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が望ましい（9.4及び10.3参照）。ネットワークサービスの可用性及びネットワークに接続したコンピュータの可用性を維持するために，さらに，特別な管理策が要求されることもある。 d) 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が望ましい。
	(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。	媒体を管理し，かつ，物理的に保護することが望ましい。 文書，コンピュータの媒体（テープ，ディスク，カセット），入力データ，出力データ及びシステムに関する文書を，損傷，盗難及び無認可のアクセスから保護するために，適切な運用手順を確立することが望ましい。	
		①	テープ、ディスク、カセット等の移動可能な記憶媒体や書類等を適切に管理すること。		8.6.1	コンピュータの取外し可能な付属媒体の管理　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が望ましい。次の管理策を考慮することが望ましい。 a) 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が望ましい。 b) 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が望ましく，そのような措置のすべてについて，監査証跡維持のための記録を保管することが望ましい（8.7.2参照）。 c) 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が望ましい。 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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(32 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	不要になった媒体を処分する際、情報漏洩を防止するための措置を講ずること。		8.6.2	媒体の処分　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が望ましい。媒体の不注意な処分によって，取扱いに慎重を要する情報が，外部の人間に漏れることがある。このようなリスクを最小限に抑えるために，媒体の安全な処分のための，正式な手順を確立することが望ましい。次の管理策を考慮することが望ましい。 a) 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，確実に保管し，さらに，安全，かつ，確実に処分（例えば，焼却，破砕）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が望ましい。 b) 安全な処分が必要と思われるものを次に掲げる。 1) 紙による文書。 2) 音声又は他の録音。 3) カーボン紙。 4) 出力した報告書。 5) 使い捨てのプリンタリボン。 6) 磁気テープ。 7) 持ち運び可能なディスク又はカセット。 8) 光学式記憶媒体（すべての製造業者のソフトウェア配布媒体を含む，あらゆる形式のもの）。 9) プログラムリスト。 10) 試験データ。 11) システムに関する文書。 c) 取扱いに慎重を要する媒体類を選び出そうとするよりも，すべての媒体類を集めて，確実に処分する方が簡単な場合もある。 d) 多くの業者が，書類，装置及び媒体の回収及び処分を行うサービスを提供している。十分な管理及び経験がある契約先を選定するために，注意を払うことが望ましい。 e) 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が望ましい。 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が望ましい。集積することによって，少量の機密情報よりも，機密ではないがまとまった量の情報の方に，より慎重な取扱いが必要になることがある。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(33 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	情報の、許可されない開示及び改ざん、誤用等を防止するため、媒体の取扱い及び保管に関する手順を定めること。		8.6.3	情報の取扱い手順　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が望ましい。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（mobilecomputing），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（5.2参照）に対応させて策定することが望ましい。次の管理策を考慮することが望ましい（5.2及び8.7.2参照）。 a) すべての媒体の取扱い及びラベル付け［8.7.2 a）参照］。 b) 認可されていない者を識別するためのアクセス制限。 c) 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。 d) 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。 e) 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。 f) 製造者の仕様書に適合した環境での媒体の保管。 g) データの配布先を最小限にすること。 h) 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。 i) 配布先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。
		④	情報システムに関するドキュメントを許可されないアクセスから保護すること。		8.6.4	システムに関する文書のセキュリティ　システムに関する文書には，取扱いに慎重を要する一連の情報［例えば，業務手続，諸手順，データ構造，及び認可手続（9.1参照）に関する記述］が含まれる。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ために，次の管理策を考慮することが望ましい。 a) システムに関する文書は，安全に保管することが望ましい。 b) 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，当該業務の管理者によって認可されることが望ましい。 c)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が望ましい。
	(7) 組織間における情報及びソフトウエアの交換			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。	組織間での情報及びソフトウェアの交換を管理すること，及び関連する法規に適合させることが望ましい（12. 参照）。 交換は，合意に基づいて実施することが望ましい。配送中の情報及び媒体を保護するための手順及び標準類を制定することが望ましい。電子データ交換，電子商取引及び電子メールに関連した業務とセキュリティとの関係及びそれらに関する管理策への要求事項を考慮することが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(34 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	取引先や協業相手等と情報を交換する場合、必要に応じて情報交換の実施に関する正式な契約を締結すること。		8.7.1	情報及びソフトウェアの交換契約　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[適切な場合には，ソフトウェア預託（escrow）条項も含むもの]を取り交わすことが望ましい。こ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が望ましい。セキュリティ条件にかかわる合意では次のことを考慮することが望ましい。 a) 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。 b) 送り主，送信，発送及び受領を通知する手順。 c) 梱包及び送信に関する必要最小限の技術標準。 d) 配送者の身分を確認する標準。 e) データが紛失したときの責任及び保証。 f) 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。それによって，ラベルの意味が直ちに理解され，かつ，情報を適切に保護することを確実にする。 g) 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（12.1.2及び12.1.4参照）。 h) 情報・ソフトウェアの記録及び読出しに関する技術標準。 i)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（10.3.5参照）。
		②	移送中の媒体を許可されないアクセス、誤用及び改ざんから保護すること。		8.7.2	配送中の媒体のセキュリティ　情報は，物理的な配送（例えば，郵便又は宅配便による媒体の送付）の途中で，認可されていないアクセス，誤用又は改ざんに対する弱点をさらすことがある。事業所間で配送されるコンピュータ媒体を保護するために，次の管理策を適用することが望ましい。 a) 信頼できる輸送機関又は宅配業者を用いることが望ましい。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，及び宅配業者の身分を確認する手順を導入することが望ましい。 b) 梱包を，配送途中に生じるかもし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，及び製造者の仕様に従うことが望ましい。 c) 取扱いに慎重を要する情報を認可されていない露呈又は改ざんから保護するために，必要ならば，特別な管理策を採用することが望ましい。例として，次のようなものがある。 1) 施錠されたコンテナの使用。 2) 手渡し。 3) 開封防止包装（開封しようとした場合，その証拠が残る）の利用。 4) 特別な場合には，貨物を複数に分け，異なる経路での配送。 5) ディジタル署名及び秘匿のための暗号の使用(10.3 参照)。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(35 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	電子取引を行う場合、詐欺行為、契約紛争、情報の許可されない開示及び改ざんを防止するための措置を講ずること。		8.7.3	電子商取引のセキュリティ　電子商取引には，電子データ交換（EDI）の利用，電子メールの利用，及びインターネットのような公衆ネットワークを通したオンライン取引の利用が含まれる。電子商取引は，不正行為，契約紛争，及び情報の露呈又は改ざんという結果をもたらすおそれがある，ネットワーク上の多くの脅威にさらされている。電子商取引をそのような脅威から保護するために，管理策を適用することが望ましい。電子商取引に関するセキュリティの考慮事項には，次の管理策を含むことが望ましい。 a) 認証。買手及び売手は，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。 b) 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。 c) 契約及びその申込手続。重要な文書の機密性，完全性及び発送・受領の証明についての要求事項は何か。契約事項の否認防止に関する要求事項は何か。 d) 価格情報。公表された価格表の完全性，及び取扱いに慎重を要する割引に関する協定の機密性にどの程度の信頼をおけるか。 e) 注文取引。注文，支払並びに納入先の宛名情報についての機密性及び完全性はどのように確保されるか。受領の確認はどのように確保されるか。 f) 審査。買手が提供する支払情報を確認するために，どの程度の審査が適当か。 g) 決済。不正行為を防ぐための最も適切な支払方法は何か。 h) 注文。注文情報の機密性及び完全性を維持するために，どのような保護が必要か。受注の漏れ又は重複した受注を防止するために，どのような保護が必要か。 i) 責任。不正な取引に対するリスクは誰が負うのか。 　これらの考慮事項の多くは，法的要求事項への適合を考慮に入れながら，10.3に示す暗号技術を適用することによって対処することができる（12.1，暗号に関連した法令については12.1.6参照）。 　電子商取引に関する当事者間の合意は，権限［上記b）参照］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が望ましい。これとは別に，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，合意を交わすことが必要かもしれない。 　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が望ましい。 　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，考慮することが望ましい（9.4.7参照）。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(36 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	電子メールの使用に関するポリシーを定め、電子メールの使用により発生しうるリスクを軽減するための措置を講ずること。		8.7.4 8.7.4.1と8.7.4.2	電子メールのセキュリティ セキュリティリスク　電子メールは，業務上の通信手段に使用されており，テレックス及び手紙といった従来の通信方式に置き代わりつつある。電子メールには，従来の業務通信の方式と異なる点がある[例えば，速さ，メッセージ構造，文書の略式，及び認可されていない行為に対するぜい(脆)弱性]。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が望ましい。セキュリティ上のリスクには，次のようなものがある。 a)メッセージへの認可されていないアクセス若しくは改ざん，又はサービスの妨害（denial of service）にかかるぜい(脆)弱性。 b)誤り（例えば，不正確な宛先，間違った宛先）にかかるぜい（脆）弱性，及びサービスの一般的信頼性と可用性とにかかるぜい(脆)弱性。 c) 通信手段の変更の，業務手続に対する影響（例えば，送信速度の高速化，又は会社間よりも，むしろ個人間でやりとりされるメッセージが公式なものとして送られることの影響など）。 d) 法的な考慮事項（例えば，作成，発信，配信及び受信に関する証拠の必要性）。 e) 外部からアクセスできる職員の名簿を公表することの問題。 f) 遠隔地の利用者からの電子メールアカウントへのアクセス管理。 電子メールについての個別方針　組織は，電子メールの使用に関して，次のことを含めた明確な個別方針を作成することが望ましい。 a) 電子メールに対する攻撃（例えば，ウイルス，傍受）。 b) 電子メールの添付ファイルの保護。 c) 電子メールを使うべきでないときに関する指針。 d) 会社の信用を傷つけるおそれのある行為（例えば，中傷的な電子メールの送信，いやがらせのための使用，認可されていない物品の購入）に対する従業員の責任。 e) 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（10.3参照）。 f) 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。 g) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(37 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	電子機器の使用に関するポリシー及びガイドラインを定め、電子機器の使用に関連したリスクを抑制すること。		8.7.5	電子オフィスシステムのセキュリティ　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，導入することが望ましい。電子オフィスシステムによって，業務情報はより迅速に広まり，共有される機会をもつ。電子オフィスシステムでは，文書，コンピュータ，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，及びファクシミリが組み合わせて用いられる。 　このような設備を相互接続することにかかわるセキュリティ上及び業務上の問題について，次の事項を含めて考慮することが望ましい。 a) オフィスシステムにおける情報のぜい(脆)弱性（例えば，通話又は多者間通話の録音，通話の機密性，ファクシミリの保存，メールの開封，メールの配信）。 b) 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（例えば，会社の電子掲示板（9.1 参照）の使用）。 c)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（5.2参照）。 d)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。 e) 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。 f) 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（4.2参照）。 g) 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。 h) 利用者の地位の識別。例えば，他の利用者のために，組織の従業員又は名簿にある請負業者の従業員の地位の区別。 i) システムがもっている情報の保持及びバックアップ（12.1.3及び8.4.1参照）。 j) 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（11.1参照）。
		⑥	組織の情報を一般に公開し利用可能にする場合の正式な許可の手順を定めること。		8.7.6（後半）	公開している電子システムは，特に，それが情報のフィードバック及び直接入力を許すものである場合には，次のように，注意深く管理することが望ましい。 a) 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（12.1.4参照）。 b) 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。 c) 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。 d) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(38 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑦	組織の情報を一般に公開し利用可能にする場合、その情報を許可されない変更から保護すること。		8.7.6（前半）	公開されているシステム　情報を公開している組織は，その情報の改ざんによって評判が傷つくことがあるので，これを防止するために，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が望ましい。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必要があるかもしれない。情報を公開する前に，正式な認可の手続がとられることが望ましい。 　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，例えば，ディジタル署名といった適切な手段によって保護することが望ましい（10.3.3参照）。
		⑧	電話やファクシミリ、ビデオ通信等を使用して情報を交換する場合、その手順を定め、必要な措置を講ずること。		8.7.7	情報交換のその他の方式　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が望ましい。これらの設備を使用していることの認識の欠如又は個別方針若しくは適切な手順の欠如が，情報を脅かす原因となることがある（例えば，公衆の場での携帯電話の盗み聞き，留守番電話の盗み聞き，ダイヤルイン音声メールシステムへの認可されていないアクセス，間違った宛先へのファクシミリの送信）。 　通信設備が故障した場合，過負荷になった場合，又は妨害された場合（7.2及び11.参照）には，事業活動は混乱し，情報が脅かされる可能性がある。認可されていない利用者が通信設備にアクセスした場合にも（9.参照），情報が脅かされる可能性がある。 　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が望ましい。この文書には，次の事項を含むことが望ましい。 a) 適切な注意を払うことの必要を，職員に意識させること。例えば，取扱いに慎重を要する情報を漏らさないように，電話を使うときには，次の人々及び方法によって盗み聞き又は傍受されないために注意を払うようにする。 1)特に携帯電話を用いている場合，すぐ近くにいる人々。 2) 盗聴器，その他の電話機又は電話線への物理的アクセスによる方法。アナログ携帯電話を用いている場合には，走査受信機（scanning receiver）を用いる方法。 3) 通話先にいる人々。 b) 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。 c) 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おそれがあるので，メッセージを残さないようにさせること。 d) 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。具体的には，次のような危険性がある。 1) ファクシミリの，受信文の取出し装置への，認可されていないアクセス。 2) 特定の番号にメッセージを送る，故意又は偶然のプログラム。 3) 電話番号を間違ってダイヤルすること又は間違って記憶された番号を用いることによる，文書及びメッセージの送付。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(39 / 79)

2002/3/28

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
7. アクセス制御					
	(1) アクセス制御に関する事業の要求事項		情報へのアクセスを制御するため。	情報へのアクセス及び業務手続は，業務及びセキュリティの要求事項に基づいて管理することが望ましい。 この場合，情報を伝える範囲及びアクセスの認可に対する個別方針を考慮することが望ましい。	
		① 情報へのアクセス制御に関する事業上及びセキュリティ上の必要性を明確にし、それに従いアクセス制御ポリシーを定めること。		9.1.1 9.1.1.1	アクセス制御方針 個別方針及び業務上の要求事項　アクセス制御についての業務上の要求事項を定義し，文書化することが望ましい。利用者ごと又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及びアクセス権を，アクセス方針宣言書に明確に記述することが望ましい。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が望ましい。 この個別方針では，次の事項を考慮に入れることが望ましい。 a) 個々の業務用ソフトウェアのセキュリティ要求事項。 b) 業務用ソフトウェアにかかわるすべての情報の識別。 c) 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員の選定基準，情報のセキュリティ水準の設定基準，情報の分類基準）。 d) 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。 e) 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（12. 参照）。 f) 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。 g) 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。
		② 情報へのアクセスは、アクセス制御ポリシーに従い制限されること。		9.1.1.2	アクセス制御の規則　アクセス制御の規則を定める際は，次の事項に注意することが望ましい。 a) 常に遵守しなければならない規則と選択的又は条件付き規則とを区別する。 b) "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。 c) 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（5.2参照）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。 d) 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。 e) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(40 / 79)

ISMS認証基準（Ver. 1.0）		JIS X 5080		
		目的		内容
	(2) ユーザアクセス管理	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。	情報システム及びサービスへのアクセス権の割当てを管理するための正規の手続が整っていることが望ましい。 手続は，新しい利用者の初期登録から，情報システム及びサービスへのアクセスを必要としなくなった利用者の最終的な登録削除まで，利用者アクセスのライフサイクルにおけるすべての段階を対象とすることが望ましい。アクセスについての特権を与えると，システムでの管理策ではその利用者を制御することができなくなるので，適切ならば，アクセス特権の付与を管理する必要性について，特別の注意を払うことが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(41 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	情報システムユーザの登録及び登録抹消の手順を定めること。		9.2.1	利用者登録　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が望ましい。 　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が望ましい。この手続には，次の事項を含むとよい。 a) 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。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が望ましい。 b) 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。アクセス権について管理者から別の承認を受けることが適切な場合もある。 c) 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（9.1参照），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（8.1.4参照）に矛盾するおそれはないか]を検査する。 d) アクセス権の宣言書を利用者に発行する。 e) 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。 f) 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を，確実にする。 g) 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。 h) 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。 i) 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。 j) 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。 　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が望ましい（6.1.4及び6.3.5参照）。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(42 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	特権の割当て及び使用を制限し管理すること。		9.2.2	特権管理　特権 利用者をシステム又は業務用ソフトウェアの管理策に優先させることを可能とする，複数の利用者をもつ情報システムの特質又は機能)の割当て及び使用は，制限し，管理することが望ましい。システム特権の不適切な使用は，不正アクセスによるシステムの障害の主要因となっていることが多い。 　複数の利用者をもつシステムで，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あっては，正規の認可手続によって特権の割当てを管理することが望ましい。次の段階を考慮するとよい。 a) 各システム製品 例えば，オペレーティングシステム，データベース管理システム，各業務用ソフトウェア）に関連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が望ましい。 b) 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，割り当てることが望ましい。 c) 割り当てられたすべての特権の認可手続及び記録を維持することが望ましい。特権は，認可手続が完了するまで，許可しないことが望ましい。 d) 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が望ましい。 e) 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，割り当てることが望ましい。
		③	情報システムユーザに対するパスワードの割当ては、確立された管理プロセスに従い実施されること。		9.2.3	利用者のパスワードの管理　パスワードは，情報システム又はサービスにアクセスする利用者が本人であることを確認する一般的な手段である。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が望ましい。管理手続の取組方法は次の要求事項を満たすことが望ましい。 a) 個人のパスワードを秘密に保ち，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（これは採用条件に含めることもできる。6.4参照）。 b) 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。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が望ましい。 c) 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。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，避けることが望ましい。利用者は，パスワードの受領を知らせることが望ましい。 　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が望ましい（9.5.4参照）。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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(43 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	情報システムユーザのアクセス権を定期的に見直すこと。		9.2.4	利用者アクセス権の見直し　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が望ましい。この見直しは，次のように実施する。 a) 利用者のアクセス権を定期的に（6ヶ月間隔が推奨される。），また，何か変更があった後に見直す（9.2.1参照）。 b) 特権的アクセス権（9.2.2参照）の認可は，更に多い頻度で見直すことが望ましい。3ヶ月間隔が推奨される。 c) 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。
	(3) ユーザの責任			認可されていない利用者のアクセスを防止するため。	認可されている利用者間の協力は，有効なセキュリティのために不可欠である。 利用者に，有効なアクセス制御を維持する自分自身の責任を認識させることが望ましい。特にパスワードの使用及び利用者が利用する装置のセキュリティに関して，その責任を認識させることが望ましい。	
		①	パスワードを設定及び使用する際、情報セキュリティ上の問題を考慮すること。		9.3.1	パスワードの使用　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が望ましい。パスワードは，利用者が本人であることを確認する手段，ひいては，情報処理設備又はサービスへのアクセス権を確立するための手段となる。すべての利用者に，次の事項を実行するように助言することが望ましい。 a) パスワードを秘密にしておく。 b) パスワードを紙に記録して保管しない。ただし，記録がセキュリティを確保して保管される場合は，その限りではない。 c) 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。 d) 最短6文字の質のよいパスワードを選択する。質のよいパスワードとは，次の条件を満たす。 1) 覚えやすい。 2) 当人の関連情報（例えば，名前，電話番号，誕生日）から，他の者が容易に推測できる又は得られる事項に基づかない。 3) 連続した同一文字，又は数字だけ若しくはアルファベットだけの文字列でない。 e) 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し（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ことが望ましい。），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。 f) 仮のパスワードは，最初のログオン時点で変更する。 g) 自動ログオン処理にパスワードを含めない（例えば，マクロ又は機能キーにパスワードを記憶させない。）。 h) 個人用のパスワードを共有しない。 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よいパスワード［9.3.1d）参照］を用いてもよいことを助言することが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(44 / 79)

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
		② 装置を常時監視することが不可能な場合、当該装置を適切に保護するための措置を講ずること。		9.3.2	利用者領域にある無人運転の装置　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が望ましい。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必要とすることもある。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が望ましい。利用者は，次の事項を実行するように助言されることが望ましい。 a) 実行していた処理（session）が終わった時点で，接続を切る。ただし，適切なロック機構（例えば，パスワードによって保護されたスクリーンセーバ）によって保護されている場合は，その限りではない。 b) 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（すなわち，パーソナルコンピュータ又は端末の電源を切るだけで済ませない）。 c) 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。
	⑷ 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。	内部及び外部のネットワークを介したサービスへのアクセスは，制御されることが望ましい。 この制御は，ネットワーク及びネットワークサービスにアクセスする利用者が，これらのネットワークサービスのセキュリティを損なわないことを確実にするために必要である。この制御は，次の条件を確実にすることによって行う。 a) 組織のネットワークと他の組織が管理するネットワーク又は公衆ネットワークとの間の適切なインタフェース。 b) 利用者及び装置の適切な認証機構。 c) 情報サービスへの利用者アクセスの制御。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(45 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	明確に許可されたサービス以外のサービスへのアクセスを防止するための措置を講ずること。		9.4.1	ネットワークサービスの使用についての個別方針　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，組織全体に影響を及ぼすことがある。利用者には，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が望ましい。この制御は，取扱いに慎重を要する，若しくは重要な業務応用ソフトウェアへのネットワーク接続，又はリスクが高い場所（例えば，組織のセキュリティ管理及び制御の及ぶ範囲外の，公衆又は外部領域）にいる利用者への接続では，特に重要である。 　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が望ましい。この個別方針は，次の事項を対象とすることが望ましい。 a) 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。 b) 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。 c) 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。 　この個別方針は，業務上のアクセス制御方針（9.1参照）と整合していることが望ましい。
		②	情報システムのユーザがコンピュータの各サービスにアクセスする場合のネットワークの経路を制御すること。		9.4.2	指定された接続経路　利用者端末からコンピュータサービスまでの経路は，管理が必要となることがある。ネットワークは，資源の共有及び経路設定の柔軟性を最大限に許容するよう設計されている。一方で，このような特質は，業務応用ソフトウェアへの認可されていないアクセス，又は情報施設の認可されていない使用のおそれを招くことにもなる。このようなリスクは，利用者端末とその利用者がアクセスすることを認可されているコンピュータサービスとの間の経路を制限する管理策（例えば，接続経路の指定）を導入することによって，軽減することができる。 接続経路を指定する目的は，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である。 このためには，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が必要である。その選択の幅をあらかじめ定めることによって，ネットワークの各点における経路設定の選択肢を制限することがである。 この例を，次に示す。 a) 専用線又は専用電話番号を割り当てる。 b) 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。 c) 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。 d) ネットワーク上で無制限に探索（roaming）することを防止する。 e) 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。 f) 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。 g)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（Virtial 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（9.4.6参照）。 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（9.1参照）に基づくことが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(46 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	情報システムに対する遠隔地からのアクセスを許可する場合、ユーザ認証を行うこと。		9.4.3	外部から接続する利用者の認証　外部からの接続は，業務情報への認可されていないアクセスのおそれを生じる。例えば，ダイヤルアップ方法によるアクセスのような場合にこのようなおそれがある。したがって，遠隔地からの利用者のアクセスには，認証を行うことが望ましい。認証の方法には種々のものがあるが，その幾つかは，他のものより，保護レベルが高い。例えば，暗号技術を使用した方法は，保護レベルの高い認証である。リスクアセスメントに基づいて，要求される保護レベルを決めることが重要である。これは，認証方法の適切な選択に必要である。 遠隔地からの利用者の認証は，例えば，暗号に基づく技術，ハードウェアトークン，又はチャレンジ-レスポンス(challenge- response)プロトコルの方法を用いて，達成することができる。専用私設回線又はネットワークの利用者のアドレスを検査する機能をもったものでも，接続元の確認に使うことができる。 コールバックの手順及び制御（例えば，コールバックモデムの利用）は，認可されていない接続又は好ましくない接続から，組織の情報処理施設・設備を保護することができる。この種の制御は，遠隔地から組織のネットワークへ接続しようと試みる利用者を認証する。この制御を用いるとき，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が望ましく，そのような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が望ましい。コールバック処理には，組織側で確実に実際の回線を切断できることを含むことも重要である。そうできない場合，遠隔地の利用者が，コールバック確認がなされたふりをして，回線を開いたままにしておくおそれがある。このおそれに対して，コールバックの手順及び制御を徹底的に試験することが望ましい。
		④	遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。		9.4.4	ノードの認証　遠隔地のコンピュータへの自動接続のための設備は，業務用ソフトウェアへの認可されていないアクセスの手段を提供することになり得る。したがって，遠隔コンピュータシステムへの接続は，認証されることが望ましい。このことは，その接続が組織のセキュリティ管理外であるネットワークを用いる場合に，特に重要である。認証及びどのようにそれが達成されるかの幾つかの例を9.4.3に示す。 ノード(node)の認証は，遠隔地からセキュリティの保たれた共有コンピュータ設備に接続された（9.4.3参照）場合，一群の遠隔地の利用者を認証するための代替手段として用いることが可能である。
		⑤	診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。		9.4.5	遠隔診断用ポートの保護　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が望ましい。多くのコンピュータ及び通信システムには，保守のために，ダイヤルアップ遠隔診断設備が付属している。これらの診断ポートが保護されていない場合，認可されていないアクセスの手段となることもある。したがって，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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(47 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑥	情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。		9.4.6	ネットワークの領域分割　情報処理施設 設備又はネットワーク設備の相互接続，若しくは共有が必要となることもある業務上の協力関係の形成に伴って，ネットワークは従来の組織の境界を超えてますます広がっている。このような広がりは，ネットワークを使用する既存の情報システムへの認可されていないアクセスのリスクを増大することにもなる。そのネットワークの中には，慎重な取扱いの必要性又は重要性から，他のネットワーク利用者からの保護を必要とするものもある。このような状況においては，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が望ましい。 大規模なネットワークのセキュリティを制御する一つの方法は，このネットワークを幾つかの論理ネットワーク領域，例えば，組織の内部ネットワーク領域と外部ネットワーク領域とに分割し，分割した個々の領域を，明確に定められたセキュリティ境界によって保護することである。このような境界は，二つの領域間のアクセス及び情報の流れを制御するために，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を取り付けることによって実現することができる。このゲートウェイは，これらの領域間の通信をフィルタにかけ 9.4.7及び9.4.8参照），また，組織のアクセス制御方針（9.1参照）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が望ましい。この種のゲートウェイの一例としては，一般にファイアウォールと呼ばれるものがある。 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 9.1参照）に基づくことが望ましく，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が望ましい 9.4.7及び9.4.8参照）
		⑦	共有ネットワークへのアクセス権限は、第4 7(1)のアクセス制御ポリシーに従い付与されること。		9.4.7	ネットワークの接続制御　共有ネットワーク，特に，組織の境界を超えて広がっているネットワークについてのアクセス制御方針の要求事項では，利用者の接続の可能性を制限する制御策の組込みが必要とされることもある。このような制御策は，事前に定められた表又は規則によって通信をフィルタにかける，ネットワークゲートウェイによって実行することができる。適用される制限は，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が望ましく 9.1参照),それらに従って維持及び更新されることが望ましい。 制限を適用することが望ましい業務用ソフトウェアの例は，次のとおりである。 a) 電子メール b) 一方向のファイル転送 c) 双方向のファイル転送 d) 対話型アクセス e) 時間帯又は日付に対応したネットワークアクセス

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(48 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑧	共有ネットワークへのアクセスを許可する場合、第4 7(1)のアクセス制御ポリシーに基づき、可能な限り経路を制御すること。		9.4.8	ネットワーク経路を指定した制御　共用ネットワーク，特に，組織の境界を超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（9.1参照）に違反しないことを確実にするために，経路指定の制御策の組込みが必要なこともある。この制御は，第三者（外部組織）の利用者と共有されているネットワークでは多くの場合不可欠である。 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が望ましい。ネットワークアドレスの変換も，ネットワークを隔離し，一つの組織のネットワークから別の組織のネットワークへ経路が拡大するのを防止するために非常に役立つ機構である。これらの制御は，ソフトウェア又はハードウェアによって実施することができる。この実施者は，組み込まれた機構の強度を認識しておくことが望ましい。
		⑨	ネットワークに関連する外部のサービスを受ける場合、そのサービスに施されたセキュリティに関する情報を入手し、これを文書化すること。		9.4.9	ネットワークサービスのセキュリティ　公衆又は私設のネットワークサービスにはいろいろなものがあり，その中には，付加価値サービスを提供するものもある。ネットワークサービスは，独自の又は複雑なセキュリティ特性になっていることがある。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が望ましい。
	⑸ 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。	コンピュータ資源へのアクセスを制限するために，オペレーティングシステムレベルでセキュリティ設備を用いることが望ましい。これらの設備は，次の事柄を行う機能をもつことが望ましい。 a) 認可されている利用者本人であることの識別並びに確認，及び必要ならば，認可されている各利用者の端末又は所在地の識別並びに確認。 b) システムアクセスの成功及び失敗の記録。 c) 認証のための適切な手段の提供。パスワードの管理システムが用いられる場合，質のよいパスワードであることを確実にすることが望ましい［9.3.1d）参照］。 d) 適切ならば，利用者の接続時間の制限。 他のアクセス制御方法が，業務上のリスクに基づいて正当と判断されるならば，その制御方法[例えば，チャレンジ-レスポンス（challenge-response)]も用いることができる。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(49 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。		9.5.1	自動の端末識別　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が望ましい。自動の端末識別は，その処理（session）が特定の場所又はコンピュータ端末からだけ開始できることが重要である場合に使用することができる技術である。端末に内蔵されている又は端末に付与されている識別子は，この端末が特定の取引処理(transaction)を開始すること又は受け取ることを許可されているかを示すために用いることができる。端末識別子のセキュリティを維持するために，端末に物理的な保護を適用することが必要であるかもしれない。利用者の認証のために，その他種々の技術も用いることができる（9.4.3参照）。
		②	情報サービスへのログオンプロセスを明確にすること。		9.5.2	端末のログオン手順　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が望ましい。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おそれを最小限に抑えるように設計することが望ましい。したがって，ログオン手順では，認可されていない利用者に不要な助けを与えないために，システムについての情報の開示は最小限にすることが望ましい。適切なログオン手順としては，次の条件を満たすことが望ましい。 a) 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。 b) 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。 c) ログオン手順中に，認可されていない利用者の助けとなる表示をしない。 d) ログオン情報の妥当性検証は，すべての入力データが完了した時点でだけ行う。誤り条件が発生しても，システムからは，データのどの部分が正しいか又は間違っているかを指摘しない。 e) 許容されるログオンの試みの失敗回数を制限し（推奨は3回），次の事柄を考慮する。 1) 失敗した試みを記録すること。 2) 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，又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。 3) データリンク接続を切ること。 f) 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。この制限から外れる場合，システムはログオンを終了する。 g) ログオンが無事できた時点で，次の情報を表示する。 1) 前回ログオンが無事できた日時。 2) 前回のログオン以降，失敗したログオンの試みがある場合は，その詳細。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(50 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	情報システムユーザは、個人専用の識別子（ユーザID）を有すること。		9.5.3	利用者の識別及び認証　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）を保有することが望ましい。利用者IDには，利用者の特権レベル（9.2.2参照）[例えば，管理者(マネージャ)，監督者(スーパーバイザ)]を表示しないことが望ましい。 明らかに業務上の利点がある例外的状況においては，利用者のグループ又は特定の業務に対して，共有利用者IDを用いることができる。このような場合，管理者の承認を文書で得ることが望ましい。この責任体制を維持するために，追加の管理策が必要なこともある。 様々な認証手順があり，それらは，利用者が主張するIDを確証するために用いることができる。パスワード（9.3.1参照）は，利用者だけが知る秘密に基づき識別・認証を提供する非常に一般的な方法である。暗号手段及び認証プロトコルによっても同様のことが可能となる。 利用者が所有するメモリトークン又はスマートカードのようなものも識別・認証のために用いることができる。個人固有の特性又は属性を用いる生体認証技術も，個人のIDを認証するために用いることができる。セキュリティを保つための技術と機構との組合せによってもより高度な認証が可能となる。
		④	パスワード管理システムは、情報システムユーザに有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を制限すること。		9.5.4	パスワード管理システム　パスワードは，コンピュータサービスにアクセスする利用者権限を検証する主要な手段の一つである。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が望ましい（パスワードの使用に関する指針については，9.3.1参照）。 適用業務によっては，独立した機関によって割り当てられる利用者パスワードを要求する場合がある。しかし，ほとんどの場合，パスワードは，利用者によって選択され，維持される。 優れたパスワードの管理システムは，次の条件を満たすものである。 a) 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ようにする。 b) 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。 c) 9.3.1に示すような質のよいパスワードを選択させるようにする。 d) 利用者が自分のパスワードを維持管理する場合，9.3.1に示すようにパスワードを変更させるようにする。 e) 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（9.2.3参照）。 f) 以前の利用者パスワードの記録を，例えば，12か月間，維持し再使用を防止する。 g) パスワードは，入力時に，画面上に表示しないようにする。 h) 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。 i) 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。 j) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(51 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	システム設定プログラムの使用を制限し管理すること。		9.5.5	システムユーティリティの使用　ほとんどのコンピュータの実装では，システム及び業務用ソフトウェアの制御を無効にすることのできる一つ以上のシステムユーティリティプログラムが組み込まれている。それらの使用は制限され，厳しく管理されることが不可欠である。次の管理策を考慮するとよい。 a) システムユーティリティのための認証手順の使用。 b)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。 c) 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。 d) システムユーティリティを臨時に使用する際の認可。 e) システムユーティリティの使用の制限(例えば，認可された変更の期間での利用)。 f) システムユーティリティのすべての使用の記録。 g) 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。 h) 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。
		⑥	情報へのアクセスに際して、脅迫の対象となり得るユーザを保護するため、脅迫に対して警報を発信する機能を備えること。		9.5.6	利用者を保護するための脅迫に対する警報　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のが望ましい。そのような警報を備えるかどうかの決定は，リスクアセスメントの評価に基づくことが望ましい。この警報に対応する責任及び手順を明確に定めることが望ましい。
		⑦	取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末をシャットダウンすること。		9.5.7	端末のタイムアウト機能　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，認可されていない者によるアクセスを防止するために，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が望ましい。こ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ともに閉じるものであることが望ましい。タイムアウトまでの時間は，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が望ましい。 パーソナルコンピュータによっては，画面表示を消し，認可されていないアクセスを防止するような，端末のタイムアウト機能を限定された形で備えるものもあるが，これらは業務用ソフトウェア又はネットワーク接続を閉じる機能はない。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(52 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑧	リスクの高いアプリケーションシステムへの接続時間は、制限されること。		9.5.8	接続時間の制限　リスクの高い業務用ソフトウェアに対しては，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が望ましい。コンピュータサービスに対して許される端末の接続時間を制限すると，認可されていないアクセスのおそれも減少することになる。このような管理策は，取扱いに慎重を要するコンピュータの業務用ソフトウェア，特に，リスクの高い場所（例えば，組織のセキュリティ管理外の公共又は外部領域）にある端末上の業務用ソフトウェアについて考慮することが望ましい。 そのような制限の例には次の事柄が含まれる。 a）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。 b）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。
	⑹ アプリケーションシステムのアクセス制御			情報システムが保有する情報への認可されていないアクセスを防止するため。	業務用システム内でのアクセスを制限するために，セキュリティ機能を用いることが望ましい。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が望ましい。業務用システムは，次の条件を満たすことが望ましい。 a) 既定の業務上のアクセス制御方針に従って，情報及び業務用システム機能への利用者アクセスを制御する。 b) システム又は業務用ソフトウェアの制御を無効にできるユーティリティ及びオペレーティングシステムのソフトウェアについて，認可されていないアクセスから保護する。 c) 情報資源を共有している他の情報システムのセキュリティを脅かさない。 d) 管理者，他の認可された者，又は明確に定められた利用者グループに情報へのアクセスを許可する。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(53 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	情報及びアプリケーションシステムへのアクセスは、第4 7(1)のアクセス制御ポリシーに従い制限されること。		9.6.1	情報へのアクセス制限　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（9.1参照）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が望ましい。アクセス制限の要求事項を満たすために，次の制御策の適用を考慮することが望ましい。 a) 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を表示する。 b) 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。 c) 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。 d) 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。さらに，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。
		②	取扱いに慎重を要する情報システムは、隔離した環境に設置されること。		9.6.2	取扱いに慎重を要するシステムの隔離　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環境を必要とすることもある。ある種の業務用システムは，損失の可能性に対して十分に敏感でなければければならないから，特別な取扱いが必要となる。その度合いによって，その業務用システムは，専用のコンピュータで実行されることが望ましい場合もあり，信頼された業務用システムとの間でだけ資源を共有することが望ましい場合もある。一方では，この業務用システムに制限事項が全くないことが示される場合もある。次の考慮事項が適用される。 a) 業務用システムの取扱いに慎重を要する度合いは，業務用ソフトウェアの管理者（4.1.3参照）によって明確に識別され，文書化されることが望ましい。 b) 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が望ましい。
	(7) システムアクセス及びシステム使用の監視			認可されていない活動を検出するため。	アクセス制御方針からのずれを検出するため，及び，セキュリティ事件・事故の場合に証拠となるように監視可能な事象を記録するために，システムを監視することが望ましい。 システムの監視を行えば，採用されている管理策の有効性を検査することができ，また，アクセス方針モデル（9.1参照）に対する適合性を確認することができる。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(54 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。		9.7.1	事象の記録　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が望ましい。監査記録には，次の事項も含めることが望ましい。 a) 利用者 ID。 b) ログオン及びログオフの日時。 c) 可能ならば，端末の ID又は所在地。 d) システムへのアクセスを試みて，成功及び失敗した記録。 e) 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。 記録保存方針の一部として，又は証拠を集めるための要求事項から，ある種の監査記録を作成することが要求されることもある（12.参照）。
		②	情報処理施設及び設備の使用を監視するための手順を定めること。		9.7.2 9.7.2.1	システム使用状況の監視 リスクに関する範囲及び手順　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が望ましい。このような手順は，明確に認可された活動だけを利用者が実行することを確実にするために必要である。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が望ましい。考慮することが望ましい領域には，次の事柄が含まれる。 a) 次のような内容を含む，認可されているアクセス。 1) その利用者 ID。 2) その重要な事象の日時。 3) その事象のタイプ。 4) アクセスされたファイル。 5) 使用されたプログラム・ユーティリティ。 b) すべての特権操作。例えば， 1) 監督者アカウントの使用。 2) システムの起動及び停止。 3) 入出力装置の取付け・取外し。 c) 認可されていないアクセスの試み。例えば， 1) 失敗したアクセスの試み。 2) 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。 3) 侵入検知システムからの警告。 d) 次のようなシステム警告又は故障。 1) コンソール警告又はメッセージ。 2) システム記録例外事項。 3) ネットワーク管理警報。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(55 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	情報処理施設及び設備の監視活動の結果を定期的に検証すること。		9.7.2.2と9.7.2.3	リスク要因　監視の結果は，定期的に見直すことが望ましい。見直しの頻度は，関係するリスクによって決めることが望ましい。考慮すべきリスク要因には，次の事柄が含まれる。 a) 業務手続に与える重要性の度合い。 b) 関係ある情報の価値，取扱いに慎重を要する度合い又は重要性に関する度合い。 c) システムへの侵入及び誤用の過去の経験。 d) システム相互接続の範囲（特に，公衆ネットワーク）。 事象の記録及び検証　記録の検証は，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ことに役立つ。セキュリティ事件・事故の場合に更に調査を必要とする可能性がある事象の例は9.7.1に示す。多くの場合，システム記録は多量の情報を含んでいるが，そのうちの多くは，セキュリティのための監視に無関係である。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，及び／又は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が望ましい。 　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が望ましい。 　記録機能が不正に変えられるとセキュリティ上の誤った判断が生じるので，記録機能のセキュリティに対しては，特に注意することが望ましい。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が望ましい。これらの変更及び問題は，次のことを含む。 a) 記録機能を働かなくすること。 b) 記録されるメッセージの形式が変更されていること。 c) 記録ファイルが改ざんされ，又は削除されること。 d) 記録ファイルの媒体が満杯となり，その後の事象を記録できなくなるか，又はすでにある記録に上書きすること。
		④	すべての重要なコンピュータにおいて時刻設定を同期化すること。		9.7.3	コンピュータ内の時計の同期　監査記録は，調査のために，又は法律若しくは懲戒にかかわる場合の証拠として要求されることがあるので，コンピュータの時計の正しい設定は，監査記録の正確さを保証するために重要である。監査記録が正確でない場合，そのような調査を妨げ，またそのような証拠の信頼性を損なうことにもなる可能性がある。 　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]に合わせることが望ましい。コンピュータ内の時計は，時間の経過に伴って狂いが生じるので，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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(56 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
	(8) モバイルコンピューティング及び遠隔地勤務			移動型計算処理(mobile computing)及び遠隔作業(teleworking)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。	要求される保護は，これら特定の作業形態が引き起こすリスクに応じたものであることが望ましい。移動型計算処理を用いるとき，保護されていない環境における作業のリスクを考慮し，適切な保護を施すことが望ましい。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が望ましい。	
		①	モバイルコンピュータを用いる場合、リスクを考慮し、モバイルコンピュータ使用ポリシーを定めた上で必要な措置を講ずること。		9.8.1	移動型計算処理　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が望ましい。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が望ましい。このような個別方針には，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が望ましい。この個別方針には，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が望ましい。 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が望ましい。これらの設備に保管され，処理される情報への，認可されていないアクセスを回避し，これらの情報の漏えい(洩)を防止するため，保護は，暗号技術（10.3参照）のような管理策を用いて適切に行うことが望ましい。 移動型計算処理の設備を公共の場所で使用するとき，認可されていない者による盗み見のリスクを避けるように注意することは重要である。悪意のあるソフトウェアに対抗する手順が整っており，それは最新のものであることが望ましい（8.3参照）。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が望ましい。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が望ましい。 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が望ましい。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，実施されることが望ましい（9.4参照）。 移動型計算処理の設備も，盗難（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が望ましい。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が望ましい。さらに，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が望ましい。移動型の装置の物理的保護についての更に多くの情報を，7.2.5に示す。 この作業形態に起因する追加のリスク及びこれに対して実行すべき管理策について，移動型計算処理を用いる要員の意識を高めるために，この要員に対する訓練を計画することが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(57 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	遠隔地勤務を許可する場合、評価されたリスクに基づき、遠隔地勤務ポリシー及び手順を定めること。		9.8.2	遠隔作業　遠隔作業（teleworking)は，通信技術を用いて，要員が自分の所属する組織の外部の決まった場所から遠隔で作業ができるようにすることである。装置及び情報の盗難，認可されていない情報の漏えい(洩)，遠隔地から組織の内部システムへの認可されていないアクセス，設備の誤用などの脅威に対して，遠隔作業の場所に適切な保護が整っていることが望ましい。遠隔作業は，経営陣によって認可され，管理されることが重要であり，この作業形態のため適切に手配されていることが重要となる。 組織は，遠隔作業を管理するための個別方針，手順及び標準を策定することを考慮することが望ましい。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が望ましい。次の事柄を考慮することが望ましい。 a) 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。 b) 提案された遠隔作業の環境。 c) 遠隔作業の通信に関するセキュリティ要求事項。組織の内部システムへの遠隔アクセスの必要性，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い，及び内部システムの取扱いに慎重を要する度合いを考慮に入れた要求事項。 d) 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。 この考慮すべき管理策及び取決めには，次の事柄が含まれる。 a) 遠隔作業活動のための適切な装置及び保管棚・庫の準備。 b)許可される作業，作業時間，保持してもよい情報の分類，及び，遠隔作業者のアクセスが認可される内部システム・サービスの明確化。 c) 安全な遠隔アクセスを図る方法も含め，適切な通信装置の準備。 d) 遠隔作業を行う場所の物理的なセキュリティ。 e) 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。 f) ハードウェア及びソフトウェアの支援及び保守の規定。 g) バックアップ及び事業継続のための手順。 h) 監査及びセキュリティの監視。 i) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(58 / 79)

2002/3/28

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
8. システムの開発及びメンテナンス						
	(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。	これには，基盤，業務用ソフトウェア及び利用者開発型ソフトウェアが含まれる。適用業務又はサービスを支える業務工程の設計及びその実施は，セキュリティのために極めて影響が大きい。セキュリティ要求事項は，情報システムを開発する前に，認識され，合意されることが望ましい。 代替手段の配備の必要性も含めて，すべてのセキュリティ要求事項は，プロジェクトの要求事項の定義の段階で明確にして，正当化し，かつ，合意し，そして情報システムの作業全体の一環として，文書化することが望ましい。	
		①	情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要求事項を明確にすること。		10.1.1	セキュリティ要求事項の分析及び明示　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を記述した文書では，管理策についての要求事項を明記することが望ましい。このような記載事項では，システムに組み込まれるべき自動化された制御を考慮し，また，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が望ましい。業務用ソフトウェアのパッケージを評価するときにも，同様に考慮することが望ましい。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てもよい。 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が望ましい。また，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その要求事項及び管理策に反映されることが望ましい。セキュリティ要求事項を分析し，この要求事項を満たすための管理策を明確にするための枠組みが，リスクアセスメント及びリスクマネジメントである。 管理策は，設計段階で導入されれば，実行中又は実行後に組み込むよりも，実施及び維持の費用が著しく安く済む。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(59 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
	⑵ アプリケーション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。	管理策及び監査証跡，又は活動記録は，利用者開発型のソフトウェアを含め，業務用システムにおいて適切に設計されることが望ましい。これらには，入力データ，内部処理及び出力データの妥当性確認を含めることが望ましい。極めて慎重な取扱いを要する，貴重な，若しくは重要な組織の資産を処理するシステム，又はそれらに影響を及ぼすシステムには，更なる管理策が必要となることもある。そのような管理策は，セキュリティ要求事項及びリスクアセスメントに基づいて決めることが望ましい。	
		①	アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能を整備すること。		10.2.1	入力データの妥当性確認　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が望ましい。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，検査することが望ましい。次の管理策を考慮することが望ましい。 a) 次の誤りを検出するための二重入力又はその他の入力検査。 1) 範囲外の値。 2) データフィールド中の無効文字。 3) 入力漏れデータ又は不完全なデータ。 4) データ量の上限及び下限からの超過。 5) 認可されていない又は一貫しない制御データ。 b) そ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。 c) 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（入力文書に対する変更はすべて，認可を得ることが望ましい。）。 d) 妥当性確認の誤りに対応する手順。 e) 入力データのもっともらしさを試験する手順。 f) 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。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(60 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	アプリケーションシステムで処理されたデータに対する改ざんを検出する機能を備えること。		10.2.2 10.2.2.1と10.2.2.2	内部処理の管理 リスクにかかわる範囲　データは，正しく入力されていても，処理の誤り又は故意の行為によって改ざんされることがある。このような改ざんを検出するために妥当性の検査をシステムに組み込むことが望ましい。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が望ましい。考慮すべき範囲には，次の事項が含まれる。 a) 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。 b) 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（8.1.1参照）。 c) 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。 検査及び管理策　必要とされる管理策は，業務用ソフトウェアの性質及びデータ改ざんの業務への影響度によって異なる。システムに組込み可能な検査例には，次のようなものがある。 a) 取引処理(transaction)の更新後のデータファイルのバランスを取るための処理（session）又はバッチの制御。 b) 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とるための制御。すなわち， 1) 各実行処理の間の制御。 2) ファイルの更新の合計値。 3) 各プログラム間の制御。 c) システム生成データの妥当性確認（10.2.1参照）。 d) 中央のコンピュータと遠隔のコンピュータとの間で，ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査（10.3.3参照）。 e) レコード及びファイルの全体のハッシュ合計(hash totals)。 f) 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。 g) プログラムが正しい順序で実行され，故障の場合は終了すること，及び問題が解決するまでは処理が停止することを確実に実施しているかの検査。
		③	メッセージの完全性を保護する必要がある場合、メッセージが改ざんされていないことを確認する機能を備えること。		10.2.3	メッセージ認証　メッセージ認証は，伝送される電子メッセージの内容の認可されていない変更又は改ざんを検出するために用いられる技法である。この技法は，物理的なメッセージ認証装置又はアルゴリズムを保有する，ハードウェア又はソフトウェアによって実施される。 　メッセージ認証は，重要性の高いメッセージ内容（例えば，電子資金移動，仕様書，契約書，提案書，その他のこれに類似した電子データ交換）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，その適用を考慮することが望ましい。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アセスメントを行うことが望ましい。 　メッセージ認証は，メッセージの内容の漏えい(洩)を保護するためには設計されていない。暗号技術（10.3.2及び10.3.3参照）は，メッセージ認証を実施するための適切な手段として用いることができる。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(61 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。		10.2.4	出力データの妥当性確認 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が望ましい。一般的に，システムは，適切な妥当性確認，検証及び試験を受けて，常に正しい出力を出す前提で構築される。しかし，これは常にそうであるとは言えない。出力の妥当性確認には，次の事項が含まれる。 a) 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。 b) 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。 c) 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。 d) 出力の妥当性確認試験に対応する手順。 e) データ出力過程にかかわるすべての要員の責任の明確化。
	(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。	暗号システム及び暗号技術を，リスクがあると考えられる情報の保護，及び他の管理策では十分な保護が得られない情報の保護に用いることが望ましい。	
		①	情報を保護するために暗号を用いる場合、リスクを考慮し、暗号使用ポリシーを定めること。		10.3.1	暗号による管理策の使用に関する個別方針 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，リスクアセスメント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が望ましい。情報に施すべき保護のレベルを決めるには，リスクアセスメントを実施することが望ましい。このアセスメントは，さらに，暗号による管理策が適しているかどうか，どんなタイプの管理策を適用すべきか，また，何の目的で，どのような業務手続に適用すべきかを決めるために利用できる。 組織は，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が望ましい。この個別方針は，暗号技術を用いてその利益を最大化し，リスクを最小化するために必要であり，不適切な又は不正な利用を避けるためにも必要である。個別方針を定めるとき，次の事項を考慮することが望ましい。 a) 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。 b) 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。 c) 役割及び責任，例えば，次の事項に対する責任。 1) 個別方針の実施。 2) かぎ管理。 d) 暗号による適切な保護レベルをどのように決めるか。 e) 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（どの解決策をどの業務手続に用いるか）。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(62 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	取扱いに慎重を要する情報や重大な情報については、機密性を保護するため暗号化すること。		10.3.2	暗号化　暗号化(encryption)は，情報の機密性を保護するために用いることができる技術であり，取扱いに慎重を要する又は重要な情報の保護のために考慮することが望ましい。 　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が望ましい。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が望ましい。さらに，暗号技術の輸出入に適用される規制も考慮することが必要である【2.1.6参照)。 　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が望ましい（10.3.5参照）。さらに，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，法律家の助言を求める必要がある場合がある。 　参考　我が国では，暗号技術の輸出に関係する法律として，“外国為替及び外国貿易管理法(昭和二十四年法律第二百二十八号)”に基づく“輸出貿易管理令(昭和二十四年政令第三百七十八号)”及び“外国差為替令(昭和五十五年政令第二百六十号)”などがあり，原則として輸出には許可が必要となる。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(63 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	電子情報の真正性及び完全性を保護するため、デジタル署名を適用すること。		10.3.3	ディジタル署名　ディジタル署名は，電子文書の真正性及び完全性を保護する手段である。例えば，誰が電子文書に署名をしたかを確認し，署名された文書内容の改ざんを検査する必要がある電子商取引に使用できる。 　ディジタル署名は，電子的に処理される文書に，その文書の形式のいかんを問わず適用できる。例えば，電子的な決済・資金移動・契約・合意書の署名に用いることができる。ディジタル署名は，一意の関係にある一対のかぎに基づく暗号技術を用いて実現できる。一対のかぎのうち，一方は，署名を作成するために使用され（秘密かぎ），他方は，署名を検証するために使用される（公開かぎ）。 　参考　この規格において，非対称暗号方式における，一対のかぎのうち，“private key”を“秘密かぎ”とし，“public key”を“公開かぎ”とした。また，共通かぎ（対称暗号）方式のおける“secret key”を“共通かぎ”とした。 　秘密かぎの機密性を保護するために注意を払うことが望ましい。この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が望ましい。さらに，公開かぎの完全性を保護することも重要である。この保護は，公開かぎ証明書の使用によって得られる（10.3.5参照）。 使用される署名アルゴリズムの種類及び品質，並びに使用されるかぎの長さを考慮する必要がある。ディジタル署名に使用される暗号かぎは，暗号化（10.3.2参照）に使用されるものとは異なることが望ましい。 　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規定した関連法令を考慮することが望ましい。例えば，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が重要である。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が必要な場合がある。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が望ましい。 　参考　我が国には，関係する法律として，電子署名及び認証業務に関する法律（平成十二年法律第百二号）が制定されている。
		④	取引に関わる紛争を解決するため、電子情報による取引事実の否認を防止するための措置を講ずること。		10.3.4	否認防止サービス　事象（契約など）又は動作（支払いなど）が起こったか，起こらなかったかについての紛争（例えば，電子契約又は電子決済におけるディジタル署名の使用にかかわる紛争）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が望ましい。これらのサービスは，それぞれの事象又は動作が起こったかどうか（例えば，電子署名された指示文書の電子メールの送信があったか否か）を立証するための証拠の一助となり得る。これらのサービスは，暗号及びディジタル署名の技術の利用に基づいている（10.3.2及び10.3.3参照）。

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
		⑤ 情報を保護するために暗号を用いる場合、関連する対策基準類や手順等に準拠し、適切に鍵管理を行うこと。		10.3.5.2	標準類，手順及び方法　かぎ管理システムは，次の事項について，一連の合意された標準類，手順及び安全な方法に基づくものであることが望ましい。 a) 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。 b) 公開かぎ証明書を生成し入手する方法。 c) 予定している利用者にかぎを配付する方法。その中には，受領したとき，かぎをどのように起動すべきかも含める。 d) かぎを保存する方法。その中には，認可されている利用者がかぎにどのようにアクセスできるかも含める。 e) かぎを変更又は更新する方法。その中には，かぎをいつ変更すべきか，また変更をどのように行うかについての規則も含める。 f) セキュリティが損なわれたかぎを処理する方法。 g) かぎを無効にする方法。その中には，例えば，かぎのセキュリティが損なわれたとき又は利用者が組織を去るときに，かぎをどのようにして取り消し又は非活性化するかも含める（ただし，この場合には，同時に，かぎを記録保管することが望ましい。）。 h) 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。 i) 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。 j) かぎを破壊する方法。 k) かぎ管理に関連する活動を記録し監査する方法。 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が望ましい。この期間は，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が望ましい。 暗号かぎへのアクセスのための法的要求を取り扱うための手続を考慮することが必要になってくる場合がある。例えば，暗号化情報は，訴訟の場合に証拠として復号された形で使用可能な状態にする必要が生じる場合がある。 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が望ましい。何者かが，利用者の公開かぎを自分のものとすり替え，ディジタル署名を偽る脅威がある。この問題は，公開かぎ証明書を用いることによって対処される。この証明書は，公開かぎ/秘密かぎのペアの所有者にかかわる情報を，公開かぎに固有の情報を結びつけることによって作成される。したがって，この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が大切である。この手続は，要求される信頼度を得る適切な管理及び手順を備えており認知されている組織であることが望ましい証明機関（certification authority）によって，通常，実施される。 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が望ましい（4.2.2参照）。
	⑷ システムファイルのセキュリティ		II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。	システムファイルへのアクセスを制御することが望ましい。システムの完全性の維持は，利用者，又は業務用システム若しくはソフトウェアを所有する開発グループの責任とすることが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(65 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	稼動中の情報システムへのアプリケーションソフトウェアの導入は適切に管理されること。		10.4.1	運用ソフトウェアの管理　運用システムでのソフトウェアの実行は，管理されることが望ましい。運用システムを損なうリスクを最小限に抑えるために，次の管理策を考慮することが望ましい。 a) 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が望ましい（10.4.3参照）。 b) 可能ならば，運用システムは，実行可能なコードだけを保持することが望ましい。 c) 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，さらに，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，実行しないことが望ましい。 d) 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が望ましい。 e) 古い版のソフトウェアは，事故対策用として保持しなければならない。 運用システムに使用されるベンダ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が望ましい。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に入れることが望ましい。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が望ましい。 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，許されることが望ましい。供給者の活動は監視されることが望ましい。
		②	テスト用のデータは適切に保護され管理されること。		10.4.2	システム試験データの保護　試験データは保護され，管理されることが望ましい。システム及び受入れの試験には，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が必要である。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が望ましい。そのような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が望ましい。試験目的で使用する場合は，運用データを保護するために，次の管理策を適用することが望ましい。 a) 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が望ましい。 b) 運用情報を試験用システムに複製する場合は，その都度，認可を受けることが望ましい。 c) 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が望ましい。 d) 運用情報の複製及び使用は，監査証跡とするために，記録することが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(66 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	プログラムソースライブラリへのアクセスを厳格に管理すること。		10.4.3	プログラムソースライブラリへのアクセス制御　コンピュータプログラムが破壊される危険性を軽減するために，プログラムソースライブラリへのアクセス全体にわたって，次のように厳しい管理を維持することが望ましい（8.3参照）。 a) 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が望ましい。 b) 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が望ましい。 c) 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が望ましい。 d) 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が望ましい。 e) 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が望ましい。 f) 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が望ましい（8.6.4参照）。 g) 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が望ましい。 h) ソースプログラムの旧版は，記録保管しておくことが望ましく，その際，それら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，明確に示すことが望ましい。 i) 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が望ましい（10.4.1参照）。
	⑸ 開発及びサポートプロセス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。	プロジェクト及び支援環境は，厳しく管理することが望ましい。 業務用システムに責任をもつ管理者は，プロジェクト又は支援環境のセキュリティにも責任を負うことが望ましい。これらの管理者は，提案されているすべてのシステム変更をレビューし，それらの変更によってシステム又は運用環境のセキュリティが絶対に損なわれないようにすることが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(67 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	情報システムの変更管理の手順を定め、変更を厳格に管理すること。		10.5.1	変更管理手順　情報システムに対する破壊の危険性を最小限に抑えるために，変更の実施は厳しく管理されることが望ましい。正式な変更管理手順を確実に実行させることが望ましい。これらの手順によって，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，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，並びに，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が望ましい。業務用ソフトウェアの変更が運用環境に影響を及ぼすことがある。実現可能ならば，業務用ソフトウェア及び運用の変更管理手順は統合されることが望ましい（8.1.2参照）。この過程には，次の事項が含まれることが望ましい。 a) 合意された認可レベルの記録を維持すること。 b) 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。 c) 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。 d) 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。 e) 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。 f) 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。 g) 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。 h) システムに関する一式の文書が各変更の完了時点で更新されること，及び古い文書類は記録保管されるか，処分されることを確実にすること。 i) 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。 j) すべての変更要求の監査証跡を維持管理すること。 k) 運用文書類（8.1.1参照）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。 l) 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。 多くの組織では，利用者が開発及び生産環境から分離された新しいソフトウェアを試験する環境をもつ。これは，新しいソフトウェアを管理し，試験目的のために使用されている運用情報に更なる追加の保護を与える手段を提供する。
		②	オペレーティングシステムを変更する場合、アプリケーションシステムの見直し及びテストを実施すること。		10.5.2	オペレーティングシステムの変更の技術的レビュー　定期的にオペレーティングシステムを変更すること（例えば，供給されたソフトウェアの更新版又はパッチを導入すること）が必要である。この変更をした場合は，業務の運用又はセキュリティに悪影響がないことを確認するために業務用システムをレビューし，試験することが望ましい。この手続には，次の事項を含むことが望ましい。 a) 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損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。 b) 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。 c) 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。 d) 事業継続計画（11.参照）に対して適切な変更がなされることを確実にすること。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(68 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	パッケージソフトウェアの変更は原則として行わないこと。		10.5.3 前半）	パッケージソフトウェアの変更に対する制限　パッケージソフトウェアの変更は行わないようにすることが望ましい。可能な限り，そして実行可能ならば，ベンダ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が望ましい。
		④	やむを得ずパッケージソフトウェアの変更が必要になった場合、変更を厳格に管理すること。		10.5.3 後半）	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，次の事項を考慮するのが望ましい。 a) 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。 b) ベンダの同意を得るべきかどうか。 c) 標準的なプログラム更新として，ベンダから必要な変更が得られる可能性。 d) 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。 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が望ましい。変更はすべて，完全に試験し，文書化し，そうすることによって，変更を，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が望ましい。
		⑤	ソフトウエアの購入、使用及び変更を厳格に管理すること。		10.5.4	隠れチャネル及びトロイの木馬　隠れチャネル(covert channels)は，幾つかの間接的で隠された手段によって情報を危険にさらすことがある。このチャネルは，コンピュータシステムのセキュリティの確保された要素とそうでない要素との両方からアクセス可能な一つのパラメタを変更することによって，又はデータの流れの中に情報を埋め込むことによって，活性化させることができる。トロイの木馬(Trojan code)は，認可されていない，容易には気づかない，及び受信者又はプログラムの利用者によって要求されていない方法で，システムに影響を及ぼすように仕組まれている。隠れチャネル及びトロイの木馬は，偶然によって起こることはほとんどない。隠れチャネル又はトロイの木馬が心配ならば，次の事項を考慮することが望ましい。 a) プログラムは定評のある開発元のものだけを購入する。 b) 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。 c) 評価された製品を用いる。 d) 使用前にすべてのソースコードを検査する。 e) いったん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。 f) 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。
		⑥	ソフトウェア開発をアウトソーシングする場合、リスクを考慮し、それに基づいた正式な契約を締結すること。		10.5.5	外部委託によるソフトウェア開発　ソフトウェア開発を外部委託する場合，次の点を考慮することが望ましい。 a) 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（12.1.2参照）。 b) 実施される作業の質及び正確さの認証。 c) 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。 d) 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。 e) コードの品質についての契約要求事項。 f) トロイの木馬を検出するための導入前試験。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(69 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
9. 事業継続管理						
	(1) 事業継続管理			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。	災害及びセキュリティ障害（例えば，自然災害，事故，装置の故障及び悪意による行為の結果）による中断を，予防管理策と回復管理策との組合せによって許容可能なレベルにまで抑えるために，事業継続管理手続を実施することが望ましい。 災害，セキュリティ障害及びサービスの喪失の結果を，分析することが望ましい。業務手続を，要求される時間内に確実に復旧できるようにするために，障害時復旧計画を立て，実施することが望ましい。そのような計画を，他のすべての管理手続のなかの必要不可欠な一部となるように，維持し，実行するのがよい。 事業継続管理には，リスクを特定して軽減し，損傷を与える事件 事故の結果を制限し，絶対必要な運転を早く確実に復旧するための管理策を含めることが望ましい。	
		①	ISMS適用範囲全体を含む組織の事業継続計画を検討し策定、維持するための管理プロセスを整備すること。		11.1.1	事業継続管理手続　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が望ましい。その手続は，事業継続管理の次の重要な要素を組み込んだものであることが望ましい。 a)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。 b)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。 c) 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。 d) 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。 e) 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。 f) 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。 g) 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。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（4.1.1参照）において，割り当てることが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(70 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		②	事業継続に取り組むため、リスク評価に基づいた戦略計画を策定すること。		11.1.2	事業継続及び影響分析　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，例えば，装置の故障，洪水及び火災を特定することから始めることが望ましい。その後，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が望ましい。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が望ましい。このアセスメントは，すべての業務手続を検討するものであり，情報処理施設に限定しない。 　リスクアセスメントの結果によって，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を立てることが望ましい。この計画を作成したならば，経営陣の承認を得ることが望ましい。
		③	重要な業務に障害または故障が発生した際に事業の運営を維持し、許容時間内に復旧させるため、必要な計画を立案すること。		11.1.3	継続計画の作成及び実施　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が望ましい。事業継続計画の作成過程では，次を考慮することが望ましい。 a)すべての責任及び緊急時手続を識別し，合意する。 b)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。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，特に注意する必要がある。 c)合意された手順及び過程の文書化。 d)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。 e)計画の試験及び更新。 　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，重点をおくことが望ましい。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，考慮することが望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(71 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	すべての計画の整合性を保証し、また、試験や整備の優先順位を明確にするため、事業継続計画全体を統括する枠組みを維持すること。		11.1.4	事業継続計画作成のための枠組み　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が望ましい。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が望ましい。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が望ましい。 　事業継続計画作成の枠組みでは，次を考慮することが望ましい。 a)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。 b)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。この手続には，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が望ましい。 c)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。 d)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。 e)計画をいつ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。 f)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。 g)個人の責任。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。必要に応じて，代わりの者を任命することが望ましい。 　各計画には特定の責任者がいることが望ましい。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の管理者の責任範囲内でたてられることが望ましい。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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(72 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑤	事業継続計画を定期的に試験し見直すこと。		11.1.5 11.1.5.1と11.1.5.2	事業継続計画の試験，維持及び再評価 計画の試験　事業継続計画は，多くの場合，誤った仮定，手落ち，装置又は要員の変更が原因となって，試験をしたときに機能しないことがある。したがって，これらの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が望ましい。そのような試験は，また，回復チームのすべてのメンバ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が望ましい。 　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，いつ試験すべきかを示すことが望ましい。計画の個々の構成要素を，頻繁に試験することが望ましい。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が望ましい。それらには次を含めるのがよい。 a)様々な状況の机上試験 障害例を用いての事業回復計画の検討)。 b)模擬試験 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)。 c)技術的回復試験 情報システムを有効に復旧できることを確実にする。)。 d)代替施設における回復試験 住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。)。 e)供給者施設及びサービスの試験 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。)。 f)全体的な模擬回復試験 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。)。 　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が望ましい。 計画の維持及び再評価　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が望ましい(11.1.1～11.1.3参照)。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が望ましい。 　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が望ましい。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が望ましい。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が望ましい。 　計画の更新を必要とする可能性がある状況の例としては，新しい装置の取得，又は運用システムのアップグレード及び次の変更が含まれる。 a)要員 b)所在地又は電話番号 c)事業戦略 d)所有地，施設，及び資源 e)法規制 f)請負業者，供給業者及び主要な顧客 g)手続，又は手続の新規設定/廃止 h) 運用上及び財務上の）リスク

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(73 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
10. 準拠						
	(1) 法的要求事項への準拠			刑法及び民法，制定法，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。	情報システムの設計，運用，使用及び管理には，法令，規制及び契約上のセキュリティ要求事項が適用されることがある。 特定の法的要求事項については，組織の法律顧問又は適切な資格をもつ法律の実務家に助言を求めることが望ましい。法的要求事項は，国ごとに異なっており，一つの国で作成され別の国へ伝送される情報（すなわち，国境を超えたデータの流れ）についても異なっている。	
		①	個別の情報システム毎に関連するすべての法規及び契約上の要求事項を明確にし、これを文書化すること。		12.1.1	適用法規の識別　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，文書化することが望ましい。これら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，文書化することが望ましい。
		②	知的財産権に関わる法的制限事項を遵守した手順を整備すること。		12.1.2 12.1.2.1と12.1.2.2	知的所有権 著作権　著作権，意匠権，商標のような知的所有権がある物件を使用する場合には，法的制限事項に確実に適合するように，適切な手続を実行することが望ましい。著作権を侵害した場合，法的措置がとられ，刑事訴訟となることもある。 法律，規制及び契約上の要求事項が，所有物の複製に制限を加えることがある。特に，これらは，組織によって開発される資料，又は開発者によって組織に使用許諾若しくは提供される資料だけを使用することを要求することもある。 ソフトウェアの著作権　ソフトウェア製品は，通常，使用許諾契約に基づいて支給されるが，この使用許諾契約では，製品の使用を指定した機器に限定し，複製もバックアップコピーの作成だけに限定することがある。次の管理策を考慮することが望ましい。 a)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。 b)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。 c)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。 d)適切な財産登録簿を維持管理する。 e)使用許諾書，マスタディスク，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。 f)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。 g)認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認する。 h)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。 i)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。 j)適切な監査ツールを用いる。 k)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（8.7.6参照）。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(74 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		③	組織の重要な記録を、紛失、消失、破壊、改ざん等から保護すること。		12.1.3	組織の記録の保護　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が望ましい。記録の中には，不可欠な事業活動を支援するために安全に保持しなければならないものがあると同様に，法定又は規制上の要求事項に適合するために安全に保持しなければならないものがある。このような記録の例としては，組織が法令上の規則若しくは規制上の規則の範囲内で事業活動しているという証拠として必要とされる記録類，潜在的な民事的若しくは刑事的措置に対して適切な防備を確実に行うために必要とされる記録類，又は株主，共同経営者及び監査人に対して組織の財務状態を正式に認めるために必要とされる記録類がある。情報保持期間及びデータの内容は，国の法律又は国家規制によって定められていることもある。 参考　帳簿書類の保存期間などに関連する定めをもつ法令として，わが国には，民法，商法，税務に関して制定された法令などがあり，電子的に保存する場合に関しては，電子計算機を使用して作成する国税関係帳簿書類の保存法の特例に関する法律(平成十年法律第二十五号)などがある。 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とよい。暗号化されたアーカイブ又はディジタル署名（10.3.2及び10.3.3参照）にかかわる暗号かぎを，安全に保管し，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が望ましい。 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が望ましい。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が望ましい。 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が望ましい。 要求されるデータを法廷で受け入れられる様式で取り出すことができるように，例えば，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が望ましい。 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が望ましい。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が望ましい。 これらの義務に適合するため，組織内では，次の措置をとることが望ましい。 a)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が望ましい。 b)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。 c)主要な情報の出典一覧を維持管理することが望ましい。 d)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が望ましい。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(75 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		④	個人情報保護に関する法規に従い、個人の情報を保護すること。		12.1.4	データの保護及び個人情報の保護　多くの国では，個人データ（一般に，その情報から生存している個人を識別できる情報）の処理及び伝送に関して規制した法令を導入している。そのような管理策には，個人情報を収集し，処理し，流布する人達に責務を課すものもあり，そのようなデータを外国へ転送する機能を制限しているものもある。 データ保護に関連して制定された法律に適合するためには，適切な管理構造及び統制が必要である。これは多くの場合，一人のデータ保護の担当役員を任命することによって達成される。ここでいうデータ保護の担当役員とは，管理者，利用者及びサービス提供者に対して，従うべき手続について，指導する役目をもつものである。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が望ましく，関連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が望ましい。
		⑤	情報処理施設及び設備の悪用を防止するための措置を講ずること。		12.1.5	情報処理施設の誤用の防止　組織の情報処理施設は，業務目的のために備えられている。それらの施設の使用は，管理者が認可することが望ましい。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が望ましい。そのような使用が，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が望ましい。 使用を監視することの合法性は，国によって異なり，そのような監視について従業員に通知しておかなければならない場合もあれば，従業員の同意を得なければならない場合もある。監視手続を実行する前に，法的な助言を受けることが望ましい。 多くの国では，コンピュータの悪用に対して，保護するための法律を施行しているか，又はその導入を検討している。認可されていない目的のためにコンピュータを使用することは，刑事犯となることもある。したがって，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が必す 須）である。このことは，例えば，利用者に認可書を与え，その写しに利用者からサインをもらい，それを組織が安全に保管することによって達成できる。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が望ましい。 参考　わが国には，関係する法律として，不正アクセス行為の禁止などに関する法律(平成十一年法律第百二十八号)があり，また，電磁的記録化記録の不正作出及び毀棄罪などが刑法に規定されている。 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が望ましい。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，それに適切に対応しなければならない。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(76 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		⑥	暗号の使用に関する法規を遵守すること。		12.1.6	暗号による管理策の規制　国によっては，暗号による管理策へのアクセス又はその使用を統制するために，協定，法律，規制，又はその他の手段を実行している。そのような統制には，次の事項が含まれることがある。 a)暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの輸入及び/又は輸出。 b)暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの輸入及び/又は輸出。 c)内容の機密性を守るためにハードウェア又はソフトウェアによって暗号化された情報への，国による強制的又は任意的アクセス方法。 　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が望ましい。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が望ましい。 　参考　10.3.2の参考を参照すること。

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(77 / 79)

ISMS認証基準（Ver. 1.0）			JIS X 5080		
			目的		内容
	⑦	訴訟に提示する証拠は、関連する法規に定められた規則に適合すること。		12.1.7 12.1.7.1と12.1.7.2と12.1.7.3	証拠の収集 証拠に関する規則　人又は組織に対する措置を支援するには，十分な証拠をもっていなければならない。この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になる。 　措置が，民事であれ刑事であれ，法律にかかわるものである場合，提示される証拠は，関連法令又は事件の審理が行われる特定の法廷の規則に定められる，証拠に関する規則に適合したものであることが望ましい。一般に，これらの規則では，次の事項を定めている。 a)証拠の容認性 証拠が法廷で使用できるかどうか。 b)証拠の重み 証拠の質及び完全性。 c)提示されるべき証拠がシステムによって保管及び処理された期間をとおして，管理策が正しく，かつ，一貫して働いていたという十分な証拠（すなわち，プロセス管理の証拠）。 証拠の容認性　証拠の容認性を達成するためには，組織は，その情報システムが，公表されている標準又は実践規範に適合することを確実にするのが望ましい。 証拠の質及び完全性　証拠の質及び完全性を達成するためには，強力な証跡が要求される。一般に，そのような強力な証跡は，次の条件のもとで達成できる。 a)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，いつそれを発見し，誰がその発見に立ち会ったかの記録をとる。どのような調査を行っても，原本に手が加えられないことが，証明できることが望ましい。 b)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が望ましい。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，立会い者がいることが望ましい。媒体の複製一組及びその記録を，安全に保管することが望ましい。 　事件・事故が最初に発見されたときは，それが訴訟になるかどうか分らない。したがって，その事件・事故の重大性が認識される前に，必要な証拠が誤って破壊されてしまう危険性がある。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が望ましい。
	⑵ セキュリティポリシーへの準拠		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。	情報システムのセキュリティは，定期的に見直すことが望ましい。 　このような見直しは，適切なセキュリティ基本方針及び技術的プラットフォームに違反しているかを見るために行われることが望ましく，情報システムをセキュリティ実行標準に適合しているかどうかのために監査することが望ましい。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(78 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	すべての手続きが情報セキュリティポリシーに準拠して実行されていることを定期的に見直すこと。		12.2.1	セキュリティ基本方針との適合　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が望ましい。さらに，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が望ましい。これらの範囲には次の対象を含めるとよい。 a)情報システム b)システム提供者 c)情報及び情報資産の所有者 d)利用者 e)経営陣 　情報システム（5.1参照）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が望ましい。システム運用の監視については，9.7による。
		②	情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的に確認すること。		12.2.2	技術適合の検査　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が望ましい。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。この種の適合検査では，専門家の技術援助を必要とする。この検査は，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が望ましい。 　適合検査としては，例えば，侵入試験がある。この試験は，この目的のために特に契約された独立した専門家によって実施される。この試験は，システムのぜい（脆）弱性の検出に役立ち，これらのぜい（脆）弱性による認可されていないアクセスの防止に管理策がどれほど有効であるかを検査することに役立つ。侵入試験の成功によって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がある場合に，注意を払うことが望ましい。 　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だけ，実施されることが望ましい。
	(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。	システムの監査中に，運用システム及び監査ツールを保護する管理策があることが望ましい。 　監査ツールの完全性を保護するため，及びその誤用を防止するための保護も要求される。	

ISMS認証基準　第4 詳細管理策とJIS X 5080 対応表(79 / 79)

ISMS認証基準（Ver. 1.0）				JIS X 5080		
				目的		内容
		①	稼動中の情報システムに対する監査を実施する場合、業務が中断するリスクを最小限に抑えるよう計画すること。		12.3.1	システム監査管理策　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，合意されることが望ましい。次の事項を守ることが望ましい。 a)監査要求事項は，担当経営陣の同意を得ることが望ましい。 b)検査の範囲は，合意され，管理されることが望ましい。 c)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が望ましい。 d)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が望ましい。それらの複製ファイルは，監査が完了した時点で消去されることが望ましい。 e)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が望ましい。 f)特別又は追加処理の要求事項は，識別され，合意されることが望ましい。 g)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，記録されることが望ましい。 h)すべての手順，要求事項及び責任について，文書化することが望ましい。
		②	システム監査ツールに対する許可されないアクセスを防止するための措置を講ずること。		12.3.2	システム監査ツールの保護　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，保護されることが望ましい。このようなツールは，開発及び運用システムから分離しておくことが望ましく，テープライブラリ，又は利用者の領域で保持しないことが望ましい。ただし，適切なレベルの保護を追加する場合は，その限りではない。