ISMS 詳細管理策

Ver. 2.0

1. はじめに

3.から12.に記載する管理目的及び管理策のリストは、JIS X 5080:2002 を参照している。本基準の第4 2.(1)で規定されたISMS のプロセスの一部として、下記のリストから管理目的及び管理策を選択すること。ただし、このリストは組織が必要とする管理目的及び管理策の全てとは限らないので、組織は必要に応じて追加の管理目的及び管理策を選択してもよい。

2. 実践規範への手引き

JIS X 5080:2002 の3.から12.は、附属書の3.から12.に規定する管理策を基にした最良な実践の導入についての助言及び手引きを提供するものである。

3. 情報セキュリティ基本方針

3.(1)	**情報セキュリティ基本方針**	
管理目的	情報セキュリティのための経営陣の指針及び支持を規定するため。	
管理策		
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。
3.(1) ②	見直し及び評価	基本方針は、依然として適切であることを確実にするために、定期的に、また影響を及ぼす変化があった場合に、見直すこと。

4. 組織のセキュリティ

4.(1)	**情報セキュリティ基盤**	
管理目的	組織内の情報セキュリティを管理するため。	
管理策		
4.(1)①	情報セキュリティ運営委員会	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、運営委員会を設置すること。運営委員会は、適切な責任分担及び十分な資源配分によって、セキュリティを促進すること。
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を利用すること。
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。
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。
4.(1)⑤	専門家による情報セキュリティの助言	専門家による情報セキュリティの助言を内部又は外部の助言者から求め、組織全体を調整すること。
4.(1)⑥	組織間の協力	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
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の実施を、他者がレビューすること。
4.(2)	**第三者によるアクセスのセキュリティ**	
管理目的	第三者によってアクセスされる組織の情報処理設備及び情報資産のセキュリティを維持するため。	
管理策		
4.(2)①	第三者のアクセスから生じるリスクの識別	組織の情報処理施設への第三者のアクセスに関連づけてリスクアセスメントを実施し、適切なセキュリティ管理策を実施すること。
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、必要なセキュリティ要求事項すべてを含んだ正式な契約に基づくこと。
4.(3)	**外部委託**	
管理目的	情報処理の責任を別の組織に外部委託した場合における情報セキュリティを維持するため。	
管理策		
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。

5. 資産の分類及び管理

5.(1)	**資産に対する責任**	
管理目的	組織の資産の適切な保護を維持するため。	
管理策		
5.(1)①	資産目録	情報システムそれぞれに関連づけてすべての重要な資産について目録を作成し、維持す
5.(2)	**情報の分類**	
管理目的	情報資産の適切なレベルでの保護を確実にするため。	
管理策		
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を考慮に入れておくこと。
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、一連の手順を定めること。

6. 人的セキュリティ			
6.(1)	**職務定義及び雇用におけるセキュリティ**		
管理目的	人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため。		
管理策			
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で定められたとおりに、職務定義のなかに文書化すること。	
6.(1)②	要員審査及びその個別方針	常勤職員、請負業者及び臨時職員を採用するときは、提出された応募資料の内容を検査すること。	
6.(1)③	機密保持契約	従業員は、入社時の雇用条件の一部として、機密保持契約書に署名すること。	
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。	
6.(2)	**利用者の訓練**		
管理目的	情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事の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。		
管理策			
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。	
6.(3)	**セキュリティ事件・事故及び誤動作への対処**		
管理目的	セキュリティ事件・事故及び誤動作による損害を最小限に抑えるため、並びにそのような事件・事故を監視してそれらから学習するため。		
管理策			
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。	
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	
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。	
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。	
6.(3)⑤	懲戒手続	従業員による組織のセキュリティ基本方針及び手順への違反は、正式な懲戒手続によって処理すること。	
7. 物理的及び環境的セキュリティ			
7.(1)	**セキュリティが保たれた領域**		
管理目的	業務施設及び業務情報に対する認可されていない物理的なアクセス、損傷及び妨害を防止するため。		
管理策			
7.(1)①	物理的セキュリティ境界	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	
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。	
7.(1)③	オフィス、部屋及び施設のセキュリティ	特別なセキュリティ要求事項のあるオフィス、部屋及び施設を保護するために、セキュリティの保たれた領域を設定すること。	
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、その領域での作業のための管理策及び指針を追加すること。	
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管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔離すること。	
7.(2)	**装置のセキュリティ**		
管理目的	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため。		
管理策			
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。	
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。	
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。	
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可能とするために、装置を正しく保	
7.(2)⑤	事業敷地外における装置のセキュリティ	組織の敷地外で情報処理のために装置を使用するいかなる場合も、管理者による認可を要求すること。	
7.(2)⑥	装置の安全な処分又は再使用	装置を処分又は再使用する前に、情報を装置から消去すること。	
7.(3)	**その他の管理策**		
管理目的	情報及び情報処理設備の損傷又は盗難を防止するため。		
管理策			
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、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の、クリアデスク方針及びクリアスクリーン方針を持つこと。	
7.(3)②	資産の移動	組織に属する装置、情報又はソフトウェアは、管理者による認可なしでもち出しできないこ	

8. 通信及び運用管理		
8.(1)	**運用手順及び責任**	
管理目的	情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。	
管理策		
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、文書化して維持すること。
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。
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ために、および監査証跡及び記録といった事件・事故に関連するデータを収集するために、事件・事故管理の責任及び手順を確立すること。
8.(1)④	職務の分離	情報若しくはサービスの無許可の変更又は誤用の可能性を小さくするために、職務及び責任領域を分離すること。
8.(1)⑤	開発施設及び運用施設との分離	開発施設及び試験施設は、運用施設から分離すること。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。
8.(1)⑥	外部委託による施設管理	外部委託による施設管理サービスを利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること。
8.(2)	**システムの計画作成及び受入れ**	
管理目的	システム故障のリスクを最小限に抑えるため。	
管理策		
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の利用を可能にするために、容量・能力の需要を監視し、将来必要とされる容量・能力を予測すること。
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。
8.(3)	**悪意のあるソフトウェアからの保護**	
管理目的	ソフトウェア及び情報の完全性を、悪意のあるソフトウェアによる被害から保護するため。	
管理策		
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。
8.(4)	**システムの維持管理**	
管理目的	情報処理及び通信サービスの完全性及び可用性を維持するため。	
管理策		
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、定期的に取得し、かつ検査する
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。運用担当者の記録は、定期的に独立した検査を受けること。
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。
8.(5)	**ネットワークの管理**	
管理目的	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため。	
管理策		
8.(5)①	ネットワーク管理策	ネットワークにおけるセキュリティを実現し、かつ、維持するために一連の管理策を実施する
8.(6)	**媒体の取扱い及びセキュリティ**	
管理目的	財産に対する損害及び事業活動に対する妨害を回避するため。	
管理策		
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を管理すること。
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。
8.(6)③	情報の取扱手順	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。
8.(6)④	システムに関する文書のセキュリティ	認可されていないアクセスからシステムに関する文書を保護すること。
8.(7)	**情報及びソフトウェアの交換**	
管理目的	管理目的：組織間で交換される情報の紛失、改ざん又は誤用を防止するため。	
管理策		
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、合意を取り交わすこと。
8.(7)②	配送中の媒体のセキュリティ	配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること。
8.(7)③	電子商取引のセキュリティ	電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること。
8.(7)④	電子メールのセキュリティ	電子メールの使用に関する個別方針を作成し、電子メールがもたらすセキュリティ上のリスクを軽減するための管理策を実施すること。
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。
8.(7)⑥	公開されているシステム	情報を公開する前に正式な認可の手続がとられ、また、情報の改ざんを防止するために公開した情報の完全性を保護すること。
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、個別方針、手順及び管理策をもつこと。

9. アクセス制御		
9.(1)	**アクセス制御に関する業務上の要求事項**	
管理目的	情報へのアクセスを制御するため。	
管理策		
9.(1)①	アクセス制御方針	アクセス制御についての業務上の要求事項を定義して文書化し、アクセスをアクセス制御方針で定義されたものに限定すること。
9.(2)	**利用者のアクセス管理**	
管理目的	情報システムへのアクセス権が、適切に認可され、割り当てられ、維持されていることを確実にするため。	
管理策		
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。
9.(2)②	特権管理	特権の割当て及び使用は、制限し、管理すること。
9.(2)③	利用者のパスワードの管理	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。
9.(2)④	利用者アクセス権の見直し	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。
9.(3)	**利用者の責任**	
管理目的	認可されていない利用者のアクセスを防止するため。	
管理策		
9.(3)①	パスワードの使用	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を、利用者に要求
9.(3)②	利用者領域にある無人運転の装置	無人運転の装置に適切な保護対策を備えていることを確実にするように、利用者に要求すること。
9.(4)	**ネットワークのアクセス制御**	
管理目的	ネットワークを介したサービスの保護のため。	
管理策		
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	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を提供すること。
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、管理すること。
9.(4)③	外部から接続する利用者の認証	遠隔地からの利用者のアクセスには、認証を行うこと。
9.(4)④	ノードの認証	遠隔コンピュータシステムへの接続は、認証されること。
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。
9.(4)⑥	ネットワークの領域分割	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の制御を、ネットワーク内に導入すること。
9.(4)⑦	ネットワークの接続制御	共有ネットワークにおける利用者の接続の可能性は、アクセス制御方針に従って制限すること。
9.(4)⑧	ネットワーク経路を指定した制御	共有ネットワークは、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと。
9.(4)⑨	ネットワークサービスのセキュリティ	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。
9.(5)	**オペレーティングシステムのアクセス制御**	
管理目的	認可されていないコンピュータアクセスを防止するため。	
管理策		
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。
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使用すること。
9.(5)③	利用者の識別及び認証	すべての利用者は、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。利用者が主張するID を確証するための適切な認証技術を選択すること。
9.(5)④	パスワード管理システム	パスワード管理システムは、質のよいパスワードであることを確実にするための、有効な対話的機能を提供すること。
9.(5)⑤	システムユーティリティの使用	システムユーティリティプログラムの使用を制限し、厳しく管理すること。
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、脅迫に対する警報を備えること。
9.(5)⑦	端末のタイムアウト	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。
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、追加のセキュリティを提供するために、接続時間に制限を設けること。

9.(6)	**業務用ソフトウェアのアクセス制御**	
管理目的	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。	
管理策		
9.(6)①	情報へのアクセス制限	情報及び業務用システム機能へのアクセスは、アクセス制御方針に従い、制限されること。
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は、専用の（隔離された）コンピュータ環境にあること
9.(7)	**システムアクセス及びシステム使用状況の監視**	
管理目的	認可されていない活動を検出するため。	
管理策		
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。
9.(7)②	システム使用状況の監視	情報処理設備の使用状況を監視する手順を確立し、監視の結果を、定期的に見直すこと。
9.(7)③	コンピュータ内の時計の同期	正確な記録のために、コンピュータ内の時計を同期させておくこと。
9.(8)	**移動型計算処理及び遠隔作業**	
管理目的	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	
管理策		
9.(8)①	移動型計算処理	移動型計算処理の設備（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等）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から保護するために、正式な個別方針を持ち、適切な管理策を採用すること。
9.(8)②	遠隔作業	遠隔作業を認可し及び管理するための個別方針、手順及び標準類を策定すること。

10. システムの開発及び保守

10.(1)	**システムのセキュリティ要求事項**	
管理目的	情報システムへのセキュリティの組込みを確実にするため。	
管理策		
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では、管理策についての要求事項を明記すること。
10.(2)	**業務用システムのセキュリティ**	
管理目的	業務用システムにおける利用者データの消失、変更又は誤用を防止するため。	
管理策		
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。
10.(2)②	内部処理の管理	処理したデータの改ざんを検出するために、システムに妥当性の検査を組み込むこと。
10.(2)③	メッセージ認証	重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合は、メッセージ認証を使用すること。
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。
10.(3)	**暗号による管理策**	
管理目的	情報の機密性、真正性又は完全性を保護するため。	
管理策		
10.(3)①	暗号による管理策の使用に関する個別方針	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。
10.(3)②	暗号化	取扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化を用いること。
10.(3)③	ディジタル署名	電子的な情報（電子文書等）の真正性及び完全性を保護するために、ディジタル署名を用
10.(3)④	否認防止サービス	事象又は動作が起こったか、起こらなかったかについての紛争の解決には、否認防止サービスを用いること。
10.(3)⑤	かぎ管理	一連の合意された標準類、手順及び方法に基づくかぎ管理システムを、暗号技術の利用を支援するために用いること。
10.(4)	**システムファイルのセキュリティ**	
管理目的	IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため。	
管理策		
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を管理する手順を持つこと。
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。
10.(4)③	プログラムソースライブラリへのアクセス制御	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、厳しい管理を維持すること。

10.(5)	**開発及び支援過程におけるセキュリティ**	
管理目的	業務用システム及び情報のセキュリティを維持するため。	
管理策		
10.(5)①	変更管理手順	正式な変更管理手順によって、情報システムの変更の実施を厳しく管理すること。
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	オペレーティングシステムを変更する場合は、業務用システムをレビューし、試験すること。
10.(5)③	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極力行わないようにし、絶対に必要な変更は厳しく管理すること。
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）又はトロイの木馬（Trojan code）の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検査すること。
10.(5)⑤	外部委託によるソフトウェア開発	外部委託によるソフトウェア開発をセキュリティの保たれたものとするための管理策を適用すること。
11. 事業継続管理		
11.(1)	**事業継続管理の種々の面**	
管理目的	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため。	
管理策		
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。
11.(1)②	事業継続及び影響分析	事業継続に対する全般的取組方法のために、適切なリスクアセスメントに基づいた戦略計画を立てること。
11.(1)③	継続計画の作成及び実施	事業運営を、重要な業務手続の中断又は障害の後、適切な時間内で維持又は復旧させるための計画を立てること。
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。
11.(1)⑤	事業継続計画の試験、維持及び再評価	事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために定期的に試験をし、定期的な見直しをすること。
12. 適合性		
12.(1)	**法的要求事項への適合**	
管理目的	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため。	
管理策		
12.(1)①	適用法令の識別	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。
12.(1)②	知的所有権（IPR）	知的所有権がある物件及びソフトウェア製品を使用する場合は、法的制限事項に適合するように、適切な手続を実行すること。
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。
12.(1)④	データの保護及び個人情報の保護	関連法令に従って個人情報を保護するために、管理策を適用すること。
12.(1)⑤	情報処理施設の誤用の防止	情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐための管理策を用いること。
12.(1)⑥	暗号による管理策の規制	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ことを目的とした、国による協定、法律、規制、又はその他の手段に、適合することを可能にするために、管理策を用いるこ
12.(1)⑦	証拠の収集	人又は組織に対する措置が、民事であれ刑事であれ、法律にかかわるものである場合、提示する証拠は、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た証拠に関する規定に適合させること。また、容認される証拠を作成するために、公表されてい
12.(2)	**セキュリティ基本方針及び技術適合のレビュー**	
管理目的	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため。	
管理策		
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。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、定期的に見直すこと。
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。
12.(3)	**システム監査の考慮事項**	
管理目的	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため。	
管理策		
12.(3)①	システム監査管理策	運用システムの監査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。
12.(3)②	システム監査ツールの保護	システム監査ツールは、誤用又は悪用を防止するために、保護されること。