18.1.3.3　保存した記録の暗号化又はディジタル署名に用いた暗号鍵及び暗号プログラムは、その記録類を保存している期間中に記録の復号が可能なように、保管する。
18.1.3.4　記録の保存に用いる媒体が劣化する可能性を考慮して記録の保存及び取扱いの手順を定める。
18.1.3.5　記録の保存及び取扱いの手順は、媒体の製造業者の推奨の仕様に従って実施する。
18.1.3.6　電子的記憶媒体を選択する場合は、将来の技術変化によって読出しができなくなることを防ぐために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確実にする手順を確立する。
18.1.3.7　満たすべき要求に応じて、許容される時間枠内及び書式で、要求されたデータを取り出すことができるような、データ保存システムを選択する。
18.1.3.8　データ保存及びデータ処理システムは、記録を確実に特定し、国又は地域の法令又は規制が適用される場合に定められている記録の保持期間を確実に特定する。
18.1.3.9　保持期間が終了した後、組織にとって必要ない場合には、データ保存及びデータ処理システムは、記録を適切に破棄できるようにする。
18.1.3.10　記録保護の目的を満たすため、組織内では、記録及び情報の保持、保存、取扱い及び処分に関する指針を発行する。
18.1.3.11　記録保護の目的を満たすため、組織内では、記録及びそれらの記録の保持期間を明確にした保持計画を作成する。
18.1.3.12　記録保護の目的を満たすため、組織内では、主要な情報の出典一覧を維持・管理する。
18.1.4　プライバシー及びＰＩＩの保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。
18.1.4.1　プライバシー及びＰＩＩの保護に関する組織の方針を確立して実施する。
18.1.4.2　プライバシー及びＰＩＩの保護に関する組織の方針は、ＰＩＩの処理に関与する全ての者に伝達する。
18.1.4.3　プライバシー及びＰＩＩの保護に関する組織の方針の順守、並びに人々のプライバシーの保護及びＰＩＩの保護に関する全ての法令及び規制の順守のために、適切な管理構造及び管理策を確立する。
18.1.4.4　プライバシー及びＰＩＩの保護の責任者（例えば、プライバシー担当役員）は、管理者、利用者及びサービス提供者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供する。
18.1.4.5　ＰＩＩの取扱い、及びプライバシーの原則の認識を確実にすることについての責任は、関連する法令及び規制に従って処置する。
18.1.4.6　ＰＩＩを保護するための適切な技術的及び組織的対策を実施する。
18.1.5　暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。
18.1.5.1　関連する協定、法令及び規制を順守するため、暗号機能を実行するためのコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制を順守する。
18.1.5.2　関連する協定、法令及び規制を順守するため、暗号機能を追加するように設計されているコンピュータのハードウェア及びソフトウェアの、輸入又は輸出に関する規制を順守する。
18.1.5.3　関連する協定、法令及び規制を順守するため、暗号利用に関する規制を順守する。
18.1.5.4　関連する協定、法令及び規制を順守するため、内容の機密性を守るためにハードウェア又はソフトウェアによって暗号化された情報への、国の当局による強制的又は任意的アクセス方法を定める。
18.1.5.5　関連する法令及び規制の順守を確実にするために、法的な助言を求める。
18.1.5.6　暗号化された情報又は暗号制御機能を、法域を越えて持ち出す前に、法的な助言を受ける。

18.2　情報セキュリティのレビュー
目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため
18.2.1　情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。
18.2.1.1　経営陣は、情報セキュリティをマネジメントする組織の取組みが、引き続き適切、妥当及び有効であることを確実にするために、独立したレビューを発議し、実施させる。
18.2.1.2　独立したレビューには、改善の機会のアセスメントを含める。
18.2.1.3　独立したレビューには、方針及び管理目的を含むセキュリティの取組みの変更について、その必要性の評価を含める。
18.2.1.4　独立したレビューは、レビューが行われる領域から独立した個人・組織（例えば、内部監査の担当部署、独立した管理者、このようなレビューを専門に行う外部関係者）が実施する。
18.2.1.5　独立したレビューは、適切な技能及び経験をもつ個人・組織が実施する。
18.2.1.6　独立したレビューの結果は、記録し、レビューを発議した経営陣に報告する。
18.2.1.7　独立したレビューの結果の記録は、維持する。
18.2.1.8　独立したレビューにおいて、情報セキュリティマネジメントに対する組織の取組み及び実施が十分でない（例えば、文書化した目的及び要求事項が、情報セキュリティのための方針群に記載された情報セキュリティに関する方向付けを満たしていない、又はこれと適合していない）ことが明確になった場合には、経営陣は是正処置の検討を指示する。
18.2.2　管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。
18.2.2.1　管理者は、方針、標準類及びその他適用される規制で定められた情報セキュリティ要求事項が満たされていることをレビューするための方法を特定する。
18.2.2.2　管理者は定めに従って効率的にレビューを行うため、自動的な測定ツール及び報告ツールを使用する。
18.2.2.3　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、不順守の原因を特定する。
18.2.2.4　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、順守を達成するための処置の必要性を評価する。
18.2.2.5　管理者によるレビューの結果、何らかの不順守を検出した場合、管理者は、適切な是正処置を実施する。
18.2.2.6　管理者によるレビューの結果、何らかの是正処置を実施した場合、管理者は、是正処置の有効性を検証し、不備又は弱点を特定するために、とった是正処置をレビューする。
18.2.2.7　管理者が実施したレビュー及び是正処置の結果を記録する、また、その記録を維持・管理する。
18.2.2.8　管理者の責任範囲に対して、独立したレビューが実施されるときは、管理者は、独立したレビュー実施者に対して、レビュー及び是正処置の結果を報告する。