11.2.7　記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。

11.2.7.1　装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。

11.2.7.2　秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊すること、又はその情報を破壊、消去若しくは上書きする。

11.2.7.3　秘密情報又は著作権のある情報を格納した記憶媒体の消去又は上書きには、標準的な消去又は初期化の機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。

11.2.8　利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。

11.2.8.1　無人状態にある装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、全ての利用者に認識させる。

11.2.8.2　利用者に、実行していた処理が終わった時点で、接続を切るよう助言する（ただし、例えば、パスワードによって保護されたスクリーンセーバなどの適切なロック機能によって保護されている場合は、その限りではない。）。

11.2.8.3　利用者に、必要がなくなったら、アプリケーション又はネットワークサービスからログオフするよう助言する。

11.2.8.4　利用者に、コンピュータ又はモバイル機器は、利用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって、認可されていない利用から保護するよう助言する。

11.2.9　書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。

11.2.9.1　クリアデスク・クリアスクリーン方針において、組織の、情報分類、法的及び契約上の要求事項、並びにそれらに対応するリスク及び文化的側面を含める。

11.2.9.2　取扱いに慎重を要する業務情報又は重要な業務情報（例えば、紙又は電子記憶媒体上の業務情報）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（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管する。

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

11.2.9.4　コンピュータ及び端末は、利用しないときは、施錠、パスワード又は他の管理策によって保護する。

11.2.9.5　コピー機及びその他の再生技術（例えば、スキャナ、ディジタルカメラ）の認可されていない利用は、防止する。

11.2.9.6　取扱いに慎重を要する情報又は機密扱い情報を含む媒体は、プリンタから直ちに取り出す。

12　運用のセキュリティ

12.1　運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため

12.1.1　操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。

12.1.1.1　情報処理設備及び通信設備に関連する操作（例えば、コンピュータの起動・停止の手順、バックアップ、装置の保守、媒体の取扱い、コンピュータ室及びメールの取扱いの管理・安全）の手順書を作成する。

12.1.1.2　情報処理設備及び通信設備に関連する操作手順には、システムの導入及び構成を含む、操作上の指示を明記する。

12.1.1.3　情報処理設備及び通信設備に関連する操作手順には、情報の処理及び取扱い（自動化されたもの及び手動によるものを含む。）を含む、操作上の指示を明記する。

12.1.1.4　情報処理設備及び通信設備に関連する操作手順には、バックアップを含む、操作上の指示を明記する。

12.1.1.5　情報処理設備及び通信設備に関連する操作手順には、スケジュール作成に関する要求事項（他のシステムとの相互依存性、最も早い作業の開始時刻及び最も遅い作業の完了時刻など。）を含む、操作上の指示を明記する。

12.1.1.6　情報処理設備及び通信設備に関連する操作手順には、作業中に発生し得る、誤り又はその他の例外状況の処理についての指示（システムユーティリティの利用の制限）を含む、操作上の指示を明記する。

12.1.1.7　情報処理設備及び通信設備に関連する操作手順には、操作上又は技術上の不測の問題が発生した場合の、外部のサポート用連絡先を含む、サポート用及び段階的取扱い（escalation）用の連絡先を含む、操作上の指示を明記する。

12.1.1.8　情報処理設備及び通信設備に関連する操作手順には、特別な出力及び媒体の取扱いに関する指示（特殊な用紙の使用、秘密情報の出力の管理（失敗した作業出力のセキュリティを保った処分手順を含む。））を含む、操作上の指示を明記する。

12.1.1.9　情報処理設備及び通信設備に関連する操作手順には、システムが故障した場合の再起動及び回復の手順を含む、操作上の指示を明記する。

12.1.1.10　情報処理設備及び通信設備に関連する操作手順には、監査証跡及びシステムログ情報の管理を含む、操作上の指示を明記する。

12.1.1.11　情報処理設備及び通信設備に関連する操作手順には、監視手順を含む、操作上の指示を明記する。

12.1.1.12　システムの管理活動のための操作手順及び文書化手順は、正式な文書として取り扱い、その手順書の変更は、管理層が認可する。

12.1.1.13　情報システムは、技術的に可能な場合には、同一の手順、ツール及びユーティリティを用いて、首尾一貫した管理を行う。

12.1.2　情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。

12.1.2.1　組織、業務プロセス、情報処理設備及びシステムの変更管理には、重要な変更の特定及び記録を含める。

12.1.2.2　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更作業の計画策定及びテストの実施を含める。

12.1.2.3　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の潜在的な影響（情報セキュリティ上の影響を含む。）のアセスメントを含める。

12.1.2.4　組織、業務プロセス、情報処理設備及びシステムの変更管理には、変更の申出を正式に承認する手順を含める。

12.1.2.5　組織、業務プロセス、情報処理設備及びシステムの変更管理には、情報セキュリティ要求事項が満たされていることの検証を含める。

12.1.2.6　組織、業務プロセス、情報処理設備及びシステムの変更管理には、全ての関係者への変更に関する詳細事項の通知を含める。

12.1.2.7　組織、業務プロセス、情報処理設備及びシステムの変更管理には、うまくいかない変更及びこれに伴う予期できない事象を取り消し、これらから回復する手順及び責任を含む、代替手順を確立することを含める。