12.5.1.7　導入したソフトウェアの管理を維持するために、システムに関する文書化と同様に、構成管理システムを利用する。
12.5.1.8　変更を実施する前に、ロールバック計画を備える。
12.5.1.9　運用プログラムライブラリの更新の全てについて、監査ログを維持する。
12.5.1.10　緊急時対応の手段として、一つ前の版のアプリケーションソフトウェアを保持する。
12.5.1.11　ソフトウェアの旧版は、そのソフトウェアが扱ったデータが保存されている間は、必要とされる情報及びパラメータの全て、手順、設定の詳細並びにサポートソフトウェアとともに保管する。
12.5.1.12　運用システムに利用される業者供給ソフトウェアは、供給者によってサポートされるレベルを維持する。
12.5.1.13　組織は、サポートのないソフトウェアに依存することのリスクを考慮して管理する。
12.5.1.14　新リリースにアップグレードするとの決定には、その変更に対する事業上の要求及びそのリリースのセキュリティ（例えば、新しい情報セキュリティ機能の導入、この版が必要になった情報セキュリティ問題の量及び質）を考慮して行う。
12.5.1.15　情報セキュリティ上の弱点を除去するか、又は低減するために役立つ場合には、ソフトウェアパッチを適用する。
12.5.1.16　供給者による物理的又は論理的アクセスは、サポート目的で必要なときに、管理層の承認を得た場合にだけ許可する。
12.5.1.17　供給者による物理的又は論理的アクセスを許可している間は、供給者の活動を監視する。
12.5.1.18　セキュリティ上の弱点を招く可能性のある認可されていない変更を回避するために、外部から供給されるソフトウェア及びモジュールは、監視し、管理する。

12.6　技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため

12.6.1　利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。
12.6.1.1　技術的ぜい弱性の管理をサポートするために必要となる具体的な情報には、ソフトウェア業者、版番号、配置状況（例えば、どのソフトウェアがどのシステム上に導入されているか。）、及びそのソフトウェアに責任のある組織内の担当者を含める。
12.6.1.2　潜在していた技術的ぜい弱性を特定したときは、適切かつ時機を失しない処置をとる。
12.6.1.3　技術的ぜい弱性の管理に関連する役割及び責任を定める。
12.6.1.4　技術的ぜい弱性の管理には、ぜい弱性監視、ぜい弱性に関わるリスクアセスメント、パッチの適用、資産移動の追跡、及び要求される全ての調整責務を含める。
12.6.1.5　技術的ぜい弱性を特定し、また、それらぜい弱性を継続して認識させるために用いる情報資源（ぜい弱性検査ツールなど。）を、ソフトウェア及びその他の技術（組織の資産目録リストに基づく。）に対応させて特定する。
12.6.1.6　技術的ぜい弱性の情報資源は、資産目録を変更したとき、又は他の新しい若しくは有益な資源を発見したときに更新を行う。
12.6.1.7　潜在的に関連がある技術的ぜい弱性の通知に対処するための予定表を定める。
12.6.1.8　潜在的な技術的ぜい弱性が特定されたときは、組織は、それと関連するリスク及びとるべき処置（例えば、ぜい弱性のあるシステムへのパッチ適用、他の管理策の適用）を特定する。
12.6.1.9　技術的ぜい弱性の扱いの緊急性に応じて、変更管理に関連する管理策又は情報セキュリティインシデント対応手順に従って、とるべき処置を実行する。
12.6.1.10　正当な供給元からパッチを入手できる場合は、そのパッチを適用することに関連したリスクを評価する（ぜい弱性が引き起こすリスクと、パッチの適用によるリスクとを比較する。）。
12.6.1.11　パッチの適用前に、それらが有効であること及びそれらが耐えられない副作用をもたらさないことを確実にするために、パッチを試験及び評価するとともに、利用可能なパッチがない場合は、以下の４点を実施する。
１．そのぜい弱性に関係するサービス又は機能を停止する。
２．ネットワーク境界におけるアクセス制御（例えば、ファイアウォール）を調整又は追加する。
３．実際の攻撃を検知するために、監視を強化する。
４．ぜい弱性に対する認識を高める。
12.6.1.12　修正パッチの適用、その他実施した全ての手順について監査ログを保持する。
12.6.1.13　技術的ぜい弱性の管理プロセスは、その有効性及び効率を確実にするために、常に監視及び評価する。
12.6.1.14　技術的ぜい弱性は、リスクの高いシステムには最初に対処する。
12.6.1.15　技術的ぜい弱性に対する有効な管理プロセスは、ぜい弱性に関するデータをインシデント対応部署に伝達し、インシデントが発生した場合に実施する技術的手順を準備するために、インシデント管理活動と整合させる。
12.6.1.16　ぜい弱性が特定されていながら適切な対応策がない場合には、その状況に対処するための手順を定める。
12.6.1.17　ぜい弱性が特定されていながら適切な対応策がない場合には、組織は、既知のぜい弱性に関するリスクを評価し、適切な検知及び是正処置を定める。

12.6.2　利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。
12.6.2.1　組織は、利用者がインストールしてもよいソフトウェアの種類について、厳密な方針を定め、施行する。
12.6.2.2　特権の許可は最小限にするという原則を適用する。
12.6.2.3　組織は、ソフトウェアのインストールの種類のうち、許可するもの（例えば、既存のソフトウェアの更新及びセキュリティパッチの適用）、及び禁止するもの（例えば、個人利用のためのソフトウェア、潜在的な悪意の有無が不明又はその疑いがあるソフトウェア）を特定する。
12.6.2.4　特権は、関連する利用者の役割を考慮したうえで付与する。

12.7　情報システムの監査に対する考慮事項

目的：運用システムに対する監査活動の影響を最小限にするため

12.7.1　運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。
12.7.1.1　システム及びデータへのアクセスに関する監査要求事項は、適切な管理層の同意を得る。
12.7.1.2　技術監査における試験の範囲を、合意し、管理する。
12.7.1.3　監査における試験は、ソフトウェア及びデータの読出し専用のアクセスに限定する。
12.7.1.4　監査における試験では、読出し専用以外のアクセスは、システムファイルの隔離された複製に対してだけ許可し、それらの複製は、監査が完了した時点で消去するか、又は監査の文書化の要求の下でそのようなファイルを保存する義務があるときは、適切に保護する。