8b-8.8.15　取得したソフトウェアについて、その業者がソフトウェアのセキュリティ更新に関する情報を定常的にリリースし、更新を自動的に適用する機能を提供している場合、組織は、自動更新を使用するかどうかを決定する。

【その他の考慮事項】

8b-8.8.16　監査ログは、技術的ぜい弱性管理で行われる全てのステップについて保持する。

8b-8.8.17　技術的ぜい弱性の管理プロセスは、その有効性及び効率性を確実にするために、定常的に監視し、評価する。

8b-8.8.18　技術的ぜい弱性に対する有効な管理プロセスは、インシデント管理活動と整合させる。

（8b-8.8.18参考）　これは、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提供するためである。

8b-8.8.19　組織が第三者のクラウドサービスプロバイダが提供するクラウドサービスを利用する場合、クラウドサービスプロバイダの資源の技術的ぜい弱性管理は、クラウドサービスプロバイダがその実施を確実に行うことを確認する。

8b-8.8.20　クラウドサービスの利用に関する合意には、次を含める。

a）技術的ぜい弱性管理に対するクラウドサービスプロバイダの責任

b）技術的ぜい弱性に関するクラウドサービスプロバイダの対応を報告するプロセス

（8b-8.8.20参考）　一部のクラウドサービスの場合には、クラウドサービスプロバイダ及びクラウドサービスカスタマにそれぞれの責任が存在する。例えば、クラウドサービスカスタマは、クラウドサービスにおいて使用する自身の資産のぜい弱性管理に責任がある。

8b-8.9　構成管理

管理策：ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視し、レビューする。

目的：　ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。

詳細管理策

【構成管理全般】

8b-8.9.1　組織は、ハードウェア、ソフトウェア、サービス及びネットワークに関して、新しく導入したシステム及び運用システムの存続期間にわたって、定義した構成（セキュリティ構成を含む。）を維持するためのプロセス及びツールを定義し、実装する。

8b-8.9.2　全ての構成変更を良好に管理することを確実にするために、役割、責任及び手順を定める。

【標準テンプレート】

8b-8.9.3　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成のための標準テンプレートを次のように定義する。

a）公開され、入手できる手引を使用する。

b）十分なセキュリティレベルを決定するために、必要な保護のレベルを考慮する。

c）組織の情報セキュリティ方針、トピック固有の方針、標準及びその他のセキュリティ要求事項を支援する。

d）組織の状況において、セキュリティ構成の実現可能性及び適用可能性を考慮する。

8b-8.9.4　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートは、定期的にレビューすることに加えて、新しい脅威又はぜい弱性に対処する必要がある場合、又は新版のソフトウェア若しくはハードウェアを導入した場合に更新する。

8b-8.9.5　ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティを保った構成の標準テンプレートの策定に当たって、次の事項を考慮する。

a）特権的又は実務管理者レベルのアクセス権をもつ識別情報の数を最小限にする。

b）不必要な、使用されていない又はセキュリティが保たれていない識別情報を無効化する。

c）不必要な機能及びサービスを無効化又は制限する。

d）強力なユーティリティプログラム及びホストパラメータ設定へのアクセスを制限する。

e）クロックを同期させる。

f）初期パスワードなどの業者による初期認証情報を導入の直後に変更し、その他の重要なセキュリティ関連パラメータの初期状態をレビューする。

g）既定の使用中断時間の後に、コンピューティング装置・機器から自動的にログオフするタイムアウト機能を作動させる。

h）使用許諾の要求事項が満たされていることを検証する。

【構成の管理】

8b-8.9.6　ハードウェア、ソフトウェア、サービス及びネットワークについて決定した構成を記録し、全ての構成変更のログを維持する。これらの記録はセキュリティを保って保管する。

（8b-8.9.6参考１）　これは、構成データベース又は構成テンプレートなど様々な方法で達成することが可能である。

（8b-8.9.6参考２）　構成の変更は、変更管理プロセスに従う。

（8b-8.9.6参考３）　構成記録には、次の事項を含み得る。

a）資産の最新の管理責任者又は連絡先情報

b）構成の最終変更日

c）構成テンプレートの版

d）その他の資産の構成との関係

【構成の監視】

8b-8.9.7　構成は、包括的なシステム管理ツール群を用いて監視する。

8b-8.9.8　構成設定を検証し、パスワードの強度を評価し、また、実施する活動を評価するために、定期的にレビューする。

8b-8.9.9　実際の構成を、定義した目標テンプレートと比較することが可能である。逸脱には、定義した目標構成を自動適用して、又は逸脱を手動で分析し、是正処置を講じて対処する。