8b-8.8　技術的ぜい弱性の管理

管理策：利用中の情報システムの技術的ぜい弱性に関する情報を獲得する。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し、適切な手段をとる。

目的：　技術的ぜい弱性の悪用を防止するため。

詳細管理策

【技術的ぜい弱性の特定】

8b-8.8.1　組織は、効果的な技術的ぜい弱性管理の前提条件として、正確な資産の目録をもつ。

8b-8.8.2　資産の目録には、ソフトウェア業者、ソフトウェア名、版番号、配置状況、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。

8b-8.8.3　技術的ぜい弱性を特定するために、組織は次の事項を考慮する。

a）技術的ぜい弱性の管理に関連する役割及び責任を定め、確立する。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、更新、資産移動の追跡、及び要求される全ての調整責務が含まれる。

b）ソフトウェア及びその他の技術に関して、関連する技術的ぜい弱性を特定し、また、ぜい弱性を継続して認識するために用いる情報源を特定する。情報源のリストは、この目録を変更したとき、又は他の新しい若しくは有益な情報源を発見したときに更新する。

c）情報システム（その構成要素を含む。）の供給者に、適用される契約に要求事項を含め、ぜい弱性の報告、取扱い及び開示を確実にすることを要求する。

d）ぜい弱性を特定し、ぜい弱性のパッチ適用が成功したかどうかを検証するために、使用している技術に適したぜい弱性スキャンツールを使用する。

e）ぜい弱性の特定を支援するために、力量があり認可された者が、計画され、文書化された、再現可能な侵入テスト又はぜい弱性アセスメントを実施する。この活動はシステムのセキュリティを危うくする可能性があるため、注意を払う。

f）第三者のライブラリ及びソースコードの使用について、ぜい弱性を追跡する。これはセキュリティに配慮したコーディングに含める。

8b-8.8.4　組織は、次の事項のための手順及び能力を開発する。

a）自らの製品及びサービス並びにこれらで使用している外部の構成要素について、ぜい弱性の存在を検知する。

b）内部又は外部の供給元からぜい弱性報告を受け取る。

8b-8.8.5　組織は、調査者及び他の人が問題を報告できるように、ぜい弱性の開示に関するトピック固有の方針の一部として公開連絡先を示す。

8b-8.8.6　組織は、ぜい弱性の報告手順、オンライン報告書式を確立し、適切な脅威インテリジェンス又は情報共有の場を利用する。

8b-8.8.7　組織は、ぜい弱性を適切に修復するために、組織におけるぜい弱性の特定を支援する動機付けとして、報酬を提供するバグ報奨金プログラムの採用を検討する。

8b-8.8.8　組織が力量のある業界団体又は他の利害関係者と情報を共有する。

【技術的ぜい弱性の評価】

8b-8.8.9　特定した技術的ぜい弱性を評価するために、次の手引を考慮する。

a）どのような対応及び修復活動が必要かを決定するために、報告書を分析及び検証する。

b）潜在的な技術的ぜい弱性を特定したときは、それに伴うリスク及び講じるべき処置を特定する。

（8b-8.8.9参考）　この処置は、ぜい弱性のあるシステムの更新又は他の管理策の適用を含む可能性がある。

【技術的ぜい弱性に対処するための適切な対策の実施】

8b-8.8.10　認可された全てのソフトウェアに、最新の承認済みパッチ及びアプリケーション更新を適用することを確実にするために、ソフトウェア更新管理プロセスを実装する。

8b-8.8.11　変更が必要な場合は、元のソフトウェアを保持し、指定された複製に変更を適用する。

8b-8.8.12　全ての変更は、必要に応じて将来のソフトウェアアップグレードに再適用できるように、完全に試験し、文書化する。

8b-8.8.13　必要に応じて、独立した評価機関がソフトウェアの変更を試験し、妥当性を確認する。

8b-8.8.14　技術的ぜい弱性に対処するために、次の手引を考慮する。

a）潜在的な技術的ぜい弱性の特定に対応して、適切に、かつ、時機を失せずに処置を講じる。関係する可能性のある技術的ぜい弱性の通知に対応するためのタイムラインを定義する。

b）技術的ぜい弱性への対処の緊急性に応じて、変更管理に関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、処置を実行する。

c）正当な供給元（組織の内部又は外部の可能性がある）からの更新だけを使用する。

d）更新を適用する前に、それが有効であること及び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、更新を試験し、評価する。

e）リスクの高いシステムには最初に対処する。

f）修復（一般にはソフトウェアの更新又はパッチ）を開発する。

g）修復又は低減策が効果的であるかどうかを確認するために試験する。

h）修復の真正性を検証する仕組みを提供する。

i）利用可能な更新がない場合、又は更新を適用できない場合は、次のような他の管理策を検討する。

1）ソフトウェア業者又はその他の関連供給元が提案する回避策を適用する。

2）そのぜい弱性に関係するサービス又は機能を停止する。

3）ネットワーク境界におけるアクセス制御を調整又は追加する。

4）ぜい弱なシステム、装置・機器又はアプリケーションを、適切なトラフィックフィルタ（ときに仮想パッチと呼ばれる。）を導入して攻撃から保護する。

5）実際の攻撃を検知するために、監視を強化する。

6）そのぜい弱性に対する認識を高める。