品質管理マニュアル

（ペネトレーションテスト編）

2026 年 1 月

株式会社　筑波総合研究所

目　　次

Ⅰ　サービス提供プロセスの管理
1　サービス利用者との侵入試験仕様調整

2　ペネトレーションテストサービスに関する事前説明、見直し時の説明

3　侵入試験に関連するインシデント発生時の対応
(1)インシデント対応手順の整備
(2)インシデント対応体制の整備
(3)顧客への説明と顧客による同意の徴求

4　顧客からの要求、意見、クレーム等への対応
(1)受付窓口の設置
(2)品質管理者による受付内容の確認

Ⅱ　対象システム等に関する調査

Ⅲ　ペネトレーションテスト方法の選定・実施

Ⅳ　アウトプットの管理

Ⅰ　サービス提供プロセスの管理

1　サービス利用者との侵入試験仕様調整

（例：試験計画、試験対象範囲、実施内容、情報の取り扱い）

(1) 手順書等の整備

① 実施計画書の作成

1） 顧客のニーズの把握

・顧客の目的、期待、スコープの理解

・仕様書がある場合：仕様書を熟読し、質問する

仕様書が無い場合：目的、期待、スコープに関しヒアリングし、提案する。

2） 実施内容、実施方法、役割分担、スケジュールを記述

② 手順書の作成

雛形に沿って下記内容の手順書を整備する

・要件毎の実施方法

・実施日程

・試験計画書（試験項目、試験方法）

2　ペネトレーションテストサービスに関する事前説明、見直し時の説明

（例：試験実施により影響が生ずる可能性、すべての脆弱性検出が困難であること）

(1) 顧客への説明

実施する診断の方法、使用するツール、被監査システムへに影響、進め方、報告書のイメージ及び取扱の制限等の説明を行う。

① 実施する監査の方法・使用するツール

② 被監査システムへに影響

③ 進め方：実施計画書作成、事前調査、監査項目提示、実施手順の提示、診断、調書の作成、報告書ドラフト作成、事実確認、報告会

④ 報告書のイメージ：報告書サンプルを提示

⑤ 取扱の制限：関係者以外は取り扱わない。顧客からの条件と、ISMS 体制下で管理

(2) 顧客による同意の徴求

3　侵入試験に関連するインシデント発生時の対応

（異常時の検知、問題の切り分け、責任範囲の明確化、復旧レベル）

(1)インシデント対応手順の整備

①顧客へ実施内容と実施時間、リスクを説明

②一般的なリスクの回避方法を説明し、顧客側の対応を依頼する

(2)インシデント対応体制の整備

①試験当日の連絡体制を確認

②開始、正常診断可否、終了の報告

(3)顧客への説明と顧客による同意の徴求

上記(1)(2)の内容を顧客に説明し、同委の徴求を行う

4　顧客からの要求、意見、クレーム等への対応

(1)受付窓口の設置

品質管理責任者とする。

(2)品質管理者による受付内容の確認

受付内容と対処内容を記録し、ISMS 責任者へ報告する。

Ⅱ　対象システム等に関する調査

1　ネットワーク構成、システム構成、重要情報等の調査

(1) ネットワーク構成図、システム構成図

① ネットワーク構成図

インターネットとの接続状況

他システムとの接続状況

セグメンテーション、ネットワーク分離方法

② システム構成

(2) 侵入試験を実施するためのシステムの動作の確認方法

① ルールセット

何をしてよいか／してはいけないか」「どこまで許されるか」「問題が起きた場合どうするか」を事前に明文化した合意文書を作成する。

② システム設定

1) ハードウェア

本番／検証／ステージングの別

試験実施時間帯（業務時間外など）

冗長構成の有無（Active/Standby 等）

フェイルオーバー設定の確認

2) 監視

IDS / IPS / WAF / EDR の有効・無効

自動遮断（Block / Quarantine）の有無

アラート通知先・通知方法

③ ログ管理

認証ログが取得されているか

攻撃トラフィックが記録されるか

SIEM 連携の有無

ログ保持期間

2　テストする必要があるシステムとデータの特定

テストする必要があるシステムとデータを特定し、テスト目標と目的を明確にする。

Ⅲ　ペネトレーションテスト方法の選定・実施

1　想定されている脅威

下記基準に基づく

【Web アプリケーション脆弱性診断において、次に示す内容相当の診断を行う】

- OWASP の定める ASVS（Application Security Verification Standard）レベル１以上
- 独立行政法人情報処理推進機構による「ウェブ健康診断仕様」が定める診断内容
- OWASP が定める「Security Testing Guideline」
- 日本セキュリティオペレーション事業者協議会及び OWASP による脆弱性診断士スキルマッププロジェクトが定める「脆弱性診断ガイドライン」

【Web アプリケーション脆弱性診断において、次に示すツールを使用して診断を行う】

- OWASP ZAP

【プラットフォーム脆弱性診断において、次に示すツールを使用して診断を行う】

- Nessus

【ペネトレーションテストにおいて、次に示す基準を使用して診断を行う】

- NIST SP800-115（Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards and Technology）
- Penetration Testing Execution Standard（PTES）
- MITRE ATT&CK に示されている攻撃手法や技術

2　サービス実施方法に関する内容

- テスト方法の選定は、契約内容や事前に把握した事項又は各種の事前調査結果からの脅威のモデリング等に基づいて行う
- ペネトレーションテスト（侵入試験）サービスで提供する検査のプロセスは、前述１に定める基準又は同等のものとする
- 実施するテスト方法には、情報セキュリティサービス基準 2-2(1)ア(イ)のａからｅまでに相当するテストを１つ以上含む
- 品質管理者によるレビュー

Ⅳ　アウトプットの管理

1　サービスの実施結果を報告するための文書の作成（例：試験結果報告書、報告会等）

- 試験結果を PTES（Penetration TestingExecution Standard）の基準または同等以上の報告書作成基準に基づき、「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示第 3 版」別表の内容を満たす試験実施報告書としてとりまとめる
- 当該案件に従事した者以外の者が行う実施結果文書の内容レビュー
- 試験結果に関する報告会の開催

２　顧客の情報を保護するための手段

・ペネトレーションテスト（侵入試験）サービスで使用した顧客の情報を保護するための手続の内容、手続きの実効性を確認する監査実施方法など

以上