# ペネトレーションテスト（侵入試験）サービス仕様

## 1. サービスの目的

本サービスは、**攻撃者の視点から対象システムに対する侵入可能性および業務影響を検証し、実効性のあるセキュリティ対策の有無を確認すること**を目的とする。

本サービスは、**脆弱性の有無を列挙すること自体を目的とせず**、侵入・権限昇格・情報到達等の **影響確認** を重視する。

## 2. 準拠基準・参照ガイドライン

本サービスは、以下の基準を参照して実施する。

- NIST SP 800-115
- OWASP Testing Guide（Web/API 対象時）
- 組織が定める情報セキュリティ規程・試験ルールセット

## 3. サービス範囲（Scope）

### 3.1 対象

- ネットワーク（外部／内部）
- Web アプリケーション
- API
- サーバ（OS／ミドルウェア）
- クラウド環境（IaaS / PaaS）

### 3.2 対象外（原則）

- 明示されていないシステム
- DoS／DDoS を目的とする試験
- 本番データの削除・改ざん

## 4. テスト方式

| 区分 | 内容 |
|---|---|
| ブラックボックス | 事前情報なし |
| グレーボックス | 一部情報・認証情報あり |
| ホワイトボックス | 設計・構成情報あり |

※方式は事前合意により決定する。

## 5. サービス内容（工程別）

### 5.1 事前準備（Planning / Preparation）

- スコープ定義
- ルールセット確認
- システム設定・稼働状態の確認
- 緊急連絡体制の確立

### 5.2 情報収集・調査

- アセット把握
- サービス／ポート確認
- 公開情報・構成情報の収集

### 5.3 侵入試行（Exploitation）

- 脆弱性の悪用可否確認
- 認証回避・突破試行
- 設定不備の悪用

### 5.4 権限昇格・横展開

- 管理者権限取得可否
- 他システムへの影響範囲確認

### 5.5 影響評価

- 情報閲覧・取得可否
- 改ざん・操作可能性
- 業務影響の有無

## 6. 禁止事項（安全確保）

- サービス停止を引き起こす攻撃
- データ破壊・恒久的変更
- マルウェア常駐
- 未承認の社会的エンジニアリング

※業務影響が懸念される場合、直ちに試験を中断する。

## 7. 合否判定基準（重要）

| 判定条件 | 結果 |
|---|---|
| 管理者権限の取得 | Fail |
| 機密情報への不正到達 | Fail |
| 権限外操作が可能 | Fail |
| 侵入不可・影響なし | Pass |

※CVSS は参考情報とし、**合否は業務影響ベースで判断**する。

## 8. 成果物（Deliverables）

### 8.1 試験報告書

- 試験概要・範囲
- 実施手法
- 再現手順
- 影響評価（機密性・完全性・可用性）
- 是正策（技術的・運用的）

### 8.2 エグゼクティブサマリー

- 経営層向け要約
- 重大リスクの整理
- 優先対応事項

## 9. ログ・証跡管理

- 試験ログの取得
- 証跡の安全な保管
- 秘密情報のマスキング
- 提供データの返却・破棄

## 10. 責任分界

| 項目 | 責任 |
|---|---|
| 試験実施 | ベンダ |
| 業務影響判断 | 委託側 |
| 是正対応 | 委託側 |
| 試験中断判断 | 双方協議 |

以上