ペネトレーションテスト

やり方の全体像

計画から報告まで、何をどう進める？

4 フェーズ・シナリオ設計・ツール・資格・案件単価を解説



手順がバラバラになるんでしゅ…

型を押さえれば迷わん。任せろ。



【解説に入る前に】サービスのご紹介

セキュリティプロ・フリーランス

セキュリティに特化したフリーランス案件の
マッチングサービス

- 最高月収 150 万円・月額 80 万円以上の案件が 80% 以上
- リモート率 80% 以上、フルリモート案件多数
- セキュリティに精通した専任エージェントが営業・単価交渉・契約を代行

詳細を見る →

セキュリティプロ・テンショク

セキュリティエンジニア / コンサルタントに
特化した転職エージェント

- 最高想定年収 1,200 万円・利用者の 85% 以上が年収アップ
- 取扱求人の約 7 割が非公開求人
- 技術がわかるアドバイザーが書類添削・面接対策・年収交渉を代行

詳細を見る →

**どちらも登録・利用は完全無料。在職中・フルリモート希望でも相談できます。
まずは市場価値の無料相談から。**

© 2026 スプラッシュエンジニアリング

脆弱性診断とペネトレーションテストの違い

脆弱性診断

網羅・洗い出し

・弱点の一覧化が目的
・広く浅く検査
・「穴の数」を見る

VS

ペネトレーションテスト

侵入シナリオの実証

・侵入可否と被害範囲の実証
・シナリオに沿って深く追跡
・「その穴から入れるか」を見る



違いの核心

問いが違うから手順が変わる補完関係

ペネトレーションテストが答える 4 つの問い

侵入経路の特定

どこから侵入されるか。リスク優先順位づけに直結

被害範囲の把握

侵入後どこまで広がるか。既存対策の実効性を確認

検知・対応力の確認

侵入を正しく検知し対応できるか。組織の信頼性向上

4 つを明確にすることで導入効果が最大化



4 フェーズで進むペネトレーションテスト

1. **計画**
   スコープ・ルール・法的合意を書面で固める
2. **探索**
   OSINT ・スキャン・脆弱性分析で攻撃仮説を構築
3. **攻撃**
   エクスプロイト・権限昇格・横展開でゴールへ到達
4. **報告**
   経営サマリ＋技術詳細の 2 層構成で再発防止に落とし込む

この 4 段階が骨格だ。外すな。



フェーズ１・２：計画と探索の進め方



計画（Planning）

スコープ・禁止事項・緊急連絡先・書面許可の取得



探索（Discovery）

OSINT 収集・ポートスキャン・脆弱性の優先度付け



計画の核心

計画省略が違法行為・本番停止事故の引き金

フェーズ３・４：攻撃と報告の進め方

攻撃（Attack）

エクスプロイト→権限昇格→横展開→目標到達の段階的実施



報告（Reporting）

２層レポート＋再発防止アクションまで明記

報告の核心

侵入成功は途中経過。改善アクションで完成

攻撃シナリオ設計：起点と目標

攻撃の起点

外部起点

公開資産スキャンからの侵入確認

内部起点

社内侵入済み前提での AD 権限拡大

端末感染起点

1 台の PC からの被害範囲測定

逆算で設計



攻撃の目標

ドメイン管理者権限

AD 全体の制御の掌握

機密情報の持ち出し

顧客データ・設計情報への到達

基幹システムへの到達

業務停止に至る中枢の掌握

情報開示レベルで選ぶ３つの手法

ブラックボックス

外部攻撃の再現

・事前情報なし
・実際の外部攻撃に近い再現性
・発見範囲は期間に依存

VS

ホワイトボックス

網羅的・深い検証

・内部情報をすべて開示
・設計レベルから深く検証
・工数は最大



手法選択の核心

目的・予算・期間の３軸で選択。中間はグレーボックス

フェーズ別の主要ツール

探索フェーズ

Nmap ・ OSINT ツール・脆弱性スキャナが基本



攻撃フェーズ

Kali ・ Metasploit ・ Burp Suite が代表

ツールの核心

ツールは手段。シナリオと手順の理解が先

独学でスキルを積む学習順序



1. **ラボ環境整備**
   仮想環境・ CTF プラットフォームで合法な練習場を確保
2. **情報収集・スキャン**
   対象の調べ方と入口の見つけ方を体系的に習得
3. **脆弱性分析**
   弱点の評価と優先度付けの考え方を習得
4. **悪用・権限昇格**
   実際の侵入手法を合法な環境での実践
5. **報告書作成**
   結果の整理と改善提案のまとめ方の習得

案件につながる資格と単価感

評価される資格

OSCP

23h45m の実技試験。侵入から報告書まで一貫評価

情報処理安全確保支援士

登録者 26,453 名の国家資格（2026 年 4 月）

市場は人材不足



フリーランス案件の単価感

中央値

月額 92.5 万円（公開案件 118 件）

レンジ

月額 50 万〜 180 万円

高単価傾向

要件定義・ PMO 等の上流工程

まとめ｜ペネトレーションテストのやり方を案件参画につなげる

- 手順の骨格は計画・探索・攻撃・報告の 4 フェーズ（NIST SP 800-115）
- 起点と目標を定めた攻撃シナリオ設計が成否の鍵
- 資格と実務スキルの両輪が、市場参入への最短ルート

NEXT ACTION

まずは市場価値の無料相談・登録

セキュリティプロ・フリーランス ＞

セキュリティプロ・テンショク ＞

