

ペンテスターとは？

仕事・年収・資格・なり方

未経験からプロへの実践ロードマップ

正社員～フリーランスの年収相場と資格選び



ペンテスターって何でしゅ？

攻撃のプロになる道を教える



【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。

● ペンテスターの仕事と役割



ペンテスターとは
企業から依頼を受け侵入テストを行う専門家



ホワイトハッカーとの違い
倫理的ハッカーの中で侵入テストを専門とする職種



本質
許可と期間内でプロとして攻撃し価値を生む仕事

● テストの進め方・4つのフェーズ

1

偵察

対象システムの情報収集と攻撃面を特定する

2

侵入

発見した脆弱性を実際に悪用してアクセスする

3

権限昇格

侵入後の被害拡大範囲を検証する

4

報告

発見事項をリスク評価とともに報告書にまとめる

報告で初めて価値が生まれる



● ペンテスター vs 脆弱性診断士

脆弱性診断士

ツール中心の網羅的診断

- ・脆弱性の洗い出しが目的
- ・ツールスキャン中心

VS

ペンテスター

手動テスト中心の侵入証明

- ・侵入しビジネス影響を証明
- ・攻撃シナリオを独自構築



差のポイント

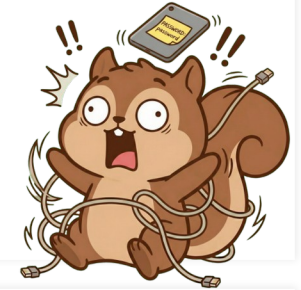
診断は穴を見つけ、ペンテストは侵入で被害を証明

● 正社員ペンテスターの年収レンジ



未経験～3年

400～600万円（Sler・ベンダー）



シニア（7年以上）

900～1,200万円以上（外資コンサル）



中堅の実態

中堅3～7年は600～900万円が市場相場

● フリーランスの月額単価相場



専門家の単価目安

公開案件 118 件の中央値 92.5 万円・ 50 ～ 180 万円



案件の取り方

エージェント経由か直請けで単価が大きく変わる



転身メリット

正社員求人は中央値 685 万円、フリーランスは 12 か月換算 1,110 万円



● 実務で評価される資格 5 選

1

OSCP

24 時間実技試験。ペンテスト業界で最重要の資格

2

CEH

外資・グローバル案件で評価される知名度の高い資格

3

GPEN

SANS トレーニング連動、企業負担向け実践資格

4

PenTest+

ベンダー中立の国際資格。ペンテスト基礎力を証明する

5

登録セキスぺ

国内唯一の国家資格。OSCP と組み合わせで最強

● 未経験からペンテスターへの道

1

0～6ヶ月

Linux・NW基礎・Python入門でインフラの土台を固める

2

6～12ヶ月

TryHackMeやSecurity+でセキュリティ基礎を習得

3

1～2年目

HackTheBoxで実践力を磨き脆弱性の原理を理解する

4

2～3年目

脆弱性診断で実務経験を積み OSCP 取得を目指す

2～3年で目指せるでしょ



● 現役エンジニアからの転身戦略

活かせる現在のスキル



SOC アナリスト

ログ分析・攻撃パターン知識



脆弱性診断士

脆弱性理解・レポーティング力



インフラエンジニア

NW・サーバー構築の深い知識

追加で必要なスキル



攻撃実行力

権限昇格・AD 攻撃の手法習得



シナリオ構築力

複数脆弱性を連鎖させる創造的思考



OSCP 取得

3～6ヶ月集中学習で実力を証明する

転身の最短ルート



● ペンテスト需要が拡大する 3つの背景



深刻な人材不足

日本 42% が必要人材を確保できず世界平均 29% を上回る



法規制の義務化

PCI DSS ・ 金融庁ガイダンスがペンテスト実施を要求



AI 時代の需要増

AI が代替できない創造的攻撃シナリオの価値が上昇

ISC2 調査：日本 42% ・ 世界平均 29% が人材不足



● ペンテスターのキャリア発展パス

1

レッドチーム

組織全体を対象とした高度な攻撃シミュレーションを指揮

2

セキュリティコンサル

ペンテスト知見を活かし経営層へ戦略的アドバイスを行う

3

CISO

攻撃者視点を持つ CISO は希少で市場価値が非常に高い

4

フリーランス独立

専門性を武器に複数クライアントへサービスを提供する

どちらの道も実績が土台だ



● まとめ | ペンテスターへの最短ルート



まず OSCP を最優先に取得し実力を客観的に証明する



脆弱性診断・SOC で土台を固めてからペンテストへ挑戦



Bug Bounty と技術発信で専門性を外部にアピールする

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 >](#)

