

ペネトレーションテスト

費用の全解剖

スコープと人で決まる？見積もりで損しない方法

費用レンジ・4 要因・節約法・単価実態を解説



結局いくらかかるんでしょ？

スコープと人で決まる。それだけだ。



【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。

● 対象別の費用レンジをつかむ

アプリ系



Web アプリ（小規模）

50 万～ 100 万円。画面・機能数が多いほど上がる



Web アプリ（中規模）

150 万～ 300 万円。認証・決済など重要機能含む



スマホアプリ

80 万～ 200 万円。iOS/Android 両対応で増加

ネットワーク系



ネットワーク（外部）

10 万～ 50 万円。公開 IP の数が費用に直結



ネットワーク（内部）

50 万～ 800 万円。規模により大幅に変動

複数社公開情報をもとにした目安



● 脆弱性診断 vs ペネトレーションテスト

脆弱性診断

広く・浅く・網羅的

- ・ 自動ツールによるスキャン中心
- ・ 既知の弱点を一覧化するベースライン
- ・ 比較的短時間・低コスト

ペネトレーションテスト

狭く・深く・シナリオ型

- ・ 熟練者の手動工数が中心
- ・ 攻撃の実現可能性を徹底検証
- ・ 目標達成できるかを問うリスク評価

VS



違いの核心

目的が違えば手間も違う。広さか深さか、目的から逆算して選べ。

● 費用を左右する 4 つの要因

1

対象の範囲・規模

IP 数・画面数が増えるほど工数が直接積み上がる

2

テスト手法の選択

ブラック / グレー / ホワイトで深度と工数が変わる

3

担当者のスキル

熟練者の手動工数が主体。誰がやるかで成果も変わる

4

報告書と再検証

リテストや対策サポートの有無が総額を大きく変える

この 4 点で読めば見積書は解読できる。



● テスト対象の範囲と規模が費用を動かす



スコープが広がると費用が増える

IP 数・画面数・連携範囲が直接工数に反映される



範囲を絞ると費用を抑えられる

守る対象を明確にするほど狙いを絞った設計ができる



スコープの核心

スコープは先に自分の言葉で定義しろ。丸投げると膨らむ。

● テスト手法 3 種類と深度の違い



ブラックボックス

事前情報なし。外部攻撃者の視点で侵入経路を探す



グレーボックス

一般ユーザー権限など一部情報を与えてテスト



ホワイトボックス

設計書・ソースコードを開示して内部から徹底検証

深く攻めるほど工数は増える。予算と目的のバランスで手法を選べ。



● 担当エンジニアのスキルと実施体制



人の実力が成果と費用を決める

自動ツールが届かない経路を掘り当てるのが人の仕事



体制が単価に反映される

人数・稼働日数・資格水準がそのまま金額に出る



人材の核心

値段の差は腕の差だ。同じツールを渡しても結果は変わる。

● 報告書の品質と再検証の落とし穴



報告書の詳細度が対策の質を決める

再現手順なき報告書は何をどう直すか分からない



リテストが別料金の罠

初回が安くても再検証が高額オプションでは総額が増える



成果物の核心

安さだけで選ぶな。対策に使えない報告書にカネを払うな。

● 見積もりで失敗しない3つのチェックポイント

1

スコープを先に固める

守りたい資産と想定脅威を社内で言語化してから発注する

2

内訳と成果物を確認

リテスト・報告会・サポートが含まれるかを分解して見る

3

同条件で相見積もり

前提を統一してから比べる。条件バラバラの比較は無意味だ

同じ土俵に乗せてから比べろ。



● 費用を賢く抑える 3つの進め方



範囲に優先順位をつけて絞る

被害インパクトが大きい資産を起点に重点検証する



診断と組み合わせる

脆弱性診断で広く押さえ、ペンテストを重点シナリオに絞る



定期実施で平準化

節目ごとの継続実施で手戻りと単発コストを削減する



削るより配分する。重点に人手を集中させてこそ費用対効果が出る。



● 費用の正体はホワイトハッカーの人件費



人的工数が費用の主成分

ライセンス費より稼働費が主。スキルが値札になる



攻撃シナリオの設計と報告書

機械では代替できない作業に最も多く時間が割かれる



費用の核心

費用＝人件費。その値札はスキルの値札そのものだ。

● フリーランス単価の実態と求められるスキル

月額単価の目安



全体中央値

92.5 万円（50 ～ 180 万円）当社公開案件 118 件



要件定義・PMO

中央値 100 万～115 万円と上位帯を形成



設計・構築・運用

中央値 90 万～92.5 万円。実力で上振れる

受け取る側に回れる



案件で評価されるスキル



攻撃シナリオの設計力

脆弱性を発見し侵入経路を描く実務力



レポーティング力

リスクを言語化し対策まで示せる報告書



実務経験と資格

OSCP・情報処理安全確保支援士が参考水準

● まとめ



費用はスコープと担当者の2点で決まる。目安は数十万～数百万円



見積もりはリテスト・報告会の有無まで内訳を分解して比べる



スキルを持てば払う側から受け取る側へ。月額中央値は 92.5 万円

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 >](#)

