

脆弱性診断士とは

年収と資格の実態

正社員約 610 万円・フリーランス月額中央値 92.5 万円の現実

資格の難易度・キャリアパス・単価を最新データで解説



国家資格じゃないと意味ないでしょか？

診れる人材が足りていない現実を知れ



【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。

● 脆弱性診断の基本業務フロー

1

情報収集

診断対象・前提条件を整理し、スコープを確定する

2

診断作業

ツールと手動を組み合わせ弱点を網羅的に洗い出す

3

トライアージ

検出結果から誤検知を精査しリスクを評価する

4

レポート作成

リスクと対策を開発者が直せる粒度でまとめる

穴を見つけ直すまでが仕事だ



脆弱性診断とペネトレの違い

脆弱性診断

網羅的な弱点の洗い出し

- ・ 弱点の網羅的な洗い出し
- ・ ツール＋手動で広く確認
- ・ 弱点一覧と改善提案が成果物

VS

ペネトレーションテスト

攻撃者視点で侵入可否を検証

- ・ 想定シナリオで深く侵入試行
- ・ 攻撃者視点で実際に侵入を試す
- ・ 侵入経路と被害想定が成果物



役割の核心

診断は健康診断、ペネトレは実地検証

● Web 診断と NW 診断の 2 系統

Web アプリ脆弱性診断



主な対象

SQLi ・ XSS など OWASP Top10



主なツール

Burp Suite で通信改ざん検証



手動の強み

ビジネスロジックの不備を精査

NW ・ プラットフォーム診断



主な対象

OS やミドルウェアの設定不備



主な手法

ポートスキャン + CVE 照合



必要な知識

通信 ・ サーバー運用の理解

2 系統を把握せよ



● ツール診断と手動診断の使い分け



ツール診断の役割

広範囲を高速網羅・典型脆弱性を検出



手動診断の役割

仕様を読んだ深掘り・誤検知の精査



共存の核心

ツールは広く浅く、人は狭く深く



● 診断士に求められる 3つのスキル



技術スキル

HTTP ・ OS ・ DB など攻撃の仕組みを理解



診断実践力

ツール操作 ・ 手動確認 ・ 誤検知の精査



報告 ・ 伝達力

CVSS と優先度付けで改善行動を促す



3つが揃って初めて単価に直結する診断士として通用する

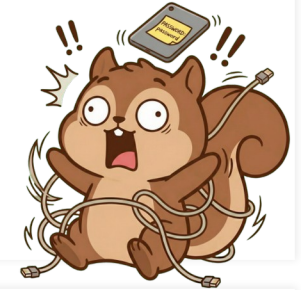


● SecuriST 認定の概要と特徴



2 区分の CBT 試験

Web ・ NW の 2 種類で随時受験が可能



受験料と試験形式

29,700 円 ・ 選択式 30 問 ・ 60 分



位置づけの核心

診断実務の基礎を証明する国内の登竜門

● 国家資格と民間資格の関係

情報処理安全確保支援士

国家資格・体系的知識を証明

- ・ IPA 管轄のセキュリティ国家資格
- ・ 登録・定期講習の維持が必要
- ・ 試験難度高め・知識の網羅性

VS

SecuriST 認定

民間認定・実技スキルを証明

- ・ GSX 提供・随時 CBT 受験可能
- ・ 実務直結の出題範囲が特徴
- ・ 未経験からの現実的な登竜門



補完の核心

知識は支援士・実技は SecuriST で証明

● 海外資格 CEH ・ OSCP の難易度比較



CEH (中級)

知識証明として国際的に認知・費用高め



OSCP (高難度)

実際に侵入成功が求められる実技試験



習得の鉄則

SecuriST で基礎→実績→OSCP が堅実



● 正社員とフリーランスの年収比較

正社員の年収相場



平均年収

正社員は公的統計で約 610 万円（令和 7 年）



上限レンジ

経験次第で 1,000 万超も存在



働き方

安定雇用・福利厚生が充実

フリーランスの月単価



中心レンジ

月額中央値 92.5 万円（50 ～ 180 万円）



想定年収

中央値のまま 12 か月で年収 1,110 万円



働き方

リモート可・週数日も選択可

需要過多が続く市場



● 未経験から目指す 4 つのステップ

1

基礎インプット

HTTP ・ OS ・ DB など通信と開発の基礎を習得する

2

演習実践

やられアプリで手を動かし攻撃手法を体感する

3

資格取得

SecuriST 認定でスキルを客観的に証明する

4

実務参画

診断会社への就職・案件参画で実績を積み上げる

学んだら必ず手を動かせ



● まとめ | 脆弱性診断士のスキルはフリーランスで最も活かせる



診断士は職種呼称・SecuriST が国内の実技登竜門・支援士と補完関係



正社員約 610 万円・フリーランス月額中央値 92.5 万円。需要過多の追い風市場が続く



Web + NW + 報告力の掛け合わせが単価上昇への現実的なルート

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 >](#)

