

Splunk 資格で 案件単価を上げる

難易度・勉強法・SOC 案件単価の完全ガイド

月額中央値 95 万円の Splunk 案件と資格活用を解説



どれから取ればいいでしゅ…

入口はひとつだけだ



【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。

● Splunk と SIEM 基盤の役割



ログ集約・検索基盤

大量ログを SPL で検索・集計・可視化する



SIEM 基盤として活用

SOC/CSIRT がセキュリティ監視に使う基幹ツール



Splunk の核心

規模の大きい現場で通用するスキルの証明になる

● Splunk 資格が評価される 3 つの背景

1

人材不足の深刻化

セキュリティ人材の需要は近年も拡大が続き人材不足は慢性化している

2

SIEM 運用需要の増加

SOC/CSIRT による常時監視体制が一般化し SIEM 人材の価値が上昇した

3

実力の共通言語

資格でスキルを客観的に示せるため採用・案件選定での差別化になる

できる奴が選ばれる時代だ



● Splunk 認定資格の 4 つの階層

1

User 認定

入門。基本検索・レポート・ダッシュボードの操作を習得する

2

Power User

実務向け。SPL コマンドとナレッジオブジェクトを実践的に活用する

3

Admin 認定

運用管理者向け。データ投入・ユーザー管理・運用設定全般を担う

4

Architect

設計者向け。分散環境の設計・サイジングを担う最上位認定

まず User から始めろ



● セキュリティ向け専門認定 3 選



ES 認定（SOC 向け）

SIEM 運用・脅威検知ルール設計をカバーする



SOAR 自動化開発

インシデント対応の自動化開発スキルを証明する



サイバー防御認定

防御分析と防御エンジニアの 2 種が最新ラインナップ



Core 認定で土台を固めてから専門認定を重ねるのが SOC 案件の近道



● 難易度の目安と初心者の入口



入門レベル（User）

基本操作の理解で挑戦可能。実機経験不要で着手しやすい



上位レベル（Admin 以上）

実機運用経験・分散環境の知識が前提となる



入門の鉄則

Core Certified User から始め一段ずつ上げるのが現実的

● 受験料・有効期限・更新要件



受験料の目安

1 試験あたり約 130 米ドル（日本円で 2 万円前後）



有効期限と更新

最上位資格基準で約 3 年。上位試験合格で再認定可能



更新の合理性

有効期限は常に最新スキルを保ち続けている証明にもなる

● Splunk 資格の勉強法 2 択

公式トレーニング活用



無料 e-learning

基礎概念から入門操作まで学べる



有料コース

実機演習で実践力を強化できる



日本語対応あり

英語不安でも着手しやすい環境

独学ロードマップ



無料検証環境

個人向け無料版で SPL を実機練習



サンプルログ実習

ダッシュボード・アラートを自作



公式ドキュメント

分からない構文を都度確認する

理論 + 実機が近道



● SOC/SIEM 案件の単価相場



フリーランス全体相場

全体は中央値 92.5 万円。 Splunk 案件 6 件は中央値 95 万円



Splunk セキュリティ案件

月 60 万～ 110 万円・中央値 95 万円。専門性で上振れ



単価の核心

希少性と専門性が、全体の中央値を上回る単価につながる

● 正社員 vs フリーランスの収入構造

正社員

安定収入モデル

- ・ 固定年収 + 賞与で安定
- ・ 組織の評価制度に準拠
- ・ 福利厚生・社会保障あり
- ・ 昇給・昇進でキャリアを伸ばす

VS

フリーランス

専門性直結モデル

- ・ 単価 × 稼働で収入が決まる
- ・ 専門性が単価に直結
- ・ 高単価案件へのアクセス
- ・ 資格が指名獲得の武器になる



判断の軸

資格 + 実務の組み合わせで両ルートとも市場価値が上がる

● 資格を案件アピールに変換する法



要件への対応づけ

資格名を案件の必須・歓迎要件に直接紐づけて記述



担当フェーズの明示

設計・構築・運用を明確に書き分けて実績を具体化する



アピールの核心

資格は実務の裏付け。経歴と組み合わせて信頼性を補強する

● まとめ



Core Certified User を起点に上位認定を段階的に積み上げる構成



受験料約 130 米ドル・有効期限 3 年の更新型認定。常に最新スキルの証明になる



資格単体でなく実務との組み合わせで、中央値月 95 万円の Splunk 案件に到達する

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 >](#)

