# AWS セキュリティ

# サービス完全整理

種類が多すぎて、どこから手をつける？

責任共有モデル・5 カテゴリ・設定ミス・案件単価を解説




どこから覚えればいいでしゅ？

地図で捉えれば一気に整理できる。



# 【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。**

© 2026 スプラッシュエンジニアリング

# 責任共有モデル：守る範囲の分担

## AWS の責任

### クラウドのセキュリティ

・データセンターの物理的な保護
・ハードウェア・ネットワーク基盤
・ホスト OS と仮想化レイヤー

VS

## 利用者の責任

### クラウド内のセキュリティ

・ゲスト OS のパッチ適用
・ IAM による適切な権限付与
・設定・データ管理・暗号化



**責任の核心**

**設定ミスは利用者側の責任領域**

# セキュリティサービスの 5 カテゴリ

1. **ID ・アクセス管理**
   誰が何にアクセスできるかを制御
2. **検出と対応**
   脅威や不審な挙動を見つけて対処
3. **データ保護**
   保存・伝送されるデータと機密情報を守る
4. **コンプライアンス**
   設定や構成を継続的に評価・監視
5. **ネットワーク保護**
   通信経路や Web アプリを攻撃から防御



# ID・アクセス管理の 3 サービス

## IAM

ユーザー・ロール・ポリシーで最小権限を実現

## IAM ID センター

複数アカウントへのアクセスを一元管理

## Organizations

マルチアカウントを統制し組織単位でルールを適用

最小権限が崩れると他の防御も無意味だ



# 脅威の検出・監視の 3 サービス

## GuardDuty

ログを解析し不審な通信・挙動を自動検出

## Inspector

EC2 やコンテナの脆弱性を継続的にスキャン

## Detective

検知した イベントの原因と関連を深掘り調査

検知→脆弱性→調査でつながる 3 点だ



# データ保護・暗号化の 3 サービス

## KMS

暗号鍵を安全に管理しデータ暗号化を支援

## Macie

S3 内の個人情報など機密データを自動で検出

## SecretsManager

API キー・パスワードを安全に保管・管理

**認証情報のソースコード直書きは厳禁だ**



# ネットワーク・アプリ保護の 3 サービス

## WAF

SQL インジェクションなど Web アプリへの攻撃を防御

## Shield

大量アクセスによる DDoS 攻撃から防護

## Network FW

VPC 通信をフィルタリングし不要な通信を遮断

階層ごとに役割を持つ多層防御が肝だ



# 統合管理・監査の 3 サービス

## Security Hub

各サービスの検出結果を集約しセキュリティ状態を可視化

## Config

リソース構成を評価し変更を継続的に追跡

## CloudTrail

API コールを記録し監査ログとして保持

**3 つが揃って初めて成立する運用体制だ**



# 起きやすい設定ミス 4 パターン

1. **S3 の公開設定**
   意図せずバケットを公開状態にしデータが外部閲覧可能に
2. **IAM の過剰権限**
   必要以上の操作を許し攻撃者に広い侵害範囲を与える
3. **SG 全開放**
   0.0.0.0/0 で通信を無制限に受け入れてしまう状態
4. **認証情報の直書き**
   コードやリポジトリに残ったキーが攻撃者に悪用される

全部やってたでしゅ…！



# 設定ミスを検知・是正するサービス

Config ・ IAM アクセス分析

設定の逸脱・不要な外部公開を継続的に自動評価



Security Hub

各チェック結果を集約し優先度つけて可視化

防御の核心

仕組みで継続的にチェックし逸脱を即検知

# AWS セキュリティ案件の単価感

## 工程別の単価中央値

**要件定義フェーズ**
中央値 112.5 万円 / 月

**設計・構築・運用**
各中央値 90 万円 / 月

**コンサルタント**
中央値 120 万円 / 月

上流が高単価だ



## 求められるスキルセット

IAM 設計・ネットワーク分離
**クラウドセキュリティ設計・構築**

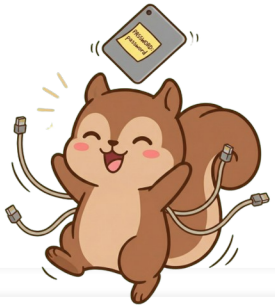
SOC 運用・ログ監視
**検知と対応の運用経験**

脆弱性診断・レビュー
**設定の妥当性を継続的に確認**

# AWS Certified Security （SCS-C03）

試験概要

65 問・ 170 分・合格スコア 750 点・受験料 300USD



想定経験水準

クラウドセキュリティ関連の 3 ～ 5 年相当の経験

活かし方の核心

資格と実績の両輪でスキルを証明

# まとめ｜AWS セキュリティを役割で捉え次の一歩へ

- 5 カテゴリの地図でサービスを役割ベースに整理
- 設定ミスは利用者責任・仕組みで自動防御が必須
- 資格と実績の両輪でフリーランス・転職市場で評価

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 ＞

