AWS セキュリティ

主要サービスと対策

設定ミスで漏れる？本当の守り方

責任共有モデル・ 10 サービス・案件直結スキルを網羅

AWS に任せれば OK でしゅ？

守るのはお前の責任だ。

【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。**

責任共有モデルの境界線

AWS の責任範囲

クラウド本体を守る

・データセンター・物理設備
・ハードウェア・ネットワーク
・ハイパーバイザー管理

VS

ユーザーの責任範囲

クラウド内を守る

・ゲスト OS のパッチ管理
・ IAM 権限・セキュリティグループ
・データ暗号化設定

境界の核心

同じ AWS でも EC2 と S3 では守備範囲が変わる。

責任誤解が招く 3 大事故

S3 公開設定ミス

ブロックパブリックアクセス未設定でデータが外部に漏れる

IAM 過剰権限

侵害時に被害がアカウント全体へ拡大してしまう

アクセスキー漏えい

コード直書きや長期放置が情報漏えいの温床になる

「AWS だから安全」という思い込みが生む、ユーザー責任の盲点。

セキュリティサービス 4 系統

1. **ID ・権限保護**
   IAM ・ Identity Center ・ KMS でアクセス制御と鍵管理を担う
2. **脅威検知**
   GuardDuty ・ Inspector ・ Macie で異常を自動検出する
3. **可視化・統制**
   Security Hub ・ Config ・ CloudTrail で構成変更を追跡・記録
4. **通信・アプリ防御**
   WAF ・ Shield ・ Network Firewall で境界を固める

4 系統を順番に固めろ。起点は ID だ。

ID ・権限を守る基本設計

IAM の最小権限設計

ルートを封印し MFA を必須化し権限を絞る

KMS 暗号鍵管理

保存・転送データを暗号化し鍵アクセスを制限

ID 管理の核心

玄関と金庫が緩ければ後段の対策は無意味だ。

脅威検知サービスの役割分担

GuardDuty

アカウント・通信の異常を継続監視し不正アクセスを検知する

Inspector

EC2 ・コンテナの脆弱性を自動評価し修正箇所を特定する

Macie

S3 内の個人情報など機密データを自動で検出・分類する

「入れて終わり」ではない。アラート運用フローがセットで初めて機能する。

可視化・統制の３本柱

Security Hub 統合監視

検知結果を集約しベストプラクティス逸脱を自動チェック

Config 構成管理

リソース設定の変更を追跡し逸脱を自動検出する

統制の核心

CloudTrail がなければ原因究明も再発防止もできない。

通信・アプリを防御する設計

WAF ・ Shield の役割

Web 層の攻撃と DDoS を境界で食い止める防御層

SG と NACL の使い分け

インスタンス単位とサブネット単位で通信を絞る

防御の鉄則

不要な扉を閉めろ。開けっ放しのポートは招待状だ。

情報漏えいを招く設定ミス

S3 ・ IAM の典型ミス

公開設定放置と過剰権限が侵害時の被害を拡大させる

アクセスキーの危険

コード直書きと長期未ローテーションが漏えい経路になる

事故の核心

漏らすのは設定を放置した人間だ。 AWS の障害ではない。

ログ設計とアラート運用の落とし穴

証跡が残らない状態

CloudTrail 未設定で操作記録がゼロになる

形骸化したアラート

量が多く誰も見ないアラートは検知ゼロと同じだ

検知の核心

まず CloudTrail を有効化しろ。証跡があれば必ず追える。

最優先の基本設定 4 つ

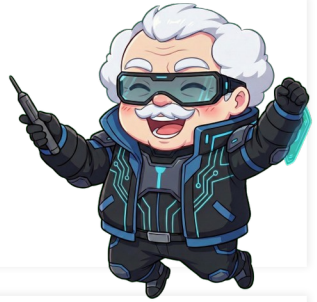
1. **ルート MFA 化**
   ルートアカウントを封印し MFA を有効化して日常運用から外す
2. **最小権限 IAM**
   IAM ユーザー・ロールを分離し権限は必要最小限に絞る
3. **S3 公開防止**
   ブロックパブリックアクセスを組織全体で有効化する
4. **KMS 暗号化**
   保存・転送データを KMS で暗号化し鍵管理を一元化する

この 4 つを潰してから他を考えろ。

継続的に回すセキュリティ運用

自動検知・是正の仕組み

Security Hub で逸脱を自動検知・通知する



証跡保全と権限棚卸し

CloudTrail を長期保全し IAM 権限を定期削除する

運用の核心

回し続ける仕組みを作った奴が最後に評価される。

AWS セキュリティのキャリア価値

市場需要と単価相場

全体中央値 92.5 万円

クラウド案件 11 件は中央値 90 万円。交差点で単価は上振れしやすい

構造的な人材不足

IPA 推計で約 23 万人中スキル充足は 9 万人強

資格と案件参画ルート

AWS 認定セキュリティ

実務 2 年＋ IT5 年の要件。実績と合わせて価値を高める

案件参画のポイント

IAM 設計・ログ監視の実績を言語化し工程を明確にする

需要急増中

まとめ｜AWS セキュリティから市場価値へ

- 責任共有モデルを起点に自分の守備範囲を明確にする
- 設定ミスと運用の甘さが事故の本質。基本設定と継続運用の 2 層で潰す
- クラウドセキュリティ人材は不足傾向。スキルが単価と市場価値に直結する

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 ＞