AWSのセキュリティサービス群のご紹介

NIST Cyber Security Framework（CSF）の5つのコア機能に対応したセキュリティ機能

CSF を活用することにより、識別、防御、検知、対応、復旧という 5 つの機能を中心としたセキュリティ対策の基盤を築き、セキュリティの強化、リスク管理の改善、組織の信頼性向上を実現できます。

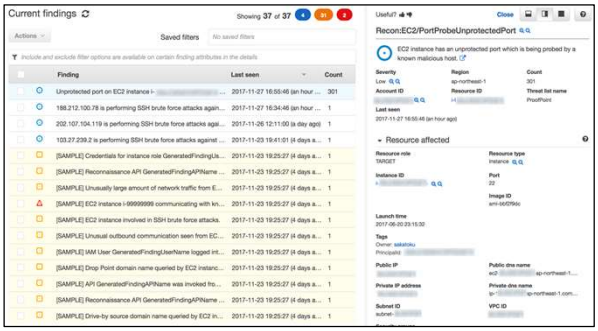
NIST サイバーセキュリティフレームワーク (CSF) ホワイトペーパー

NIST CSF に対して AWS 環境を評価し、実装および運用しているセキュリティ対策（“クラウド内のセキュリティ” とも呼ばれる責任共有モデルのお客様の担当部分）を改善できます。お客様が NIST CSF に迅速に準拠できるように、私たちは、AWS のクラウドサービス、ならびに関連するお客様の責任と AWS の責任について詳細に説明した資料を提供しています。

インテリジェントな脅威検出でアカウントを保護 Amazon GuardDuty

〔 特　徴 〕

- ○ セキュリティの観点から脅威リスクを検知するAWS　マネージド・サービス
- ○ 悪意のあるIPアドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威を認識
- ○ エージェント、センサー、ネットワーク アプライアンス　等は不要
- ○ EC2の悪意のあるファイル（マルウェア等）検出



〔 価格体系 〕

- ○ 30日間の無料枠からお試し下さい
- ○ Amazon GuardDuty には 2 種類の料金体系
  - 分析された AWS CloudTrail イベントの数量（1,000,000 イベントあたり）
  - 分析された Amazon VPC フローログと DNS ログデータの量（GB あたり）

Amazon GuardDutyの特徴、機能、料金についての情報はこちら

Amazon GuardDuty がマルウェア対策機能を追加