ソリューション・ブリーフ

# Security for the Cloud

## 集中管理と可視化でクラウドに安心を

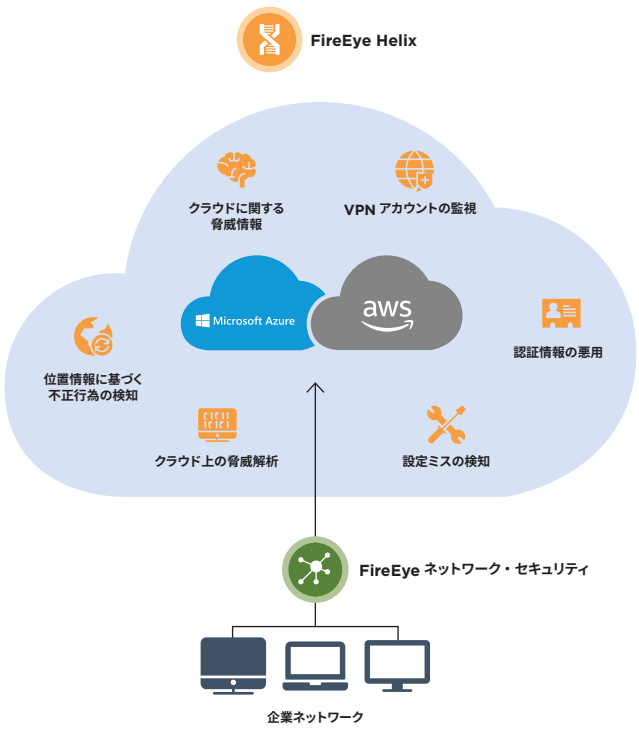
**ハイライト**

- クラウド・インフラの脆弱性と脅威をリアルタイムで可視化
- クラウド侵害の原因となり得る認証情報の不正使用と設定ミスを検知して防止
- CloudTrail、S3 および ELB ログの監視と収集を一元化してセキュリティ対策を簡略化

組織は、業務をクラウドに移行する中でさまざまなセキュリティ上の課題に直面しています。設定が不適切な認証、ずさんなキー管理、セキュリティで保護されていない API は、攻撃者がクラウド・インフラへ侵入する経路の一例にすぎません。攻撃者は次に、アプリケーションを乗っ取り、気付かれないうちにクラウド内を移動し、認証情報を取得して機密データを窃取します。クラウドはオンプレミス・テクノロジーと同様に攻撃に対して脆弱であるにもかかわらず、その保護に必要なツールを保有している組織は一握りです。

IaaS（Infrastructure as a Service）と PaaS（Platform as a Service）のプロバイダーは、セキュリティに対する責任共有モデルを採用しており、クラウドに保存したデータを保護することは顧客自身の責任となっています。クラウド・インフラを保護するために、組織はユーザーの認証情報を保護し、脆弱性を予防的に特定して、セキュリティの監視を一元化する必要があります。

このような高度なセキュリティ機能は、一元的な可視性、設定監視、ユーザー振る舞い解析によって、クラウドに潜む高度な攻撃を検知するセキュリティ・オペレーション・プラットフォームである、FireEye Helix によって実現することができます。




FireEye によって実現するクラウド・インフラのセキュリティ

## FireEyeソリューションとは

可視化機能とインテリジェンスによって
未知の脅威を可視化

認証情報の不正使用と
クラウドの設定ミスを防止

一元管理されていない資産を追跡

### 認証情報の悪用を検知

侵害を受けたアカウントを特定して
アラートを生成

### 位置情報に基づく不正行為の検知

地理情報から判断して
物理的に不可能なログインを検知

### クラウド設定ルール、解析、連携

クラウドの設定ミスを検知して自動的に復旧し、
レポートを生成

### VPN アカウント侵害の検知

データセンター・ログイン、ジオ・インフィジビリティ、
IP 異常検知に依存するヒューリスティック技術を
応用して、VPNベースの潜在的な脅威を特定

### クラウドに関する脅威情報

コンテキスト情報で
Amazon GuardDuty アラートを強化して、
脅威の検知と対応を効率化

### ネットワークの監視

WAN回線上の異常な活動を検知して、
企業ネットワークとIaaSおよびPaaSクラウド間の
攻撃者の移動を阻止

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

**ファイア・アイ株式会社**
〒101-0054 東京都千代田区神田錦町 3-22
テラススクエア 8 階 | 03-4577-4401 |
Japan@fireeye.com



**会社概要**

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEye の革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名な Mandiant® コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEye は準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。

FIREEYE™