

# マルウェア感染などにより 不正な通信を行う端末を 即時に隔離

## 情報セキュリティ事故の増加

標的型攻撃やランサムウェアによる被害は近年の大きな脅威となっています。侵入の痕跡を隠しながら活動するマルウェアなど、手段が高度化しています。万が一の重大な被害を回避するには、異常な状態を早期に検知すると同時に、初動対応を早く行えるよう準備することが非常に重要です。

# 不正通信端末 遮断ソリューション

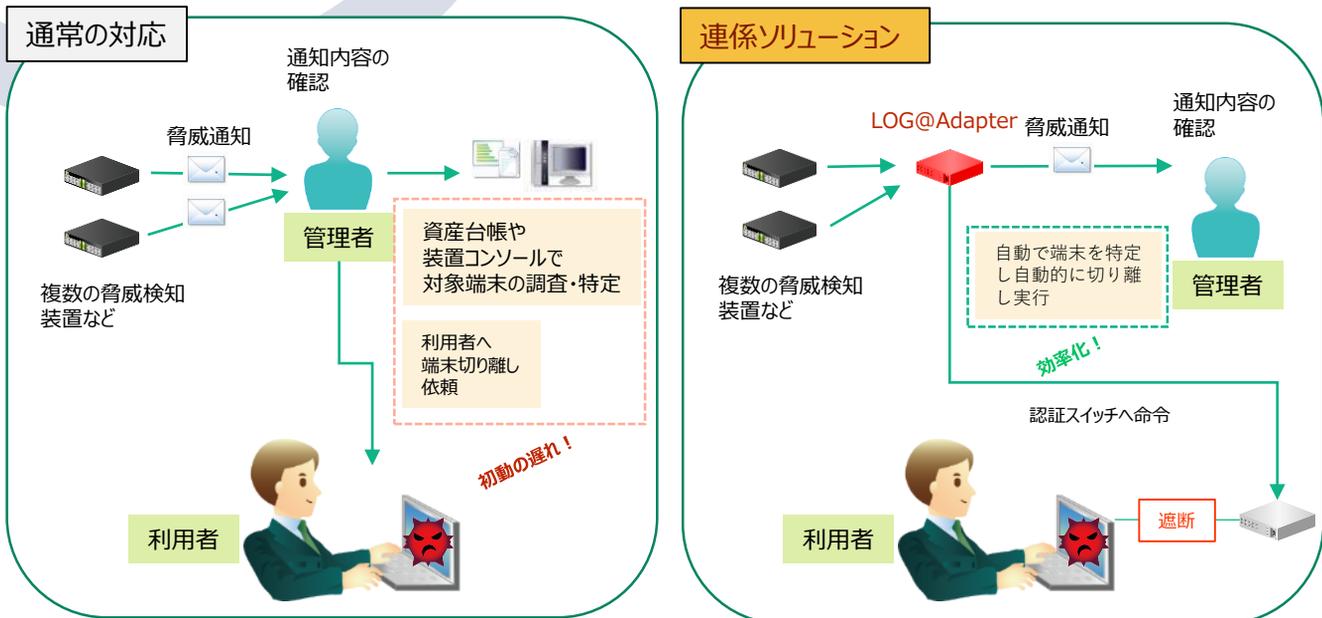
## 万が一、攻撃を受けた場合でも、 自動的に端末をネットワークから隔離



インシデント対応における初動（脅威検知、端末特定、脅威遮断）を効率化します。

### ■ ソリューション概要

- 脅威検知装置から脅威を通知
- LOG@Adapterで解析し端末を特定
- 端末を自動的に遮断し、管理者に通知



## 次世代ファイアウォール連係

### ソリューション構成製品

#### アプリケーション、ユーザー、コンテンツを独自の識別技術で可視化しサイバー攻撃に対抗する、次世代ファイアウォール

次世代ファイアウォールシリーズは、ポート番号ではなく利用しているアプリケーションの識別、IPアドレスではなくユーザー名でのトラフィック制御、リアルタイムに脅威を制御するコンテンツ識別、ハイパフォーマンスを実現するアーキテクチャ、さらには未知のマルウェア検知や振る舞い検知機能を搭載した市場をリードする次世代ファイアウォールです。

ネットワークロケーション	データセンター/クラウド	エンタープライズ境界	分散型エンタープライズ/BYOD
次世代ファイアウォール製品群	 <p>アプライアンス: PA-200, PA-500, PA-30x0, PA-50x0, PA-70x0</p> <p>仮想ソフトウェア: VM-Series VM-100,200,300,1000-HV</p>		
サブスクリプションサービス	脅威防御 URLフィルタリング Global Protect™ WildFire™		
管理システム	Panorama および M-100 アプライアンス		
OS	PAN-OS™		

※弊社販売取扱製品

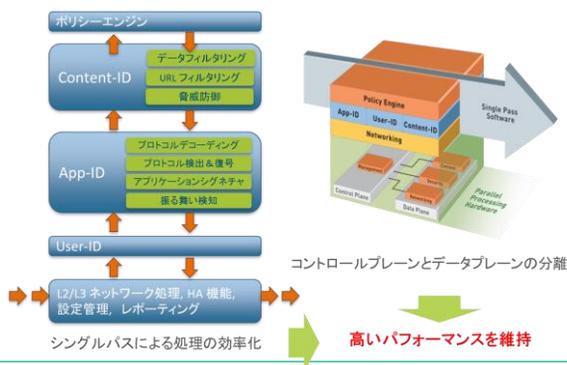


### Palo Alto Networks, Inc.

#### 次世代ファイアウォールのアプリケーション識別

- 全トラフィックのアドレス、ポート、プロトコルの情報に加え、アプリケーション情報も自動的に取得し、識別します。
- SSLにも対応しています。(復号化してアプリケーション識別を行います。)
- ビジネス、インターネット、ネットワークと2,000種類以上のアプリケーションとプロトコルを幅広くサポートし、DB更新により毎週続々と対応数を拡大しています。
- お客様の自社開発のアプリケーションにもリクエストベースで対応しています。
- その場でカスタムシグネチャを作成することも可能です。

#### ◆ 次世代ファイアウォールのアーキテクチャ



#### 認証ログを可視化するsyslog管理アプライアンス

## LOG Adapter



- 誰が・誰が・どのPCで・どのスイッチ&ポートから、接続しているか把握
- 認証スイッチやIPSなどの不正通信検知装置、Account@Adapter+と連携して、認証スイッチから不正通信端末をログアウト

ログ検索機能	レポート機能	ログアクション機能	APRESIA、ALAXALA、Aruba	QuOLA@Adapter	関係機能	端末遮断機能

### エイチ・シー・ネットワークス株式会社

〒111-0053 東京都台東区浅草橋1-22-16 ヒューリック浅草橋ビル4F  
お問い合わせ: <https://www.hcnet.co.jp/inquiry/>

Account@Adapter, LOG@Adapter, QuOLA@Adapter, およびそのロゴは、エイチ・シー・ネットワークス株式会社の登録商標です。記載されている社名および製品名は、各社の商標または登録商標です。掲載した商品は、改良のため予告なしに内容を変更することがあります。掲載製品の写真の一部はイメージです。記載の製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規則などの外国の輸出関連法規をご確認のうえ、必要の手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。

#### ▼ 動作イメージ

