マルウエ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

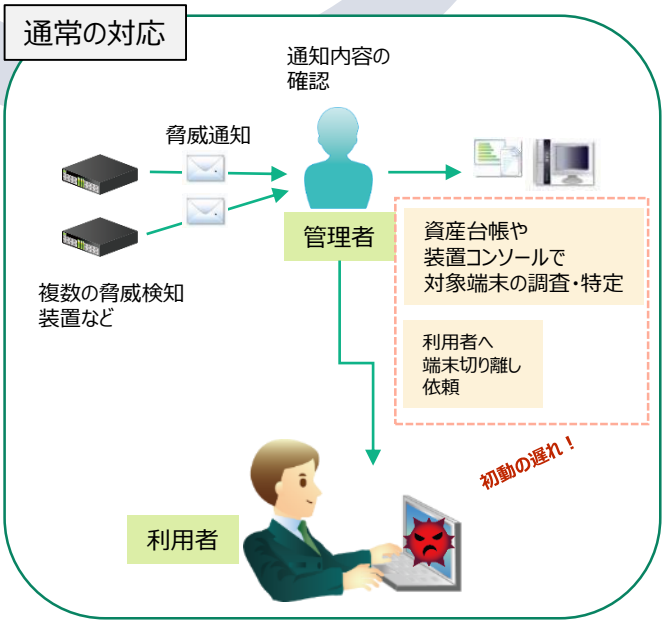
標的型攻撃やランサムウエアによる被害は近年の大きな脅威となっています。侵入の痕跡を隠しながら活動するマルウエアなど、手段が高度化しています。万が一の重大な被害を回避するには、異常な状態を早期に検知するのと同時に、初動対応を早く行えるよう準備することが非常に重要です。

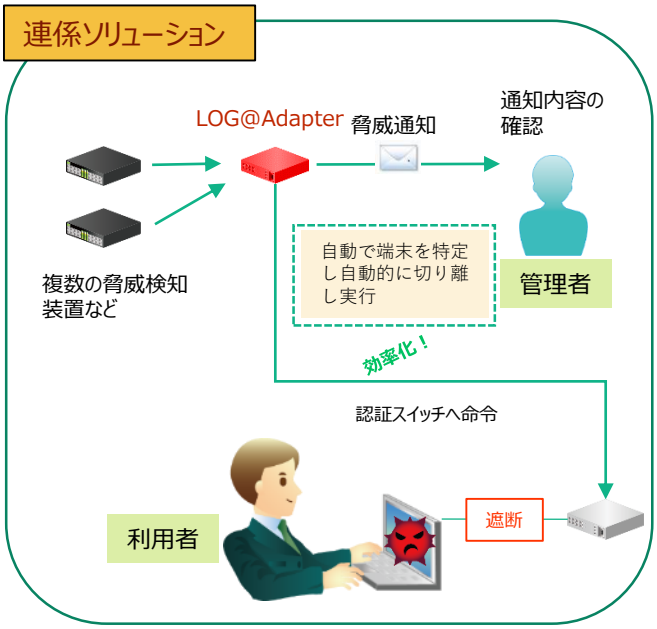
不正通信端末 遮断ソリューション

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





エイチ・シー・ネットワークス株式会社

多層防御連係シリーズ　外部脅威対策編

次世代ファイアウォール連係

■ ソリューション構成製品

多様化するサイバー攻撃から保護するUTM/次世代FWアプライアンス

FORTINET

サイバー攻撃によるセキュリティ被害は年々深刻化しており、侵害された場合の企業に与えるダメージも大きくなっています。
FortiGate®アプライアンスは、導入規模に応じた幅広いラインナップでどの業務形態にも適用することができ、ウイルス対策、ランサムウエア対策、侵入検知・遮断、スパム対策、アプリケーション可視化、Webフィルタリングなどあらゆる攻撃に多彩なUTM機能で高度なセキュリティ脅威や標的型攻撃に対して業界最高の保護機能を提供します。

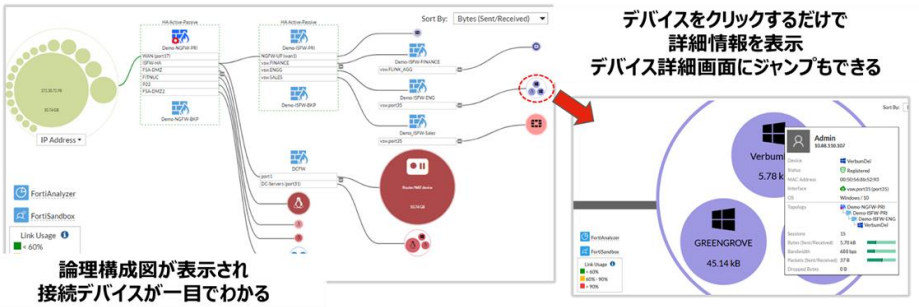
製品の特長

- ネットワーク全体の可視化(右図)
- 標的型攻撃対策の自動運用
- Security Fabric

※弊社販売取扱製品

ネットワーク全体の可視化

- FortiViewで、ネットワークトラフィックをあらゆる角度から可視化
- ワンクリックで、送信元、送信先、アプリケーション種別、脅威、インターフェース、デバイス、ポリシー及び国別にトラフィックを表示できます。



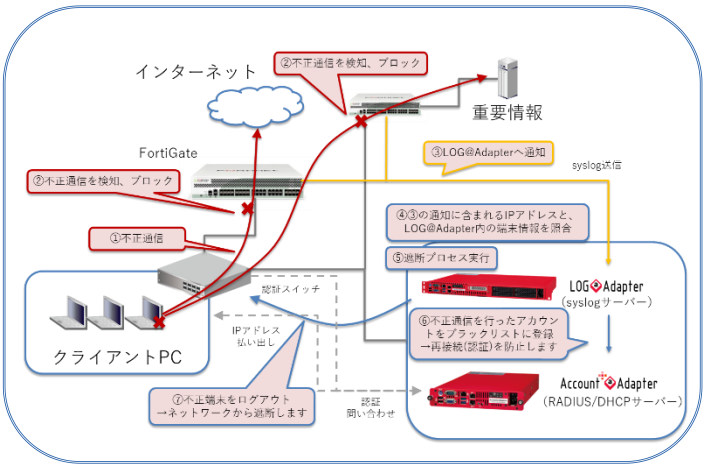
認証ログを可視化するsyslog管理アプライアンス

LOG@Adapter ログ アダプター

●いつ・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+と連係して、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 連係機能　端末遮断機能

▼ 動作イメージ



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4 F
お問い合わせ： https://www.hcnet.co.jp/inquiry/

Printed in Japan '18-04