



アプリケーション連携ソリューション

AMF-SECurity

標的型サイバー攻撃拡散防止対策

Endpoint Protection

Cortex XDR™ × AMF-SEC



マルウェア/ランサムウェア感染端末を エッジスイッチで遮断隔離！拡散防止！

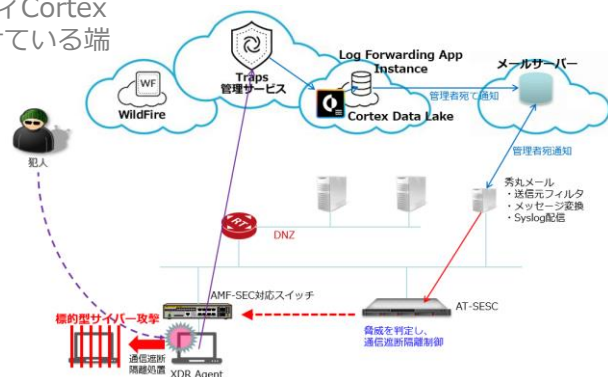
■SDNによる新たなソリューション

アライドテレシスのSDN/アプリケーション連携ソリューション「AMF-SEC (旧称Secure Enterprise SDN)」と、クラウド型次世代エンドポイントセキュリティ Cortex XDR™ (旧称 Traps™) により検出した標的型サイバー攻撃感染端末の通信をエッジスイッチにて通信遮断および検疫隔離を動的に行う情報漏洩被害拡散防止対策ソリューションです。エンドポイント上での脅威を阻止するだけでなく、クラウド システム向けセキュリティ、ネットワーク セキュリティと連携し、サイバー攻撃を阻止することが出来ます。

◆ 標的型サイバー攻撃対策

パロアルトネットワークス社次世代エンドポイントセキュリティCortex XDR™ からの下記検知通知により、標的型サイバー攻撃を受けている端末の検知と自動連携し、エッジスイッチにて被疑端末の通信を確実に遮断隔離、情報漏洩および被害の拡散を防止します。

- WildFire 仮想Sandbox解析により脅威を検知
- WildFire Hash分析により脅威を検知
- Traps 機械学習により未知の脅威を検知
- Traps 振る舞い解析によりランサムウェアを検知



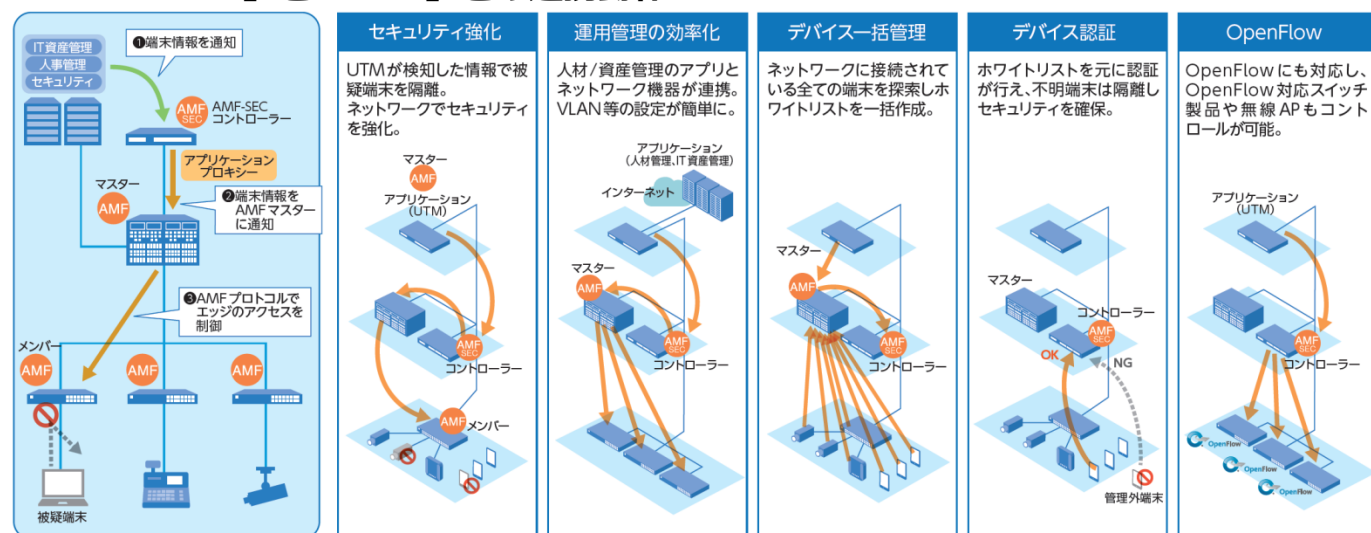
エンタープライズ市場に最適なセキュリティソリューション

「AMF-SECurity」

～アプリケーション連携による企業向けのSDNを実現～

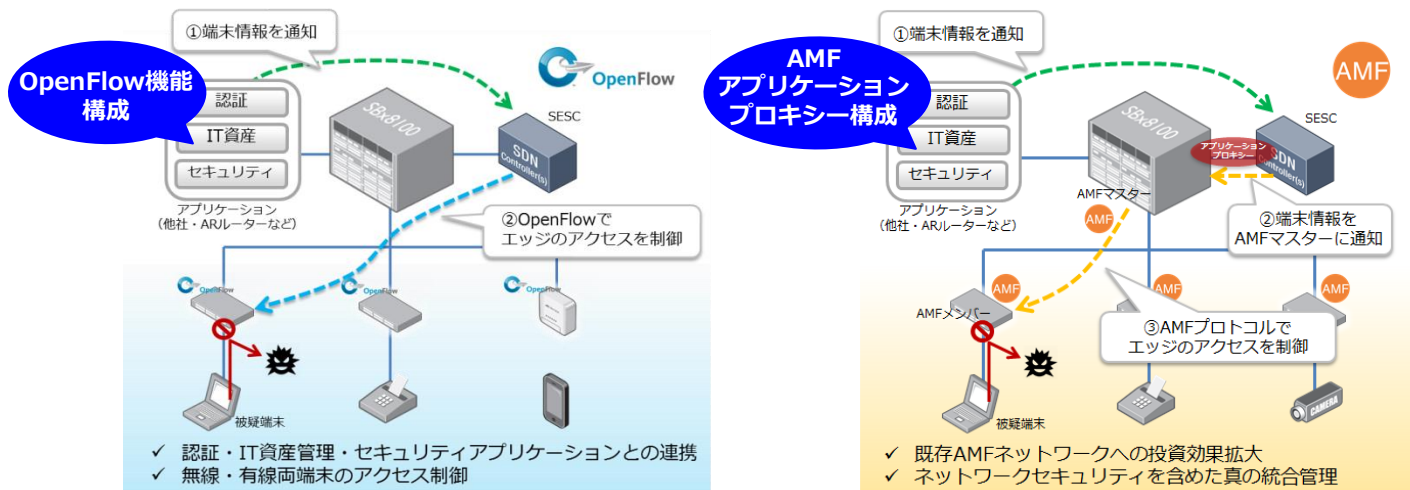
企業のネットワーク運用を最適化するソリューションとしてAMF-SECを開発しました。アプリケーションと連携・連動するネットワークによってユーザートラフィックの動的制御機能をご提供します。セキュリティの強化と、ネットワークの運用にかかるコストの削減、運用負荷の低減を実現しました。以下に、アライドテレシスが提案する「AMF-SEC」およびネットワーク統合管理機能AMFとの連携機能「AMFアプリケーションプロキシ」をご紹介します。

1. 「AMF-SEC」と「AMF」との連携動作



2. OpenFlow構成とAMFアプリケーションプロキシ構成

ネットワーク統合管理機能AMFマスターを介し、各種アプリケーションからの情報により、AMFマスターがエッジのAMFメンバーを制御、端末の通信制御（ホワイトリスト/ブラックリスト制御）を実現します。※ AT-SESC v1.6.0よりホワイトリスト制御に対応



本資料に関する
ご質問やご相談は

TEL: 0120-860442
アライドテレシス株式会社

製品の詳しい情報は
(特徴、仕様、マニュアル等)

ホームページ
<http://www.allied-teleasis.co.jp>