Allied Telesis

2021 Fortress Cyber Security Awards Network security 受賞

2020 Global Excellence Awards Insider Threat Solution GOLD受賞

Network Products Guide 2020 IT World Awards Endpoint Security Solution GOLD受賞

RSA Conference 2020 InfoSec Awards 2部門受賞

2020 Cybersecurity Product / Service Awards Endpoint Security BRONZE受賞

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

Palo Alto Networks Next-Gen Firewall × 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

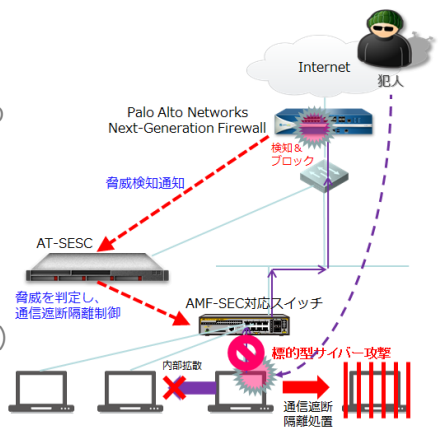
アライドテレシスのSDN/アプリケーション連携ソリューション「AMF-SEC (旧名Secure Enterprise SDN)」と、パロアルトネットワークスの次世代ファイアウォールとの連携により、マルウェアやランサムウェア感染等の脅威感染の可能性がある被疑端末の通信遮断、および検疫隔離を動的に行う情報漏洩被害拡散防止対策ソリューションです。
仮にマルウェアが被疑端末上でIPアドレスを変更し、通信継続を試みても、MACアドレス制御によりアクセス管理および制御を行うため確実に被疑端末を遮断隔離することが可能です。

◆ ふるまい検知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型ファイアウォールが保持する下記脅威検知機能により、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。

- URL（危険なURLへのアクセス）
- Spyware（アンチスパイウェアプロファイルによる脅威）
- Virus（アンチウイルスプロファイルによる脅威）
- Vulnerability（脆弱性保護プロファイルによる脅威）
- WildFire（WildFire™クラウドベースの分析サービスによる脅威）
- WildFire-Virus（WildFire™クラウドベースの分析サービスによるウイルス）

連携対象モデル：PAシリーズ、および、VMシリーズ



Allied Telesis

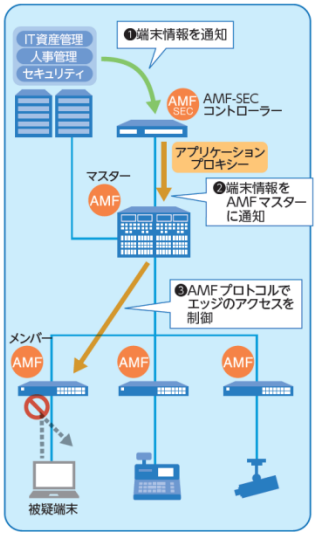
エンタープライズ市場に最適なセキュリティソリューション

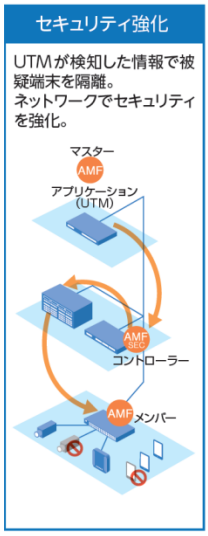
「AMF-SECurity」

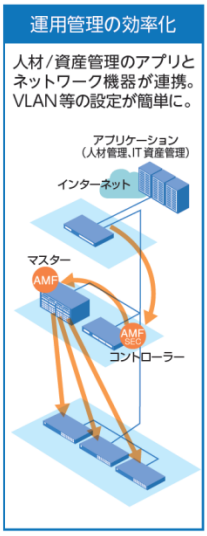
～アプリケーション連携による企業向けのSDNを実現～

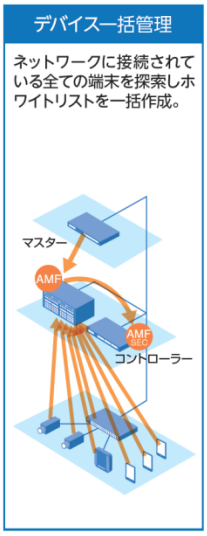
企業のネットワーク運用を最適化するソリューションとしてAMF-SECを開発しました。アプリケーションと連携・連動するネットワークによってユーザートラフィックの動的制御機能をご提供します。セキュリティの強化と、ネットワークの運用にかかるコストの削減、運用負荷の低減を実現しました。以下に、アライドテレシスが提案する「AMF-SEC」およびネットワーク統合管理機能AMFとの連携機能「AMFアプリケーションプロキシー」をご紹介します。

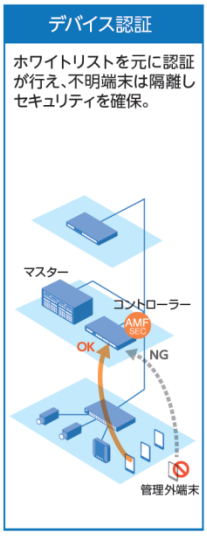
1.「AMF-SEC」と「AMF」との連携動作

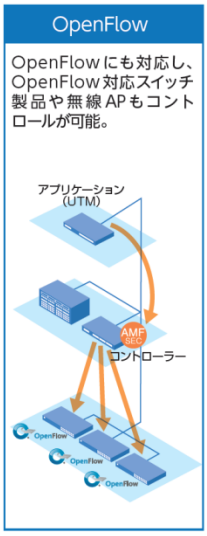






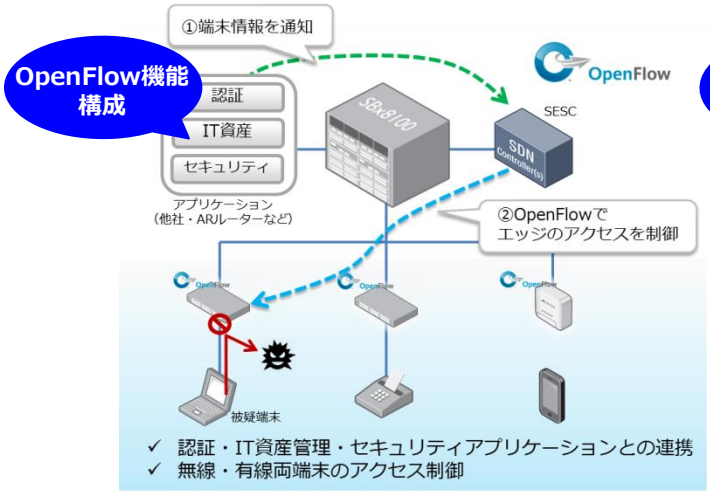


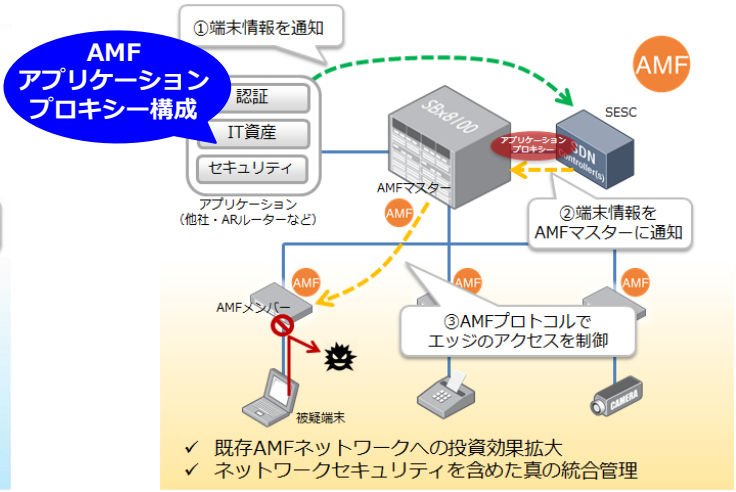




2.OpenFlow構成とAMFアプリケーションプロキシー構成

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-telesis.co.jp