



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

FFR yarai × 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、FFRIの標的型攻撃対策エンドポイントセキュリティソフトウェア「FFR yarai」との連携により、マル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。通常マルウェア感染端末は通信ケーブルを抜き電源を落とし、情報システム部にて被害状況の確認と正常化作業を行います。昨今のマルウェアは安易に電源を落とすと端末上から履歴を含め形跡を消してしまうものも現れております。AMF-SECでは被害の拡散を防御しつつ被害状況の確認が可能な環境をご提供いたします。

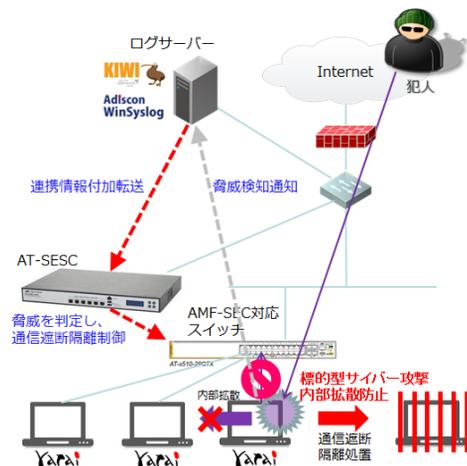
◆ ふるまい検知

FFR yaraiに搭載されているプログレッシブ・ヒューリスティック技術（攻撃者の思考を先回りした先進的な検知ロジックを搭載する5つのエンジンにより、検査対象のプログラムを多角的なアプローチで分析。既知・未知に関わらず、マルウェアや脆弱性攻撃を高精度で検知・防御）と連携し、エッジスイッチにて被疑端末の通信を確実に遮断隔離し、被害の拡散はもとより、被害状況の確認・正常化作業環境を提供いたします。

従来型の対策とFFR yarai(標的型攻撃対策)の違い



FFRIのプログレッシブ・ヒューリスティック技術



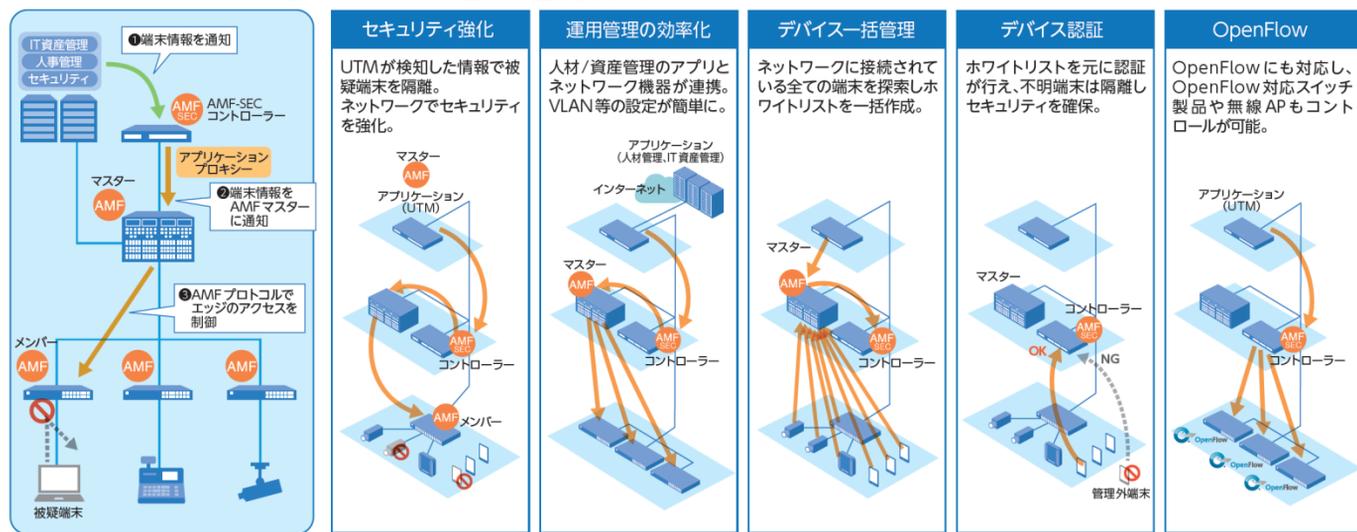
# エンタープライズ市場に最適なセキュリティソリューション

# 「AMF-SECURITY」

～アプリケーション連携による企業向けのSDNを実現～

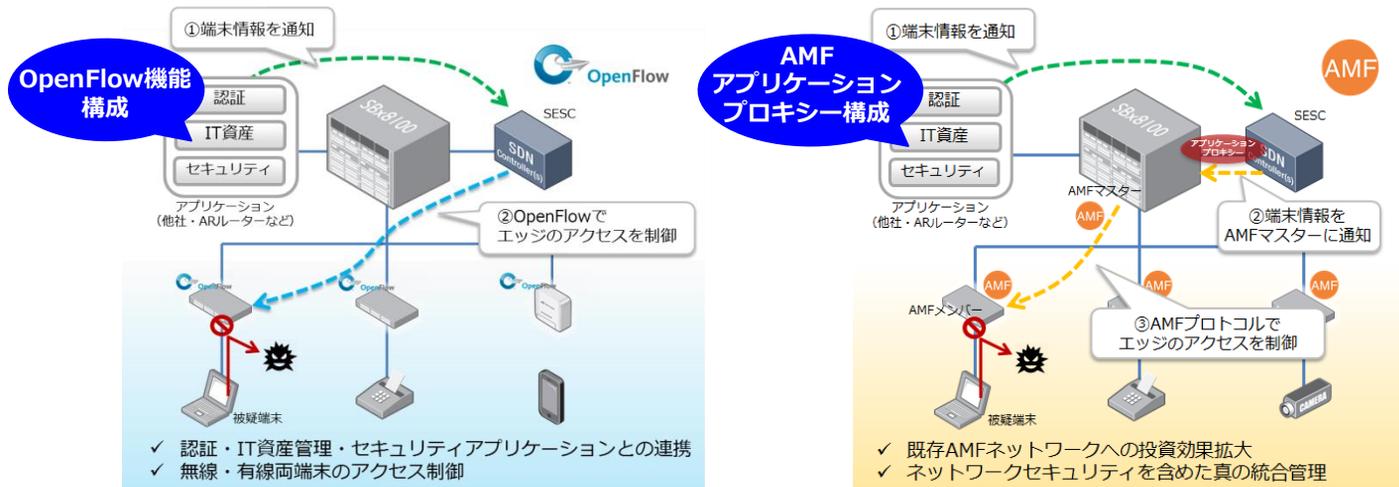
企業のネットワーク運用を最適化するソリューションとしてAMF-SECを開発しました。アプリケーションと連携・連動するネットワークによってユーザートラフィックの動的制御機能をご提供します。セキュリティの強化と、ネットワークの運用にかかるコストの削減、運用負荷の低減を実現しました。以下に、アライドテレシスが提案する「AMF-SEC」およびネットワーク統合管理機能AMFとの連携機能「AMFアプリケーションプロキシ」をご紹介します。

## 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>