



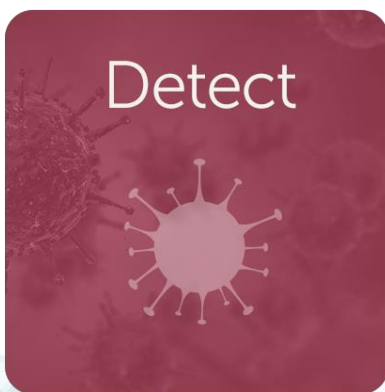
アプリケーション連携ソリューション

# AMF-SECurity

サイバー攻撃拡散防止内部対策

## Lastline Enterprise

## Lastline Breach Defender × AMF-SEC



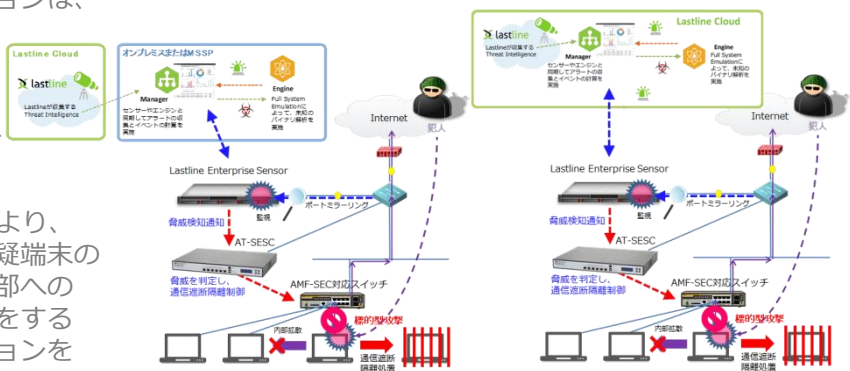
# サイバー攻撃感染デバイスを エッジスイッチで遮断隔離！拡散防止！

### ■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、ラストラインの標的型攻撃内部対策ソリューション「Lastline Enterprise」または「Lastline Breach Defender」との連携により、不正デバイスの通信をエッジスイッチにて遮断/隔離し被害の拡散防止をするセキュリティソリューションを提供してまいります。

### ◆ふるまい検知標的型サイバー攻撃対策

ラストラインの標的型攻撃対策ソリューションは、フルシステムエミュレーション技術による高度なマルウェア検出技術とネットワークフロー解析技術を融合させて、高度な回避型マルウェアによるセキュリティ違反から、官公庁や企業などの組織を守ります。Lastline Enterprise または Lastline Breach DefenderとSESを連携することにより、標的型攻撃を受けマルウェアに感染した被疑端末の通信をエッジスイッチにて遮断隔離し、外部への情報漏洩防止と共に内部への被害拡散防止をするネットワークセキュリティ強化ソリューションを提供します。



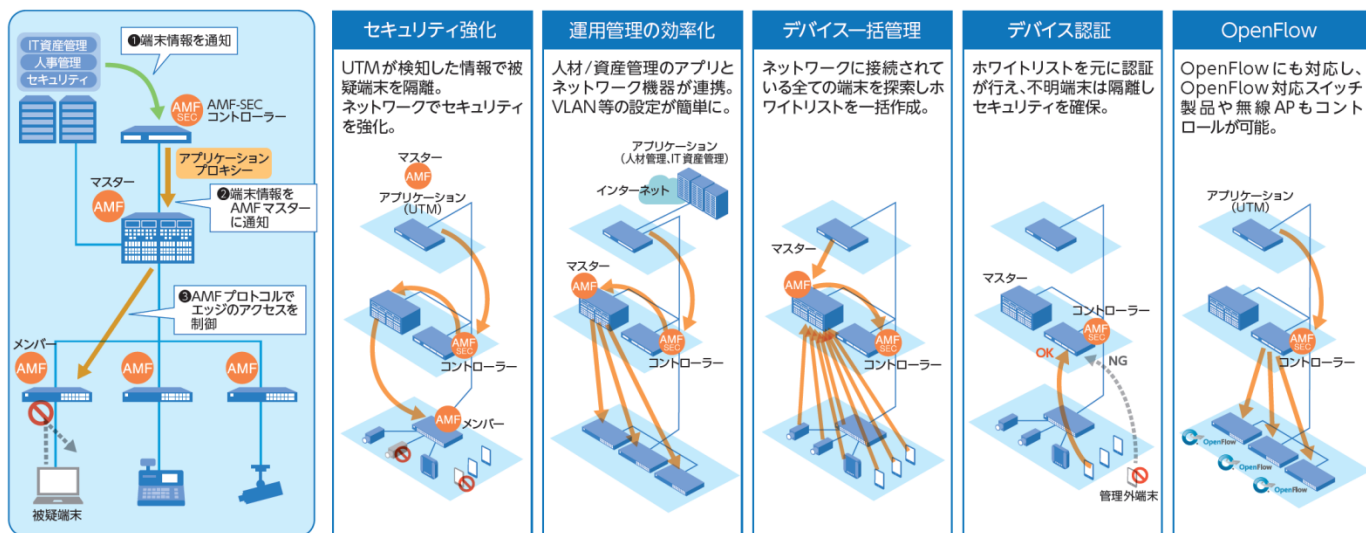
## エンタープライズ市場に最適なセキュリティソリューション

# 「AMF-SECURITY」

～アプリケーション連携による企業向けのSDNを実現～

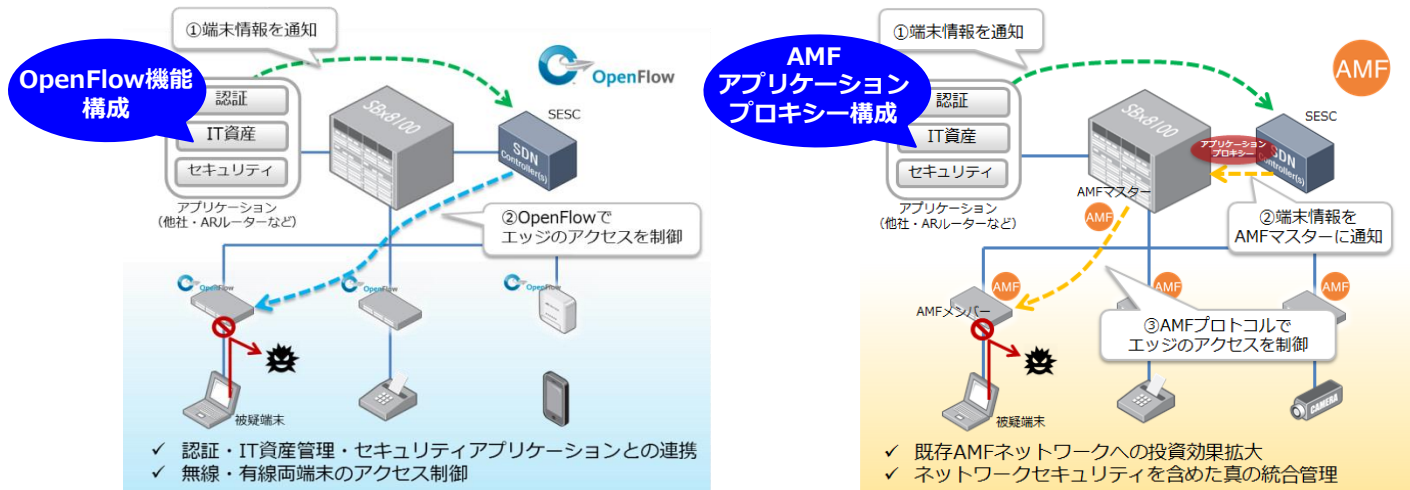
企業のネットワーク運用を最適化するソリューションとしてAMF-SECを開発しました。アプリケーションと連携・連動するネットワークによってユーザートラフィックの動的制御機能をご提供します。セキュリティの強化と、ネットワークの運用にかかるコストの削減、運用負荷の低減を実現しました。以下に、アライドテレシスが提案する「AMF-SEC」およびネットワーク統合管理機能AMFとの連携機能「AMFアプリケーションプロキシ」をご紹介します。

### 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>