The Guaranteed Network
いちばん近くで、もっと先へ。

ネットワークスイッチから支えるセキュリティ
～サイバー攻撃・内部不正対策ソリューション～

アラクサラネットワークス株式会社セッション

【はじめに】

IoT時代の到来と共に、キャンパスネットワークにおいてもPCやサーバのみではなく、スマートデバイスやカメラ等、オフィシャルやプライベートの区別なくさまざまな端末がつながるようになってきています。この状況において、今やキャンパスネットワークはこれまでのファイアウォールとウィルス対策ソフトの導入のみでは対応できない脅威にさらされているといえます。

これらの脅威に対し、アラクサラネットワークスでは3つのソリューションをその解決や対策に提案いたします。

1. ポリシーベースミラーリング　　通過するトラフィックの特定フローのみをミラーする機能
2. ホワイトリストスイッチ　　正規のフローからホワイトリストを自動生成できるスイッチ
3. 無線LAN認証ソリューション　　同一SSID(VLAN)内の認証済端末相互の通信をローカルで可能に。

【1. ポリシーベースミラーリング】

AX8600S/AX8300S シリーズにおいて、有効なデータのみを抽出しセキュリティ装置（フォレンジック、IDS/IPS、Sandbox、etc.）に複数転送可能です。昨今求められるログの保全にも効果を発揮します。

また複数ポートへの転送も可能ですので、負荷分散も実現しセキュリティ装置の帯域や性能の最適化にも寄与します。

【2. ホワイトリストスイッチ】

登録期間内には普通のスイッチとして機能し、その間通信したトラフィックフローからホワイトリストを自動的に生成します。その後運用期間に入ると、未学習のフローに対して廃棄/通知 or 通知のみを選択できます。これによりPC のみならずあらゆる端末の動作を管理することが運用者に負荷をかけることなく可能となり、未知の脅威やマルウェアの感染抑止に大きな効果を発揮します。

【4. 無線 LAN 認証ソリューション】

一般に無線 LAN 環境下で端末認証を導入した場合、その同一 AP 配下では認証･未認証の端末が混在した際にその相互の通信を遮断することはできません。そこで各端末相互の通信を抑止する機能を AP に導入すると、今度は同一 AP 配下での認証済み端末相互の通信が出来ない現象が生じます。この状況を AX2530S において同一ポート内での折返通信機能をサポートすることでバックボーン側に負荷をかけることなく解決いたします。