無線・有線 LAN の統合認証と検疫

小林一生
伊藤忠テクノソリューションズ株式会社
エンタープライズ技術第 2 部

概要：高度なセキュリティと管理者の負担軽減、ユーザの利便性を実現しながら、無線 LAN だけでなく、有線 LAN との統合管理も行うことができる、アルバネットワークス社の製品を通して、キャンパス環境への無線 LAN の導入のポイントを考えます。

キーワード：無線 LAN、セキュリティ

1. モバイルシステム導入の条件

ノート PC の普及に伴い、大学では無線 LAN のニーズが高まってきています。

しかし、費用の面もさることながら、無線 LAN を構築するために、いくつかの懸念事項＝必要条件を明らかにしていく必要があります。モバイルシステム導入の必要条件としては、ネットワークの安全性、ネットワークの実用性、システムの管理性の 3 つがあげられます。しかし、実際にどう実現していくかというところが課題です。

無線ネットワークで、この 3 つの条件を満たすには、いろいろな機能が必要です。ファイアウオールやゲートウエイ、ルータ、そして、無線 LAN の IDS[1]、IPS[2] といった侵入検知、無線通信上の電波の状態、環境の整備、暗号化の機能を持った機器が必要になります。このような機能をすべて 1 台のハードウエアに集約したもの、これがアルバネットワークス[3] の製品です。（図 1）

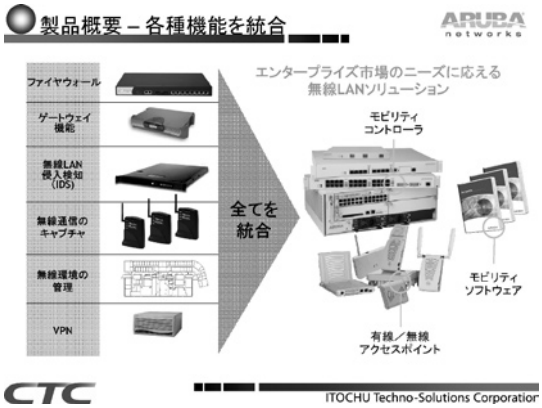

図 1. 各種機能を統合

2. 革新的アーキテクチャ

図 2 の左の絵は、従来のよくあるアクセスポイント（AP）の機能です。1 台の AP の中にすべての機能を集約しています。802.a/b/g、電波のアンテナ、マネジメント環境、セキュリティポリシー、ルーティング、暗号化、認証、これをすべて 1 台の AP で賄っています。

これに対してアルバは、AP としては何もやっていません。AP は電波の部分しか管理していないというのが、アルバの特徴です。そのため、マネジメントや、アクセスリスト、モビリティ、転送、暗号化、認証といったすべての機能をスイッチ上で提供しています。

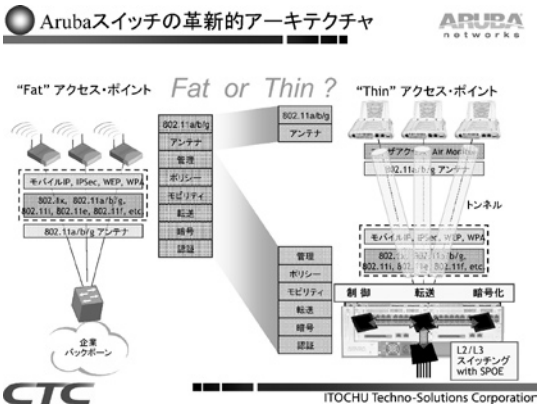

図 2. 革新的アーキテクチャ

AP とスイッチは、GRE トンネルというトンネル技術を使って接続されます。

スイッチ側で暗号化することにより、どのような利点があるかというと、左側の絵では無線電波の中では暗号化されていますが、有線にデータが流れる時には暗号化されません。それに対して、アルバは無線部分はもちろん、有線を利用したときも、スイッチまで暗号化されたままで通信が行われます。そのため、セキュリティを重要視するため、無線 LAN を使用できないと考えられる、例えば

事務系のネットワークにも適した製品です。

通常のFAT APを設置することを考えた時、APにつけるIPアドレスやSSID[4]、認証方法、暗号化、セキュリティ管理、すべて考える必要があり、しかもAPごとに全部設定しなければなりません。それに対してアルバのThin APでは、AP自身のIPアドレスと名前（ホスト名）、集中管理を行うWLANスイッチのIPアドレスをAPに設定するだけです。

細かな設定項目は全てWLANスイッチで一括設定となります。

保守メンテナンス時も、前述の項目だけを入力するのみですから、大変簡単です。

次に、GREトンネルについてです。ユーザの端末がAPに接続すると、アルバWLANスイッチ上につくられた、仮想セグメントに割り振られます。従来のFAT APの例と違うのは、無線セグメントすべてを論理的に集約できるところです。GREトンネルによって、物理的なセグメントの影響を受けず、論理的な無線セグメントを容易に構築できるだけではなく、APとユーザの管理をも一元的に管理できるのです。

また論理的に集約することで、ポートやAP単位という形でのセキュリティではなく、ユーザに対して割り当てることができます。

3. セキュリティ機能

セキュリティ機能の認証の部分で、キャプティブポータルというウェブ認証の機能があります。特に大学では、どんな端末をユーザが使っているのか、全く分かりません。ウインドウズ、マック、リナックスもあります。そのため、メーカに依存するような認証方式やエージェントが必要な認証方式を選択することは困難です。ブラウザによる認証方式をサポートすることが重要です。

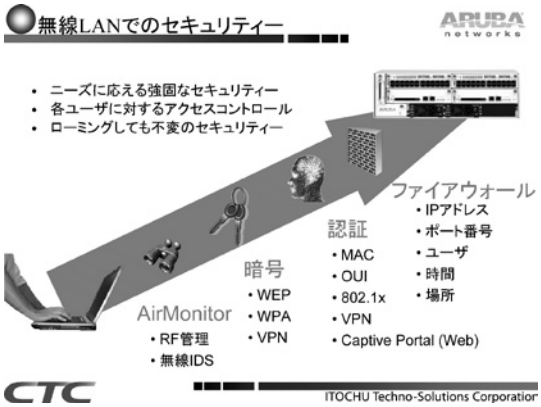

図3.　無線LANでのセキュリティ

エアモニタという機能は、無線の電波状況やどんなAPが周りにあるか、どんな端末があるかを監視します。これにより、不正なユーザやAPを検知・排除することができます。

WLANスイッチでは、検出されたAPを管理者が許可したものか、不正なものか自動分類し、そのAPを無効化することができます。

また、APや端末の位置特定も可能です。どこに該当のAPや端末がいるのかを特定できるのです。エアロスカウトという製品と連携させることで、さらに詳細な位置特定も可能となります。

ユーザセントリックなセキュリティとして、まず認証前は無線にアソシエートしたタイミングで、認証パケットしか通らないようなロール（Logon Role）がユーザに割り当てられます。これで認証要求をして、認証サーバから返ってきたロール情報を元に、ユーザに対して適正なアクセス条件を割り当てます。（図4）

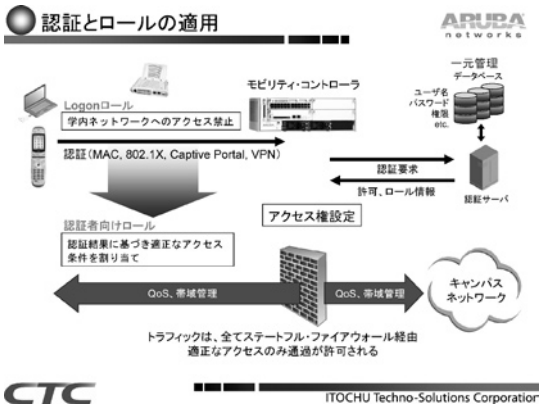

図4.　認証とロールの適用

4.　有線LANとの統合

有線APの製品もアルバは発売しています。有線でも同様の認証、暗号化を行います。これによって有線も無線も同じ認証手順でログインできるので、ユーザに二重に使い方を覚えてもらう必要がないという、運用面のメリットがあります。

有線APを使った例を紹介します。これは都内の某私立大学で実際に導入された例です。その大学は、夏休みや冬休みの時期にしか使われないセミナーハウスを持っていました。それまでは、そこに64kbpsの専用線などを引いて運用していましたが、回線費用が

高く、昨今のネットワークとしては大変遅いものでした。

ご提案した構成が、図5になります。回線はADSLやBフレッツという安価な回線を引き、そこにアルバAPを設置しただけの構成です。セミナーハウス側で、端末がネットワークに接続しようとすると、学内に設置してあるアルバスイッチに論理的に集約され、そこで認証、暗号化を行います。これにより、セミナーハウスごとに認証手順を変えなくてもよくなりました。セミナーハウスには、このAPを設置してくださいと管理人にお願いするだけで、簡単に学内と同じ環境が提供できます。

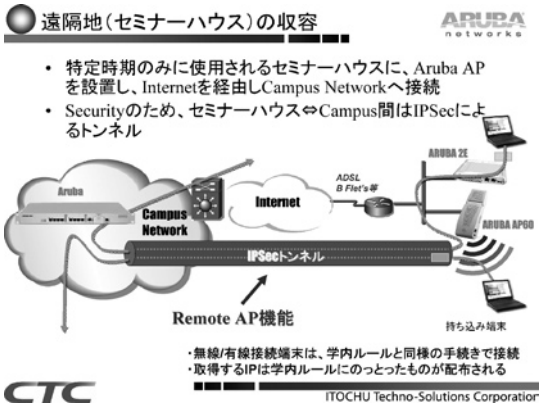

図5　遠隔地の収容

このような使い方もできます。自宅に置いたAPから、学内のネットワークにつなぐこともでき、遠隔授業はもちろん、通学が困難な学生が自宅から利用することもできます。

Fortigateという UTMの製品との提携で、さらにセキュリティの高い環境を構築できます。これも、先ほどの私大で実際に導入された例です。通常のデータはGREトンネルを通ってキャンパスネットワークに出ていきます。特定の通信（HTTP、FTPなど）がきた場合のみ、Fortigateにリダイレクトし、ここでIDSやIPS、アンチウイルスについて、パケットをチェックします。問題がなければキャンパスネットワークへ出て行くことが可能ですが、もし問題が発見された場合は、その通信を止め、ユーザに対して『あなたが通信をしようとしたサイト、またはダウンロードしたファイルに関してはウィルスに感染しています』というWARNINGメッセージを表示します。

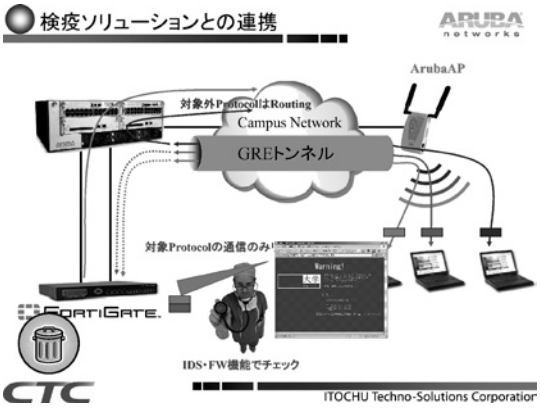

図6.　検疫ソリューションとの連携

5.　設計・運用・構築のポイント

無線LANを構築するときには、サイトサーベイが必要になり、これに結構費用がかかります。アルバには、APの配置計画と配置結果を表示する導入支援ツールが標準でついています。

キャンパス環境では、先生や学生が勝手にAPをつけることがあると思います。情報センターの方がAPを設置して、チャンネルを設定しても、電波が干渉して使えないというクレームが入ってくることもあります。しかし、アルバのAPを使えば、周りの電波状況を見て、チャンネルを選択してくれます。

電波環境を動的に確認・変更することができるため、次に挙げる有用な機能も実装できます。

隣のAPが壊れたら、近いところにいるAPが相手の分までカバーするように電波出力を動的に変更する、セルフヒーリングという機能。

よくある例として、授業で無線を使う時、学生が席の後ろの方に集まる傾向がありますが、その場合、1台のAPに端末が集中してしまうため、このような場合には、『他のAPに接続するように』と指令を出し、集中を防ぐ負荷分散機能があります。

今後、次期OSではワイヤレスメッシュ[5]に対応する予定です。有線が引けないような場所に無線APだけを持っていって、無線エリアを広げることができます。キャンパス環境では、中庭や外に設置したい場合に、構築・拡張が容易で、ケーブリングコストが削減できるというメリットがあります。

6.　まとめ

ユーザのある意味『わがまま』なニーズに応えるのがアルバのソリューションです。

認証や、セキュリティに関する様々な機能を提供しながら、自由度の高いネットワーク環境を実現します。大学が抱える、無線LANを構築する上での課題を解決できるのではないでしょうか。

参考URL等

1) ネットワークへの侵入を検知して管理者に通報するシステム
2) サーバやネットワークへの不正侵入を阻止するツール
3) http://www.arubanetworks.co.jp/
4) IEEE 802.11シリーズの無線LANにおけるアクセスポイントの識別子
5) 通信機能を持った端末同士が相互に通信を行なうことにより、網の目（mesh）状に形成された通信ネットワーク