高密度環境でも安定・セキュアなネットワークを実現する Aruba 無線 LAN と ClearPass

下野 慶太
アルバネットワークス株式会社

概要：大学の大ホール、コンピュータ室等、端末が非常に多い環境で無線 LAN を構築する時に必要な動的負荷分散機能の ClientMatch と、全てのユーザと端末を簡単、セキュアに無線 LAN に接続するために必要な ClearPass 統合認証基盤の使い方を解説します。

キーワード：無線 LAN、セキュリティ、アクセス制御、ポリシー管理、認証、ゲストアクセス

1. はじめに

大学を始めとする教育機関でモバイル端末の活用が急拡大しています。今までは講師が自分用のノート PC を講義で利用したり、食堂や図書館などのオープンスペースで一部の学生が利用しているだけでした。しかし、講義中にタブレットでメモを取ったり、コンピュータ教室の PC をモバイル化、もしくは BYOD で生徒自身の端末を使って講義を行ったりと、利用シーンが広まってきています。

モバイル端末の活用に伴い、無線 LAN 環境の整備も進んでいますが、講義で使う場合、無線 LAN の機種選定、設計が今までとは大きく異なり、課題が大きく 2 つ出てきます。1 つが狭いエリアに端末が密集する「High Density 環境」であること。もう 1 つが不特定端末が接続してくることによる「セキュリティリスクの増加」です。今回はこの 2 つの課題をどの様に解決できるか、実際の事例を元に解説します。

2. High Density 環境に最適な無線 LAN

端末が増加すると単純にスループットが下がります。その理由は「無線 LAN アクセスポイント（AP）の性能」と、「AP 間の負荷分散機能」が関係しています。

2.1 無線 LAN アクセスポイントの性能

無線 LAN を使う上で暗号化は必須です。安価で性能の低い AP は CPU などの処理能力が低く、接続端末数の増加に伴い、著しく性能が下がります。特に、家庭用機器は同時に何十台も端末が繋がることを想定していないため、High Density 環境には向いていません。Aruba の AP-225 であれば、チャネル当り 50 台、計 100 台程度の端末が同時に接続しても良いように設計されています。

2.2 動的な AP 間の負荷分散機能の必要性

無線 LAN は、同一チャネル（電波の周波数帯）に接続する端末数が増加すると、全体のスループットが下がる特性があります。50 台が接続すると、1 台の時と比べて約 30% 下がるといったデータがあります。これは無線 LAN が採用している CDMA/CA が原因で避けることができません。

そこで重要になってくるのがダイナミックな負荷分散機能です。High Density 環境では複数の AP を設置し、1 チャネル当たりの接続端末台数が 50 台以下になるようにしてあげれば良いのです。Aruba の無線 LAN は ClientMatch という機能でこれを実現しています。一般的に、無線 LAN 端末がどの AP に繋がるかは端末に依存しています。また、端末は一度 AP に繋がると、できるだけ繋がったままの状態を維持しようとするため、移動等により他の AP に繋がった方が良い場合でもうまく切り替わらない事が多くあります。Aruba の無線 LAN はコントローラが AP を管理しており、AP が端末情報をコントローラに定期的にレポートしています。そのため、各端末がどの AP に繋がるのが最適か、コントローラが常に俯瞰的にみて判断することが可能になります。ClientMatch の機能を使うことで、AP へ接続済みの端末であっても、強制的に最適な AP に接続し直すことが可能となっています。ClientMatch の技術は端末に依存することなく利用可能です。この技術は特許も取得しているため、Aruba だけが実現できる技術です。

実際に ClientMatch の機能の有無でどのような違いがでるかを簡単に表したのが図 1 です。ClientMatch 無しの環境では一部の AP に端末が偏っているため、これらの端末の通

信速度は遅くなってしまいます。Client Match 有りの環境では、各端末が最適な AP に接続できているため、通信速度はほぼ同じになっていることが分かります。

端末が増加してくると、この差はより顕著になるため、High Density 環境ではコントローラによる集中制御と ClientMatch による動的な負荷分散機能が重要になってきます。

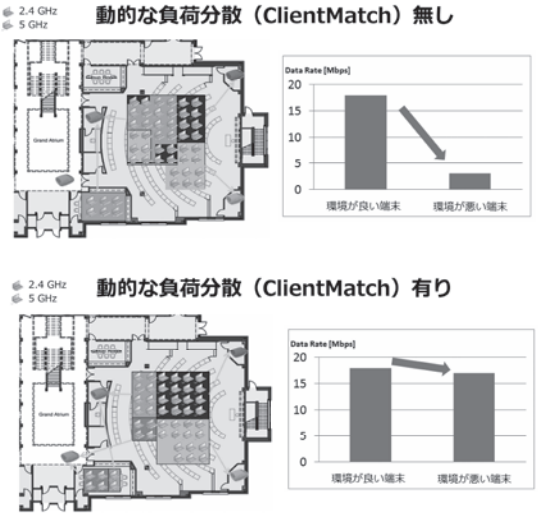

図 1　動的な負荷分散（ClientMatch）の効果

3.　セキュリティリスクの増加に対応した無線 LAN

無線 LAN セキュリティの懸念点は、大きく「盗聴」と「不正アクセス」の 2 つに分かれます。盗聴を防ぐには「暗号化」、不正アクセスを防ぐには「認証（ユーザ ID・パスワード）」を使います。ただ、1 人で 2 ～ 3 台の端末を使う現在では、ユーザ認証だけでは無制限に端末が繋がってくることになってしまうため、デバイス自体も認証する仕組みが必要になっています。さらに、IoT（Internet of Things）でネットワークに接続してくる端末が急増するに伴い、有線・無線 LAN に限らず脆弱性のある端末が学内に接続されるリスクが高くなっています。最近のネットワークは、重要なデータを持つサーバはデータセンターでしっかり管理されているため、攻撃者は直接サーバを狙うのでは無く、内部の脆弱性のある端末を探しだし、そこを踏み台にしてサーバにアクセスする傾向にあります。そこで、セキュアなネットワークを構築するためには、ユーザや端末などのロールベース（役割毎）のアクセス制御が必要になります。図 2 の様に、ロールベースのアクセス制御を取り入れると、万が一脆弱性のある端末がウィルスに感染しても、その被害を最小限に留めることが可能です。

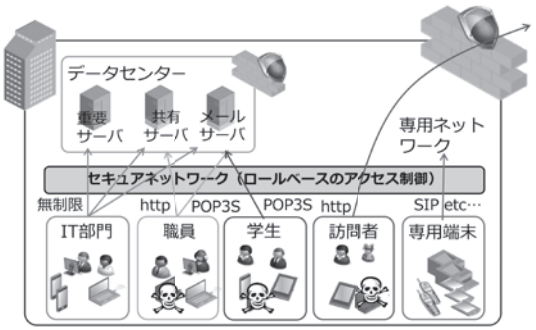

図 2　ロールベースのアクセス制御

3.1　Windows XP 対策も簡単にできる Aruba 無線 LAN

Aruba の無線 LAN 機器にはファイアウォールが内蔵してあります。このファイアウォールによって無線 LAN だけでロールベースのアクセス制御を簡単に行う事が可能です。さらに、単純なポリシーであれば、デバイスタイプ毎のアクセス制御も可能で、例えば、「Windows XP 端末だけは学内にアクセスさせない」といったことが実現できます。設定も非常に簡単で、4 行程のコマンドだけで実現できます。

国内の Aruba をご利用の N 大学様では、誰が使っているかに関わらず、Windows XP 端末が学内無線 LAN にアクセスすると、「Windows XP は許可されていないので、しかるべき手段で OS をアップグレード後にアクセスして下さい」といった注意喚起を表示する Web ページにしかアクセスできないようにしています。

3.2　無線 LAN セキュリティの特徴

よく街中のホットスポットなどで、キーを紙で貼っている場合があります。PSK のキーが分かると、フリーのツールで簡単に暗号化を解読できるので盗聴を完全に防ぐことはできません。もちろん、不特定多数には使わせ無いという一定の効果はあります。また、Web 認証は暗号化の仕組みは考慮していな

表 1　無線 LAN セキュリティ・認証の特徴

種類	認証対象	暗号化	セキュリティ	備考
IEEE802.11	共有鍵（PSK）	△	-	共有鍵方式は KEY が分かれば簡単に解読できる
MAC 認証	MAC アドレス	×	△	無線クライアントの認証機能がない場合に利用。ファイアウォールなどとの併用が必要
Web 認証	ユーザ名・パスワード	×	△	ブラウザが使えれば端末は問わない。暗号化は考慮されていない。
802.1x EAP-PEAP	サーバ証明書・ ユーザ名・パスワード	○	○	比較的手軽に利用が可能。 端末を制限する仕組みは無い。
802.1x EAP-TLS	クライアント証明書・ サーバ証明書	○	◎	無線クライアントに証明書のインストールが必要。証明書 /CA のための追加費用が必要

いので、ゲストアクセスなど、盗聴を考慮する必要が無いゲストアクセス等で使用するべきでしょう。

表 1 が無線 LAN セキュリティ設定、認証の特徴をまとめたものになります。この表からも分かる通り、盗聴を防ぐには 802.1x 認証を使う必要があります。不正アクセスを防ぐ為にも 802.1x 認証は非常に有効です。さらに、802.1x EAP-TLS のクライアント証明書を使った認証を使うことで端末を制限することも可能です。そこで課題となるのは、どの様にしてクライアント証明書を端末にインストールするかです。IT 管理者が全ての端末を預かってクライアント証明書をインストールするのは非常に手間です。学生の BYOD まで考えると尚更です。そこでクライアント証明書を簡単に端末にインストールする手段が求められてきます。

3.3　大学ネットワークに求められる無線 LAN の特徴

大学のネットワークには様々なユーザがアクセスしてきます。一般の企業に比べると、ユーザの入れ替わりも毎年多く発生します。学会や共同研究員等で一時的なゲストアクセスも必要になります。この様な大学のネットワーク、特に無線 LAN では以下の様な課題が出てきます。（弊社アンケート結果より）

- ゲストアクセスのアカウントを発行する頻度が多く、手間・コストがかかる
- 同じゲストアクセスを使うユーザでもアクセスポリシーは異なるが、分けるのが手間で実質できていない
- 毎年入れ替わる学生用の端末にクライアント証明書をインストールするのに手間・コストがかかる、もしくはクライアント証明書は導入していない
- 学生と教員のネットワークが混在している
- BYOD まで管理しきれないので無制限にアクセスを許可している

つまり、ユーザが多すぎて管理にコストがかかるため、結局コストをかけず管理が甘くなり、セキュリティリスクが大きくなっているのです。本来は不特定多数のユーザが多いからこそ、きちんと管理してセキュリティリスクを最小限にする必要があります。

Aruba の ClearPass 統合認証基盤は、ユーザ管理にかかる手間・コストを最小限に抑えながらポリシー管理を実現できるため、上記に挙げた課題は全て解決することが可能です。ClearPass の一番大きな機能は、ユーザや端末タイプに応じた細かなポリシー管理です。標準的な RADIUS サーバの機能も全て兼ね備えているので、大学等教育研究機関の間で相互利用を実現する Eduroam との連携も可能です。それに加え、「メール認証機能も兼ね備えた豊富なゲストアクセス」と「無線 LAN 設定・クライアント証明書のインストールプロセスを自動化した Onboard 機能」を持っており、これらを活用することでユーザや端末の管理コストを大幅に削減できます。

3.4　多彩な ClearPass のゲストアクセス機能

ClearPass のゲストアクセス機能は細かな設定が可能です。例えば、ゲストアクセス時に、自動的に承認者にメールを送信し、承認者がそのメールに書かれている URL をクリックし、そのゲストを承認して初めてゲストアクセスが可能、といったプロセスを自動化できます（図 3）。その他、ゲストのメールア

ドレス宛にパスワードを配信することで、メールアドレスの正当性を確認したり、誰でも簡単に使えるように、Facebook 等の SNS アカウントでログインできる機能もあります。また、ゲストのタイプ毎にロールを分けることもできるので、同じゲストアクセスでも、インターネットだけだったり、一部の学内システムにはアクセスできたりといったポリシー管理まで実現できます。今挙げた機能は全て、IT 管理者が関与することなく利用できます。つまり、ゲストが訪問してくる度に IT 管理者がゲストアカウントを発行する手間は一切かかりません。大学の様に毎日多数のゲストが訪れる環境では非常に大きなメリットです。

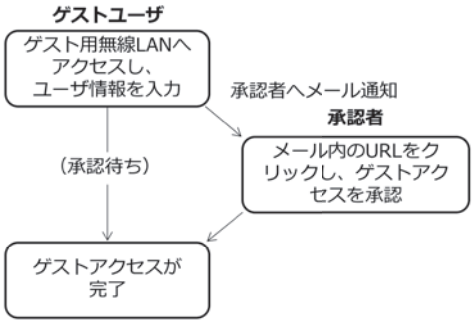

図 3　承認型ゲストアクセスのプロセス

3.5　簡単・セキュアに無線 LAN へ接続させる ClearPass の Onboard

Onboard は「乗せてあげる」という意味合いがあり、ClearPass の Onboard はまさに、「無線 LAN に端末をセキュアに乗せてあげる（＝接続してあげる）」ことが可能な機能です。例えば、端末が Onboard が有効な無線 LAN に接続すると、自動的に Onboard 用の Web ページが表示されます。そこで、学内のユーザ ID を使ってログインすると、そのユーザ ID に紐づいた端末の Profile（クライアント証明書＋無線 LAN の設定）が自動でインストールされ、セキュアな 802.1x EAP-TLS を使って無線 LAN にアクセスすることが出来ます。

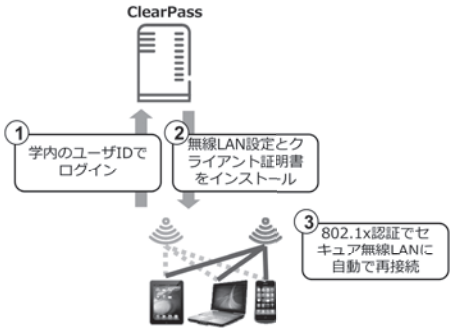

図 4　Onboard を使ったセキュア無線 LAN

ここでも重要なのは、このプロセスに IT 管理者は一切関与する必要が無いという点です。従って、学内の端末や BYOD が増加しても、ユーザが自分で Onboard を使えば IT 管理者の負荷は増えません。さらに、全てのプロセスが自動化されているため、ユーザも、使いたい時にすぐに使えるという大きなメリットがあります。もちろん、Onboard を使った端末情報は ClearPass に登録されるので、IT 管理者は登録された端末を管理・監視・制限することが可能です。例えば、BYOD は Onboard を使い、BYOD 以外は IT 管理者が登録すれば、BYOD、その他の端末を区別して、アクセスポリシーを変えることも可能です。

ClearPass を使った学内無線 LAN のポリシーを表 2 にまとめています。この中で、IT 管理者自身が直接設定・管理するユーザ・端末は一番上の職員・教員の支給端末だけです。その他は、ClearPass のゲストアクセスと Onboard を使ってユーザが自ら端末を登録するため、管理者は登録された情報を管理するだけになります。この様に、手間・コストを抑えつつ適切にユーザや端末を管理することで、IoT 時代にも耐えうるセキュアな無線 LAN を構築することができます。

表2　ユーザ・端末に応じた簡単・セキュアな無線 LAN アクセス

ユーザ タイプ	セキュリティ設定	ロール名 （ポリシー）	接続方法
職員・教員	802.1x 認証 （EAP-TLS）	employee	IT 管理者が端末をキッティングして無線 LAN 設定とクライアント証明書をインストール
学生・BYOD	802.1x 認証 （EAP-TLS）	student	学生が自分で端末を登録し、無線 LAN 設定とクライアント証明書をインストール
外部の学生	802.1x 認証 （EAP-TLS/PEAP）	e-student	Eduroam のアカウントを持っているユーザはそのアカウントでアクセス
ゲスト（一般）	ゲストアクセス （Web 認証）	guest	メールアドレスを入力したユーザは誰でもアクセス
ゲスト （共同研究員）	ゲストアクセス （Web 認証）	co-worker	メールアドレスを入力後、承認者が承認したユーザだけアクセス
ゲスト （海外から来日）	ゲストアクセス （Web 認証）	guest	Facebook や Twitter 等の SNS アカウントでアクセス
Windows XP	−	windows-xp	無条件でどこにもアクセスできない
スマートフォン	−	smartphone	インターネットと一部の Web サーバのみ