Part 2 ベンダー動向

AP設置で広がるビジネス 照準は企業向けSI提案

自社サービスにユーザーを呼び込むため、各事業者による激しい競争が展開されているホットスポット市場。その裏ではネットワーク機器メーカー・ベンダー同士も火花を散らしている。無線LANのセキュリティ機能の強化やコンテンツ配信システムの提供等、事業者の法人需要を拡大させる製品、システムを展開するだけではなく、自らが事業者となり、無線LAN市場の拡大を狙うメーカーも登場している。パート2では、各社のホットスポット市場への取り組みをレポートするとともに、通信機ディーラーにとってどのようなビジネスチャンスが存在しているのか探っていく。

根強いセキュリティへの不安

パート1でも触れたように、ホットスポットサービスの事業を確立するためには、まずもって企業ユーザーを取り込んでいかなければならない。ホットスポット市場をターゲットにシステムを提供するメーカー・ベンダーでも自社製品やソリューションの強化を図る等、法人需要拡大のためのさまざまな施策を展開している。

各社が最初に着手したのは、企業がホットスポットを利用するにあたって最も不安な要素としてあげている「無線LANにおけるセキュリティの脆弱性」の解消だ。

従来の無線LANでは、セキュリティを確保する手段として、第三者による不正な侵入を遮断する「MACアドレスフィルタリング」や、情報の漏洩を防御するための暗号化技術「WEP(Wired Equivalent Privacy)」等が利用されてきた。

しかし、現状ではWEPのセキュリティホールの存在等、これらの技術の脆弱性が指摘されており、企業ユーザーの利用促進にブレーキをかけている。あるネットワークインテグレーターの技術者は、「WEPの解析ツールもインターネット上でフリーで配布されており、手馴れた人間ならほんの数分でトラフィックを解読できる」と警告する。

こうした問題に対してメーカー各社では自社の無線製品に対するセキュリティ機能の強化を進めている。その1つが、「IEEE802.1x/EAP」の実装とRADIUSサーバーとの連携だ。

メルコでは無線LAN製品「AirstatinProインテリジェントアクセスポイントWLM/WLM2シリーズ」でIEEE802.1x/EAPへの対応を実現している。

さらに同社では日本ルーセント・テクノロジーとパートナーシップを結び、ルーセントのIEEE802.1x/EAP RDIUS認証サーバー「Navis Radius」との連携による認証情報や各デバイスの管理と、堅固なセキュリティを実現している。メルコ・ネットワーク事業部マーケティンググループの柚木原功氏は、「WEPのセキュリティの脆弱さを不安に思っていたユーザーは多く、IEEE802.1xに注目が集まっている。キャリアだけではなく、企業からも今回のセキュリティソリューションに対して数多くの引き合いを獲得している」と語る。また、日本ルーセント・テクノロジー・エッジアクセスグループ、システムエンジニアの西村光生氏も、「国内無線LAN製品市場で圧倒的なシェアを持つメルコと提携することで私どものセキュリティソリューションの展開に一層の弾みをつけることができる」と期待する。

一方、シスコシステムズも「Cisco Aironetシリーズ」においてIEEE802.1x/EAPへの対応を行っているほか、EAPを独自に拡張させたLEAP(Lightweight Enterprise Authentication Protocol)を搭載している。さらに、同一アクセス環境内にあるクライアント同士の通信を無効にし、データをアップリンクだけに制限する新技術「PSPF(Public Secure Packet Forwarding)」を開発。これにより、他クライアントからデータを盗み見られてしまう「クライアント間アタック」を回避できるようにしている。

また、「Cisco Secure Access Contorol Server」などのEAP対応RADIUSサーバーを利用し、セキュリティや認証情報の中央集中管理を可能とする仕組みを提供している。

セキュリティの強化策として、最近注目を集めているのがホットスポット上でのVPNの実現だ。

具体的には、IPレイヤのVPNプロトコルであるIPsecを利用し、無線LAN通信においてもVPNを実現するというものだ。ユーザーのパソコンにIPsecクライアントソフトを搭載し、企業オフィス側にはVPN装置を設置、ユーザー・オフィス間の通信を暗号化することでホットスポットからでもよりセキュアな通信が実現する。

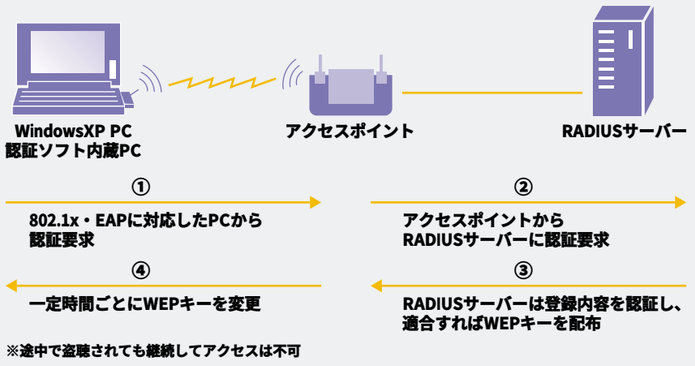
日本ルーセント・テクノロジーはメルコとの提携において、VPNファイアウォール製品「Brickシリーズ」とメルコのAirstationシリーズを組み合わせたソリューションの展開も進めている。

また、シスコシステムズも、同社のVPN装置「VPN3000シリーズ」とAironetシリーズを連携させ、セキュリティの強化を展開している。

メーカー各社によるセキュリティ機能の強化が果敢に進められているが、実際にホットスポットにおけるセキュリティの強化はこれからという事業者がほとんどのようだ。

あるネットワークインテグレーターの担当者は、「現在、各社が重視しているのは、サービスエリアの拡大であり、まず“陣取り合戦”に意識が向いている。セキュリティの強化等、付加価値の向上については次の段階での提供を計画しているようだ」と話している。

図1 802.1x/EAPとRADIUSサーバーの利用例



コンテンツ配信もサポート

日本エリクソン・事業開発本部先端モバイル技術部長の藤岡雅宣氏は、「セキュリティの強化に加え、ローミング機能とコンテンツサービスの提供がホットスポットの利用増には不可欠」と強調する。

現状のホットスポットサービスを見ると、特定の事業者と提携しているファーストフード店やコーヒーショップなどで無線アクセスをしたい場合、提供事業者のサービスに加入していなければ利用できない。そのため、すでに他の事業者のホットスポットサービスに加入しているユーザーは、そこでの利用を断念せざるを得ない。

しかし、「場所を問わない接続性」をホットスポットの第1のメリットとするならば、ローミングによる事業者を越えたシームレスな利用環境が提供されなければならない。

また、ADSL等の安価な高速回線が家庭にまで普及している現状では、追加で月額料金を支払ってでもホットスポットサービスを利用したくなるような付加価値の提供が重要になる。

こうしたニーズに対応できるインフラ構築のために、日本エリクソンでは、ホットスポットにおけるローミングとローカルコンテンツサービスの提供を実現するシステム「ノマディックP2P」を展開している。

ノマディックP2Pは、「モビリティ・

WEP
Wired Equivalent Privacy
無線LANの標準規格であるIEEE802.11のオプションとして提供されるセキュリティ機能。データを暗号化しMAC用データを付加、無線通信におけるエラーや改ざんをチェックする。最近、セキュリティホールの発見による脆弱性が指摘されており、暗号鍵を強化させた「WEP2」の仕様策定が進められている

RADIUS
Remote Authentication Dial In User Service：アクセスを希望するユーザーを認証するためのプロトコル。クライアントサーバー方式で作動し、RADIUSサーバーはユーザー情報を管理、ユーザーから送られてきたIDをチェックした後、ハッシュ関数のMD5を使ったチャレンジ・レスポンス形式で暗号通信を行いパスワード認証を実行する

IPsec
IP security protocol：インターネット標準プロトコルであるTCP/IPにセキュリティ機能を付加するプロトコルの総称。IPパケットの認証を行うAH(Authentication Header)とIPパケットの暗号化を行うESP(Encapsulating Security Payload)、および鍵交換(IKE:Internet Key Exchange)などが含まれている