Part 2 セキュリティ動向

新技術登場で不安払拭へ スイッチベンダーの参入相次ぐ

「無線LANの企業導入推進の最大のキーワードはセキュリティ」――提案活動を行っている、メーカー・SIベンダーの担当者は口を揃える。

既存の無線LAN製品ではセキュリティを確保するための手段として、①MACアドレスによるフィルタリング、②SSID等のID認証、③802.11bのオプション機能である暗号化技術「WEP(Wired Equivalnet Privacy)」――などが利用されていた。

しかし、今、これらのセキュリティ技術の弱点が問題視されている。

まず、①だが、MACアドレスによるフィルタリング機能はユーザー自身を認証するものではない。そのため、無線LANカードやPCを紛失したり盗まれた場合、悪意のある第三者によってネットワークに不正アクセスされてしまうことが起こりうる。

さらに最近では、盗聴ツールを用いることで無線LAN通信中のクライアントからMACアドレスを傍受し、「なりすまし」によって無線LAN経由で社内ネットワークに不正侵入されるケースもある。

②のSSIDは、クライアントとアクセスポイントに最大32文字の任意のコードを設定、アクセスポイントは同一のコードが設定されたクライアントのみ通信を行わせる技術だが、クライアントカード側のSSIDを設定しないで、「空白」または「ANY」にした場合、アクセスポイント側のSSIDが自動的に取得されてしまうという問題点がある。

さらに③のWEPにおいても、2001年、カリフォルニア州立大学バークレー校の研究者によってセキュリティホールの発見が発表されて以来、その欠点が次々に発見されている。

このように、現状の無線LANのセキュリティ技術は数々の欠点が広く知られるところになっており、「無線LANはセキュリティに対して脆弱」というイメージは簡単に払拭できなくなっていた。

進む認証と暗号化機能の強化

しかし、最近では従来の無線LANの欠点をカバーし、セキュリティを強化するための新たな技術が登場している。その代表が、①暗号化技術「WPA(Wi-Fi Protected Access)」、②ユーザー認証規格「IEEE802.1x」――だ。

①のWPAは、固定暗号鍵を用いるWEPに対して動的暗号鍵を使用したより強固な暗号化機能に加え、ユーザー認証の仕組みを持った技術。

無線で通信されるデータは、固有の暗号鍵を使用して暗号化されるとともに、暗号鍵を自動的に生成し配布する「TKIP」(Temporal Key Integrity Protocol)と呼ばれる技術を用いることで堅牢なセキュリティを実現する。

無線LAN規格の標準化組織であるWi-Fiアライアンスが8月31日以降、無線LAN製品のWi-Fi申請に際してWPAへの対応を必須条件としたことからも、今後一層の普及が予想されている。

実際、各メーカーでは自社製品へのWPAの搭載を進めており、間もなく対応製品の市場投入が開始される見込みだ。

WPAの登場に対してSI側の反応はどうか。

データクラフトジャパン・マネージドサービス本部エンジニアリンググループチーム3の矢萩陽一チームリーダーは、「実際の運用にあたって、WPAを用いた場合の実行速度はどの程度になるのかを考えていかなければならない。また初期段階ではメーカー各社のインプリメントの方式にも差が出てくるので、当面は各社の動向を見極めながら、実製品が登

SSID
無線LANにおいて、特定のクライアントと接続するための識別コード。SSIDを用いてワイヤレス通信を行う場合は、アクセスポイントと同じSSIDを無線クライアント側に設定する