第2特集 便利で快適！ワイヤレスオフィスの作り方

Part 4 歴史から振り返る

ワイヤレスLAN環境セキュリティと無理のない運用

株式会社ライブドア
伊勢 幸一 *ISE Kouichi*
情報環境技術研究室　執行役員 CTA室長

無線（ワイヤレス）LAN環境は瞬く間に普及し、普通に皆さん使うものになりました。本章では、セキュリティについて歴史から振り返り、広域無線LANサービス運用のケーススタディをベースに、オフィスで使用方法の注意点を解説します。

無線LANの始まりをひもとく

ブロードバンド元年

西暦2001年、SFの世界ではHAL9000を載せたディスカバリー号が木星を目指し、モノリスがヒトに大きな変革をもたらすことになっていますが、筆者達を取り巻くインターネット環境にも大きな変革がありました。それまでインターネットといえば、電話回線を利用したダイヤルアップによって数十kbps程度の速度で接続していましたが、ADSLという高速広帯域通信技術によってアナログ電話回線を用いた数Mbpsでの常時接続ができるようになり、この2001年をブロードバンド元年と呼びました。

無線LAN元年

そしてもう1つの大きな変革が無線LANの出現です。無線LAN自体はかなり以前からありましたが、通信速度が1～2Mbpsといった低速ネットワークにもかかわらず、親機（アクセスポイント：以後AP）が数十万円、子機（ステーション：以後STA）側でも十数万円とたいへん高価な機器を必要とし、PCにビルトインされている10/100MbpsEthernetに比べるとあまりメリットがありません。したがって無線LANは一部の特別な用途にだけ利用されるにとどまり、通常のPCユーザ、インターネットユーザが利用するケースはほとんどありませんでした。

ところが、1999年に最大11Mbpsの高速無線LAN規格802.11bが採択され、これに呼応する形で2000年にApple社がAPで数万円、STAアダプタが1万円台という格安無線LANデバイスAirMac（海外ではAirPort）を発売します。そして翌2001年、ブロードバンド元年とシンクロするかのようにIBM社から無線LAN機能内臓のThinkPad S30という製品が出荷され、PCがSTAアダプタや周辺機器なしで無線LANを利用できるようになったのです。

このころ、国内のPC周辺機器メーカーはAP機能つきADSLルータを1万円台で提供するようになり、瞬く間に一般家庭内に無線LAN環境が浸透していくことになります。

さらに2003年には最大54Mbpsの802.11gが標準化され、2004年にはニンテンドーDSやソニーPSPといった小型ゲーム機にも無線LAN機能が内蔵されるようにもなり、無線LANが身近なネットワークとなってきます。そして、その潮流はエンタープライズ環境へも影響を与え、オフィス内LANが無線化されるケースが増えていきます。社員の席が決まっていないフリーアドレス方式のオフィスではEthernetではなく社員全員が無線LANによってイントラシステムにアクセスする環境も見かけるようになりました。

無線LAN環境のセキュリティ

セキュリティ問題

企業のオフィスで無線LANを導入しようとするとき、最も懸念される事項にセキュリティがあります。もちろん無線LANにおける最適なAP設置計画や、APから社内LAN環境とのネットワークをどうするかという検討も必要ですが、全社員に100BASE-Tコネクティビティを提供するような大規模LAN構築に比べると、それほど重大なファクターではありません。むしろ無線LANの導入において重要なことは、どのように情報セキュリティを保全するかという一点に尽きるといっても過言ではないでしょう。

情報セキュリティとは情報の機密性、完全性、可用性を保つことですが、LAN環境においてはネットワークシステム内での盗聴、なりすまし、改ざんを防止することになります。無線LANでは無線通信の特性上、STAとAP間の通信データは同じ通信範囲であればどのSTAでも受信できます。したがって、STAとAP間の通信データに平文を使うと、周囲のSTAから、その内容は丸見えとなってしまいます。そこで、最低限STAとAP間の通信を暗号化し、盗聴(正確には盗聴されても内容が解読できない)を防ぐ必要があるのです。

暗号化方式概略

現在、この無線LANのセキュリティ対策にはWEP(Wired Equivalent Privacy)とWPA(Wi-Fi Protected Access)というプログラムが広く利用されています。しかし、これらの暗号化アルゴリズム、認証方式の組み合わせが複雑であるため、セキュリティの専門家でなければ全体を正確に把握することが難しくなっています。もともと無線LANに関する暗号化、認証方式の規格はIEEE802.11シリーズの中で規定されており、WEP、WPAという規格名はWi-Fi Allianceという組織が802.11シリーズに準拠して作成した相互接続性認証プログラムの名称です。このあたりからすでに混乱の兆しを発していますが、これら認証プログラムは次に示すような暗号化と認証、そして改ざん防止という要素から構成されています。

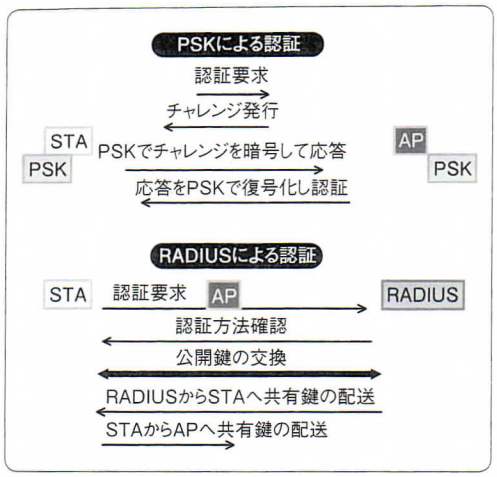
●暗号化方式

現在無線LANで利用されている暗号化方式として、WEPでは64ビットと128ビットのRC4アルゴリズムが利用され、WPAではWEPのRC4をベースに鍵の生成方法や通信途中での鍵変更といった改良を加えたTKIP(Temporal Key Integrity Protocol)がサポートされています。また、WPA2では128ビットAESをベースにしたCCMP(Counter-mode CBC-MAC Protocol)が使われています。最近では変則的にTKIPのアルゴリズムにRC4ではなく128ビットAESを利用できるWPA機器や、CCMPではなくTKIPが使えるWPA2機器もあるようです。

●鍵配布方法と認証

無線LANにおける暗号鍵方式は基本的に共有鍵(秘密鍵)方式です。その鍵の配布方法には鍵をあらかじめSTAに配布するPSK(Pre Shared Key)パーソナルモードと、接続要求ごとに鍵を配布するエンタープライズモードに分けられます。同時に鍵の配布方法によってSTAがAPに接続する際の認証方式が決まり、パーソナルモデルは共有鍵が一致しているかどうかだけで認証し、エンタープライズモードは事前にSTA側に配布されたデジタル証明書(サプリカント:PEAPのようにサプリカントが不要な認証方式もあります)とAPとは別途用意されたRADIUSサーバとのEAP-TLSによって認証を行います(**図1**)。エンタープライズモードも通信データの暗号は共有鍵方式ですが、共有鍵の交換に公開鍵方式が利用され、安全にSTAとAP間で共有鍵を交換することを可能にしています。

▼図1　PSKとRADIUSによる認証



● 改ざん検出方法

改ざん検出ではWEPとWPAで利用されているICV(Integrity Check Value)と、WPA2で利用されているMIC(Message Integrity Code)の2種類があります。各WEP、WPA、WPA2において利用されている認証、暗号、改ざん検出方式の組み合わせを**表1**に整理しておきます。

それぞれの詳細内容は専門記事や文献をご参照いただくとして、ここでは無線LANでのデータ通信にはEthernetなどの有線通信とは異なり、データリンクレベルでの暗号化がたいへん重要視されていることを理解していただければ十分でしょう。

WEP/WPAの問題点と課題

しかし、これらの暗号化方式によって完全に盗聴、なりすまし、改ざんが防止できるわけではありません。2002年の時点でWEP暗号が第三者に解読可能であるという報告があり、あとに中間者攻撃によって1分もかからず鍵が解読できるという論文も2007年に公開されています。WPAに関しても2004年に辞書攻撃に対する脆弱性が指摘され、2009年にはWPA-TKIPが数分で解読できてしまうという報告がなされています。今のところ、WPA2の脆弱性に関する情報は公開されていませんが、これもセキュリティの研究が進むに伴い、いずれは何らかの脆弱性が指摘される可能性はあります。

これら報告されている脆弱性は、それぞれWEPやWPAの暗号化鍵を知らない第三者が暗号化されたSTA-AP間通信フレームを傍受することで、その鍵が解読できるというセキュリティ障害です。しかし、通常公衆無線LANや企業内オフィスでの無線LANでは利用者全員が同じWEPキーやWPAキーを共有利用するのが一般的であり、共有鍵方式における「鍵の機密性」が最初から破綻しています。つまりWEPでもWPA、WPA2であってもPSKによる事前鍵配布をしている限り、セキュリティ対策がまったく施されていないのと同じです。

もし、オフィスユースにPSK方式で鍵を配布するのであれば、少なくとも社員の入退職に伴い鍵を変更し再配布する必要がありますが、人事情報の更新と情報システムデータとの連動はどこの会社でもなかなかうまくリンクしないものです。また鍵が更新されたことに気づかない社員からネットにつながらないという膨大な問い合わせに対処することなるのは明白です。したがって、本来企業内オフィスにて無線LAN環境を導入するにはWPA2とRADIUS認証によるエンタープライズ方式にするべきですが、この場合でも社員全員の端末にサプリカントを配布する運用はシステム管理者にとって大きな負担となり、また証明書コストもバカになりません。どちらにしてもたいへんな労力とコストが課せられることになります。

▼表1　暗号化方式チャート

	WEP	WPA	WPA2
パーソナルモードPSK	64/128ビット RC4 ICV	64/128ビット RC4＋TKIP ICV	128ビット AES＋CCMP MIC
エンタープライズモード		64/128ビット RC4＋TKIP ICV EAP＋RADIUS	128ビット AES＋CCMP MIC EAP＋RADIUS

ライブドアケーススタディ

本誌10月号第2特集『あなたの会社のネットワーク管理、どうしていますか？』で「第4章ライブドアの流儀から考える、社内システム効率化の課題」でも触れましたが、筆者の社内ネットワークはツイストペアケーブルによるEthernet LANと無線LANとを併用した構成になっています。2005年からlivedoorWirelessというブランドで公衆無線LANサービスを提供しており、オフィス内無線LANはその公衆無線LANサービスの基盤をそのまま流用していると述べました。ここで、ケーススタディとしてライブドアの社内無線LANの概要を紹介しますが、前述のとおり基盤が公衆無線LANの流用であることから一般的な企業内無線環境とは異なる状況にあるかもしれません。

簡単にlivedoorWirelessのスペックを**表2**に示します。livedoorWirelessとその基盤を流用した社内無線LAN環境を認証の観点からみた全体システム構成を**図2**に示します。

▼表2　livedoorWirelessサービス要項

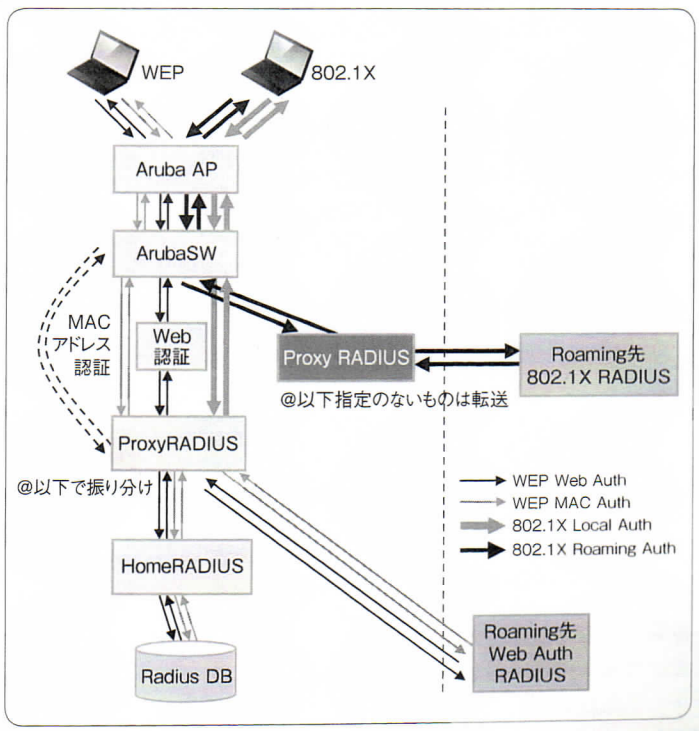
対応エリア	東京都、千葉県、神奈川県、埼玉県、その他一部地域
アクセスポイント設置場所	東京電力柱（山手線圏内）、カフェ、飲食店、商業施設、大型家電量販店など
利用料金	初期設定費用　1,050円（税込）、月額利用料　525円（税込）
無線LAN規格	IEEE802.11b/gに準拠
セキュリティ	128bit WEPキー、16進数・ASCII
ログイン認証	IDとパスワードによるWebブラウザでの認証 MACアドレスによる認証

AP従属問題

livedoorWirelessにおけるAP従属はWEPキーのみによる認証です。したがってAPへの従属はWEPキーさえ知っていれば会員でなくとも誰でもできます。オフィス内無線LANではAP従属の時点でSTAのMACアドレスによるフィルタリングを施すケースがありますが、公衆無線LANにおいて一般利用者のMACアドレスをすべて登録申請してもらい、AP従属認証をMACアドレスによって行うというのは現実的ではありません。またオフィス内用であっても、利用者のSTAすべてのMACアドレスフィルタをメンテナンスすることはたいへんな作業であり、また突発的な来客や暫定的な利用に対し、すべて事前にMACアドレスの登録が必要となると著しく利便性を損ないます。

APへの無許可STAの従属を制限しなければならない理由は何でしょうか？　もちろん非常に多くの無許可STAが1つのAPに従属するとAP-STA間の性能が劣化していきますが、正規のSTAの通信を阻害するほどの無許可STAを

▼図2　livedoorWirelessシステム概要



APの電波の届く範囲で大量に用意し、APに対してDoS攻撃を行う者が社内にいるとは考えにくく、また悪意のある部外者が行う可能性があるとしても、それはオフィス内や敷地内への不信人物の侵入を許していることを意味するのでまったく別のセキュリティ問題でしょう。

インターネット接続認証

APへのDoS攻撃より、無許可STAが自社ネットワークからインターネット側へスパムやマルウェアを送出したり、外部サーバへのアタックなどが行われたりするほうが問題です。つまり、無許可STAに対してはそのSTAがAPからインターネット側にパケットを送出できないようにするだけで十分なのです。livedoorWirelessではSTAのインターネット接続に対し、Webサイトでユーザ IDとパスワードによる認証とMACアドレス認証によって行っています。通常はAPに従属したあと、STAがインターネットにアクセスしようとした時点で認証ページにリダイレクトし、IDパスワードによって認証します。あらかじめ会員ページから利用する携帯ゲーム機や携帯端末のMACアドレスを登録しておくと、AP従属した時点でMACアドレスによる認証を行い、登録されているMACアドレスと一致した時点でインターネットアクセスの認証が行われインターネットへの接続が可能となるようになっています。

SSL化の重要性

無線LANに限らず、ISPによるインターネット接続サービスではネットワーク側での暗号化、認証等々の処理は施されていません。したがって、STAとAP間がどのように強固なセキュリティで守られていたとしてもSTAからインターネット上のサイトに対し、平文でアカウントとパスワードを入力したり、クレジットカード番号などを入力したりしてしまうと、経路途中において個人情報の盗聴、改ざんの恐れがあります。これは無線LANセキュリティとは別の問題ですが、個人情報や決済情報などを入力する場合、そのサイトとの通信がSSL化され、デジタル証明書発行などのセキュリティ対策がなされているかどうかを確認することが大切です。また個人情報に限らず企業情報や秘匿情報をインターネット側から利用する場合でもSSL化された安全なセッションで行うべきでしょう。逆に言うと、サーバと端末間のセッションが常にSSLによる安全なセッションで保たれるのならば、STAとAP間の通信を二重に暗号化する必要はないことになります。

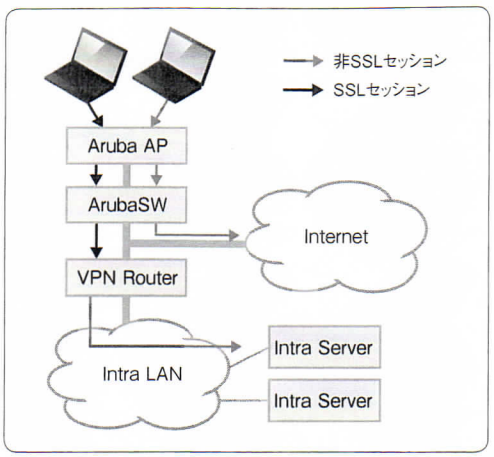
ライブドアのSSL用法

社内イントラネットのサーバ群は基本的に社内LANからのみアクセスされることを前提としているので、各サーバはSSL化されていません。つまりWebサーバはHTTPSではなくHTTPであり、メールサーバもPOPSやIMAPSではなくPOP、IMAPです。またファイルサーバなども接続する際のユーザパスワード認証はありますが、NetBIOSやNBT、NFSセッションがSSL化されているわけでもありません。

したがってファイアウォールやProxyを介してイントラシステムにアクセスする場合、そのままでは社内機密情報がインターネット上を平文で通過することになりセキュリティ上大きな問題となります。そこで、インターネット側から社員がイントラシステムにアクセスする場合にはSSLをサポートするVPNルータを介して社内イントラシステムと端末との間に安全なトンネルを張って行われます。

ライブドア社内無線LANのAPは公衆無線LANと同様にグローバルインターネットセグメントに接続されています。当然ながら社内イントラネットに直接アクセスすることはできません。そこで社内無線LANからイントラネットにアクセスする場合でもこのVPNトンネルが利用されます。そのためSTA-AP間が特に暗号化されていなくても、社内情報が経路途中で盗聴さ

▼図3　VPNルータを介した無線LANからのイントラアクセス



れ改ざんされる危険性は非常に低くなっています。つまり脆弱性が指摘されているWEPによる無線LAN通信であっても傍受したデータはSSL化されているため第三者に解読されることはほとんどありません(**図3**)。

このように、より上位のレイヤで安全な通信を担保することで、無線LAN通信のもつ脆弱性をカバーしているのです。もちろんフリーアドレスオフィスのように全社員が常に無線LANによってイントラシステムを利用するような場合にはそれ相応の性能を持つ高価なVPNルータを複数接地する必要も出てきますが、ライブドアでは常時自席で利用するものではなく、会議や打ち合わせ、面会など、自席から離れた場所でイントラシステム情報を閲覧する場合に利用されるため、EthernetLANと同じ性能が必ずしも要求されるわけではなく、低価格なVPNルータで事足りているのです。

オフィス用無線LANの運用

オフィス内無線LANの利用において情報セキュリティ施すには2つの考え方があります。1つは現段階でもっとも安全だと評価されているWPA2によって盗聴、なりすまし、改ざんを防止することです。もう1つはWEPやWPAといったPSKによる最低限のセキュリティ対処を施し、Webサーバとブラウザ間、メールサーバとメーラー間などの通信をSSL/TLS化することによって保全を図るという方法があります。

フリーアドレス方式によって全社員が無線LANを利用する環境では前者が適しており、打ち合わせや会議などそれだけの一時的な無線LAN利用であれば後者が適しています。ただし、後者の場合、すべてのサーバのセッションをSSL化し、すべてに正規のSSL証明書をインストールするとかなりのコストが発生するので現実的ではありません。SSL-VPNルータなどを介在させ無線LAN網とイントラネット間のセキュリティを集約すると良いでしょう。

終わりに

ネットワーク環境やイントラシステムを構築する上でセキュリティを軽視することがあってはなりませんが、セキュリティにこだわり過ぎるのも程度問題です。結局システムや技術によって100%安全なセキュリティを実現することは不可能であり、最終的にはユーザのモラルとリテラシに依存するため、どんなにコストを掛けて投資をしても利用者であるユーザしだいでその投資は無意味と化してしまいます。

問題はユーザのモラルとリテラシを考慮したうえで、システムやネットワーク側でのセキュリティをどのレベルで担保するかということです。これはそれぞれの目的用途と規模、そして環境事情により決定するものであり、これらを考慮せず、すべてのレイヤでセキュリティ機関から推奨される最強レベルのセキュリティ対策を施すことは無駄です。

情報セキュリティというものは最終的にユーザによって担保されるものであり、暗号化技術、認証方法はその補助的なツールでしかないという事実を認識し、システムの構築を実施すべきであると考えます。SD