無線LANセキュリティサポート技術

Wireless LAN Security Support Technologies

大下　敏明　■OSHITA Toshiaki
高木　雅裕　■TAKAGI Masahiro
奥田　健一　■OKUDA Kenichi

通信速度の高速化，機器の低価格化に伴って市場に広がり始めた無線LANシステムは，今までのLANシステムと異なり，無線LAN機器の設定が管理されていないと第三者が不正にLANシステムにアクセスするなど，セキュリティが重要な要素であることが明確になってきた。しかし，単純に無線LANシステムに暗号化技術や認証技術を取り入れるだけでは，使い勝手の悪いものになってしまう。東芝ソリューション(株)と東芝は，ユーザーにとって利便性の良い無線LANセキュリティ技術として，WirelessServ$_{TM}$ MobileGateと東芝無線LANセキュリティツールを開発した。

Wireless LAN systems featuring improved transmission speeds and low-cost equipment have appeared on the market. Unlike wired LAN systems, however, additional security measures must be taken into consideration because unauthorized access by attackers may occur if a wireless LAN system is not properly managed. On the other hand, the adoption of encryption technology and user authentication technology may make the system less user-friendly.

In response to this situation, Toshiba Solutions Corp. and Toshiba have developed WirelessServ$_{TM}$ MobileGate and the Toshiba wireless LAN security tool as wireless LAN security support technologies for the convenience of users.

1　まえがき

無線LANシステムのセキュリティについては，様々な方式で無線LAN機器ベンダーが実装している。IEEE802.11b(米国電気電子技術者協会規格802.11b)で採用されているWEP(Wired Equivalent Privacy)，その脆弱(ぜいじゃく)性を改善するために開発されたWPA(Wi-Fi®(注1) Protected Access)，IEEE802.1Xによる認証・鍵配布とWEPを組み合わせたセキュリティなどがある。

併せて無線LANのデータ転送速度の高速化も進んできて，無線LANシステムの仕様は乱立状態にある。

このような背景において，無線LANシステムのセキュリティに求められる要件は以下のように定義できる。

⑴　コストパフォーマンスが良く，強いセキュリティ
⑵　オフィスで利用できるスケーラビリティ
⑶　容易な運用管理
⑷　既存の無線LAN機器への適用性
⑸　セキュリティ機能を利用し，ユーザーにとって利便性の良い付加機能

東芝ソリューション(株)と東芝は，これらの要件を満たすために2種類のセキュリティサポート技術を開発した。

一つは，無線LANシステムを複数のネットワークセグメント(事務所と会議室あるいは社内移動先など)で構築し，無線LANシステム内で安全にノート型パソコン(PC)などを移動して使用できる環境の構築をサポートするWirelessServ$_{TM}$ MobileGate(以下，MobileGateと略記)である。

もう一つは，無線LANを既に構築した小規模なネットワークセグメントで無線LANシステムのセキュリティを強化する，東芝無線LANセキュリティツール(TOSHIBA Wireless Security：以下，TWSecと略記)である。

ここでは，これらのサポート技術が，どのように無線LANシステムのセキュリティに求められる要件を実現しているかについて述べる。

(注1)　Wi-Fiは，米国Wi-Fi Allianceの登録商標。

2　MobileGateによる無線LANセキュリティのサポート

MobileGateは，インターネット標準のMobile IP(IP Mobility Support for IPv4/RFC3344)とIPSEC(Security Architecture for the Internet Protocol/RFC2401)とを用い，先に定義した無線LANシステムのセキュリティ要件を満たす商品である。

2.1　データ暗号化と付加価値の実装

MobileGateはサーバのWindows®(注2)上で動作するサーバソフトウェア(以下，MobileGateサーバと略記)とWindows®ノート型PC上で動作するクライアントソフトウェア(以下，MobileGateクライアントと略記)で構成されている。

このMobileGateサーバとMobileGateクライアントは，Windows®のTCP/IP（Transmission Control Protocol/Internet Protocol）ドライバの下位に位置づけられる中間ドライバとして動作する（MobileGateドライバソフトウェア）。このため，サーバ上のアプリケーション及びノート型PC上のアプリケーションからは直接，無線LANセキュリティサポート機能が見えない仕組みになっている。

Mobile IP技術とは，エージェント機能（ホームエージェント，フォーリンエージェント）が保持するパケットカプセリング転送機能と，モバイルノード機能が保持するパケットデカプセリング機能，移動先検出・登録機能により実現される，ネットワークやそれに接続するコンピュータに影響を与えないモバイルサポートプロトコルである。

Mobile IPの機能を実現するため，MobileGateサーバにはMobile IPのホームエージェント機能とフォーリンエージェント機能を，MobileGateクライアントにはMobile IPのモバイルノード機能を実装している。MobileGateクライアントをふだんネットワークを利用している事務所から別フロアにある会議室などに移動するとモバイルノード機能が働き，MobileGateクライアントのモバイルノード機能が“MobileGateサーバのフォーリンエージェント機能経由ホームエージェント機能に移動登録”というパケットを定期的に送付する。その後，MobileGateクライアントはパケットを送信する際に必ずMobileGateサーバを経由する。MobileGateクライアントあてのパケットはMobileGateサーバが代理で受信し，移動先のMobileGateクライアントに転送する。これによりMobileGateクライアントユーザーは，どこに移動しても事務所のネットワークと同じ環境を手に入れることができる。この際に合わせて，MobileGateサーバとMobileGateクライアントで実装しているIPSECの機能により，MobileGateサーバとMobileGateクライアントでやり取りされるパケットは，無線LAN機器でサポートされている暗号アルゴリズムよりも強力なトリプルDES（Data Encryption Standard）によって暗号化される（**図1**のケース1）。

Mobile IPでは，移動していないモバイルノードは通常のパケットのやり取りとなってしまう。MobileGateクライアントも単純な実装では，移動していない事務所などのネットワークでは通常のノート型PCとして動作してしまい，パケットの暗号化が行われない。このため，Mobile IP機能を拡張し，移動していないネットワークでもパケットが暗号化されるように実装を行った。具体的にはMobileGateサーバではMobileGateクライアントが移動していない場合でもロケーションを把握し，MobileGateクライアントあてのパケットを代理で受信し，MobileGateクライアントに暗号化して転送する。MobileGateクライアントは，すべての送信パケットをMobileGateサーバに暗号化して送信する（図1のケース2）。

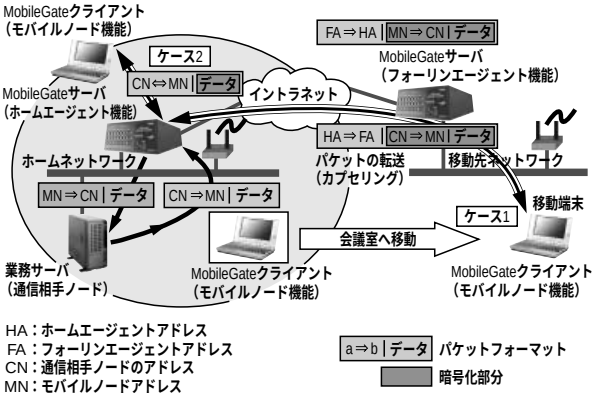

図1．WirelessServ™ MobileGateの動作概要 ― 事務所でも移動先でもデータ暗号化により安全に通信が行える。

Operation of WirelessServ™ MobileGate

2.2 アクセス制御のサポート

今日，IEEE802.11bで採用されているWEP方式の脆弱性を改善するため，IEEE802.1Xによる認証・鍵配布とWEPを組み合わせた無線LANセキュリティ方式が無線LAN機器ベンダーから各種リリースされている。しかし，無線LANシステムを一つのベンダーに統一しなければならなかったり，デジタル証明書をすべてのノート型PCにインストールし運用管理しなければならないなど，無線LANシステム導入者や無線LANシステム管理者に対する負荷は大きなものとなってきている。このため，無線LANシステムを容易に導入できるようにアクセス制御機能も実装した。

図2のように，MobileGateサーバをLANインタフェースが2個あるサーバにインストールする。そしてLANインタフェースの片側を無線LANのアクセスポイントのみのネットワークとする。この構成は無線LANのセキュリティを確保する際によく用いられる“無線LANのDMZ（DeMilitarized Zone：非武装地帯）”という方式である。通常のサーバでこの構成を実現すると，サーバがルータと位置づけられ二つのネットワークセグメントとなる。二つのネットワークセグメントになると，一つの部門に二つのネットワークが存在し，ネットワーク管理者が二つのIPアドレス体系を管理する必要がある。このため，MobileGateサーバではサーバの片側のLANインタフェースにブリッジタイプのドライバを実装し，サーバがあたかも一つのネットワークで動作するように実現した。そして，このドライバと連携してネットワーク機器やサーバのアクセス認証に使用されるRADIUS（Remote Authentication Dial-

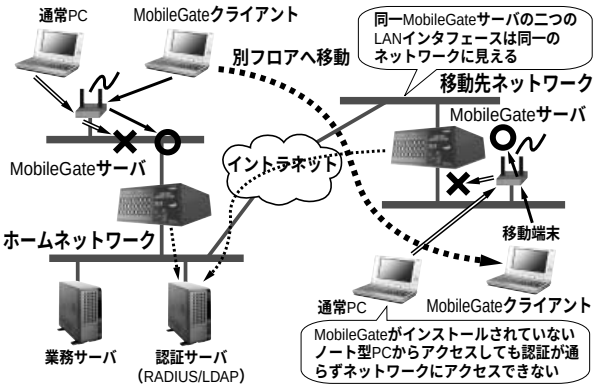

図2．アクセス制御の適用例 ― 通常のノート型PCでは基幹ネットワークに入ることができない。

Example of application of access control

In User Service)，LDAP(Lightweight Directory Access Protocol)への利用者認証サービス機能を動作させた。あわせてブリッジタイプドライバは，ネットワークレイヤレベルのパケットフィルタリングを実現することで，ネットワークに影響を与えず無線LAN機器を選ばないアクセス制御機能を実現した。

2.3　容易な運用管理とスケーラビリティの実現

このほか，運用管理を容易にするためMobile IP環境下でのDHCP(Dynamic Host Configuration Protocol)完全サポート(Mobile IPではモバイルノードに固定のIPアドレスを付与することが前提であるが，固定のIPアドレスを必要としない実装を実現)やMicrosoft®(注3)のActive Directory(ディレクトリサービス)から登録ユーザー名を参照する機能，設定情報をダウンロードする機能などを実現した。また，部門内のサーバにインストールして使用する規模(移動メンバーが20人程度)を想定し商品化を行った。これにより，ユーザーが求める無線LANシステムのセキュリティ要件を満たす商品となった。MobileGateは，当社のワイヤレスソリューションであるシームレスオフィス™でも使用されている。

3　TWSecによる無線LANセキュリティのサポート

ここでは，既に構築済みの比較的小規模な無線LANセグメントのセキュリティを強化するため試作したTWSecの概要を述べる。

TWSecは，ネットワーク層(IP層など)ではなく，リンク層(Ethernet(注4)層)においてデータを保護するセキュリティプロトコルである。主な機能は次のとおりであり，**図3**のようなネットワーク構成で使用される。

⑴　無線LAN端末とネットワーク間の相互認証に基づくセッション鍵の共有

⑵　リンク層フレームの秘匿，送信元の認証，第三者による改ざんと再利用の防止

認証サーバとTWSecブリッジの機能を同一のノードで動作させる小規模な構成も可能である。

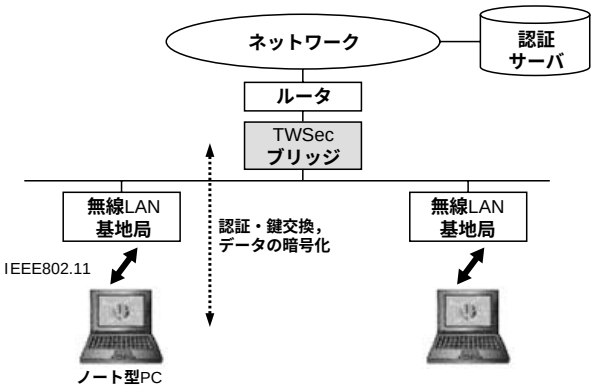

図3．TWSec使用時のネットワーク構成 ― TWSecは無線LAN端末とネットワークの間のブリッジとして動作し，セキュリティ機能を実現する。

Network configuration at time of TWSec use

3.1　認証及び鍵交換

最初に無線LANを使用する端末とTWSecブリッジは相互認証を行う。認証が成功していない段階では，端末から送信されたデータフレームはTWSecブリッジですべて破棄される。これにより権限のない端末がネットワークにアクセスすることを阻止できる。また，端末によるTWSecブリッジの認証は，端末が悪意のある第三者に接続されることを防止する。

端末を認証するために必要となる一連の情報は，TWSecブリッジを経由して認証サーバへ送られる。認証が成功した場合は，端末とTWSecブリッジとの間でデータフレームを暗号化して送受信するのに必要な情報(セッション鍵(暗号化用，認証用)，有効期限など)が，認証サーバからTWSecブリッジ及び端末に安全に送られる。これらのやり取りは，Needham Schroeder Protocolと呼ばれる共通鍵方式の認証・鍵交換プロトコルをベースとしている。端末認証のための情報を認証サーバに集中しているため，基地局の数が増えた場合でも管理は比較的容易である。

3.2　データフレームの暗号化と認証

認証・鍵交換が完了すると，端末はTWSecブリッジとの間で暗号化されたデータフレームのやり取りを行えるよ

(注2)，(注3) Microsoft,Windowsは，米国Micrisoft Corporationの米国及びその他の国における登録商標。

(注4) Ethernetは，日本における富士ゼロックス(株)の商標。

うになる。

端末が使用する暗号化用のセッション鍵には，端末からの上り・下りそれぞれの通信に対して，ユニキャスト通信用とブロードキャスト通信用の計4種類のものがある。ユニキャスト及び端末からの上り方向のブロードキャスト用の鍵は端末ごとに固有であるため，他の正規のTWSec端末から通信内容をのぞき見られることはない。一方，下り方向のブロードキャストフレームは正規のすべての端末で受信されるべきものであるため，すべての端末で共通に所持しているブロードキャスト用の鍵を用いて暗号化される。

また，暗号化に使用するアルゴリズムは，任意の方式を選択することが可能なようになっているが，デフォルトではAES（Advanced Encryption Standard）128ビットをCBC（Cipher Block Chaining）モードで使用する。AESは米国でDESの後継として選ばれた暗号化アルゴリズムで，セキュリティの強度と計算時間の早さが特長である。

また，暗号化して送受信するデータフレームにはMAC（Message Authentication Code）と呼ぶ認証用のコードを付加する。これは，送受信されたデータフレームが第三者によって改ざんされていないことと，データフレームを送信した相手が正しいことを証明するために必要となる。デフォルトではHMAC-MD5（Keyed Hashing for Message Authentication Code-Message Digest 5）と呼ばれるアルゴリズムを使用してMACを生成する。

TWSecを用いる場合のプロトコルスタックを**図4**に示す。本来送信すべきEthernetフレームをTWSecフレームとしてカプセル化して送信するため，上位層のプロトコルがIP以外でも適用できる。また，既存の無線LAN基地局とは別の装置として，TWSecブリッジを設置することが可能である。この場合，図1に示したように複数の無線LAN基地局のセキュリティ機能を一台のTWSecブリッジで賄うことが可能になる。

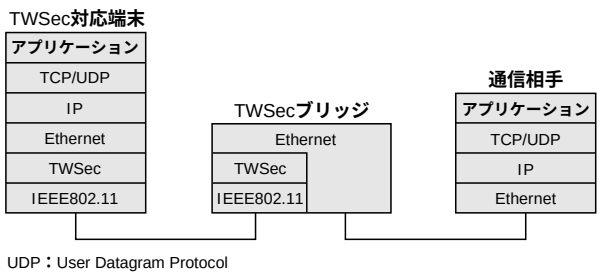

図4．プロトコルスタックの構成 ― Ethernetフレームをカプセル化するのが特長である。
Composition of protocol stack

3.3 動作環境と性能評価

TWSecはWindows® 98SE, 2000, XP及びLinux，BSD（Berkeley Software Distribution）（FreeBSD, NetBSDなど）といった様々なプラットホームの上で動作する。

TWSecをIEEE802.11bの無線LAN上で実際に動作させた場合の評価結果を**図5**に示す。WEPを用いる場合とほぼ同等のスループットを維持したまま，セキュリティを向上できることがわかる。

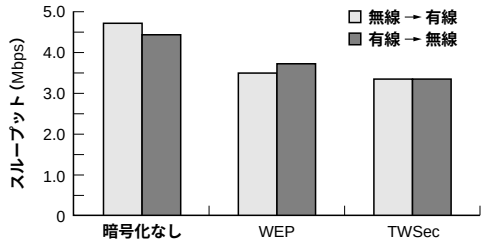

図5．性能評価結果 ― WEPと同等のスループットを実現した。
Performance evaluation result

4 あとがき

小規模な無線LANシステムのセキュリティはTWSec，複数部門やロケーションが介在する無線LANシステムのセキュリティはMobileGateと，様々なシステムの規模に応じた技術の適用が可能となった。

今後無線LANシステムのセキュリティは，共通の技術かつ強固なセキュリティ強度と認証機能を実装した商品が市場に広がってくると予想される。今後も最新の無線LANセキュリティサポート技術を開発し，商品やサービスへの展開を図っていく。

大下　敏明　OSHITA Toshiaki
東芝ソリューション（株）プラットフォームソリューション事業部参事。ネットワークソフトウェアの開発及びカスタマーサポート業務に従事。情報処理学会会員。
Toshiba Solutions Corp.

高木　雅裕　TAKAGI Masahiro
研究開発センター 通信プラットホームラボラトリー研究主務。ネットワークプロトコルの開発に従事。電子情報通信学会会員，ACM会員。
Communication Platform Lab.

奥田　健一　OKUDA Kenichi
東芝ソリューション（株）プラットフォームソリューション事業部主任。ネットワークソフトウェアの開発及びカスタマーサポート業務に従事。
Toshiba Solutions Corp.