セキュリティを向上させた無線LANアクセスポイント

Enhanced-Security Wireless LAN Access Points

鈴木　康一　■SUZUKI Koichi
渡邉　博之　■WATANABE Hiroyuki
落合　民哉　■OCHIAI Tamiya

ポータビリティを特長とする無線LANは，近年，通信速度の高速化が実現されたことにより急速な伸びを示している。しかし，無線を使っているため，有線によるネットワークに比べて盗聴や侵入の危険が高いことが問題となっている。

これを解決するため東芝では，セキュリティを向上させた無線LANアクセスポイントを開発した。この装置は企業や官公庁，通信事業者のように強固なセキュリティが必要な顧客に最適であると考えている。今後は，標準化の動向やユーザーのニーズに合わせて，更に機能の拡充を進めていく。

Wireless LANs have rapidly progressed in recent years as higher communication speeds have become available in addition to the advantage of portability. However, because they use radio frequency technology, wireless networks are more at risk from tapping and hacking compared to a hard-wired network. Secure wireless LANs are therefore desired.

To meet these requirements, Toshiba has developed enhanced-security wireless LAN access points for users requiring high security including corporations, public offices, and communication common carriers. We will continue to improve this technology to satisfy users' needs in the future.

1 まえがき

ブロードバンド・モバイル時代を迎え，これまで無線LANは家庭向け用途を中心に急速な伸びを見せている。ところが無線という性格上，セキュリティ対策が不十分であると外部から盗聴されたり侵入されたりする可能性がある。特に，ネットワークの規模が大きく重要なデータを扱っている企業・官公庁，通信事業者では強固なセキュリティが必要となっている。

これに対し東芝では，⑴IEEE802.1X（米国電気電子技術者協会規格802.1X）対応をはじめとする強固なセキュリティ，⑵IEEE802.11a/b/gの各種クライアントを同時に収容し，最大伝送速度54 Mbpsを実現する高性能，⑶屋内／屋外設置を問わず，種々のシステム要求に対応できるフレキシビリティを特長とする無線LANアクセスポイントを開発した。

以下に，この装置が適用されるアプリケーション例と，前記の三つの特長について述べる。

2 アプリケーションの例

今回開発した無線LANアクセスポイントは，主に二つの利用形態を想定している。

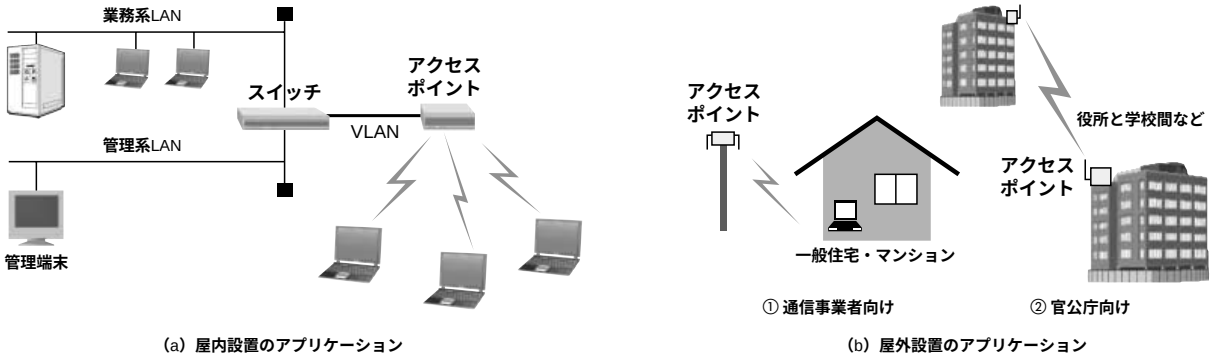
一つは，**図1**の(a)に示すように屋内に設置される形態であり，代表的なアプリケーションは社内LANへの適用である。これまで有線で構成されていた社内LANを無線LANに置き換えることでケーブルの敷設が不要になり，レイアウト変更が容易になるという利点がある。更に，無線LANにより企業内通信にポータビリティが加わり，場所を問わず電子メール，ウェブアクセス，データ通信などの企業アプリケーションを提供することができる。このアプリケーションでは，パソコンに無線LANカードを実装し，オフィスや工場内でパソコンを持ち歩き，どこでも通信を担保する使用方法を想定する。

これらの社内LAN用途では，ネットワーク管理を含めた強固なセキュリティと，現在の有線LANと同等の速度を達成する高性能化が重要なキー技術となる。

もう一つのアプリケーションは図1の(b)に示す屋外に設置される形態である。図中①で示す通信事業者向けのアプリケーションでは，屋外に設置された無線LANアクセスポイントと一般家庭・マンション間を無線で接続し，インターネット接続のサービスを提供する。

②に示す官公庁向けのアプリケーションとしては，官公庁や自治体の主要拠点間を無線LANで接続することによりイントラネットを構成する。更に，監視カメラからの画像情報をネットワークへ接続するための無線アクセスとして使われる用途もある。

これら屋外設置のアプリケーションでは，先に述べたキー技術に加え，屋外環境に耐える高信頼性と種々のシステム要求に対して柔軟に対応することができるフレキシビリティが要求される。



(a) 屋内設置のアプリケーション　　(b) 屋外設置のアプリケーション

図1．無線LANアクセスポイントが使われるアプリケーション―屋内設置と屋外設置の二つの形態が想定され，これらのアプリケーションは，ネットワークの規模が大きく，重要なデータを扱っていることから特に強固なセキュリティが必要である。

Wireless LAN access point applications

3 主要性能と特長

この装置の主要性能を**表1**に示す。

この無線LANアクセスポイントは，2章で述べたアプリケーションで必要なキー技術を以下の方法で実現している。

⑴ 強固なセキュリティ

ⓐ 高度なクライアント認証機能であるIEEE802.1Xをサポート

ⓑ 40/104ビットWEP（Wired Equivalent Privacy）に加え，更に強固な暗号方式であるAES（Advanced Encryption Standard）をサポート

ⓒ 管理者アクセスセグメントをVLAN（Virtual LAN）によりユーザーセグメントと分離

ⓓ 製品の国際セキュリティ評価認定であるISO/IEC15408（国際標準化機構／国際電気標準会議規格15408）セキュリティターゲットを取得予定

⑵ 高性能　2.4 GHz帯と5 GHz帯の同時通信が可能な構成とし，IEEE802.11a/b/gいずれのクライアントも収容可能

ⓐ 最大54 Mbpsの高速アクセスを実現

ⓑ ソフトウェアの変更により将来QoS（Quality of Service）などへの対応が可能

⑶ フレキシビリティ

ⓐ アプリケーションに適した最適なアンテナを選択可能

ⓑ 屋外で使用可能な4.9 GHz/5.0 GHz帯をサポート

ⓒ 屋外環境にも設置可能な屋外タイプも用意

表1．無線LANアクセスポイントの主な仕様

Main specifications of wireless LAN access points

項　目	仕　様
規　格	IEEE802.11a，IEEE802.11b，IEEE802.11gに準拠
使用周波数（MHz）	4,900～5,000，5,030～5,091，5,150～5,250，2,400～2,497
伝送速度（Mbps）	1～54（2.4 GHz帯），6～54（5 GHz帯）
有線LANインタフェース	10BASE-T/100BASE-TX
管理系プロトコル	SNMP，HTTP
セキュリティ	WEP40/104/128ビット，MACアドレスフィルタリング，IEEE802.1X（EAP-MD5/EAP-TLS/EAP-TTLS/PEAP），AES，IEEE802.11i（将来対応予定）
周囲温度条件（℃）	屋内タイプ：＋5～＋40 屋外タイプ：－20～＋50

4 セキュリティの向上

無線LANで使われているWEPによる暗号方式は，同じ暗号鍵を長い期間使用し続けるため，その脆弱（ぜいじゃく）性が指摘されている。このため，この装置の開発にあたっては，IEEE802.1Xによる認証をはじめとする各種のセキュリティ機能を搭載した。以下に，この装置のソフトウェア構成を含めて各機能について述べる。

4.1 ソフトウェア構成

無線LANアクセスポイントのソフトウェア構成を**図2**に示す。

IEEE802.1X機能部は，EAPOL（Extensible Authentication Protocol Over LAN）フレーム／RADIUS（Remote Authentication Dial In User Service）パケット送受信と解釈を行い，MAC（Media Access Control）認証機能部はMAC認証を行う。

なお，今回開発したアクセスポイントの管理系プロトコルにはSNMP（Simple Network Management Protocol），HTTP（HyperText Transfer Protocol）/HTTPS（HTTP over transport layer Security/secure sockets layer），FTP（File Transfer Protocol）/TFTP（Trivial FTP）及びSSH（Secure SHell）をサポートしている。

4.2 セキュリティ機能

セキュリティの向上は，主に認証機能と暗号化によって実

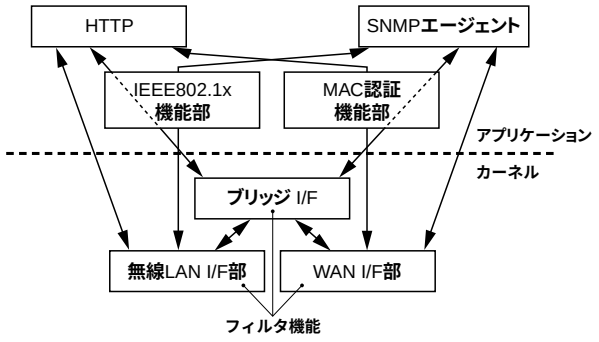


図2．無線LANアクセスポイントのソフトウェア構成 ― 種々の管理系プロトコルに対応することで，ネットワークの規模に応じた最適なプロトコルを選択可能である。

Software architecture of wireless LAN access points

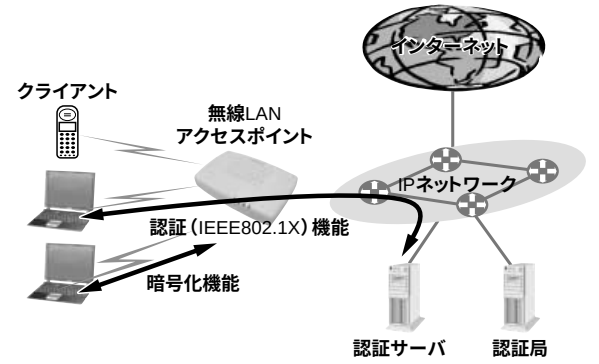


図3．セキュリティ機能の概念 ― 認証（IEEE802.1X）により，クライアントと認証サーバ間の識別と認証を行う。暗号化機能は無線区間の暗号化を行う。

Concept of security function

現する。各機能の概念を**図3**に示す。

次に，今回実装したセキュリティ機能について述べる。

4.2.1　認証方式（IEEE802.1X）　今回開発した無線LANアクセスポイントでは，認証方式としてIEEE802.1Xで標準化されているEAP-MD5（EAP-Message Digest 5），EAP-TLS（EAP-Transport Layer Security），EAP-TTLS（EAP-Tunneled TLS）及びPEAP（Protected EAP）のすべてをサポートしている。

なかでもEAP-TTLSやPEAPは，クライアント認証をパスワードで行い，認証サーバのみ電子証明書で行うため，EAP-TLSのように電子証明書の管理が煩雑でなく，運用に対する負荷が限定的となる。

4.2.2　暗号化方式　WEPによる暗号が脆弱なのは，一定時間WEPで暗号化されたデータをキャプチャすることにより，WEP鍵が露見してしまうことによる。今回開発した無線LANアクセスポイントでは，認証方式（IEEE802.1X）で再認証した際，WEP鍵の更新により同一のWEP鍵が継続して使われることがないように対処している。また，WEPが標準で採用している暗号アルゴリズムRC4（Ron's Code 4）自体に脆弱性があるため暗号鍵を突き止められやすい。次世代の共通鍵暗号化方式であるAESを使うことにより，RC4の脆弱性にも対処できるようにしている。

今後，WPA（Wi-Fi®(注1) Protected Access）で標準化が進められているTKIP（Temporal Key Integrity Protocol）及びIEEE802.11iの動向に合わせて，更に強固な暗号化方式の製品化に取り組んでいく。

4.2.3　その他のセキュリティ機能　その他のセキュリティ機能として，不正なユーザーからの接続を制限するためのMACアドレス，IP（Internet Protocol）アドレス，Ethernet(注2)のタイプフィールド及びTCP（Transmission Control Protocol）/UDP（User Datagram Protocol）ポート番号によるフィルタリング機能を設けている。アクセスを拒否したい場合は，事前に登録しておくことでアクセスを拒否することができる。

また，ESS-ID（Extended Service Set Identifier）をANYに設定したクライアントのアクセス拒否，ビーコンにESS-ID（Extended Service Set IDentification）を乗せない機能などにより，ESS-IDが漏れることを防ぐ機能を持つ。更に，管理情報とユーザー情報をVLANで分離して管理情報がユーザー側に流れるのを防ぐ機能，同一アクセスポイントを経由したクライアント間の通信を禁止する機能も実装した。長時間の無通信状態や，長時間の接続状態を検出してクライアントの接続を強制的に切断する機能などもセキュリティを向上させるために有効である。

4.2.4　ISO/IEC15408認証　今回開発した無線LANアクセスポイントは，これまで述べたようにセキュリティ対策を十分に行った製品と考えている。それを公式に示すため，ISO/IEC15408（情報セキュリティ）認証取得を目指して作業を進めている。

2001年3月29日の行政情報化推進各省庁連絡会議で，“（前略）～今後の情報システムの構築に当たっては，可能な限り，次のような方法等により，ISO/IEC15408に基づいて評価又は認証された製品等の利用を推進するものとする。”と了承されている。2003年度に入り環境が整ってきており，今後の官公庁向けの製品納入に対して，ISO/IEC15408の評価又は認証が必要になってくるものと考えられる。

4.3　将来機能

将来的には4.2.2項で述べたWPAやIEEE802.11iだけでなく，IEEE802.1Xの認証状態により接続できるネットワーク

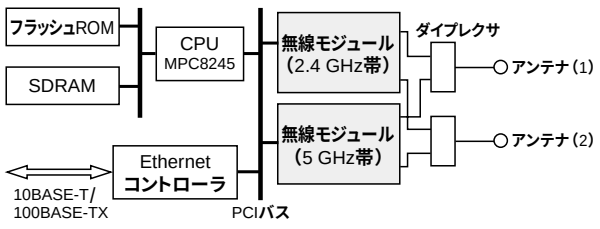
（注1）　Wi-Fiは，米国Wi-Fi Allianceの登録商標。
（注2）　Ethernetは，日本における富士ゼロックス（株）の商標。

を分けることができる認証VLANの機能や，IPv6などにも対応していくことも視野に入れている。

5 高性能とフレキシビリティの実現

5.1 ハードウエア構成

この装置の系統を**図4**に示す。



SDRAM：Synchronous DRAM　PCI：Peripheral Component Interconnect

図4．無線LANアクセスポイントの構成 ― 無線モジュールを二つ実装し，IEEE802.11a/b/gのクライアントを同時に収容できる構成とした。

Configuration of wireless LAN access points

IEEE802.11bに加え，最大54 Mbpsの通信規格であるIEEE802.11aと11gに準拠したクライアントと同時に通信可能とするため，二つの無線部を内蔵している。図4中，無線モジュール(2.4 GHz帯)がIEEE802.11bと11gのクライアントを収容し，無線モジュール(5 GHz帯)がIEEE802.11aのクライアントを収容する。

無線部は，最適なアンテナを選択するダイバーシチ方式を採用しているため，それぞれの無線部で各々二つのアンテナが必要となる。今回は，2.4 GHz帯と5 GHz帯で共用できるデュアルバンドアンテナとダイプレクサを組み合わせることにより，二つのアンテナを両方の無線部で共用する構成とした。アンテナの本数を削減したことで，装置外観の改善と容易な設置を実現している。

制御部は，データの処理能力を高めるため，CPUにMPC8245を採用しており，高スループットを実現している。有線側のインタフェースは10BASE-T又は100BASE-TXとしており，将来はEthernetケーブルからの給電を可能とするIEEE802.3afにも対応していきたい。

5.2 装置外観

オフィスなどの屋内に設置する無線LANアクセスポイントの外観を**図5**に示す。アンテナは外部アンテナを基本としており，装置背面にコネクタで接続される。アンテナは，その設置場所やクライアントのカバーエリアに応じて最適な利得と指向性を選択する必要がある。外部アンテナとすることで，種々のアンテナを接続することが可能となり，柔軟な対応ができるようにしている。そのほか，装置の背面には有線インタフェース

図5．無線LANアクセスポイント装置(屋内設置タイプ) ― アンテナは外部アンテナを装置背面に接続する構成とし，種々のアンテナが選択できるようにしている。

Wireless LAN access point for indoor use

コネクタ，保守のためのシリアルポートを用意している。

装置の内部ユニットは，屋外の温度環境に耐えうる設計としており，ケースを変えることで屋外設置も可能としている。屋外設置の場合，ケースはアルミダイキャスト製とし，直射日光，雨，腐食性ガスなどの過酷な屋外環境に十分耐えうる高信頼性を実現している。

6 あとがき

ここで述べた無線LANアクセスポイントは，各種のセキュリティ機能を実現することで，より強固なセキュリティを実現した。このため，セキュリティ対策が必須なアプリケーションに十分適用することが可能である。

この装置が適用を想定しているアプリケーションは，いずれもネットワークの規模が大きいため，無線LANアクセスポイントもシステム全体との協調が必要である。今後ともユーザーのニーズに合わせて機能や性能の充実を図るとともに，当社がこれまで培ってきたシステムインテグレーションと協調することで，今までにない新しい価値を創造していきたい。

鈴木　康一　SUZUKI Koichi

社会ネットワークインフラ社　通信システム事業部　通信映像プラットフォーム設計部参事。無線通信機器の開発設計に従事。

Telecommunications Systems Div.

渡邉　博之　WATANABE Hiroyuki

社会ネットワークインフラ社 通信システム事業部 通信システム技術部参事。通信機器の開発設計に従事。

Telecommunications Systems Div.

落合　民哉　OCHIAI Tamiya

社会ネットワークインフラ社 通信システム事業部 通信システム技術部グループ長。通信システムエンジニアリング業務に従事。電気学会，電子情報通信学会会員。

Telecommunications Systems Div.