安全で快適な無線LANシステムの構築

Integration of Secure and User-Friendly Wireless LAN Systems

小野田　実　　**河井　宣之**
■ONODA Minoru　■KAWAI Nobuyuki

無線LANは，低価格・高速化が進み，システム導入される機会が増加している。しかし，傍受や不正アクセスなどのセキュリティの問題，他の電波使用機器や無線LANとの電波干渉など，課題を抱えている状況でもある。東芝では，これらの課題を解決し，安全で快適な無線LANシステムを提供するソリューションと各種サービスを用意している。

In recent years there have been increasing opportunities to integrate network systems with wireless LAN. On the other hand, there are some issues involved including interception, unauthenticated access to the system, rogue access points, and interference with other wireless LANs or wireless systems.

Toshiba is providing wireless solutions incorporating various services to meet customers' needs.

1 まえがき

無線LANは，低価格化，高速化が進み，企業や家庭で導入が進んでいる。1999年にIEEE802.11b（米国電気電子技術者協会規格802.11b）が標準化され，11 Mbpsという速度を実現，世界的に各社から標準準拠の製品が登場した。日本においても，法改正により使用可能チャネルが増加し，世界と共通の周波数帯となったことで，世界標準化による低価格化の恩恵を受けられることとなり，近年の普及に至っている。

無線LANにより，クライアントの移動性が向上し，パソコン（PC）を持ち歩く，場所を気にせずにシステムにアクセスするなどの，無線LANの特長を生かした利用をすることができる。低価格化ともあいまって，企業の事務所，工場などの製造現場での使用のほか，デパート催事場などでの臨時的な使用，喫茶店や空港・駅などの無線LANスポット，そして家庭に至るまで多様な場所で使用されるようになった。

しかし，一方で，セキュリティの問題も指摘され，企業の情報システム担当部門では，導入に二の足を踏む場合があることも事実である。

また，電波を使用することから，無線LANを快適に使用するためには，電波伝播（でんぱ）状況の把握，競合や干渉の問題への対処なども必要である。更に，構築した無線LANシステムのパフォーマンスやセキュリティを維持するための対応策も，十分に検討・用意しておく必要がある。

ここでは，無線LANシステム構築，及び維持に関しての課題の提示と，それらに対するソリューションについて述べる。

2 無線LANシステム導入の課題

2.1 セキュリティ上の課題

無線LANを使用することにより，移動性向上などのメリットを得られるが，特有のセキュリティ上の課題も存在している。無線LANを使用する場合には，以下の課題に対処する必要がある。

⑴ 傍受　　無線LANは電波を使用するため，有線LANと異なり，離れた地点での電波傍受が可能である。無線LAN上のパケットに暗号化を施し対処するのが一般的であるが，無線LAN標準の暗号化方式であるWEP（Wired Equivalent Privacy）には脆弱（ぜいじゃく）性が指摘されており，インターネット上で解読用のフリーソフトウェアが公開されている状況である。

⑵ 不正アクセス　　傍受した結果などにより，セキュリティが破られてしまえば，離れた地点から，すなわち管理者の目の届かない地点からの，なりすましによる不正アクセスも可能となる。

⑶ 不正アクセスポイントの設置　　基幹LANにセキュリティ未対策のアクセスポイントを接続された場合には，外部に対して大きなセキュリティホールを提供することとなる。アクセスポイントの低価格化に伴い，特に悪意を持たない内部者が，効率アップの目的で個人的に基幹LANにノーガードのアクセスポイントを接続し，基幹LANトラフィックを筒抜けにしてしまった事例がメディアなどでも報告されている。

⑷ 移動アクセスによる問題　　統一されたセキュリティポリシーのもとで，システム構築・導入していない場合，

つまり，同じ企業の中でも部課単位などの個別組織で運用している場合など，各運用単位でセキュリティレベルに統一性がない可能性がある。重要な情報にアクセスする人が，セキュリティレベルの低い場所で無線LANを使用すると，情報漏えいの可能性が生じる。

2.2 電波の問題

無線LANは電波を使うため，干渉などによりスループットが低下したりする問題が生じることがある。電波に関連した問題は，下記のように分類することができる。

⑴ 既存の無線LANとの競合・干渉　　無線LANは，基本的に免許なしで自由に使用できるため，近くの場所で異なるユーザーが同時にシステムを構築し，お互いに競合・干渉してしまう可能性がある。

⑵ 他の無線装置との相互干渉　　無線LANのうち，2.4 GHz帯を使用するものについては，他の無線装置からの電波と干渉する可能性がある。これは，2.4 GHz帯がISM（Industrial, Scientific and Medical）バンドとして種々の装置で共用されていることによる。電子レンジ，医療機器，アマチュア無線，移動体識別システムなどが該当し，無線LAN側が影響を受ける場合のほか，逆に相手システムに影響を与える場合もある。

3 無線LANソリューション

前記の課題に対処するため，システムの企画，設計，構築展開，運用の各段階で，ソリューションを用意している（**図1**）。

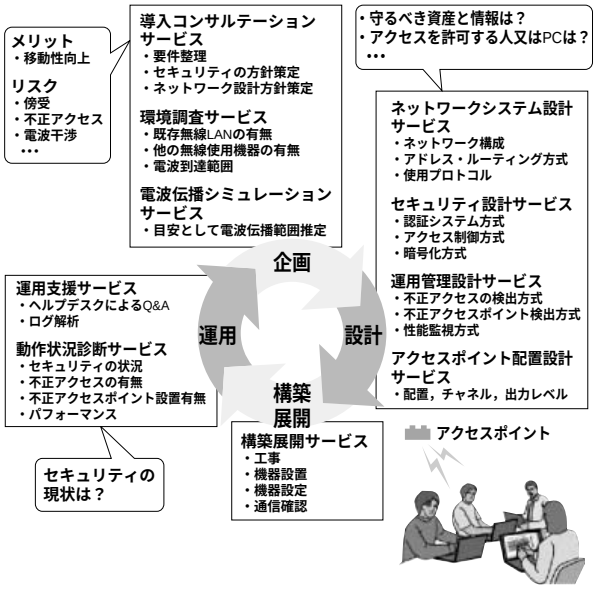

図1．無線LANソリューションの概要 ― システム構築の各段階で，課題に対処するソリューションを提供する。
Outline of wireless LAN solution

3.1 企画段階

⑴ 導入コンサルテーションサービス　　前記のような課題に対処し，無線LANの特長を生かしたシステムを構築するためには，企画段階での検討が重要である。“導入コンサルテーションサービス”により，システムへの要求条件を踏まえ，最適なシステムとなるよう，コンサルティングを行う。

セキュリティ面の課題については，システム全体として検討して方針を策定する必要がある。

ⓐ 守るべき資産と情報は何か
ⓑ アクセスを許可する人，又はPC
ⓒ クライアントの移動の範囲
ⓓ 上位層，アプリケーションとの関係

これらを整理し，システム内の無線LANの位置づけを明確にし，前述の課題に対処するためのセキュリティの方針，ネットワーク設計方針を定める。

更に，導入後のセキュリティ維持のために，下記についての運用管理の仕組みを検討する。

ⓐ 不正アクセスの検出
ⓑ 不正アクセスポイントの検出
ⓒ 策定した方針を逸脱しないようにすること

また，電波関連の課題への対処として，この段階で電波環境の調査を行い，無線LANの使用に問題がないかどうかの確認が必要である。そして，電波環境が導入後に変化することを考慮し，導入後の性能監視も，併せて検討する。

以下，システムでの検討の例を示すが，考え方はひととおりではない。

ⓐ 公衆用無線LANスポットでの検討例　　喫茶店などでインターネットへのアクセスを提供する無線LANスポットの例では，守るべき情報は接続者のPC内の情報となる。接続者どうしで通信ができないような仕組みが必要となる。また，インターネット経由で会社の基幹LANと接続するような場合は，利用者にセキュリティの確保を委ねる。また，導入前には，近隣の既存無線LANや電波使用機器との相互干渉についての調査を行う，などの検討が必要である。

ⓑ 企業の基幹LANに接続する際の検討例　　企業の基幹システムに組み込む場合には，守るべき情報は社内の業務サーバはじめ社員のPCの内部情報などすべてとなるが，情報の重要度に応じてセキュリティレベルを分ける必要がある。無線LANを介してアクセスできるのは社員のみとするため，アクセス時に認証を行う必要があり，社内に構築したPKI（Public Key Infrastructure）に沿って電子証明書による認証を行う。構築後のセキュリティの維持のために，不正

アクセスや不正アクセスポイントの検出機構を運用管理システムに取り入れる，などの検討が必要である。

⑵ 環境調査サービス　　無線LANシステムを導入する場合には，現状稼働している他の無線LANを認識し，設置場所やチャネル割当に反映させ競合しないようにする必要がある。また，他の無線システムが稼働しているかどうかの調査も必要である。

無線LANアナライザ及びスペクトラムアナライザを使用して，設置予定地（サイト）の電波状況を測定して調査結果を報告する“環境調査サービス”を用意し，事前の環境調査に適用している。

⑶ 電波伝播シミュレーションサービス　　建物が未完成の場合や実測が困難な場合などは，計算機による電波伝播のシミュレーションが，カバー範囲の推定やアクセスポイントの台数の見積もりの目安として有効な場合がある。建物とフロアのレイアウトや建材の情報から電波伝播のシミュレーション（**図2**）を行い，結果を報告する“電波伝播シミュレーションサービス”を提供している。

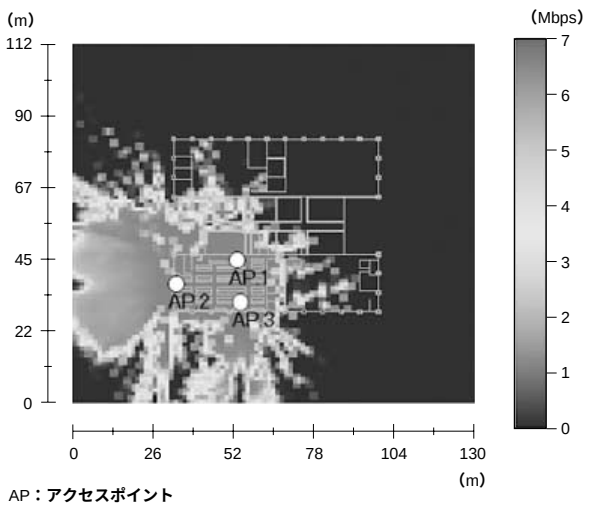

図2．電波伝播シミュレーションの出力例―サイトの伝播シミュレーション結果をグラフィカルに出力する。
Example of simulation output

3.2　設計段階

⑴ ネットワークシステム設計サービス　　企画段階での検討の結果，導出された設計方針に合ったネットワークシステムを設計する“ネットワーク設計サービス”を提供している。企業の基幹LANに接続する場合などには，セキュリティ強度を高める必要があり，以下のようなソリューション サービスと併せて適用している。

⑵ セキュリティ設計サービス　　前述のように，セキュリティはシステム全体として対応し，システム全体の方針に沿って無線LAN部分の対応も決める必要があり，“セキュリティ設計サービス”として，対応している。

ここでは，無線LAN部分としての対策例を述べる。まず，なりすましや不正アクセスを防ぎ，許可された人あるいはPCだけがアクセスできるようにするため，認証機構を設ける必要がある。認証サーバを設け，中継役となるアクセスポイントやVPN（Virtual Private Network）ゲートウェイ装置との間で認証のためのやりとりを行い，その結果により，アクセスの可否の制御をアクセスポイントやVPNゲートウェイで行う。

認証の観点では，“認証システムソリューション”を用意し，認証システムやPKIの構築，及びコンサルテーションを提供している[(1)]。

実際のアクセス制御は，アクセスポイントで行う場合にはIEEE802.1X（Port-Based Network Access Control：ポート単位でアクセス制御を行うことを目的とした規格）の仕組みを使用して行う。認証サーバによって認証されたユーザーの通信だけがアクセスポイントを介して通信できるようアクセス制御を行う。暗号化の面では，IEEE802.1Xには，暗号鍵の更新の仕組みが備わっているため，WEPで使用する鍵を短期間で変化させることにより，現実的に解読が不可能な状況を作ることが可能であり，傍受のリスクに対応することができる（**図3**）。また，TKIP（Temporal Key Integrity Protocol）やAES（Advanced Encryption Standard）などの新しい

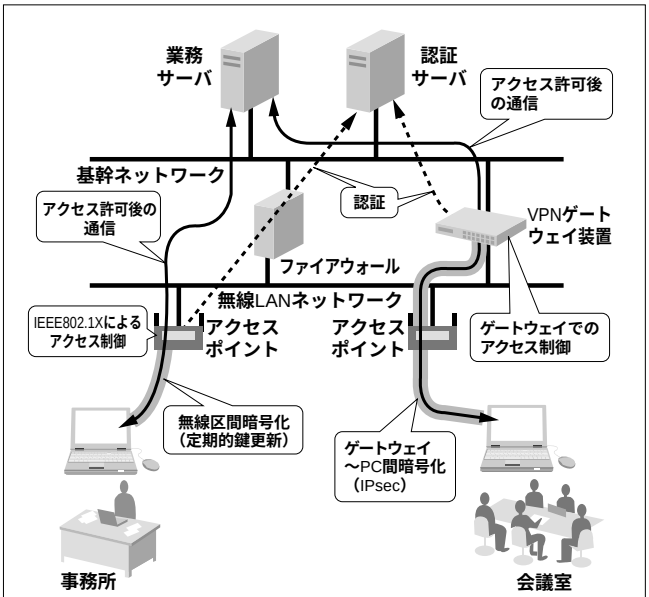

図3．認証システム例―認証サーバを設け，事務所からはアクセスポイントで中継してクライアントの認証を行う。会議室からは，VPNゲートウェイで中継して認証を行う。
Example of authentication and access control

無線LAN暗号化方式の採用も，標準化の進展により視野に入ってきている。

また，VPNゲートウェイを利用する場合は，VPNゲートウェイ装置の機能により，ユーザー単位やプロトコル単位で細かなアクセス制御が可能である。暗号化の観点では，VPNゲートウェイとPCの間でIPsec（Internet Protocol security protocol）などのVPNプロトコルを使用してIP層でのセキュアな通信路を確保し，傍受のリスクに対応する（図3）。

⑶ 運用管理設計サービス　　運用管理についても，セキュリティと性能の維持の観点で，システム全体で検討・設計する必要があり，“運用管理設計サービス”として対応している。

無線LANにおいては，不正アクセスや不正アクセスポイントの設置について，管理者は常に注意する必要がある。運用管理システムの一環として，これら不正の検出を行う不正アクセス検出機構を用意し，運用管理システムと連携させ対応する。資産管理情報と管理された有線LANからの情報によって正規のアクセス以外のアクセスを検出する方法，及び無線LANのパケットを採取して，あらかじめ設定したポリシーとの乖離（かいり）により，不正アクセスや不正アクセスポイントの検出を行う方法（無線LAN侵入検知装置）とを用意している。

⑷ アクセスポイント配置設計サービス　　無線LANの電波伝播は，建物の構造や什器（じゅうき）のレイアウトなどにより変化する。アクセスポイントの設置にあたっては，電波伝播の状況を把握したうえで，カバーしたい範囲に電波が確実に届くよう，配置設計をする必要がある。前記電波環境調査と併せ，事前に調査をし，アクセスポイントの配置設計を行う“アクセスポイント配置設計サービス”を提供している。

3.3 構築展開段階

実際の構築展開を行う“構築展開サービス”を提供している。工事，機器設置，機器設定，通信確認などを行う。

3.4 運用段階

⑴ 運用支援サービス　　システムの稼働開始後の運用段階では，用意した運用管理システムにより，性能監視や不正アクセスの監視を行う。セキュリティやパフォーマンスの維持のために，ヘルプデスクを設け，Q＆Aやログ解析などの“運用支援サービス”を用意し，サポートを行う。

⑵ 動作状況診断サービス　　現状の状況を把握したいという調査の要求に対応するため，無線LANの動作状況を診断する“動作状況診断サービス”を用意している。無線LAN侵入検知装置をサイトに設置し，セキュリティの状況を診断して報告し，適切な対処につなげていくことを目的としている。セキュリティ的に不十分なまま使用されているおそれがある場合や定期的に診断を行いたい場合に適用することができる。

4 あとがき

無線LANシステム構築における課題の提示と，対応するソリューションについて述べた。

今後，無線LANは，標準化や各ベンダーからリリースされる新しい発想の製品により，いっそう高度なセキュリティが実現されるであろう。また，セキュリティの観点だけでなく，シームレスローミングやQoS（Quality of Service）を実現した“無線LANスイッチ”などにより，無線LANは更に快適に，かつ広範囲な用途に利用される可能性を秘めている。

今後は，無線LANに関する更に新しい技術を取り入れたネットワークインテグレーションに関するソリューションを提供していく。

文　献

⑴ 新藤清史，ほか．セキュリティプラットフォームサービス．東芝レビュー．**58**，1，2003，p.22－26.

小野田　実　ONODA Minoru
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プラットフォームソリューション第三担当主任。ネットワークインテグレーション業務に従事。
Toshiba Solutions Corp.

河井　宣之　KAWAI Nobuyuki
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プラットフォームソリューション第三担当参事。ネットワークインテグレーション業務に従事。
Toshiba Solutions Corp.