

セキュア無線ネットワークソリューション

中川 達実 鈴木 一義

最近の無線ネットワークは、国際標準が整備され、高速化技術、セキュリティ技術が革新されたことにより、急速に発展してきている。特に、企業内ネットワークでは無線LANの利用が増えている。通信速度も無線と有線での伝送方式の差異により有線LANと同等とはいかないが、通常の使用では問題ないレベルになってきている。弱いと言われていたセキュリティ面での脆弱性もクリアし、セキュリティ技術を備えていない場合の有線LANよりも簡単に安全性が高いシステムを構築することが可能となってきている。

本稿では、近年の無線LANの動向とOKIのセキュア無線ネットワークソリューションを紹介する。

無線ネットワークの技術動向

近年、無線LANは、IEEE802.11委員会による国際標準化により急速に発展し、当初の無線LANにあった遅い、危ないというイメージは払拭されてきた。高速化に関しては、最大伝送速度54Mbit/sの規格であるIEEE802.11aおよびIEEE802.11gが主流となっており、さらに、現在策定中のIEEE802.11nという規格では、伝送速度100Mbit/sを超えるものとなっている。

一方、セキュリティ技術に関しては、IEEE802.11i規格が策定されている。これは、無線LANにおける認証と通信の暗号化に関する機能を規定した規格であり、IEEE 802.1x認証、AES方式による通信の暗号化を実現している。

また、従来のアクセスポイント(AP)のみで無線を制御する単独型から拠点にコントローラを持ち複数のAPを制御する中央制御型の登場により、管理面でも大規模ネットワーク適用への可能性が高くなってきている。

無線ネットワークの市場動向

市場動向として企業には以下のような無線LAN導入の潜在的なニーズがある。

*1) ARUBAはAruba Networks,Inc.の登録商標です。

- 複雑なネットワークケーブルを排除したい。
- 会議室等へ移動しても自由にPCを使用できるようにしたい。
- レイアウト変更工事等のネットワーク管理コストを軽減したい。

これまでは、セキュリティ、通信速度など技術的課題が理由で、金融機関をはじめとする高いセキュリティを必要とする企業での導入気運は高まらなかった。しかし、前述のように技術的課題が解決した今、金融機関にて無線ネットワーク導入に向けた気運が高まっている。さらに、最近では、無線LANにも対応した携帯電話（携帯／無線LANデュアル端末）の登場により、音声も含めたネットワークのコードレス化も期待されている。

OKIセキュア無線ネットワークソリューションの特長

OKIでは、以上のような状況に対応するため、米Aruba Networks社と提携し同社のネットワーク製品を中心にセキュア無線ネットワークソリューションを提供している。

図1が無線LANのシステム構成図である。本システムは、以下の特長を持つ中央制御型の無線LANであり、セキュアで利便性の高い無線LAN環境を実現している。

- 世界最高水準のセキュリティ機能
- 充実した導入支援、運用管理機能
- 第3世代携帯電話における無線LANでの音声対応機能

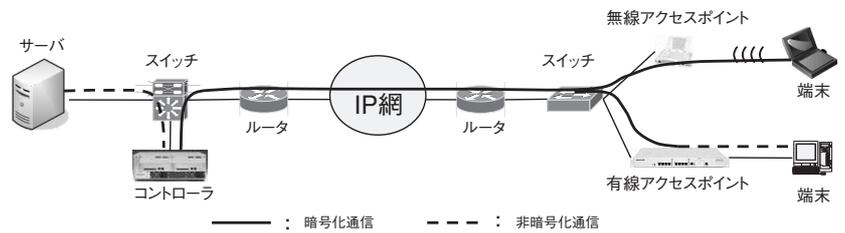


図1 ARUBA^{*1)} 無線LANシステム構成例

世界最高水準のセキュリティ機能

- (1) 端末間の通信をEND-to-ENDで暗号化
無線LAN区間で暗号化されたデータを端末-コント

ローラ間の有線区間でも解凍することなく端末から端末までの全区間（これをEND-to-ENDと言う）で暗号化されたセキュアな通信を行うことができる。

また、本アクセスポイントでは無線区間の暗号を解凍しないため、アクセスポイントにおいて暗号キーや認証情報を持つ必要がないため、アクセスポイントを盗難されても設定内容を読み取られる心配がない。

(2) ステートフルファイアウォール

コントローラはネットワークからアプリケーションの通信までのアクセス制御ができるステートフルファイアウォール機能を内蔵し無線LAN端末に対して、アクセス制御を実施することができる。また無線LAN端末ごとに異なるセキュリティポリシーを割り当てることが可能である。このポリシーはプロトコル制御、特定サーバへのアクセス制御はもとより、プライオリティ、帯域幅、時間帯等を指定することが可能であり、複雑な企業のアクセス制限の要求に応えられるものである。

(3) 有線端末の管理

有線アクセスポイントを用いて、有線端末を接続すると無線LAN端末と同じようにコントローラにて運用管理することが可能となり有線端末、無線LAN端末の両方を一元管理できる。この際、有線アクセスポイントとコントローラの間も暗号化することができるため、有線端末でも特別なソフトウェアなしにネットワークの暗号化が実現可能となる。

(4) 不正アクセスポイントの検出と無効化

コントローラはエアーモニター機能により、周囲の電波を定期的にスキャンし、不正アクセスポイントを検出することができる。管理下の端末が不正アクセスポイントに接続しようとする時、接続を強制的に切断することも可能である。

充実した導入支援、運用管理機能

(1) 無線LAN運用管理機能

端末のモニタリング機能、不正アクセスポイントや干渉アクセスポイントなどのレポート機能が標準機能としてコントローラに搭載されているため、別途管理システムを構築する必要がない。

(2) 端末の位置表示機能

複数のアクセスポイントにより、クライアントの位置情報を算出し、マップ上に表示することができる。これ

により、不正な端末の位置の特定に使うこともできる。

(3) 導入設置の簡易性

コントローラとアクセスポイント間はGREトンネルまたはIPsecという方式で接続される。これにより、既存のルータネットワークを透過的に伝送できるため、無線LAN導入時の変更を最小限に抑えられる。

(4) 無線チャンネルと出力レベルの自動調整

無線チャンネルと無線出力の調整を、周囲の無線LAN環境に応じて自動的に調整することができる。これにより、アクセスポイントが故障しても隣接するアクセスポイントの無線出力を自動的に増大することにより、通信のリカバリーが可能となる。

第3世代携帯電話における無線LANでの音声対応機能

最近の第3世代携帯電話は無線LAN機能を有しているものもあり、無線LAN上で音声通話を行うことができる。本システムでは、音声品質を向上させるために、端末の優先制御、省電力モード、高速ハンドオーバーに対応している。特に、無線LANで移動端末による音声通話を行う場合、そのリアルタイム性、移動が伴う通信の継続性に、特に注意が必要となるが容易に導入することが可能となる。

以上のような特長を持つ中央制御型の無線LANをOKIは提供している。次に本無線LANを応用したソリューションについて紹介する。

無線LANソリューション

無線LAN技術を用いたソリューションは従来のケーブルレスからセキュリティおよびモビリティを求めるソリューションへと変化してきている。

また、技術の進歩による有線LAN同等の通信速度の実現やセキュリティの確保、コンシューマ向け無線LANの普及にともない企業で使用するアクセスポイントの低価格化も進んでいる。これらにより単にLAN構築の1つの手段として無線LANを選択する企業も増えている。

たとえば、金融機関において設置場所が決まっているATMのような特定業務専用の装置は有線LAN、行員が使用するパソコンやロビー内のマルチメディア表示板などは、無線LANと使い分けることにより柔軟に行内LANを構築することが可能である。

さらにARUBA無線LANには、特徴の一つである無線アクセスポイントと同じ機能を持った有線用アクセスポイントが用意されているため、端末の管理を有線、無線を問わず一元的に行うことが可能となり、端末管理の面

からも有効な構築が可能である。

特に新規に行内や店舗内のLANを敷設するような場合には、有線LANと無線LANをうまく組み合わせることにより、構築コストや機器移動時の移設コストの削減ばかりでなく、日々の業務における利便性の向上は計り知れないものがある。

以上のような、通常のLAN構築での導入以外に、無線を有効に活用したソリューションを紹介する。

(1) 営業店ロビーにおける顧客とのコミュニケーション強化

本ソリューションは営業店にて待ち時間に携帯無線端末を使用していただくことにより顧客とのコミュニケーションを強化するソリューションである。図2がその簡単な構成図および運用例である。

運用方法は顧客が来店時ロビーにて受付カードを受け取る代わりに携帯無線端末を受け取る。携帯無線端末は営業店システムと連携しており、受付時に口座番号や来店目的を確認し、取引順番が来るまで各種コミュニケーションをとるツールとなる。たとえば、入力した口座番号よりCRMシステムと連携しキャンペーン情報など、顧客に合った情報を携帯無線端末に表示したり、興味のある近隣店舗の情報を表示したりする。従来マルチメディア表示板などの大型ディスプレイで表示していた内容を、個人個人の携帯端末に表示することが可能であり、さらに、双方向通信機能を利用することにより、各種情報提供以外にアンケートなどの収集も可能である。

また、事前取引内容を入力しておけば、窓口の取引順番が来たときには携帯端末の画面に窓口への誘導を促すメッセージをポップアップ表示するとともに、事前に入力しておいた情報を無線LANにて転送し、窓口処理の

短縮を図ることも可能である。

携帯端末は専用の機器でなくとも、WiFi仕様に準拠した携帯ゲーム機やPDAなど市販の機器にて安価に構築可能である。

(2) イベント会場などの臨時店舗ソリューション

ここでは、屋外でのモビリティの要件を実現したソリューション例を示す。行内のネットワーク環境を容易に屋外で実現するソリューションである。

ソリューションイメージ図を図3に示す。

行内のコントローラと屋外のアクセスポイント間で、IPsecによる暗号化を行うことにより、VPN用の専用装置を用いることなくVPN化することが可能である。

さらにコントローラにはファイアウォール機能があるため不正侵入を防止することができる。アクセスポイントとコントローラ間のネットワークは、安価なインターネットや将来に向けては、一般的にホットスポットと呼ばれている公衆無線LANでも実現可能である。図3のようなシステムにて容易にVPNを構築できるため、住宅展示場でのローン相談のための臨時出張所や入学式、マンション内覧会などのイベント時の振込口座開設などの相談窓口として利用できる。さらにパソコンなどのデータ用端末以外に、無線IP電話なども無線LANに収容できるため内線電話としての利用も可能となり、既設店舗に近い環境を構築できる。

同様な構築例として在宅ワーク環境の実現がある。先ほどの例は屋外での臨時出張所での使用であるが、アクセスポイントを行員の自宅に設置し、自宅のインターネットまたは公衆無線LAN環境に接続することにより、行内と同じセキュリティ環境を簡単に構築でき、在宅勤務を可能とする。無線IP電話を使用することにより内線

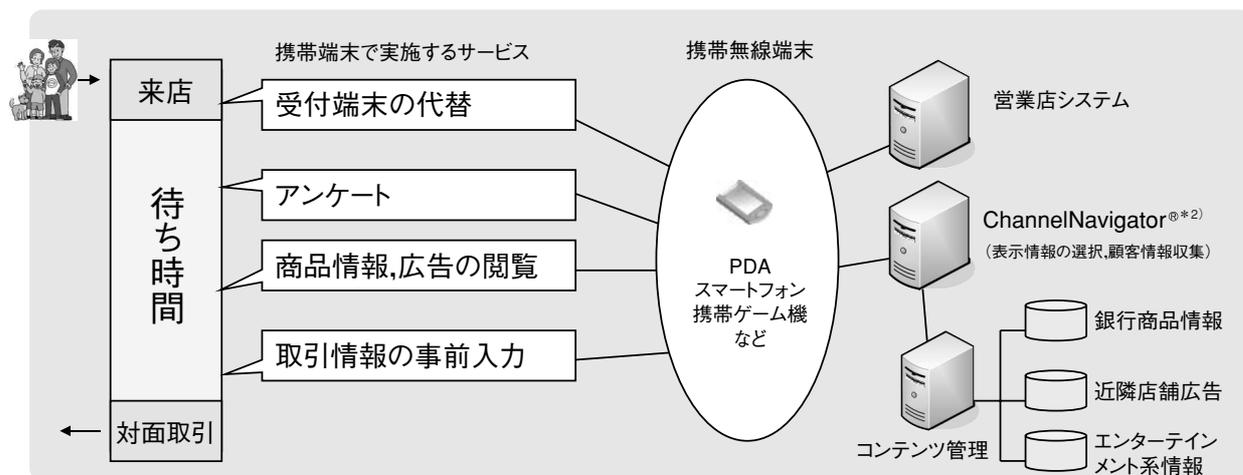


図2 顧客とのコミュニケーション強化の運用例

*2) ChannelNavigatorは沖電気工業株式会社の登録商標です。

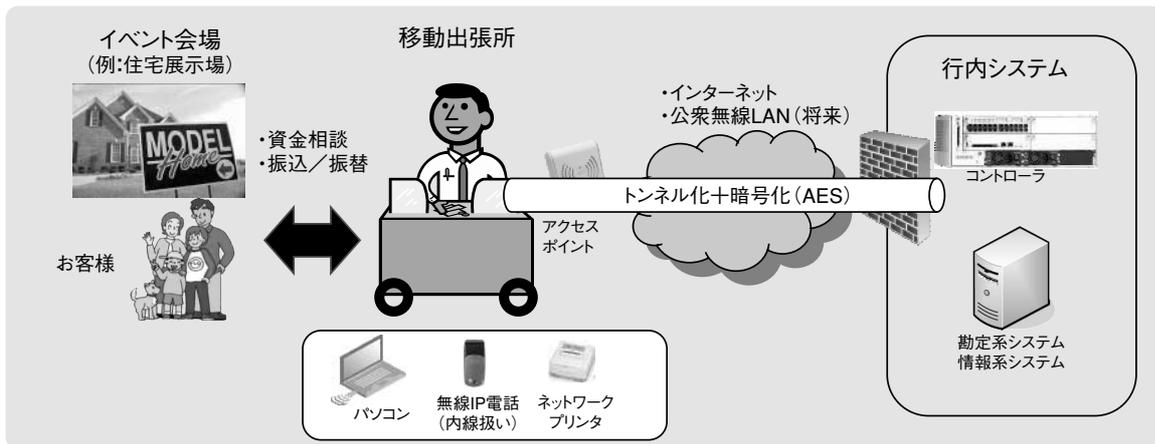


図3 臨時店舗ソリューションイメージ図

電話も行内の自席と同じ番号にて通話可能なため、従来の単なるリモートアクセス環境から仮想行内環境を実現できる。以上のような構築でもVPN専用装置などは必要なく、アクセスポイントとWiFiに準拠した無線端末があれば容易に構築可能である。

おわりに

従来、無線LANは有線LANに比べて、通信速度やセキュリティの面で弱く、金融機関など高いセキュリティを要求される用途には不向きとされてきた。しかし、無線LANの技術が進化し、高速化やセキュリティ強化などの技術が標準化され、端末までの制御を適切に集中管理することにより、従来のデメリットは払拭されつつある。

今後LANは、ノイズが多いなどの特別な環境以外は無線LANが主流になっていくと考えられる。すでにホーム

ユースなどでは無線LANが当たり前となっている。次世代の無線LANに求める要件は、更なる高機能と同時に、有線LAN以上の構築のしやすさがポイントとなるであろう。

OKIは今後もARUBAとの提携を生かし無線LANの高機能、高性能を進めると同時に無線LANのメリットを生かしたソリューションを開発していく所存である。◆◆

● 筆者紹介

中川達実：Tatsumi Nakagawa. OKIネットワークインテグレーション株式会社 ソリューションビジネス本部 金融ソリューション部

鈴木一義：Kazuyoshi Suzuki. 金融ソリューションカンパニー 金融システム本部 金融ユビキタスサービス開発部

TIPS

【基本用語解説】

IEEE802.11委員会

IEEE（米国電気電子技術者協会）のLANの標準化を行う委員会の一つであり、無線LANの標準化を行っている。

AES方式

米国標準技術局によって規格化が行われている次世代の標準暗号方式の名称。

GREトンネル

ある電文を、別なプロトコルでカプセル化して通信を行うトンネル方式の1つで、パケットをIP内でカプセル化して通信を行う方式である。

IPsec (Security Architecture for Internet Protocol)

IPsecは、IPパケット単位でデータを暗号化しセキュリ

ティの確保を行うプロトコルである。インターネットを利用したVPN通信に多く利用されている。

CRMシステム

Customer Relationship Managementシステムの略で顧客情報の管理・分析等を行うシステム。

WiFi

Wi-Fi Alliance（米国の業界団体）によって無線LAN機器の相互接続性を認定されたことを示す名称。

VPN

仮想プライベートネットワークの略で一般的な公衆網を、暗号化技術などを使用してあたかも通信相手が固定された専用線のように使用方法または技術。