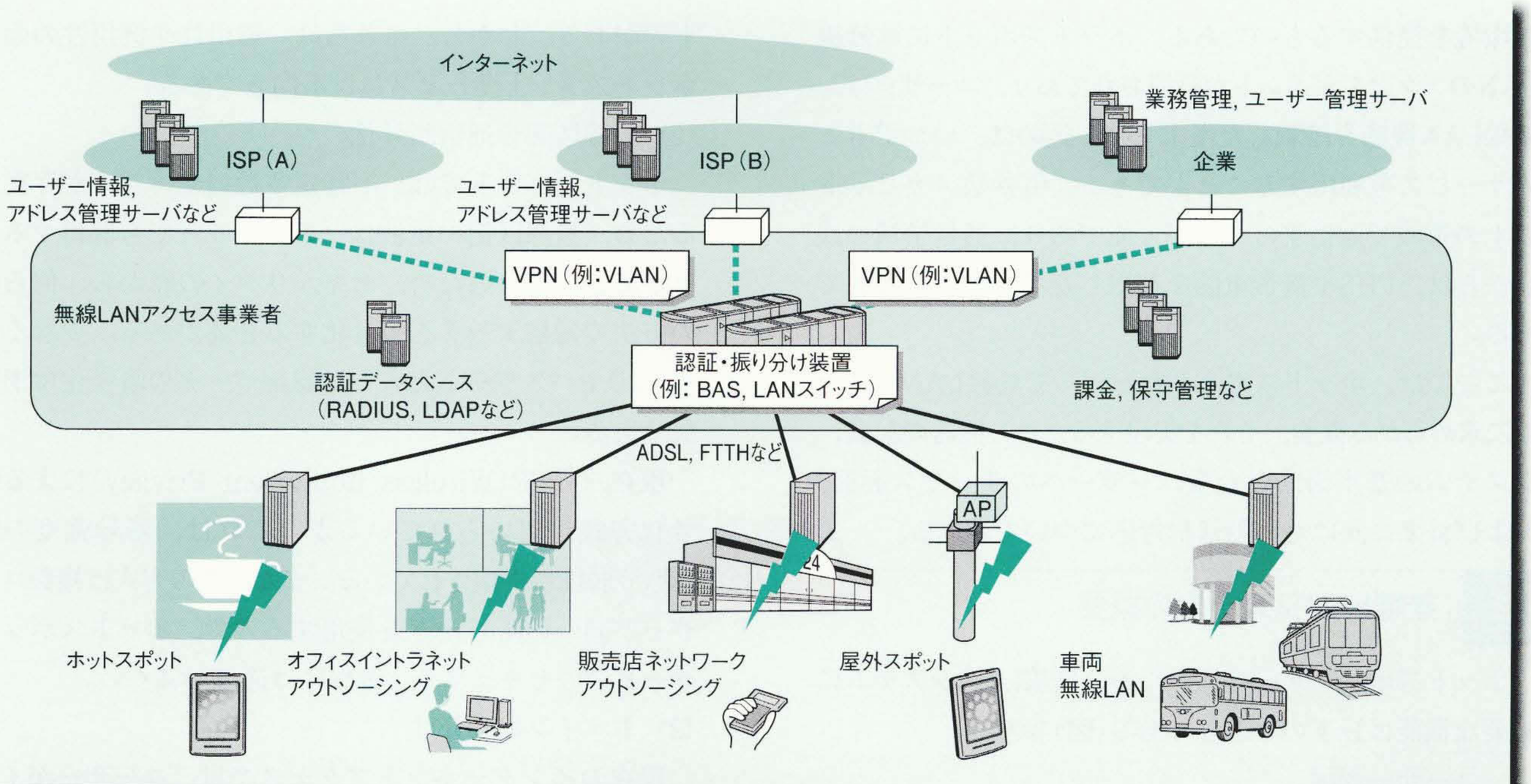
ホットスポットサービスのための無線LANシステムソリューション

Wireless LAN Solutions for Hotspot Services

新保　勲　*Isao Shimbo*　白井啓介　*Keisuke Shirai*
柴田治朗　*Haruo Shibata*　田中宏司　*Kôji Tanaka*



注：略語説明
ISP（Internet Service Provider），VPN（Virtual Private Network），VLAN（Virtual LAN），RADIUS（Remote Authentication Dial-in User Service）
LDAP（Lightweight Directory Access Protocol），BAS（Broadband Access Server），ADSL（Asymmetric Digital Subscriber Line）
FTTH（Fiber to the Home），AP（Access Point）

無線LANシステムソリューションの構成例
アクセスポイントと認証・振り分け装置（BAS，LANスイッチ）で「ユーザー認証」，「無線区間の通信暗号化」，および「ドメイン振り分け」を実現する無線LANシステムの構成例を示す。

近年，ADSLやCATVなどのブロードバンド回線が急速に家庭へ普及し，低価格で広帯域なワイヤレスデバイスとして，無線LAN機器が浸透してきている。これに伴い，空港やホテルなどに無線LANアクセスポイントを設置し，ここから，いつでもインターネットにアクセスできる「ホットスポットサービス」が注目を集めている。

無線LANは上位プロトコルに依存しないため，IPv6との親和性も高く，いつでも，どこでもというユビキタスな環境の実現基盤として適している。

しかし，公衆の場やオフィスなどで利用する場合は，ユーザーの認証や，データ通信の暗号化など，セキュリティ対策が必要である。

日立製作所は，IPv6システムの研究・開発に加え，通信事業者がホットスポットサービスを提供できるように，セキュリティを高めた広帯域無線LANソリューションを提案している。さらに，このホットスポットサービスを拡張し，VPNへの展開や移動通信への対応を図ることも検討している。

1　はじめに

近年，ADSL（Asymmetric Digital Subscriber Line）やCATV，FTTH（Fiber to the Home）などのブロードバンド回線が急速に普及している。一般ユーザーが，毎秒数メガビットから100 Mビット/sのインターネットアクセス環境を，低コストで導入することができるようになってきているからである。

オフィスや家庭だけでなく，外出先でもこのようなブロードバンド環境を利用したいというニーズが高まり，

無線LANを用いた「ホットスポットサービス」が注目を集めている。

このサービスは，空港や駅，ホテルなどのホットスポットと呼ばれる場所で，無線LANを用いてパソコンやPDA(携帯情報端末)のユーザーにインターネットアクセス環境を提供するものである。ホットスポットには無線LANのアクセスポイントが設置されており，ユーザーは，無線LAN機能を搭載した端末を持ち込めば，いつでもこのサービスを利用することができる。毎秒数メガビット以上の帯域で通信することが可能であり，通信帯域の観点からは，PHSや携帯電話を利用した場合よりも有利である。

ここでは，ホットスポットサービスで無線LANシステムに求められる機能，それを実現するための機器の配備，システムの基本構成と企業ユーザーへのサービス展開，および将来に向けた移動通信対応について述べる。

2 無線LANシステムの概要

ホットスポットサービスのための無線LANシステムに必要な機能は以下のとおりである(**図1**参照)。

(1) ユーザー認証

不正ユーザーのアクセスを防止するためには，ユーザーが無線LANシステムに接続する際に，何らかの形でユーザー認証を必要とする。その方法には，ユーザーID(Identification)やパスワードによる認証のほか，電子証明書による認証などがある[1)]。

現在，無線LAN製品の認証機構としては，無線LANネットワークカードの固有IDである「MACアドレス(Media Access Control Address)」や，独自仕様によるものがある。しかし，これらは，運用性や汎用性の面でホットスポットサービスには不向きである。

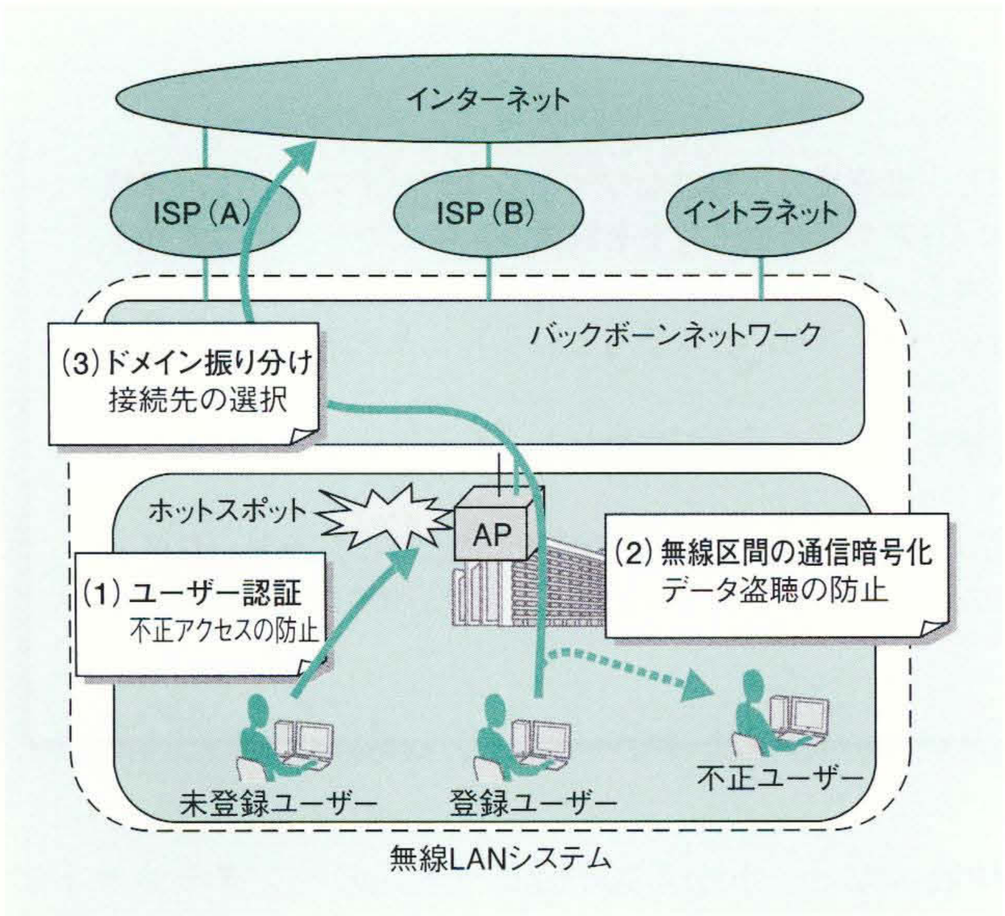
(2) 無線区間の通信暗号化

ホットスポットでは，不特定多数のユーザーが存在するため，無線区間の電波はどのユーザーでも取得することができる。そのため，セキュリティの面から，何らかの方法で通信データを暗号化する必要がある。少なくとも，IDやパスワードといった認証データの暗号化は不可欠である。

現在，WEP(Wireless Equivalent Privacy)による暗号化方式が用いられているが，これは，暗号強度の脆(ぜい)弱性が指摘されている。また，この方式は複数ユーザーが同一の暗号かぎを使用するので，ホットスポットサービスのセキュリティ確保には適用しにくい。

(3) ドメイン振り分け

現在のインターネットアクセスでは，ユーザーがインターネット サービス プロバイダー(ISP)と契約し，ADSLやFTTHなどのアクセス回線からISPに接続する。その際，アクセス回線を提供する通信事業者によっては，複数のISPを利用することも可能である。この場合，ユーザーが接続を希望するISPへユーザートラヒックを振り分ける必要がある。無線LANシステムでも同様の機能が適用でき，これにより，ユーザーの利便性が向上する。また，これをVPN(Virtual Private Network)への振り分けに応用することができる。



注：略語説明　ISP(Internet Service Provider)，AP(Access Point)

図1　ホットスポットサービスで無線LANシステムに求められる機能

無線LANシステムには，「ユーザー認証」，「無線区間の通信暗号化」，および「ドメイン振り分け」機能が必要である。

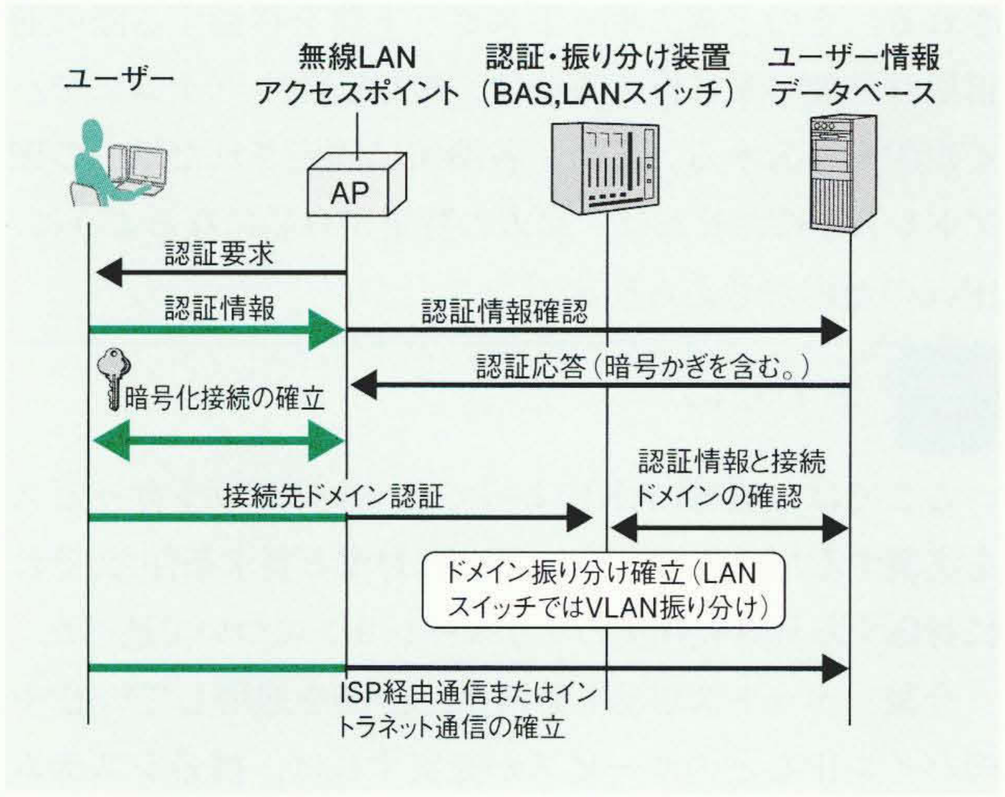
3 無線LANシステムへの適用技術

2章に述べた要求機能は，無線LANシステム内の無線LANアクセスポイントと，ブロードバンドアクセスサーバ(BAS)やLANスイッチなどの認証・振り分け装置に分けて配備される(**図2**参照)。

3.1 無線LANアクセスポイント

アクセスポイントは，ホットスポットごとに配置する。このアクセスポイントでは，「ユーザー認証」と「無線区間の通信暗号化」を行う。

アクセスポイントでは，接続するたびにユーザーの認証が要求される。正しく認証が行われたユーザーのトラヒックは転送されるが，認証されないユーザーのトラ



注1：━━(暗号化通信)
注2：略語説明
BAS(Broadband Access Server)

図2　アクセスポイントと認証・振り分け装置でのユーザー接続動作

アクセスポイントでは「ユーザー認証」と「無線区間の通信暗号化」を行い，認証・振り分け装置では「ドメイン振り分け」と「ユーザー認証(振り分け用)」を行う。

ヒックは破棄される。こうすることにより，不正なユーザーがシステムを利用することを防ぐ。

ユーザー情報については，認証ごとに，RADIUS(Remote Authentication Dial-in User Service)かLDAP(Lightweight Directory Access Protocol)を用い，データベースに問い合わせる。

認証時には，ユーザーごとに異なる暗号かぎを配布し，そのかぎを用いて無線区間の通信暗号化を行う。さらに，一定の時間間隔で暗号かぎを更新することにより，通信データの不正な解読に対する強度も向上させる。

これを実現するために，“IEEE802.1x”[2]機能をアクセスポイントに搭載する。この規格はIEEE(Institute of Electrical and Electronics Engineers)で標準化されていることから，今後の汎用性も高い。

3.2　認証・振り分け装置(BAS, LANスイッチ)

ADSLなどのユーザー認証とドメイン振り分け機能には，ブロードバンド アクセス サーバ(BAS)が利用されている場合が多い。しかし，同様の仕組みは，LANスイッチのユーザー認証とVLAN(Virtual LAN)機能との組合せでも実現することができる。

3.1で述べたアクセスポイントと同様のユーザー認証機能を搭載することにより，認証後にユーザーを適切なVLANに接続させることもできる。インターネット サービス プロバイダー(ISP)やバーチャル プライベート ネットワーク(VPN)ごとにVLANを割り当てることで，ドメイン振り分けを実現する。

4　システムの構成例

3章で述べたアクセスポイントとLANスイッチを核としたホットスポットサービスの無線LAN基本構成を**図3**に示す。

4.1　イーサネット※)拡張による基本構成

「ユーザー認証」と「無線区間の通信暗号化」にアクセスポイントを，「ドメイン振り分け」にLANスイッチのVLAN振り分け機能をそれぞれ用いることで，システム全体をイーサネット網で構成することができる。

イーサネット網には以下のような利点がある。

(1) イーサネットレベルの高速フォワーディングを行うので，ネットワーク的なボトルネックが少ない。

(2) 上位プロトコルの影響が大きくないことから，IPv6(Internet Protocol Version 6)への移行時のシステムへのインパクトが少ない。

また，アクセスポイントでのユーザー認証時の情報により，ユーザーが接続しているホットスポットを特定することができ，その位置情報を活用したロケーションサービスも展開することができる。

例えば，ホットスポットがファストフード店やコンビニエンスストアにある場合，商品の割引券をユーザーに

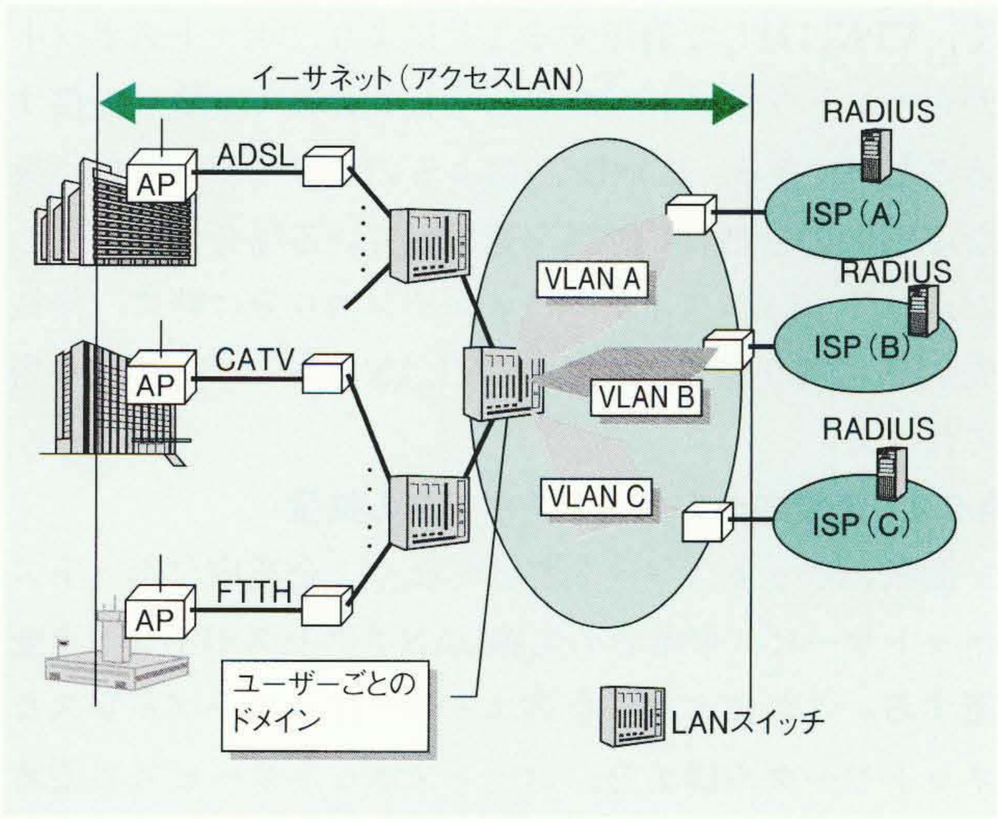
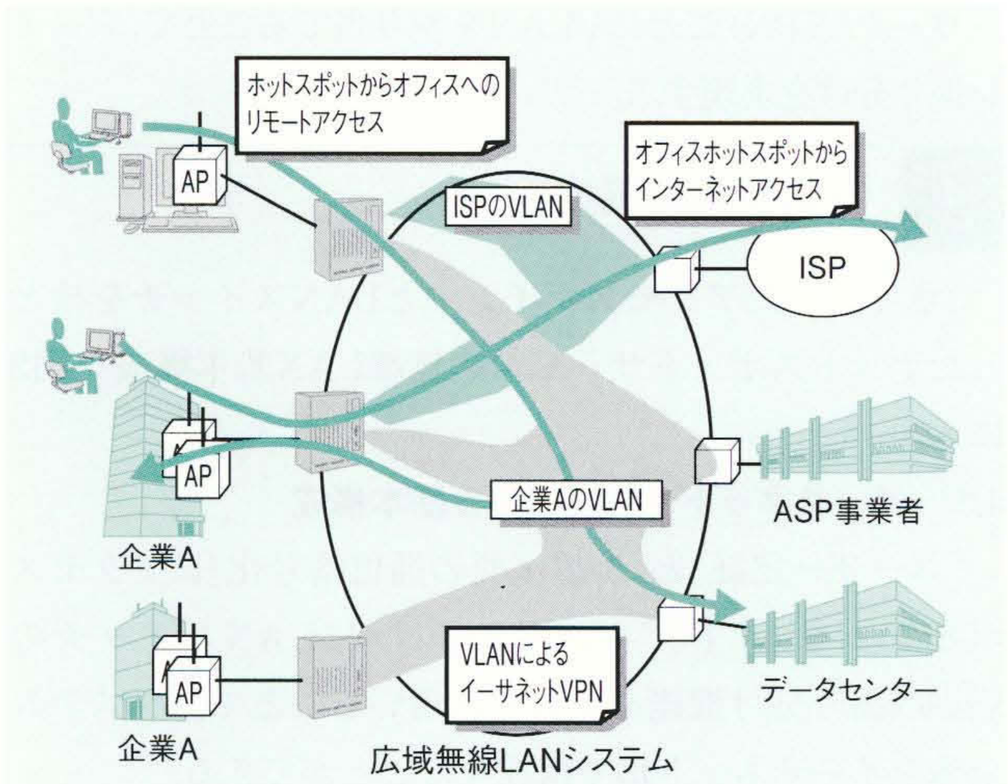


図3　無線LANシステムの基本構成

イーサネットによるアクセス網の構築が可能なことから，広帯域かつ上位プロトコル〔IP(Internet Protocol)〕などの変更に伴う影響を最小限に抑えることができる。

※) イーサネットは，富士ゼロックス株式会社の商品名称である。



注：略語説明 ASP(Application Service Provider)

図4 企業ユーザーへのサービス展開例

企業ユーザーへのサービスには，ホットスポットからのリモートアクセス環境の提供や，企業内ネットワークへのホットスポットの拡張がある。

配信するなどのサービスができる。

4.2 企業ユーザーへのサービス展開

企業ユーザーへのサービス展開としては，以下のようなアプローチが可能である(**図4**参照)。

(1) ホットスポットからのイントラネット接続

(2) 企業内へのホットスポットの拡張

4.2.1 ホットスポットからのイントラネット接続

「ドメイン振り分け」機能を，ISP振り分けだけではなく，VPNに対して適用することにより，ホットスポットからイントラネットへのリモートアクセス環境も提供することができる。広域LANによるVPNサービスでは，異なるVPNの分割にVLANを適用している場合が多い。したがって，LANスイッチのドメイン振り分け時に，接続先VPNに割り当てられているVLANにユーザーを割り当てればよい。

4.2.2 企業内へのホットスポットの拡張

公衆のホットスポットだけでなく，企業内にホットスポットサービス事業者の無線LANアクセスポイントを配置する。これにより，企業ユーザーは，ケーブルレスなネットワークの構築を，ホットスポットサービス事業者にアウトソーシング(外部委託)することができる。

4.3 移動通信への拡張

ホットスポットが拡大し，地域を連続的にカバーできるようになれば，携帯電話のように移動しながら通信することも可能となる。その場合，VoIP(Voice over Internet Protocol)やビデオチャットのような使用形態が想定される。そのとき，ホットスポット間を移動する際の通信切れを最小限に抑えるには，無線LANシステムにモバイルIPを導入する。また，各端末に固定された単一のIPアドレスを持たせれば，端末の特定が容易になるように，IPv6の適用が考えられる。

5 おわりに

ここでは，無線LANによってホットスポットサービスを実現するための，ネットワークに対する要求条件と，それに対応する日立製作所のソリューションについて述べた。

今後，ホットスポットが増え，IPv6を適用してVoIPやモバイルIPなどのサービスが充実すれば，携帯システムと競合するレベルに成長する可能性もある。

日立製作所は，ユーザーに有用なソリューションの提案を目指し，今後も研究・開発を進めていく考えである。

参考文献

1) 萱島，外：ブロードバンド時代のネットワークセキュリティ，日立評論，**84**，5，379～382(2002.5)

2) IEEE Draft P802.1X/D11, Standard for Port based Network Access Control

執筆者紹介

新保 勲
1975年日立製作所入社，情報・通信グループ ネットワークソリューション事業部 キャリアソリューション本部 所属
現在，IPシステムのエンジニアリングの取りまとめに従事
電子情報通信学会会員
E-mail：ishinbo @ itg. hitachi. co. jp

柴田治朗
1986年日立製作所入社，情報・通信グループ ネットワークソリューション事業部 キャリアソリューション本部 第二部 所属
現在，IPシステムのエンジニアリングの取りまとめに従事
電子情報通信学会会員
E-mail：harshiba @ itg. hitachi. co. jp

白井啓介
1991年日立製作所入社，情報・通信グループ ネットワークソリューション事業部 キャリアソリューション本部 第二部 所属
現在，IPシステムのエンジニアリングに従事
E-mail：k-shirai @ itg. hitachi. co. jp

田中宏司
1999年日立製作所入社，情報・通信グループ ネットワークソリューション事業部 キャリアソリューション本部 第二部 所属
現在，IPシステムのエンジニアリングに従事
電子情報通信学会会員
E-mail：koujtana @ itg. hitachi. co. jp