
NRI White Paper

実オフィス環境下における 企業内無線LAN環境の有効性評価

要約

現在、無線LAN及びその関連分野に対する関心が高まっている。無線LAN関連機器が、比較的安価で導入することで、使い勝手が向上したことを契機に、無線LANの普及が一気に広がっている。多くの企業が無線LAN導入に関心を示しているものの、なかなか実際に導入まで踏み切ることが困難なようである。特に企業で大規模に利用する場合、相当に険しい壁に直面する。その壁は「無線LANならではの特性を踏まえた設計・構築ノウハウが必要」であること、そして「採用すべきセキュリティの決め手がない」ことである。

野村総合研究所およびNRIデータサービスでは、企業における無線LAN環境に関する実証実験を実施し、実オフィス環境内における無線LAN環境(今回はIEEE802.11b)の有効性、特に「スループット性能」及び「セキュリティ性能」に関する検証を行った。

本実証実験を通じて、企業情報システムにおけるネットワーク・インフラの一つとして、無線LANは有効であることが明らかになった。さらに、無線LANによる情報システム環境が、ユーザーにとって快適かつ安心した環境となるためには、当然のことながら、実績やノウハウに基づいた手順と手段で設計・構築することが極めて重要である。パフォーマンスの優劣は、無線LANのAPの配置の仕方でも過言ではない。無線LANを心配視するのではなく、有線LANと無線LANを適材適所に使い分けながら、安全で使い勝手に優れたネットワーク・インフラ環境を実現し、企業内情報システムの高度化に貢献することが期待される。

株式会社野村総合研究所

事業戦略コンサルティング部 高橋

NRIデータサービス株式会社

基盤プロジェクト部

向山

NRI White Paper

実オフィス環境下における企業内無線LAN環境の有効性評価

目次

I 本実証実験の目的	2
II 企業における無線LAN環境の有効性.....	3
1. 企業IT革命は新たなステージへ	3
2. 無線LANに関する市場/技術動向	5
1) 無線LAN規格の動向.....	5
2) 無線LANコミュニティの形成.....	7
3. 企業内無線LAN環境構築に関する基本的な考え方	8
1) 無線LANの設計フロー.....	9
2) 要件の整理	9
4. 無線LAN環境におけるセキュリティ対策の基本的な考え方.....	12
1) セキュリティの仕組み	12
2) より高度なセキュリティ機能	16
3) 企業内無線LAN構築におけるセキュリティ面での課題	21
4) 企業内無線LANにおけるセキュリティ構築	24
III システム構成概要.....	29
1. ハードウェア構成	29
2. ソフトウェア構成.....	30
IV 実験内容とその結果	31
1. 実験対象項目の概要	31
2. 実験結果	32
1) 無線LANの実用性.....	32
2) 移動時の有用性	47
3) 製品間の相互接続性.....	52
4) 電波干渉性.....	54
V 結論.....	60

I 本実証実験の目的

わずらわしいケーブル接続によるネットワーク構築に代わる手段として、無線LANが注目を集めている。近年無線LANの性能向上は目ざましく、ケーブル接続並みの高速通信、低価格化、ノートPCなどモバイル端末への実装という、普及につながる3つの要素が実現されている。PCはオフィスや家庭など屋内で机に座って使うものという固定観念は薄れ、いつでもどこでもブロードバンド・ネットワークにつながる快適なコンピューティング環境が現実のものとなりつつある。

このようなことが追い風になり、無線LANはいつでもどこでもネットワークを利用できる環境を実現するツールとして関心は高まる一方である。但し、企業での利用となると、セキュリティへの不安や運用管理ノウハウ不足など、システム担当者サイドの心理的導入障壁は高く、実際はそれほど普及が進んでいないというのが実態である。この傾向は、企業規模が大きくなるほど顕著化するように見られる。

しかし、新たな企業ネットワークとして、無線LANに対するユーザの関心は高く、それらに応えるように、無線LAN関連の製品開発は急速に進展しつつある。セキュリティや運用管理製品の中にも、国内企業のユーザ事情を考慮した製品が登場し始めており、無線LANインフラ構築面での導入障壁は、段階的とはいえ着実に低くなりつつある。

さらに、2003年3月、モバイル・コンピューティング向けに最適なパフォーマンスを発揮するように設計されたNote型PC向け最新テクノロジー「Intel® Centrino™ モバイルテクノロジー(以下、「Centrino」)」が、インテルよりリリースされた。Centrinoを搭載した端末は、無線LAN(現時点ではIEEE802.11b)機能を標準で装備しており、バッテリーによる長時間の連続使用が可能であるなど、無線LANに接続する有力端末の一つとして注目を集めている。

このように、企業向け無線LANの導入環境の向上に伴い、無線LANの導入を検討する企業が増えていくであろう。しかしながら、実際の無線LAN構築には、機器やソフトウェアの性能向上だけではカバーできない、無線ならではの構築・運用ノウハウが必要となる。言い換えると、無線ならではの構築・運用ノウハウを正確に認識し、実践することにより、最適な企業内無線LAN環境の構築・運用に近づくことができる。

そこで、野村総合研究所とNRIデータサービスは、上記の状況を鑑み、無線LANの特性を把握しながら、実オフィス環境における無線LAN環境の有効性について評価を行った。今回の評価項目は、基本的な構築ノウハウに関わる項目をメインとした。

以上まとめると、本実証実験の目的は下記の通りである。

< 実オフィス環境下における企業内無線LAN環境の有効性評価 >
スループット性能の評価
セキュリティ性能の評価
(特にレベルに応じたシステム構成のあり方)

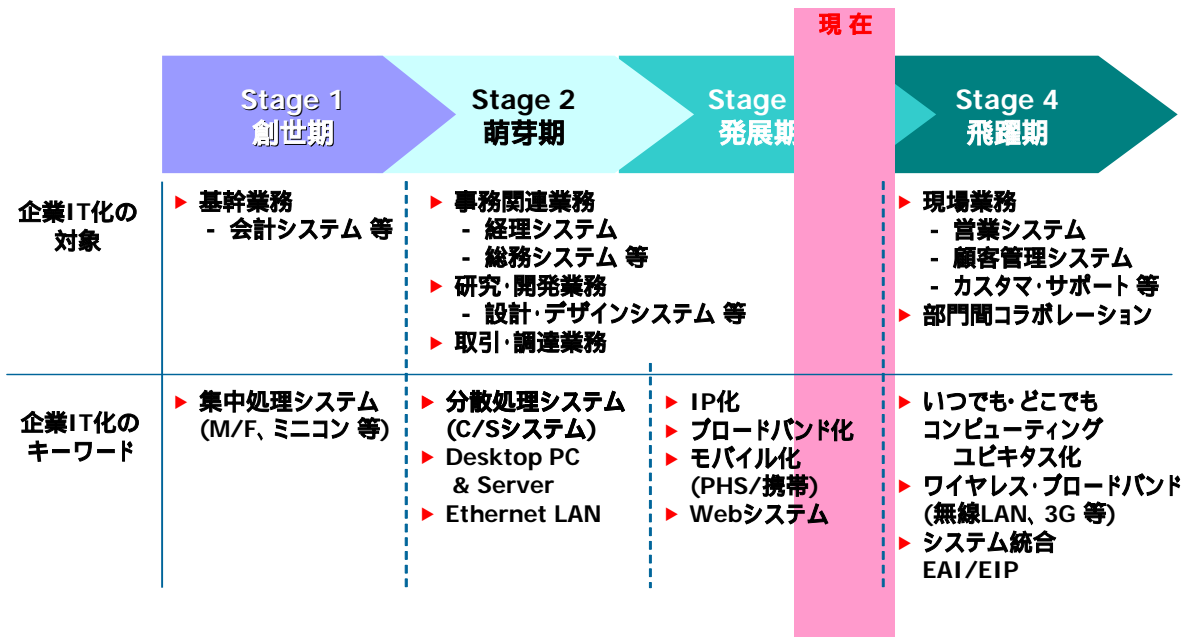
II 企業における無線LAN環境の有効性

1. 企業IT革命は新たなステージへ

急速な進歩を続けている「企業活動におけるIT化の波(=企業IT革命)」は、今まさに新たなステージへと進化しようとしている。これまで、企業活動とITソリューションは密接で不可欠な関係を築いてきた。この傾向は、ITソリューション技術の進展につれ、業務環境の改善、業務の効率化、生産性の向上、意思決定の迅速化など、企業活動の多種多様な分野へと拡がりつつある。

これまでの企業IT革命は、業務の効率化や生産性の向上など、業務活動面におけるIT化を中心に展開されてきた。これからの企業IT革命は、整備された情報システムを、あらゆる業務シーンで利用してもらえるステージ実現するステージへと進化していくと考えられる。

図表II-1：業務システムの変遷



このような動きの中、“いつでも・どこでも”を実現する手段として、無線LANによるソリューションが注目を集めている。

とはいうものの、普及が進んでいるのは家庭やSOHOが中心で、企業での本格的導入はあまり進んでいないというのが実態である。家庭などに比べ、企業で導入する場合、有線によるネットワークとは異なる、無線特有の考え方を相当検討しなくてはならない。特に、無線LAN部分におけるセキュリティ対策については、まだまだ不確定要素も多く、決め手となるソリューションが確立されていない状況である。確かに、無線LANの導入メリット以上に、課題や問題点ばかりがクローズアップされるため、企業側としては無線LAN導入に躊躇せざるを得ないのかも知れない。

一方で、ここへ来て、無線LANに対する関心の高まりに対して、このようなネガティブな状況を打破しようとする動きが本格化しようとしている。セキュリティの分野を中心に、設計構築・運用ノウハウが蓄積され、様々なソリューションが現れ始めている。これを期に、企業での無線LAN導入が本格化すると期待されている。

本稿では、無線LANの動向をまとめるとともに、野村総合研究所およびグループ各社における、無線LAN環境の構築に関する基本的な考え方について記述する。

2. 無線LANに関する市場/技術動向

1) 無線LAN規格の動向

現在、無線LANの規格はいくつか存在しているが、企業向けとしてはIEEE802.11規格が主要なものである。標準化の動向についても、IEEE802.11を中心に作業が進められている。技術的な詳細な動向については、各種専門資料を参考にしていただきたい。

IEEE802.11規格の動向

- ・ IEEE802.11a/b/g等の通信速度に関する仕様が策定済み。今後は、HiperLAN2が先行して仕様化しているQoSやパワーマネジメントの仕様、ならびに脆弱性が指摘されているWEPを補強するセキュリティ仕様策定がメインとなる見込みである。
- ・ IEEE802.11bは実績としては古く、比較的安価に構築可能であることから、「家庭」、「SOHO」、「企業(小規模利用)」、そして空港やホテル、コーヒーショップなどにおける「公衆無線LAN環境(いわゆるホットスポット)」など様々なシーンで利用され、一番普及している無線LANの規格である。企業でセキュアに利用するには更なる検討が必要である。さらに、多くのユーザで共有して利用するには、速度の面で難がある。
- ・ IEEE802.11aについては、今後セキュリティが強化された製品が出てくる見込みであり、セキュリティ面が考慮された高速アクセスが可能になる。
- ・ IEEE802.11gは2003年6月、IEEE(米国電気電子技術者協会)により標準仕様として承認された。IEEE802.11gは、IEEE802.11bと同じ周波数帯域(2.4GHz)と搬送周波数を利用しており、同一ネットワーク上でそれぞれの規格に対応する機器が混在する場合でも、IEEE802.11g機器は通信速度をIEEE802.11bと同じ11Mbpsに下げることにより、相互通信が可能となる。標準化の決定を受け、セキュリティ対応など、企業向けIEEE802.11g関連製品のリリースが今後本格化すると予想される。IEEE802.11gの標準化を待ち無線LANの導入を控えていた企業、IEEE802.11bから移行する企業など、IEEE802.11gに関連するユーザ企業の動向が注目される。

HiperLAN 2規格の動向

- ・ 欧州ETSI BRANにて策定された5GHz帯無線通信仕様であり、欧州の標準規格として位置付けられている。対応製品は現状未発表である。QoS等機能が充実しており、機能面では同じく5GHzを利用するIEEE802.11aより優れているものの、対応製品発売時期、コストによってはIEEE802.11aに駆逐される恐れがある(現状のIEEE802.11a製品は欧州では利用できない)。

Bluetooth規格の動向

- ・ 携帯端末等に搭載されている「Bluetooth Ver. 1.1」の次の仕様「Ver. 2」が現在策定中である。Bluetooth Ver.2の仕様は高速化の他、接続対象、アプリケーション別に仕様が策定されており、データ通信機器としての無線LANの使い方よりも単距離の機器間コミュニケーション(PAN : Personal Area Network)への利用を目指す方向にある。

図表II-2：無線LAN規格の特徴

無線規格仕様	内容
IEEE802.11a	高速通信可能 (54Mbps：実効速度：20Mbps) 5GHz帯を利用するため、ISMバンド製品との干渉なし WEPセキュリティの脆弱性 実売コスト高 (PCカード：2~3万円、AP：5~10万円) × IEEE802.11bと使用周波数が異なるため互換性なし × 屋外使用は禁止 (但し、緩和検討中)
IEEE802.11b	高速通信可能 (11Mbps：実効速度：6Mbps) 高速仕様IEEE802.11gが仕様決定 ノート型PCへの実装化など、無線LANインターフェースとして最も普及 WEPセキュリティの脆弱性 IEEE802.11a製品に比べ低コスト × ISMバンドを利用するため、家電製品等との干渉
IEEE802.11g	高速である (54Mbps：実効速度：20Mbps) IEEE802.11b製品と相互通信が可能 (見込み) × ISMバンドを利用するため、家電製品等との干渉 × 対応製品の充実化はこれから
HiperLAN2 (HiSWAN a)	QoS対応、通信速度、セキュリティ、送信電力コントロールなど 仕様が充実 5GHz帯を利用するため、ISMバンド製品との干渉なし × 対応製品について未定
Bluetooth	消費電力が小さく、モバイル機器への実装が有効 モバイル機器間通信/PAN(Private Area Network)向き × 通信速度が遅い (理論上720kbps) × カバレッジエリアが狭い (10m)

その他、UWB(Ultra Wideband)など短距離向けの高速無線通信技術もある。

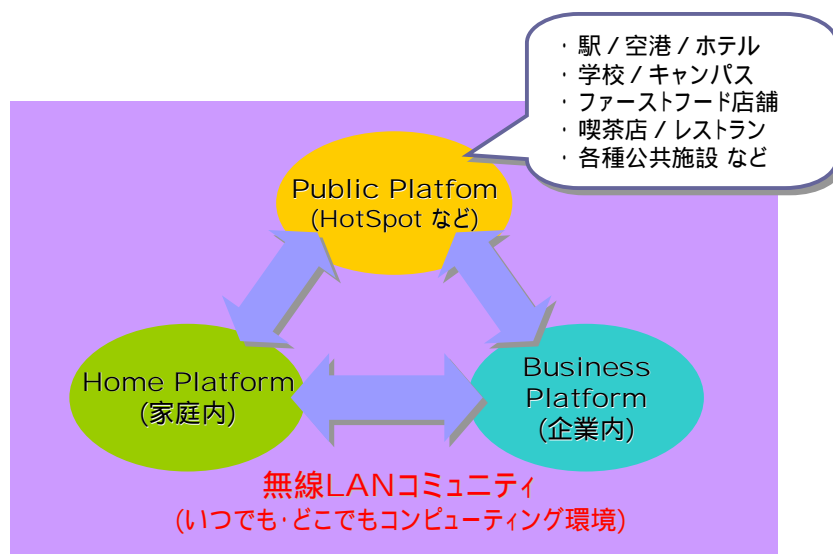
2) 無線LANコミュニティの形成

無線技術の発展に伴い、電話の世界が有線による固定電話から無線による携帯電話へ急速にシフトし、「いつでも・どこでもコミュニケーション」の環境が実現した。この流れは、コンピューティングの世界へと展開中であり、「いつでも・どこでもコンピューティング」環境の実現に向けて動きつつある。その中で大きな役割を果たしているのが無線LAN技術(IEEE802.11)である。

近年、比較的安価で導入することでき、使い勝手が向上したことを契機に、無線LANの普及が一気に広がった。これまで、無線LANの導入箇所と言えば、ネットワークの配線が困難な箇所や新規にネットワークを敷設する箇所などが多かった。現在では、手軽にネットワーク環境を構築できることが受け入れられ、無線LANの適用範囲は拡大傾向にある。

無線LANの主なユーザは、「公共(公衆無線LAN環境など)」、「家庭」、「企業(行政機関も含む)」である。将来的にはこれらが相互に連携しあい、シームレスな「無線LANコミュニティ」が形成され、「いつでも・どこでもコンピューティング環境」のが実現すると考えられる

図表II-3：無線LANコミュニティ(イメージ)



3. 企業内無線LAN環境構築に関する基本的な考え方

企業において無線LANを利用することは、下記に示すような、無線ならではのメリットが考えられる。実際、無線LANを導入している企業によると、「従業員の志気(やる気)が向上した」など、数字には中々表れない、定性的な効果もあるようである。

< 企業における無線LAN導入のメリット >

- ・ オフィスや屋外を問わず、無線LANが利用できる場所であればどこでも、企業システムを快適な環境で利用可能。
業務環境の改善向上 & 業務生産性の向上
- ・ オフィスレイアウトの変更やユーザの増減などに柔軟に対応可能
システム管理者における運用管理負荷が軽減
- ・ 顧客や訪問者に対しても、ブロードバンド・ネットワーク環境を提供可能
顧客や訪問者へのサービス向上
- その他、企業側の設計やポリシー次第で、あらゆるメリットが実現可能

このように、無線LANならではの特有のメリットがあるのにも関わらず、実際にはそれほど導入が進んでいないのが実態である。その主要な理由としては、電波は広い範囲に届くため、ケーブルを用いた1対1の物理的な接続に比較してセキュリティ面に対して弱いと考えられていることが挙げられる。

更に、業界標準化の動向と低価格化で急激に無線LANの市場が拡大しているため、ネットワーク設計や運用などの方式、仕組みの確立が追いついていないことも、導入進展を阻害している要因として考えられる。

< 企業における無線LANの導入障壁 >

無線LAN特有の設計・構築方法

APの設置場所、同時アクセス台数、スループット維持 等

無線LANにおけるセキュリティ管理 技術の標準化動向が不明確

無線LANにおける運用管理

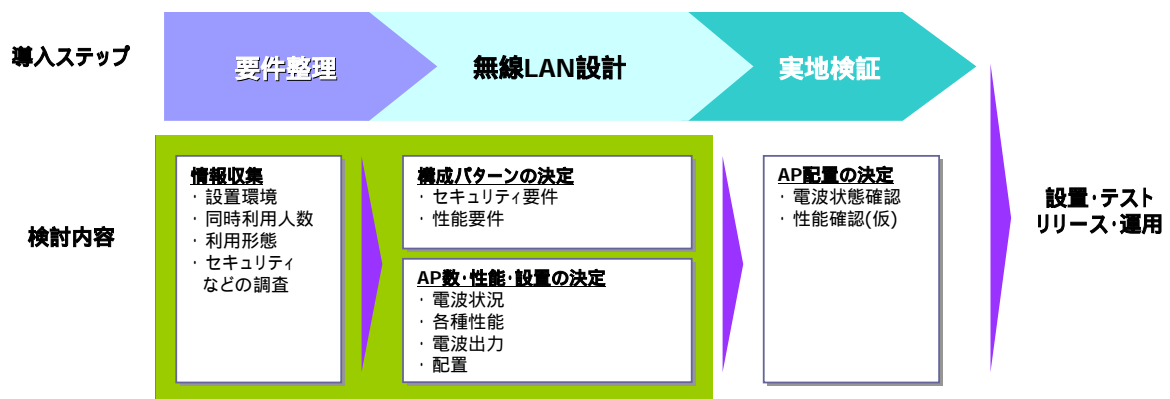
無線LAN導入で重要なのは、標準技術への対応ではなく、企業各社でのセキュリティ・ポリシーや運用・管理方法を早期に確立することである。そのためには、セキュリティ技術や標準技術の進展に期待して無線LAN導入に躊躇するのではなく、ノウハウ蓄積といったレベルから、段階的に導入を進めていくことが重要であると考えられる。

野村総合研究所およびグループ各社における、企業内無線LAN環境構築に関する基本的な考え方について、以下に示す。また、無線LANのセキュリティに関しては、「4. 無線LAN環境におけるセキュリティ対策の基本的な考え方」でより詳細に示す。

1) 無線LANの設計フロー

- 野村総合研究所およびグループ各社が考える「無線LANの設計フロー」について、下記に示す。

図表II-4：無線LANの設計フロー



2) 要件の整理

無線LANを設計する際に検討すべき要件について、以下に示す。

図表II-5：無線LANの設計における検討要件

検討要件		検討内容
セキュリティ要件	利用場所	屋外、屋内、店舗、オフィスなどの区分 例) オフィス内での利用
	利用者	利用者の区分 例) 社員が利用。それ以外は利用不可。
	情報の重要度	利用する情報に対する重要性 例) 機密度の高い情報のやり取りはあるか？
環境要件	利用場所の広さ	無線LANを利用する場所の縦方向・横方向の長さおよび面積 例) 縦40m横30m
	利用場所のレイアウト	利用場所に存在する区画、什器などの配置 例) 会議室、パーティション、壁、床などの配置図

	電波干渉の可能性のある機材	無線LANの利用する周波数帯に干渉する電波を使っている機材の確認 外部、または内部のAPからの電波確認 例) Bluetooth機器、電子レンジ、医療用機器などの有無 他のビルからの電波
性能要件	利用人数	利用する人数 例) 最大30人、通常20人
	利用時間	利用している時間帯、ピーク時間など 例) 9:00-20:00が利用時間 ピーク時間帯9:00-10:00および17:00-18:00
	利用頻度	利用するアプリケーションと頻度 例) 1時間に10ページのWebページ閲覧 ピーク時はある時点で半数の人がネットワーク帯域を使用
	レスポンスタイム	レスポンスタイム (サーバ処理時間等、無線以外の要素はここでは考慮せず) 例) ピーク時に社内Webページが3秒以内に表示されること

その他、価格要件、納期要件についても検討する必要がある。

[特に無線LANで必要な検討要件]

利用場所・利用者・情報の重要度

- ・ とともにセキュリティ・レベルを決定する際に必要な情報である。企業の機密管理事項などを取り扱う際には性能だけではなく、セキュリティを特に考慮すべきである。ネットワークを流れる情報、または接続されている端末上の情報の重要度を確認し、どの程度のセキュリティ(性能)が必要かを見極める必要がある。これらの要件による構築パターンの選択については後に述べる。

利用場所の広さ

- ・ IEEE802.11bでは電波の最大到達距離が100mとされている。ただしこれはIEEE802.11bの1Mbpsモードの最大距離であり、11Mbps(最大スループット)で通信できる範囲はその半分以下である。したがって何も障害物や妨害電波がない状態ではAPからせいぜい半径50m以内が通信可能範囲である。

利用場所のレイアウト

- ・ 電波はその性質上、通信路上にある物体によって反射したり、吸収されたりする。そのため直接目では確認できないAPからの電波が受信できることもある。逆にAPとクライアントの距離は近いが、通信路上に障害物があるため通信ができなくなる場合もある。以下に電波を反射するもの、電波を通さないものを例示する。
 - 反射するもの：
 - 金属のドア、パーティションなど (ただし電波が透過するものもあるので注意が必要)
 - 電波を通さないもの：
 - 石、コンクリートなど

電波干渉の可能性のある機材

- ・ 同じ周波数帯を利用する通信機器や、他の機械やモーターなどから発するノイズなどが原因で、無線LANの電波と干渉を起こし通信を妨害することがある。特にIEEE802.11b規格では免許不要で自由に利用できる2.4GHz周波数帯 (ISMバンドと呼ばれる) を利用しているため、以下のようなものが近辺にあるかどうか留意する必要がある。
 - Bluetooth、電子レンジ、医療用機器、万引き防止用装置

[有線LANでも必要な検討要件]

利用人数 / 性能

- ・ 利用者は、有線ではネットワーク回線を共有するが、無線でも同様に電波帯域を共有する。フレームの衝突回避制御方法は異なっているが、無線のCSMA/CA方式でも、複数のクライアントが帯域をほぼ平等にシェアする。利用頻度にもよるが、利用人数が増えれば増えるほど、一人当たりが利用できる帯域は少なくなり、スループットは低下する。これらを元に1つのAPに対してどれぐらいの人数が利用できるかを考えると、10～30人という数字が目安となる。

利用頻度

- ・ 上記で述べた利用人数と共に、ユーザのネットワーク利用頻度は無線LANの性能と関係がある。ネットワークの利用頻度が高い場合には、他人が帯域を利用している割合が高くなり、一人当たりが利用できる帯域は少なくなる。

レスポンスタイム

- ・ 上記で述べたように、帯域をユーザが共有するため、ラッシュ時の性能を考慮した設計が必要となる。1対1で通信した場合のスループットを人数分で割った値が最大帯域となる。

4. 無線LAN環境におけるセキュリティ対策の基本的な考え方

1) セキュリティの仕組み

現在無線LANを検討する上で最も大きな課題になっているのが「セキュリティ対策」である。テーマそのものが社会的にクローズアップされている上に、最近特に無線LANにおけるセキュリティの脆弱性が指摘されることが多くなっている。

有線LANと比較して無線LANが特徴的なのは、その物理的な性質上、常に盗聴の危険性にさらされていることである。したがって、無線LANのセキュリティを考慮する際には、無線LANクライアントからAPへのアクセスの可否を規制する認証機能(アクセス制御機能)と、ネットワークを流れるデータそのものの暗号化機能が必要になる。基本的な対策としては、

- ・ 認証については「ESS-IDとMACアドレス・フィルタリング」
- ・ 暗号化については「WEP (Wired Equivalent Privacy)」

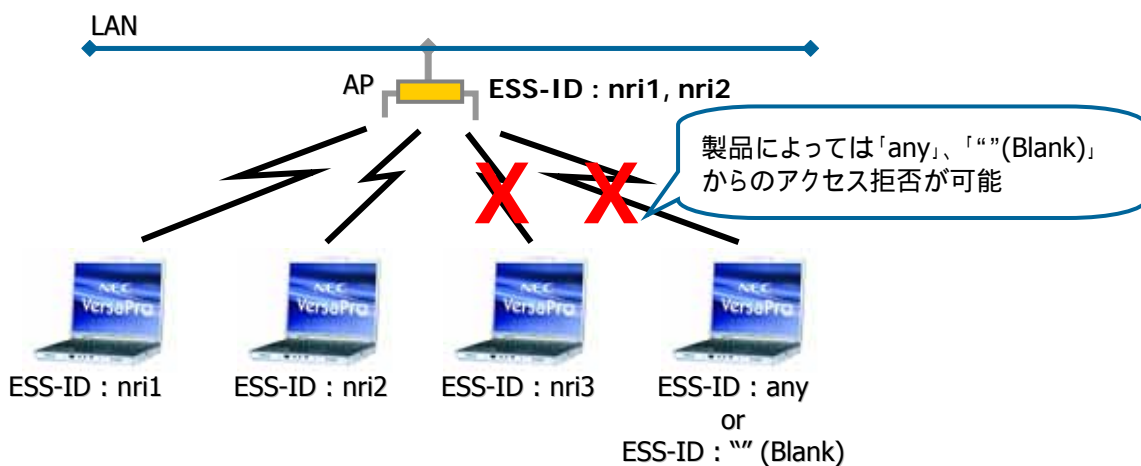
という機能を活用することが最初のステップであると考えられる。以下それぞれについて解説する。

(1) ESS-ID

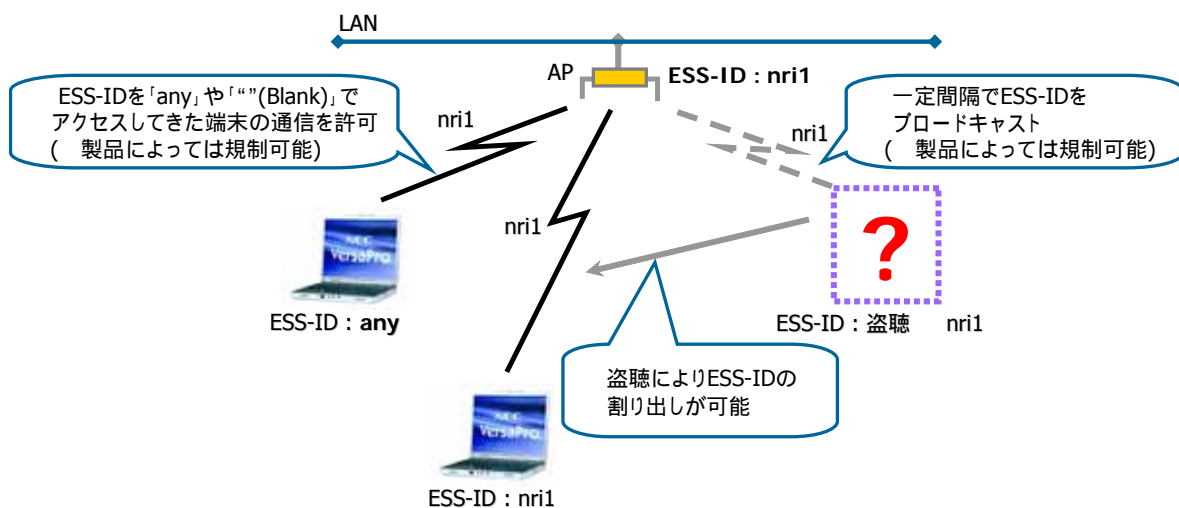
ESS-IDとは無線LANクライアントと無線LANアクセスポイント(AP)が相互に認識を行う機能である。この機能をセキュリティ対策として活用することができる。あらかじめAP側に接続を許可するESS-IDを登録しておくことで、登録していないESS-IDからのアクセスを拒否することができる。ただし、APに付属のユーティリティソフトや、「Net Stumbler」のようなインタ - ネット上にフリ - で公開しているAP 検知ツールを利用すれば、そのAPに登録されているESS-IDの登録情報を知ることができてしまう。これはAP側が自ら登録しているESS-IDをブロードキャストしているためである。また、端末側のESS-IDに「any」と登録するか、何も登録しない(「空白」)とその端末からのアクセスを拒否できない。そこで最近では多くの製品が、ESS-IDを隠蔽したり、無線LAN クライアント側のESS-IDが「any」あるいは「空白」の場合にはAPにアクセスさせない機能を追加するようになった。しかしこうした対策を行ったとしてもセキュリティ対応としての効果は低い。通信を行っている無線データそのものを捕捉すればやはりESS-IDを入手できてしまうためである。

残念ながら、ESS-IDで行えるセキュリティ対策はこのレベルである。しかし一番の問題はこうした初歩的な対策すら施していないAP がいまだに非常に多いことなのだ。まずはセキュリティ対策の第一歩として行う必要はある

図表II-6 : ESS-IDによるセキュリティ対策



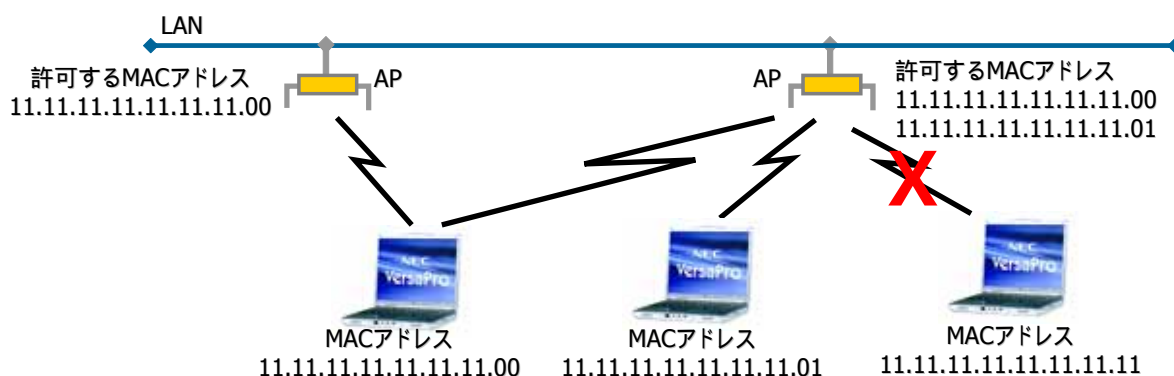
図表II-7 : ESS-IDによるセキュリティの脆弱性



(2) MACアドレスフィルタリング

MAC アドレスとは製品ごとにメーカーが割り当てる番号のことで、世界で一つのユニークな番号が16進数で「xx:xx:xx:xx:xx」というように振られる。ネットワークにつながる機器であればルータやサーバ等あらゆる機器についてMACアドレスは付与される。MACアドレスフィルタリングとは、APに登録されたMACアドレスを持つ無線LANカードのみアクセスを許可する、不正アクセスに対応したセキュリティ機能である。ESS-IDは相手を特定する機能しか持っていないのに対し、MACアドレスフィルタリングの場合は登録されていないMACアドレスを持つ無線LANクライアントからの接続を拒否することができる。

図表II-8 : MACアドレスフィルタリングの仕組み

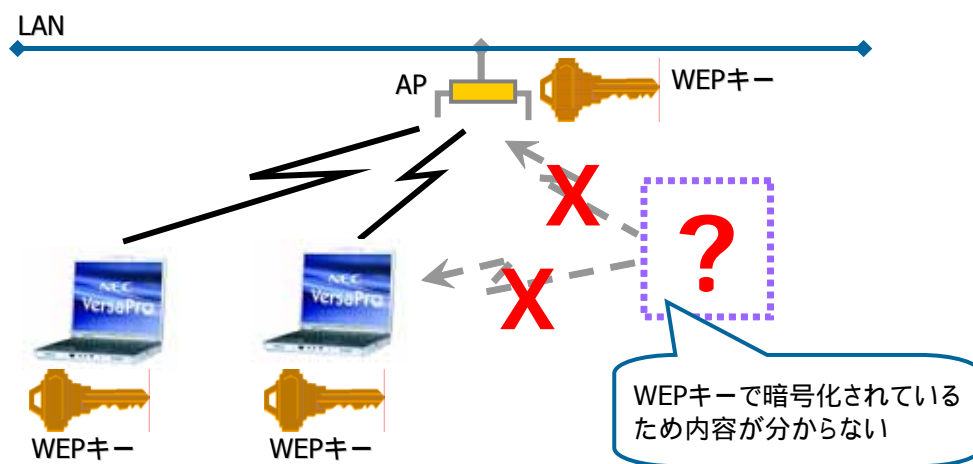


(3) WEP (Wired Equivalent Privacy)

無線LANクライアントとAP間の通信を暗号化する仕組みである。ユーザで設定する秘密鍵(通常104ビットと40ビットの2種類ある)と自動で設定されるIV(Initialization Vector : 24ビット)からなるWEPキー(128ビットまたは64ビット)をもとにRC4方式に基づいて暗号化を行う。128ビットWEPの方が暗号強度は高い。

しかし、WEPにもやはり欠点がある。一つはIVに関する問題である。WEPキーにはユーザが自由に設定を入れるユーザ設定部とあらかじめメーカー側で設定を行う自動設定部があり、この自動設定部のことをIVと呼ぶ。64bit、128bitの2パターンあるWEPキーのうち、いずれも後半部分の24ビットがIVに割り当てられている。製品によってはこのIVの内容が通信ごとに変化しない。また変化する場合でも比較的推測しやすい場合が多いのである。もう一つは前半のユーザ設定部である。ここで利用している「RC4」という秘密鍵の仕組みが現在では相当知られており、インターネット上でも解読用のツールが公開されてきている(例「AirSnort」、「WEPCrack」、「bsd-airtools」)。また秘密鍵部分は固定であるため、時間をかけて、ある程度の分量の packets を盗聴すれば比較的解読が容易可能といった問題点にも考慮する必要がある。

図表II-9 : WEPによる暗号化



以上、前述したように無線LANの基本的なセキュリティ技術は現段階では万全とは決して言えない。そこで最近ではこうしたセキュリティの脆弱性に対応していくつかの方法が検討されてきている。その方法について、「2) より高度なセキュリティ」で紹介する。

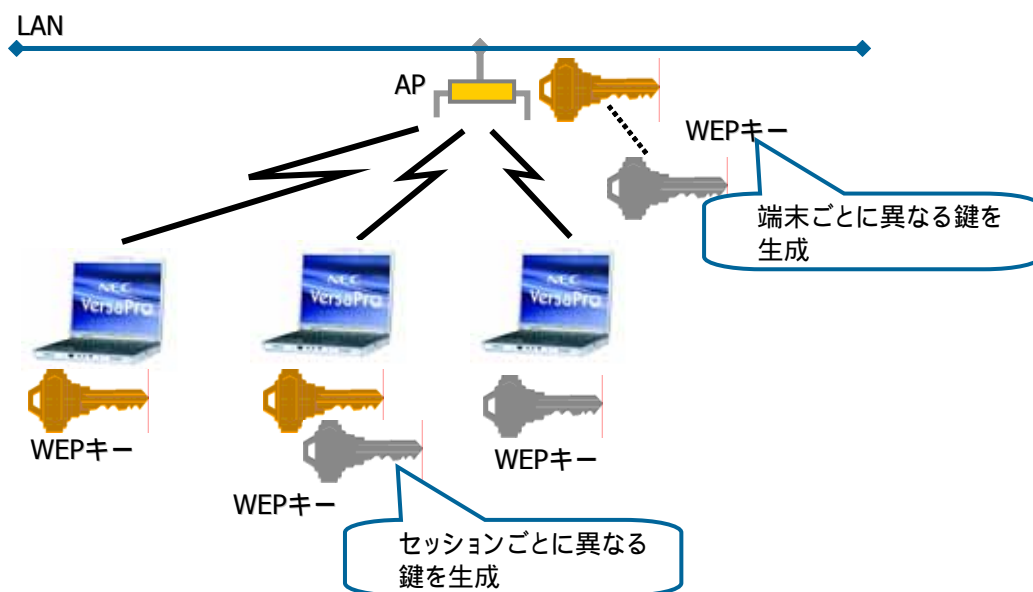
2) より高度なセキュリティ機能

(1) 動的なWEPキー/TKIP

WEPキーの問題の一つは、キーそのものが固定であるので時間をかければ解読が可能という点がある。これに対し、まずは無線LAN機器メーカー各社が独自に対応を開始した。細かいメカニズムは各社で異なるものの、基本的にはWEPキーを一定間隔(通常は15分から1時間程度に設定)で動的に変化させることができるような対策を行ってきた。しかも端末ごとあるいはセッションごとにWEPキーが異なるので、ある端末のWEPが解読されたとしても影響を最小範囲に留めることができる。

一方でIEEE802.11i(P19「2.4.4 WPA」参照)ではWEPの後継規格としてやはり動的にWEPキーを変化させるTKIP(Temporal Key Integrity Protocol)の仕様を策定している。TKIPではWEPキーの動的な変換に加え、暗号化そのものの生成手順を複雑化している。また、MIC(Message Integrity Code)等の機能を追加してWEPが持つ改ざんへの脆弱性にも対策を行っている。すでに一部のメーカーがサポートを表明しており、今後WEPの後継規格として採用が進むと思われる。

図表II-10：動的なWEP/TKIPによる暗号化



(2) AES

WEP で使っているRC4 の脆弱性を補う形で採用が期待されているのがAES(Advanced Encryption Standard)である。この技術はベルギーの暗号学者2 人によって開発された。既にアメリカ政府ではVPN 等で有名なDES(Data Encryption Standard)に変わる暗号方式として採用している。RC4 に比べ長い暗号鍵にも対応可能で、現時点では堅牢な暗号化方式として評価が高い。IEEE802.11i での標準化が見込まれているが、すでに一部製品では対応が発表されている。

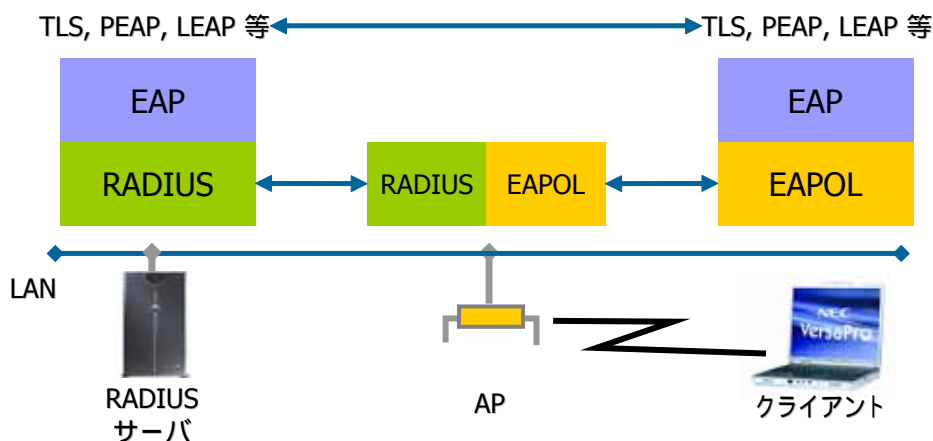
(参考) RC4とAES

WEP、動的なWEP、TKIP といずれの暗号化においても暗号方式として活用されているのはRC4である。AESは暗号方式としては堅牢であるもののその処理は複雑であるため、APの性能に大きく影響する。十分な性能を確保した新製品であれば実装が進む可能性はあるが、既存APIについてはファ - ムウェアのバ - ジョンアップ対応がどの程度行えるか難しいところである。

(3) IEEE802.1x

ESS - ID、MAC アドレスフィルタリングといった脆弱な認証技術に対して、高度な認証方式として活用が広がっている技術がIEEE802.1xである。もともとは有線LAN への不正なアクセスを防止する目的で策定されてきたが、現在では無線LANの認証技術として注目されるようになった。ポ - トごとにユ - ザ認証を行い、認証されていないクライアントからの通信は遮断する。ESS-IDやMACアドレスフィルタリングではAPと無線LAN クライアント間で認証を行っているのに対し、IEEE802.1xではAPの背後に認証用サーバ(RADIUSサーバ : Remote Authentication Dial-In User Service Server)を立ててユ - ザ認証を行う。ESS-IDやMACアドレスフィルタリングのようにAP毎の設定ではなく、RADIUSサーバ側でAPを一括して設定できるため運用効率も高い。

図表II-11：無線LANにおけるIEEE802.1xの仕組み



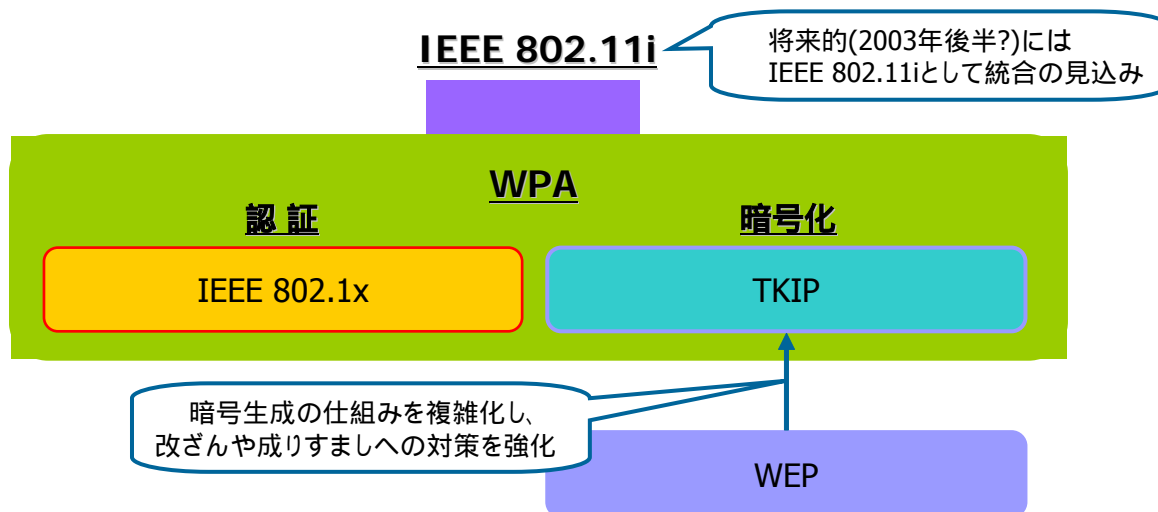
(参考) IEEE802.1x の認証プロトコル

IEEE802.1x は複数のレイヤ - のプロトコルを組み合わせることで構成されている。ポイントとなるのがEAP(Extensible Authentication Protocol)層である。下記の通り、無線LAN 機器やRADIUSサーバが認証を行う際のフレームワークを提供し、利用するプロトコルを選択できるようにする。認証プロトコルに関しては、現状ではEAP-MD5やEAP-TLS、EAP-TTLSといった標準的な手順の他に、ベンダ - 独自のLEAPや、数社が共同で策定にあっているPEAP等の認証方法を使うケースも多い。

(4) WPA (WiFi Protected Access)

認証機能のIEEE802.1xと暗号化のTKIPを一つにまとめた仕様としてWPAがある。2002年10月31日にWiFiアライアンス(IEEE802.11製品の相互接続性検証や認証を行っているアメリカの非営利団体)から発表され、対応製品のリリースが始まっている。WEPの上位互換として現在流通している無線LAN製品でも利用が可能である点などから、高度なセキュリティの実現方法として期待されている。ちなみに、WiFiアライアンスでは1年以上前からWEPの脆弱性を克服するためIEEE802.11iというセキュリティに関する包括的な規格の標準化を進めていた。WPAはこのIEEE802.11iのサブセットとして位置付けられている。IEEE802.11iの策定は、2003年末までかかると見られているが、どうやらここ1年以内にもう一度セキュリティを取り巻く情勢変化がありそうである。

図表II-12 : WPAの位置付け



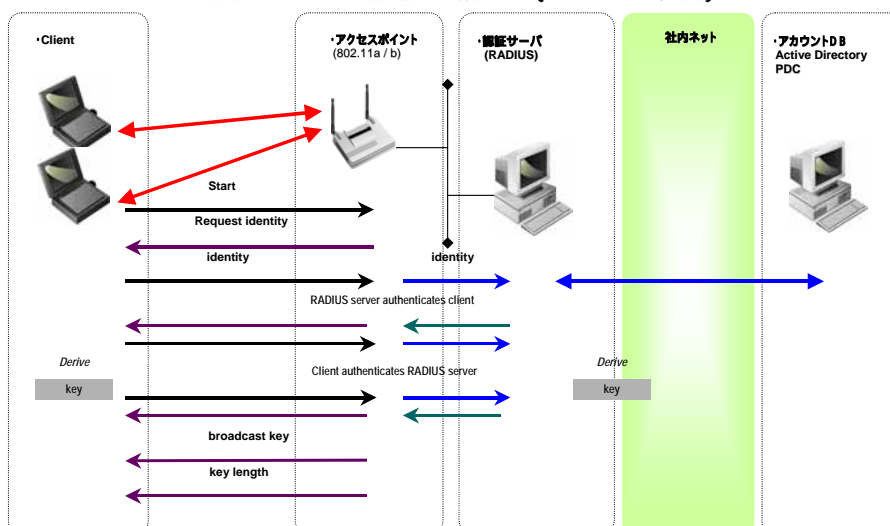
(参考) IEEE802.1xを巡る認証規格の動向

現在、IEEE802.1xを実現する認証規格が乱立状態にあり、その動向が注目されている。この中でも企業における実践的な方式として注目されているのがCisco社の「LEAP」とFunk社の「TTLS」である。両方式には下記図表に示すような特徴がある。認証サーバ・クライアント双方がユーザIDとパスワードで認証するLEAPに対し、TTLSはクライアントのみLEAP同様ユーザID、パスワードで認証するものの、サーバ側には電子証明書を持たせることにより認証を確立している。

図表II-13： IEEE802.1xを実現する認証規格の違い

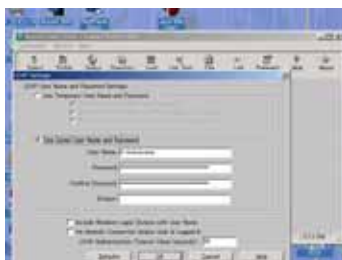
認証方式	クライアント認証	サーバ認証	概要
LEAP	パスワード認証	パスワード認証	・Cisco社独自の認証プロトコル ・外部向けに仕様公開を表明
TTLS	パスワード認証	電子証明書	・Funk SoftWare社独自

図表II-14 認証の流れ (LEAPの場合)



これでは、無線LANを導入しても、認証する回数が増えてしまい、ユーザIDとパスワードを入力する手間が煩雑になることが考えられる。しかし、この点はアプリケーション・サイドで解決されている。LEAP、TTLSともに、クライアント側にインストールされた認証アプリケーションで一度設定すればあとは自動的に入力することができる。このように、適したノウハウやソリューションを活用することにより、複雑に思われがちな無線LANでも、有効に設計構築&運用することができるのである。

図表II-15： LEAP用クライアント設定ツール(ACU)のユーザID/パスワード設定画面



(5) VPN

リモートアクセスや社内WANでVPN(Virtual Private Network)を利用している企業は多い。無線LAN固有のセキュリティ技術ではないが、暗号化の仕組みであるIPSec(IP Security Protocol)を活用することでセキュリティ強度を高めることができる。すでにVPN装置があれば、無線LANクライアントにVPNソフトを追加し、VPNと無線LANを組み合わせた構成を採用する企業は多い。

動的なWEPキーやTKIPのような無線LAN独自の暗号化技術とは異なるため、主に技術面以外の特徴について比較を示す

図表II-16：動的なWEPキー/TKIPとVPNの特徴

	動的なWEPキー/TKIP	VPN
特徴	WEP暗号(Layer 2)	IPSec (Layer 3)
必要な構成	<ul style="list-style-type: none">IEEE802.1x対応APと無線LANカードRADIUSサーバ(認証を行う場合)	<ul style="list-style-type: none">通常のAP、無線LANカードVPN装置
性能上の考慮点	<ul style="list-style-type: none">WEPキー変更時の認証アクセスのみなので1台で多くの認証が必要(RADIUS)	<ul style="list-style-type: none">全ての通信がVPN装置で暗号・復号処理されるためボトルネックとなりやすい
ベンダーの構築経験ノウハウ	<ul style="list-style-type: none">経験ノウハウ・レベルは非常に浅い	<ul style="list-style-type: none">リモートアクセスやインターネットVPNソリューションとして多数の構築経験あり

3) 企業内無線LAN構築におけるセキュリティ面での課題

現在無線LANを検討するうえで最も大きな課題となっているのがセキュリティである。セキュリティというテーマそのものが社会的に大きくクロ-ズアップされていることもあるが、最近特に無線LANにおけるセキュリティの脆弱性が指摘されることが多くなった。

有線LANと比較して無線LANが特徴的なのは、その物理的な性質上、常に盗聴や不正アクセスの危険にさらされているということである。したがって、無線LANクライアントからAPへのアクセスの可否を規制する認証機能と、ネットワークを流れるデータそのものの暗号化機能という2つの技術的対策を講じなければならない。認証機能と暗号化機能(秘匿)の両方を実現する方法はあるが、コストや設計時点での工数との兼ね合いで実装手段を検討すべきである。場合によっては要件そのものの再確認に立ち返る必要性もある。

(1) 無線LANのセキュリティ・リスク

通信の漏洩、盗聴

- ・ 電波の届く範囲であれば、建物の外からでもAPとクライアント間の通信が盗聴される危険がある。また、電波の盗聴はその事実が発覚しにくく、盗聴された情報が不正に利用されることを未然に防止することは困難である。

AP 経由の不正アクセス

- ・ ファイアウォールで守られた社内LANは、一般的にはセキュリティが不十分である。何らかの手段により一旦APに接続できると、社内LANを経由した不正アクセスが広がる危険性がある。

なりすましAP

- ・ 正規のAPの近くに設置された「なりすましAP」にクライアントが接続すると、認証画面から入力されるユ-ザID およびパスワードは容易に盗まれる危険性がある。

クライアントへの不正アクセス

- ・ 無線LANカードを装着したクライアントPCは、セキュリティが十分でない場合も多く、不正アクセスされる危険性がある。不正アクセスしたPCを踏み台にして社内LANが攻撃される危険性もある。

業務妨害

- ・ APとクライアント間の通信を、干渉やDos(サービス妨害)の意図で妨害される危険性がある。
- ・ 建物の外からの妨害も可能である。

社内LAN を踏み台とした外部サーバへのアクセス

- ・ 社内LANおよびインタ-ネットへの接続が踏み台にされることもありうる。外部サーバが被害を蒙れば、損害賠償請求される場合もある。

不正AP からの情報漏洩

- ・ 社員のみならず、施設内にアクセスできる部外者によって勝手に設置されたAPから、企業情報が漏洩してしまう危険性がある。

(2) 基礎技術での限界

前述で説明したように、セキュリティに関する基礎技術要素としては、下記の3つの方法がある。

ESS-ID (無線LANクライアントとAP間の相互認証機能のためのID)

MACアドレスフィルタリング (製品ごとに割り当てられたユニークな番号で通信相手を制限)

WEPキー (無線LAN クライアントとAP 間の通信の暗号化)

いずれも基本的なレベルでの認証と暗号化機能であり、企業システムとしての無線LAN システムとしては不十分である。

ESS-IDにより、このID を知っているユーザからのアクセスのみを許可しESS-IDを知らない第三者が容易にアクセスしてくるのを防ぐことができる。ESS-IDで行えるセキュリティ対策はこのレベルであり、ESS-IDの設定すら施していないAP がいまだに非常に多い。

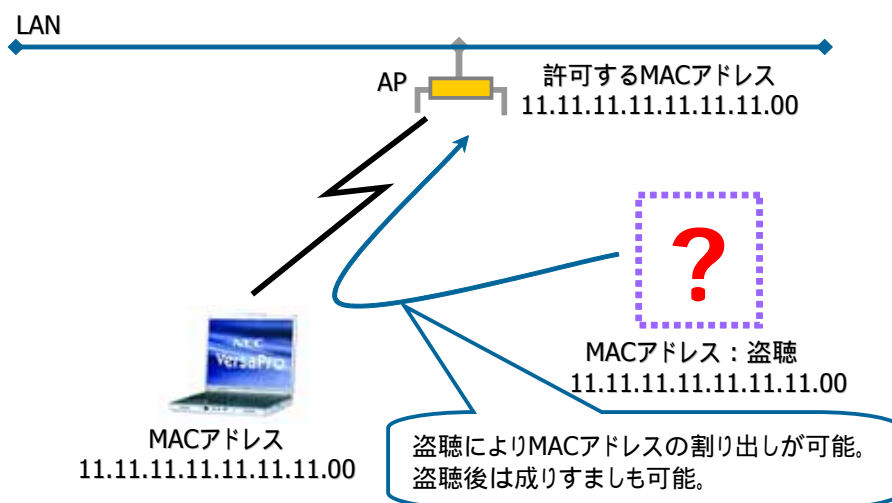
また、ESS-IDはAPがブロードキャストしているためAP付属のユーティリティソフトで判別が可能であり、さらにESS-ID隠蔽機能やESS-IDステルス機能などによる秘匿も電波が盗聴されれば意味をなさない。ESS-ID のみでは実質的なセキュリティ対策にはならない。

MACアドレスフィルタリングもいくつかの欠点を抱えている。すべてのAPに対してどのクライアントとの接続を許可するかをAPに登録する必要があり、クライアントの利用状況にあわせて都度、APのMACアドレス情報を更新しなければならないため、運用上、負荷がかかる。

また、無線LANクライアントからAPに対してアクセスを試みる際のMAC アドレス情報は暗号化されておらず、漏洩・盗聴に対しては無防備である。さらに詐称の問題もある。APに登録された有効なMAC アドレスを詐称してアクセスを試みてきた場合、AP側では詐称を判断する機能を持っていない。

このことは有効な無線LAN カードが盗まれてしまった場合にも当てはまる。つまり、権限のある個人がアクセスをしてきているのかどうかまではわからない。登録されたMAC アドレスを何らかの方法で知られてしまった段階でセキュリティ機能をほとんど果たせなくなる

図表II-17 : MACアドレスフィルタリングの脆弱性



次にWEPキーであるが、解読ツールがインターネットで公開されているなど暗号化としては脆弱であることが弱点である。さらに、同一のAPに接続する端末間でWEPキーが共通しているため暗号が解読された場合の影響範囲が広い。

図表II-18：インターネット上で公開されているWEPキー解読ツール

ツール名	URL
Air Snort	http://airsnort.shmoo.com/
WEPCrack	http://WEPcrack.sourceforge.net/
bad-airtools	http://www.dachb0den.com/projects/bsd-airtools.html/

以上述べたように、ESS-IDとMAC アドレスによって確保できるセキュリティのレベルは低い。また、WEPキ - も解読される危険性がある。業務システムなど高いセキュリティレベルが求められる場合はこれらの基礎技術に加え、より強固な手段をとる必要がある

(3) より高度なセキュリティ技術とその限界

基礎技術による機能の欠点を補うためには、認証用サ - バを立てたユ - ザ認証(IEEE802.1x準拠)の仕組みやWEPキーの脆弱性を補う新しい暗号化方式AES を採用するなどのほか、VPN(Virtual Private Network)を構築することでセキュリティの強化を図る方法もある。しかし、これらについてもまだ以下のような問題点がある。

まず動的なWEPキ - であるが、無線LAN機器メ - カ各社が独自に対応を開始したこともあり、現在のところ標準は確立されておらず製品間の互換性保証がない。IEEE802.11iで策定しているTKIP(Temporal Key Integrity Protocol)は、すでに一部のメ - カ - がサポ - トを表明しているものの、WEPの後継規格として定着には至っていない。このことは、AESについても言える。AESは、IEEE802.11a に対応製品が発売されているが、IEEE802.11bではまだ一部チップメ - カ - が対応を発表している段階である。今後の対応製品の拡大が期待される。IEEE802.11iやWPAも、まだ製品の登場までには時間が必要である。

IEEE802.1x準拠で認証サ - バ(RADIUSサ - バ)を別途立てる場合、コスト面や運用面で負担が増加してしまう。従って、不正アクセスに対する対策を大幅に強化するのであれば、コストとの釣り合いで中規模以上のオフィス環境に限定した導入形態となる。

セキュリティ面の課題を解決するためにVPNでセキュリティを確保するという手段が有効であるが、この場合にはVPN装置の処理能力に性能劣化が大きいので、十分な処理能力を持つVPN 装置を使うことが重要である。

企業向け無線システムや一般通信サービス(公衆網含む)向けシステムの導入にあたっては、IEEE802.1x準拠のEAP(Extensible Authentication Protocol)とRADIUSサ - バを組み合わせ、これを企業内サ - バとVPN 接続するという方法がお奨めであるが、コストに見合っているのか判断が必要である。

4) 企業内無線LANにおけるセキュリティ構築

セキュリティ面の不安がなく企業システムとして無線LANを導入する場合、どのようなシステム構成をとればいいのか。ESS-ID、MACアドレスフィルタリング、WEPではセキュリティ手段としては脆弱であり、これら以上のセキュリティ強化策をとり入れた構築が必要である。企業システムとして実用に耐え得るセキュリティは、認証と暗号化によりユーザ認証耐性、暗号化耐性、パスワードクラック耐性から、高い、中位の2つのレベルが考えられる。簡易レベルも挙げられるが、企業向けとしては相応しくない。

構築事例や実証実験などの結果を踏まえ、NRIグループでは、この2つのセキュリティレベルにしたがって、2つの無線LANシステムの構成を基本に設計することを推奨している。暗号化機能と認証機能の両面から、企業システムとして必要なセキュリティ強度を決めることで、いずれの構成タイプを実装するのがよいか概ね決定される。

図表II-19：セキュリティと強度

セキュリティレベル	ユーザ認証耐性	暗号解読耐性	パスワードクラック耐性	主な利用シーン
高度レベル	(満たしている)	(満たしている)	(満たしている)	機密度の高い情報を社員(相当)がアクセスする環境
基本レベル	(満たしている)	(満たしている)	(部分的に満たしている)	社員や来訪者がアクセスする環境
簡易レベル	(満たしている)	× (満たしていない)	× (満たしていない)	オープン・スペースで、不特定多数が利用する環境としてのセキュリティレベルであり、企業システムとしては適さない

認証には、APへの不正アクセス防止機能のほか、電波漏洩防止機能やAP設定、APからの電波出力調整も含まれる。

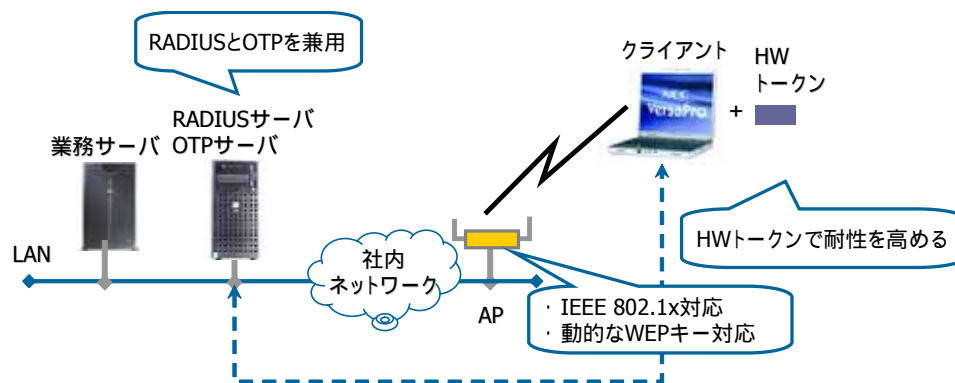
次に、各セキュリティレベル別のシステム構成パターンについて説明する。

(1) 高度セキュリティ・パターン：セキュリティ・レベルが非常に高いレベル

利用者としては、ユーザ登録に加え、ハードウェア・トークン等のユーザ・パスワード以外の認証情報を持っている人を想定したセキュリティ・レベルである。IEEE802.1x(認証)、動的なWEPキー(暗号化)ともセキュリティ強度の高いソリューションである上に、ワンタイムパスワード(OTP)等を活用することによって、さらにパスワード以外の認証情報を付加している。RC4はWEPでも利用されていてすでに脆弱性が指摘されている暗号方式でセキュリティ強度は高いとは言えないので、DESの次期バージョンとして期待されているAES方式が望ましい(AESはいまだに解読されていないため実装できれば非常にセキュリティ強度は上がるが、現在のところAES対応の製品はIEEE802.11aで一部発売が始まったばかりである)。

動的なWEPキーに替わるTKIPの標準化が進み実装ができれば、OTP以外の組み合わせの部分は2002年10月に発表されたWPAに近く、望ましい実装手段と考えられる。こちら、一部チップメーカーがWPA対応を発表したものの製品が出揃うのは2003年下期以降と見られる。

図表II-20：高度セキュリティ・パターンの構成イメージ



セキュリティ方式

	基本形	高度化
認証	-	IEEE 802.1x + ワンタイムパスワード
暗号化	ESS-ID RC4 + WEP	AESまたは独自暗号方式 + 動的なWEPキー

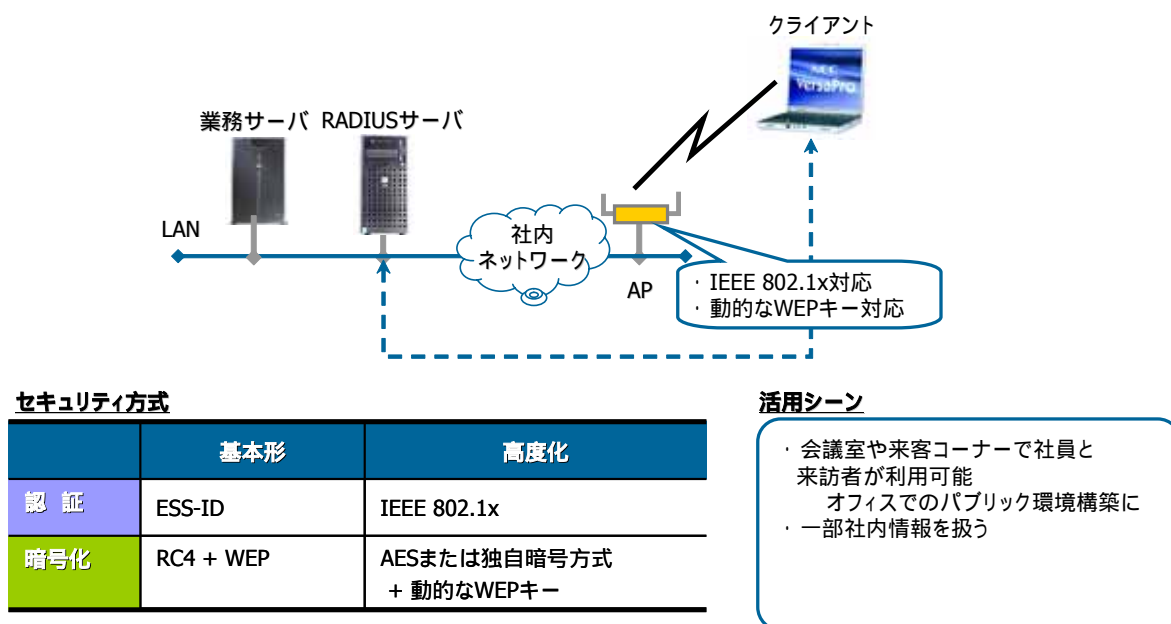
活用シーン

- ・ オフィスや店舗で社員のみが利用可能とする
- ・ 顧客情報等機密性の高い情報を扱う

(2) 基本セキュリティ・パターン：セキュリティ・レベルが基本レベル

利用者としては、ユ - ザ登録のみされている人を想定したセキュリティ・レベルである。セキュリティが非常に高い場合の構成(高度セキュリティ・パター - ン)からOTPを除いた構成である。今後しばらくの間企業内LAN構築で最も採用されるケ - スが多いと予想される。セキュリティレベルが非常に高い場合と同じく、RADIUSサ - バが一元的に認証機能を担うことでユ - ザ追加や変更等のたびに対象のクライアントごとに設定を変更する必要がないため、AP数が数十台以上の規模であれば管理面でも効率化を図ることができる。

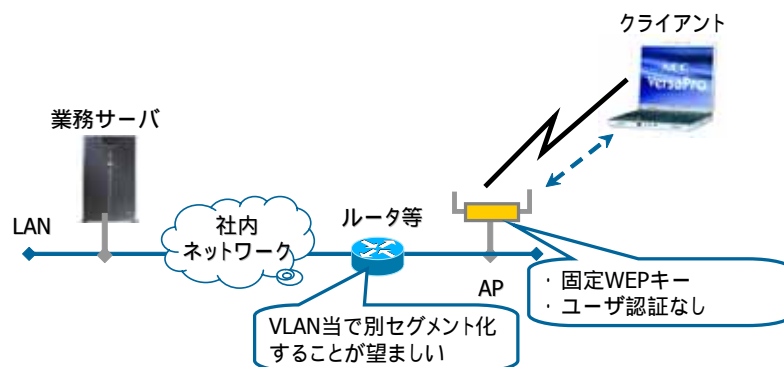
図表II-21：基本セキュリティ・パターンの構成イメージ



(3) 簡易セキュリティ・パターン：セキュリティ・レベルが簡易レベル

ユ - ザは接続情報を知っている人であり、ユ - ザ認証を必要としないセキュリティ・レベルである。基本的なセキュリティ対策のみを行った場合の構成である。現実的には導入されている無線LANの多くが上記のようなパターンである。認証、暗号化ともすでに脆弱性が周知となっており、社内情報を扱う場合セキュリティ・レベルとしては不十分である。しかし導入するAP/クライアント数によっては、定期的にWEPキ - の変更を行ったり、管理者以外にはESS-ID やWEPの内容を通知しない等、運用でカバーできるケースも考えられる。

図表II-22：簡易セキュリティ・パターンの構成イメージ



セキュリティ方式

	基本形	高度化
認証	ESS-ID、MAC	-
暗号化	RC4 + WEP	-

活用シーン

- ・ホットスポットのように誰でも利用可能にする環境。
- ・社内情報は一切扱わない

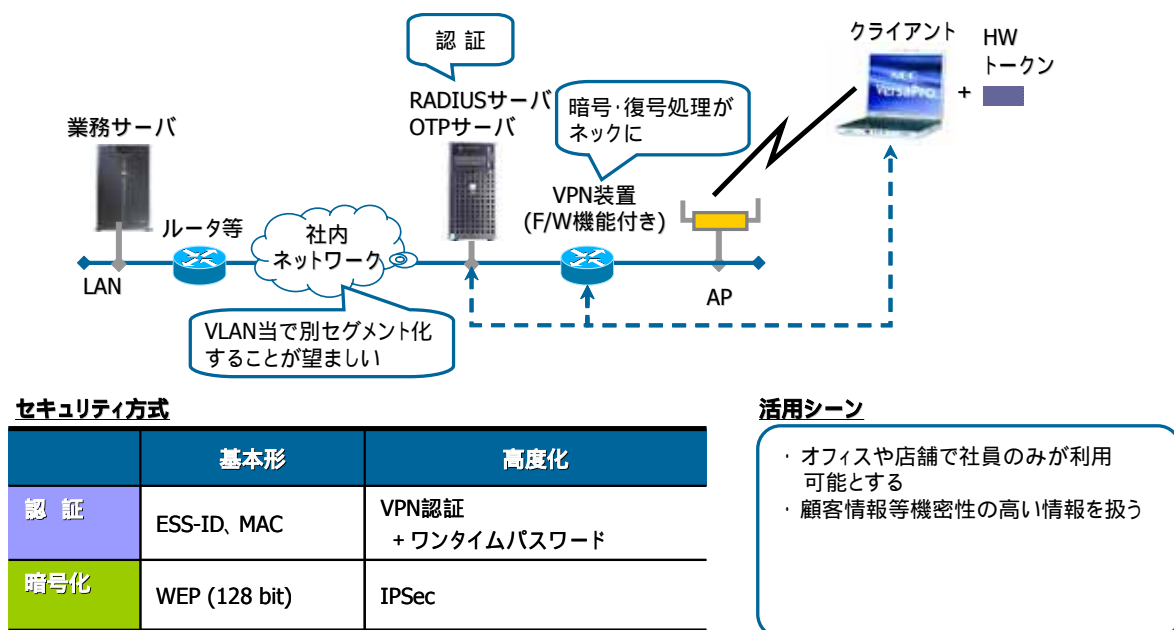
(4) VPNによるセキュリティ・パターン：セキュリティ・レベルが高度レベル

上記パターンは、あくまでも無線LAN単独でセキュリティ要件を満たす構成であるが、上述したように、標準化や製品化がニーズに追いついていないという状況であり、リモートアクセスやWANで既に広く利用されているVPNを活用してセキュリティ要件を満足するシステム構成とするケースも多い。

無線LANシステムは信頼できないネットワークと位置付け、無線LANと企業内の基幹ネットワークの間をファイアウォール技術で守りVPN認証やIPSecにOTPを追加した構成とすることで、高度セキュリティパターンと同様に非常に高いセキュリティ・レベルを実現できる。現段階では値段が高いIEEE802.1xやTKIP対応等のAPや無線LANカードを用意する必要がないという利点がある。しかも、VPN自体が無線LAN固有のセキュリティ技術に比べてすでに多くの実績を積んでいる点でも評価できる。

しかし、ここでも注意しなければならない点がいくつかある。一つはVPN装置における暗号化・復号化処理のボトルネックである(AP/クライアントの数にもよる)。またVPN装置の設置位置についても注意しなければならない。基本的にAPそのものはWEPでしか守られていないため、万が一WEPが破られた場合、APのセグメントに存在するPCやサーバにアクセスされる恐れがある。したがって、APを別セグメント化する等の対策が必要になる。

図表II-23：VPNによる高度セキュリティ・パターンの構成イメージ



VPNを利用する場合にも、ユーザ認証方式次第ではセキュリティ・レベルを変えることができる。高いセキュリティ・レベルであれば、VPNセッション暗号化とワンタイムパスワードなどの組み合わせでユーザ認証を行い、それより低いセキュリティ・レベルであればワンタイムパスワードは利用せずに、ユーザ認証後にVPNセッションを確立する方式をとることになる。

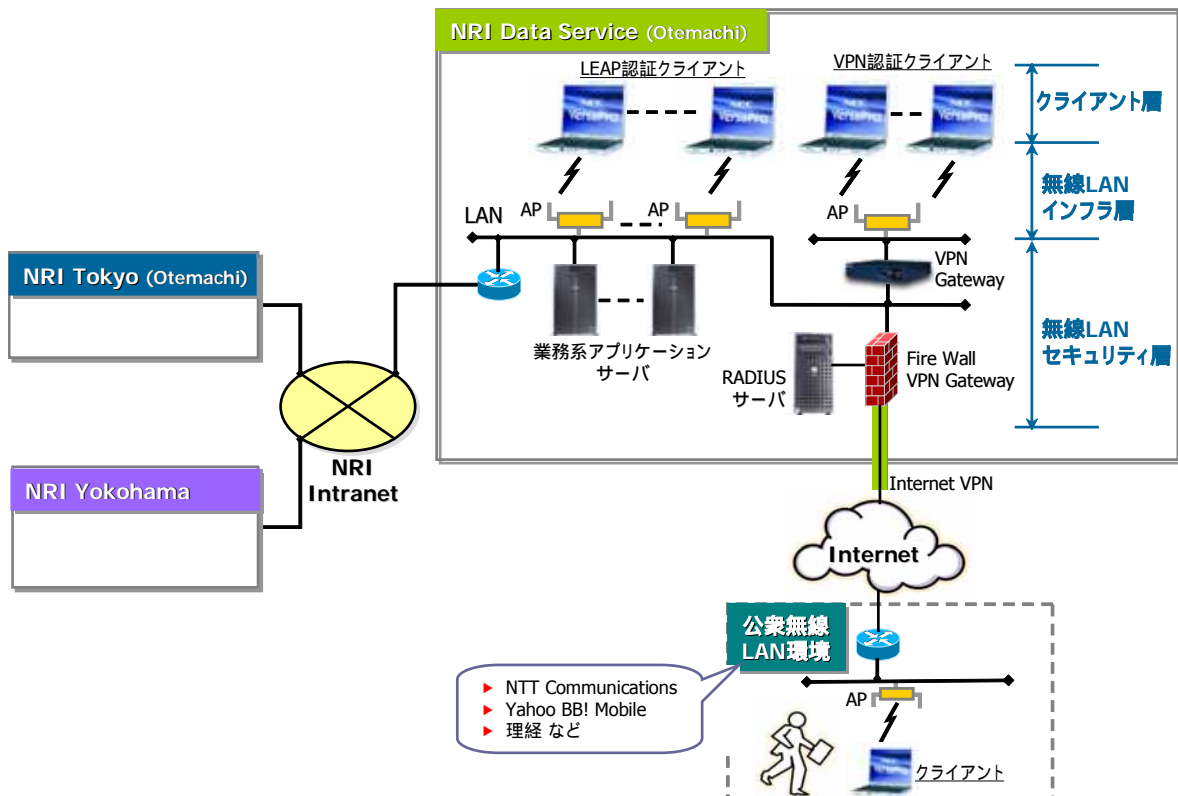
III システム構成概要

1. ハードウェア構成

今回のベンチマーク・テストは、試験的な環境ではなく、NRIデータサービス社内で実際利用されている実環境を用いて行い、図表III-1に示す実験環境構成で実施した。また今回の実験環境は、「クライアント層(Note型PC)」、「無線LANインフラ層(無線LANアクセスポイント)」、そして「無線LANセキュリティ層(VPNゲートウェイ、RADIUSサーバ)」の3つの層から構成され、ベンチマークの対象はクライアント層のハードウェアのみである。

今回の実験のクライアント層には、日本電気(株)殿(以下、「NEC」とする)の協力により、NEC社製のNote型PC製品(Centrino PCと非Centrino PC)を使用した。

図表III-1：実験環境構成 (全体イメージ)



今回のベンチマーク・テストは、NRIデータサービスにおける実オフィス環境で実施した。

今回の実験で使用したハードウェアのスペックについて、図表III-2に示す。

図表III-2：ハードウェア・スペックの概要

Hardware		台数	CPU	DRAM	
クライアント層 (Note型PC)	Centrino	NEC VersaPro VA13F/VH	2台	Intel Pentium-M Processor 1.3GHz	512MB
	Pentium III	NEC VersaPro VA10J/VH	2台	Mobile Intel Pentium III Processor-M 1.0GHz	512MB
無線LAN インフラ層	無線LAN アクセス ポイント	Cisco Aironet AP350	4台	-	
		Cisco Aironet AP1200	1台	-	
無線LAN セキュリティ層	RADUISサーバ IBM xSeries 260		1台	Intel Pentium III 1.2GHz	512MB
	業務系サーバ (HTTP/FTP) DELL GX150		3台	Intel Pentium III 900MHz	256MB
	VPN機器 Cisco VPN3000		1台	-	

2. ソフトウェア構成

今回の実験で使用したソフトウェアについて、図表III-3に示す。

図表III-3：ソフトウェア一覧

Hardware		OS	Application
クライアント	NEC VersaPro VA13F/VH	Microsoft Windows XP	Microsoft Web Application Stress Tool 1.1
	NEC VersaPro VA10J/VH	Microsoft Windows XP	Microsoft Web Application Stress Tool 1.1
無線LAN インフラ層	Cisco Aironet AP350	Version 11.21	-
	Cisco Aironet AP1200	Version 11.54	-
無線LAN セキュリティ層	RADUISサーバ IBM xSeries 260	Microsoft Windows 2000 SP3	Cisco ACS
	業務系サーバ (HTTP/FTP) DELL GX150	Microsoft Windows 2000 SP1	WAR FTP 1.65 Apache 2.0

IV 実験内容とその結果

1. 実験対象項目の概要

本実証実験における実験対象項目を下記に示す。これら項目は、無線LAN設計時におけるプレ・テストで評価する必要のある項目である。

図表IV-1：本実証実験における実験対象項目

実験対象項目		実験内容
1 無線 LAN の実用性		
1-1	ネットワーク性能	1) 電波伝送距離 <ul style="list-style-type: none"> a. 障害物なし b. 障害物あり c. AP の送信出力調整 2) 電波の指向性 (参考) オフィス環境における電波強度分布 3) 同時接続台数とスループット性能
1-2	アプリケーション利用時における性能 (コンテンツによるスループットの変化 など)	1) Ping 2) FTP 3) Streaming Data 4) 業務系アプリケーション (オフィス系アプリケーション)
2 移動時の有用性：Mobility 性能		
2-1	ローミング性能	1) 移動による再設定有無 2) 再接続時間有無
2-2	バッテリー稼働性能	・バッテリーを用いた際の連続利用可能時間
2-3	公衆無線 LAN 環境からの接続	・公衆無線 LAN サービス - Internet VPN 経由による企業内システムへの接続
3 製品間の相互接続性		
3-1	AP = Cisco 製	1) Cisco 製 AP - Cisco 製カード接続 2) Cisco 製 AP - 非 Cisco 製カード接続 3) Cisco 製 AP - Centrino 接続
3-2	AP = 非 Cisco 製	1) 非 Cisco 製 AP - Cisco 製カード接続 2) 非 Cisco 製 AP - Centrino 接続
4 電波干渉性		
	電波干渉性	チャンネル間隔—スループットの関係 AP 間隔—スループットの関係 電波を発生する機器の影響

2. 実験結果

1) 無線LANの実用性

- ・ 無線LANは有線LANに比べ、電波の到達距離や指向性など、無線特有の伝送性能を考慮したうえで設計する必要がある。本節では、無線LANに関する特有性を明らかにし、どのレベルであればネットワークとして実用的であるかについて記述する。

(1) ネットワーク伝送性能

電波伝送性能

電波の指向性

同時接続台数とスループット性能

(2) アプリケーション利用時におけるネットワーク伝送性能

コンテンツサイズとスループット性能

電波状況の変化時(= 電波劣化状況時)におけるアプリケーションの動作

(1) ネットワーク伝送性能

電波伝送性能

- ・ 実オフィス環境において、無線LAN(IEEE802.11b)の電波伝送距離がどの程度であるのか、その実態について明らかにする。
- ・ APとクライアントとの距離が電波強度とクオリティに及ぼす影響について。下記のパターン。
 - a. 「障害物なし」のパターン
 - b. 「障害物あり」パターン
 - c. 「APからの電波出力を変化させた」パターン

a. 「障害物なし」のパターン

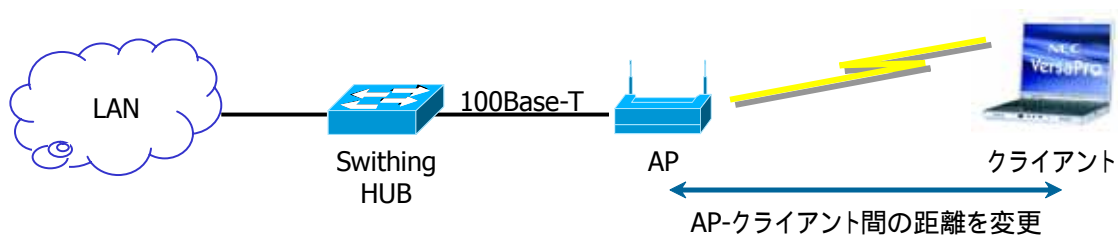
【実験内容】

- ・ APとクライアントとの距離による、「電波強度」と「クオリティ」の変化を測定
- ・ 電波伝送距離と電波強度 / クオリティの関係を明らかにする

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 変化 : 1m, 5m, 10m, 20m, 30m
障害物	・ なし
測定時間	・ 60秒間

図表 IV-2 : 実験構成図 (障害物無し)

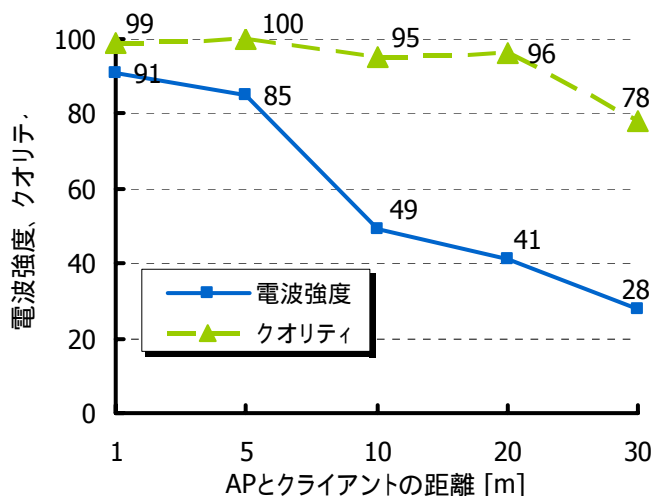


【実験結果】

- ・ 電波強度は距離とともに減衰する傾向にある。5mで電波強度85程度、10mで同50弱、20mで同40程度と減少していく。
- ・ ネットワークとしての実用性を示す「クオリティ」で見ると、設計基準として90以上と設定すると、20m以内となるように利用環境を整備する必要があることが分かる。
- ・ 30m以上は離れた環境でのクオリティの確保は厳しいと見られる。

図表 IV-3 : 電波伝送性能実験結果 (障害物無し)

- AP - クライアント間の距離と電波強度 / クオリティの関係



b. 「障害物あり」のパターン

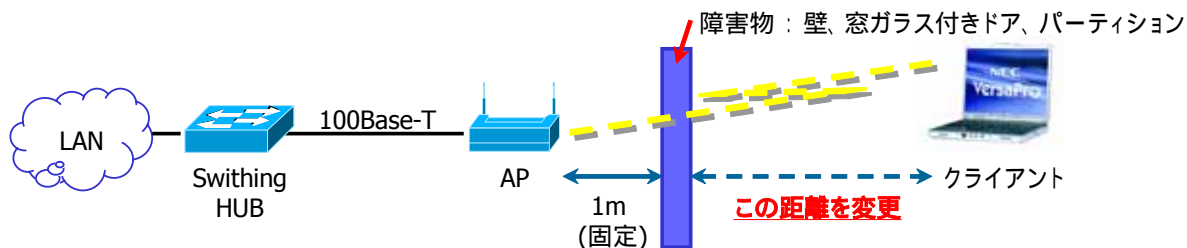
【実験内容】

- ・ APとクライアントとの間に障害物がある環境において、APとクライアント間の距離と電波強度/クオリティと同じ項目を測定
- ・ 障害物がある環境下での、電波伝送距離と電波強度/クオリティの関係を明らかにする

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 変化 : 1m, 4m (AP-障害物の距離は1mで固定)
障害物	・ 3パターン - 壁 (鉄筋コンクリート製) - 窓ガラス付きドア - パーティション (可動式仕切り)
測定時間	・ 60秒間

図表 IV-4 : 実験構成図 (障害物あり)



図表 IV-5 : 電波伝送実験での障害物



a. 壁 (鉄筋コンクリート)



b. 窓ガラス付きドア



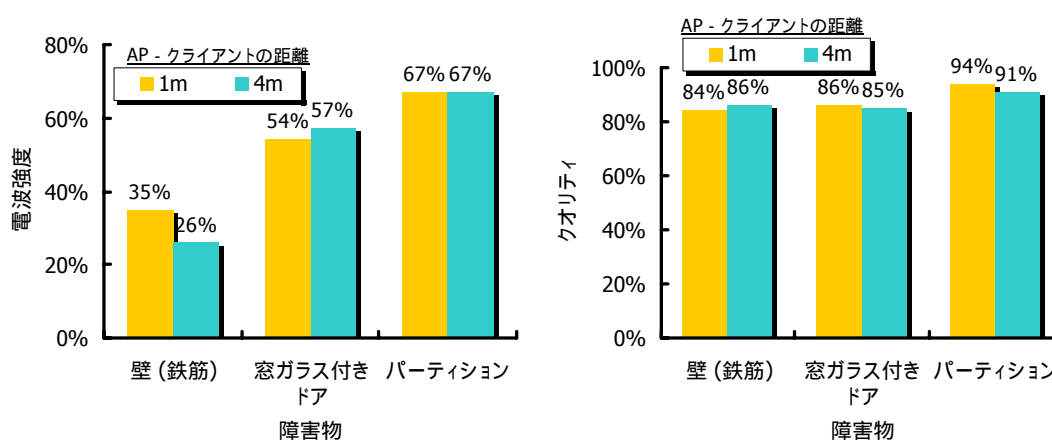
c. パーティション

【実験結果】

- ・ 壁、窓ガラス付きドア、パーティションといったオフィス環境内の障害物は、AP - クライアント間の距離が1~4m程度であれば、電波強度は弱くなるものの、クオリティ・レベルでは実質的に利用できる状況にある。APと障害物の距離が近い場合(APと壁の距離が1m程度)、通常のオフィスビルの壁程度であれば、見た目では大丈夫に見えても、壁を通じて電波が漏洩する可能性が高いことが分かる。
- ・ 外部への電波漏洩を防ぐためには、十分距離を確保してAPを設置する必要がある。

図表 IV-6 : 電波伝送性能実験結果 (障害物あり)

- AP - クライアント間の距離と電波強度 / クオリティの関係 -



c. 「APからの電波出力を変化」のパターン

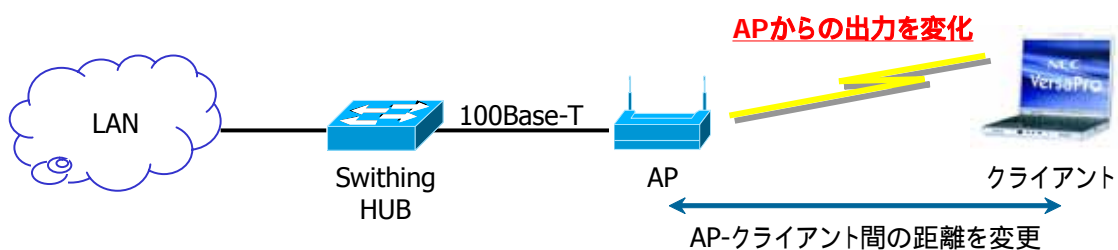
【実験内容】

- ・ APからの電波出力を変えながら、APとクライアント間と電波強度/クオリティの関係を測定。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 変化 : 1m, 5m, 10m, 20m, 30m
障害物	・ なし
測定時間	・ 60秒間

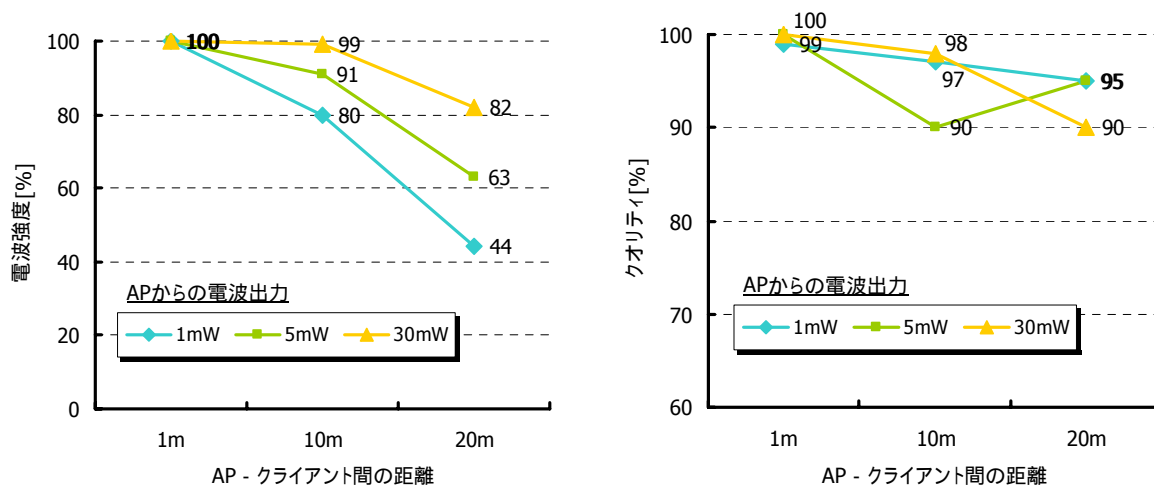
図表 IV-7 : 実験構成図 (APからの出力を変化)



【実験結果】

- ・ 電波出力を高めると、電波強度は向上。
- ・ クォリティに関しては、電波出力を高くすると全体的に向上するが、不安定な状況になる。輻射の影響が考えられる。

図表 IV-8 : AP-クライアント間距離と電波強度/クォリティの関係 (APからの電波出力を変化)




電波の指向性

【実験内容】

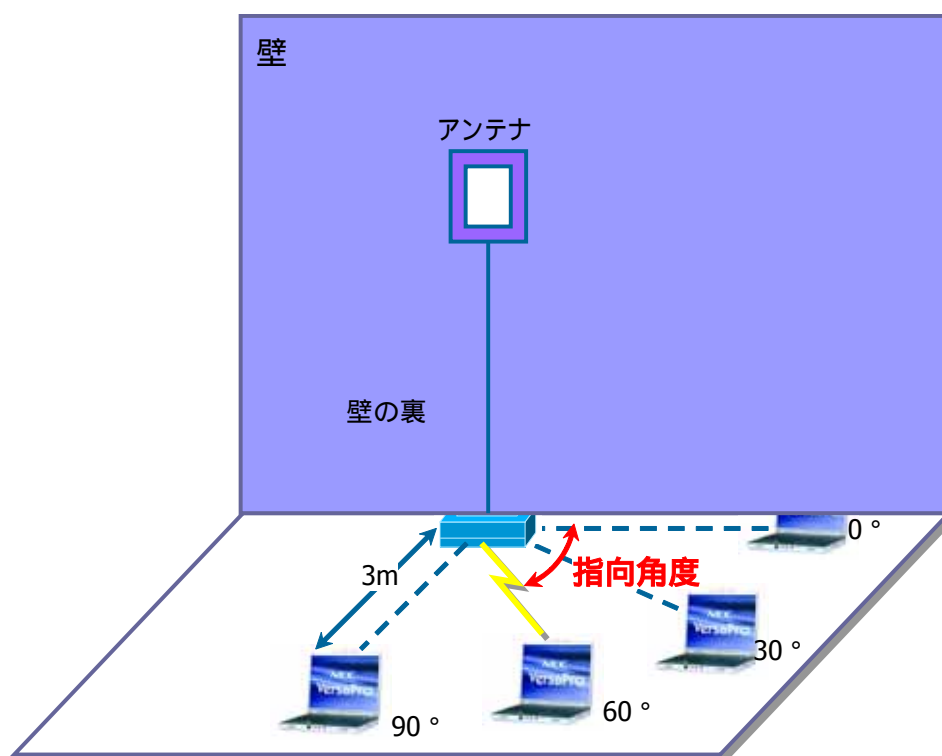
- ・ アンテナからの電波指向性による電波強度の変化について測定。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 固定 : 3m
障害物	・ なし
測定時間	・ 60秒間
使用アンテナ	・ AIR - ANT1729



図表 IV-9 : 実験構成図

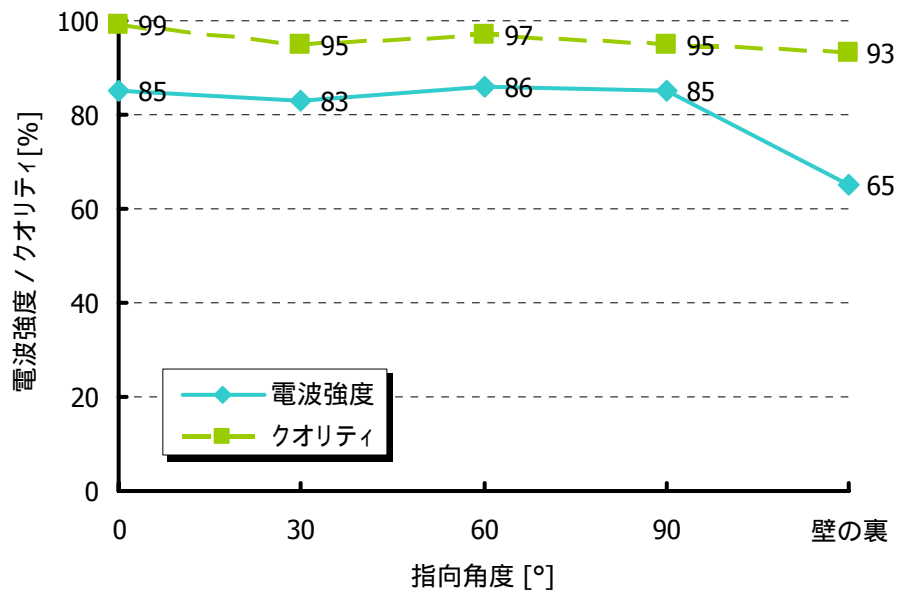


指向角度 0°、30°、60°、90° 及び壁の裏について電波強度を測定

【実験結果】

- ・ アンテナを使用し、AP - クライアント間の距離が3m程度の場合、電波指向性による電波出力およびクオリティの変化はほとんど見られない。

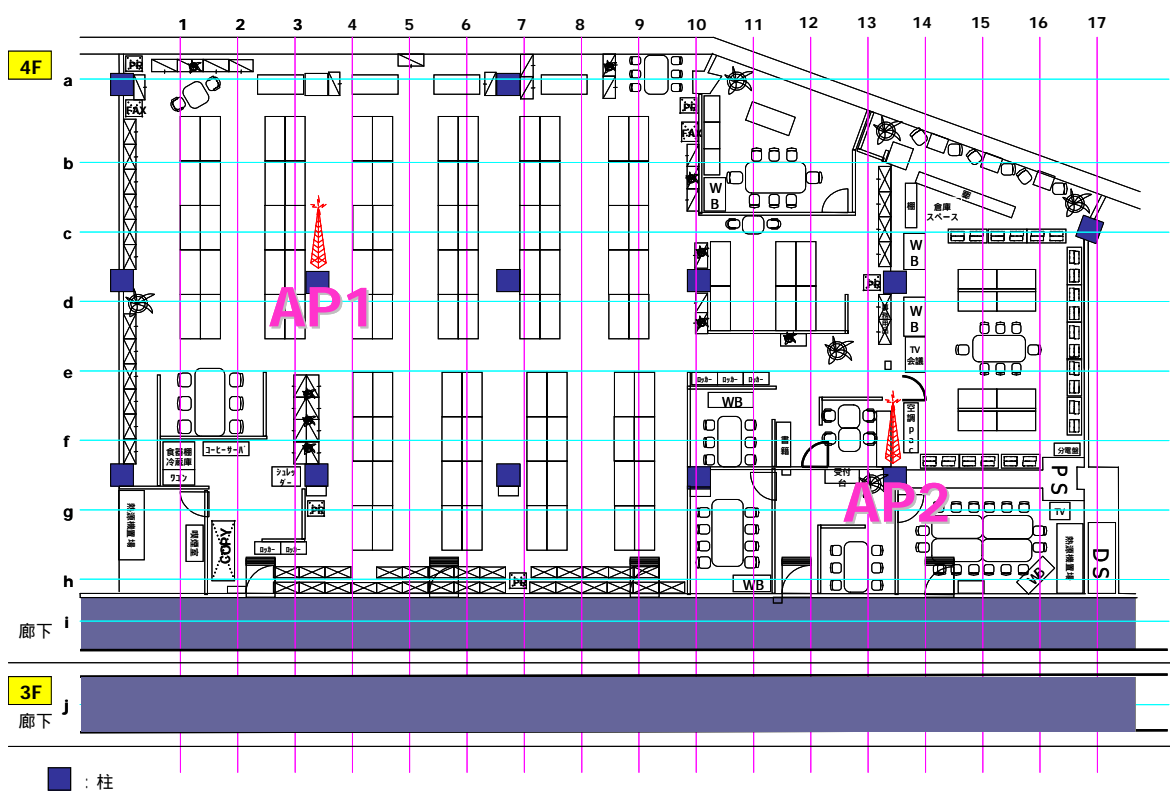
図表 IV-10 : 電波指向性に関する実験結果



(参考) オフィス環境内における電波強度分布の状況

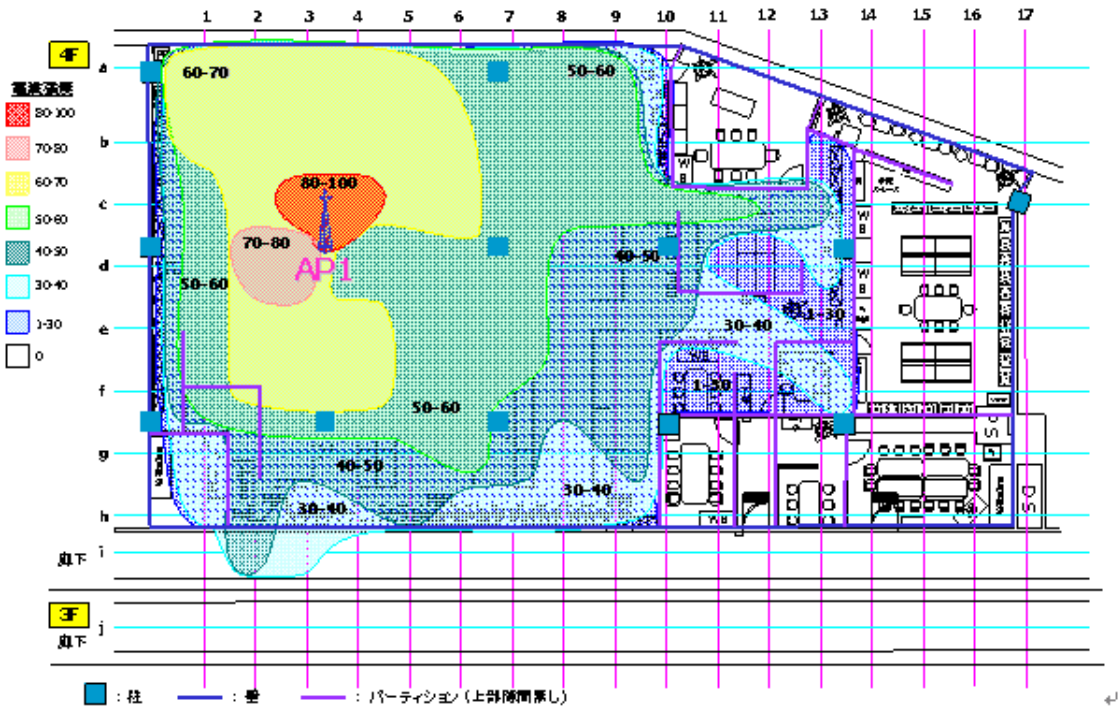
- ・ 今回実証実験を行った実オフィス環境において、2箇所に置かれたAPからの電波強度分布状況がどのようになっているか、その測定結果について示す。
- ・ この結果から分かるように、通常のオフィス環境程度の距離であれば、無線LANの電波指向性が及ぼす電波強度への影響は小さいと考えられる。むしろ、APとの距離が5m以上になると、部屋の柱や障害物(パーティションなど)の影響が電波強度に影響し始めることが分かる。

図表 IV-11 : オフィス環境概要図 (実証実験対象)

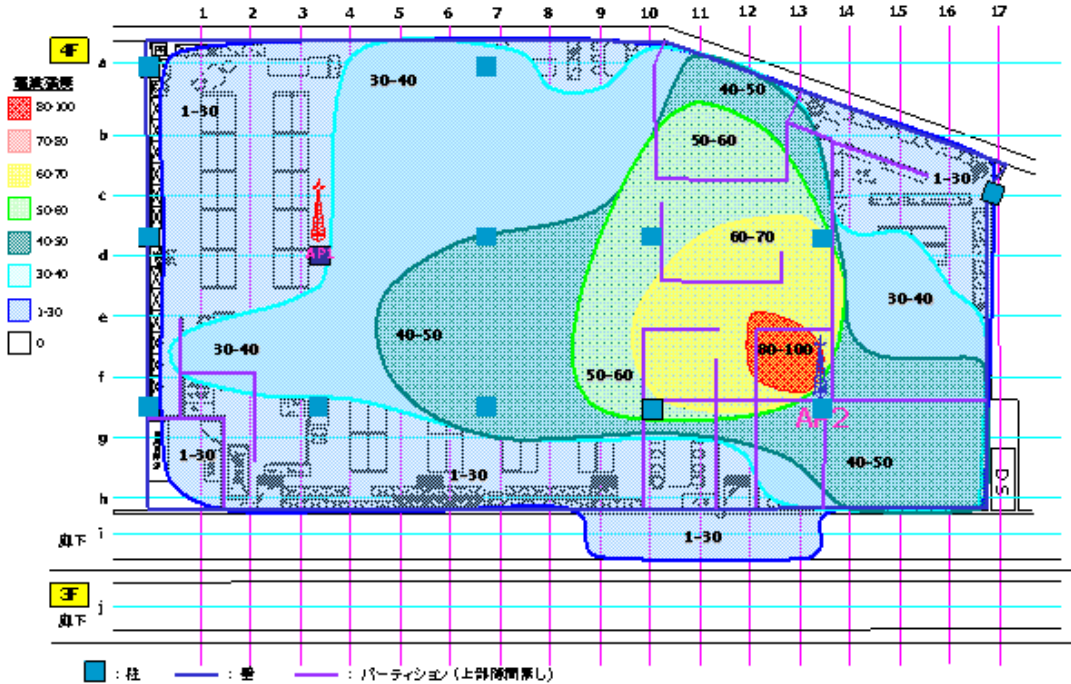


APは2箇所に設置

図表 IV-12 : オフィス環境における電波強度分布図 (AP1のみ)



図表 IV-13 : オフィス環境における電波強度分布図 (AP2のみ)



同時接続台数とスループット性能

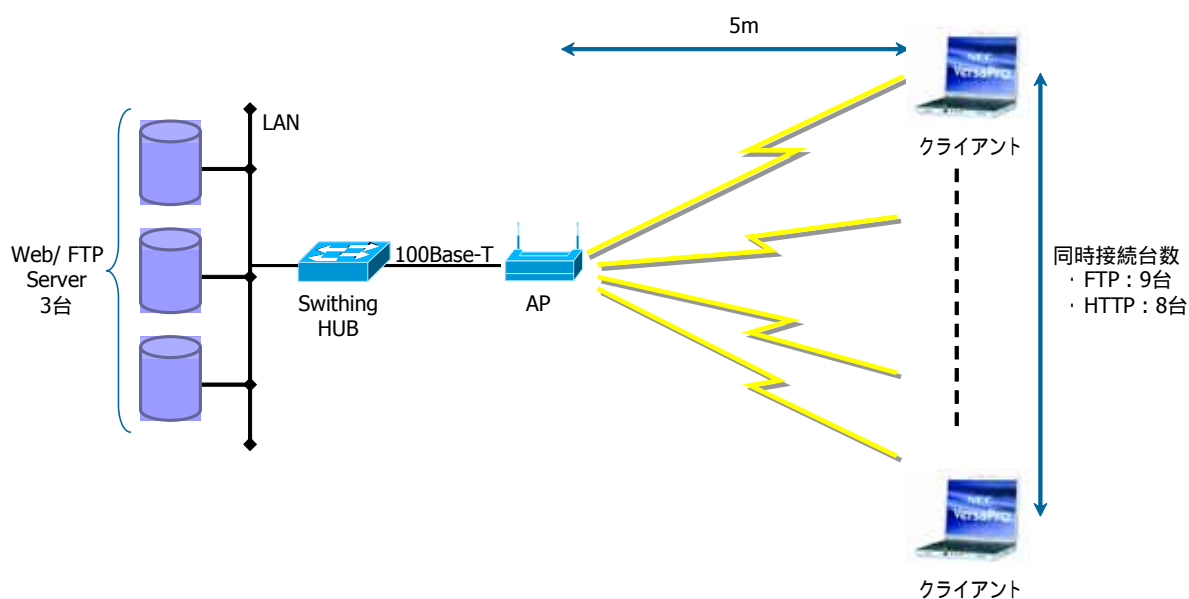
【実験内容】

- ・ 1つのAPに、同時に接続する端末台数を増やすことにより、どの程度スループット(KB/Sec)が変化するののかについて明らかにする。

【実験環境とその構成】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 固定 : 5m
障害物	・ なし
通信方式	・ FTP / HTTP (Web Application Stress Tool使用)
コンテンツサイズ	・ 5MB
最大同時接続台数	・ FTP : 9台, HTTP : 8台
測定時間 / 実験回数	・ コンテンツのダウンロードが終わるまで / 3回

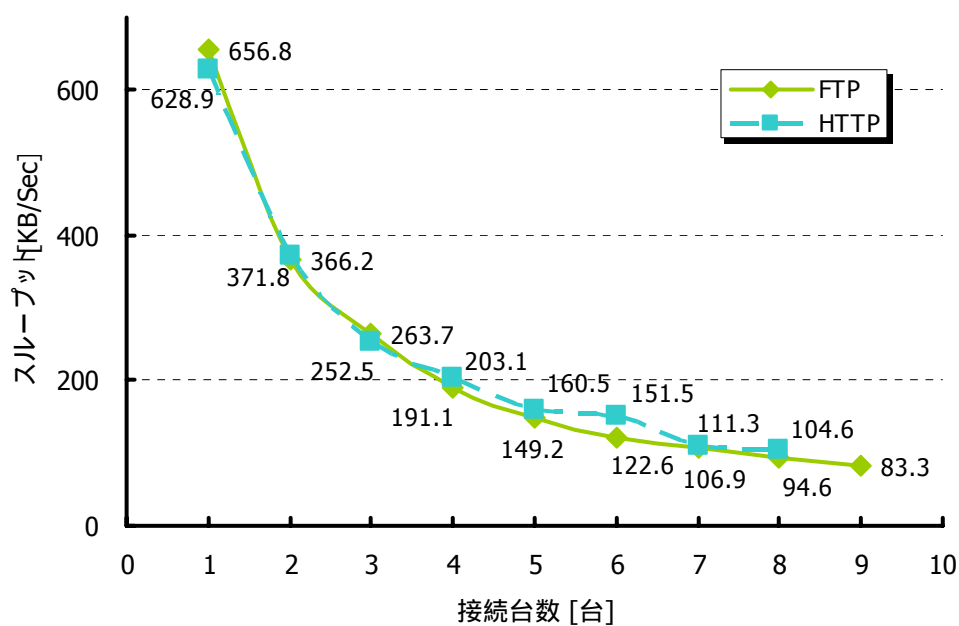
図表 IV-14 : 実験構成図



【実験結果】

- ・ 同時接続台数の増加に伴い、スループットは反比例的に減少傾向が見られる。
- ・ 快適な無線LAN環境を構築するには、利用するアプリケーションが必要とするスループットに基づいて、同時接続台数を設定することが重要である。

図表 IV-15 : 同時接続台数とスループットに関する実験結果 (1台当たりの値)



最大同時接続台数 : FTPでは9台、HTTPでは8台。

(2) アプリケーション利用時におけるネットワーク伝送性能

- 本節では、通常の業務で使用するアプリケーションの利用時において、無線LANのネットワーク伝送性能がどのように変化するかについて明らかにする。その際の「評価項目」及び「検証アプリケーション」を下記に示す。

評価項目	検証アプリケーション
コンテンツサイズとスループット性能	a. ping (ICMP) b. FTP
電波状況の変化時 (= 電波劣化状況時) におけるアプリケーションの動作	c. オフィス系アプリケーション (Microsoft PowerPoint、Microsoft Visio) d. e-mail e. Web f. 動画画像Streaming

コンテンツサイズとスループット性能

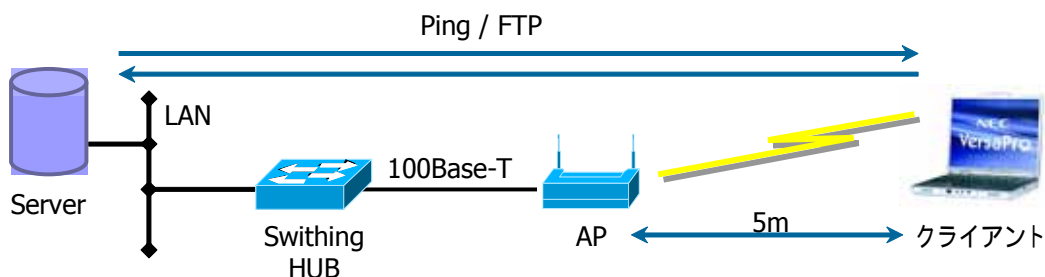
【実験内容】

- 無線LAN環境下におけるpingとFTPについて、コンテンツ・サイズ (= パケット・サイズ) とスループット (= KB/sec) の関係を明らかにする。

【実験環境とその構成】

実験環境	実験スペック
電波出力	<ul style="list-style-type: none"> AP : 1mW / クライアント : 30mW 固定 : 5m なし ICMP(ping) およびFTP ping : 60秒間 / 3回 FTP : コンテンツのダウンロードが終わるまで / 3回
AP - クライアントの距離	
障害物	
通信方式	
測定時間 / 実験回数	

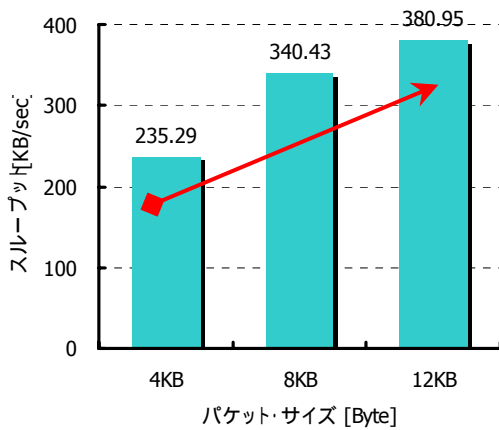
図表 IV-16 : 実験構成図



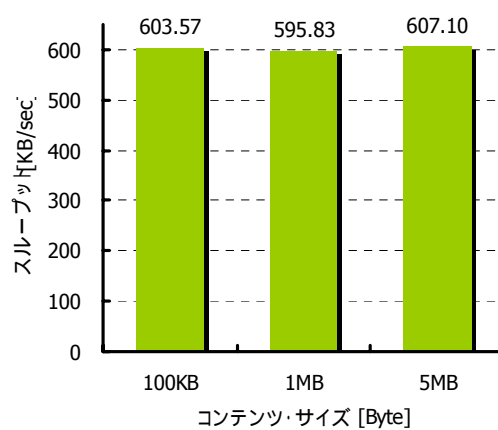
【実験結果】

評価項目	実験結果
a. ping (ICMP)	<ul style="list-style-type: none"> • パケットサイズが大きくなるにつれ、スループットも向上する傾向が見られる。 有線LANと同様の傾向
b. FTP	<ul style="list-style-type: none"> • コンテンツサイズによる伝送性能への影響は、特に見られない。

図表 IV-12 : pingに関する実験結果



図表IV-13 : FTPに関する実験結果



60秒間のスループット量

電波状況の変化時におけるアプリケーションの動作

【実験内容】

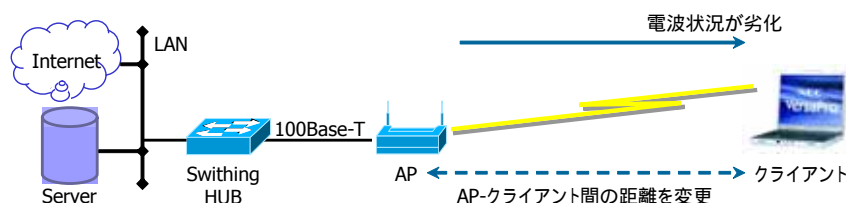
- 電波強度が弱くなるといった電波状況が変化した際において、アプリケーションの利用にどのような影響があるか明らかにする。

【実験環境と構成図】

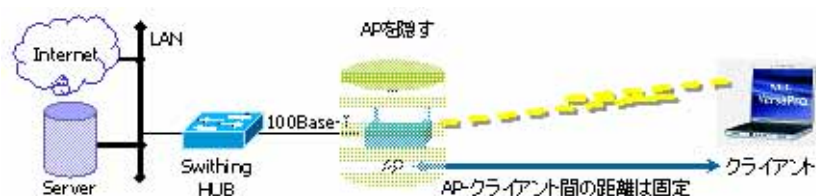
実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 固定 : 5m
障害物	・ なし
検証アプリケーション	c. オフィス系アプリケーション (Microsoft PowerPoint, Microsoft Visio) d. e-mail e. Web f. 動画Streaming
電波障害パターン	・ 電波劣化 : AP - クライアント間の距離を遠くする ・ 電波断続 : APを隠す ・ 電波切断 : APをシャット・ダウン
測定時間 / 実験回数	・ 60秒間 / 3回

図表 IV-19 : 実験構成図 (電波劣化 / 電波断続 / 電波切断)

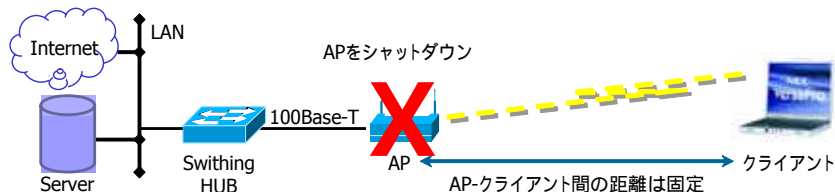
電波劣化



電波断続



電波切断



【実験結果】

評価項目		実験結果
c. オフィス系アプリケーション - Microsoft PowerPoint XP - Microsoft Visio XP	電波劣化	<ul style="list-style-type: none"> PowerPoint、Visioともに、電波が劣化しても、ファイルを開く・保存する動作に変化は見られない。
	電波断続	<ul style="list-style-type: none"> PowerPoint、Visioともに、ファイル開く・保存処理に通常より時間を要する。 但し、通信中に電波が断続しても、ファイルを開く・保存する動作に変化は見られない。
	電波切断	<ul style="list-style-type: none"> PowerPoint及びVisioともに、サーバ上にあるファイルの読み込みそして保存の最中に電波を切断するとエラーになり、処理の実行ができない。 アプリケーションは引き続き利用できる。
d. e-mail - AI-Mail - Microsoft Outlook	電波劣化	<ul style="list-style-type: none"> 電波到達エリア内であれば、AI-Mail、Outlookともに正常にメールの受信が可能。
	電波断続	<ul style="list-style-type: none"> AI-Mail、Outlookともに、メールの受信は可能。但し、通常より時間を要する。
	電波切断	<ul style="list-style-type: none"> アプリケーションにより動作が異なる。 Outlookでは、切断1分後にタイムアウトメッセージがでて、再接続オペレーションが必要。 AI-Mailでは受信中の画面が続く。再接続後も受信画面のまま。再送受信をしようとするとエラーメッセージがでる。
e. Web	電波劣化	<ul style="list-style-type: none"> 電波の劣化によるWebブラウザの動作への影響は見られない。正常に利用可能。
	電波断続	<ul style="list-style-type: none"> 電波が断続すると、Webブラウザの表示はされるものの、表示時間が遅くなる。
	電波切断	<ul style="list-style-type: none"> 電波が切断されると、Webブラウザの表示が中断する(有線LANと同様の動作)。
f. 動画像Streaming - Windows Media Player 8	電波劣化	<ul style="list-style-type: none"> 電波が切断されない限り、電波強度・品質の劣化による影響は見られない。
	電波断続	<ul style="list-style-type: none"> 音声・画像が断続的になる。 Media Playerがエラー「サーバに接続できない」をだすまでは(約10秒)、音声画像とも断続的である。
	電波切断	<ul style="list-style-type: none"> 電波切断後、音声・画像が途絶える。約3分後に、サーバに接続できないので再試行するようメッセージが表示される。 接続オペレーションができない(Media Playerがフリーズ)ため、アプリケーションの再起動が必要。

2) 移動時の有用性

- ・ 無線LANの特徴の一つであるモビリティ性能について評価を行う。
- ・ 本実験では、移動時の有用性に関連する項目として、下記について明らかにした。
 - (1) ローミング性能
 - (2) バッテリー性能：最新モバイルCPU「Centrino」搭載Note型PCのバッテリー性能についても評価
 - (3) Public無線LANからの接続

(1) ローミング性能

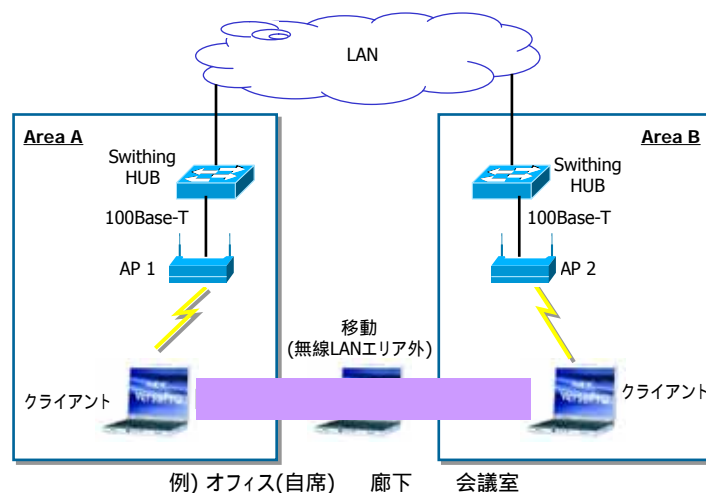
【実験内容】

- ・ 異なる無線LANエリア間を移動した際、継続的にアプリケーションを利用し続けることができるかについて検証する。
- ・ 本実験では、無線LANにローミング性能に関し、「移動による再設定の有無」、「再接続時間の有無」について検証する。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP：1mW / クライアント：30mW
AP - クライアントの距離	・ 変化 / 移動
障害物	・ なし
使用アプリケーション	・ Microsoft Windows Media Player 8.0
実験回数	・ 3回

図表 IV-20 : 実験構成図



通信中に電波が途絶える（クライアントPCを移動させる）

【実験結果】

実験内容	実験結果
1) 移動による再設定の有無	・ 異なるAP間(図表ではAP1とAP2)のSSIDが同じであれば、再設定をすることなく、継続的に利用可能である。 ・ Windows XPを利用する場合、 <u>再接続のためのオペレーション</u> は必要なく、継続的に利用することが可能。また
2) 再接続時間の有無	・ 再接続には1分程度要する

- ・ 同じSSIDを使用するなど、適切な設定をすることによって、AP間を移動するような利用が可能になる。

(2) バッテリー稼働性能

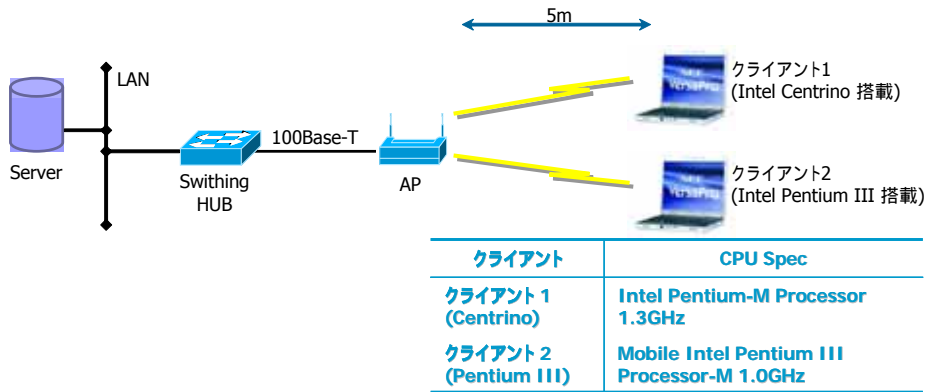
【実験内容】

- ・ 無線LANを使用した実業務環境下において、Note型PCをバッテリーのみで使用した場合、継続してどの程度使用し続けることができるかについて明らかにした。
- ・ モバイル向け最新テクノロジー「Intel Centrinoモバイルテクノロジー」搭載のNote型PCと、既存のIntel Pentium III搭載のNote型PCとを比較して計測を行った。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 固定 : 5m
障害物	・ なし
使用アプリケーション	・ 実業務環境下で計測 (無線LAN使用) <u>主な業務アプリケーション</u> - Microsoft Word / Excel - Microsoft Explorer - Mailer 無線LAN経由でデータを断続的に送受信している状態を計測
実験回数	・ ディスプレイ輝度最高 / 最低レベル 各3回 ディスプレイ輝度は8段階

図表 IV-21 : 実験構成図



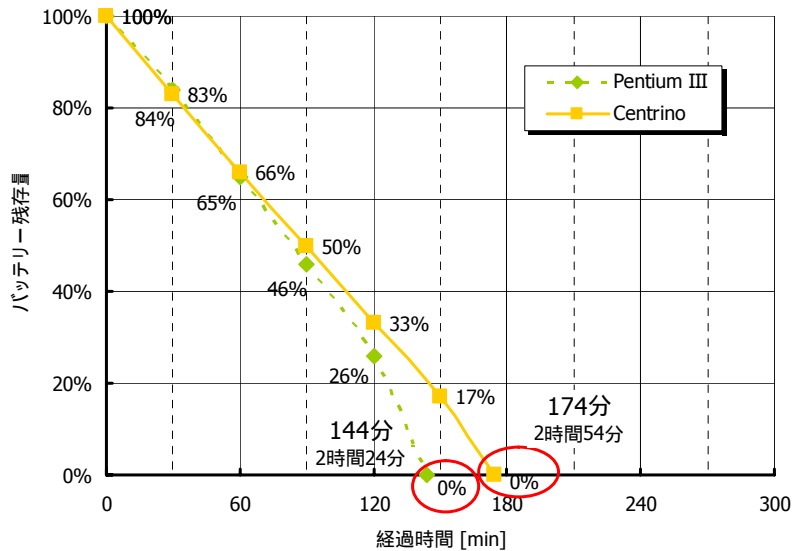
Pentium IIIは超低消費電力型の比較的新しいモデルを使用。

【実験結果】

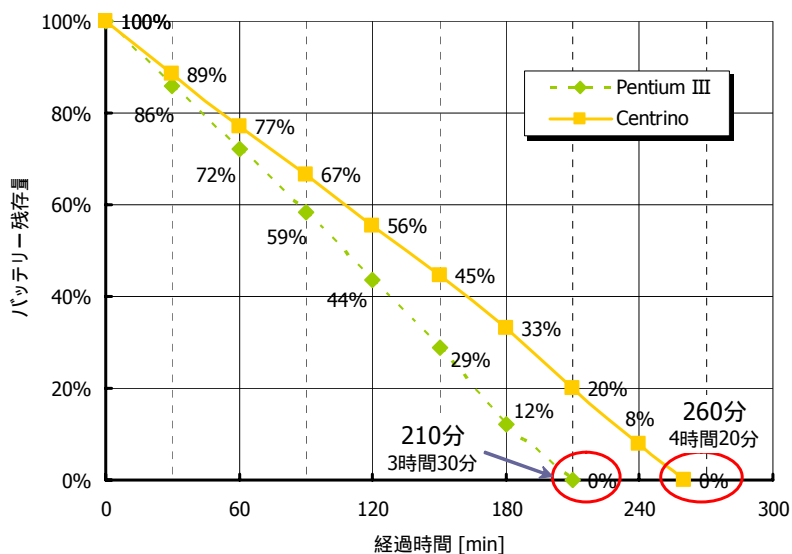
実験結果

- ・ バッテリー駆動による継続使用時間は、Pentium IIIで2時間20分強～3時間30分(輝度最低～最高)、Centrinoで3時間弱～4時間20分(同)。
- ・ Centrinoを用いることで、Pentium IIIに比べて40～50分長く継続的な使用が可能に。

図表 IV-22 : 経過時間とバッテリー残存量の関係 (ディスプレイ輝度最高)



図表 IV-23 : 経過時間とバッテリー残存量の関係 (ディスプレイ輝度最低)



(3) 公衆無線LAN環境からの接続

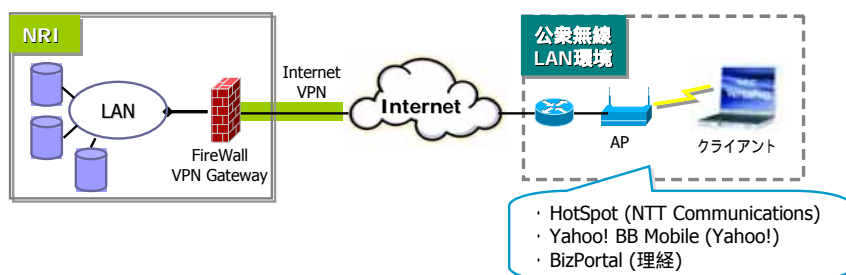
【実験内容】

- ・ 「公衆無線LAN環境 Internet VPN経由」で社内ネットワークへのアクセスが可能か、そして社内システムが利用可能かどうか検証
- ・ 本実証実験では、下記の公衆無線LANサービス提供する環境からの接続について検証した。
 - HotSpot (NTT Communications)
 - Yahoo! BB Mobile (Yahoo!)
 - 理経 (BizPortal)

【実験環境と構成図】

- ・ 実験スペックは公衆無線LANサービス環境に応じる。

図表 IV-24 : 実験構成図



【実験結果】

実験結果

- ・ 今回検証した公衆無線LANサービス全てにおいて社内システムへのアクセスが可能であった。
- ・ ただし、公衆無線LANサービスへの登録、セッティング方法や接続方法など、実際の使い勝手に関しては困難な面も多く見られた。ITリテラシのレベルによっては、利用するハードルが高いことも想定される。

図表IV-25：公衆無線LANサービスからの接続性

HotSpotサービス	検証場所	方法	認証		割り当てられるIPアドレス	操作性	Internet VPN経由アクセス
			左記認証キーの公開	その他の認証			
HotSpot (NIT Communicatios)	Desk@ (大手町店)	ESSID+WEPキー	個別に通知	-	グローバル (Class B)		
Yahoo! BB Mobile (Yahoo!)	Starbucks Coffee (八重洲地下店)	ESSID+WEPキー	Webで公開	-	プライベート (ClassC)		
BizPotal (理経)	センチュリーハイアットホテル / アイランドタワー (新宿)	ESSID+WEPキー	Webで公開	ユーザID / パスワード (スクラッチカードを配布)	グローバル (Class B)		

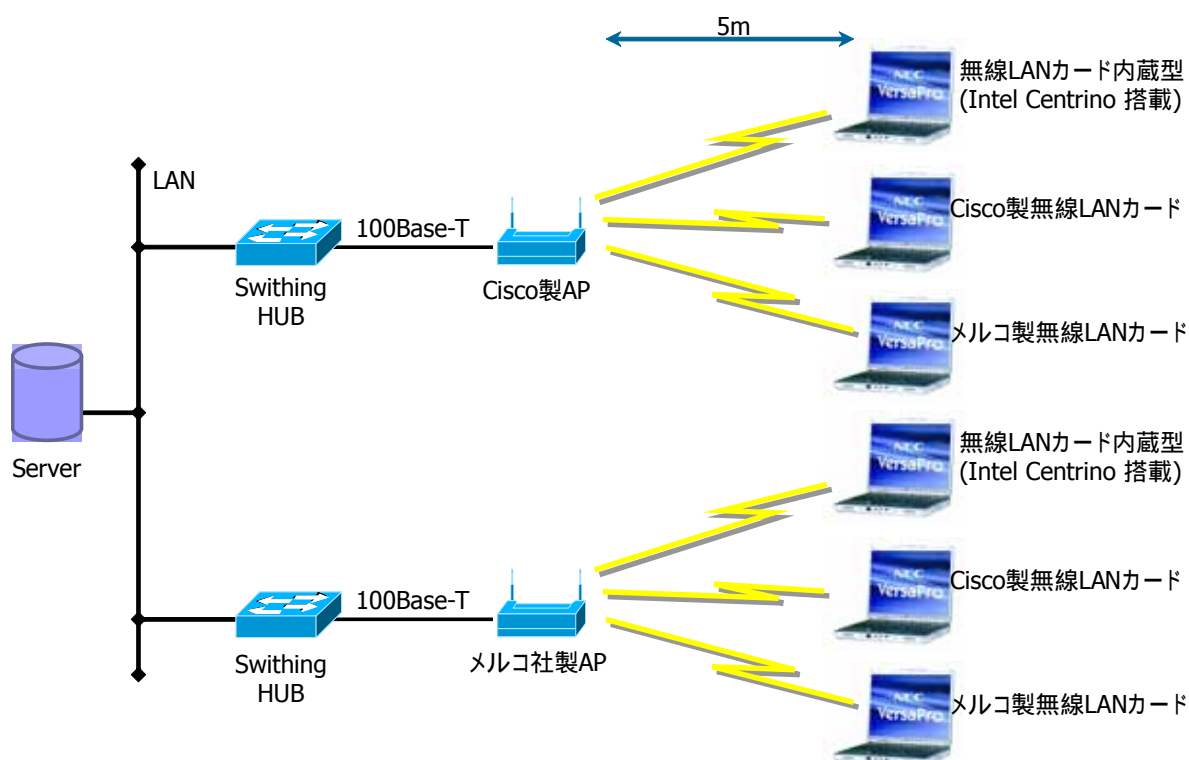
3) 製品間の相互接続性

- ・ AP - 無線LANカード(内蔵型も含む)の組み合わせについて、同一及び異なるベンダー製品間の相互接続性に関する検証を行った。また、接続の可能性のみならず、スループットの変化についても明らかにする。
- ・ 本実験では、Cisco製とメルコ製のAPと無線LANカード、無線LAN内蔵型のIntel Centrinoモバイルテクノロジー搭載Note PCについて検証した。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 固定 : 5m
障害物	・ なし
実験方法	・ コンテンツサイズ別スループットを測定
実験回数	・ 3回

図表 IV-26 : 実験構成図

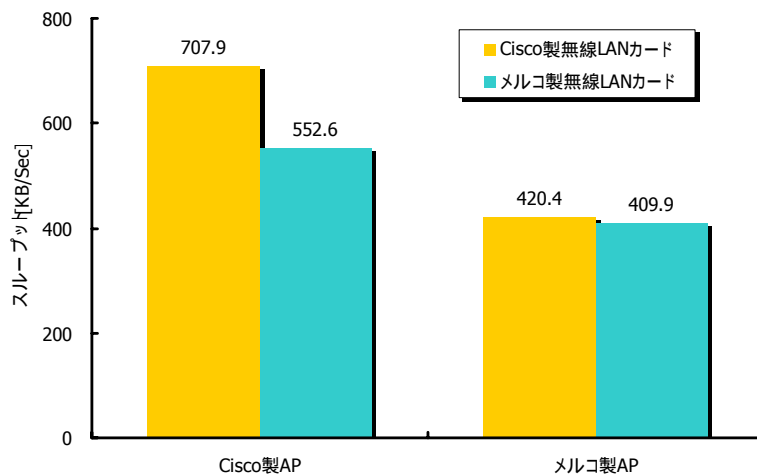


【実験結果】

実験結果

- ・ 同一メーカーのAPとカードの接続(Cisco製AP~Cisco製カード、メルコ製AP~メルコ製カード)は問題ない。
- ・ Cisco製AP~メルコ製カードの接続は、Cisco製APのLEAPの使用を停止することにより接続可能。ただし、Cisco製カードを利用する場合より、スループットが20%強劣化。
- ・ メルコ製AP~Cisco製カードは問題なく接続可能。カードベンダーによる性能はほぼ同等。
- ・ Centrinoについては、どちらのAPともに接続可能。ただし、11ch、14chの2種類のモデルが存在するため、チャンネルのセットアップの確認が必要。

図表IV-27：相互接続性とスループット



4) 電波干渉性

- ・ 複数のAPを設置する場合、電波が交わる場所ではスループットが低下し、データが破壊されることがある。
- ・ 本実証実験では、電波干渉に影響する要因として、下記の項目について検証する。

チャンネル間隔 : チャンネル間隔 - スループットの関係

AP間隔 : AP間隔 - スループットの関係

電波を発生する機器の影響

チャンネル間隔 - スループットの関係

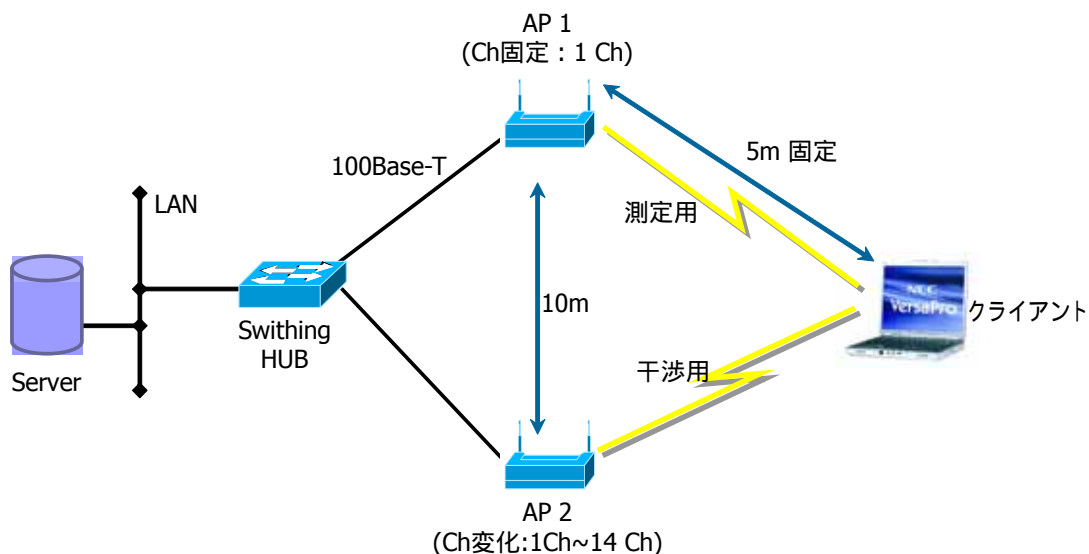
【実験内容】

- ・ 複数のAPを設置する場合、APのチャンネル間隔の設定により、スループットがどのように変化するか明らかにする。
- ・ 本実証実験では、FTPとHTTPについて検証する。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW (AP測定用) / 20mW (AP干渉用) クライアント : 30mW
AP - クライアントの距離	・ 固定 : 5m
障害物	・ なし
通信方式	・ HTTP, FTP
実験方法	<u>HTTP</u> ・ チャンネル間隔別スループット(KB/Sec)を測定 ・ 観測時間 : 60秒 ・ フレームサイズ : 50KB <u>FTP</u> ・ チャンネル間隔別スループット(KB/Sec)を測定 ・ ダウンロードが終わるまで ・ ファイルサイズ : 1MB
実験回数	・ HTTP, FTPともに各3回

図表 IV-28 : 実験構成図

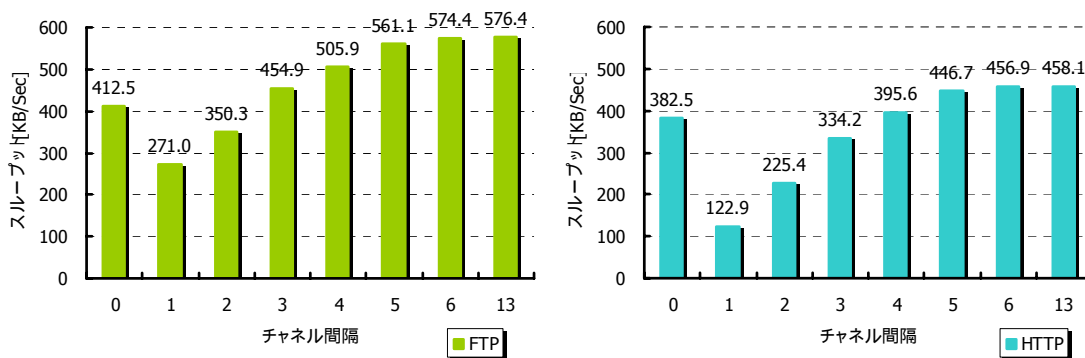


【実験結果】

実験結果

- ・ 複数のAPを近接して設置する場合、有効なスループットを確保するためには、チャンネルを5～6以上間隔をあけて設定する必要がある。
- ・ チャンネル間隔が5以下になると干渉を起し、スループットが低下。ただし、同一チャンネルの場合、低下は小さい。

図表IV-29 : チャンネル間隔 - スループットの関係 (FTP/HTTP)



AP間隔 - スループットの関係

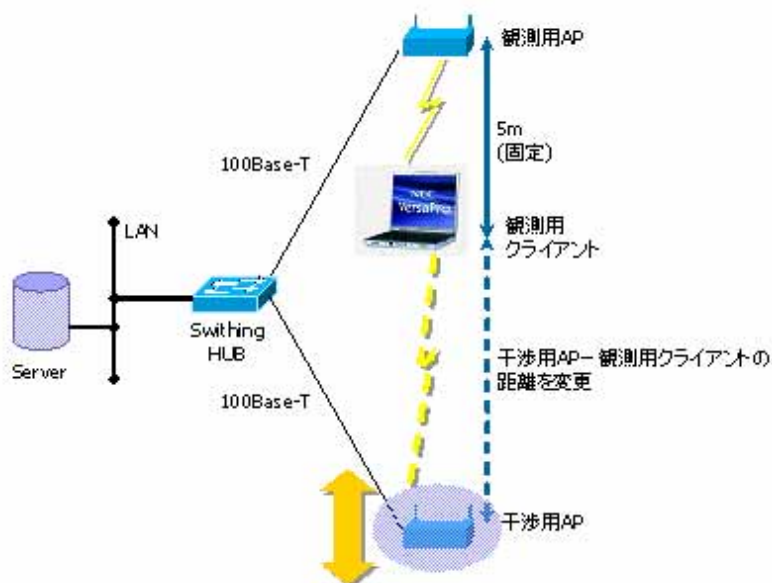
【実験内容】

- ・ 複数のAPを設置する場合、AP間の間隔がスループットに対してどの程度影響を及ぼすか明らかにする。
- ・ 本実証実験では、「チャンネル間隔 - スループットの関係」と同様に、FTPとHTTPについて検証する。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 観測用APとの距離 : 固定 5m ・ 干渉用APとの距離 : 変化
障害物	・ なし
通信方式	・ HTTP、FTP
実験方法	<p><u>HTTP</u></p> <ul style="list-style-type: none"> ・ AP間隔別スループット(KB/Sec)を測定 ・ 観測時間 : 60秒 ・ フレームサイズ : 50KB <p><u>FTP</u></p> <ul style="list-style-type: none"> ・ AP間隔別スループット(KB/Sec)を測定 ・ ダウンロードが終わるまで ・ ファイルサイズ : 1MB
実験回数	・ HTTP、FTPともに各3回

図表 IV-30 : 実験構成図



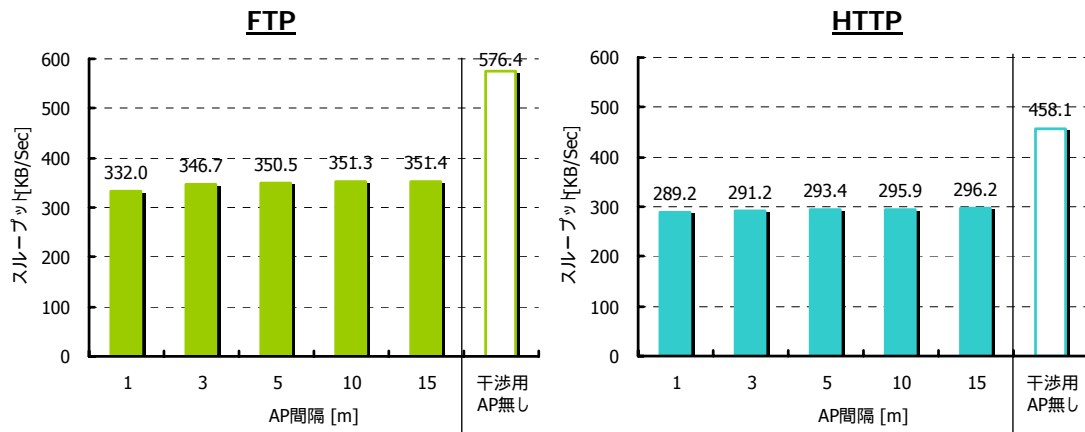
「観測用AP - クライアント - 干渉用AP」は直線状に配置

【実験結果】

実験結果

- ・干渉用APとクライアントの距離が15m以内であれば、干渉による性能劣化の度合いには変化が見られない。
- ・AP間の干渉を無くす上で、「干渉用APとクライアントの距離 = 15m程度」では不十分であることが分かった。

図表IV-31 : AP間隔 - スループットの関係 (FTP/HTTP)



電波を発生する機器の影響

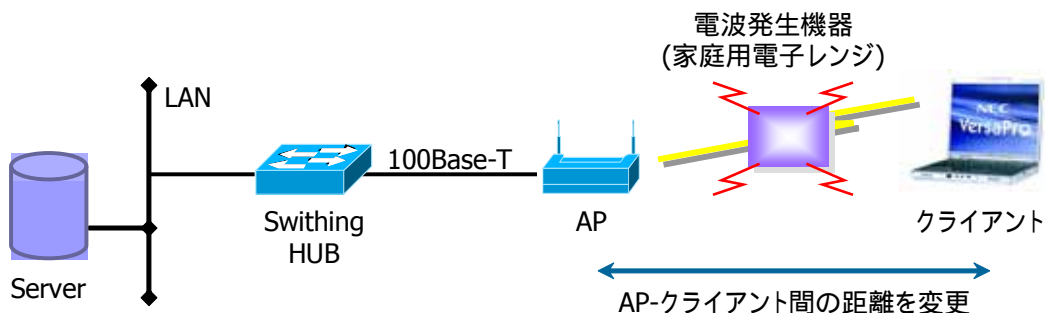
【実験内容】

- ・ 2.4GHz帯の電波を発生する機器(今回は家庭用電子レンジ)を使用する場合、無線LANのスループットがどの程度変化するか明らかにする。
- ・ 本実証実験では、
、
と同様に、FTPとHTTPの変化について検証する。

【実験環境と構成図】

実験環境	実験スペック
電波出力	・ AP : 1mW / クライアント : 30mW
AP - クライアントの距離	・ 観測用APとの距離 : 固定 5m ・ 干渉用APとの距離 : 変化
障害物 (電波発生機器)	・ 家庭用電子レンジ (SHARP製) - 定格高周波出力 550W
通信方式	・ HTTP、FTP
実験方法	HTTP ・ AP - クライアント間のスループット(KB/Sec)を測定 ・ 観測時間 : 60秒 ・ フレームサイズ : 50KB FTP ・ AP - クライアント間のスループット(KB/Sec)を測定 ・ ダウンロードが終わるまで ・ ファイルサイズ : 1MB
実験回数	・ HTTP、FTPともに各3回

図表 IV-32 : 実験構成図

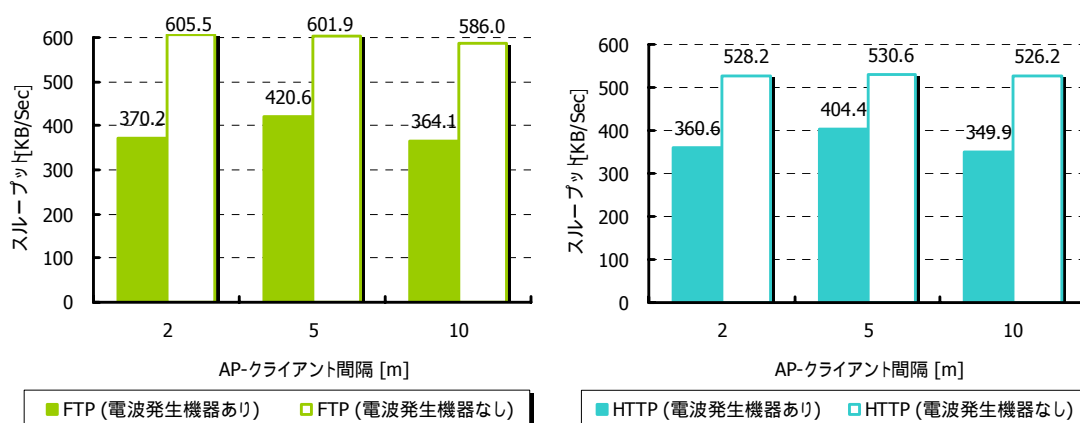


【実験結果】

実験結果

- ・ 家庭用電子レンジによる性能劣化は3割程度。
- ・ 今回の場合、APとクライアントの距離を10m離れていても、干渉による性能劣化の度合いには影響しない。

図表IV-33 : AP間隔 - スループットの関係 (FTP/HTTP)



V 結論

本実証実験を通じて、企業情報システムにおけるネットワーク・インフラの一つとして、無線LANは有効であることが明らかになった。さらに、無線LANによる情報システム環境が、ユーザにとって快適かつ安心した環境にするためには、実績やノウハウに基づいた、きちんとした手順と手段で設計・構築することが、当然のことながら大変重要である。パフォーマンスの優劣は、無線LANのAPの配置の仕方によって決まると言っても過言ではない。適材適所で有線LANと無線LANを使い分けることにより、安全で使い勝手に優れたネットワーク・インフラ環境が実現し、企業内情報システムの高度化に貢献することが期待される。

無線LAN導入で重要なことは、標準技術への対応ではなく、企業各社でのセキュリティ・ポリシーや運用・管理方法を早期に確立することである。そのためには、セキュリティ技術や標準技術の進展に期待して無線LAN導入に躊躇するのではなく、できるだけ早い段階から、ノウハウ蓄積といったレベルから、段階的に導入を進めていくことが重要であると考え。業務環境の改善向上や生産性向上などといった、無線LANならではのメリットをできるだけ多く享受しながら、自社独自の活用法を見だし、ノウハウを蓄積していくことが得策である。

今後、セキュリティの強化仕様のIEEE802.11iや、高速な無線LAN規格であるIEEE802.11gなどの標準化作業が急ピッチで進められ、今後無線LAN環境はより快適で安全なものになるであろう。さらに、2003年3月には、無線LANの利用を基本にして設計された「インテルCentrinoモバイル テクノロジー」がリリースされ、これを搭載したモバイル端末が次々に登場するであろう。無線LAN環境はますます魅力的で身近なものになり、無線LANコミュニティの健全なる形成へと展開していくことが期待される。