

オフィスネットワークのセキュリティ対策と最新構築事例

Security Measures for Office Networks and Latest Installation Case

松本 哲也 *
Tetsuya Matsumoto

* ソリューションビジネス本部 システム事業部 インフラソリューション統括部 プロフェッショナルサービス部

近年、企業の労働環境の変化により、オフィスのネットワーク環境もフリースペース化への対応や、無線化などのニーズが高まってきている。それに伴い、従来のオフィスネットワークで必要とされたコスト・信頼性・高性能の要件に加えて、セキュリティ対策の考慮が必要不可欠となっている。ここでは、オフィスネットワークの現状と課題をまとめ、最近のセキュリティ対策を施したネットワーク構築事例を紹介する。

In recent years, due to changes in the working environments of companies, there is a growing demand for networks to be able to adapt to free space offices or wireless working environments. In addition to the requirements for cost, reliability, and high performance in previous office networks, consideration of security measures is becoming essential. In the following section, the current status and problems faced by office networks will be summarized, and a case study of a recent network installed with security measures will be discussed.

1 まえがき

近年の個人情報漏洩事故や個人情報保護法の施行に伴い企業オフィスのネットワーク環境も内部アクセスに対するセキュリティ対策のニーズが高まってきている。

雇用環境の変化によるパート・アルバイト、派遣社員など非正規社員のネットワーク利用機会の増加や、オフィスの有効活用のための無線 LAN 化も一因と言える。

企業のネットワークインフラでの内部セキュリティ対策はユーザー認証規格 IEEE802.1x¹⁾に基づいて認証されたユーザーにだけ通信を許可したり、無線 LAN 区間の暗号化を行って盗聴を防止したり、不正侵入防御システム IPS (Intrusion Prevention System の略) の採用などが挙げられる。

当社では 1995 年よりネットワーク構築サービスを提供しており、2004 年 7 月には「PFU 検疫ネットワークシステム」²⁾の提供を開始した。

本稿では、ネットワークトレンドの変化を振り返り最新のセキュリティ対策を取り入れたオフィスネットワークの構築技術について、事例を交えて述べる。

2 オフィスネットワークの現状と課題

2.1 オフィスネットワークの現状

現在の一般的なオフィスネットワークの構成と課題を図 - 1 に示す。

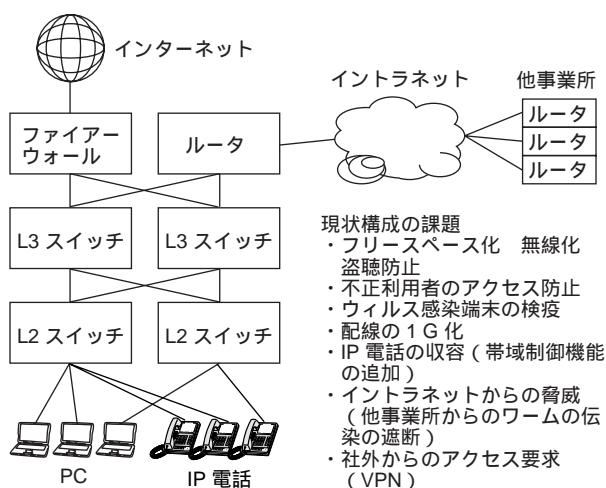


図 1 現在のオフィスネットワーク構成と課題
(Fig.1-Configuration of current office networks and associated problems)

ここで、オフィスネットワークを構成する技術の成熟度を要約すると以下のとおりである。

(1) 高速・高信頼性

基本的な構成は以下に示すように確立している。近年は登場する技術トレンドに対応する状況。オフィスネットワークの高速・高信頼性の変遷を図-2に示す。

1) 基幹ネットワーク

1998年頃のL3スイッチ二重化の技術で確立。ギガイーサネット等への高速化がトレンド。

2) 事業所間WAN

構成は1990年頃の技術で確立。キャリアの提供サービスに合わせ成長している。

経営層からのコストダウンに対する要求からIP-VPNや広域イーサネット、インターネットVPNへの移行がトレンド。

3) 端末

有線LANは1994年頃に技術が確立。100Base-TXや1000Base-TによるUTP(Unshielded Twist Pair)ケーブルによる配線が主流。無線LANは規格が出揃ったものの、脆弱性などセキュリティ面で難があり技術未確立。

(2) セキュリティ

インターネット接続に伴う外部からの脅威についての対策技術は確立。

内部セキュリティ対策が課題(認証や検疫など)。

(3) 音声ネットワーク

IP電話化が近年のトレンド。既存構成では帯域制御や優先制御の考慮が無く、移行にはイントラネット全体の見直しが必要。

2.2 オフィスネットワークの課題と対策

現在のオフィスネットワーク構成の課題と対策を以下に示す。

(1) フリースペース化への対応

オフィススペースの有効活用、柔軟なレイアウト変更を容易とするため無線LANの利用を推進するニーズの高まりがある。無線LAN利用に際して、盗聴防止や暗号化などセキュリティ考慮が必須と言える。

(2) 不正利用者のアクセス防止

外部からの不正アクセスによる機密情報漏洩を防止するため、無線LAN、有線LANを問わず、ユーザー認証により限られた人へのみネットワークサービスを提供し、ネットワークの利用履歴を管理する仕組みが必要である。

(3) ウィルス感染端末の検疫

近年のウィルス感染による被害は、ワーム^{注1)}の増殖活動を原因とする基幹業務の停止や、情報漏洩事故など企業活動に直接影響を与えうる脅威となってきた。オフィス内に常設の端末はウィルス検疫ソフトウェアの導入により対策を施しているため、近年はモバイル端末などの持込PCによる被害が主となりつつある。ウィルス感染した端末や感染する脆弱性を有する端末のネットワーク利用を制限する検疫システムの導入などが必要である。

当社ではこのニーズに応えるため、2004年7月より「PFU 検疫ネットワークシステム」を提供している。

(4) 有線LANの1 Gbps化

スイッチングハブやLANカードの低価格によりUTPケーブルでのギガイーサネットの利用が一般的と

	1990	1994	1998	2002	2006
基幹ネットワーク	Ethernet (10 Mbps)	FDDI Fast Ethernet (100 Mbps)	L3 スイッチ二重化 (100 Mbps x n)	(1 Gbps x n)	(10 Gbps x n)
事業所間WAN	専用線 + バックアップ回線 専用線 (128 Kbps)	フレームリレー網 (128 Kbps)	ATM (6 Mbps)	IP-VPN 網 広域イーサネット (~ 100 Mbps)	(~ 1 Gbps)
端末	有線 LAN AUI (10 Mbps)	UTP (10 Mbps)	(100 Mbps) 無線 LAN (11 Mbps)	(100 Mbps) (54 Mbps)	(1 Gbps) (54 Mbps x n)

図 2 オフィスネットワークの変遷
(Fig.2-Trends of office networks)

注 1) ワームとはコンピュータウィルスの分類の一つで主に自己増殖を目的とした不正プログラムを呼ぶ。

なりつつある。局所的な帯域拡張はルータやスイッチングハブなどのバッファ領域を圧迫する結果となり、全体のバランスを考慮した帯域拡張が必要である。

(5) IP 電話の収容

電話機の IP 化によって PBX など交換機設備のコストを削減するニーズが高まってきている。伝送遅延に対する要求が厳しい音声データの転送に対応するため、低速な LAN, WAN 環境では帯域拡張や優先制御、帯域制御の追加などの考慮が必要である。

(6) イン트라ネットからの脅威

限られた利用者によりのみネットワークサービスを提供、不正利用者の排除を目的にユーザー認証や無線 LAN の盗聴対策や暗号化、及び内部への不正アクセスを防止するための IPS による侵入防御システムの導入などが挙げられる。

(7) 社外からのアクセス要求 (VPN)

時間の有効活用のため、自宅のインターネット接続環境から社内イン트라ネット接続を行いたいというニーズの高まりがある。一般に IPsec や SSL を使用した VPN 接続による暗号化対策が行われている。

次章で有線 LAN, 無線 LAN の認証による不正利用者のアクセス防止の事例を紹介する。

3 最近の構築事例

本章で述べるのは当社が最近構築を担当したオフィスネットワーク事例である。

3.1 構築の背景

今回紹介するお客様は、新規事業所の開設に伴いネットワークインフラの整備を検討していた。

当社は検討フェーズより参加、最新のセキュリティ対策による無線・有線統合認証ネットワークの構築に至った。

3.2 新ネットワークに対する要件

新ネットワークに対する要件として以下に示すようなものがあつた。

- 1) 高速性, 高信頼性。
- 2) 利用者は無線 LAN と有線 LAN の 2 種類どちらでも利用可能。
- 3) フリースペース化により利用者の端末接続場所を固定しないネットワーク使用。
- 4) 利用者認証による不正者のネットワーク利用防止,

非正規従業員のネットワーク利用制限。

5) 外部 (インターネット) に対するセキュリティ対策。

6) 内部 (イン트라ネット) に対するセキュリティ対策。ワーム検知や防御, 不正通信の検知や防御など。

3.3 ネットワークの設計

お客様の要件を基に以下の設計を行った。

新ネットワークの構成を図 - 3 に示す。

(1) 幹線ネットワーク

幹線ネットワークは光ファイバケーブルを使用し、ギガイーサネット (1000Base-SX) を敷設した。幹線ネットワークの帯域を増強するため、物理的に複数のインターフェースを論理的に一つにするリンクアグリゲーション機能を使用した。この機能により幹線は 1000Base-SX × 2 本で全二重 2 Gbps の帯域を確保した。この機能は構成する回線の障害時に動的に縮退して継続利用が可能のため、回線の信頼性向上策としても機能する。

また、幹線を構成する機器は全て冗長化、バックアップ経路も予め確保することで更に信頼性を高めた。

(2) 経路制御方式

従来の高信頼性ネットワークではレイヤー 2 のループ回避を特長とするスパンニングツリープロトコル、レイヤー 3 の耐障害性や負荷分散を特長とする VRRP (Virtual Redundant Routing Protocol) プロトコル、レイヤー 3 のバックアップや経路の動的変更を特長とする Dynamic ルーティングプロトコル (RIP や OSPF など) を併用する経路制御方式が一般的であった。

本ネットワークではレイヤー 2 の経路切り替えに時間を要するスパンニングツリープロトコルはあえて利用しない論理設計とした。レイヤー 3 は VRRP プロトコルだけをを用いた構成とし設計を簡易化した。これにより、各経路、機器障害時の経路切り替えを数秒単位の瞬断レベルにまで早める設計とした。

(3) 認証方式と認証サーバの配置

図 - 4 に認証システムの構成を示す。利用者認証の認証方式は IEEE802.1x を採用、全フロア L2 スイッチと無線アクセスポイントに IEEE802.1x 機能を有する機種を選定した。認証方式に IEEE802.1x を採用した理由は、端末が直接接続されるエッジデバイス (無線アクセスポイントや L2 スイッチ) レベルまでユーザー認証によるアクセス制御が可能となる点からであ

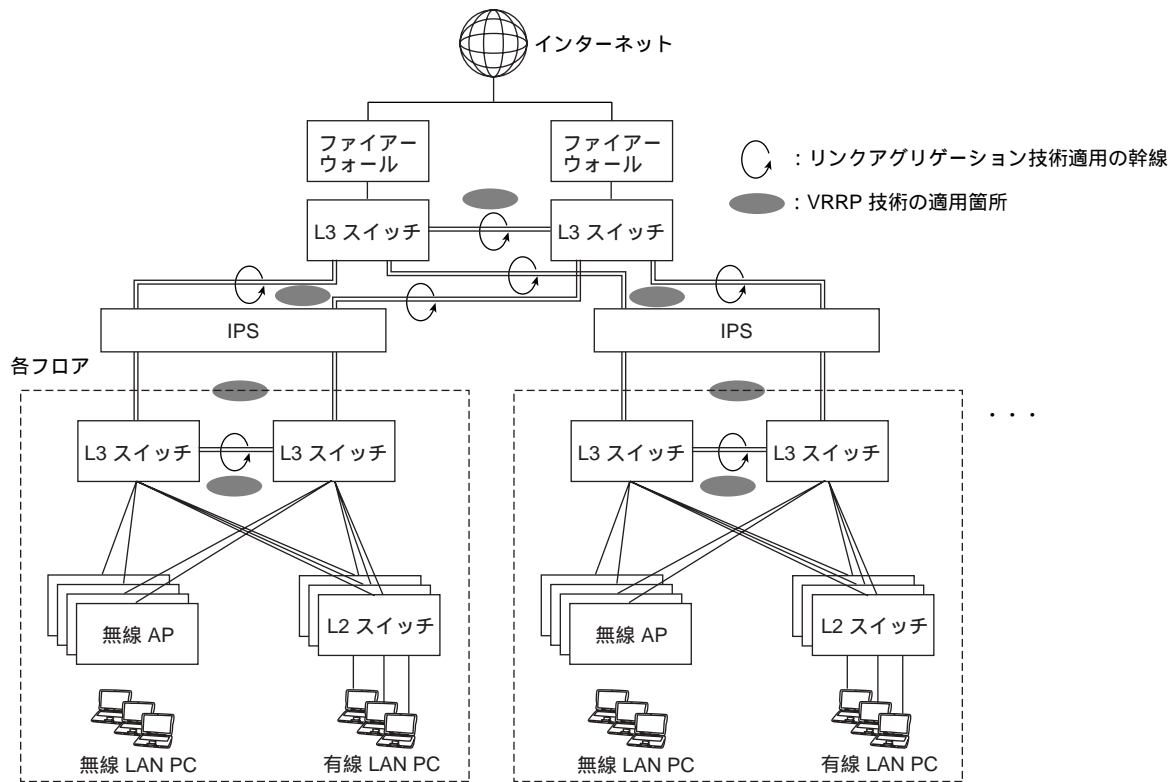


図 3 構成の概要
(Fig.3-Configuration outline)

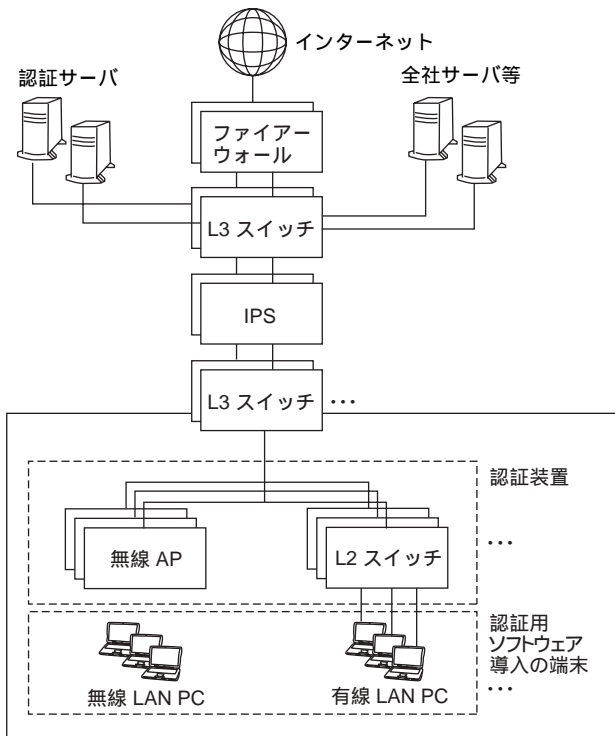


図 4 認証システムの構成
(Fig.4-Configuration of authentication system)

る．ネットワークリプレイスの場合，全エッジデバイスのリプレイスが必要となり導入が困難となりがちであるが，新規導入という点から IEEE802.1x をサポートする装置を選定し，導入が容易であった．

認証機能の停止は全ネットワークアクセスの停止となるため，認証サーバは冗長化し，幹線 L3 スイッチに直結する配置とした．

(4) 認証方式の選択

IEEE802.1x の認証方式の選択には以下の点を考慮した．

1) セキュリティ強度

必要とされるセキュリティ強度に適した認証タイプを選定した．固定パスワードから脆弱性が指摘される認証タイプ EAP-MD5 は検討対象から除外した．なお，セキュリティ強度は高い程良い．

2) 導入や管理の容易性

管理者が電子証明書を発行する証明局サーバを運用可能か．電子証明書の利用が必要な方式は電子証明局サーバの構築やクライアントへの電子証明書の配付など，導入時だけでなく運用への負担も大きい．

3) 利用者端末の種類

利用者端末の種類は限定することが可能か。なお、本ネットワークでは Windows^{注2)} 2000 又は Windows XP に限定が可能であった。

上記より各認証方式は、有線 LAN は EAP-PEAP、無線 LAN は EAP-LEAP を選択した。

EAP-PEAP は Windows 2000 SP4、Windows XP SP1 で標準機能としてサポートしている認証方式であり、電子証明書もサーバが正規のサーバであることを証明するためにのみ利用する事で導入は容易で、セキュリティ強度的にも十分であると判断した。

EAP-LEAP は Cisco 社独自方式であり、無線 LAN カードも Cisco 社製使用に限定されるが、互換機能の CCX (Cisco Compatible Extensions) 対応製品での利用も可能である。CCX 対応製品は利用者端末の機種で対応可能であった事、ワンタイムパスワードをサポートし、導入が非常に容易であることなどから選択した。

(5) 利用者のアクセス制御

正規従業員と非正規従業員（外注者）とが混在するオフィス環境の中で、各々がアクセスできるネットワークを分離するため、及び不正利用者（未登録者）のネットワークアクセスを防止するために、認証ネットワークを導入した。さらに、将来的には不正な PC（ウイルスパターンが最新でないなど）を検出するための検疫ネットワーク導入が容易である事を条件にした。

まず、予めユーザー区分（正規従業員 / 非正規従業員）毎に VLAN を分割して配置、レイヤー 2 レベルでネットワークの閉域性を確保し、各 VLAN（ユーザー区分）からアクセス可能な範囲を L3 スイッチやファイアーウォールで設定を行った。

認証サーバにはユーザーごとにユーザー区分で設定した VLAN 番号を属性情報の一部として設定した。これにより、利用者端末を LAN 接続する物理的な場所や接続形態（有線又は無線）によらずに IEEE802.1x によるユーザー認証後にユーザーが所属する VLAN 番号を動的に割当てされることを可能とした。

(6) セキュリティ対策

1) 外部セキュリティ対策

外部からの不正アクセス防止のため、ファイアーウォールを配置した。

2) 内部セキュリティ対策

ウイルス感染した端末による不正な通信や、セキュリティ上問題のある通信を自動的に検知し、内部ネットワークへの通信を遮断するために IPS を設置した。また各クライアントに対してはウイルス対策ソフトウェアを導入した。

3) 無線 LAN セキュリティ対策

盗聴防止のために電波強度のチューニングや無線 LAN のグループを指定する設定である ESS-ID の隠蔽、利用者端末とアクセスポイントに設定する共通の鍵を利用して通信データを暗号化し盗聴を防ぐ WEP は、WEP の鍵が固定で更新されることが少なく計算により解かれてしまうという鍵脆弱性に対応するための暗号化方式（暗号鍵の自動交換）などの対策を行った。

4) 有線 LAN セキュリティ対策

IEEE802.1x を利用し接続ポート単位でのユーザー認証を行った。IEEE802.1x を利用できないポートは MAC アドレスフィルタ機能等で補完した。

3.4 認証ネットワーク設計・運用のポイント

IEEE802.1x 認証ネットワークの設計・運用にあたり、以下に留意する必要がある。

(1) IEEE802.1x / EAP 方式の選定

IEEE802.1x で標準の認証方式である EAP では様々な方式を選択することができる。最もセキュリティ強度の高い方式としては現在「EAP-TLS」と言えるが、自営の証明局サーバが必要など、導入のハードルは高い。

利用者端末の環境や運用者のスキルに応じて適切な方式を選択する必要がある。表 - 1 に EAP 認証タイプの一覧を示す。

(2) 利用者への配慮

利用者の利便性を高めるように、次の要素について配慮が必要となる。

1) インストールの容易さ

利用者端末への設定はできる限り単純であることが望ましい。利用者端末へ証明書の配付が必要となる EAP-TLS の場合は電子証明書の配付方法や管理方法を検討する必要がある。

2) 起動時の待ち時間

IEEE802.1x 認証の開始契機はポートのリンクアップであるが、利用者端末の起動までの時間が長いと、タイムアウトにより認証できないこともありえる。利用者端末の起動を待たずに IEEE802.1x 認証がタイ

注 2) Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標である。

表・1 IEEE802.1x 規格 / EAP 認証タイプ

認証方式	ユーザー識別方法	認証方法	長所	短所
EAP-MD5	固定パスワード	CHAP に似たチャレンジ方式。	・導入は容易。	・パスワードに対する辞書攻撃の危険性があり、一般に利用されない。 ・相互認証無し。
EAP-TLS	電子証明書	認証サーバとクライアントの相互認証方式。	・EAP の中で最高の認証確度。 ・動的 WEP キー交換。 ・IETF による標準化済。	・証明局設置による運用負担高。
EAP-TTLS	固定パスワード	サーバ認証は電子証明書、クライアント認証はユーザーIDやパスワード。	・TLS と比較して導入し易い。 ・動的 WEP キー交換。 ・対応クライアントが多い。	・ベンダーの独自仕様のため、認証用クライアントソフトウェアは別途必要。 ・パスワードに対する辞書攻撃の危険性あり。
EAP-PEAP	EAP サーバ実装に依存	サーバ認証は電子証明書、クライアント認証はユーザー ID やパスワードを利用。	・Windows2000 SP4, Windows XP SP1 で標準サポート。 ・ワンタイムパスワードをサポート。	・Windows 端末に限定される。
EAP-LEAP	固定パスワード	ユーザー ID やパスワードによるクライアント、サーバ相互の認証。	・ユーザーベースの認証で管理が容易。シングルサインオン可能。	・Cisco Systems 社の独自方式。
EAP-FAST	固定パスワード	秘密鍵（対象鍵）アルゴリズムにより認証プロセスを暗号化。	・EAP-LEAP のセキュリティ強度を強化。 ・EAP-LEAP からの移行が容易。	・Cisco Systems 社の独自方式。

ムアウトしないよう考慮する必要がある。

3) 運用の容易さ

IEEE802.1x 認証以外に、端末自体の認証等、起動時にユーザー操作が必要な作業はできるだけ少なくする方法が望ましい（ワンタイムパスワードの利用可否など）。

(3) 認証システムの管理

1) 認証サーバの運用

認証サーバのバックアップ方式や同期方式、新規利用時や利用停止時などユーザー管理の仕組みを検討する必要がある。また、ユーザー自身がパスワードを変更できる仕組みの検討も必要となる。

2) ログ管理

不正利用があった場合のログ調査を可能とするため、アクセスログの管理方式を検討する必要がある。

3.5 将来構想

今回のお客様のケースでは IEEE802.1x ユーザー認証の導入までを行った。IEEE802.1x インフラは完備されたため、今後新たな EAP への移行や検疫機能の追加は容易に可能な構成であり機能拡張をご提案していく。

4 むすび

企業のオフィスネットワークにとってセキュリティ対策に終わりは無く、今後も新たな脅威が次々と発生するものと予想される。今回ご紹介した IEEE802.1x も、単体では効果が限られ、様々な方策を組み合わせることで、セキュリティ強度を高めていくことが可能となる。

IEEE802.1x 対応のハードウェアは近年低価格化が進み、L2 スイッチングハブや無線アクセスポイントの標準的な機能となりつつあり、今後導入が進む機能として考えられる。

当社は新たな脅威をできる限り排除できるよう今後もお客様の最適なセキュリティシステム構築を支援していく。

参考文献

- 1) 北井：無線 LAN 環境のユーザ認証ソフト Safeauthor, *PFU Tech. Rev.*, 14,2,pp.25-34 (2003)。
- 2) 平松, 濱野, 高橋：検疫ソフトウェア iNETSec Inspection Center, *PFU Tech. Rev.*, 16,1,pp.29-34 (2005)。