〈ソリューション〉

UNIVERGEオフィスセキュリティソリューション

UNIVERGE Office Security Solutions

向山信一* 宮原吉郎* 飯塚幸至* 伊藤晴紀*
Shinichi Mukouyama Kichiro Miyahara Koji Iizuka Haruki Itoh

要 旨

日本はブロードバンド回線や3Gモバイルが普及し，世界で最も進んだユビキタス環境を持っています。NECでは，このユビキタス環境を有効に活用し，企業の知的生産性を向上させるソリューションを「UNIVERGE」として体系化しました。しかし，ユビキタス環境が進展し，誰でもどこでも高速にインターネットにアクセスできるようになると，ウイルスやワームによる被害や，機密情報や個人情報の漏えいなど企業オフィスにおけるセキュリティの脅威が増大します。「UNIVERGE」において，そのオフィスのセキュリティ対策を提供するのが「UNIVERGEオフィスセキュリティソリューション」です。

本稿では，UNIVERGEオフィスセキュリティの体系と，新しい強化ソリューションについて紹介します。

In Japan, we can easily access the network in the advanced ubiquitous network environment with widely spread of broadband lines and 3G mobile networks. “UNIVERGE Solutions” offer some solutions for enterprise users to improve their productivity by making use of their IT infrastructure and ubiquitous wideband network. On the other hand, as the broadband network infrastructure is provided well and everybody can get access anytime and anywhere, security threats (virus, worms, information leakage and so on) grow larger. “UNIVERGE Office Security Solutions” offer the enterprise users some countermeasure for security breach in the “UNIVERGE” solutions.

This paper describes the system of “UNIVERGE Office Security Solutions” and introduces new solutions.

1．まえがき

NECでは，企業の知的生産性の向上を目的とする「ブロードバンドオフィス」を業界に先駆けて提唱しました。

このブロードバンドオフィスを実現するソリューションがUNIVERGEソリューションであり，特にブロードバンドオフィスのセキュリティ対策全般を担うのがUNIVERGEオフィスセキュリティソリューションです。

企業のセキュリティ対策に目を向けると，近年のIT化進展に伴い，その脅威は増大する一方です。続発するウイルス・ワームによる被害を始め，最近では大規模な個人情報の漏えい事件がマスコミで報道され，社会問題となっています。これらの情報漏えい事件は，企業内部に原因があるといわれます。

従来のセキュリティ対策では，守るべきものは社内（閉じられた空間）にあり，外部から身を守ることが中心でした。しかし，ブロードバンドオフィスでは，パソコンや情報を持ち歩いて業務に使うことになるため，開放された空間でのセキュリティ対策が求められます。情報漏えい事件を見ても，内部のセキュリティ対策が重要であることは明白です。

UNIVERGEオフィスセキュリティソリューションでは，端末，サーバ，アプリケーション，そしてネットワークを統合し，受動的から能動的なセキュリティ対策へシフトすることをめざし，ブロードバンドオフィス向けのセキュリティソリューションとして体系化しました。

2．UNIVERGEオフィスセキュリティの体系

企業のセキュリティに対する要求は様々ですが，それらセキュリティ対策のすべてを一度に導入するのは難しい面があります。現実には，将来像を見据えながら，段階的な導入を行っていく必要があります。

UNIVERGEオフィスセキュリティソリューションでは，セキュリティ対策のモデル化，段階的導入を考慮して，以下の3タイプに体系化しました。

(1) UNIVERGEセキュリティ らくモデル
個別の技術課題に対する解決策

(2) UNIVERGEセキュリティ らくモデル拡張オプション
モデルと組み合わせて利用し，モデルの機能を拡張でき

* UNIVERGEソリューション推進本部
UNIVERGE Solutions Promotion Division

るオプション

(3) UNIVERGEセキュリティ ソリューション

モデルを組み合わせることにより，さらに上位のセキュリティ要件を実現するソリューション

本稿では，新たに強化したセキュリティソリューションについて紹介します。

3．強化ソリューション

3.1 セキュアIPテレフォニー

IPテレフォニーは，IP網を利用して音声を伝送するVoIP技術を使って提供される電話サービスです。IP網を利用しデータ系ネットワークと統合することが可能であるため，専用で保有していた回線を削減できるなど大幅にTCOを削減するメリットがあります。しかしその一方で，データ系ネットワーク同様の様々なセキュリティの脅威にも直面することになります。

セキュリティの脅威には，電話の通話を制御するIP-PBXへの不正アクセス，音声通話の盗聴，IP-PBXなど制御サーバへのDoS攻撃によるシステムダウンなどが挙げられ，これらの脅威への対策は必要不可欠です。IP-PBXへの不正アクセスには通信に必要のないポートを閉じるなどサーバを要塞化することで対応します。音声通話の盗聴には呼制御や音声の通信暗号化で対応します。また，DoS攻撃には，ファイアウォールやIDSなどを利用してシステム全体で防御します。

また，音声通話がセキュリティを確保しながら，すでにデータ系ネットワークに導入されているファイアウォールを通過できるようにする必要もあります。音声通話で利用する通信ポートは通話のたびに変動しますし，音声通話はトランスポートプロトコルとしてUDPを使用しますので，ファイルウォールに大きな穴を開けなければなりません。これにより新たなセキュリティ上の問題が生じることがあるので，ファイアウォールが音声通話プロトコルを理解して，動的に通信ポートを開閉することが必要になります。

セキュアIPテレフォニーソリューションを導入すれば，データ系と同じレベルのセキュリティを達成し，IPテレフォニーを安心してお使いいただける環境を提供します。セキュアIPテレフォニーの全体像を**図1**に示します。

3.2 認証VLANらくモデル

最近のセキュリティ被害の大きな傾向として，不正アクセスによる情報漏えい，ウイルス・ワーム感染による被害の2つが挙げられます。

前者の情報漏えいによる大きな影響として，信用の失墜による被害が挙げられます。たとえば不正アクセスにより顧客情報が漏えいした場合を考えます。この場合，ただ単に情報が悪用されるだけで済まず，これまで築き上げてきた企業イメージが一夜にして崩れてしまいます。このような信用の失墜は企業の業務継続に深刻な打撃を与えます。

後者のウイルス・ワーム感染については，MSブラスターやNetSky，その他多数の亜種による被害がありますが，これらは年々被害が増加しています。さらに全世界規模でのブロードバンド化により，ワームが瞬く間に全世界に蔓延するなど，その感染速度も速まっています。これらワームは既知のセキュリティホールを悪用したものがほとんどで，常に最新のパッチを適用するなどきちんとした運用・管理を行っていれば防げますが，実際には十分な運用ができていないのが現状です。

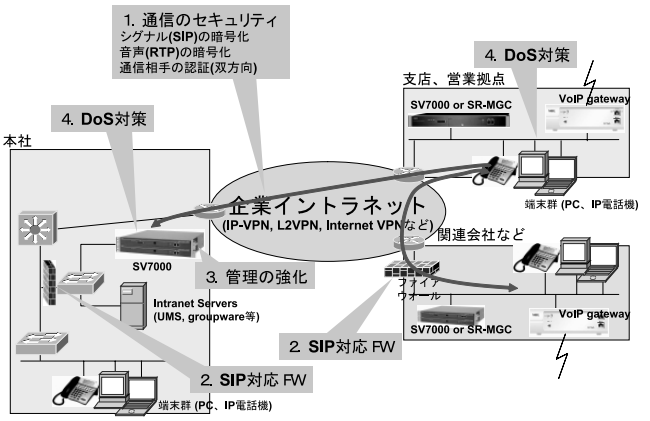

図1 セキュアIPテレフォニーの全体像
Fig.1 Secure IP Telephony.

これらセキュリティ上の脅威に対する1つの解決方法として，ネットワーク接続時にユーザ認証を行うシステム導入が考えられます。認証機能付きのネットワーク機器により，許可ユーザ以外のネットワーク利用を禁止します。さらに動的VLAN機能とスイッチのアクセスコントロール機能を併用することで，ネットワークレベルで接続先をコントロールすることが可能です。

スイッチによる認証機能はいくつかありますが，このなかでもIEEE 802.1Xの規格に準拠した方式が一般的です。UNIVERGEではこのIEEE 802.1X対応のUNIVERGE QX-Sシリーズと認証サーバUNIVERGE RD1000を組み合わせた認証VLANらくモデル（**図2**）をリリースしています。

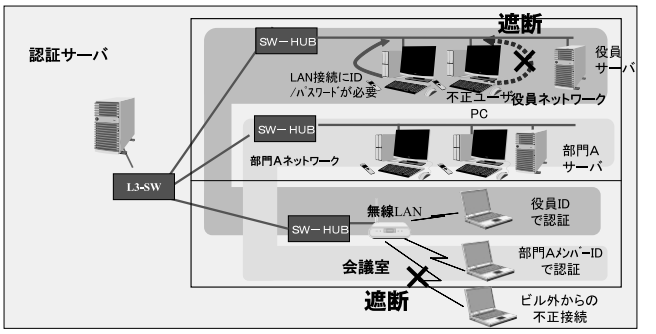

図2 認証VLANらくモデルのイメージ
Fig.2 Authenticated VLAN “ RAKU-Model ”.

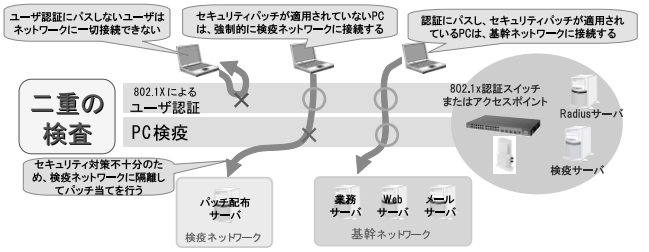

図3　PC検疫ソリューション感染防止のイメージ
Fig.3　PC quarantine solution (infection prevention).

3.3　PC検疫ソリューション

認証VLANらくモデルを利用することで不正ユーザによる接続を制限することができますが，ウイルス・ワーム対策としてはまだ不十分です。接続した正規ユーザがクライアントパソコンの運用をきちんと行っていないと，ウイルスやワームに感染することを防ぐことができないからです。そこでネットワーク接続時にPCのセキュリティレベルをチェックし，接続可否を行う検疫システムが有効です。

UNIVERGEでは認証VLANらくモデルとPCのパッチ適用状況を管理可能なCapsSuiteを組み合わせたPC検疫ソリューション感染防止（**図3**）をリリースしています。PC検疫ソリューション感染防止では，ネットワーク接続時に，802.1Xによるユーザ認証に加えてPCのパッチ適用状況を検査します。ここで必要なパッチが適用されていない場合，該当端末は検疫ネットワークに隔離されます。検疫ネットワークからはパッチ配布サーバのみ接続可能で業務ネットワークには影響を与えない仕組みになっていて，社内ネットワークへのウイルス・ワーム感染を防止することができます。

多くの他社検疫システムは隔離機能のみを提供しているのに対し，UNIVERGEのソリューションは治癒機能も提供している点が特長として挙げられます。検疫ネットワークに接続されると，未適用パッチ一覧が画面上に表示されるので，そこからエンドユーザは必要なパッチを適用します。これにより最新パッチの適用も徹底させることが可能です。

PC検疫ソリューション感染防止により不正ユーザによるアクセスや既知のセキュリティホールを利用したウイルス・ワームの「感染防止」は可能ですが，ゼロデイアタックのような未知のワームや，検疫通過後にUSBメモリ等で感染ファイルを持ち込んだ場合などの感染拡散防止にはやや不十分です。これを補完する方式としてWormGuard IPシリーズとWebSAM SecureVisor（InterSec NQ30a含む）を組み合わせたPC検疫ソリューション拡散防止（**図4**）が利用できます。このソリューションには以下のような特長があります。

① WormGuard IPシリーズが未知・既知ワームを検知・感染端末を特定
② WormGuard IPシリーズがワームの通信を遮断。同時に，WebSAM SecureVisorへ感染端末情報を通知

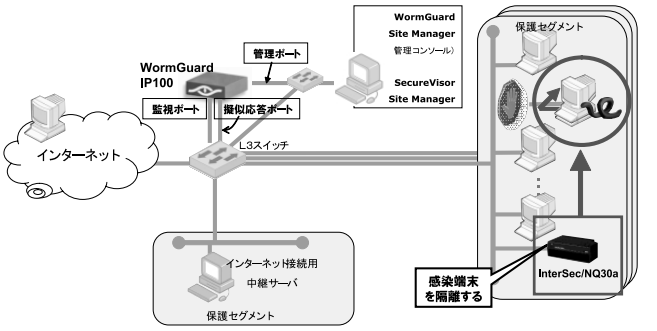

図4　PC検疫ソリューション拡散防止のイメージ
Fig.4　PC quarantine solution (infection control).

③ WebSAM SecureVisorが感染端末を隔離することで，全社的なワームの「拡散防止」が可能

3.4　データ集中化ソリューション

オフィスのデスクワーク用の総合業務端末として一般化しているクライアントPCですが，高度な通信機能，HDの大容量化，携帯性向上が進んだ結果，機密情報と顧客情報を内蔵ディスクに蓄積したままオフィス外へ持ち出すことが容易になり，情報漏えいの危険性が高まっています。

事実，ノート型PCの盗難，置き忘れが原因で大規模な顧客情報漏えい事故がたびたび発生し，平成17年4月の個人情報保護法の本格施行後も，同様な事故が後を絶ちません。

このような状況から端末にデータを蓄えない「シンクライアント」を利用した情報セキュリティのコンセプトが注目を浴びています。

Citrix社のMetaFrameはシンクライアントシステムを実現する代表的なミドルウェアで，従来のクライアントPC内で行っていたアプリケーション環境を複数ユーザまとめてサーバに集約できます。

アプリケーションはサーバ内で動作し，その画面イメージのみをクライアント端末へ送り，端末からは，キーボードとマウスの入力情報がサーバへ送られるため，データの実体はクライアントPCのディスクにもメモリにも残さないで，データの閲覧や更新などの作業ができます。

データ集中化ソリューション（**図5**）が解決しようとす

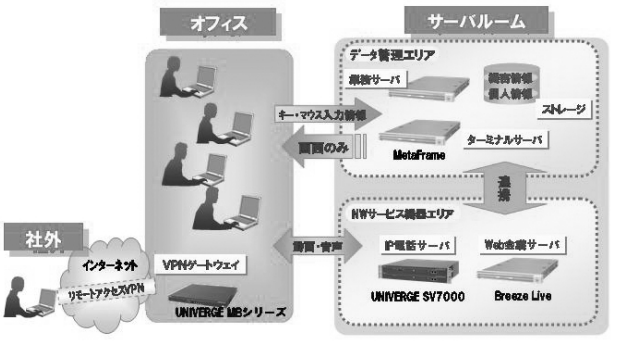

図5　データ集中化ソリューションのイメージ
Fig.5　Image of “ data centralizing solution ”.

る課題は，上記の情報漏えい対策だけでなく，UNIVERGEが提唱するブロードバンドオフィスによる知的生産性の向上をも含みます。

一般に，セキュリティを強固にしていくと操作や環境に制約が多くなり使い勝手が悪くなります。セキュリティと利便性をなるべく高いレベルでバランスさせることが肝要です。

MetaFrameのような画面転送方式は，元来，音声や動画などのマルチメディアの通信には対応しておらず，ソフトフォンやWeb会議，動画コンテンツを満足に利用できません。年々改善されてきていますが，まだ十分使用に耐える性能には至っていません。

データ集中化ソリューションでは，このような課題を解決するため，①重要データは，前記MetaFrameを利用してシンクライアントシステムを構築してアプリケーション環境ごとサーバルーム（データ集中管理エリア）に閉じ込め，②端末には通常のPCを用い，管理者が行うMetaFrameのポリシー設定機能で，データコピー（クリップボード）やプリントアウトの制限を実施，③端末にはMetaFrameと別ウィンドウでソフトフォンやWeb会議クライアントを動作させる，④電子電話帳などアプリケーションに連動したソフトフォンの発呼や，任意の資料を参加者全員で閲覧しながら行うWeb会議を実現する仕組みを提供しています。

電子電話帳に関しては，MetaFrameサーバ上で展開することにより，社外からの利用でもセキュリティを確保します。その上で，ワンクリックで発呼を実現するため，電子電話帳に埋め込まれたcalltoタグの情報と，あらかじめ登録された自ソフトフォン番号をMetaFrameサーバー内のダイアラー経由でIPテレフォニーサーバへ引き渡して発呼要求する機構を実装しています。これにより，社内・社外を問わず，安全かつ快適に電子電話帳を利用することができます。

4．むすび

以上，UNIVERGEオフィスセキュリティの体系と強化ソリューションについて紹介しました。近年，Webアプリケーションの脆弱性をついた攻撃や，メールを経由してウイルスが蔓延するケースが増えていますので，今後Webやメールなどアプリケーションに特化したセキュリティソリューションを開発し，提供していきたいと考えています。

＊ MetaFrameは，Citrix System,Inc.の登録商標です。

筆者紹介

Shinichi Mukouyama
向山　信一　1990年,NEC入社。現在，UNIVERGEソリューション推進本部ソリューション開発部マネージャー。

Kichiro Miyahara
宮原　吉郎　1980年，NEC入社。現在，UNIVERGEソリューション推進本部ソリューション開発部エキスパート。電子情報通信学会会員。

Koji Iizuka
飯塚　幸至　1996年，NEC入社。現在，UNIVERGEソリューション推進本部ソリューション開発部主任。

Haruki Itoh
伊藤　晴紀　1996年，NEC入社。現在，UNIVERGEソリューション推進本部ソリューション開発部主任。