企業音声ネットワークにおけるセキュリティ

作間　哲夫　　濟木　実
斎藤　牧人

2002年に始まったADSLの低価格化と同時に始まった家庭向けIP電話サービスは低料金，無料キャンペーン競争などにより爆発的に普及し，約2年で500万加入にまで広まった。大手通信事業者のIP電話サービス参入や企業向けサービス開始によって，信頼性，品質面でVoIPが実用レベルに達したと広く認識されるようになった。このため，企業の音声ネットワークを全面的にVoIPに置き換えるIP-PBXの導入が急速に進んでいる。IP-PBXはIP電話機が使えるPBXとしてだけでなく，LAN環境で利用が進んでいたe-mail，web，chat，グループウェアなどと連携した新しいコミュニケーションシステムの中核としての役割が期待されている。

IP-PBXの登場により企業ネットワークはデータ系と音声系のネットワークが一つに融合するため，従来に無い音声系ネットワーク特有のセキュリティ対策が必要となる。本稿では最初にデータネットワークのセキュリティ対策について述べ，次に，IP-PBXの導入に伴う音声ネットワークへの新たなセキュリティ技術について解説する 。

企業ネットワークシステム構成動向

従来の企業ネットワークはデータネットワークと音声専用ネットワークが独立していたが，IP-PBXの登場により両者がIPプロトコルのもとで統合したものとなる。すなわち，従来の音声専用ネットワークでPBXと個々の端末を結んでいた回線に代わってイーサネット（LAN）によって結ばれることになる。IP-PBXシステムを導入した場合の企業ネットワークシステム例を**図1**に示す。データネットワークは社内サーバ，PC，インターネットとの境界に置かれるファイアウォール（F/W）およびそれらを結ぶLANで構成される。また，音声ネットワークはデータネットワークのLANを利用し，IP-PBX，課金サーバ，プロビジョニングサーバ，監視サーバなどのサーバとIP電話端末，ソフトフォン搭載PC，既存電話／端末／回線収容装置（LTU），IP電話網接続のためのゲートウェイ（GW），既存PBXを収容するGWなどの端末で構成される。また，音声ネットワークで使用される代表的な通信プロトコルにはIP-PBXと端末間の呼制御を行うSIP（Session Initiation Protocol），端末間の音声通信を行うRTP（Realtime Transport Protocol）の他に端末の情報設定を行うDHCP（Dynamic Host Configuration Protocol），TFTP（Trivial File Transfer Protocol），障害監視や保守用のSNMP，TELNET（SSH）などが使用される。

データネットワークのセキュリティ技術

音声サービスとデータサービスが統合した企業ネットワークで基盤となるデータネットワークで用いられるセキュリティ対策について以下に述べる。

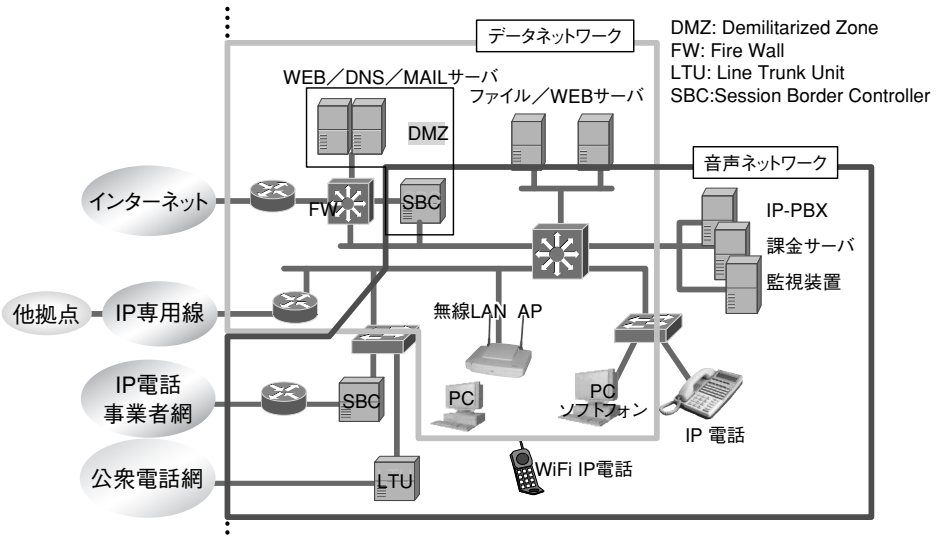

図1　企業ネットワークシステム

(1) 不正侵入・不正アクセス対策

不正侵入ではインターネットからの侵入，無線LANからの企業システム外部からの侵入を対策する必要がある。

NAPT（Network Address Port Translation）は社内で使用するローカルIPアドレス／ポートと社外に見せるグローバルIPアドレス／ポートを変換する。さらに，社内で使用するIPアドレス／ポートを隠蔽することができるため，社外からの不正侵入を防止することができる。また，F/Wは指定したルールにもとづいてパケットを通過させたり，廃棄したりする。ルールでは通過／廃棄するパケットのIPアドレス，TCP/UDPポート番号，LANインタフェースのなどを指定することができる。また，インターネットからの特定のアクセスを許可する非武装地帯DMZ（Demilitarized Zone）とインターネットからのアクセスを許可しない社内LANを分離することができる。これによりインターネットに公開するWebサーバ，FTPサーバ，メールサーバ，DNSサーバなどをDMZに設置することにより，サーバの公開と社内LANへの不正アクセスを防止することができる。なお，F/Wは基本的に既知の攻撃を防御するものであるが，最近では未知の攻撃，異常を検知するIDS（Intrusion Detection System）やFW機能と連携して不正パケットを排除するIPS（Intrusion Prevention System）の導入も進んでいる。

(2) 情報の改ざん・ねつ造対策

無線LANの標準であるIEEE802.11ではセキュリティに関してWEP（Wired Equivalent Privacy）を規定しているが，共有暗号キーが短い，暗号キー列作成に使われるIV（Initial Vector）が暗号化されずに交換される，IVの動的変更の規定がない，MACアドレスが暗号化されずにブロードキャストされるなどの脆弱性があるため[1)]，通信内容の傍受，アクセスポイントの乗っ取り，LANへの不正侵入などの恐れがある。これらの問題を改善したIEEE802.11iが6月に承認された。Wi-Fiアライアンスではこれを先取りしたWPA（Wi-Fi Protected Access）を規定しているが，IEEE802.11iの承認を受けてWPA2として9月より相互接続認定の開始を発表した。無線LANアクセスポイント（AP）ではWEPとWPAを混在して使用できないため，すべての端末をWPA対応製品に置き換える必要がある。

(3) なりすまし対策

インターネットから社内ネットワークへの接続では単純なパスワード認証や毎回パスワードが変わるワンタイムパスワードが広く利用されている。最近ではICカードや指紋などの生体認証の利用が始まっている。社内ネットワークへの接続後にはメールサーバやファイルサーバなど各サーバ／サービス利用時にパスワード認証される。IEEE802.1xは認証された端末のみにLANへのアクセスを許可することにより，不正な端末がLANにつながることを防止する技術である。LAN SWや無線LAN APに端末を接続する際に端末あるいは利用者を認証する。また，端末や利用者の認証に加えて，最新のOSパッチが適用されているか，アンチウィルスソフトのパターンファイルが最新かなどを確認する製品が登場しており，社内に持込まれるノートPCによるウィルス感染防止対策として期待されている。なお，IEEE802.1xはLAN SWや無線LAN APに直接接続する全装置に対して実施するのが望ましいが，未対応のPCやIP接続プリンタ，ハブの接続などに課題がある。

(4) サーバ攻撃（DoS対策）

DoS攻撃は大量のパケットを送りつけることよりネットワーク機器やサーバのCPUやメモリなどのリソースを消費させその機能を停止させる。インターネットからのDoS攻撃ではインターネットから直接パケットを受けるルータ，F/WおよびDMZのサーバで対DoS設定や過トラフィックのフィルタリング設定などと同時に機器の負荷分散によって対処される。

(5) 盗聴対策

盗聴は通過するパケットを捕らえて解読するものである。インターネット経由での社内LANへの接続ではIPSecやSSL-VPNなどによりパケットが暗号化される。社内の通信ではSWハブを用いてネットワークを構成することにより基本的に盗聴を防ぐことができる。無線LANではIEEE802.11iを導入することにより無線区間の盗聴を防止できる。ただし，SWハブやルータのポートミラーリング設定やLANへのハブの挿入などにより盗聴が可能となる。

(6) 脆弱性対策

サーバ／PC用OSやネットワーク機器の脆弱性が公表され，その脆弱性を利用した不正侵入，DoS攻撃，ウィルス・ワームが発生するようになった。このため脆弱性の公表と同時に発表されるパッチや回避策を処置する。

音声・データネットワーク統合上のセキュリティ課題

データネットワーク単独の場合にはさまざまなセキュリティ対策がとられてきたが，音声ネットワークとデー

タネットワークを統合する上で以下のような課題がある。

①多くの企業で社内からインターネットへのwebやftpアクセス，インターネットからのメール受信が許可されているため，悪意ある危険なプログラムを意図せずにPCに取り込み，実行している可能性がある。CDやDVDなどの媒体からからも同様である。
②必ずしも全てのPCにOSの脆弱性に対する最新パッチが適用されていない。あるいは，駆除されていないウィルス・ワームが存在し活動している可能性がある（**図2**）。
③音声通信で使用するRTPのポート番号はSIPによる呼制御の段階で決まるが，F/Wはあらかじめ通過を許可するパケットを指定する必要があるため，RTPで使用する全てのポートを通過許可せざるを得ない。
④NAPTはトランスポートレイヤでのアドレスを変換するが，VoIPの呼処理で使用するSIPのアプリケーションレベルのアドレス変換に対応できない。

また，悪意あるプログラムやウィルス・ワームによる問題は顕在化した場合には対処されるが，PCやネットワーク機器の高性能化，LANの高速化によって相対的に被害が小さければ見過ごされる恐れがある。音声ネットワークではIP-PBXやIP電話端末の機能停止に至らずとも，リアルタイム性を要求されるために通話品質の悪化として影響を及ぼす恐れがある。

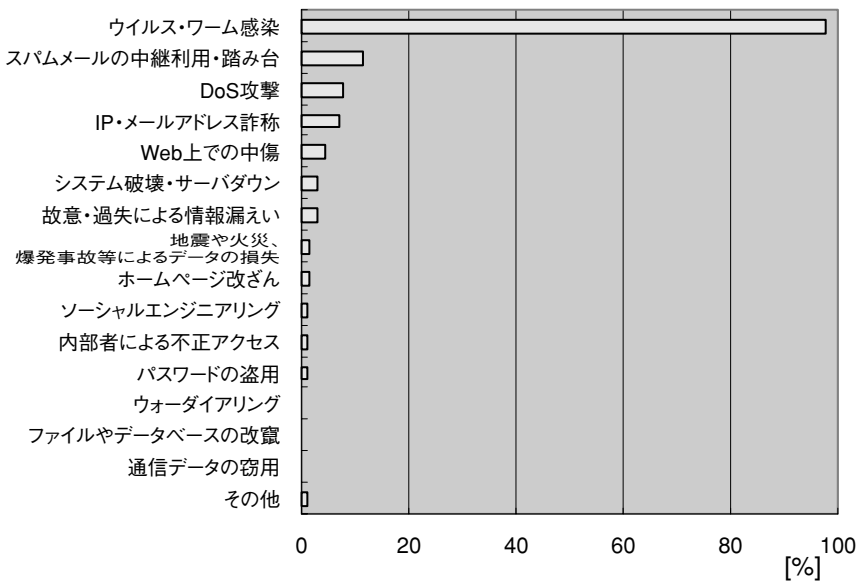

図2　侵害事案の内容
出展：総務省「情報セキュリティに関する実態調査」[2)]
侵害事案のあった上場企業267社の侵害事案の内容

音声サービスセキュリティ対策

前章で述べたデータネットワークでのセキュリティ対策に加えて，音声ネットワーク特有のセキュリティ対策について以下に述べる。

（1）音声／データネットワークの分離

一つの物理的なLANを仮想的に独立した複数のLANに分離するVLANを使って音声ネットワークとデータネットワークを分離することができる。音声用VLANには端末とIP-PBXのみを収容する。PC用ポートを備えるIP電話端末製品ではPC用ポートからの通信とIP電話からの通信は別VLANを割当てる必要がある。データ用VLANからの不正パケットの侵入を防止し，音声用VLANにはVoIP関係のパケットだけが通信されるため，音声ネットワークのセキュリティを高めることができる。

ソフトフォン搭載PCは一般のPCとしてもIP電話としても使用するため，VoIP関連パケットだけを通信する音声用VLANに収容することはできない。ソフトフォン搭載PCはデータ用VLANに収容し，音声用とデータ用のVLAN間はVoIP関連パケットのみを通過するようネットワーク機器を設定する。

（2）不正侵入対策

VoIPに対応した不正侵入対策ではSBC（Session Border Controller）が使用される。SBCは**図1**に示すように社内外ネットワークの境界に設置され，VoIPに対応したNAPT/ALGやF/W機能を提供する。NAPTがトランスポートレイヤでのIPアドレス／ポート番号を変換するのに対して，アプリケーションレベルゲートウェイ（Application Level Gateway：ALG）ではアプリケーションレベルでのIPアドレス／ポート情報を変換する。また，音声パケットを運ぶRTPプロトコルで使用するポート番号はSIPによる呼制御で動的に決定される。このため，SBCではSIPプロトコルに関連づけてRTPパケットのローカルネットワークのプライベートアドレスとポート番号を，インターネットなどで使用するグローバルアドレスとポート番号に変換する（NAPT）。

F/W機能ではRTPポートを動的に

開閉する。初期状態では全てのRTPポートは閉められている。SBCは通過するSIPパケットを監視し，呼の成立を検出すると対応するRTPポートを開け，呼の終了を検出すると対応するRTPポートを閉める。これにより未使用のRTPポートを閉じることができセキュリティを高めることができる。

携帯電話のワン切りやスパムメールによる被害が発生しているが，これらに相当するものがIP電話やSIPアプリケーションの分野にも登場する可能性が高い。これらに対応するには着呼頻度の計測と一定頻度以上の着呼要求の破棄，発呼者ブラックリストの作成とリスト該当者からの着呼要求の破棄によって不必要なVoIPパケットが社内に流れ込まないようSBCで対応する必要がある。

(3) なりすまし対策

IP電話機，WiFi電話機をIEEE802.1x対応とすることによりIP電話機のなりすましを防止する。

(4) 盗聴対策

音声通信には端末ー端末間の音声通信と端末とIP-PBX間の呼制御とがありそれぞれで暗号化に関するRFCが規定されている。音声通信の暗号化にはSRTP（Secured RTP），呼制御ではSIPの場合S/MIME（S/MIME Version 3 Message Specification），TLS（Transport Layer Security）の使用がRFC3261で規定されている。IP電話機やIP-PBXでこれらに対応することにより盗聴を防止できる。

(5) DoS対策

DoS攻撃の多くは先に述べた音声／データネットワークの分離により防止することができる。しかし，呼制御プロトコルを使った攻撃，正規の端末による高負荷状態，端末あるいはネットワーク機器の故障／バグによる異常トラフィックへの対応が必要になる。

データサービスとリアルタイム性の要求される音声サービスでは高負荷状態での対応が異なる。たとえばWebサーバでは高負荷状態によりブラウザ画面の更新が遅くなった場合，利用者は応答を待つか中断するのが一般的である。一方，音声サービスでは高負荷状態によって呼び出し音が出るまで（無音）の時間が長くなると，利用者は再発呼を繰り返すため，高負荷状態で更に負荷が増す。このため，電話交換システムでは過負荷時に通話状態回線の切断要求は受け付け，新たな発呼要求を拒否する必要がある。

従来のPBXでは電話機を収容する個々の回線を監視することにより端末からの要求を検出する。このため，PBXのCPUやメモリなどの状況によって過負荷状態を検出すると，発呼監視処理を停止することによりCPUの負荷を上げることなく新たな要求の受付を止めることができた。IP-PBXでは全てのIP電話機からの信号がIPパケットとしてLANインタフェースから入力されるため，受信した後にしか破棄すべきものかどうかを判断できない。このため，DoS攻撃や異常トラフィックによる過負荷状態でもIP-PBXは全てのパケットを受信し，CPUやメモリリソースを消費することになる。

この問題の解決としてIP-PBXの前段にアプリケーションレベルでのトラフィック制御装置を置くなど，今後，大規模IP-PBXシステムを構築するに向けてアーキテクチャとして対策が必要になる。

ま と め

企業ネットワークのセキュリティ対策はコスト，安全性，利便性のトレードオフがある。IP-PBXは，企業の重要な通信基盤であった電話通信機能を提供するものであるため，その導入にあたっては，既存のデータ系ネットワークのセキュリティポリシーに応じた慎重なセキュリティ対策が必要となる。

また，音声だけではなく，映像，データと複合したセキュリテイ対策が重要になるものと考える。弊社は既に情報通信融合ソリューションの核であるSS9100システムIP-PBXへセキュリテイ対策に鋭意取り組み，お客さまに安心，安全なソリューションをご提供する所存である。

◆◆

■参考文献

1）Joon S. Park, Derrick Dicoi: “WLAN Security : Current and Future” IEEE INTERNET COMPUTING, Vol.7 No.5, pp.60–65, 2003
2）総務省: “情報セキュリティに関する実態調査” 2004年7月

●筆者紹介

作間哲夫：Tetsuo Sakuma. IPソリューションカンパニー ソリューション開発本部 インキュベーション推進部
濟木実：Minoru Saiki. IPソリューションカンパニー ソリューション開発本部 インキュベーション推進部
斎藤牧人：Makito Saitou. IPソリューションカンパニー ソリューション開発本部 インキュベーション推進部