Part 3 技術解説[ネットワーク編]

IPセントレックスにおけるセキュリティ向上のポイント

NTTコミュニケーションズ ブロードバンドIP事業部
VoIPサービス部 担当部長　小島秀爾(こじま・しゅうじ)

企業ネットワークの新しい選択肢として、IPセントレックスサービスに注目が集まっている。NTTコミュニケーションズの小島秀爾氏に、キャリアネットワーク側の対策も含めたIPセントレックスのセキュリティについて解説していただく(編集部)。

昨今のブロードバンドアクセスの伸びを背景に、個人も企業もIP電話に高い関心を示している。

一般的に「IP電話」と呼称されているものは、個人向けのインターネット電話と企業向けのIPセントレックスに大別されるが、各々におけるトラブル対策としては、次のようなことを考えなければならない。

・個人の場合:完全にインターネットにさらされているため、IP電話を利用するうえでも、世の中を騒がしているウィルスの脅威に対する対策が施されている必要がある。

・企業の場合:ほとんどがプライベートアドレスで運用され、NATやファイアーウォール機能が具備されているので、IP電話固有のセキュリティ対策をさらに施すためにどうすればよいかを考慮する必要がある。

本稿では、企業向けのIPセントレックスに焦点を絞って、セキュリティを中心とした課題のクリア方法について述べることにする。

IP電話における課題と解決策

まず、サービス品質の観点からIP電話の課題を考えてみると、

①接続品質:つながりやすさ、ダイヤルトーン、ビジートーンなどの応答時間等

②音声品質:音の大きさ、音質(特に高音域)、途切れの有無等

③システムの安定性:サービス中断がないこと、システムメンテナンスの停止の有無等

④緊急呼の扱い:警察・消防等への接続性

などがあげられる。

これらの中で、特に音声品質については、非リアルタイムで通信に多少の遅延があっても問題はないデータに対して、音声はリアルタイムであり、通信の遅延がそのまま品質に影響する。しかも、人間の感覚は鋭敏で音質にかなり敏感であるため、品質の劣化が大きな問題となる可能性もある。そこで、品質確保の秘訣としては、以下のようなことを考慮する必要がある。

●アクセス回線帯域

遅延時間による音の途切れを解消するには、上り下り双方向での帯域確保が重要となる(帯域の小さいほうに従属する)。

●優先制御

データ通信との混在のケースでは、音声の優先制御またはルートの分離が有効。経験的には、メガビットクラスの帯域があれば4チャネル程度の通話には支障ない(ただし、全帯域を消費するような特殊なファイル転送等を行っていないこと)が、安心のためには優先制御があったほうがよい。IP-VPNは帯域制御(優先制御)がしやすいが一般的に帯域が狭く、広帯域にすると高価になる。また、広域LANでも優先制御サービスが可能になった(NTTコミュニケーションズでは、2月20日から「e-VLAN」において優先制御機能を提供)。

●音声圧縮と無音処理

少ない帯域でも良好な音声コーデック(G.729等)の利用や無音圧縮などの工夫もある。ただし、チューニングが必要。

これらの要素を踏まえると、現状でIPセントレックスを利用する場合には、SE/SI作業が必須となる。

次に、IPセントレックスサービスのセキュリティという点を捉えてみると、想定される危険因子としては大きく分けて以下の3つが考えられる。

(1)CA(Call Agent)自体への攻撃(内容改ざん等)

LANへの侵入、オペレーションシステムへの攻撃、データ流出等

(2)利用者への攻撃(なりすまし)

ユーザー側LANへの攻撃、踏み台、なりすまし(誤課金)、盗聴等

(3)サービスの停止(DoS攻撃)

輻輳の発生、ポートスキャン、バッファオーバーフロー等

これらに対する対策として、大別すると3つの対策因子が考えられる(**図1**参照)。

a)CA自体での防御(ネットワーク側)

・相手IPアドレスの区別、ポートの管理、Telnet/FTP等のセキュリティ強化

・脆弱性のあるハード/OSを用いない等

b)ルーター等のネットワーク設計(ネットワーク側、ユーザー側)

・ルーティング情報の配信先限定、適切なOS/ファームのアップデート

・アクセスリスト等のメンテナンス、ping/trace route等への対応、IPアドレスの変換

c)ユーザー側ネットワークでの防御

・データ/音声のネットワーク分離、グローバル-プライベートのNAT利用、IPsec等の暗号化/IP音声暗号化/コーデック等

図1　IPセントレックスサービスでのセキュリティ/品質確保の実現例

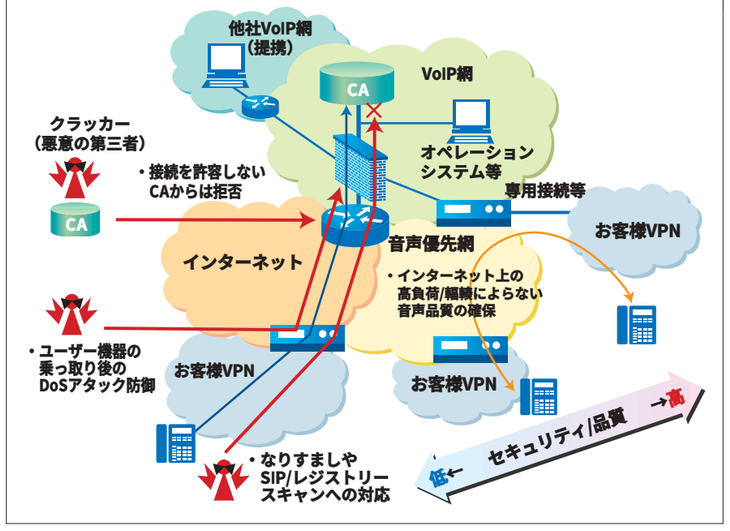
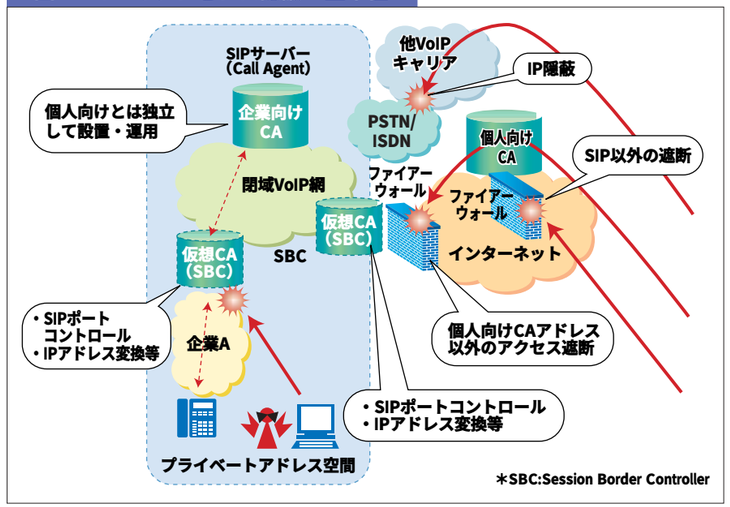


図2　CAのプレゼンス隠蔽・堅牢性



ネットワーク側のセキュリティ対策

では、ネットワーク側と(ユーザーの)LAN側に分けて、それぞれどのようなセキュリティ対策を施すべきかを具体的に紹介していこう。

まず、ネットワーク側で実施すべきセキュリティ対策としては、大きく4つの因子が必要と考えられる。

)CAのプレゼンス隠蔽

CAの存在すなわちIPアドレスを隠す、該当アクセスを遮断するという対策。具体的には、①仮想CA(セッションボーダーコントローラー:SBC)をネットワークの境界に設け、ダイレクトにCAにアクセスできないように遮断、②ファイアーウォールでSIP以外を遮断したりルートチェック

特集1 ユーザーを困らせない IP電話トラブル対策