

標準のファイアーウォールでは、VoIP アプリケーションに対するセキュリティが不完全です。VoIP アプリケーションの設置や操作は非常に複雑で、VoIP ネットワークが直面している脅威に対し完全に対処する事ができません。このアプリケーションノートでは、それらの問題点について述べます。

ボイスオーバーIP (VoIP) アプリケーション、およびそれに関連するユニファイドメッセージングアプリケーションは、非常に複雑です。この複雑さは、提供するサービスのレンジが広い事とこれらのアプリケーションが直面しているセキュリティに対する脅威の両面から明白です。セッション開始プロトコル (SIP) は、VoIP をはじめビデオやインスタントメッセージ、他のユニファイドメッセージングアプリケーション等幅広く利用されています。このアプリケーションノートでは、このような複雑な状況下の中で、特に、SIP ベースのアプリケーションを使用する場合、通常のファイアーウォールにセキュリティを委ねる事がいかに危険であることを説明します。

私達の業界では、IP レベルのセキュリティについては、すでに一般的に周知されており、ほとんどのファイアーウォール製品は、WEB や e-mail などの標準アプリケーションを安全に使用できる事を保証しています。しかしながら、VoIP はこれらの標準アプリケーションとは異なり、標準ファイアーウォールでは、VoIP セキュリティの完全なソリューションにはなりません。

この理由を理解するために、私達は VoIP システムが直面している脅威の中身を知る必要があります。これらの脅威は、主に次の 3 つのグループに分けられます。

1. IP ネットワークレベルの脅威：

WEB や e-mail が直面しているような他の一般のアプリケーションが直面しているのと同様の脅威

2. DOS 攻撃や、コールディスラプションアタックを含むアプリケーション及びプロトコルレベルの脅威：これらのアタックは、サービスの品質に重大な影響を与え、最悪サービス停止の引き金になる可能性があります。

3. 権限の無いコールモニタリング (盗聴)、コールフルディング、迷惑電話を含むコンテンツレベルの脅威

料金詐欺などの他の脅威は、アプリケーションとコンテンツの両方のグループになります。

ファイアーウォールは IP ネットワークレベルの脅威に対して有効です。しかしながら、これらは汎用の装置であり、多くの場合 VoIP が利用される以前に開発されたもので、それらは VoIP メッセージのコンテンツに対してまで調べることができません。これは、汎用のファイアーウォールが VoIP のアプリケーションやコンテンツレベルの脅威に対し、何ら有効ではない事を意味します。

問題を複雑にさせるのは、SIP と他のプロトコルの違いによります。VoIP は一般のファイアーウォールのモデルに適合しません。全てのファイアーウォールは、ネットワークアドレス変換 (NAT) を行います。これは、一方ではセキュリティのため、もう一方では、プライベートな LAN ネットワークアドレスと公のインターネットアドレスを変換し、相互接続をするために行います。ファイアーウォールを通り抜ける際に、NAT によってパケットのソースアドレスや、送付先アドレスを変換します。問題は、プロトコルの中に含まれるパケットにネットワークアドレスを埋め込む際に発生します。汎用のファイアーウォールは、パケットコンテンツを調べないので、これらの埋め込まれたアドレスを翻訳することができません。つまり、VoIP パケットでは、埋め込まれたアドレスは呼び出す際のエンドポイントとして定義されるため、この状況下では結果的に相手呼び出すことができません。

これは、汎用のファイアーウォールがアプリケーションやプロトコルおよびコンテンツに対する脅威から VoIP システムを保護する事ができないだけでなく、NAT 変換により、VoIP システムに必要なプロトコルが壊される事を意味します。VoIP システム設計者は、この問題に対処するために最大限の努力をしなければなりません。これらの問題はファイアーウォールの設定を、音声及びデータアプリケーションの両方において適切に動作させると同時に、双方のセキュリティを保たなければならないという、動作とセキュリティの妥協を生じさせる点です。このリスクは、例えば

自宅から DSL ルータを経由して電話をする場合や、会社のファイアーウォールを通して IP-PBX から電話をかける際など、一つのファイアーウォールや NAT ゲートウェイを VoIP アプリケーションが通過した際に必ず発生します。VoIP 接続が 2 番目の NAT ゲートウェイを通過する時、対処方のいくつかは、NAT 変換を行なうためこの問題が発生します。これは、遠隔 NAT トラバーサルとして知られている問題です。

### SIP におけるファイアーウォール

多くのファイアーウォールベンダーが、“SIP 対応”として彼らの製品を広告しています。しかし、厳密に言えば、“SIP 対応”は SIP レベルのあらゆるコンテンツにおいて、メッセージソースアドレス及び、目的地ネットワークアドレスを適切に変更（上位アプリケーションが処理）できる製品にのみ適用されるべきです。実際には、ファイアーウォールが SIP を通す事ができれば、“SIP 対応”という言葉が使用されているのが現状で、ほとんどのファイアーウォールがこれに当てはまります。完全な“SIP 対応”ファイアーウォールは、NAT 及び遠端 NAT トラバーサルの困難な問題を解決する機能を持っていますが、それでも SIP 特有のアプリケーションや、プロトコルあるいはコンテンツレベルの脅威に対して防御する機能を持っていません。これは、盗聴やコールディスラプション、DOS 攻撃に関する脅威を残す事になります。

### リスク

標準のファイアーウォールや“SIP 対応”と謳っているファイアーウォールで、VoIP や他のユニファイドメッセージングアプリケーションを使用している場合、アプリケーションやプロトコル、コンテンツレベルに対する脅威に対しては、保護されていないため、電話における会話を含め、あらゆる情報交換の機密性や保全性を危険にさらすものです。また、DoS アタックのレンジに対する脅威についても保護されておらず、重大な問題を引き起す可能性が内在しており、最悪サービスが停止する事態を招く恐れもあります。さらに、根本的なプロトコルの複雑さは、VoIP を扱う際のファイアーウォール設定を非常に難しいものにさせるため、設定の方法によっては、他のアプリケーションにも危険が及ぶリスクがある事を意味します。

### UM Labs

UM Labs が開発した SIP セキュリティゲートウェイは、SIP ベースの VoIP 及びユニファイドメッセージングアプリケーションの包括的なセキュリティを提供するために設計された製品です。UM Labs ゲートウェイの中の、エントリーレベルの製品は、ローミングユーザや、ホームワーカーを対象としており、SIP トランクスにセキュアに接続する事を保証する製品です。そして、より大きな企業やサービスプロバイダ用にはその規模に応じた製品を提供します。それぞれの製品は、IP ネットワークレベルの脅威を含め、“SIP 対応”ファイアーウォールや、通常のファイアーウォールではカバーされていない、より高いレベルの脅威についても保護できる機能を兼ね備えています。

| 機能                         | UM Labs | SIP Aware Firewalls |
|----------------------------|---------|---------------------|
| 盗聴対策                       | ◎       | ×                   |
| 妨害電話、冗雑電話対策                | ◎       | ×                   |
| コールディスラプションアタック対策          | ◎       | ×                   |
| SIP レベル DoS アタック対策         | ◎       | ×                   |
| 他のアプリケーション動作を妨害しない VoIP 動作 | ◎       | ○                   |
| Far-End NAT トラバーサル         | ◎       | ◎                   |
| ローカル NAT                   | ◎       | ◎                   |
| IP レベルセキュリティ               | ◎       | ○                   |

より詳細な情報は、WEB サイトをご覧ください。 <http://www.um-labs.com>