

### 管理方法

- セキュアで直観的な Web GUI
- リモート Syslog
- 効率的なソフトウェアのアップグレード方式を採用
- ポリシーベースのコールアーカイブ機能 (要追加ライセンス)

### 仕様

- 1u ラック型アプライアンス
- 4 x Gigabit Ethernet ポート (RJ-45)
- ハードウェア RAID ディスク
- 冗長化とロードバランスの為にクラスタサポート
- 1 x RS-232 コンソールポート
- 1 台で最大 500 同時通話をサポート
- クラスタ構成で、最大 1,000 同時通話をサポート

### 準拠規格

#### ハードウェア

- RoHS
- WEE

#### ソフトウェア

- RFC 3261
- RFC 3711
- RFC 4568
- RFC 2617

### ライセンス形態と出荷時期

- ライセンスは 50 から 1,000 同時通話用から選択可
- 2008 年 9 月出荷予定

### 国内総代理店

株式会社ジーメイジャー・ジャパン  
東京都新宿区歌舞伎町 2-4-14-411  
Email: [info@g-major.com](mailto:info@g-major.com)  
Tel: 03 4590 2779

### ソリューション

UM Labs の RC-4200 は、VoIP やビデオ会議、SIP ベースのインスタントメッセージやプレゼンスベースのアプリケーション等の遠隔 SIP 接続に必要なセキュリティ管理のフルセット機能を持った、非常に費用対効果の高い、SIP セキュリティゲートウェイです。

EC-4200 は、音声とデータを安全に統合するセキュリティ環境を実現するため、SIP アプリケーションや、コンテンツコントロールを行う上で必要なネットワークセキュリティ機能 (ファイアーウォール機能) と、暗号化されたコールセットアップやメディアトラフィックを通過させるゲートウェイとしての両機能を提供します。これらの管理は、シグナリング (SIP) とメディア (RTP) の両方において、認証サービスと共に提供され、すべてのリモート接続のための完全なプライバシーと機密性を確実にします。

EC-4200 は、RAID 技術によりフォルト・トレラント対応がされた 1u のラックマウント型アプライアンスシステムで、2 台以上のシステム構成により、一層高い冗長化を実現します。また、クラスタ構成の EC-4200 では、最大で 1,000 同時通話をサポートします。

### 利点

- リモートユーザ及び SIP トランクにおける包括的なセキュリティを低価格にて実現
- SIP アプリケーションのセキュリティ、管理、暗号化、認証機能を完全な IP ファイアーウォール機能とともに提供できるため、設定を簡単にかつ設置までの時間を極力短縮する事が可能です。
- VoIP アプリケーションレベル専用のゲートウェイ及びファイアーウォールして動作するため、すでに導入済の企業内ファイアーウォールの設定を変更する必要がなく、他のアプリケーションのセキュリティ管理に影響することなく、安心して導入ができます。
- RFC 標準規格に完全適合していますので、あらゆる標準 SIP 規格の VoIP フォンや IP-PBX との相互運用性を持っています。
- ローカル NAT 及びファアード NAT 越えをサポートしていますので、リモートユーザが、サードパーティのファイアーウォールや、他の NAT ゲートウェイを経由して接続している場合でも、特別なプロトコルサポートを必要とする事なくサービスを提供できます。
- クラスタ構成による冗長化とロードバランシングを実現

### 導入

The EC-4200 の強固な IP ファイアーウォール・セキュリティレイヤは、企業内で既に使用されている一般的なファイアーウォールと並行して導入することが可能です。この推奨構成により、既存の企業内ファイアーウォールのセキュリティ設定を変更することなく、セキュアな VoIP 専用チャンネルを提供すると同時に、音声品質を保全することが可能となります。

更に EC-4200 は、別の導入方法として、既存ファイアーウォールの DMZ 内に設定することも可能です。

UM Labs の SIP セキュリティ・コントローラシリーズは、VoIP 及びその他のユニファイド・メッセージング (UM) アプリケーションに対し、簡単かつ費用対効果の高いセキュリティ機能を提供します。各製品は、強固なファイアーウォールグレードによるセキュリティ対応と、アプリケーション及びコンテンツに特化したコントロールを行うことで、VoIP 及び UM に対する全ての脅威に対応します。

## 製品の主な特長

**企業ネットワークへのセキュリティ脅威に対する防御及び制御機能と安全なサービス環境を提供**

### 各種脅威に対する防御機能

VoIP/SIP セキュリティへの脅威

- SIP /RTP DoS 攻撃
- スプーフィング
- メディア異常
- 不正 SIP メッセージ
- 盗聴

IP セキュリティレベルでの脅威

- ステートフル IP ファイアーウォール
- RTP ストリームに対するダイナミック・ピンホール攻撃

### 制御機能

オペレーティングシステム

- ファイアウォールグレード・セキュリティ
- VoIP サービスにおける最適化

### サービスの最適化

NAT 越えサポート

- ローカル NAT
- Far-End NAT 越え (複雑な STUN を使用しないで実現)

### 機密性

- SIP-over-TLS, 最大 256 ビット AES
- SDES 鍵交換による SRTP サポート
- ZRTP 鍵交換による SRTP サポート (要追加ライセンス)
- SRTP ゲートウェイ (終端機能を含む)
- SRTP パススルー
- セキュアラインによる音声通知 (オプション)
- 全ての SIP 要求に対する HTTP ダイジェスト認証

## チャレンジ

今後、広く普及が予想されるユニファイドメッセージング (UM) では、E メールやインスタントメッセージ、VoIP やビデオ会議のように非常に広範囲にわたるアプリケーションを統括しなければなりません。これらのアプリにとって重要なことは、相手ユーザに今応答できるかどうかのシグナルを出せる事と、コールやメッセージを最も効率よくルーティングする方法を確立することです。また、これらのアプリケーションは、全て IP ネットワーク上で動作するものですが、それらのセキュリティ要件は、全く異なっています。

例えば、インスタントメッセージのセキュリティ要件は、Eメールのようなコンテンツフィルタリングや、スパムに対する防御が必要となる一方、VoIP やビデオ会議のためのセキュリティコントロールは、リアルタイムにアプリケーションの種別を認識し、コールフローディングに対する防御や、認証されていないコールをモニタリングする必要があります。

VoIP と UM アプリケーションのセキュリティ要件は、一般目的に使用されている汎用ファイアーウォールが満たしている機能より複雑で、これらのファイアーウォールでは、VoIP や UM に関わる全ての脅威を防ぐ事ができません。複雑な環境を持つ VoIP と UM アプリケーションにとって、真に有効なセキュリティとは、アプリケーションとコンテンツの防御に特化した機能と、強固なファイアーウォール・セキュリティ制御とが一体となったものでなくてはなりません。

UM Labs のセキュリティ・コントローラは、全てのタイプのネットワークにおける VoIP 及び UM に関するセキュリティを、費用効率よく配置できるように設計されています。

### ビジネス要件

VoIP と UM アプリケーションが提供する主な恩恵の1つは、音声電話とビデオ会議機能を他のメッセージングアプリケーションと統合して、組織全体にその統合サービスを広げられる点です。VoIP サービスはあらゆる SIP アドレスに対し直接コール及びトランク接続コールができるため、標準の電話サービスと置き換える事が可能になります。

この事による利点を最大限に引き出すためには、2つの要件が重要となります。第一に、音声とデータネットワークとの完全な統合。第二に、既存のセキュリティに対し VoIP トラフィックを通すように変更し、SIP トランクへの接続を社外にいるユーザやリモートユーザに対して許可するにしなければなりません。しかしながら、現在の多くの VoIP システムでは、この設計と実装を両立できない為、音声とデータを別々のネットワークに実装するか、もしくはファイアーウォールが VoIP トラフィックを遮断するように設定してしまうため、VoIP アプリが正常に動作しないという問題が起っています。