

## Cisco IOS Firewall の SIP 拡張機能によるセキュア ユニファイド コミュニケーションの実現

シスコ ユニファイド コミュニケーションの完全性および可用性の向上

### 概要

多くの企業ではユニファイド コミュニケーション(単一ネットワーク インフラストラクチャ上でのデータ、音声、および映像の統合)を利用することで、通信コストを大幅に削減すると同時に、従業員の生産性とモビリティを高めることに成功しています。ユニファイド コミュニケーション システムを保護してサービスの可用性とシステムの完全性を維持することは、このようなユニファイド コミュニケーションの利点を実現する上で非常に重要です。シスコではシステムの保護を強化するため、シスコ ユニファイド コミュニケーションのすべてのアプリケーションとシステムに複数のセキュリティ対策を導入することを推奨しています。ユニファイド コミュニケーション システムの主要な構成要素には、エンドポイント、コール制御、アプリケーション、そしておそらく最も重要な統合型 IP ネットワーク インフラストラクチャの 4 つがあります。ルータをベースにしたシスコのセキュリティ ソリューションは、これら 4 つの構成要素のセキュリティ保護を可能にし、セキュアなユニファイド コミュニケーション アーキテクチャを構築する際の安定した基盤として機能します。Cisco IOS® Firewall では、ユニファイド コミュニケーションの構成要素の完全性と可用性を維持するのに役立つシステムのセキュリティとポリシー制御機能が利用できます。

### 利点

シスコのセキュア ユニファイド コミュニケーションには、次のような利点があります。

- シスコ ユニファイド コミュニケーションのセキュリティ上の脅威の軽減: セキュリティ上の脆弱性を悪用しようとする行為、および企業のセキュリティ ポリシーや業界のベスト プラクティスと異なる動作を見逃しません。
- シスコ ユニファイド コミュニケーションの完全性の向上: 通信要求が正しいものであることを確認し、ユニファイド コミュニケーション システムの主要な要素を保護します。
- システム可用性の維持: 主要なユニファイド コミュニケーション サービス(通信ゲートウェイや基盤となるネットワーク インフラストラクチャなど)で、高い可用性や、サービス停止を狙った攻撃への耐性を維持するのに役立ちます。
- ネットワーク管理と IT スタッフの生産性の向上: 一貫性があり、効率的なシスコ ユニファイド コミュニケーションのセキュリティ ポリシーと手順の実施が企業内で可能になります。
- シスコ ユニファイド コミュニケーションの総所有コスト(TCO)の削減: 一貫性のあるセキュリティ コントロールを導入(たとえば、リモート サイトのセキュリティとユニファイド コミュニケーションを共通のデバイス上に統合)することで、ユニファイド コミュニケーション システムの操作手順を改善します。

## SIP

Session Initiation Protocol(SIP)は、1人または複数の参加者とのセッションの確立、変更、および切断を行うアプリケーション層の制御(シグナリング)プロトコルです。これらのセッションには、インターネット電話、マルチメディア配信、およびマルチメディア会議などが含まれます。SIPはHTTPに類似した、要求/応答型のトランザクションプロトコルです。各トランザクションは、サーバで特定のメソッド(機能)を呼び出す要求と、1つまたは複数の応答で構成されます。

SIPではプロキシサーバを使用し、ユーザの現在位置への要求のルーティング、サービスを使用するユーザの認証と許可、プロバイダーの呼ルーティングポリシーの実行、およびユーザへの各種機能の提供を行います。SIPは異なる複数のトランスポートプロトコル上で動作します。

### Cisco IOS Firewall による音声セキュリティの強化

Cisco IOS FirewallのSIP保護はCisco IOS Firewallの拡張機能で、RFC 3261に準拠したSIPトラフィックの検査と制御を行うことができます。このSIP保護機能は、重要なシステムリソースの脆弱性を悪用する際に使用される不正なSIPシグナリングや要求が、有効なSIPエンドポイントや呼制御リソースに悪影響を及ぼさないようにします。不正パケット(プロトコルファジングともいう)はユニファイドコミュニケーションシステムを悪用する代表的な手段です。Cisco IOS Firewallでは、これらの不正パケットをフィルタリングし、システムの悪用を効果的に防ぎます。

Cisco IOS FirewallのSIP検査はプロトコル適合性の検査だけでなく、きめ細かなアプリケーションポリシーの適用にも役立ちます。Cisco IOS FirewallのSIP検査には、許可されたサービスだけを使用できるようにする各種ツールが用意されています。また、さまざまなフィルタリングオプションを使用して、ネットワークアドレスだけでなく、ユーザや電話番号に基づいてポリシーを適用することができます。このように、Cisco IOS FirewallのSIP検査はユニファイドコミュニケーションに完全に対応したセキュリティプラットフォームとして利用できます。

Cisco IOS FirewallのSIP保護は、SIPの各種セキュリティ要件に対応し、以下の方法でシスコユニファイドコミュニケーション製品ラインの新機能のサポートを向上させます。

- 不適切または悪意のあるトラフィックの制限: Cisco IOS FirewallのSIP保護は、必須ヘッダーフィールドの遵守、許可されていないヘッダーフィールドの制限、各メッセージのコンテキストにおけるヘッダーパラメータの有効性の確認、および未知のSIPメソッドへの設定可能なポリシーの適用を通じて、不正なトラフィックを利用した攻撃が成功する可能性を減少させます。
- 管理の容易性を保証: Cisco IOS FirewallのSIP検査では、構成の変更が必要になった場合に、SIPイベントやSIPメッセージに関するSyslogメッセージを提供することで、新しいメソッドや拡張機能の設定、動的な追加を行うことができます。
- SIPの機能を拡張する新しい規格に対するサポートの追加: SIP-TCP、Session Description Protocol(SDP; セッション記述プロトコル)のグループ化(RFC 3388)、sip-outbound(draft-ietf-sip-outbound)、代替ネットワークアドレスタイプ(RFC 4091)、非対称ルーティングのサポート/rport(RFC 3581)、およびSIPマルチパートMIME(Multipurpose Internet Mail Extensions)
- Cisco CallManagerのアップグレードおよびIP-IPゲートウェイバージョンのサポート: Cisco Unified CallManagerバージョン5およびCisco Unified CallManager Expressバージョン4.0の要件に対応できるようにSIPサポートをアップデートし、Cisco CallManager Express v3.xおよびCisco CallManager v4.x以上と整合性のあるCisco IP-IPゲートウェイバージョンとの相互運用性を提供します。

Cisco IOS Firewall の SIP 保護は、次の方法を使用して DoS 攻撃を防ぎます。DoS 攻撃によってリソースが枯渇すると、ユニファイド コミュニケーションの音声システムが中断してしまう可能性があります。

- SIP INVITE および REGISTER メッセージのレートリミット
- SIP メッセージ総数のレートリミット
- アクティブ コール数の制限

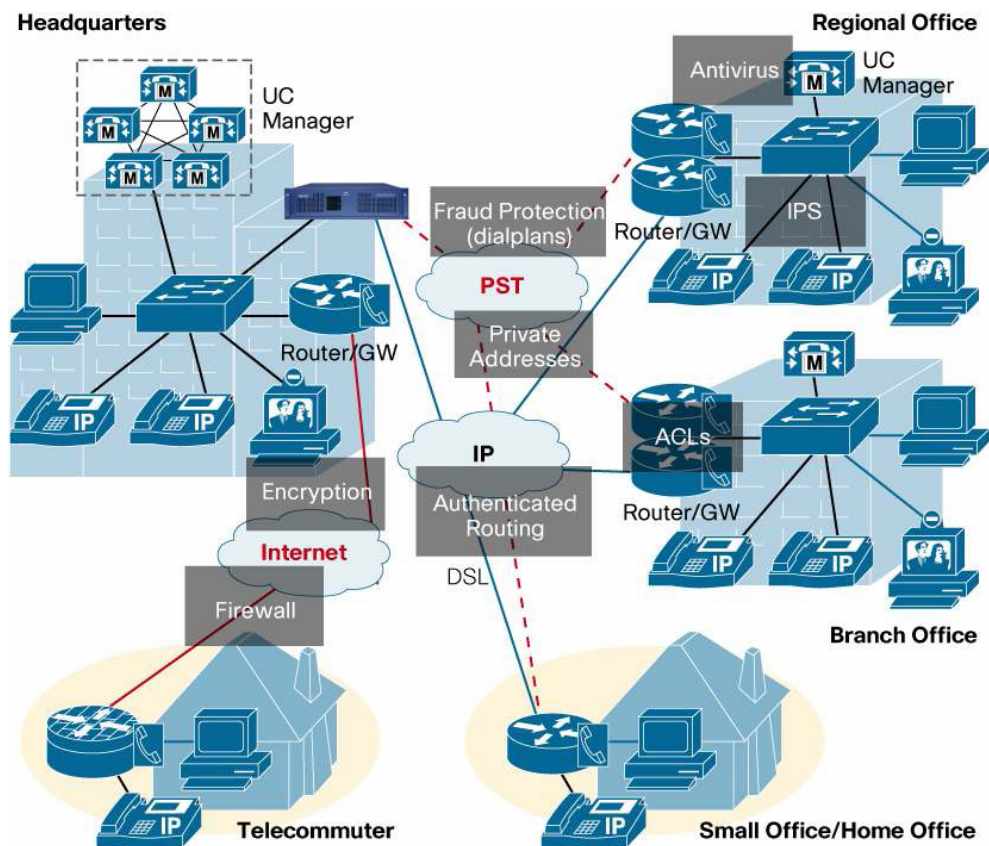
SIP アプリケーションおよび検査制御では、SIP アプリケーションのアクティビティをきめ細かに制御できます(表 1)。

表 1 SIP アプリケーションおよび検査制御による SIP アプリケーション アクティビティの詳細な制御

機能	利点
発信者および着信者のブラックリスト/ホワイトリスト	通話先を制限することにより、不正な通話料金発生の可能性を軽減する
SIP メッセージのフィルタリング: <ul style="list-style-type: none"> <li>• メソッド(またはメソッド グループ)</li> <li>• Uniform Resource Identifier(URI; ユニフォーム リソース識別子)または URI グループ</li> <li>• SIP バージョン</li> <li>• SIP ヘッダー フィールド</li> </ul>	問題がないことがわかっているコンテンツへの SIP メッセージを制限して、呼び出しリソースやエンドホストへの攻撃を抑制する
Via ヘッダーの IP アドレスや名前に基づく SIP メッセージのフィルタリング機能	特定の DoS 攻撃を防御し、発信元または宛先のエンドホストを外部から保護する
エンドポイントのソフトウェア バージョンの非開示	攻撃者がホストのフィンガープリントから脆弱性を発見するような偵察活動を防止する
コンテンツ長と実際のパケット長のクロス チェック	バッファ オーバーラン/アンダーラン攻撃の可能性を軽減する
以下を指定する機能 <ul style="list-style-type: none"> <li>• 総メッセージ長に基づく SIP メッセージ</li> <li>• 最小/最大コンテンツ長</li> <li>• メソッド、URI、Via ヘッダー、全ヘッダーなどの各種フィールドの最小/最大長</li> </ul>	バッファ オーバーフローおよび DoS 攻撃を制限し、きめ細かなアプリケーション制御を可能にする
コンテンツ タイプに基づくメッセージ フィルタリング機能	SIP で伝送されるコンテンツ タイプを管理し、不適切または悪意のあるデータを伝送する可能性のある不要なコンテンツ タイプをフィルタリングする
インスタント メッセージングの無効化機能	望ましくない SIP インスタント メッセージング アプリケーションの動作をブロックする

図 1 は、セキュア ユニファイド コミュニケーションで、推奨されるマルチレイヤ アーキテクチャを示しています。

図 1 シスコが推奨する、セキュア ユニファイド コミュニケーションのマルチレイヤ アーキテクチャ



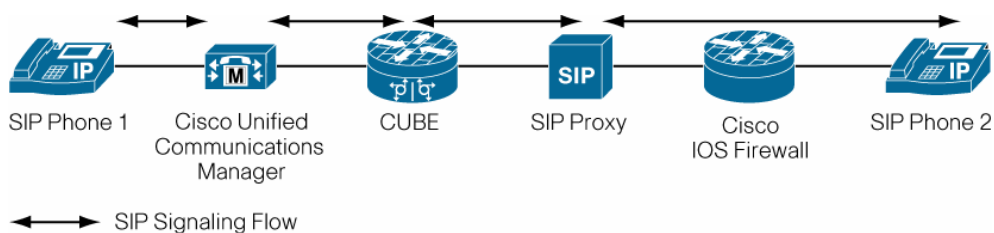
**構成例**

以下の構成例は、Cisco IOS Firewall がユニファイド コミュニケーションの構成要素 (Cisco Unified Communications Manager、Cisco Unified Border Element、およびエンドポイントなど) を保護する上で重要な役割を果たしています。

**構成 1: SIP トランク ベース接続**

これはサービス プロバイダーの SIP トランクを使用してリモート ブランチ サイトへのアクセスを提供する標準的な構成です (図 2)。Cisco Unified Border Element は、サービス プロバイダーが提供する SIP トランク サービスを使用して、本社サイトにある Cisco Unified Communications Manager との SIP トランク連動を提供します。ブランチ サイト (Cisco IP Phone を使用) は Cisco IOS Firewall で保護されています。これにより、リモート サイトはサービス プロバイダー ネットワークに安全に接続することができます。

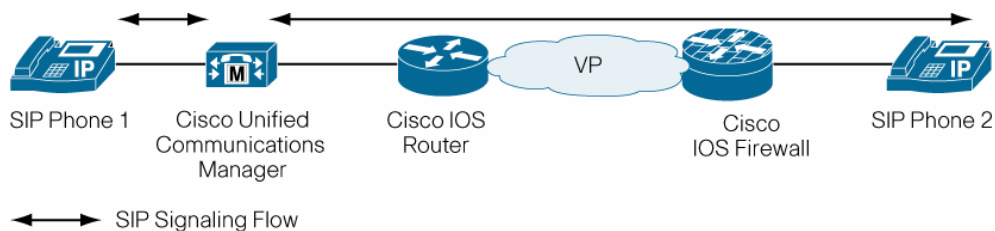
図 2 SIP トランクベース接続の構成



## 構成 2: 企業の在宅勤務者用の構成

この構成例は、VPN トンネルを介した本社と企業の在宅勤務者サイトとの接続を示しています。ベースとなる伝送路には WAN (専用線またはインターネット接続) が使用されています。リモート側の電話機は本社の Communications Manager に登録します。ただし、信頼できない WAN 接続からリモート サイトを保護するために、Cisco IOS Firewall で本社のユニファイド コミュニケーション リソースと電話機間の通信を保護できるようになっています。

図 3 企業の在宅勤務者用の構成



## まとめ

Cisco IOS Firewall の SIP 検査および制御は、データ ネットワーク、ユニファイド コミュニケーション インフラストラクチャのリソース (Cisco Unified Communications Manager や Cisco Unified Communications Manager Express など)、および IP テレフォニーのエンドポイントとリソース (IP フォン、Cisco UnityR、および Cisco TelePresence リソースなど) の保護に役立つきめ細かなネットワークトラフィック保護機能を備えています。これらのリソースの保護を強化することで、音声およびデータ リソースの信頼性、パフォーマンス、およびセキュリティを確保し、さまざまなビジネス ニーズに対応できる実効性のある環境を実現できます。

## 関連情報

Voice-over-IP (VoIP) システムの保護に関する NIST 勧告 (英語)

<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

シスコのセキュアなユニファイド コミュニケーション

<http://www.cisco.com/jp/go/secureuc/>

Cisco IOS Firewall

<http://www.cisco.com/jp/go/iosfw/>

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。



**シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

**お問い合わせ先**