Cisco ASA 5500 シリーズを利用したユニファイド コミュニケーションの展開

シスコ ユニファイド コミュニケーションは、固定/モバイル ネットワーク上の音声、ビデオ、データ、およびモバイルのアプリケーションを一つにまとめて、いつでもどこからでも容易にコラボレーションを実現するソリューションです。

概要

あらゆる規模のビジネスが、ユニファイド コミュニケーションの利点を得るために IP テレフォニーに移行しつつあります。シスコのユニファイド コミュニケーション製品は、業務の合理化、従業員の生産性向上、ビジネス コミュニケーションの最適化、顧客対応の充実に役立ちます。ユニファイド コミュニケーション ベースのネットワークを攻撃から保護することは、ビジネスの継続性と完全性を維持していく上で非常に重要であるため、シスコはセキュリティ機能をユニファイド コミュニケーション製品に組み込み、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスにおいてもセキュリティの充実を図りました。

Cisco ASA 5500 シリーズは、小規模ビジネスやブランチ オフィス、エンタープライズ、データ センター環境に対応した多機能セキュリティ アプライアンス ファミリです。これらのアプライアンスは、ユニファイド コミュニケーション向けに音声およびビデオの最先端のセキュリティ サービスを提供し、堅牢なファイアウォール、機能充実の IP Security（IPsec）および Secure Sockets Layer（SSL）VPN、侵入防御、コンテンツ セキュリティ機能を備えています。また、これらのプラットフォームでは、ユニファイド コミュニケーションの展開にあたり、30,000 台までの電話機を保護でき、また、幅広いユニファイド コミュニケーション プロトコルのアプリケーション インスペクションが可能です。このプロトコルとは、Skinny Client Control Protocol（SCCP）、Session Initiation Protocol（SIP）、H.323、Media Gateway Control Protocol（MGCP）、Computer Telephony Interface Quick Buffer Encoding（CTIQBE）、Real-Time Transport Protocol（RTP）、Real-Time Transport Control Protocol（RTCP）などです。

Cisco ASA 5500 シリーズのユニファイド コミュニケーション機能

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、音声やビデオなどリアルタイムのユニファイド コミュニケーション アプリケーションを安全に保護するように設計されています。このアプライアンスは、ユニファイド コミュニケーションの展開における重要な要素（ネットワーク インフラストラクチャ、呼制御プラットフォーム、IP エンドポイント、ユニファイド コミュニケーション アプリケーション）をすべて保護します。ユニファイド コミュニケーション システムに組み込まれたセキュリティ機能を補完するさらなるセキュリティ機能を提供し、またレイヤ保護機能も備えています。以下の特徴があります。

- **アクセス コントロール**：動的できめ細かいポリシー アクセス コントロールによって、ユニファイド コミュニケーション サービスへの不正アクセスを防ぎます。
- **脅威の防御**：システム悪用の試みからユニファイド コミュニケーション インフラストラクチャを保護します。

- **ネットワーク セキュリティ ポリシーの適用**：アプリケーションおよびユーザに対する効果的なユニファイド コミュニケーション ポリシーを作成および管理します。
- **音声暗号化サービス**：Cisco Transport Layer Security（TLS）Proxy によって、シグナリングおよびメディアを暗号化しながら、セキュリティ ポリシーを維持することができます。
- **ユニファイド コミュニケーションの境界セキュリティ サービス**：SSL および IPsec VPN サービスに加え、フォン プロキシ、モビリティ プロキシ、プレゼンス フェデレーションなどのセキュリティ サービスによって、リモート ユーザ、モバイル ソリューション、ビジネス間コラボレーションに至るまで安全にコミュニケーション サービスを拡大していくことができます。

アクセス コントロール

アクセス コントロールは、システム内のリソースおよびサービスに対して認証されたアクセスのみを許可する基本的なセキュリティ機能です。ユニファイド コミュニケーションでは、攻撃からの防御の第一線として、Cisco Unified Communications Manager およびその他のアプリケーションサーバに対してネットワーク レイヤのアクセス コントロールを提供するということと深い関係があります。Cisco Unified Communications Manager サーバへのアクセスを制限することは、攻撃者がシステムの脆弱性を探ったり、不正なネットワーク チャネルを通じてアクセスを試みる危険を大幅に減らします。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、音声およびビデオが認識可能であり、最新のユニファイド コミュニケーションで使用されるプロトコル（SIP、SCCP、H.323、MGCP）を検査し、ポリシーを適用することができます。アクセス コントロール リスト（ACL）などの従来のネットワーク アクセス コントロールのメカニズムでは、これらの複雑なプロトコルを、多くの企業が求めているようにきめ細かくかつ動的に処理することはできません。

従来のデータ アプリケーションとは異なり、ユニファイド コミュニケーション プロトコルは、シグナリング コントロール チャネル内でポート情報を交換することによって通信方法を動的にネゴシエーションします。ACL のような静的アクセス コントロールのメカニズムでは、オープンするポートを追跡できず、その結果、脆弱なアクセス コントロールを適用せざるを得ず、効果的なアクセス ポリシーの実装能力が制限されてしまいます。

Cisco ASA 5500 シリーズ適応型セキュリティアプライアンスは、開くべき認証済みの接続を動的に追跡でき、セッションが終了するとすぐにこの接続を閉じることができます。このようなレベルの制御能力が、音声プロトコル認識に対応した Network Address Translation（NAT）などのその他のインテリジェントなサービスと結び付き、Cisco ASA 5500 シリーズのアプライアンスは、近年のユニファイド コミュニケーション プロトコルの要件に適さない従来のプラットフォームと一線を画す製品になっています。

脅威の防御

Cisco ASA 5500 シリーズは、システムの完全性およびアベイラビリティに脅威を与える一般的な攻撃からシスコ ユニファイド コミュニケーションのアプリケーションを保護します。このような攻撃には、通話の盗聴、ユーザのなりすまし、通話料金詐欺、DoS 攻撃などがあります。これらの攻撃のほとんど（特に DoS）は、不正な形式のプロトコル パケットを送出してユニファイド コミュニケーションの呼制御システムおよびアプリケーションを攻撃

することから始まります。Cisco ASA 5500 シリーズは、重要なユニファイド コミュニケーション サーバに向かうトラフィックのプロトコル適合性および準拠性のチェックを実行します。たとえば、アプライアンスを流れていくメディアが本当に音声メディア（RTP）であるのかを確認し、また、攻撃者が呼制御システムを破壊させるような不正な音声信号を送信するのを防御します。シグナリングとメディアが標準 RFC に準拠しているかをチェックする機能を提供することで、Cisco ASA 5500 シリーズは重要システムを最前線で効果的に防御する役割を果たします。

プロトコルの適合性のチェック機能に加え、Cisco ASA 5500シリーズ アプライアンスの多機能セキュリティ サービスは、侵入防御サービスを提供するように拡張することができます。Cisco ASA 5500 シリーズAdvanced Inspection and Prevention Security Services Module（AIP SSM）は、ハードウェアを使用した侵入防御システム（IPS）機能を内向きのトラフィックに適用して、ユニファイド コミュニケーションの呼制御サーバおよびアプリケーション サーバに対する既知の攻撃を停止させます。Cisco Unified Communications Manager および Cisco Unified Communications Manager Express における Product Security Incident Response Team（PSIRT）の脆弱性を保護するユニファイド コミュニケーションの一連の IPS シグニチャが用意されているため、IT 管理者はユニファイド コミュニケーション サーバにただちにパッチを適用しなくても、即座に保護を有効にすることができます。プロトコルの適合性と侵入防御を組み合わせることによって、一般的なユニファイド コミュニケーションへの脅威に対するネットワーク レイヤの防御は堅牢になります。

ネットワーク セキュリティ ポリシーの適用

ユニファイド コミュニケーションの展開では、通常、企業のセキュリティ部門が設定したセキュリティ ポリシーの要件を適用する必要があります。Cisco ASA 5500 シリーズの洗練されたユニファイド コミュニケーション セキュリティ機能を使用すれば、企業はユニファイド コミュニケーションのトラフィックに対してきめ細かいアプリケーション レイヤ ポリシーを適用して、セキュリティ コンプライアンスの要件を満たすことができます。たとえば、特定の発信者またはドメインからのコールを許可または拒否したり、特定のブラック リストやホワイト リストを適用できます。ネットワーク ポリシーをエンドポイントやアプリケーションに拡張して、たとえば呼制御サーバに登録された電話機からのコールだけを許可したり、SIP を介したインスタント メッセージングなどのアプリケーションを拒否することが可能です。

音声およびビデオ暗号化サービス

コンプライアンスまたはセキュリティ ポリシー上の理由から、企業では音声およびビデオのトラフィックを機密扱いとすることが求められる場合があります。エンドツーエンドの暗号化はときに、ネットワーク セキュリティ アプライアンスからメディアやシグナリングのトラフィックを「見えない」状態にしてしまい、アクセス コントロールや脅威防御などのセキュリティ機能を危殆化してしまう可能性があります。このような場合、ファイアウォール機能と暗号化された音声との間の相互運用性が失われ、双方の重大なセキュリティ要件をも満たすことができなくなります。

Cisco ASA 5500 シリーズの暗号化プロキシ ソリューションは、例外サポート（ TLS プロキシ）機能をシスコ ユニファイド コミュニケーション システムに提供します。このデバイスが、Cisco Unified Communications Manager 認証ドメインにおいて信頼できるデバイスとなることで、音声およびビデオのエンド ポイント はトラフィックを安全に認証および暗号化できます。Cisco ASA 5500 シリーズは、プロキシとしてこれらの接続を復号化し、脅威に対し

て必要とされる保護およびアクセス コントロールを適用し、Cisco Unified Communications Manager サーバへのトラフィックを再度暗号化して機密性を維持できるようにします。このような統合化によって、不十分なサブセットを適用するのではなく、必要なセキュリティ対応策すべてを展開する柔軟性を企業に提供することが可能になります。

境界セキュリティ サービス

境界セキュリティ サービスには以下のものがあります。

- **SSL および IPsec VPN**：Cisco ASA 5500 シリーズは、複数のオフィスやリモート ユーザ間の安全な高速音声通信およびデータ通信を促進する SSL または IPsec VPN サービスを使用して、柔軟かつ安全な接続をサポートします。これらのアプライアンスは、サービス品質（QoS）機能をサポートし、遅延が問題となる音声やビデオなどのアプリケーションを信頼性の高い、ビジネス品質で配信するのに役立ちます。優先順位と帯域幅の適切な制限が音声およびビデオ フローに適用されるように、ユーザごと、グループごと、トンネルごと、フローごとに QoS ポリシーを適用できます。さらに、事前接続のポスチャ評価とセキュリティ チェックにより、VPN ユーザが誤ってネットワーク攻撃を持ち込まないようにします。Cisco SSL および IPsec ソリューションは、Cisco IP Communicator、Cisco Unified Mobile Communicator、および Cisco Personal Communicator などのソフト クライアントのユニファイド コミュニケーション トラフィックを保護するのに理想的です。
- **フォン プロキシ**：Cisco ASA フォン プロキシ機能は、セキュアなリモート アクセスを実現するために、Cisco SRTP および TLS による暗号化されたエンドポイントの終端処理を容易にします。Cisco ASA フォン プロキシによって、大規模な VPN リモート アクセス用のハードウェアを導入せずにセキュアな電話機を大規模展開することができます。エンドユーザのインフラストラクチャは IP エンドポイントのみでよく、VPN トンネルやハードウェアは伴いません。Cisco ASA フォン プロキシは、Cisco Unified Phone Proxy の代替製品です。
  Cisco ASA フォン プロキシをソフトフォン アプリケーションの音声およびデータ VLAN をセグメンテーションするために導入することも可能です。Cisco ASA アプライアンスを通して Cisco IP Communicator のトラフィック（メディアおよびシグナリングの両方）をプロキシし、音声およびデータ VLAN 間で安全にコールを接続することができます。
- **モビリティ プロキシ**：Cisco ASA モビリティ プロキシは Cisco Unified Mobile Communicator ソフトウェアと Cisco Unified Mobility Advantage サーバとの間の安全な接続を促進します。Cisco ASA アプライアンスは、Cisco Unified Mobile Communicator ソフトウェアおよびサーバ間の TLS 接続を代行受信することができ、新しい Multichassis Multilink PPP（MMP）インスペクション エンジンを使用してポリシーを検証し、モビリティ トラフィックに適用できます。Cisco ASA アプライアンスは、Cisco Unified Communications 7.0 Systems と共に起動するモビリティ ソリューションの必須コンポーネントであり、Cisco Unified Mobility Proxy に取って代わります。
- **プレゼンス フェデレーション**：Cisco ASA 5500 シリーズは Cisco Unified Presence と Microsoft Office Communications Server（OCS）Presence ソリューションとの間のセキュアなプレゼンス フェデレーションを実現します。2 つの企業が、互いのユーザと最もうまく連絡を取りコミュニケーションを交わす方法や、利用可能な共

通のコミュニケーション形態に関してプレゼンス情報を共有することで、より効率的なコラボレーションを可能にします。Cisco ASA 5500 シリーズ アプライアンスは、プレゼンス フェデレーション ソリューションの必須コンポーネントです。

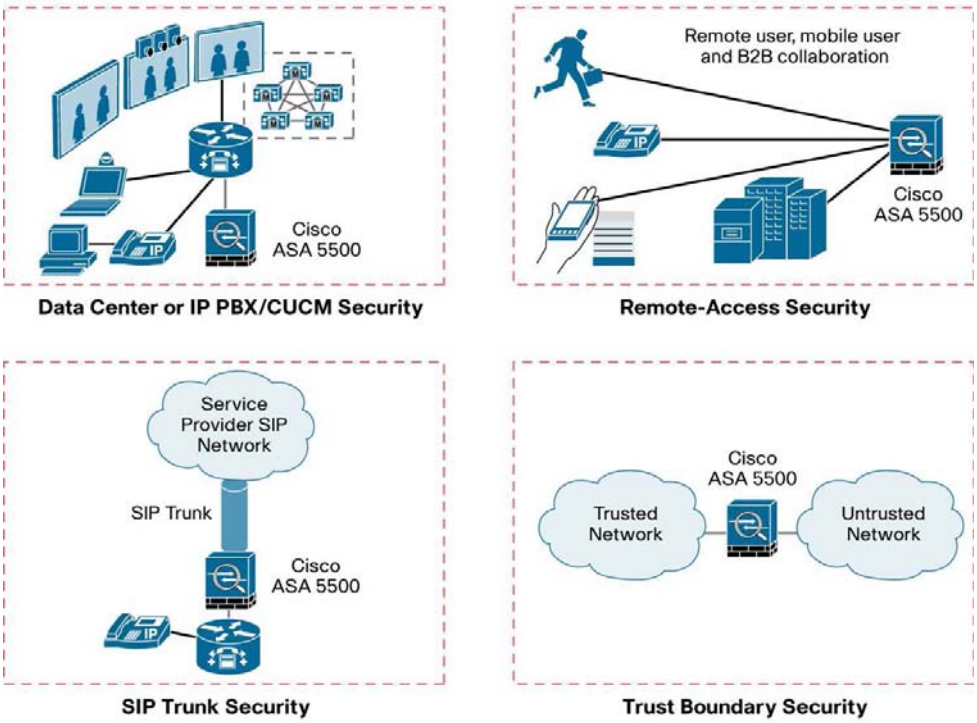
展開時のトポロジ

図1 に示すように Cisco ASA 5500 シリーズはネットワーク全体で使用することによって、呼制御システム、エンドポイント、アプリケーション、およびその下にあるインフラストラクチャを攻撃から保護します。以下のようなトポロジがあります。

- **呼制御サーバの保護**：クライアントからこれらのサーバへのアクセスを制御することで、パフォーマンスやアベイラビリティに影響を与える恐れのある悪質なネットワーク接続や不正なネットワーク接続から保護することができます。ステートフルな検証によって、接続がアクセス制御ポリシーに従い、期待される振る舞いに適合しているかを確認することで、Cisco ASA プラットフォームはセキュアなユニファイド コミュニケーションの展開における最前線の防御を提供します。
- **リモートアクセス セキュリティ**：Cisco ASA 5500 シリーズは、SSL および IPsec VPN、フォン プロキシ、モビリティ プロキシ、プレゼンス フェデレーションなどのセキュリティ サービスを提供し、在宅勤務者の電話、Cisco IP フォン、Apple iPhone などのサードパーティの電話、携帯電話、ビジネス間のフェデレーション展開の安全を保ちます。
- **SIP トランク セキュリティ**：企業は通信費を抑えるために SIP トランク アーキテクチャに移行しつつあります。Cisco ASA 5500 シリーズの堅牢な SIP セキュリティ機能は、SIP トランクを介したあらゆる攻撃を防御します。
- **「信頼できる」境界と「信頼できない」境界**：Cisco ASA 5500 シリーズを信頼できるネットワークと信頼できないネットワークとの間のセキュリティ デバイスとして配置し、信頼できないネットワークの脆弱性が信頼できるネットワークに影響を及ぼさないようにすることができます。Cisco ASA 5500 シリーズ アプライアンスを音声およびデータの VLAN 間のトラフィックのプロキシ処理に使用したり、DMZ アーキテクチャで外部アクセスから内部ネットワークを安全に保つことができます。

Cisco ASA 5500 シリーズで利用可能な各種モデルの中から、企業は 1 つのセキュリティ製品ファミリを標準とし、その一方で個々のトポロジまたはロケーションごとに異なるパフォーマンス要件を満たす特定のモデルを配置することができます。

図 1　Cisco ASA 5500 シリーズの展開トポロジ



Cisco ASA 5500 シリーズは、ユニファイド コミュニケーション ネットワークの音声およびビデオのセキュリティ機能の包括的スイートです。表 1 に、このスイートの機能と利点を示します。

表 1.　機能と利点の概要

機能	詳細
ユニファイド コミュニケーション アプリケーションのインスペクションと制御	• サポートされているプロトコルは SIP、SCCP、H.323、MGCP、RTP および RTCP、TCP、CTIQBE、Real Time Streaming Protocol（RTSP）です。
SIP アプリケーションのインスペクションと制御	• User Datagram Protocol（UDP）および TCP ベースの SIP 環境両方のための SIP トラフィックの詳細なインスペクション サービスを提供します。ユニファイド コミュニケーションへの攻撃に対する保護のきめ細かな制御が可能です。 • SIP アプリケーションのインスペクションと制御によって、RFC 3261 を含む各種 SIP RFC に対するプロトコルの準拠性が確保されます。SIP の状態認識機能と追跡機能を備え、必須ヘッダ フィールドが必ず存在することを確認し、禁止されているヘッダ フィールドを排除できるので、不正な形式のパケットを利用した攻撃からビジネスを保護できます。 • SIP ベースの IP フォンや Microsoft Windows Messenger などのアプリケーション用に、Network Address Translation（NAT）および Port Address Translation（PAT）によるアドレス変換をサポートします。また、コール転送などの高度なサービスも提供します。 • SIP の状態認識や追跡、DoS 攻撃を防止するための SIP トラフィックのレート制限機能（特定のプロキシからの SIP トラフィックが不正プロキシ サーバからの SIP トラフィックをブロックするのを防止）、メディアに対する RTP および RTCP 検証などの包括的な脅威防御機能をサポートします。 • SIP アプリケーションのインスペクションと制御により、きめ細かいユニファイド コミュニケーションのポリシーの設定が可能になります。SIP Uniform Resource Identifier（URI）フィルタの設定による発信者および受信者の許可および拒否、ホワイトリストおよびブラックリストを利用した着信コール、発信コールの許可および拒否などがあります。SIP アプリケーションのインスペクションと制御によって、SIP 経由のインスタント メッセージングなどのアプリケーションの使用の許可や拒否、特定の SIP メソッドの許可や拒否（ユーザ定義のメソッドを含む）を行うこともできます。

機能	詳細
H.323　セキュリティ サービス	• H.323 セキュリティ サービス バージョン 1–4 は、Direct Call Signaling（DCS）および Gatekeeper Router Control Signaling（GKRCS）と組み合わせて、H.323 制御のさまざまな voice-over-IP（VoIP）環境で柔軟なセキュリティ統合機能を提供します。 • これらのサービスでは NAT および PAT がサポートされており、これには T.38 プロトコル（FoIP のリアルタイム伝送方式を定義する ITU 規格）を使用した fax over IP（FoIP）などの高度な機能も含まれます。 • H.323 トラフィックの脅威防御もサポートされています。たとえば、通話時間を制限したり、H.225 Registration, Admission, and Status（RAS）パケットが「out of state」となるのを防止したり、メディアに対する RTP および RTCP を検証したりします。 • H.323 サービスに関するきめ細かいポリシー設定も可能です。発信または着信電話番号のフィルタリングによる悪意のある発信者からのコールの防止、特定のメディア タイプのフィルタリングによるサービスの制限などが可能です。
SCCP　セキュリティ サービス	• 高度な SCCP インスペクション サービスが、Cisco Unified IP Phones、Cisco Unified Personal Communicator、Cisco IP Communicator などの SCCP アプリケーションをサポートし、セキュリティを柔軟に統合します。 • 最大 SCCP メッセージ長の設定によるバッファ オーバーフロー攻撃の回避、TCP SCCP 接続および SCCP オーディオ ビデオ メディア接続に対するタイムアウトの調整機能、RTP および RTCP によるメディアの検証など、包括的脅威防衛機能を提供します。 • SCCP トラフィックに対するきめ細かいポリシーの設定を可能にします。登録済み電話機によるコールでのみ Cisco ASA アプライアンスを介したトラフィック送信を可能にしたり、メッセージ ID をフィルタリングすることによって特定のメッセージのみを許可または拒否することができます。
MGCP　セキュリティ サービス	• 機能豊富な MGCP セキュリティサービスは、メディア ゲートウェイとコール エージェント間、またはメディア ゲートウェイとメディア ゲートウェイ コントローラ間の MGCP ベースの接続を対象とした NAT および PAT ベースのアドレス変換サービスを支援します。
RTSP　セキュリティ サービス	• Cisco IP/TV、Apple QuickTime、RealNetworks RealPlayer などのクライアントとサーバ間の通信制御に使用される RTSP プロトコルのインスペクションを支援します。 • RTSP メディア ストリームを対象とした NAT および PAT ベースのアドレス変換サービスにより、リアルタイム ネットワーキング環境でのサポートを強化します。
断片化および細分化されたマルチメディア ストリームのインスペクション	• 断片化または細分化された H.323、SIP、SCCP ベースの音声およびマルチメディア ストリームのインスペクションを支援し、これらに特有のユニファイド コミュニケーションへの攻撃を防止します。
高度な TCP セキュリティ エンジン	• SYNC クッキーを利用した SYN フラッドなどの複数の攻撃からネットワークを保護し、また、プロトコルのファジー化や再伝送スタイルの time-to-live（TTL; 存続可能時間）検知回避攻撃からネットワーク エンドポイントを保護します。 • 複数の TCP パケットを使用したセグメント攻撃に対して、TCP パケットを再構成して防御するスマート TCP プロキシ機能が用意されています。 • 高度な技術により攻撃を検知するための TCP トラフィックの正規化サービスを提供します。フラグおよびオプションの高度なチェック機能、TCP パケットのチェックサム検証機能、再伝送パケットの改ざんの検知機能などがあります。
RTP および RTCP インスペクション サービス	• SIP および SCCP 接続など、ユニファイド コミュニケーションの検査エンジンで開かれたメディア接続において RTP および RTCP トラフィックを検証します。 • RTP および RTCP トラフィックを対象としたセキュリティ ポリシーの設定を支援します。RFC 1889 への準拠の検証、シグナリングと RTP との間のメディア値の相互チェックによるペイロード タイプの検証、バージョン番号、ペイロード タイプの整合性、シーケンス番号、同期ソース（SSRC）のポリシングなどが行われます。
脅威の防御	
侵入防御サービス	• オプションの Cisco ASA 5500 シリーズ AIP SSM は侵入防御サービスを適用し、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と呼制御サーバを IPS シグニチャ ベースの攻撃から保護します。ユニファイド コミュニケーションに合わせて最適化された IPS サービスにより、H.323 および H.225 検査エンジンなどの特定のユニファイド コミュニケーション エンジンをサポートし、また呼制御サーバでの OS 攻撃の防御を支援します。 • 異常検知、OS フィンガープリンティング、Risk-Rating などの独自の侵入防御機能によって、脅威に対するより優れたコンテキストを提供し、誤検知を防止します。
コンテンツ　セキュリティ サービス	• 電子メールおよび Web トラフィックを検証するための、ゲートウェイベースのコンテンツ インスペクション機能の実装を支援します。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から、ウィルス、ワーム、スパム、フィッシング、マルウェア等による攻撃を確実に排除します。
暗号化サービス	

機能	詳細
TLS プロキシ	• TLS プロキシは、暗号化されたシグナリングによってユニファイド コミュニケーション ファイアウォールが動的にポートを開いたり、ポリシーを適用できなくなったりした場合に、暗号化されたシグナリングとファイアウォールの統合の問題を解決します。Cisco Unified Communications Manager System 内の信頼できるデバイスとして、Cisco ASA アプライアンスが暗号化シグナリングを代行受信し、エンドポイントとの相互認証を実施し、シグナリングを復号化します。シグナリングが復号化されると、アプライアンスは必要なシグナリング情報をすべて取得し、インスペクションとポリシー適用アクションをすべて実行します。セキュアな接続をエンドツーエンドで維持するため、アプライアンスは次にセカンダリ TLS セッションを開始した後、制御を Cisco Unified Communications Manager に戻します。エンドポイントと Cisco Unified Communications Manager との間のシグナリングおよび通信は機能的に維持されたまま、ファイアウォールがユニファイド コミュニケーション セキュリティ サービスを提供することができます。 • TLS プロキシ サービスは、SIP、SCCP のいずれのエンドポイントもサポートし、Cisco Unified IP Phones と包括的に統合されます。
境界セキュリティ サービス	
フォン プロキシ	• フォン プロキシは、TLS または SRTP で暗号化された SCCP および SIP の Cisco Unified IP Phone エンドポイントを終了することで、リモート アクセス VPN デバイスがなくてもセキュアなリモート アクセスを可能にします。Cisco Unified Communications Manager の混在モードと非セキュア モードをサポートします。既存のファイアウォールの背後に、または統合ファイアウォールまたはフォン プロキシ アプライアンスとして、フォン プロキシを展開することができます。 • セキュア VLAN トラバーサルは、ソフトフォン トラフィックのすべてを Cisco ASA アプライアンスを経由してプロキシできるように、ソフトフォン アプリケーションのセキュリティを確保します。Cisco IP Personal Communicator は認証モードでサポートされます。
モビリティ プロキシ	• モバイル プロキシが Cisco Unified Mobility ソリューションを保護し、Cisco Unified Mobility Proxy に取って代わります。このプロキシには新たな検査エンジンが組み込まれており、モビリティ トラフィックを検証します。ダウンロードされた Cisco Unified Mobile Communicator ソフトウェアのプロトコルへの適合性や HTTP インスペクションが含まれます。
プレゼンス	• Cisco Unified Presence と Microsoft Presence ソリューションとのフェデレーションに必須のこのコンポーネントは、プレゼンス情報を安全に維持し、2 社のセキュリティ ポリシー（ホワイト リスト、ブラック リスト、プロトコル準拠）を適用します。
SSL およびIPsec VPN	• ユニファイド コミュニケーションおよびデータ トラフィックのいずれにも対応した、暗号化された堅牢な SSL および IPsec VPN サービスが、エンドポイントに対する事前接続のポスチャ評価を実施し、VPN トラフィックにポリシーおよびインスペクション機能を適用して、リモート ユーザがネットワークに脆弱性を持ち込むのを防止します。Cisco AnyConnect クライアントは、Datagram Transport Layer Security（DTLS）をサポートし、音声を最適化します。Apple iPhone などのサードパーティ製エンドポイントの安全を確保します。

発注情報

シスコ製品の購入方法の詳細については、「発注方法」および表 2 ～ 4 を参照してください。ソフトウェアをダウンロードするには Cisco Software Center にアクセスしてください。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの注文については、お客様のユニファイド コミュニケーションの展開を保護するため、以下の3 つのオプションを用意しています。

- **オプション 1**：ユニファイド コミュニケーション プロキシ ライセンス：Cisco Unified Communications プロキシ ソフトウェア ライセンスを個別に注文します（ASA-UC-X）。フォン プロキシ、モビリティ プロキシ、プレゼンス フェデレーション、TLS プロキシの各機能の利用が可能です。これらの機能は組み合わせて、表 2 に示す最大セッション数まで対応できます。

表 2. シスコ ユニファイド コミュニケーション プロキシの最大セッション数

	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580
ユニファイド コミュニケーション プロキシの最大セッション数	24	100	1000	2000	3000	10,000

- **オプション 2**：Cisco ASA 5500 Unified Communications Edition バンドル：Cisco ASA 5500 Unified Communications Edition のバンドルは、ユニファイド コミュニケーション プロキシ ライセンスがバンドルされるアプライアンスを提供しており、1 つのハードウェアおよびソフトウェア製品 ID で、フォン プロキシ、モビリティ プロキシ、プレゼンス フェデレーション、TLS プロキシ機能を、ベースとなるファイアウォールおよび VPN 機能と共に提供します。

表 3. Cisco ASA 5500 シリーズ Unified Communications Edition の発注情報

製品名	製品番号
Cisco ASA 5520 適応型セキュリティ アプライアンスのユニファイド コミュニケーション セキュリティ機能	
Cisco ASA 5520 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、ファスト イーサネット インターフェイス × 1、UC プロキシ セッション × 1000、IPsec VPN ピア × 750、SSL VPN ピア × 2、アクティブ/アクティブおよびアクティブ/スタンバイ ハイ アベイラビリティ、トリプル データ暗号化規格/高度暗号化規格（3DES/AES）ライセンス	ASA5520-UC-BUN-K9
Cisco ASA 5520 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、ファスト イーサネット インターフェイス × 1、UC プロキシ セッション × 1000、IPsec VPN ピア × 750、SSL VPN ピア × 2、アクティブ/アクティブおよびアクティブ/スタンバイ ハイ アベイラビリティ、DES ライセンス	ASA5520-UC-BUN-K8
Cisco ASA 5540 適応型セキュリティ アプライアンスのユニファイド コミュニケーション セキュリティ機能	
Cisco ASA 5540 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、ファスト イーサネット インターフェイス × 1、UC プロキシ セッション × 2000、IPsec VPN ピア × 5000、SSL VPN ピア × 2、3DES/AES ライセンス	ASA5540-UC-BUN-K9
Cisco ASA 5540 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、ファスト イーサネット インターフェイス × 1、UC プロキシ セッション × 2000、IPsec VPN ピア × 5000、SSL VPN ピア × 2、DES ライセンス	ASA5540-UC-BUN-K8
Cisco ASA 5550 適応型セキュリティ アプライアンスのユニファイド コミュニケーション セキュリティ機能	
Cisco ASA 5580 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、UC プロキシ セッション × 5000、IPsec VPN ピア × 10,000、SSL VPN ピア × 2、3DES/AES ライセンス	ASA5580-20-UC-K9
Cisco ASA 5580 Adaptive Security Appliance UC Security Edition：ギガビット イーサネット インターフェイス × 4、UC プロキシ セッション × 5000、IPsec VPN ピア × 10,000、SSL VPN ピア × 2、DES ライセンス	ASA5580-20-UC-K8

- **オプション 3**：Cisco Secure Unified Communications バンドル：シスコ ユニファイド コミュニケーション ソリューションをご購入される場合、Cisco Unified Communications Manager および Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスを含むバンドルをご注文できます。これらのバンドルは、ダイナミック発注ツールまたはオンライン発注ツールを使用して構成する場合、Cisco Unified Communications Manager サーバごとに Cisco ASA 5500 シリーズ モデルの推奨製品が示されます。

表 4. Secure Unified Communications バンドルの発注情報

製品名	製品番号
Cisco Secure Unified Communications Bundle（Cisco Unified Communications Manager 6.0 を含む）	SEC-Unified-CM-6.0

製品名	製品番号
Cisco Secure Unified Communications Bundle（Cisco Unified Communications Manager 6.1を含む）	SEC-Unified-CM.6.1
Cisco Secure Unified Communications Bundle（Cisco Unified Communications Manager 7.0 を含む）	SEC-Unified-CM.7.0

シスコ ユニファイド コミュニケーション サービス

シスコ ユニファイド コミュニケーション サービスは、セキュアで復元力のあるシスコ ユニファイド コミュニケーション ソリューションを展開することで、コストの節約と生産性の向上をスピードアップするサービスです。シスコと認定パートナーが提供するサービスはいずれも、固定/モバイル ネットワーク上の音声、ビデオ、データ、およびモバイルのアプリケーションの一本化に関する実証された方法論に基づいています。サービスに対するシスコ独自のライフサイクル アプローチを通して、お客様の真のビジネス優位性確立を加速する、さまざまなテクノロジーを提供します。

関連情報

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの詳細については、http://www.cisco.com/go/asa を参照するか、最寄のシスコ代理店にお問い合わせください。

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
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00 ～ 12:00、13:00 ～ 17:00
http://www.cisco.com/jp/go/contactcenter/

お問い合せ先