

Secure RTP によるメディアの認証と暗号化

シスコのアクセス ルータ製品が持つメディア認証およびメディア暗号化の機能を使用することにより、Time Division Multiplexing (TDM; 時分割多重) ポートまたはアナログ音声ゲートウェイ ポートで終端する音声会話を盗聴から確実に保護することができます。これらの機能は、信頼性と拡張性を兼ね備え、LAN や WAN を通じた IP コミュニケーションにセキュアな環境を提供します。

製品概要

大企業のブランチ オフィスや中小・中堅企業は、運営費の削減、生産性の向上、ネットワーク管理の簡素化を図るため、IP コミュニケーションへの移行を進めています。Cisco 1700 から Cisco ISR (Integrated Services Router) 3800 まで広範なプラットフォームを揃えたシスコのアクセス ルータ製品は、非常に負荷の高い企業環境に対しても、強力かつ拡張性の高い IP コミュニケーション ソリューションを幅広く提供できるように設計されています。

シスコのアクセス ルータ製品は、さまざまな音声セキュリティ機能を備えており、IP コミュニケーション ソリューションを導入する企業に最高レベルのセキュリティ保護を提供します。同業他社の多くは、付加的な拡張とポイント型の製品ソリューションによって、個々のコンポーネントを保護しています。シスコでは、自己防衛型ネットワーク構想に基づくマルチレイヤ ソリューションによって、ネットワークそのものからエンドポイントやアプリケーションへとセキュリティを拡大する方式を採っています。このように包括的かつ階層的なアプローチでセキュリティに取り組んでいるのはシスコだけです。ベスト プラクティスの詳細や、お客様のネットワークのセキュリティ対策に役立つツールについては、Cisco SAFE ブループリントをご覧ください。

防御の第 1 段階は、音声ドメインへのアクセスを制御および防止することです。そして、Secure RTP (SRTP) を使用したメディア暗号化によって、第 2 段階の保護が提供されます。メディア暗号化機能を利用すると、音声会話が暗号化されるため、たとえ内部または外部のハッカーが音声ドメインへの侵入とアクセスに成功したとしても、音声会話が理解されることはありません。SRTP は、音声パケットのために特別に設計されたプロトコルで、AES 暗号化アルゴリズムに対応し、Internet Engineering Task Force (IETF) RFC 3711 標準となっています。SRTP を使用したメディア暗号化は、帯域効率の面で IPSec よりも優れています。

シスコ アクセス ルータのメディア暗号化機能は、Cisco IP Phone のメディア暗号化機能と Cisco CallManager の両方と連動し、ゲートウェイ間の呼だけでなく、MGCP モードの IP Phone とゲートウェイ間の呼にもセキュリティを提供します。したがってお客様は、メディアが終端するゲートウェイ インターフェイスのタイプに応じて、アナログ電話コール、ファックス コール、または IP Phone とゲートウェイ間の呼を保護できます。Cisco CallManager が生成した音声暗号鍵は、暗号化シグナリング パスを通り、Transport Layer Security (TLS) を使用して Cisco IP Phone へ、IPSec を使用してゲートウェイへと送信されます。

シスコ アクセス ルータのメディア暗号化機能は、IOS ソフトウェア 12.3(5th)T (IOS PI-5 リリース) から、Advanced Enterprise Services と Advanced IP Services の IOS ソフトウェア フィーチャ セットへのアップグレードによって利用可能となります。この機能を使用するには、PVDMM2、NM-HD、および NM-HDV2 音声ゲートウェイ ネットワーク モジュールに組み込まれている Digital Signal Processor (DSP; デジタル信号プロセッサ) モジュール上での設定が必要です。

機能

メディアの認証および暗号化ソリューションの詳細な機能は、以下の表のとおりです。

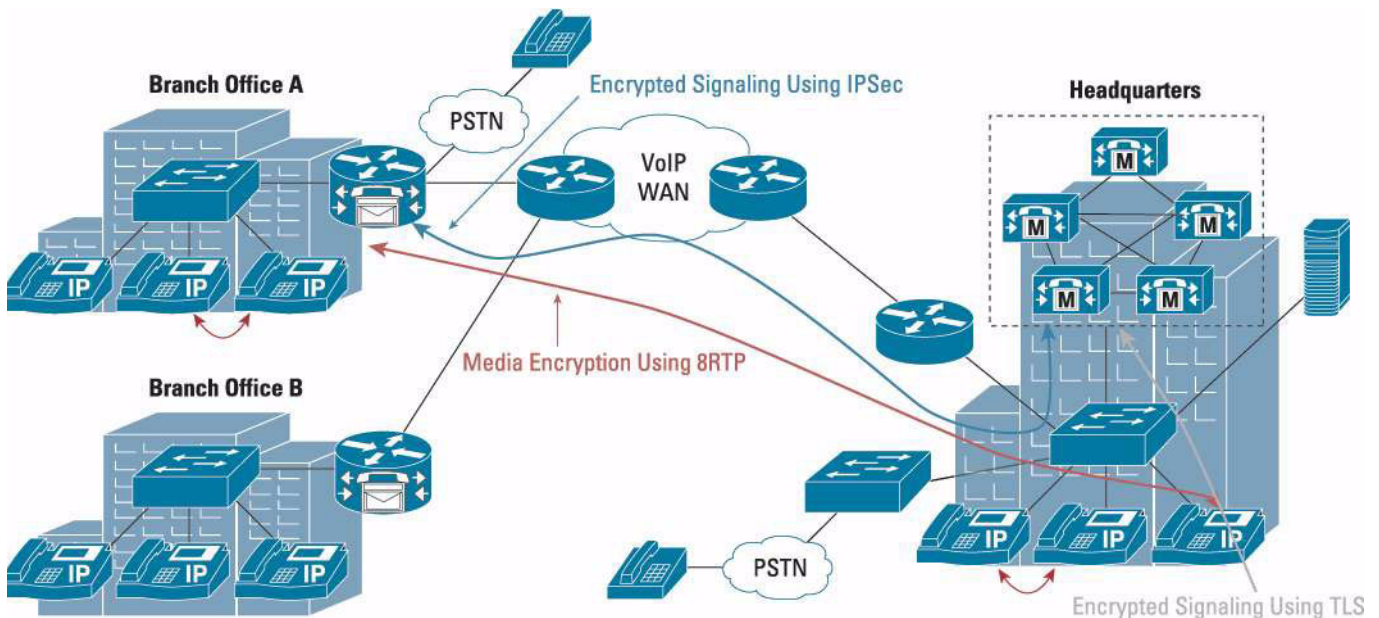
表 1 機能

認証および暗号化の機能	認証および暗号化のアルゴリズム	プロトコル/コーデック/モジュールのサポート	その他の機能
SRTP を使用した音声 RTP ストリームのメディア暗号化	AES-128 暗号化アルゴリズムのサポート	Cisco CallManager とゲートウェイの間における MGCP 0.1 モード通信プロトコルのサポート	セキュアなエンドポイントとセキュアでないエンドポイントの間の呼に対する SRTP/RTP フォールバック
Secure RTP Control Protocol (RTCP) を使用した RTCP 情報の交換	HMAC Secure Hash Authentication Algorithm (SHA 1) のサポート	音声コーデック、G.711、G.729A、G.729 のサポート	Survivable Remote Site Telephony (SRST) モードの呼に対する SRTP/RTP フォールバック
IPSec によるゲートウェイと Cisco CallManager 間のシグナリングの認証と暗号化		この機能をサポートしているモジュール：PVDM2-8、PVDM2-16、PVDM2-32、PVDM2-48、PVDM2-64、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、NM-HDV2-2T1/E1	SRTP を使用したメディア暗号化された呼での Compressed RTP (CRTP) のサポート

利用方法

シスコ アクセス ルータのメディア認証およびメディア暗号化機能は、Cisco IP Phone のメディア暗号化機能や Cisco CallManager と連動し、WAN または LAN を通じた IP コミュニケーションにセキュアな環境を提供します。以下の図では、ブランチ オフィス A にある音声ゲートウェイ ネットワーク モジュール上で、暗号化音声コールに対して SRTP が使用されています。これによってオフィス内のアナログ電話機同士またはファックス同士の間で安全な呼が確立されます。同様に、ブランチ オフィス A にある TDM エンドポイントまたはアナログ電話機から本社にある Cisco IP Phone へも安全な呼が確立されます。また、ブランチ オフィス A にあるゲートウェイと Cisco CallManager の間のシグナリングは IPSec で保護され、本社の IP Phone と Cisco CallManager の間のシグナリングは TLS で保護されます。

図 1 メディアの認証と暗号化



主な機能と利点

メディアの認証と暗号化

現在のメディア暗号化機能は、エンドツーエンド（Cisco IP Phone 間）で音声コールを暗号化します。シスコ アクセス ルータにメディア暗号化機能が導入されたことにより、IP Phone とゲートウェイの間およびゲートウェイ間に安全な呼を確立できるようになりました。お客様は、IETF RFC 3711 標準ベースの SRTP を使用して、暗号化された呼を PSTN ゲートウェイに発信できます。SRTP は、ほかの暗号化ヘッダーを追加することなく、音声パケットのペイロードだけを暗号化するため、SRTP で暗号化された音声パケットは RTP 音声パケットとほとんど区別が付きません。その結果、新たに何かを開発したりパケットを操作したりしなくても、Quality of Service (QoS; サービス品質) や CRTP のような機能に対応できます。また SRTP は、DES や 3DES アルゴリズムよりも高レベルのセキュリティと速度を備えた AES 暗号化アルゴリズムを使用しています。音声暗号鍵は呼単位で作成されるので、高度なセキュリティ保護が保証されます。さらにメディア認証機能によって、呼を暗号化するゲートウェイや IP Phone の身元を検証できます。

SRTP を使用したメディア暗号化は、LAN 上の音声のプライバシーや機密性を内部の脅威から保護するのに最適です。また、メディア暗号化は、データ用に配備されている VPN インフラストラクチャを使用することで、IP WAN またはインターネットを経由した利用も可能です。

シグナリングの認証と暗号化

ゲートウェイと Cisco CallManager の間のシグナリングの認証と暗号化は IPSec で保護されます。そのため、DTMF 番号、パスワード、暗証番号 (PIN)、および音声暗号鍵などのシグナリング情報が保護されていることが保証されます。IOS で利用可能なソフトウェアベースの IPSec と、AIM-VPN モジュールを使用するハードウェアベースの IPSec の両方がサポートされているので、柔軟な構成が可能です。

暗号化コールのスケーラビリティ

SRTP のメディア暗号化は、ルータの CPU ではなく、DSP モジュールで実行されます。DSP を搭載した音声ゲートウェイ インターフェイスの数を増やすか、プラットフォーム（サービス統合型ルータなど）に組み込む DSP の数を増やせば、安全な呼に利用できる DSP の数を増やすことができるので、効率的な拡張が可能です。

効率的な遅延最適化とチャネル容量への影響

暗号化コールにおいて、鍵の交換は通常の MGCP コール セットアップのなかで完了し、特別なメッセージは挿入されないの
で、コール セットアップに遅延が生じることはありません。また、SRTP によるメディア暗号化は DSP 上で実行されます。ルー
タの CPU で実行されるのでも、音声パケットを処理するための専用暗号化エンジンで実行されるのでもないため、音声メディ
アの遅延も生じません。

G.729 モードと G.729a モードでは、暗号化された呼によるチャネル容量への影響はありません。また、G.711 モードでもチャ
ネル容量への影響も最小限で済みます。DSP 単位でのチャネルへの影響は、以下の表のとおりです。

コーデック	通常の音声コール /DSP	暗号化音声コール /DSP
G.711	16 コール	10 コール
G.729a	8 コール	8 コール
G.729	6 コール	6 コール

管理機能

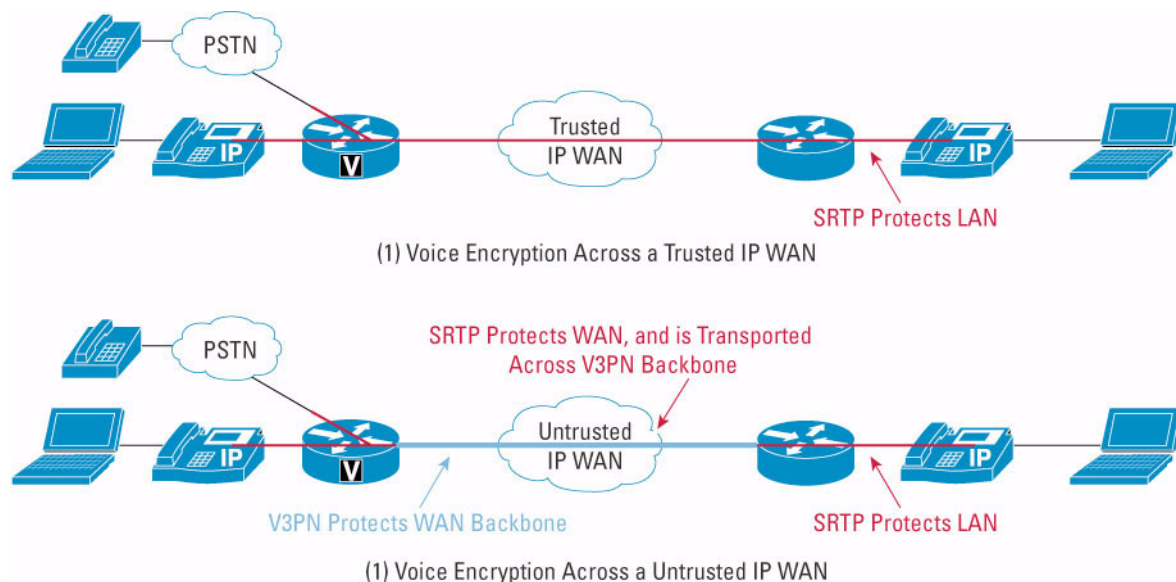
メディアの認証と暗号化は、CLI（コマンドライン インターフェイス）コマンドを使って、シスコのアクセス ルータに簡単に
設定できます。また、ロック アイコン インジケータのような Cisco IP Phone の機能によって、IP Phone とゲートウェイ間の暗
号化電話コールを視覚的に確認することもできます。コール フロー内にメディア暗号化をサポートしていないデバイスがある
場合や、セキュリティが何らかの理由で脆弱化した場合は、ロック アイコンは表示されません。CLI コマンドは、暗号化され
た呼に関する詳細情報の表示と確認や、呼のデバッグにも使用されます。

SRTP と IPSec V3PN の位置づけ

SRTP と IPSec VPN には、技術的にいくつか相違点があります。最も大きな違いは、SRTP がエンドツーエンド（IP Phone 間）
の暗号化を提供できるのに対し、IPSec VPN はルータ間のトンネルベースの暗号化であるという点です。また、SRTP は音声パ
ケットのみを暗号化しますが、IPSec VPN トンネルではデータ、音声、およびビデオを伝送できます。

SRTP は、IPSec VPN を補完する音声暗号化手段として使用できます。信頼できる WAN ネットワークを持つ大企業や中小・中
堅企業では、ネットワークをまたがるエンドツーエンドの音声暗号化に SRTP を使用できます。しかし、ほとんどの企業は、イ
ンターネットやサービス プロバイダーが管理する WAN を使って業務を行っています。したがって、WAN が安全であるとは
限らず、ブランチ オフィス間で安全にデータを伝送するためには VPN トンネルを使用する必要があります。SRTP を使用すれ
ば、データに使用している IPSec VPN ネットワークと同じ WAN 内で音声を保護できます。これを以下に図示します。

図 2 SRTTP および V3PN



サポート リリース

表 2 サポート リリース

モジュール サポート	プラットフォーム サポート	出荷開始時期	リリース (内部使用のみ)
NM-HD-1V、NM-HD-2V、 NM-HD-2VE	Cisco 2600XM、2691、ISR 2811、 ISR 2821、ISR 2851、3660、3700、 ISR 3800	2004 年 9 月	IOS 12.3(11)T および今後の Cisco CallManager リリース
NM-HDV2、NM-HDV2-1T1/E1*、 NM-HDV2-2T1/E1*	Cisco 2600XM、2691、ISR 2811、 ISR 2821、ISR 2851、3700、ISR 3800	2004 年 9 月	IOS 12.3(11)T および今後の Cisco CallManager リリース
PVDM2-8、PVDM2-16、PVDM2-32、 PVDM2-48、PVDM2-64	Cisco ISR 2811、ISR 2821、ISR 2851	2004 年 9 月	IOS 12.3(11)T および今後の Cisco CallManager リリース

* 日本では、E1 に設定されたモジュールのサポートは提供いたしません。

PVDM2 パケット / 音声 DSP モジュールは、Cisco ISR 2811/2821/2851 のオンボード スロットで使用できます。また、シスコ アクセス ルータの音声ゲートウェイ モジュールは、メディア暗号化をサポートしている Cisco 7940/7960/7970 IP Phone との相互運用性を提供します。Cisco 7970 は Cisco CallManager 4.0 リリースを使ってメディア暗号化をサポートできますが、Cisco 7960/7940 IP Phone については将来の Cisco CallManager リリースでメディア暗号化をサポートします。

まとめ

メディア認証とメディア暗号化は、IP コミュニケーションを導入している大企業や中小・中堅企業に新たなセキュリティレイヤをもたらします。TDM ポートとアナログ音声ゲートウェイ ポートのどちらで終端する音声会話も、標準ベースの暗号化を使用して LAN および WAN 内での盗聴から保護することができます。

製品仕様

表 3 製品仕様

製品の互換性	Cisco CallManager
ソフトウェアの互換性	Cisco IOS 12.3(11)T リリース Advanced IP Services イメージ Advanced Enterprise Services イメージ
プロトコル	Cisco MGCP 0.1

発注情報

表 4 発注情報

製品名	製品番号
IP コミュニケーション高密度デジタル音声ネットワーク モジュール	NM-HDV2
IP コミュニケーション高密度デジタル音声ネットワーク モジュール (内蔵 T1/E1 ポート × 1)	NM-HDV2-1T1/E1*
IP コミュニケーション高密度デジタル音声ネットワーク モジュール (内蔵 T1/E1 ポート × 2)	NM-HDV2-2T1/E1*
1 スロット IP コミュニケーション音声 / ファックス ネットワーク モジュール	NM-HD-1V
2 スロット IP コミュニケーション音声 / ファックス ネットワーク モジュール	NM-HD-2V
2 スロット IP コミュニケーション拡張音声 / ファックス ネットワーク モジュール	NM-HD-2VE
8 チャンネル パケット ファックス / 音声 DSP モジュール	PVDM2-8
16 チャンネル パケット ファックス / 音声 DSP モジュール	PVDM2-16
32 チャンネル パケット ファックス / 音声 DSP モジュール	PVDM2-32
48 チャンネル パケット ファックス / 音声 DSP モジュール	PVDM2-48
64 チャンネル パケット ファックス / 音声 DSP モジュール	PVDM2-64

* 日本では、E1 に設定されたモジュールのサポートは提供いたしません。

©2005 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
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。



シスコシステムズ株式会社

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

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

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先