



# SIP シグナリング暗号化

SIP シグナリング暗号化は、すべての SIP メッセージを発信側から着信側のドメインに送信するセキュアな暗号化転送を提供します。これにより、要求は着信側に安全に送信されます。SBC は、SIP シグナリング暗号化に対して次のサポートを提供します。

- セキュリティ保護された SIP コールは SBC を通過できます。
- SIP 隣接は、セキュリティ保護されていないとして設定されるか、非暗号化関連メカニズム（1つの信頼できる物理層リンクまたは信頼できるネットワークとのインターフェイスなど）によってセキュリティ保護されているとして設定されるか、または暗号化によってセキュリティ保護されているとして設定される場合があります。
- 暗号化がサポートされていないときにリモート ピアが暗号化を使用しようとする、着信接続および発信接続はすぐに終了します。
- 暗号化が必要なときにリモート ピアが暗号化を使用しない場合、着信接続および発信接続はすぐに終了します。
- 該当する show コマンドを使用することにより、特定の SIP 隣接に設定されたセキュリティ サポートのレベルを表示できます。
- 信頼できない隣接で受信したコールは、安全に暗号化された発信隣接でルーティングされない場合があります。
- 暗号化によってセキュリティ保護された隣接は、デフォルトでは、ポート 5061 で受信します。このポートは、異なる値に設定される場合があります。
- リモート ピアにより提供される証明書内の Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) は、要求を送信したドメインと照らし合わせてチェックされます。この 2 つが一致しない場合、信号はドロップされます。

## SIP シグナリング暗号化機能の履歴

リリース	変更点
Release 3.4.1	Cisco XR 12000 シリーズ ルータにこの機能が追加されました。
Release 3.5.0	変更なし

## この章の構成

この章で説明する内容は、次のとおりです。

- SIP シグナリング暗号化の実装の前提条件 (p.SBC-218)
- SIP シグナリング暗号化の実装の制約事項 (p.SBC-218)
- SIP シグナリング暗号化について (p.SBC-219)
- SIP シグナリング暗号化の設定方法 (p.SBC-221)
- 隣接に設定されているセキュリティ レベルを表示する show コマンドの例 (p.SBC-222)
- 参考資料 (p.SBC-223)

## SIP シグナリング暗号化の実装の前提条件

次に、SIP シグナリング暗号化を実装するための前提条件を示します。

- SIP シグナリング暗号化機能には、セキュリティ パッケージが必要です。
- ストア認証は、CEPKI インフラストラクチャにより生成されます。

## SIP シグナリング暗号化の実装の制約事項

SIP シグナリング暗号化には、次の制約事項が適用されます。

- 隣接が接続されている間、SIP 隣接でセキュリティ ポリシーを変更することはできません。
- SBC で唯一必要な暗号化サポートは、Transport Layer Security (TLS) での Secure Sockets Layer (SSL) です。IPSec および SCTP 暗号化はサポートされていません。
- SIP TLS コールでは、k9sec.pie をインストールし、SBC を設定する前にルータ証明書を設定する必要があります。このプロセスに従わない場合、SBC は TLS コールを拒否します。
- 証明書を生成、保存、または維持するには、SBC は不要です。この機能は CEPKI インフラストラクチャにより行われます。
- 暗号化された隣接は、暗号化されていないトラフィックを受け入れません。
- 暗号化されていない隣接は、暗号化されたトラフィックを受け入れません。
- SBC は、3xx リダイ렉션またはターゲットリフレッシュの結果として、セキュアな要求をセキュアでないターゲットにリダイレクトしたり、セキュアでない要求をセキュアなターゲットにリダイレクトしたりすることはありません。たとえば、SIPS Uniform Resource Identifier (URI; ユニフォーム リソース識別子) 宛てのコールは、SIP URI にはリダイレクトできません。これを試みた場合、負の INVITE 応答または両者への BYE が送信されることによってコールは拒否されます。
- エンドポイントは、SIPS 通信アドレスを提供しないかぎり、SIPS address-of-record の登録が許可されません。
- セキュリティ保護されていない隣接からセキュリティ保護されている隣接へのコールは許可されません。
- SBC では、信頼できるネットワーク エlement によるコールのセキュリティ ダウングレードに対する保護は行いません。発信コールがセキュアな隣接からプロキシに送信され、プロキシがこれをセキュアでないターゲットにリダイレクトしたのち SBC に返した場合、SBC は、このコールを信頼できない隣接から新しいターゲットに転送する場合があります。SBC はプロキシと安全に接続しているため、プロキシのルーティングの決定を信頼します。上記の例では、SBC では 2 つのコール レッグを異なるコールとして認識するため、着信コール レッグがセキュリティ保護されていたものだという事は判断できません。

## SIP シグナリング暗号化について

コールをルーティングまたは拒否する場合の 2 つの主要なセキュリティ上のポイントは、次のとおりです。

- SIPS URI へのコールは、セキュアである必要があります。SIP URI へのコールは、セキュアである必要はありません。
- 信頼できる隣接で受信された信号は、セキュアであるとみなされます。信頼できない隣接で受信された信号は、セキュアでないといみなされます。

### 隣接でのセキュリティ設定

次の 3 つのオプションを使用して、SIP 隣接にクライアントおよびサーバのセキュリティ サポートを個別に設定できます。

- **untrusted** : この隣接はいかなる手段によってもセキュリティ保護されていません。この隣接からはセキュアでないコール (SIPS URI 宛てではないコール) のみが送信できます。
- **trusted-encrypted** : この隣接では、セキュリティを保証するためにシグナリング暗号化が使用されます。暗号化には、ルータのデフォルトの証明書とキーが使用されます。この隣接からはセキュアなコール (SIPS URI へのコール) のみが送信できます。
- **trusted-unencrypted** : この隣接でのすべてのメッセージにセキュアなシグナリングを保証するために、SIP 以外のメカニズムが使用されます。たとえば、1 つの信頼できる物理リンクというメカニズムが使用される場合があります。この隣接からは、セキュアなコールもセキュアでないコールも送信されます。この設定により、暗号化をサポートしないエンドポイントがセキュアな SIP コールに参加できます。

### User Agent Server (UAS; ユーザ エージェント サーバ) 側の処理

着信要求は、2 つの点に基づいてマーキングされます。発信側が信頼できるかどうか、およびコールのターゲットがセキュアかどうかです。

発信側の信頼性は、次のように決定されます。

- 信頼できる隣接から着信した SIP 要求は、信頼できる要求としてマーキングされます。
- 信頼できない隣接から着信した SIP 要求は、信頼できない要求としてマーキングされます。

望ましいターゲットのセキュリティは、次のように決定されます。

- SIPS URI への要求は、発信セキュリティを必要とする要求としてマーキングされます。
- SIP URI への要求は、発信セキュリティを必要としない要求としてマーキングされます。

発信側が信頼できず、ターゲットがセキュリティを必要とする場合、着信要求は拒否されます。その他の組み合わせは、いずれもルーティング処理に転送されます。

### ルーティング処理

Routing Policy System (RPS; ルーティング ポリシー システム) ポリシーは、次のデフォルトの動作により、次に要求をどこにルーティングするかを決定します。

- コールが発信セキュリティを必要とする場合、RPS は信頼できる (trusted) 発信隣接のみを考慮します。
- コールが発信セキュリティを必要としない場合、RPS は信頼できない (untrusted) 発信隣接、または信頼できる暗号化されていない (trusted-unencrypted) 発信隣接を考慮します。

RPS がコールに適切な発信隣接を見つけることができない場合、コールは拒否されます。

## User Agent Client (UAC; ユーザ エージェント クライアント) 側の処理

発信隣接では、当初の要求の URI スキームを保存し、コールの当初のターゲットが SIPS URI であった場合、コールが SIPS URI に送信されるように保証します。また、コールの当初のターゲットが SIP URI であった場合、コールは SIPS URI に送信されます。

3xx クラスの応答およびターゲットリフレッシュの指示を受信すると、通信設定が検査されます。信頼できない隣接では、コールのターゲットは、SIPS ターゲットに再ルーティングできません。同様に、信頼できる隣接では、コールのターゲットは、SIP ターゲットに再ルーティングできません。リモートピアがこれを試みた場合、コールは拒否されます。

# SIP シグナリング暗号化の設定方法

ここでは、SIP シグナリング暗号化の設定手順を示します。

## SIP シグナリング暗号化の設定

### 手順の概要

1. `configure`
2. `sbc service-name`
3. `sbe`
4. `adjacency sip adjacency-name`
5. `security type`
6. `commit`
7. `exit`
8. `show services sbc service-name sbe adjacencies`

### 詳細手順

	コマンドまたはアクション	説明
ステップ 1	<code>configure</code>  例: RP/0/0/CPU0:router# <code>configure</code>	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	<code>sbc service-name</code>  例: RP/0/0/CPU0:router(config)# <code>sbc mysbc</code>	SBC サービス モードを開始します。 <ul style="list-style-type: none"><li>• サービス名を定義するには、<code>service-name</code> 引数を使用します。</li></ul>
ステップ 3	<code>sbe</code>  例: RP/0/0/CPU0:router(config-sbc)# <code>sbe</code>	SBC の SBE 機能モードを開始します。
ステップ 4	<code>adjacency sip adjacency-name</code>  例: RP/0/0/CPU0:router(config-sbc-sbe)# <code>adjacency sip test</code>	SBE SIP 隣接モードを開始します。 <ul style="list-style-type: none"><li>• サービス名を定義するには、<code>adjacency-name</code> 引数を使用します。</li></ul>

## ■ 隣接に設定されているセキュリティ レベルを表示する show コマンドの例

	コマンドまたはアクション	説明
ステップ 5	<b>security type</b>  <b>例:</b> RP/0/0/CPU:router(config-sbc-sbe-adj-sip)# security trusted-encrypted	この隣接でトランスポートレベルのセキュリティをどのように実装するかを詳細に設定します。このコマンドの no 形式を使用すると、この隣接がセキュリティ保護されないことを指定します。このフィールドは、隣接が接続されていない場合にのみ変更できます。  type に指定できる値は、次のとおりです。 <ul style="list-style-type: none"> <li>untrusted — 隣接はセキュリティ保護されません。</li> <li>trusted-encrypted — 隣接は暗号化によりセキュリティ保護されます。</li> <li>trusted-unencrypted — 隣接は、ほかの方法（1つの専用物理リンクなど）によりセキュリティ保護されていると想定されます。</li> </ul>
ステップ 6	<b>commit</b>  <b>例:</b> RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# commit	設定の変更を保存します。コンフィギュレーションセッションを維持したまま、設定変更を実行コンフィギュレーション ファイルに保存するには、 <b>commit</b> コマンドを使用します。
ステップ 7	<b>exit</b>  <b>例:</b> RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# exit	SIP モードを終了し、SBE モードに戻ります。exit コマンドを繰り返し入力して、モードを終了します。
ステップ 8	<b>show services sbc service-name sbe adjacencies</b>  <b>例:</b> RP/0/0/CPU0:router# show services sbc mysbc sbe adjacencies	すべての隣接で設定されているセキュリティ サポートのレベルを表示します。

## 隣接に設定されているセキュリティ レベルを表示する show コマンドの例

```
# show services sbc sbe adjacencies
SBC Service "TestSBC"
Adjacency SipA (SIP)
  Status:           Attached
  Signaling address: 10.1.0.2:5060
  Signaling-peer:   1.2.3.4
  Account:          ISP123
  Security:         Trusted-Encrypted
```

## 参考資料

ここでは、SBC での SIP シグナリング暗号化に関する参考資料について説明します。

## 関連資料

関連トピック	資料のタイトル
Cisco IOS XR マスター コマンド リファレンス	『Cisco IOS XR Master Commands List』
Cisco IOS XR SBC インターフェイス コンフィギュレーション コマンド	『Cisco IOS XR Session Border Controller Command Reference』
Cisco IOS XR ソフトウェアを使用するルータの初期システム ブートアップおよび設定情報	『Cisco IOS XR Getting Started Guide』
Cisco IOS XR コマンド モード	『Cisco IOS XR Command Mode Reference』

## 規格

規格	タイトル
この機能による新規または変更された規格のサポートはありません。また、この機能による既存の規格サポートに変更はありません。	—

## MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索し、ダウンロードするには、次の URL にある Cisco MIB Locator を使用して、Cisco Access Products メニューからプラットフォームを選択します。 <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFC

RFC	タイトル
RFC 3261	『SIP: Session Initiation Protocol』
RFC 2543	『Session Initiation Protocol』

## 技術サポート

説明	リンク
シスコ テクニカルサポート Web サイトには、製品、テクノロジー、ソリューション、テクニカルティップス、およびツールへのリンクなど、数千ページにわたる検索可能な技術コンテンツが含まれています。Cisco.com 登録ユーザは、このページにログインし、さらに多くのコンテンツにアクセスできます。	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>