セッション開始プロトコル（SIP）発信認証

SBC は SIP 発信認証をサポートしています。ネットワーク エンティティ同士が SIP を使用して通信する場合は、一方のエンティティが他方に対してチャレンジを行い、相手が自分のネットワークに SIP シグナリングを送信することが許可されているかどうか判断する必要がよくあります。SIP 認証モデルは、RFC 2617 に記述されているように、HTTP ダイジェスト認証に基づいています。

（注） パスワードが暗号化されずに送信される基本認証の使用は、SIP では許可されません。

SIP 発信認証の機能履歴

リリース	変更内容
リリース 3.4.1	この機能は、Cisco XR 12000 シリーズ ルータで導入されました。
リリース 3.5.0	変更なし。
リリース 3.5.1	**authentication-realm** コマンドが変更されました。

内容

このモジュールの構成は次のとおりです。

SIP 発信認証を実装するための前提条件

SIP 発信認証を実装するためには、次の前提条件が必要です。

- 1 つ以上の認証領域を指定する前に、SIP 隣接を設定する。
- 自己認証に使用できるドメイン セット（レルム）で SBC を設定します。これらの各ドメインによりチャレンジが行われたときに提供するユーザ名とパスワードを設定する。この設定は隣接ごとに行う。

（注） 隣接ごとに複数のレルムを設定でき、使用できるメモリ容量を考慮しなければ、レルムの数に制限はありません。同じユーザ名とパスワードを使用して異なるレルムを設定できます。また、各レルムは異なるユーザ名とパスワードを使用して異なる隣接に設定できます。ただし、1 つのレルムは隣接ごとに 1 回しか設定できません。

SIP 発信認証の実装上の制約事項

次に、SIP 発信認証に適用される制約事項を示します。

- SBC は、既存の認証レルムと同じドメイン名で認証レルムを設定しようとするどのような試行も拒否します。この制約事項は隣接単位で有効となります。同じドメイン名の認証レルムを複数の隣接に設定できます。

（注） 現行の CLI では、ユーザが同じ隣接に同じドメインで 2 つの認証レルムを設定することを禁止しています。これが試行された場合は、CLI は、2 番めの認証レルムの設定を最初の認証レルムの再設定と解釈し、適宜ユーザの認定証を更新します。

- 各認証レルムは、隣接ごとに 1 つのユーザ名とパスワードしか設定できません。

SIP 発信認証について

SBC での発信認証の設定

SIP 隣接を設定する場合に、ユーザが 1 つ以上の認証レルムを指定できます。各認証レルムはそれぞれリモート ドメインを表しており、SBC はそこから隣接の認証確認を受信します。認証レルムを設定するときには、SBC がそのレルムで自己認証するのに使用する正しいユーザ名およびパスワードを指定する必要があります。SBC は、各隣接の有効な認証レルムをすべて格納します。

SBC に対するリモート デバイスの認証

SBC は、送信済みの要求に関連付けることができる SIP 401 応答または 407 応答を受信すると、添付されている認証確認を確認します。SBC は、隣接で認証確認を受信した場合、その認証確認が隣接に設定されている認証レルムのいずれかに一致すると必ず応答します。設定されている認証レルムと一致しない認証チャレンジは、オリジナルの要求を受信した、その隣接の SBC のシグナリング ピアにそのまま渡されます。

認証確認への応答を生成するために、SBC は次の処理を実行します。

1. まず、発信隣接に設定されている認証レルムのリストを使用して、チャレンジのレルム パラメータを検索します。
2. 次に、該当する認証レルムのパスワードを見つけ、このパスワードとチャレンジに含まれているナンス パラメータとを組み合わせ、そのハッシュを作成して認証応答を生成します。
3. 認証確認側が保護品質として **auth-int** を要求した場合、SBC はメッセージ本文全体のハッシュも生成して応答に含めます。
4. SBC は、次のパラメータ値を含めて、Authorization（または Proxy-Authorization）ヘッダーを作成します（RFC 2617 に準拠）。
   - チャレンジに含まれているナンス
   - チャレンジに含まれているレルム
   - Digest-URI をチャレンジ要求の SIP URI に設定
   - Message-QOP を **auth** に設定
   - 前述のように計算された応答
   - 該当する認証レルムに指定されたユーザ名
   - チャレンジに **opaque** パラメータが含まれていた場合、応答時に変更されずに戻されます。
   - チャレンジに **qop-directive** パラメータが含まれる場合、このナンスを元に計算した応答を使用して、要求を送信した回数を **nonce-count** パラメータに設定します。
   - SBC が応答する必要があるどの認証確認にもドメイン パラメータが含まれているとは想定されていないことに注意してください。このパラメータは、SBC が最も頻繁に受信する認証確認である Proxy-Authenticate 認証確認には使用されません。ドメイン パラメータが含まれている場合、SBC はそのパラメータを無視します。
5. 最後に、SBC は計算した応答および受信したナンスを認証レルムの他のデータとともに格納します。これにより、SBC は同じナンスでこのレルムから送信される後続の認証確認に迅速に応答できます。応答を保存するためのリソースが不足している場合でも、SBC はそのまま処理を続行します。次回認証確認をこのレルムから受信したときに、SBC は応答を再計算する必要があります。SBC は、保存した応答を再利用する場合、ナンスと応答のペアとともに格納されているナンス カウントを更新します。これにより、SBC は Authorization 応答の **nonce-count** フィールドに値を正しく入力できます。

SIP 発信認証の設定方法

ここでは、SIP 発信認証の設定手順について説明します。この手順により、ユーザは隣接に対して 1 つ以上の認証レルムを追加または削除できます。

SIP 発信認証の設定

手順の概要

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*

5. **authentication-realm inbound** <*domain*> | **outbound** <*domain*> <*username*> <*password*>
6. **commit**
7. **exit**
8. **show services sbc** *service-name* **sbe adjacency** *adjacency-name* **authentication-realms**
9. **show services sbc** *service-name* **sbe all-authentication-realms**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# configure`	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	**sbc** *service-name* **例：** `RP/0/0/CPU0:router(config)# sbc mysbc`	SBC サービスのモードを開始します。 • *service-name* 引数を使用して、サービスの名前を定義します。
ステップ 3	**sbe** **例：** `RP/0/0/CPU0:router(config-sbc)# sbe`	SBC の Signaling Border Element（SBE）機能のモードを開始します。
ステップ 4	**adjacency sip** *adjacency-name* **例：** `RP/0/0/CPU0:router(config-sbc-sbe)# adjacency sip test`	SBE SIP 隣接のモードを開始します。 • *adjacency-name* 引数を使用して、サービスの名前を定義します。
ステップ 5	**authentication-realm inbound**<*domain*>**outbound** <*domain*><*username*><*password*> **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# authentication-realm example.com usersbc passwrdsbc`	指定した隣接に指定のドメイン用の認証クレデンシャルを設定します。このコマンドは、隣接を接続する前または後に実行することができます。 このコマンドの **no** バージョンを使用すると、特定の隣接の認証レルムの設定を解除します。 • inbound：着信認証レルムの指定。 • outbound：発信認証レルムの指定。 • domain：認証認定証が有効である対象ドメイ名。 • username：特定のドメインで SBC を識別するユーザ名。 • password：特定のドメインでユーザ名を認証するためのパスワード。
ステップ 6	**commit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# commit`	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 7	**exit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# exit`	adj-sip モードを終了し、SBE モードに戻ります。
ステップ 8	**show services sbc** *service-name* **sbe adjacency** *adjacency-name* **authentication-realms** **例：** `RP/0/0/CPU0:router# show services sbc mySbc sbe adjacency SipToIsp42 authentication-realms`	特定の SIP 隣接に対して現在設定されているすべての認証レルムを表示します。
ステップ 9	**show services sbc** *service-name* **sbe all-authentication-realms** **例：** `RP/0/0/CPU0:router# show services sbc mySbc sbe all-authentication-realms`	すべての SIP 隣接に対して現在設定されているすべての認証レルムを表示します。

show コマンドの例

```
# show services sbc mySbc sbe adjacency SipToIsp42 authentication-realms
Configured authentication realms
--------------------------------
Domain       Username  Password
Example.com  usersbc   passwordsbc


# show services sbc mySbc sbe all-authentication-realms
Configured authentication realms
--------------------------------
Adjacency: SipToIsp42
Domain       Username  Password     Example.com  usersbc   passwordsbc
Remote.com   usersbc   sbcpassword

Adjacency: SipToIsp50
Domain       Username  Password
Example.com  user2sbc  password2sbc
Other.com    sbcuser   sbcsbcsbc
```

その他の関連資料

ここでは、SBC での SIP 発信認証に関する関連資料について説明します。

関連資料

関連項目	マニュアル 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を初回に起動し設定するための情報	『*Cisco IOS XR Getting Started Guide*』
Cisco IOS XR コマンド モード	『*Cisco IOS XR Command Mode Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB の場所を特定して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。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』
RFC 2543	『*Session Initiation Protocol*』
RFC 2617	『*HTTP Authentication: Basic and Digest Access Authentication」*』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html