音声とビデオのプロトコルのインスペクションの設定

この章では、アプリケーション レイヤ プロトコル インスペクションを設定する方法について説明します。インスペクション エンジンは、ユーザのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルでは、高速パスでパケットを渡すのではなく、ASA で詳細なパケット インスペクションを行う必要があります。そのため、インスペクション エンジンがスループット全体に影響を与えることがあります。

ASA では、デフォルトでいくつかの一般的なインスペクション エンジンがイネーブルになっていますが、ネットワークによっては他のインスペクション エンジンをイネーブルにしなければならない場合があります。

この章は、次の項で構成されています。

- 「CTIQBE インスペクション」（P.11-1）
- 「H.323 インスペクション」（P.11-2）
- 「MGCP インスペクション」（P.11-12）
- 「RTSP インスペクション」（P.11-17）
- 「SIP インスペクション」（P.11-21）
- 「Skinny（SCCP）インスペクション」（P.11-33）

CTIQBE インスペクション

この項では、CTIQBE アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「CTIQBE インスペクションの概要」（P.11-1）
- 「制限事項」（P.11-2）

CTIQBE インスペクションの概要

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を越えてコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

制限事項

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションは、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- CTIQBE インスペクションのデバッグにより、メッセージ送信が遅延することがあり、これによってリアルタイム環境のパフォーマンスに影響が出る可能性があります。このデバッグまたはログをイネーブルにし、ASA を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと同じポートにスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

H.323 インスペクション

この項では、H.323 アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「H.323 インスペクションの概要」（P.11-3）
- 「H.323 の動作」（P.11-3）
- 「H.245 メッセージでの H.239 サポート」（P.11-4）
- 「制限事項」（P.11-5）
- 「Select H.323 Map」（P.11-5）
- 「H.323 Class Map」（P.11-5）
- 「Add/Edit H.323 Traffic Class Map」（P.11-6）
- 「Add/Edit H.323 Match Criterion」（P.11-6）
- 「H.323 Inspect Map」（P.11-7）

- 「Phone Number Filtering」（P.11-8）
- 「[Add/Edit H.323 Policy Map]（セキュリティ レベル）」（P.11-9）
- 「[Add/Edit H.323 Policy Map]（詳細）」（P.11-10）
- 「Add/Edit HSI Group」（P.11-11）
- 「Add/Edit H.323 Map」（P.11-11）

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager や VocalTec Gatekeeper など、H.323 準拠のアプリケーションをサポートします。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。ASA は、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 6 までサポートします。

H.323 インスペクションをイネーブルにした場合、ASA は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 8 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して、H.323 サーバへの TCP 接続を確立し、Q.931 コール セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、ASA が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。

（注）　RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート

- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

RAS シグナリング用に予約済み H.323 ポート 1719 のトラフィックを許可する必要があります。さらに、H.225 コール シグナリング用に、予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時には、ASA は、ACF および RCF メッセージのインスペクションに基づいて、H.225 接続を開きます。

H.225 メッセージを検査した後、ASA は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。ASA を通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同一の TCP パケットで送信される必要はないため、ASA は、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。ASA は、次のメッセージに備えて、TPKT 長が含まれるレコードを接続ごとに保持します。

ASA でメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、ASA がその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

（注） ASA は、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 インスペクションを受けるパケットが通る各 UDP 接続は、H.323 接続としてマークされ、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインで設定された H.323 タイムアウト値でタイムアウトします。

（注） Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス / ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。

H.245 メッセージでの H.239 サポート

ASA は、2 つの H.323 エンドポイントの間に存在します。2 つの H.323 エンドポイントが、スプレッドシート データなどのデータ プレゼンテーションを送受信できるようにテレプレゼンテーション セッションをセットアップするとき、ASA はエンドポイント間で H.239 ネゴシエーションが成功することを保証します。

H.239 は単一のコールで H.300 シリーズのエンドポイントに追加ビデオ チャネルを開く機能を提供する規格です。コールで、エンドポイント（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネルを送信します。H.239 ネゴシエーションは H.245 チャネルで発生します。

ASA が追加メディア チャネル用とメディア制御チャネル用のピンホールを開きます。エンドポイントは、Open Logical Channel Message（OLC; オープン論理チャネル メッセージ）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.245 バージョン 13 の一部です。

テレプレゼンテーション セッションの復号化と符号化はデフォルトでイネーブルにされます。H.239 の符号化と復号化は ASN.1 コーダによって実行されます。

制限事項

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション インスペクションは、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、ASA の問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

Select H.323 Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select H.323 Map]

[Select H.323 Map] ダイアログボックスでは、H.323 マップを選択または新しく作成できます。H.323 マップにより、H.323 アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select H.323 Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default H.323 inspection map]：デフォルトの H.323 マップの使用を指定します。
- [Select an H.323 map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

H.323 Class Map

[Configuration] > [Global Objects] > [Class Maps] > [H.323]

[H.323 Class Map] ペインでは、H.323 インスペクションのクラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name]：H.323 クラス マップの名前を示します。

- [Match Conditions]：クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：H.323 クラス マップの基準を示します。
  - [Value]：H.323 クラス マップで照合する値を示します。
- [Description]：クラス マップの説明を示します。
- [Add]：H.323 クラス マップを追加します。
- [Edit]：H.323 クラス マップを編集します。
- [Delete]：H.323 クラス マップを削除します。

Add/Edit H.323 Traffic Class Map

[Configuration] > [Global Objects] > [Class Maps] > [H.323] > [Add/Edit H.323 Traffic Class Map]

[Add/Edit H.323 Traffic Class Map] ダイアログボックスでは、H.323 クラス マップを定義できます。

フィールド

- [Name]：H.323 クラス マップの名前を 40 文字以内で入力します。
- [Description]：H.323 クラス マップの説明を入力します。
- [Add]：H.323 クラス マップを追加します。
- [Edit]：H.323 クラス マップを編集します。
- [Delete]：H.323 クラス マップを削除します。

Add/Edit H.323 Match Criterion

[Configuration] > [Global Objects] > [Class Maps] > [H.323] > [Add/Edit H.323 Traffic Class Map] > [Add/Edit H.323 Match Criterion]

[Add/Edit H.323 Match Criterion] ダイアログボックスでは、H.323 クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type]：基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：H.323 トラフィックに適用する照合基準を指定します。
  - [Called Party]：受信側を照合します。
  - [Calling Party]：発信元を照合します。
  - [Media Type]：メディア タイプを照合します。
- [Called Party Criterion Values]：H.323 受信側の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：H.323 発信元の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Media Type Criterion Values]：照合するメディア タイプを指定します。
  - [Audio]：音声タイプを照合します。
  - [Video]：ビデオ タイプを照合します。
  - [Data]：データ タイプを照合します。

H.323 Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [H.323]

[H.323] ペインでは、H.323 アプリケーションの事前に設定されたインスペクション マップを表示できます。H.323 マップでは、H.323 アプリケーション インスペクションのデフォルト設定値を変更できます。

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステート トラッキング、H.323 通話時間制限の適用、音声 / ビデオ制御をサポートします。

フィールド

- [H.323 Inspect Maps]：定義されている H.323 インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい H.323 インスペクション マップを設定します。H.323 インスペクション マップを編集するには、[H.323 Inspect Maps] テーブルで H.323 のエントリを選択し、[Customize] をクリックします。
- [Delete]：[H.323 Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    H.225 状態確認：ディセーブル

    RAS 状態確認：ディセーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制しない
  - Medium

H.225 状態確認：イネーブル

RAS 状態確認：イネーブル

発信側の番号：ディセーブル

通話制限時間：ディセーブル

RTP 準拠：適用強制する

ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない

- High

H.225 状態確認：イネーブル

RAS 状態確認：イネーブル

発信側の番号：イネーブル

通話制限時間：1:00:00

RTP 準拠：適用強制する

ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- [Phone Number Filtering]：[Phone Number Filtering] ダイアログボックスが開き、電話番号フィルタを設定できます。
- [Customize]：[Add/Edit H.323 Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトの Medium レベルに戻します。

Phone Number Filtering

[Configuration] > [Global Objects] > [Inspect Maps] > [H323] > [Phone Number Filtering]

[Phone Number Filtering] ダイアログボックスでは、電話番号のフィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add Phone Number Filter] ダイアログボックスが開き、電話番号のフィルタを追加できます。
- [Edit]：[Edit Phone Number Filter] ダイアログボックスが開き、電話番号を編集できます。
- [Delete]：電話番号のフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

[Add/Edit H.323 Policy Map]（セキュリティ レベル）

[Configuration] > [Global Objects] > [Inspect Maps] > [H323] > [H323 Inspect Map] > [Basic View]

[Add/Edit H.323 Policy Map] ペインでは、H.323 アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- [Description]：H323 マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High、Medium、Low）を選択します。
  - Low：デフォルト

    H.225 状態確認：ディセーブル

    RAS 状態確認：ディセーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制しない
  - Medium

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：ディセーブル

    通話制限時間：ディセーブル

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない
  - High

    H.225 状態確認：イネーブル

    RAS 状態確認：イネーブル

    発信側の番号：イネーブル

    通話制限時間：1:00:00

    RTP 準拠：適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用：する
  - [Phone Number Filtering]：[Phone Number Filtering] ダイアログボックスが開き、電話番号のフィルタを設定できます。
  - [Default Level]：セキュリティ レベルをデフォルトに戻します。
- [Details]：詳細な設定を行うための [State Checking] タブ、[Call Attributes] タブ、[Tunneling and Protocol Conformance] タブ、[HSI Group Parameters] タブ、および [Inspections] タブを表示します。

[Add/Edit H.323 Policy Map]（詳細）

[Configuration] > [Global Objects] > [Inspect Maps] > [H323] > [H323 Inspect Map] > [Advanced View]

[Add/Edit H.323 Policy Map] ペインでは、H.323 アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：H.323 マップの追加時に H.323 マップの名前を入力します。H.323 マップの編集時には、事前に設定した H.323 マップの名前が表示されます。
- [Description]：H.323 マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルと電話番号フィルタリング設定を表示します。
- [State Checking]：このタブで H.323 インスペクション マップの状態確認パラメータを設定します。
  - [Check state transition of H.225 messages]：H.323 の状態確認を H.225 メッセージに適用します。
  - [Check state transition of RAS messages]：H.323 の状態確認を RAS メッセージに適用します。
  - RFC メッセージを確認し、RFQ メッセージ内のコール シグナル アドレス用のピンホールを開きます。

（注） Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス / ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。[H.323 Inspect Map] のオプションを設定して、このオプションをイネーブルにすることができます。

- [Call Attributes]：このタブで H.323 インスペクション マップのコール属性パラメータを設定します。
  - [Enforce call duration limit]：通話を一定の時間で制限します。

    [Call Duration Limit]：通話制限時間（hh:mm:ss）。
  - [Enforce presence of calling and called party numbers]：通話設定時に、強制的に発信側の番号を送信します。
- [Tunneling and Protocol Conformance]：このタブで H.323 インスペクション マップのトンネリングとプロトコル準拠パラメータを設定します。
  - [Check for H.245 tunneling]：H.245 のトンネリングを許可します。

    [Action]：Drop connection または Log。
  - [Check RTP packets for protocol conformance]：ピンホールの RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- [HSI Group Parameters]：このタブで HSI グループを設定します。

  - [HSI Group ID]：HSI グループの ID を示します。
  - [IP Address]：HSI グループの IP アドレスを示します。
  - [Endpoints]：HSI グループのエンドポイントを示します。
  - [Add]：[Add HSI Group] ダイアログボックスが開き、HSI グループを追加できます。
  - [Edit]：[Edit HSI Group] ダイアログボックスが開き、HSI グループを編集できます。
  - [Delete]：HSI グループを削除します。
- [Inspections]：このタブで H.323 インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：H.323 インスペクションの基準を示します。
  - [Value]：H.323 インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add H.323 Inspect] ダイアログボックスが開き、H.323 インスペクションを追加できます。
  - [Edit]：[Edit H.323 Inspect] ダイアログボックスが開き、H.323 インスペクションを編集できます。
  - [Delete]：H.323 インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

Add/Edit HSI Group

[Configuration] > [Global Objects] > [Inspect Maps] > [H323] > [H323 Inspect Map] > [Advanced View] > [Add/Edit HSI Group]

[Add/Edit HSI Group] ダイアログボックスでは、HSI グループを設定できます。

フィールド

- [Group ID]：HSI のグループ ID を入力します。
- [IP Address]：HSI の IP アドレスを入力します。
- [Endpoints]：エンドポイントの IP アドレスとインターフェイスを設定します。
  - [IP Address]：エンドポイントの IP アドレスを入力します。
  - [Interface]：エンドポイントのインターフェイスを指定します。
- [Add]：定義された HSI グループを追加します。
- [Delete]：選択した HSI グループを削除します。

Add/Edit H.323 Map

[Configuration] > [Global Objects] > [Inspect Maps] > [H232] > [H323 Inspect Map] > [Advanced View] > [Add/Edit H323 Inspect]

[Add/Edit H.323 Inspect] ダイアログボックスでは、H.323 インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：H.323 インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：H.323 トラフィックに適用する照合基準を指定します。
  - [Called Party]：受信側を照合します。
  - [Calling Party]：発信元を照合します。
  - [Media Type]：メディア タイプを照合します。
- [Called Party Criterion Values]：H.323 受信側の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：H.323 発信元の照合方法を指定します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Media Type Criterion Values]：照合するメディア タイプを指定します。
  - [Audio]：音声タイプを照合します。
  - [Video]：ビデオ タイプを照合します。
  - [Data]：データ タイプを照合します。
- [Multiple Matches]：H.323 インスペクションの複数の照合文を指定します。
  - [H323 Traffic Class]：H.323 トラフィック クラスを照合します。
  - [Manage]：[Manage H.323 Class Maps] ダイアログボックスが開き、H.323 クラス マップの追加、編集、削除ができます。
- [Action]：Drop Packet、Drop Connection、または Reset。

MGCP インスペクション

この項では、MGCP アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「MGCP インスペクションの概要」（P.11-13）

- 「Select MGCP Map」（P.11-15）
- 「MGCP インスペクション マップ」（P.11-15）
- 「Gateways and Call Agents」（P.11-15）
- 「Add/Edit MGCP Policy Map」（P.11-16）
- 「Add/Edit MGCP Group」（P.11-17）

MGCP インスペクションの概要

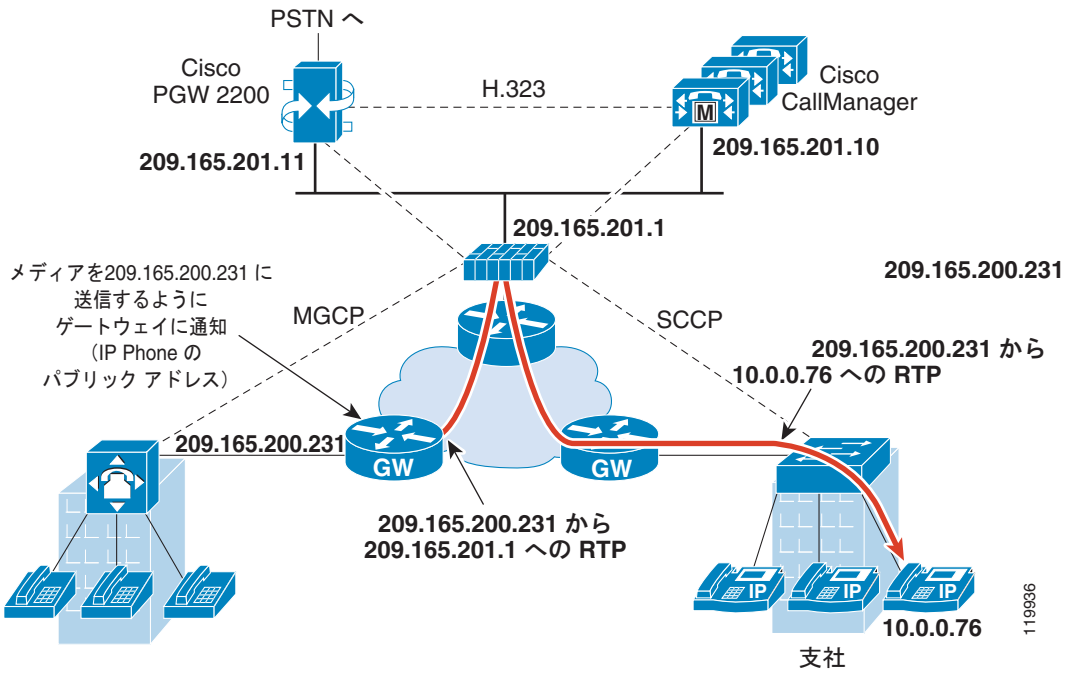
MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用するマスター / スレーブ プロトコルです。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 *soft PBX* インターフェイスを Voice over IP ネットワークに提供します。

（注） ASA バージョン 7.1 からのアップグレード時にポリシーがエラーにならないように、レイヤ 7 およびレイヤ 3 のポリシーにはすべて固有の名前を付ける必要があります。たとえば、以前に設定されたポリシー マップの名前が以前に設定された MGCP マップと同じである場合は、アップグレードの前に変更する必要があります。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。図 11-1 に、MGCP でどのように NAT が使用されるかを示します。

図 11-1　NAT と MGCP の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

MGCP トランザクションは、コマンドと必須応答で構成されます。次の 8 種類のコマンドがあります。

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

最初の 4 つのコマンドは、コール エージェントからゲートウェイに送信されます。Notify コマンドは、ゲートウェイからコール エージェントに送信されます。ゲートウェイは、DeleteConnection を送信することもあります。MGCP ゲートウェイをコール エージェントに登録するには、RestartInProgress コマンドを使用します。AuditEndpoint コマンドおよび AuditConnection コマンドは、コール エージェントからゲートウェイに送信されます。

すべてのコマンドは、コマンド ヘッダーと、その後ろに続くオプションのセッション記述で構成されます。すべての応答は、応答ヘッダーと、その後ろに続くオプションのセッション記述で構成されます。

- ゲートウェイがコール エージェントからのコマンドを受信するポート。通常、ゲートウェイは UDP ポート 2427 を受信します。

- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 を受信します。

（注） MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、ASA は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

Select MGCP Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select MGCP Map]

[Select MGCP Map] ダイアログボックスでは、MGCP マップを選択または新しく作成できます。MGCP マップにより、MGCP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select MGCP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default MGCP inspection map]：デフォルトの MGCP マップの使用を指定します。
- [Select an MGCP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

MGCP インスペクション マップ

[Configuration] > [Global Objects] > [Inspect Maps] > [MGCP]

[MGCP] ペインでは、MGCP アプリケーションの事前に設定されたインスペクション マップを表示できます。MGCP マップでは、MGCP アプリケーション インスペクションのデフォルト設定値を変更できます。MGCP マップを使用して、VoIP デバイスと MGCP コール エージェント間の接続を管理できます。

フィールド

- [MGCP Inspect Maps]：定義されている MGCP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい MGCP インスペクション マップを設定します。
- [Edit]：[MGCP Inspect Maps] テーブルで選択した MGCP のエントリを編集します。
- [Delete]：[MGCP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

Gateways and Call Agents

[Configuration] > [Global Objects] > [Inspect Maps] > [MGCP] > [Gateways and Call Agents]

[Gateways and Call Agents] ダイアログボックスでは、ゲートウェイとコール エージェントのグループをマップに設定できます。

フィールド

- [Group ID] : コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。0 ～ 2147483647 の範囲の値を指定できます。[Criterion] : インスペクションの基準を示します。
- [Gateways] : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
- [Call Agents] : コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- [Add] : [Add MGCP] ダイアログボックスが表示され、新規のアプリケーション インスペクション マップを定義できます。
- [Edit] : [Edit MGCP] ダイアログボックスが表示され、アプリケーション インスペクション マップ テーブルで選択したインスペクション マップを修正できます。
- [Delete] : アプリケーション インスペクション マップ テーブルで選択したインスペクション マップを削除します。

Add/Edit MGCP Policy Map

[Configuration] > [Global Objects] > [Inspect Maps] > [MGCP] > [MGCP Inspect Map] > [View]

[Add/Edit MGCP Policy Map] ペインでは、MGCP アプリケーション インスペクション マップのコマンド キュー、ゲートウェイ、およびコール エージェントの設定値を設定できます。

フィールド

- [Name] : MGCP マップの追加時に MGCP マップの名前を入力します。MGCP マップの編集時には、事前に設定した MGCP マップの名前が表示されます。
- [Description] : MGCP マップの説明を 200 文字以内で入力します。
- [Command Queue] : このタブで MGCP コマンドの許容キュー サイズを指定します。
  - [Command Queue Size] : キューに入れるコマンドの最大数を指定します。1 ～ 2147483647 の範囲の値を指定できます。
- [Gateways and Call Agents] : このタブでゲートウェイとコール エージェント グループをマップに設定します。
  - [Group ID] : コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。ゲートウェイの IP アドレスは、1 つのグループ ID だけに関連付けできます。同じゲートウェイを別のグループ ID で使用できません。0 ～ 2147483647 の範囲の値を指定できます。[Criterion] : インスペクションの基準を示します。
  - [Gateways] : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを識別します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。

- [Call Agents]: コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを識別します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
- [Add] : [Add MGCP Group] ダイアログボックスが表示され、ゲートウェイとコール エージェントの新規の MGCP グループを定義できます。
- [Edit] : [Edit MGCP] ダイアログボックスが表示され、[Gateways and Call Agents] テーブルで選択した MGCP グループを修正できます。
- [Delete] : [Gateways and Call Agents] テーブルで選択した MGCP グループを削除します。

Add/Edit MGCP Group

[Configuration] > [Global Objects] > [Inspect Maps] > [MGCP] > [Add/Edit MGCP Group]

[Add/Edit MGCP Group] ダイアログボックスでは、MGCP アプリケーション インスペクションがイネーブルのときに使用される MGCP グループのコンフィギュレーションを定義できます。

フィールド

- [Group ID] : コール エージェント グループの ID を指定します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。
  - [Gateway to Be Added] : 関連付けられたコール エージェントによって制御されるメディア ゲートウェイの IP アドレスを指定します。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（2727）に送信します。
  - [Add] : 指定した IP アドレスを IP アドレス テーブルに追加します。
  - [Delete] : 選択した IP アドレスを IP アドレス テーブルから削除します。
  - [IP Address] : コール エージェント グループに設定されているゲートウェイの IP アドレスを一覧表示します。
- Call Agents
  - [Call Agent to Be Added] : コール エージェント グループの MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを指定します。通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（2427）に送信します。
  - [Add] : 指定した IP アドレスを IP アドレス テーブルに追加します。
  - [Delete] : 選択した IP アドレスを IP アドレス テーブルから削除します。
  - [IP Address] : コール エージェント グループに設定されているコール エージェントの IP アドレスを一覧表示します。

RTSP インスペクション

この項では、RTSP アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「RTSP インスペクションの概要」（P.11-18）
- 「RealPlayer の使用方法」（P.11-18）

- 「制限事項」（P.11-19）
- 「Select RTSP Map」（P.11-19）
- 「RTSP Inspect Map」（P.11-19）
- 「Add/Edit RTSP Policy Map」（P.11-20）
- 「Add/Edit RTSP Inspect」（P.11-20）

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、ASA は RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続によって使用されます。

（注）　Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声 / ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA は、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合は、サーバは ASA との相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、ASA では、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、ASA は、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer の使用方法

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバからクライアントに、またはその逆に **access-list** コマンドを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、ASA で、**inspect rtsp** *port* コマンドを追加します。

制限事項

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化する可能性があり、ASA はフラグメント化されたパケットに対して NAT を実行できません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

Select RTSP Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select NetBIOS Map]

[Select RTSP Map] ダイアログボックスでは、RTSP マップを選択または新しく作成できます。RTSP マップにより、RTSP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select RTSP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default RTSP inspection map]：デフォルトの RTSP インスペクション マップの使用を指定します。
- [Select a RTSP inspect map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。

RTSP Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [RADIUS]

[RTSP] ペインでは、RTSP アプリケーションの事前に設定されたインスペクション マップを表示できます。RTSP マップでは、RTSP アプリケーション インスペクションのデフォルト設定値を変更できます。RTSP マップを使用して、RTSP トラフィックを保護できます。

フィールド

- [RTSP Inspect Maps]：定義されている RTSP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい RTSP インスペクション マップを設定します。
- [Edit]：[RTSP Inspect Maps] テーブルで選択した RTSP のエントリを編集します。

- [Delete]：[RTSP Inspect Maps] テーブルで選択したインスペクション マップを削除します。

Add/Edit RTSP Policy Map

[Configuration] > [Global Objects] > [Inspect Maps] > [MGCP] > [MGCP Inspect Map] > [View]

[Add/Edit RTSP Policy Map] ペインでは、RTSP アプリケーション インスペクション マップのパラメータとインスペクション設定値を設定できます。

フィールド

- [Name]：RTSP マップの追加時に RTSP マップの名前を入力します。RTSP マップの編集時には、事前に設定した RTSP マップの名前が表示されます。
- [Description]：RTSP マップの説明を 200 文字以内で入力します。
- [Parameters]：このタブで、メディア ポート ネゴシエーション中の予約済みポートの使用を制限し、URL の長さ制限を設定できます。
  - [Enforce Reserve Port Protection]：メディア ポート ネゴシエーション中の予約済みポートの使用を制限できます。
  - [Maximum URL Length]：メッセージで許容される URL の最大長を指定します。6000 以下の値を指定します。
- [Inspections]：このタブで RTSP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：RTSP インスペクションの基準を示します。
  - [Value]：RTSP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add RTSP Inspect] ダイアログボックスが開き、RTSP インスペクションを追加できます。
  - [Edit]：[Edit RTSP Inspect] ダイアログボックスが開き、RTSP インスペクションを編集できます。
  - [Delete]：RTSP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

Add/Edit RTSP Inspect

[Configuration] > [Global Objects] > [Inspect Maps] > [SIP] > [SIP Inspect Map] > [Advanced View] > [Add/Edit SIP Inspect]

[Add/Edit RTSP Inspect] ダイアログボックスでは、RTSP インスペクション マップの照合基準、値、およびアクションを定義できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

- [Criterion]：RTSP トラフィックに適用する照合基準を指定します。
  - [URL Filter]：URL フィルタリングを照合します。
  - [Request Method]：RTSP の要求方式を照合します。
- [URL Filter Criterion Values]：URL フィルタリングを照合するために指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [URL Filter Actions]：プライマリ アクションおよびログを設定します。
  - [Action]：Drop connection または Log。
  - [Log]：イネーブルまたはディセーブルにします。
- [Request Method Criterion Values]：照合する RTSP 要求方式を指定します。
  - [Request Method]：要求方式を announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかから指定します。
- [Request Method Actions]：プライマリ アクションを設定します。
  - [Action]：Limit rate (pps)。

SIP インスペクション

この項では、SIP アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「SIP インスペクションの概要」（P.11-22）
- 「SIP インスタント メッセージ」（P.11-22）
- 「Select SIP Map」（P.11-23）
- 「SIP Class Map」（P.11-24）
- 「Add/Edit SIP Traffic Class Map」（P.11-25）
- 「Add/Edit SIP Match Criterion」（P.11-25）
- 「SIP インスペクション マップ」（P.11-27）
- 「[Add/Edit SIP Policy Map]（セキュリティ レベル）」（P.11-28）
- 「[Add/Edit SIP Policy Map]（詳細）」（P.11-29）
- 「Add/Edit SIP Inspect」（P.11-31）

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、ASA は SIP VoIP ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 3261
- SDP：Session Description Protocol、RFC 2327

ASA 経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP インスペクションは、それらの埋め込まれた IP アドレスに NAT を適用します。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
  - スタティック PAT の設定は、SIP インスペクションではサポートされません。スタティック PAT が Cisco Unified Communications Manager 用に設定されている場合は、SIP インスペクションが SIP パケットをリライトできません。Cisco Unified Communications Manager に 1 対 1 のスタティック NAT を設定します。
- SDP 部分の所有者 / 作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）-Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されている SIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注）　現在は、チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションは、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションでは、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されます。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。ASA は、これらのメディア アドレス / ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがどの RTP ポートで受信するかを知らされるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、ASA のコンフィギュレーションで特別に許可されない限り、ASA を通過できません。

Select SIP Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select SIP Map]

[Select SIP Map] ダイアログボックスでは、SIP マップを選択または新しく作成できます。SIP マップにより、SIP アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SIP Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SIP inspection map]：デフォルトの SIP マップの使用を指定します。
- [Select a SIP map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。
- [Enable encrypted traffic inspection] チェックボックス：プロキシ タイプを選択するオプション ボタンをイネーブルにする場合に選択します。
- Proxy Type

  - [TLS Proxy] オプション ボタン：TLS プロキシを使用して、暗号化トラフィックのインスペクションをイネーブルにします。
  - [Phone Proxy] オプション ボタン：電話プロキシを、[TLS Proxy Name] フィールドから選択した TLS プロキシに関連付けることを指定します。

    [Configure] ボタン：[Configure the Phone Proxy] ダイアログボックスを開き、そこで電話プロキシのコンフィギュレーション設定を指定または編集できます。
  - [UC-IME Proxy] オプション ボタン：UC-IME プロキシ（Cisco Intercompany Media Engine Proxy）を、[TLS Proxy Name] フィールドから選択した TLS プロキシに関連付けることを指定します。

    [Configure] ボタン：[Configure the UC-IME Proxy] ダイアログボックスを開き、そこで UC-IME プロキシのコンフィギュレーション設定を指定または編集できます。
- [TLS Proxy Name]：既存の TLS プロキシの名前。
- [Manage]：TLS プロキシを追加するための [Add TLS Proxy] ダイアログボックスを開きます。

電話プロキシまたは UC-IME プロキシに一度に割り当てることができるのは、1 つの TLS プロキシのみです。電話プロキシまたは UC-IME プロキシ インスペクションに複数のサービス ポリシー ルールを設定し、異なる TLS プロキシをそれらのルールに割り当てようとすると、ASDM は、電話プロキシと UC-IME インスペクションに設定されているその他のすべてのサービス ポリシー ルールが、最後に選択された TLS プロキシを使用するように変更されるという警告を表示します。

UC-IME プロキシ コンフィギュレーションでは、2 つの TLS プロキシ（発信トラフィック用と着信トラフィック用）が必要です。TLS プロキシを UC-IME プロキシに直接関連付けるのではなく、電話プロキシの場合のように、TLS プロキシは SIP インスペクション ルールを介して UC-IME プロキシに間接的に関連付けられます。

SIP インスペクション アクションの定義時に、TLS プロキシを電話プロキシに関連付けます。ASDM は、この関連付けを既存の電話プロキシに変換します。

SIP Class Map

[Configuration] > [Global Objects] > [Class Maps] > [SIP]

[SIP Class Map] ペインでは、SIP インスペクションの SIP クラス マップを設定できます。

インスペクション クラス マップで、アプリケーションのトラフィックをアプリケーション固有の基準と照合します。次に、クラス マップをインスペクション マップから特定して、アクションをイネーブルにします。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるという点です。インスペクション クラス マップは DNS、FTP、H.323、HTTP、IM、SIP のアプリケーションでサポートされます。

フィールド

- [Name]：SIP クラス マップの名前を示します。
- [Match Conditions]：クラス マップに設定されているタイプ、照合基準、値を示します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：SIP クラス マップの基準を示します。
  - [Value]：SIP クラス マップで照合する値を示します。
- [Description]：クラス マップの説明を示します。
- [Add]：SIP クラス マップを追加します。

- [Edit] : SIP クラス マップを編集します。
- [Delete] : SIP クラス マップを削除します。

Add/Edit SIP Traffic Class Map

[Configuration] > [Global Objects] > [Class Maps] > [SIP] > [Add/Edit SIP Traffic Class Map]

[Add/Edit SIP Traffic Class Map] ダイアログボックスでは、SIP クラス マップを定義できます。

フィールド

- [Name] : SIP クラス マップの名前を 40 文字以内で入力します。
- [Description] : SIP クラス マップの説明を入力します。
- [Add] : SIP クラス マップを追加します。
- [Edit] : SIP クラス マップを編集します。
- [Delete] : SIP クラス マップを削除します。

Add/Edit SIP Match Criterion

[Configuration] > [Global Objects] > [Class Maps] > [SIP] > [Add/Edit SIP Traffic Class Map] > [Add/Edit SIP Match Criterion]

[Add/Edit SIP Match Criterion] ダイアログボックスでは、SIP クラス マップの照合基準と値を定義できます。

フィールド

- [Match Type] : 基準に一致したトラフィックをクラス マップに含めるか、または一致しないトラフィックを含めるか指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion] : SIP トラフィックに適用する照合基準を指定します。
  - [Called Party] : To ヘッダーに指定された受信側を照合します。
  - [Calling Party] : From ヘッダーに指定された発信元を照合します。
  - [Content Length] : ヘッダーのコンテンツの長さを照合します。0 ～ 65536 の範囲の値です。
  - [Content Type] : ヘッダーのコンテンツ タイプを照合します。
  - [IM Subscriber] : SIP IM の加入者を照合します。
  - [Message Path] : SIP の Via ヘッダーを照合します。
  - [Request Method] : SIP の要求方式を照合します。
  - [Third-Party Registration] : サード パーティの登録要求者を照合します。
  - [URI Length] : SIP ヘッダーにある URI を照合します。0 ～ 65536 の範囲の値です。
- [Called Party Criterion Values] : 照合する受信側を指定します。正規表現で照合します。
  - [Regular Expression] : 照合する定義された正規表現を一覧表示します。
  - [Manage] : [Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Calling Party Criterion Values]：照合する発信元を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Content Length Criterion Values]：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。
- [Content Type Criterion Values]：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - [SDP]：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - [Regular Expression]：正規表現を照合します。

    [Regular Expression]：照合する定義された正規表現を一覧表示します。

    [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

    [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

    [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [IM Subscriber Criterion Values]：照合する IM 登録者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Message Path Criterion Values]：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Request Method Criterion Values]：照合する SIP 要求方式を指定します。
  - [Request Method]：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- [Third-Party Registration Criterion Values]：照合するサード パーティの登録要求者を指定します。正規表現で照合します。

  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [URI Length Criterion Values]：SIP ヘッダーで指定した値より長い、選択したタイプの URI を照合します。
  - [URI type]：SIP URI または TEL URI を指定して照合します。
  - [Greater Than Length]：長さをバイト単位で指定します。

SIP インスペクション マップ

[Configuration] > [Global Objects] > [Inspect Maps] > [SIP]

[SIP] ペインでは、SIP アプリケーションの事前に設定されたインスペクション マップを表示できます。SIP マップでは、SIP アプリケーション インスペクションのデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタント メッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

フィールド

- [SIP Inspect Maps]：定義されている SIP インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい SIP インスペクション マップを設定します。SIP インスペクション マップを編集するには、[SIP Inspect Maps] テーブルで SIP のエントリを選択し、[Customize] をクリックします。
- [Delete]：[SIP Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制しない

    SIP 準拠：ステート チェックとヘッダー検証を実行しない
  - Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

サーバとエンドポイントの IP アドレスを非表示：ディセーブル

ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：しない

SIP 準拠：ステート チェックで失敗したパケットをドロップ

– High

SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：禁止

サーバとエンドポイントの IP アドレスを非表示：ディセーブル

ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル

1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：する

SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

– [Customize]：[Add/Edit SIP Policy Map] ダイアログボックスを開き、追加の設定を行います。
– [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

[Add/Edit SIP Policy Map]（セキュリティ レベル）

[Configuration] > [Global Objects] > [Inspect Maps] > [SIP] > [SIP Inspect Map] > [Basic View]

[Add/Edit SIP Policy Map] ペインでは、SIP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- [Description]：SIP マップの説明を 200 文字以内で入力します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  – Low：デフォルト

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

    SIP トラフィック以外の SIP ポート使用：許可

    サーバとエンドポイントの IP アドレスを非表示：ディセーブル

    ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

    1 以上の宛先ホップ カウントを保証：イネーブル

    RTP 準拠：適用強制しない

    SIP 準拠：ステート チェックとヘッダー検証を実行しない

  – Medium

    SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：許可

サーバとエンドポイントの IP アドレスを非表示：ディセーブル

ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル

1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：しない

SIP 準拠：ステート チェックで失敗したパケットをドロップ

- High

SIP インスタント メッセージ（IM）の拡張機能：イネーブル

SIP トラフィック以外の SIP ポート使用：禁止

サーバとエンドポイントの IP アドレスを非表示：ディセーブル

ソフトウェアのバージョンと SIP 以外の URI をマスク：イネーブル

1 以上の宛先ホップ カウントを保証：イネーブル

RTP 準拠：適用強制する

ペイロードを音声やビデオに限定してシグナリング交換を適用：する

SIP 準拠：ステート チェックとヘッダー検証で失敗したパケットをドロップ

- [Default Level]：セキュリティ レベルをデフォルトに戻します。

- [Details]：追加の設定を行うフィルタリング、IP アドレスのプライバシー、ホップ カウント、RTP 準拠、SIP 準拠、フィールド マスク、およびインスペクションの設定値を表示します。

[Add/Edit SIP Policy Map]（詳細）

[Configuration] > [Global Objects] > [Inspect Maps] > [SIP] > [SIP Inspect Map] > [Advanced View]

[Add/Edit SIP Policy Map] ペインでは、SIP アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SIP の追加時に SIP マップの名前を入力します。SIP マップの編集時には、事前に設定した SIP マップの名前が表示されます。
- [Description]：SIP マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルを表示します。
- [Filtering]：このタブで SIP のフィルタリングを設定します。
  - [Enable SIP instant messaging (IM) extensions]：インスタント メッセージの拡張機能をイネーブルにします。デフォルトはイネーブルです。
  - [Permit non-SIP traffic on SIP port]：SIP トラフィック以外に SIP ポートの使用を許可します。デフォルトは許可です。
- [IP Address Privacy]：このタブで SIP の IP アドレスのプライバシーを設定します。
  - [Hide server's and endpoint's IP addresses]：IP アドレスのプライバシーをイネーブルにします。デフォルトでは、ディセーブルです。
- [Hop Count]：このタブで SIP のホップ カウントを設定します。

  - [Ensure that number of hops to destination is greater than 0]：Max-Forwards ヘッダーの値が 0 かどうかのチェックをイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。

- [RTP Conformance]：このタブで SIP の RTP 準拠を設定します。
  - [Check RTP packets for protocol conformance]：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。

- [SIP Conformance]：このタブで SIP の SIP 準拠を設定します。
  - [Enable state transition checking]：SIP のステート チェックをイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。
  - [Enable strict validation of header fields]：SIP ヘッダー フィールドの検証をイネーブルにします。

    [Action]：Drop packet、Drop Connection、Reset、または Log。

    [Log]：イネーブルまたはディセーブルにします。

- [Field Masking]：このタブで SIP のフィールド マスクを設定します。
  - [Inspect non-SIP URIs]：Alert-Info と Call-Info ヘッダーに含まれる SIP 以外の URI インスペクションをイネーブルにします。

    [Action]：Mask または Log。

    [Log]：イネーブルまたはディセーブルにします。
  - [Inspect server's and endpoint's software version]：User-Agent と Server ヘッダーに含まれる SIP エンドポイントのソフトウェア バージョンをインスペクションします。

    [Action]：Mask または Log。

    [Log]：イネーブルまたはディセーブルにします。

- [Inspections]：このタブで SIP インスペクションのコンフィギュレーションを表示して、追加や編集ができます。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：SIP インスペクションの基準を示します。
  - [Value]：SIP インスペクションで照合する値を示します。
  - [Action]：照合条件が一致したときのアクションを示します。
  - [Log]：ログの状態を示します。
  - [Add]：[Add SIP Inspect] ダイアログボックスが開き、SIP インスペクションを追加できます。
  - [Edit]：[Edit SIP Inspect] ダイアログボックスが開き、SIP インスペクションを編集できます。
  - [Delete]：SIP インスペクションを削除します。
  - [Move Up]：インスペクションをリストの上に移動します。
  - [Move Down]：インスペクションをリストの下に移動します。

Add/Edit SIP Inspect

[Configuration] > [Global Objects] > [Inspect Maps] > [SIP] > [SIP Inspect Map] > [Advanced View] > [Add/Edit SIP Inspect]

[Add/Edit SIP Inspect] ダイアログボックスでは、SIP インスペクション マップの照合基準と値を定義できます。

フィールド

- [Single Match]：SIP インスペクションに照合文が 1 つだけの場合に指定します。
- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：SIP トラフィックに適用する照合基準を指定します。
  - [Called Party]：To ヘッダーに指定された受信側を照合します。
  - [Calling Party]：From ヘッダーに指定された発信元を照合します。
  - [Content Length]：ヘッダーのコンテンツの長さを照合します。
  - [Content Type]：ヘッダーのコンテンツ タイプを照合します。
  - [IM Subscriber]：SIP IM の加入者を照合します。
  - [Message Path]：SIP の Via ヘッダーを照合します。
  - [Request Method]：SIP の要求方式を照合します。
  - [Third-Party Registration]：サード パーティの登録要求者を照合します。
  - [URI Length]：SIP ヘッダーの URI を照合します。
- [Called Party Criterion Values]：照合する受信側を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Calling Party Criterion Values]：照合する発信元を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラス マップを設定できます。
- [Content Length Criterion Values]：指定値より長い SIP コンテンツ ヘッダーを照合します。
  - [Greater Than Length]：ヘッダーの長さをバイト単位で入力します。
- [Content Type Criterion Values]：照合する SIP コンテンツ ヘッダーのタイプを指定します。
  - [SDP]：SDP タイプの SIP コンテンツ ヘッダーを照合します。
  - [Regular Expression]：正規表現を照合します。

[Regular Expression]：照合する定義された正規表現を一覧表示します。

[Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。

[Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。

[Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。

- [IM Subscriber Criterion Values]：照合する IM 登録者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Message Path Criterion Values]：照合する SIP の Via ヘッダーを指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [Request Method Criterion Values]：照合する SIP 要求方式を指定します。
  - [Request Method]：次の中から要求方式を指定します。ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- [Third-Party Registration Criterion Values]：照合するサード パーティの登録要求者を指定します。正規表現で照合します。
  - [Regular Expression]：照合する定義された正規表現を一覧表示します。
  - [Manage]：[Manage Regular Expressions] ダイアログボックスが開き、正規表現を設定できます。
  - [Regular Expression Class]：照合する定義された正規表現クラスを一覧表示します。
  - [Manage]：[Manage Regular Expression Class] ダイアログボックスが開き、正規表現クラスマップを設定できます。
- [URI Length Criterion Values]：指定値より長い SIP ヘッダーの URI を指定して照合します。
  - [URI type]：SIP URI または TEL URI を指定して照合します。
  - [Greater Than Length]：長さをバイト単位で指定します。
- [Multiple Matches]：SIP インスペクションの複数の照合文を指定します。
  - [SIP Traffic Class]：SIP トラフィック クラスを照合します。
  - [Manage]：[Manage SIP Class Maps] ダイアログボックスが開き、SIP クラス マップの追加、編集、削除ができます。
- [Actions]：プライマリ アクションおよびログを設定します。

- [Action]：Drop packet、Drop Connection、Reset、または Log。（注）要求方式が invite か register の場合は、Limit rate (pps) アクションを使用できます。
- [Log]：イネーブルまたはディセーブルにします。

Skinny（SCCP）インスペクション

この項では、SCCP アプリケーション インスペクションについて説明します。この項は、次の内容で構成されています。

- 「SCCP インスペクションの概要」（P.11-33）
- 「Cisco IP Phone のサポート」（P.11-34）
- 「制限事項」（P.11-34）
- 「Select SCCP (Skinny) Map」（P.11-34）
- 「SCCP (Skinny) Inspect Map」（P.11-35）
- 「Message ID Filtering」（P.11-36）
- 「[Add/Edit SCCP (Skinny) Policy Map]（セキュリティ レベル）」（P.11-37）
- 「[Add/Edit SCCP (Skinny) Policy Map]（詳細）」（P.11-38）
- 「Add/Edit Message ID Filter」（P.11-39）

SCCP インスペクションの概要

（注）　電話プロキシは、Cisco Unified Communications アーキテクチャの一部であり、IP 電話の導入をサポートします。ASA での電話プロキシのセットアップについては、第 16 章「Cisco 電話プロキシの設定」を参照してください。

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注）　ASA は、SCCP プロトコル バージョン 19 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

（注）　電話プロキシは、Cisco Unified Communications アーキテクチャの一部であり、IP 電話の導入をサポートします。ASA での電話プロキシのセットアップについては、第 16 章「Cisco 電話プロキシの設定」を参照してください。

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べてセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、アクセス リストやスタティック エントリは必要ありません。

制限事項

SCCP に対する現在のバージョンの PAT および NAT サポートに適用される制限は、次のとおりです。

- PAT は、**alias** コマンドを含むコンフィギュレーションでは動作しません。
- 外部 NAT および PAT はサポート*されません*。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、ASA は現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注）　ASA は、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

Select SCCP (Skinny) Map

[Add/Edit Service Policy Rule Wizard] > [Rule Actions] > [Protocol Inspection] タブ > [Select SCCP Map]

[Select SCCP (Skinny) Map] ダイアログボックスでは、SCCP (Skinny) マップを選択または新しく作成できます。[SCCP (Skinny)] マップにより、SCCP (Skinny) アプリケーション インスペクションで使用されるコンフィギュレーションの値を変更できます。[Select SCCP (Skinny) Map] テーブルには、アプリケーション インスペクションで選択可能な事前に設定されたマップのリストが表示されます。

フィールド

- [Use the default SCCP (Skinny) inspection map]：デフォルトの SCCP (Skinny) マップの使用を指定します。
- [Select an SCCP (Skinny) map for fine control over inspection]：定義済みのアプリケーション インスペクション マップを選択するか、新しいマップを追加できます。
- [Add]：そのインスペクションの [Add Policy Map] ダイアログボックスを開きます。
- [Encrypted Traffic Inspection]：インスペクション マップの TLS プロキシ設定を指定できます。
  - [Do not inspect Encrypted Traffic]：Skinny アプリケーション インスペクションの検査をディセーブルにします。
  - [Use Phone Proxy to enable inspection of encrypted traffic]：ASA で設定された Phone Proxy を使用して Skinny アプリケーション トラフィックを検査します。第 16 章「Cisco 電話プロキシの設定」を参照してください。
  - [Use TLS Proxy to enable inspection of encrypted traffic]：TLS プロキシを使用して、暗号化されたトラフィックのインスペクションをイネーブルにすることを指定します。

    [TLS Proxy Name]：既存の TLS プロキシの名前。

    [New]：TLS プロキシを追加するための [Add TLS Proxy] ダイアログボックスを開きます。

SCCP (Skinny) Inspect Map

[Configuration] > [Global Objects] > [Inspect Maps] > [SCCP (Skinny)]

[SCCP (Skinny)] ペインでは、SCCP（Skinny）アプリケーションの事前に設定されたインスペクション マップを表示できます。SCCP（Skinny）マップでは、SCCP（Skinny）アプリケーション インスペクションのデフォルト設定値を変更できます。

Skinny アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

フィールド

- [SCCP (Skinny) Inspect Maps]：定義されている SCCP (Skinny) インスペクション マップを一覧表示するテーブルです。
- [Add]：新しい SCCP（Skinny）インスペクション マップを設定します。SCCP（Skinny）インスペクション マップを編集するには、[SCCP (Skinny) Inspect Maps] テーブルで SCCP（Skinny）のエントリを選択し、[Customize] をクリックします。
- [Delete]：[SCCP (Skinny) Inspect Maps] テーブルで選択したインスペクション マップを削除します。
- [Security Level]：セキュリティ レベル（High または Low）を選択します。
  - Low：デフォルト

    登録：適用強制しない

    メッセージの最大 ID：0x181

プレフィックスの長さの最小値：4

メディア タイムアウト：00:05:00

シグナリング タイムアウト：01:00:00

RTP 準拠：適用強制しない

- Medium

  登録：適用強制しない

  メッセージの最大 ID：0x141

  プレフィックスの長さの最小値：4

  メディア タイムアウト：00:01:00

  シグナリング タイムアウト：00:05:00

  RTP 準拠：適用強制する

  ペイロードを音声またはビデオに限定してシグナリング交換を適用：しない

- High

  登録：適用強制する

  メッセージの最大 ID：0x141

  プレフィックスの長さの最小値：4

  プレフィックスの長さの最大値：65536

  メディア タイムアウト：00:01:00

  シグナリング タイムアウト：00:05:00

  RTP 準拠：適用強制する

  ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- [Message ID Filtering]：[Messaging ID Filtering] ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
- [Customize]：[Add/Edit SCCP (Skinny) Policy Map] ダイアログボックスを開き、追加の設定を行います。
- [Default Level]：セキュリティ レベルをデフォルトの Low レベルに戻します。

Message ID Filtering

[Configuration] > [Global Objects] > [Inspect Maps] > [SCCP (Skinny)] > [Message ID Filtering]

[Message ID Filtering] ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
- [Criterion]：インスペクションの基準を示します。
- [Value]：インスペクションで照合する値を示します。
- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。

- [Add] : [Add Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
- [Edit] : [Edit Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- [Delete] : メッセージ ID のフィルタを削除します。
- [Move Up] : エントリをリストの上に移動します。
- [Move Down] : エントリをリストの下に移動します。

[Add/Edit SCCP (Skinny) Policy Map]（セキュリティ レベル）

[Configuration] > [Global Objects] > [Inspect Maps] > [SCCP (Skinny)] > [SCCP (Skinny) Inspect Map] > [Basic View]

[Add/Edit SCCP (Skinny) Policy Map] ペインでは、SCCP（Skinny）アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name] : SCCP（Skinny）マップの追加時に SCCP（Skinny）マップの名前を入力します。SCCP（Skinny）マップの編集時には、事前に設定した SCCP（Skinny）マップの名前が表示されます。
- [Description] : SCCP（Skinny）マップの説明を 200 文字以内で入力します。
- [Security Level] : セキュリティ レベル（High または Low）を選択します。
  - Low : デフォルト

    登録 : 適用強制しない

    メッセージの最大 ID : 0x181

    プレフィックスの長さの最小値 : 4

    メディア タイムアウト : 00:05:00

    シグナリング タイムアウト : 01:00:00

    RTP 準拠 : 適用強制しない
  - Medium

    登録 : 適用強制しない

    メッセージの最大 ID : 0x141

    プレフィックスの長さの最小値 : 4

    メディア タイムアウト : 00:01:00

    シグナリング タイムアウト : 00:05:00

    RTP 準拠 : 適用強制する

    ペイロードを音声またはビデオに限定してシグナリング交換を適用 : しない
  - High

    登録 : 適用強制する

    メッセージの最大 ID : 0x141

    プレフィックスの長さの最小値 : 4

    プレフィックスの長さの最大値 : 65536

メディア タイムアウト：00:01:00

シグナリング タイムアウト：00:05:00

RTP 準拠：適用強制する

ペイロードを音声またはビデオに限定してシグナリング交換を適用：する

- [Message ID Filtering]：[Messaging ID Filtering] ダイアログボックスが開き、メッセージ ID フィルタを設定できます。
- [Default Level]：セキュリティ レベルをデフォルトに戻します。

- [Details]：追加の設定を行うパラメータ、RTP 準拠、メッセージ ID のフィルタリング設定値を表示します。

[Add/Edit SCCP (Skinny) Policy Map]（詳細）

[Configuration] > [Global Objects] > [Inspect Maps] > [SCCP (Skinny)] > [SCCP (Skinny) Inspect Map] > [Advanced View]

[Add/Edit SCCP (Skinny) Policy Map] ペインでは、SCCP（Skinny）アプリケーション インスペクション マップのセキュリティ レベルと追加の設定値を設定できます。

フィールド

- [Name]：SCCP（Skinny）マップの追加時に SCCP（Skinny）マップの名前を入力します。SCCP（Skinny）マップの編集時には、事前に設定した SCCP（Skinny）マップの名前が表示されます。
- [Description]：DNS マップの説明を 200 文字以内で入力します。
- [Security Level]：設定するセキュリティ レベルとメッセージ ID のフィルタリング設定を表示します。
- [Parameters]：このタブで SCCP（Skinny）のパラメータを設定します。
  - [Enforce endpoint registration]：Skinny エンドポイントを登録してから通話を受発信します。

    [Maximum Message ID]：SCCP メッセージ ID に使用できる最大値を指定します。
  - [SCCP Prefix Length]：Skinny メッセージのプレフィックスの長さを指定します。

    [Minimum Prefix Length]：SCCP プレフィックスの長さの許容最小値を指定します。

    [Maximum Prefix Length]：SCCP プレフィックスの長さの許容最大値を指定します。
  - [Media Timeout]：メディア接続時のタイムアウト値を指定します。
  - [Signaling Timeout]：シグナリング接続時のタイムアウト値を指定します。
- [RTP Conformance]：このタブで SCCP（Skinny）の RTP 準拠を設定します。
  - [Check RTP packets for protocol conformance]：ピンホールをフローする RTP/RTCP パケットがプロトコルに準拠しているかどうかをチェックします。

    [Limit payload to audio or video, based on the signaling exchange]：ペイロード タイプを強制的に音声やビデオにして、シグナリング交換を適用します。
- [Message ID Filtering]：このタブで SCCP（Skinny）のメッセージ ID フィルタリングを設定します。
  - [Match Type]：一致タイプを示します。肯定一致と否定一致があります。
  - [Criterion]：インスペクションの基準を示します。
  - [Value]：インスペクションで照合する値を示します。

- [Action]：照合条件が一致したときのアクションを示します。
- [Log]：ログの状態を示します。
- [Add]：[Add Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを追加できます。
- [Edit]：[Edit Message ID Filtering] ダイアログボックスが開き、メッセージ ID のフィルタを編集できます。
- [Delete]：メッセージ ID のフィルタを削除します。
- [Move Up]：エントリをリストの上に移動します。
- [Move Down]：エントリをリストの下に移動します。

Add/Edit Message ID Filter

[Configuration] > [Global Objects] > [Inspect Maps] > [SCCP (Skinny)] > [SCCP (Skinny) Inspect Map] > [Advanced View] > [Add/Edit Message ID Filter]

[Add Message ID Filter] ダイアログボックスでは、メッセージ ID のフィルタを設定できます。

フィールド

- [Match Type]：トラフィックと値を一致させるかどうかを指定します。

  たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。
- [Criterion]：SCCP (Skinny) トラフィックに適用する照合基準を指定します。
  - [Message ID]：指定したメッセージ ID を照合します。

    [Message ID]：SCCP メッセージ ID に使用できる最大値を指定します。
  - [Message ID Range]：指定範囲のメッセージ ID を照合します。

    [Lower Message ID]：SCCP メッセージ ID に使用できる下限値を指定します。

    [Upper Message ID]：SCCP メッセージ ID に使用できる上限値を指定します。
- [Action]：Drop packet。
- [Log]：イネーブルまたはディセーブルにします。