参考資料

イベント ログ レベルについて

すべてのイベントには、1 ～ 4 の範囲で関連付けられたレベルがあり、レベル 1 のイベントが最も重要と見なされます。次の表に、さまざまなイベントに割り当てられるレベルの概要を示します。

レベル	割り当てられるイベント
1	登録要求やコール試行などの高レベルイベント。人間が簡単に読み取れます。次に例を示します。 • コール試行/接続/切断 • 登録試行/承認/拒否
2	すべてのレベル 1 のイベントに加えて、次のイベントがあります。 送受信されたプロトコル メッセージのログ（SIP、H.323、LDAP など）。H.460.18 キープアライブや H.245 ビデオ高速更新などのノイズの多いメッセージは除きます。
3	すべてのレベル 1 およびレベル 2 のイベントに加えて、次のイベントがあります。 • プロトコルのキープアライブ • コール関連の SIP シグナリング メッセージ
4	最も詳細なレベル：レベル 1、レベル 2、およびレベル 3 のすべてのイベントに加えて、次のイベントがあります。 • ネットワーク レベルの SIP メッセージ

Expressway によってログに記録されるすべてのイベントと、それらがログに記録される詳細レベルの完全なリストについては、イベントとレベルの項を参照してください。

イベント ログ形式

イベント ログは、UNIX syslog 形式の拡張として表示されます。

```
date time process_name: message_details
```

値は次のとおりです。

フィールド	説明（Description）
date	メッセージが記録された現地の日付。
time	メッセージが記録された現地の時刻。

フィールド	説明（**Description**）
process_name	ログ メッセージを生成するプログラムの名前。次のようなものが含まれます。 • **tvcs**（Expressway プロセスから発信されるすべてのメッセージの場合） • **web**（すべての Web ログインおよび設定イベントの場合） • **licensemanager**（コール ライセンス マネージャから発信されるメッセージの場合） • **b2bua**（B2BUA イベントの場合） • **portforwarding**（Expressway-C と Expressway-E 間の内部通信の場合） • **ssh**（Expressway-C と Expressway-E 間の ssh トンネルの場合） ただし、Expressway で実行している他のアプリケーションからのメッセージの場合は異なります。
message_details	メッセージの本文（詳細については、メッセージの詳細フィールドの項を参照してください）。

管理者イベント

管理者セッションに関連するイベントは次のとおりです。

- Admin Session Start
- Admin Session Finish
- Admin Session Login Failure

メッセージの詳細フィールドには次が含まれます。

- セッションが関連する管理者の名前および IP アドレス
- ログインが試行、開始、または終了された日時

メッセージの詳細フィールド

tvcs プロセスからログに記録されたすべてのメッセージについては、`message_details` フィールドにメッセージの本文が格納されます。このフィールドは、人間が判読できる、スペースで区切られた複数の `name=value` ペアで構成されています。

`message_details` フィールドの最初の名前要素は常に `Event` であり、最後の名前要素は常に `Level` です。

次の表に、message_details フィールド内の考えられるすべての名前要素を、それぞれの説明とともに通常の表示順で示します。

（注） 次に説明するイベントに加え、非アクティブの状態が1時間経過するごとに、MARK文字列を含む syslog.info イベントがログに記録されます。これは、ロギングがまだアクティブであることを確認するためです。

名前	説明（Description）
イベント	ログ メッセージが生成される原因となったイベント。Expressway によってログに記録されるすべてのイベントと、それらがログに記録されるレベルのリストについては、イベントとレベルを参照してください。
ユーザー	ログイン試行が行われたときに入力したユーザ名。
ipaddr	ログインしたユーザの送信元 IP アドレス。
プロトコル（Protocol）	通信に使用されたプロトコルを示します。有効な値は次のとおりです。 • TCP • UDP • TLS
理由	イベントに関連する理由に関する情報を含んだテキストの文字列。
サービス	通信に使用されたプロトコルを示します。次のいずれかになります。 • H.323 • SIP • H.225 • H.245 • LDAP • Q.931 • NeighbourGatekeeper • クラスタリング • ConferenceFactory
メッセージタイプ	メッセージのタイプを指定します。

名前	説明（**Description**）
Response-code	SIP 応答コードか、または H.323 およびインターワーキング コールの場合は SIP 同等応答コード
Src-ip	送信元 IP アドレス（通信を確立しようとしたデバイスの IP アドレス）。これは、IPv4 アドレスか IPv6 アドレスです。
Dst-ip	宛先 IP アドレス（通信試行の宛先の IP アドレス）。宛先 IP は Src-ip と同じ形式で記録されます。
Src-port	送信元ポート：通信を確立しようとしたデバイスの IP ポート。
Dst-port	宛先ポート：通信試行の宛先の IP ポート。
Src-alias	存在する場合は、メッセージの発信者に関連付けられた最初の H.323 エイリアス。 存在する場合は、メッセージの発信者に関連付けられた最初の H.164 エイリアス。
Dst-alias	存在する場合は、メッセージの受信者に関連付けられた最初の H.323 エイリアス。 存在する場合は、メッセージの受信者に関連付けられた最初の H.164 エイリアス。
詳細	イベントの説明的な詳細。
Auth	コール試行が正常に認証されたかどうか。
メソッド	SIP メソッド（INVITE、BYE、UPDATE、REGISTER、SUBSCRIBE など）。
お問い合わせ	連絡先：REGISTER のヘッダー。
AOR	レコードのアドレス。
Call-id	コール ID ヘッダー フィールドは、特定の招待、または特定のクライアントのすべての登録を一意に識別します。
コールシリアル番号	特定のコールのすべてのプロトコル メッセージに共通のローカル コール シリアル番号。
タグ	タグは、コールのすべてのフォークについて、Expressway ネットワーク上のすべての検索とプロトコル メッセージに共通です。
ルーティング済みコール	Expressway がコールのシグナリングを取得したことを示します。

名前	説明（Description）
移行後	• REGISTER 要求の場合：REGISTER 要求の AOR。 • INVITE の場合：ダイヤルされた元のエイリアス。 • その他のすべての SIP メッセージの場合：宛先の AOR。
Request-URI	この要求の送信先のユーザまたはサービスを示す SIP または SIPS URI。
Num-bytes	メッセージで送受信されたバイト数。
Protocol-buffer	メッセージが復号化できなかったときにバッファに含まれていたデータを表示します。
期間	要求/付与された登録満了期間
時刻	YYYY/MM/DD-HH:MM:SS 形式の完全な UTC タイムスタンプ。この形式を使用することによって、シンプルな ASCII テキストの並べ替え/順序付けを時刻で自然に並べ替えることができます。これは、標準的な syslog タイムスタンプの制限により含まれています。
レベル	イベントログレベルについての項で定義されているイベントログのレベル。
UTC 時間	イベントが発生した時刻。UTC 形式で表示されます。

イベントとレベル

次の表に、イベントログに表示される可能性があるイベントのリストを示します。

イベント	説明（Description）	レベル
Alarm acknowledged	管理者がアラームを確認しました。**Detail** イベントパラメータによって問題の特性に関する情報が提供されます。	1
Alarm lowered	アラームを発生させる原因となった問題が解決されました。**Detail** イベント パラメータによって問題の特性に関する情報が提供されます。	1
Alarm raised	Expressway が問題を検出し、アラームが発生しました。**Detail** イベント パラメータによって問題の特性に関する情報が提供されます。	1

イベント	説明（**Description**）	レベル
Admin Session CBA Authorization Failure	Expressway が証明書ベースの認証を使用するように設定されている場合にログイン試行が失敗しました。	1
Admin Session Finish	管理者がシステムからログオフしました。	1
Admin Session Login Failure	管理者としてのログイン試行が失敗しました。これは、誤ったユーザ名またはパスワード（あるいはその両方）が入力されたために発生した可能性があります。	1
Admin Session Start	管理者がシステムにログオンしました。	1
Application Exit	Expressway アプリケーションが終了しました。さらに詳しい情報が、**Detail** イベントパラメータに示される場合があります。	1
Application Failed	Expressway アプリケーションは予期しない障害によりサービスが停止しました。	1
Application Start	Expressway が起動しました。より詳しい情報が、**Detail** イベント パラメータに示される場合があります。	1
Application Warning	Expressway アプリケーションはまだ実行していますが、回復可能な問題が発生しています。より詳しい情報が、**Detail** イベントパラメータに示される場合があります。	1
Authorization Failure	ユーザが無効なクレデンシャルを持っている、またはアクセスグループに属していない、あるいはアクセスレベルが「「なし」」のグループに属しています。リモート認証が有効になっている場合に適用されます。	1
Beginning System Backup	システム バックアップが起動しました。	1
Beginning System Restore	システムの復元が開始されました。	1
Call Answer Attempted	コールへの応答を試行しました。	1
Call Attempted	コールを試行しました。	1
Call Bandwidth Changed	コールのエンドポイントがコールの帯域幅を再ネゴシエートしました。	1
Call Connected	コールが接続されました。	1

イベント	説明（**Description**）	レベル
Call Diverted	コールを転送しました。	1
Call Disconnected	コールが切断されました。	1
Call Inactivity Timer	コールは、非アクティビティにより切断されました。	1
Call Rejected	コールが拒否されました。**Reason** イベントパラメータには、H.225 追加原因コードのテキスト表現が含まれています。	1
Call Rerouted	Expressway で **[コールシグナリングの最適化（Call signaling optimization）]** が *[オン（On）]* に設定されており、コール シグナリング パスから Expressway が除外されています。	1
CBA Authorization Failure	証明書ベースの認証を使用したログイン試行が認証の失敗により拒否されました。	1
Certificate Management	セキュリティ証明書がアップロードされたことを示します。詳細については、**Detail** イベント パラメータを参照してください。	1
Completed System Backup	システムのバックアップが完了しました。	1
Completed System restore	システムの復元が完了しました。	1
Configlog Cleared	オペレータがコンフィギュレーション ログをクリアしました。	1
Decode Error	SIP メッセージまたは H.323 メッセージの復号化中に構文エラーが発生しました。	1
Diagnostic Logging	診断のロギングが進行中であることを示します。**Detail** イベント パラメータに追加の詳細情報が示されます。	1
Error Response Sent	TURN サーバがクライアントに（STUN プロトコルを使用して）エラー メッセージを送信しました。	3
Eventlog Cleared	オペレータがイベント ログをクリアしました。	

イベント	説明（**Description**）	レベル
External Server Communication Failure	外部サーバとの通信が予期切失敗しました。**Detail** イベントパラメータで「「応答なし」」と「「応答拒否」」を区別する必要があります。関係するサーバは次のとおりです。 • DNS • LDAP サーバ • ネイバー ベートキーパー • NTP サーバ • ピア	
Hardware Failure	Expressway ハードウェアに問題があります。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	
License Limit Reached	特定の機能のライセンスの制限に到達しました。**Detail** イベント パラメータに関連する機能や制限が示されます。 これが頻繁に発生する場合は、シスコの担当者に連絡し、ライセンスを追加購入してください。	
Message Received	着信 RAS メッセージを受信しました。	2
Message Received	着信 RAS NSM キープアライブ、ピア間の H.225、H.254、または RAS メッセージを受信しました。	3
Message Received	（SIP）着信メッセージを受信しました。	4

イベント	説明（**Description**）	レベル
Message Rejected	次の 2 つの理由のどちらかで発生した可能性があります。 • 認証が有効になっており、エンドポイントがメッセージ（登録要求など）の Expressway への送信試行に失敗した場合。これは、エンドポイントが認証クレデンシャルを提供していないか、またはクレデンシャルが Expressway が予期していたものと一致しないかのいずれかの場合に発生します。 • クラスタリングが有効になっていてもクラスタ上の帯域幅が同一に設定されておらず、さらに、Expressway が不明なピア、リンク、パイプ、サブゾーン、またはゾーンに関連するメッセージを受信した場合。	
Message Sent	送信 RAS メッセージを送信しました。	2
Message Sent	送信 RAS NSM キープアライブ、H.255、H.245、またはピア間の RAS メッセージが送信されました。	3
Message Sent	（SIP）送信メッセージを送信しました。	4
Operator Call Disconnect	管理者がコールを切断しました。	1
Outbound TLS Negotiation Error	Expressway は TLS で別のシステムと通信できません。イベント パラメータで詳細情報が提供されます。	1
Package Install	言語パックなどのパッケージがインストールされたか、または削除されました。	2
Policy Change	ポリシー ファイルが更新されました。	1
POST request failed	HTTP POST 要求が未許可セッションから送信されました。	1
Provisioning	プロビジョニング サーバからの診断メッセージ。**Detail** イベント パラメータに追加情報が示されます。	1

イベント	説明（**Description**）	レベル
Reboot Requested	システム リブートが要求されました。**Reason** イベント パラメータに具体的な情報が示されます。	1
Registration Accepted	登録要求が承認されました。	1
Registration Refresh Accepted	登録の更新またはキープアライブの要求が承認されました。	3
Registration Refresh Rejected	登録更新の要求が拒否されました。	1
Registration Refresh Requested	登録の更新またはキープアライブの要求を受信しました。	3
Registration Rejected	登録要求が拒否されました。**Reason** イベント パラメータと **Detail** イベント パラメータに、拒否の特性に関する情報が示されます。	1
Registration Removed	Expressway によって登録が削除されました。**Reason** イベント パラメータに登録が削除された理由が示されます。理由は次のいずれかです。 • 認証の変更（Authentication change） • ゾーンの競合（Conflicting zones） • オペレータによる強制削除（Operator forced removal） • オペレータによる強制削除（すべての登録を削除）（Operator forced removal (all registrations removed)） • 登録を優先（Registration superseded.）	1
Registration Requested	登録が要求されました。	1
Relay Allocated	TURN サーバ リレーが割り当てられました。	2
Relay Deleted	TURN サーバ リレーが削除されました。	2
Relay Expired	TURN サーバ リレーの期限が切れました。	2
Request Failed	Conference Factory への要求が失敗しました。	1

イベント	説明（**Description**）	レベル
Request Received	コール関連の SIP 要求を受信しました。	2
Request Received	非コール関連 SIP 要求を受信しました。	3
Request Sent	コール関連の SIP 要求を送信しました。	2
Request Sent	非コール関連の SIP 要求を送信しました。	3
Request Successful	成功した要求が Conference Factory に送信されました。	1
Response Received	コール関連の SIP 応答を受信しました。	2
Response Received	非コール関連 SIP 応答を受信しました。	3
Response Sent	コール関連 SIP 応答を送信しました。	2
Response Sent	非コール関連のSIP応答を送信しました。	3
Restart Requested	システムの再起動が要求されました。**Reason** イベント パラメータに具体的な情報が示されます。	1
Search Attempted	検索を試行しました。	1
Search Cancelled	検索がキャンセルされました。	1
Search Completed	検索が完了しました。	1
Search Loop detected	Expressway は **[コールループ検出（Call loop detection）]** モードになっており、ループ化された検索のブランチを特定し、終了させました。	2
Secure mode disabled	Expressway は正常に **[高度なアカウントセキュリティ（Advanced account security）]** モードを終了しました。	1
Secure mode enabled	Expressway は正常に **[高度なアカウント セキュリティ（Advanced account security）]** モードを開始しました。	1
Security Alert	Expressway でセキュリティ関連の潜在的な攻撃が検出されました。	1
Success Response Sent	TURN サーバがクライアントに（STUN プロトコルを使用して）成功メッセージを送信しました。	3

イベント	説明（**Description**）	レベル
System backup completed	システムのバックアップ プロセスが完了しました。	1
System Backup error	システムのバックアップ試行中にエラーが発生しました。	1
System backup started	システムのバックアップ プロセスが開始しました。	1
System Configuration Changed	システムの設定項目が変更されました。**Detail** イベント パラメータに、変更された設定項目の名前と新しい値が格納されます。	1
System restore completed	システムの復元プロセスが完了しました。	1
System restore backing up current config	システムの復元プロセスが現在の設定のバックアップを開始しました。	1
System restore backup of current config completed	システムの復元プロセスが現在の設定のバックアップを完了しました。	1
System restore error	システムの復元を試行中にエラーが発生しました。	1
System restore started	システムの復元プロセスが開始しました。	1
System Shutdown	オペレーティング システムがシャットダウンされました。	1
System snapshot started	システム スナップショットが開始されました。	1
System snapshot completed	システム スナップショットが完了しました。	1
System Start	オペレーティング システムが起動しました。起動に問題がある場合は、**Detail** イベント パラメータに追加情報が格納されることがあります。	1
TLS Negotiation Error	Transport Layer Security（TLS）接続がネゴシエートに失敗しました。	1
Unregistration Accepted	登録解除要求が承認されました。	1
Unregistration Rejected	登録解除要求が拒否されました。	1
Unregistration Requested	登録解除要求を受信しました。	1

イベント	説明（**Description**）	レベル
Upgrade	ソフトウェアアップグレードプロセスに関連するメッセージ。**Detail**イベントパラメータに具体的な情報が示されます。	1

CPL リファレンス

コール処理言語（CPL）はコール処理を定義するための XML ベースの言語です。ここでは、Expressway の CPL の実装に関する詳細を示します。CPL 標準規格の RFC 3880.と併せてお読みください。

Expressway には数多くの強力な組み込みトランスフォーメーション機能が備わっています。そのため、高度なコール処理ルールが必要な場合にのみ、CPL が必要になります。

Expressway はほとんどの CPL 標準規格と、一部の TANDBERG 定義の拡張機能をサポートします。トップ レベルのアクションである `<incoming>` と `<outgoing>`（*RFC 3880* で説明）はサポートされません。代わりに、`<taa:routed>`セクション内の CPL の単一のセクションをサポートします。

CPL スクリプトを Expressway にアップロードすることによってコール ポリシーを実装する場合、そのスクリプトは XML スキーマと照合してシンタックスが確認されます。スキーマには、基本の CPL 仕様用のスキーマと TANDBERG 拡張機能用のスキーマの 2 つがあります。どちらのスキーマも Web インターフェイスからダウンロードして、Expressway へのアップロードの前にスクリプトを検証するために使用できます。

次に、シンタックスを許可されるようにする名前空間の正しい使用方法を示します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="reception@example.com">
    <proxy/>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

送信元アドレスと宛先アドレスの形式

この項の説明でコールの送信元エイリアスまたは宛先エイリアスに言及する場合は、サポートされているすべてのアドレス形式（URI、IP アドレス、E.164 エイリアスなど）を意味します。

CPL アドレス スイッチ ノード

address-switch ノードによって、コールの送信元エイリアスまたは宛先エイリアスに基づき、スクリプトは異なるアクションを実行できます。照合するフィールドを指定してから、アドレス ノードのリストに考えられる一致と関連付けられたアクションを含めます。

address-switch には、field と subfield という 2 つのノード パラメータがあります。

アドレス

address 構造体を address-switch 内に使用して、照合するアドレスを指定します。正規表現の使用をサポートします。

有効な値は次のとおりです。

is=string	選択したフィールドとサブフィールドが指定した文字列と正確に一致しています。
contains=string	選択したフィールドとサブフィールドに指定した文字列が含まれています。CPL 標準規格のみで表示サブフィールドでのこの照合が可能です。ただし、Expressway ではどのタイプのフィールドでもこの照合が可能です。
サブドメイン = 文字列	選択したフィールドが数字（電話のサブフィールドなど）の場合、これはプレフィックスとして一致します。たとえば、address subdomain-of=「555」 は 5556734 などと一致します。フィールドが数字でない場合は、通常のドメイン名の照合が適用されます。たとえば、address subdomain-of=「company.com」 は nodeA.company.com などと一致します。
regex=「regular expression」	選択したフィールドとサブフィールドは指定した正規表現を照合します。

すべてのアドレスの比較では大文字と小文字の違いが無視されます。たとえば、address is=「Fred」 は fred、freD などと一致します。

フィールド

address-switch ノード内では、必須の field パラメータで考慮対象のアドレスを指定します。次に、サポートされる属性とその解釈を示します。

フィールド パラメータの属性	SIP	H.323
`unauthenticated-origin`	着信メッセージの 「From」 フィールドと 「ReplyTo」 フィールド。	コールを開始した元の LRQ または ARQ の送信元エイリアス。SETUP を RAS の先行メッセージなしに受信した場合は、発信元は SETUP から取得されます。
`authenticated-origin` および `origin`	正しく認証されている場合（または関連する **[認証ポリシー（Authentication Policy）]** が *[認証済みとして処理（Treat as authenticated）]* の場合）は、メッセージの 「From」 フィールドと 「ReplyTo」 フィールド。それ以外の場合は `not-present` です。	正しく認証されている場合（または関連する **[認証ポリシー（Authentication Policy）]** が *[認証済みとして処理（Treat as authenticated）]* の場合）は、コールを開始した元の LRQ または ARQ の送信元エイリアス。それ以外の場合は `not-present`。SETUP メッセージは認証されないため、Expressway が SETUP メッセージを先行する RAS メッセージなしに受信した場合、発信元は常に `not-present` になります。
`originating-zone`	コールの発信元のレッグのゾーンまたはサブゾーンの名前。コールがネイバー ゾーン、トラバーサル サーバ ゾーン、またはトラバーサル クライアント ゾーンから発信された場合、これはゾーン名と等しくなります。コールがローカル サブゾーンのいずれか内のエンドポイントから発信された場合、これはサブゾーンの名前になります。コールがその他のローカルに登録されたエンドポイントから発信された場合、これは 「DefaultSubZone」 になります。それ以外の場合は、「DefaultZone」 になります。	
`originating-user`	**関連する [認証ポリシー（Authentication Policy）]** が *[クレデンシャルの確認（Check credentials）]* または *[認証済みとして処理（Treat as authenticated）]* の場合、これは認証に使用されたユーザ名になります。それ以外の場合は `not-present` になります。	
`registered-origin`	コールが登録済みのエンドポイントから発信された場合、これは登録したエイリアスのリストになります。それ以外の場合は `not-present` になります。	
`destination`	宛先エイリアス。	

フィールド パラメータの属性	SIP	H.323
original-destination	宛先エイリアス。	

適用する認証ポリシー設定は、着信メッセージの送信元に応じて、関連ゾーン用に設定されています。

選択したフィールドに複数のエイリアスが含まれている場合、Expresswayは次のアドレス ノードに進む前に各アドレスノードをすべてのエイリアスで照合しようとします。つまり、いずれかのエイリアスに一致する場合はアドレス ノードは一致します。

サブフィールド

address-switch ノードでは、オプションのサブフィールド パラメータで考慮するアドレスに部分を指定します。次の表に、サブフィールドの定義をエイリアス タイプごとに示します。

照合するエイリアス タイプにサブフィールドが指定されていない場合は、`not-present` アクションが実行されます。

address-type	コールを発信したエンドポイントのタイプに基づいて、`h323` または `sip` のいずれかになります。
user	URI エイリアスの場合は、これによってユーザ名の部分が選択されます。H.323 ID の場合は ID 全体、E.164 番号の場合は番号全体になります。
ホスト	URI エイリアスの場合は、これによってドメイン名の部分が選択されます。エイリアスが IP アドレスの場合は、このサブフィールドはドット付き 10 進法形式の完全なアドレスになります。
tel	E.164 番号の場合は、これによって数字の文字列全体が選択されます。

alias-type	エイリアスのタイプの文字列表現を指定します。タイプは、エイリアスの形式から推定されます。可能なタイプは次のとおりです。 • アドレス タイプ • 結果 • URI • url-ID • H.323 ID • h323-ID • ダイヤル番号 • dialedDigits

otherwise

otherwise ノードは、address-switch で指定されているアドレスが見つかったものの、先行するアドレス ノードが 1 つも一致しなかった場合に実行されます。

Not-Present

not-present ノードは、address-switch で指定されているアドレスがコール セットアップ メッセージに含まれていなかった場合に実行されます。この形式は、認証を使用するときに最も有効です。認証が有効になっている Expressway は、ポリシーを実行するときに認証されたエイリアスのみを使用します。そのため、認証されていないユーザからコールを受信したときに not-present アクションを使用し、適切なアクションを実行します（「認証されたユーザの発信者名の確認」の例を参照してください）。

参照先

CPL スクリプトは評価されるため、proxy ノードが実行される場合はコールの宛先として使用されるアドレス（H.323 ID、URL、および E.164 番号）のリストを保持します。taa:location ノードを使用して場所の設定を変更することで、コールを異なる宛先にリダイレクトできます。

スクリプト実行の開始時に、場所の設定は元の宛先に初期化されます。

次の属性は taa:location ノードでサポートされます。正規表現の使用をサポートします。

Clear = 「yes」 | 「no」	新しいロケーションを追加する前に現在の場所の設定をクリアするかどうかを指定します。デフォルトでは、この場所が設定の末尾に追加されます。

`url=string`	場所の設定に追加される新しい場所。所定の文字列でURL（`user@domain.com`など）、H.323 IDまたはE.164番号を指定できます。
`priority=<0.0..1.0>` | 「random」	0.0 ～ 1.0の範囲の浮動小数点数か、または、同じ範囲内の乱数を割り当てる`random`のいずれかとして指定されます。1.0が最も高いプライオリティです。同じプライオリティの場所の検索は並行して実行されます。
`regex=「<regular expression>」 replace=「<string>」`	正規表現に一致する場所を変更する方法を指定します。
`source-url-for-message=「<string>」`	指定された文字列でFromヘッダー（送信元エイリアス）を置換します。
`source-url-for-message-regex=「<regular expression>」` together with `source-url-for-message-replace=「<string>」`	指定した置換文字列で、正規表現に一致するFromヘッダー（送信元エイリアス）を置換します。複数のFromヘッダーがある場合（H.323のみに適用）、一致しないFromヘッダーは変更されずにそのまま残ります。

Fromヘッダーの送信元URLが変更されると、対応する表示名も変更された送信元URLのユーザ名の部分に一致するように変更されます。

Rule-Switch

CPLのこの拡張機能は、コールの送信元と宛先の両方に基づいて決定を下す必要があるコールポリシーのスクリプトを簡単にするために提供されています。`taa:rule-switch`には、順番にテストされる多くのルールを含めることができます。一致が検出されるとすぐにそのルール要素内のCPLが実行されます。

各ルールは次のいずれかの形式である必要があります。

```
<taa:rule-switch>
 <taa:rule origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule authenticated-origin="<regular expression>" destination="<regular expression>"
 message-regex="<regular expression>">
 <taa:rule unauthenticated-origin="<regular expression>" destination="<regular expression>"
 message-regex="<regular expression>">
 <taa:rule registered-origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-user="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-zone="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
</taa:rule-switch>
```

さまざまなoriginセレクタの意味は、CPL アドレス スイッチ ノードの項で説明されているとおりです。

message-regex パラメータでは、着信 SIP メッセージ全体に対して正規表現を照合させることができます。

（注） message-regex パラメータを含むルールは H.323 コールを照合しません。

プロキシ

proxy ノードでの実行時に、Expressway はコールを現在のロケーション設定で指定された場所に転送しようとします。ロケーション設定に複数のエントリがある場合は、分岐されたコールになります。現在のロケーション設定が空の場合は、元の宛先にコールが転送されます。

proxy ノードでは、次のオプション パラメータがサポートされます。

timeout=<1..86400>	秒単位で指定されたタイムアウト時間
stop-on-busy = 「yes」	「no」	ビジー応答を受信した場合に検索を停止するかどうか

プロキシ アクションによって、次の表に示す結果となる可能性があります。

failure	プロキシがコールのルーティングに失敗しました
busy	宛先を検出したが、ビジー状態になっています
noanswer	宛先を検出したが応答がありません
redirection	Expressway がコールのリダイレクトを求められています
default	他の結果が適用されない場合に実行する CPL

CPL はこれらの結果に基づいて、さらにアクションを実行することができます。どの結果ノードも proxy ノード内に含まれる必要があります。例：

```
<proxy timeout="10">
 <busy>
  <!--If busy route to recording service-->
  <location clear="yes" url="recorder">
   <proxy/>
  </location>
 </busy>
</proxy>
```

拒否

`reject` ノードが実行された場合、Expressway はそれ以降のスクリプト処理を中止し、現在のコールを拒否します。

ここでは、カスタムの拒否文字列である `status=string` オプションと `reason=string` オプションがサポートされており、ストリングの一貫性を確保するためにこれらを一緒に使用する必要があります。

サポートされていない CPL 要素

Expressway は現在、CPL RFC で説明されている一部の要素をサポートしていません。次の要素のいずれかを含むスクリプトをアップロードしようとすると、エラー メッセージが生成され、Expressway は既存のポリシーを使用し続けます。

現在、次の要素はサポートされません。

- time-switch
- string-switch
- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

CPL の例

ここでは、CPL 選択の例を示します。

- 認証されたユーザの発信者名確認
- ドメインに基づいた発信者名確認
- ローカルに登録されたエンドポイントからのコールのみの許可
- デフォルト ゾーンとデフォルト サブゾーンからのコールのブロック
- ローカル ゲートウェイへのアクセスの制限

CPL の例：認証されたユーザの発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。「コールポリシーについて」を参照してください。

この例では、認証された送信元アドレスを持つユーザからのコールのみが許可されます。認証を有効化する方法の詳細については、「デバイス認証について」を参照してください。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="authenticated-origin">
   <not-present>
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：エイリアスに基づいた発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。「コールポリシーについて」を参照してください。

この例では、ユーザ ceo が、ユーザ `vpsales`、`vpmarketing`、または `vpengineering` からのコールのみを受け入れます。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="ceo">
```

```
    <address-switch field="authenticated-origin">
     <address regex="vpsales|vpmarketing|vpengineering">
      <!-- Allow the call -->
      <proxy/>
     </address>
     <not-present>
      <!-- Unauthenticated user -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </otherwise>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ドメインに基づいた発信者名確認

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。「コールポリシーについて」を参照してください。

この例では、ユーザの fred が annoying.com のすべてのユーザ、または認証されていないユーザからのコールを受け入れません。その他のすべてのユーザはコールが許可されます。

コールが Expressway-E を通じて着信する場合は、望ましくないコールがネットワーク内に進行しないように Expressway-E での発信者名確認を推奨します。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="fred">
    <address-switch field="authenticated-origin" subfield="host">
     <address subdomain-of="annoying.com">
      <!-- Don't accept calls from this source -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <not-present>
      <!-- Don't accept calls from unauthenticated sources -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- All other calls allowed -->
      <proxy/>
     </otherwise>
```

```
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ローカルに登録されたエンドポイントからのコールのみの許可

（注） この例では、管理者がローカルに登録されたエンドポイントから発信されたコールのみを許可しようと考えています。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <reject status="403" reason="Only local endpoints can use this Expressway"/>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：デフォルト ゾーンとデフォルト サブゾーンからのコールのブロック

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。「コールポリシーについて」を参照してください。

ローカルに登録されたエンドポイントからのコールのみを許可するスクリプトは、デフォルト ゾーンまたはデフォルト サブゾーンからでなく、設定されたゾーンからのコールを許可するように拡張できます。

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <address-switch field="originating-zone">
     <address is="DefaultZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <address is="DefaultSubZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
```

```
     </address>
     <otherwise>
      <proxy/>
     </otherwise>
    </address-switch>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL の例：ローカル ゲートウェイへのアクセスの制限

（注） この動作はコール ポリシー ルールを使用して設定できるため、CPL スクリプトを使用して行う必要はありません。ただし、UI によって設定されたルールとアップロードされた CPL スクリプトを組み合わせて使用することはできないため、UI ルールを使用して実装できない CPL 要件がある場合は、すべてのルールにスクリプトを使用する必要があります。「コールポリシーについて」を参照してください。

次の例では、ゲートウェイが 9 のプレフィックスで Expressway に登録されており、管理者は組織外からのコールをゲートウェイを通じてルーティングしないようにしたいと考えています。

これを行うには、`address-switch` ノードを使用する方法と `taa:rule-switch` ノードを使用する方法の 2 つがあります。次に、それぞれの例を示します。

（注） Cisco Unified Communications Manager でコールルーティングを使用すると、同じ結果を取得できます。この例が示されているのは、これらのタイプのコールがネットワークのさらに深い部分に到達するのを防ぎたいと思う場合があるためです。

address-switch ノードの使用：

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address regex="9(.*)">
    <address-switch field="originating-zone">
     <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
     <address is="TraversalZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

taa:rule-switch ノードの使用

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <taa:rule-switch>
   <taa:rule originating-zone="TraversalZone" destination="9(.*)">
    <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </taa:rule>
   <taa:rule origin="(.*)" destination="(.*)">
    <!-- All other calls allowed -->
    <proxy/>
   </taa:rule>
  </taa:rule-switch>
 </taa:routed>
</cpl>
```

デバイス認証用の LDAP サーバの設定

LDAP サーバ上の H.350 ディレクトリ サービスに対してデバイスを認証するように Expressway を設定できます。

ここでは、次の方法について説明します。

- LDAP サーバにインストールする必要がある H.350 スキーマのダウンロード
- Expressway で使用するための 2 つの一般的なタイプの LDAP サーバのインストールと設定
  - Microsoft Active Directory用の LDAP サーバの設定
  - OpenLDAP サーバの設定

H.350 スキーマのダウンロード

次の ITU 仕様で、LDAP サーバにインストールする必要があるスキーマについて説明します。

H.350	マルチメディア会議用のディレクトリ サービス アーキテクチャ：ネットワーク上のエンドポイントを表現する LDAP スキーマ
H.350.1	H.323 用のディレクトリ サービス アーキテクチャ：H.323 のエンドポイントを表現する LDAP スキーマ
H.350.2	H.235 用のディレクトリ サービス アーキテクチャ：H.235 の要素を表現する LDAP スキーマ

H.350.4	SIP 用のディレクトリ サービス アーキテクチャ：SIP のエンドポイントを表現する LDAP スキーマ

スキーマは Expressway の Web インターフェイスからダウンロードできます。次の手順を実行します。

1. **[設定（Configuration）]** > **[認証（Authentication）]** > **[デバイス（Devices）]** > **[H.350 ディレクトリ スキーマ（H.350 directory schemas）]** に移動します。ダウンロード可能なスキーマのリストが表示されます。
2. 各ファイルの横にある **[ダウンロード（Download）]** ボタンをクリックし、ファイルを開きます。
3. ブラウザの **[名前を付けて保存（Save As）]** コマンドを使用してファイルをファイル システムに保存します。

Microsoft Active Directory用の LDAP サーバの設定

前提条件

次の手順は、Active Directory がすでにインストールされていると想定しています。Active Directory のインストールの詳細については、Windows のドキュメントを参照してください。

次の手順は、Windows Server 2003 Enterprise Edition 用です。このバージョンの Windows を使用していない場合は、手順が異なります。

H.350 スキーマのインストール

H.350 スキーマのダウンロード、次のようにインストールします。

コマンド プロンプトを右クリックし、[管理者として実行（Run as administrator）] を選択して管理者特権でのコマンドプロンプトを開きます。ファイルごとに次のコマンドを実行します。

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

値は次のとおりです。

`<ldap_base>` は Active Directory サーバのベース DN です。

H.350 オブジェクトの追加

組織階層を作成します。

1. Active Directory の **[ユーザとコンピュータ（Users and Computers）]** MMC スナップインを開きます。
2. ベース DN で、[新しい組織ユニット（New Organizational Unit）] を右クリックします。
3. *h350* という組織ユニットを作成します。

独自の組織ユニット内に H.350 ディレクトリを保持して H.350 オブジェクトを他のタイプのオブジェクトと区別することをお勧めします。これによって、BaseDN への Expressway 読み取りアクセスのみを許可するアクセス制御を設定してディレクトリの他のセクションへのアクセスを制限できます。

H.350 オブジェクトを追加するには、次の手順を実行します。

1. 次の内容の ldif ファイルを作成します。

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@X
```

2. 次のコマンドを使用して ldif ファイルをサーバに追加します。

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

値は次のとおりです。

`<ldap_base>` は Active Directory サーバのベース DN です。

上記の例では、`MeetingRoom1` の H.323 ID エイリアス、`626262` の E.164 エイリアス、および `MeetingRoom@X` の SIP URI を持つ単一のエンドポイントを追加します。また、エントリには認証時に使用された、ID が `meetingroom1`、パスワードが `mypassword` の H.235 および SIP クレデンシャルも存在します。

H.323 の登録では、H.323 と H.235 の属性を検索し、SIP は SIP の属性を検索します。したがって、エンドポイントを 1 つのプロトコルだけで登録する場合は、もう一方のプロトコルに関連するエレメントを組み込む必要はありません。

（注） `ldif` ファイル内の SIP URI には、プレフィックスとして `sip:` が付けられている必要があります。

エイリアスが LDAP データベース内にない場合の動作の詳細については、「LDAP を使用したデバイスの認証」の項の登録用エイリアスのソースを参照してください。

TLS での保護

TLS を使用するように Active Directory を有効にするには、証明書を要求し、Active Directory サーバにインストールする必要があります。証明書は次の要件を満たす必要があります。

- ローカル コンピュータの個人証明書ストアにあること。これは、[証明書（Certificates）] MMC スナップインを使用して確認できます。
- 証明書に関連付けられている秘密キーの取得方法に関する機密情報がローカルに保存されていること。証明書を表示すると、「「この証明書に対応する秘密キーを所有しています（You have a private key that corresponds to this certificate）」」というメッセージが表示されます。
- 強力な秘密キー保護が有効になっていない秘密キーを所有していること。これはキー要求に追加できる属性です。
- Enhanced Key Usage の拡張にサーバ認証オブジェクトの識別子が含まれており、これもキー要求の一部になっていること。
- ドメイン コントローラとクライアントの両方が信頼する CA から発行されていること。
- ドメイン コントローラの Active Directory 完全修飾ドメイン名が件名フィールドの共通名、またはサブジェクト代替名拡張子の DNS エントリに含まれていること。

LDAP サーバへの接続上で TLS を使用するように Expressway を設定するには、CA の証明書を信頼できる CA 証明書としてアップロードする必要があります。これを行うには、Expressway で **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できる CA 証明書（Trusted CA certificate）]**に移動します。

OpenLDAP サーバの設定

前提条件

次の手順では、OpenLDAP サーバがすでにインストールされていることを前提としています。OpenLDAP のインストールの詳細については、http://www.openldap.org にあるマニュアルを参照してください。

次に、Linux プラットフォームで OpenLDAP の標準インストールを使用する例を示します。他のプラットフォームのインストールについては、OpenLDAP のコンフィギュレーション ファイルの場所が異なる場合があります。詳細については、OpenLDAP のインストール マニュアルを参照してください。

H.350 スキーマのインストール

1. Expressway からすべてのスキーマ ファイルをダウンロードします（**[設定（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [LDAP スキーマ（LDAP schemas）]**）。ファイル名のすべての文字が小文字であり、各ファイル名には .schema 拡張子が付けられていることを確認します。したがって

   commobject.schema

   h323identity.schema

   h235identity.schema

   sipidentity.schema

2. 各スキーマ ファイルのインデックスは slapcat を使用して特定します。たとえば、**commobject.schema** の場合は次のようになります。

   ```
   スド スラップキャット -f schema_convert.conf -F ldif_output -n 0 |grep コミュニケートオブジェクト、cn=スキーマ
   ```

   この場合は、次のような情報が返されます。`dn:cn={14}commobject、cn=schema、cn=config`

   波カッコ {} 内のインデックス値は異なります。

3. `slapcat` を使用して、各スキーマ ファイルを ldif 形式に変換します。前のコマンドによって返されたインデックス値を使用します。たとえば、**commobject.schema** の場合は次のようになります。

   ```
   slapcat -f schema_convert.conf -F ldif_output -n0 -H
   ldap:///cn={14}commobject,cn=schema,cn=config -l cn=commobject.ldif
   ```

4. テキスト エディタを使用して、新たに作成したファイル（commobject ファイルの場合は **cn=commobject.ldif**）を編集し、次の行を削除します。

   ```
   structuralObjectClass:
   entryUUID:
   creatorsName:
   createTimestamp:
   entryCSN:
   modifiersName:
   modifyTimestamp:
   ```

5. `ldapadd` を使用して、各スキーマを ldap データベースに追加します。たとえば、**cn=commobject.ldif** の場合は次のようになります。

   ```
   sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=commobject.ldif
   ```

   （`cn` の後ろのバックスラッシュはエスケープ文字です）。

6. 各スキーマ ファイルに上記のステップを繰り返します。

詳細については、https://help.ubuntu.com/13.04/serverguide/openldap-server.html を参照してください。

H.350 オブジェクトの追加

組織階層を作成します。

1. 次の内容の `ldif` ファイルを作成します。

   ```
   # This example creates a single organizational unit to contain the H.350 objects
   dn: ou=h350,dc=my-domain,dc=com
   objectClass: organizationalUnit
   ou: h350
   ```

2. 次の形式の `slapadd` を使用して、この ldif ファイルをサーバに追加します。

   ```
   slapadd -l <ldif_file>
   ```

   この組織ユニットは、Expressway が検索を実行する BaseDN を形成します。この例では、BaseDN は `ou=h350,dc=my-domain,dc=com` となります。

独自の組織ユニット内に H.350 ディレクトリを保持して H.350 オブジェクトを他のタイプのオブジェクトと区別することをお勧めします。これによって、BaseDN への Expressway 読み取りアクセスのみを許可するアクセス制御を設定してディレクトリの他のセクションへのアクセスを制限できます。

（注） `ldif` ファイル内の SIP URI には、プレフィックスとして `sip:` が付けられている必要があります。

H.350 オブジェクトを追加するには、次の手順を実行します。

1. 次の内容の ldif ファイルを作成します。

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=mydomain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@domain.com
```

2. 次の形式の `slapadd` を使用して、この ldif ファイルをサーバに追加します。

```
slapadd -l <ldif_file>
```

上記の例では、`MeetingRoom1` の H.323 ID エイリアス、`626262` の E.164 エイリアス、および `MeetingRoom@domain.com` の SIP URI を持つ単一のエンドポイントを追加します。また、エントリには認証時に使用された、ID が `meetingroom1`、パスワードが `mypassword` の H.235 および SIP クレデンシャルも存在します。

H.323 の登録では、H.323 と H.235 の属性を検索し、SIP は SIP の属性を検索します。したがって、エンドポイントを 1 つのプロトコルだけで登録する場合は、もう一方のプロトコルに関連するエレメントを組み込む必要はありません。

エイリアスが LDAP データベース内にない場合の動作の詳細については、「LDAP を使用したデバイスの認証」の項の登録用エイリアスのソースを参照してください。

TLS での保護

LDAP サーバへの接続は、Transport Level Security（TLS）を接続上で有効にすることによって暗号化できます。これを行うには、Expressway がサーバの ID を検証できるように LDAP サーバの X.509 証明書を作成する必要があります。証明書を作成した後は、証明書に関連付けられた次の 3 つのファイルを LDAP サーバにインストールする必要があります。

- LDAP サーバの証明書
- LDAP サーバの秘密キー

- LDAP サーバの証明書の署名に使用された認証局（CA）の証明書

3 つのファイルはすべて PEM ファイル形式である必要があります。

LDAP サーバは、証明書を使用するように設定する必要があります。次の手順を実行します。

- /etc/openldap/slapd.conf を編集し、次の 3 つの行を追加します。

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

TLS 設定を有効にするには、OpenLDAP デーモン（`slapd`）を再起動する必要があります。

LDAP サーバへの接続上で TLS を使用するように Expressway を設定するには、CA の証明書を信頼できる CA 証明書としてアップロードする必要があります。これを行うには、Expressway で **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[信頼できる CA 証明書（Trusted CA certificate）]**に移動します。

コラボレーションソリューションアナライザツールの使用

コラボレーション ソリューション アナライザは、Cisco Technical Assistance Center（TAC）が導入の検証（およびログファイル解析）を支援するために作成したものです。たとえば、ビジネス ツー ビジネス コール テスターを使用して、コールの検証とテストを行うことができます。これには、Microsoft インターワーキングコールが含まれます。

コラボレーション ソリューション アナライザを使用するには、カスタマー アカウントまたはパートナー アカウントが必要です。

スタート ガイド

1. ログ分析ツールを使用する予定の場合は、最初に、お使いの Expressway のログを収集します。
2. https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/にログインします

   X12.6 からは、**[診断ロギング（Diagnostic logging）]** ページの **[ログの分析（Analyze log）]** ボタン（**[メンテナンス（Maintenance）]** > **[診断（Diagnostics）]**）を使用し、コラボレーションソリューションアナライザのトラブルシューティングツールへのリンクを開けます。
3. 使用するツールをクリックします。たとえば、ログを使用するには、次のようにします。
   1. [ログ分析（Log analysis）] をクリックします。
   2. ログファイルをアップロードします。
   3. 分析するファイルを選択します。
   4. **[分析の実行（Run Analysis）]** をクリックします。

ツールはログファイルを分析し、生のログよりも理解しやすい形式で情報を表示します。たとえば、ラダー図を生成して SIP コールを表示することができます。

デフォルトの SSH キーの変更

デフォルトキーを使用すると、Expressway に対して確立された SSH セッションが「「中間者」」攻撃に対して脆弱になる可能性があります。そのため、Expressway に一意の新しい SSH キーを生成することを推奨します。

Expressway が工場出荷時のデフォルトの SSH キーで設定されているままである場合は、「「セキュリティアラート：SSH サービスはデフォルトキーを使用しています（Security alert: the SSH service is using the default key）」」というアラームメッセージが表示されます。

Expressway に新しい SSH キーを生成するには、次の手順を実行します。

1. CLI に *root* としてログインします。
2. `regeneratesshkey` と入力します。
3. `exit` と入力して root アカウントからログアウトします。
4. Web インターフェイスにログインします。
5. **[メンテナンス（Maintenance）]**>**[再起動（Restart）]** に移動します。「**再起動（Restart）**」ページが表示されます。
6. 現在実行されているコールと登録の数を確認します。
7. **[システムの再起動（Restart system）]** をクリックし、求められたら再起動を確認します。

クラスタ化された Expressway システムがある場合は、クラスタ ピアそれぞれに新しい SSH キーを生成する必要があります。各ピアに順番にログインし、上記の手順に従います。クラスタ化を解除したり、複製を無効にしたりする必要はありません。

SSH を使用して Expressway へ次回ログインする際に、Expressway のキー ID が変更されたという警告を受け取る場合があります。この警告を抑制するには、SSH クライアントに適したプロセスに従ってください。

その後で Expressway が以前のバージョンの Expressway ファームウェアにダウングレードされた場合は、デフォルトの SSH キーが復元されます。

デフォルト設定の復元（初期設定へのリセット）

まれに、システムで「「factory-reset」」スクリプトを実行する必要が生じる場合があります。これは、ソフトウェアイメージを再インストールし、設定をデフォルトの最小機能にリセットするものです。

はじめる前に

システムの最初のセットアップ以降に、アップグレードした場合、リセットにより、最新のソフトウェア バージョンが再インストールされます。

工場出荷時のリセット手順は、重大な障害が発生した後のシステム リカバリを目的としています。**物理ストレージから情報を消去するためのセキュリティ メカニズムとしては設計されていません。**リセットを使用して、システムを「「クリーン」」または「「空白」」の安全な状態に戻すことはしないようにしてください。リセットは、システムを最小の設定状態に戻すことだけを目的としています。

システムは、リセットによってインストールされたソフトウェア バージョンに現在適用されるデフォルト設定値を使用します。これは特にシステムが古いバージョンからアップグレードされている場合など、以前に設定された値と異なる可能性があります。特に、これは多重化されたメディア ポートなどのポート設定に影響する場合があります。デフォルトの設定を復元した後は、必要に応じて、これらのポート設定を、ファイアウォールが想定しているものと一致するポート設定にリセットしてください（次に、必要に応じてオプション キー、SSHキーとFIPS140モードのようないくつかの設定値を保持することは可能ですが、これらの値をすべてリセットすることをお勧めします）。

前提条件

- このプロセスを完了するには仮想マシン コンソールが必要になるため、**VM コンソールを開くための適切な VMware アクセスが必要**です。
- 以下で説明する手順は、正常にインストールされた最新のソフトウェア イメージに基づいてシステムを再構築します。再インストールには、**/mnt/harddisk/factory-reset/** システム フォルダに格納されている次の 2 つのファイルが使用されます。これらのファイルがシステムに存在しない場合があります（最も一般的にはアップグレードされていない新規 VM のインストールの場合）。その場合、ルートとして SCP を使用して、ファイルを配置する必要があります。
  - 16 文字のリリース キーが含まれた、*rk* という名前のテキスト ファイル
  - .tar および .gz 形式のソフトウェア イメージが含まれた、*tandberg-image.tar.gz* という名前のファイル。ダウンロードしたバージョン固有の tar ファイルの名前を *tandgz-image.tar.gz* に手動で変更する必要があります。

デフォルト設定へのリセット プロセス

この手順はコンソールから実行する必要があります（または、ハードウェアベースの CE アプライアンスの場合は、オプションでキーボードとモニターを使用してアプライアンスへの直接接続を使用できます）。ネットワーク設定が書き換えられるため、すべてのコールとリセットを開始するために使用した SSH セッションが切断され、手順によって生成される出力を確認できなくなります。

このプロセスには約 20 分かかります。

1. **root** としてシステムにログインします。
2. `factory-reset` と入力します。
3. 必要に応じて質問に回答します。以下の推奨される応答を入力すると、システムが完全にリセットされ、工場出荷時のデフォルト状態に戻ります。

プロンプト	推奨される応答
オプション キーを保持しますか [はい/いいえ] ?（Keep option keys [YES/NO]?）	NO
FIPS140 設定を保持しますか [はい/いいえ] ?（Keep FIPS140 configuration [YES/NO]?）	NO
IP 構成を保持しますか [はい/いいえ] ?（Keep IP configuration [YES/NO]?）	NO
ssh キーを保持しますか [はい/いいえ] ?（Keep ssh keys [YES/NO]?）	NO
サーバー証明書、関連するキー、および CA 信頼ストアを保持しますか [はい/いいえ]（Keep server certificate, associated key and CA trust store [YES/NO]?） このオプションでは SNI/ドメイン証明書は保持されません。どのように応答するかにかかわらず、これらの証明書は常に削除されます。（[はい（Yes）] と応答した場合）サーバー証明書とそれに関連付けられているキーと CA 信頼ストアのみが保存されます。	NO
root パスワードおよび管理者パスワードを保持しますか [はい/いいえ] ?（Keep root and admin passwords [YES/NO]?）	NO
ログ ファイルを保存しますか [はい/いいえ] ?（Save log files [YES/NO]?）	NO

4. 操作を続行することを確定します。
5. VM 起動後に、インストール ウィザードが表示されます。VM コンソールを使用してウィザードを完了する必要があります。ステップ 3 での応答に応じてウィザードの質問の一部はスキップされますが、IP 設定とパスワードを維持しているとしても、VM コンソールを使用してインストール ウィザードを完了する必要があります。

（注） 使用していた FIPS140 を再び有効にする場合は、FIPS140-2 暗号化モードの設定に関するこのガイドの項を参照してください。

USB スティクによるリセット - CE ハードウェアアプライアンス

このセクションは、VM ベースの仮想化 Expressway には適用されません。

Cisco TAC は、代替リセット方法を提案して、ソフトウェアイメージを USB スタックにダウンロードしてから、USB 接続された状態でシステムを再起動します。

この方式を使用した場合は、USB スティックの使用後の消去と再構築が必要です。あるシステムをリセットしてから USB スティックを抜き取り、それを別のシステムに再使用しないでください。

（注） リセット機能は、内部リカバリパーティション（IRP）を通じて CE ハードウェアアプライアンスに組み込まれています。詳細については、インストールおよびアップグレードガイドページの『*CEnnnn* アプライアンス のインストールおよびアップグレードガイド』を参照してください。

パターン マッチングの変数

Expressway では、許可リストと拒否リスト、事前検索変換、検索ルールやゾーン変換を構成する際に、多数の機能でパターンマッチングが利用されます。

これらのパターン マッチのそれぞれで、Expressway ではパターンをチェックする前に現在の設定値で置換する変数を使用できます。

これらの変数は、次のいずれかまたは両方として使用できます。

- 検索するパターンのすべてまたは一部
- 検出されたパターンを置換する文字列のすべてまたは一部

変数は、すべてのタイプのパターン（プレフィックス、サフィックス、正規表現、および完全一致）で使用できます。

次の表に、変数として有効な文字列と、それらが表現する値を示します。

文字列	返される値の表現	パターンフィールドでの使用時	置換フィールドでの使用時
%ip%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V4 Address xConfiguration Ethernet 2 IP V6 Address	すべての IPv4 アドレスと IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv4%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 2 IP V4 Address	LAN 1 および LAN 2 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv4_1%	xConfiguration Ethernet 1 IP V4 Address	LAN 1 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 1 IPv4 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。
%ipv4_2%	xConfiguration Ethernet 2 IP V4 Address	LAN 2 に現在設定されている IPv4 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 2 IPv4 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。

文字列	返される値の表現	パターンフィールドでの使用時	置換フィールドでの使用時
%ipv6%	xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V6 Address	LAN 1 および LAN 2 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	該当なし
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	LAN 1 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 1 IPv6 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。
%ipv6_2%	xConfiguration Ethernet 2 IP V6 Address	LAN 2 に現在設定されている IPv6 アドレスに一致しています。 Expressway がクラスタの一部である場合にすべてのピアアドレスに適用されます。	LAN 2 IPv6 アドレスで文字列を置き換えます。 Expressway がクラスタの一部である場合は、ローカルピアのアドレスが常に使用されます。
%systemname%	xConfiguration SystemUnit Name	Expressway のシステム名に一致しています。	Expressway のシステム名で文字列を置き換えます。

パターンが特定の名前に一致するかどうか、および予想どおりに変換されているかどうかは、[パターンの確認（Check pattern）]ツール（**[メンテナンス（Maintenance）]>[ツール（Tools）]>[パターンの確認（Check pattern）]**）を使用してテストできます。

ポート リファレンス

Cisco Expressway シリーズ設定ガイドのページに用意されている、ご使用のバージョンに対応する『*Cisco Expressway IP Port Usage Configuration Guide*』を参照してください。

正規表現

正規表現は、エイリアストランスフォーメーション、ゾーントランスフォーメーション、CPL ポリシー、ENUM など、数多くの Expressway 機能と組み合わせて使用できます。Expressway は POSIX 形式の正規表現構文を使用します。次の表に、正規表現構文で一般的に使用される特殊文字を示します。これは、使用可能なすべての表現のサブセットでしかありません。正規表現構文の詳細については、『*Regular Expression Pocket Reference*』という資料を参照してください。

文字	説明（**Description**）	例
.	任意の単一文字と一致します。	
\d	任意の 10 進数（0 ～ 9）と一致します。	
*	直前の文字または式の 0 回以上の繰り返しと一致します。	.* は、文字のシーケンスと一致します。
+	直前の文字または式の 1 回以上の繰り返しと一致します。	
?	直前の文字または式の 0 回または 1 回以上の繰り返しと一致します。	`9?123` は、9123 および 123 と一致します。
{n}	直前の文字または式の n 回の繰り返しと一致します。	`\d{3}` は 3 桁の数字と一致します。
{n,m}	直前の文字または式の n ～ m 回の繰り返しと一致します。	`\d{3,5}` は、3 桁、4 桁、5 桁の数字と一致します。
[...]	一連の指定した文字と一致します。セット内の各文字を個別に指定するか、または、範囲内の最初の文字、その後に - 文字、その後に範囲内の最後の文字を入力して、範囲を指定することができます。 [] 内では特殊文字を使用できません。特殊文字はそのままの文字として扱われます。	`[a-z]` は英字と一致します。 `[0-9#*]` は単一の E.164 文字と一致します。E.164 文字のセットは、0 ～ 9 の数字とハッシュキー（#）およびアスタリスクキー（*）から構成されます。

文字	説明（Description）	例
[^...]	指定した文字のセットを除くすべてと一致します。セット内の各文字を個別に指定するか、または、範囲内の最初の文字、その後に - 文字、その後に範囲内の最後の文字を入力して、範囲を指定することができます。 [] 内では特殊文字を使用できません。特殊文字はそのままの文字として扱われます。	`[^a-z]` は英字以外の文字と一致します。 `[^0-9#*]` は 0 ～ 9 の数字、ハッシュ キー（#）、およびアスタリスク キー（*）以外と一致します。
(...)	一連の一致文字をまとめてグループ化します。グループは、置換文字列の一部として、文字列 \1、\2 などを使用して順番に参照できます。	ユーザのフルネームが含まれている URI をイニシャルに基づいた URI に変換するように正規表現を組み立てることができます。正規表現 `(.).*_(.).*(@example.com)` はユーザの `john_smith@example.com` と照合し、置換文字列 `\1\2\3` を使用して `js@example.com` に変換します。
|	1つの表現または代替表現に一致します。	`.*@example.(net|com)` はドメイン `example.com` またはドメイン `example.net` の URI と一致します。
\	正規表現の特殊文字をエスケープします。	
^	行の先頭を示します。 開き大カッコの直後に使用されると、大カッコ内の文字セットは否定されます。	`[^abc]` は、a、b、c、のいずれでもない任意の単一文字と一致します。
$	行の末尾を意味します。	`^\d\d\d$` は正確に 3 桁の文字列と一致します。

文字	説明（Description）	例
(?!...)	否定先読み。存在すべきでない副次式を定義します。	`(?!.*@example.com$).*` は `@example.com` で終了しない文字列と一致します。 `(?!alice).*` は `alice` で開始されない文字列と一致します。
(?<!...)	否定後読み。存在すべきでない副次式を定義します。	`.*(?<!net)` は `net` で終了しない文字列と一致します。

正規表現の比較は大文字と小文字を区別しません。

正規表現の使用例については、CPL の例の項を参照してください。

サポートされる文字

Expressway は CLI や Web インターフェイスにテキストが入力されると、次の文字をサポートします。

- A ～ Z および a ～ z の文字
- 10 進数（0 ～ 9）
- アンダースコア (_)
- マイナス記号/ハイフン（-）
- 等号（=）
- プラス記号 (+)
- アットマーク（@）
- カンマ（,）
- ピリオド/終止符（. ）
- 感嘆符（! ）
- スペース

次の文字は特に許可されていません。

- タブ
- 山カッコ（< と >）
- アンパサンド（&）
- キャレット (^)

特定のテキスト フィールド（[管理者（Administrator）] グループを含む）には異なる制限事項があります。これらについては、本ガイドの関連する項に示します。

大文字と小文字の区別

CLIやWebインターフェイスを使用して入力するテキスト項目は大文字と小文字が区別されません。例外として、パスワードとローカル管理者名は大文字と小文字が区別されます。

製品 ID と対応するキー

Cisco PID（製品識別子）は、製品名、モデル名、または製品番号とも呼ばれる場合があります。次に、ソフトウェアバージョンに応じて Expressway に適用できる PID の例を示します。多くは、後のソフトウェアバージョンで段階的に廃止されています。たとえば、リリースキーは Cisco Expressway 製品の X12.5.4 から使用されなくなりました。

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
リリース キー	LIC-SW-VMVCS-K9	16 桁の数	VCS 制御 VCS Expressway	システムを有効にする。キーはソフトウェアのシリアル番号と特定の基本バージョンに固有です。ほとんどの機能は、このキーなしでは無期限には機能しません。
リリース キー	LIC-SW-EXP-K9	16 桁の数	Expressway-C Expressway-E	システムを有効にする。キーはソフトウェアのシリアル番号と特定の基本バージョンに固有です。ほとんどの機能は、このキーなしでは無期限には機能しません。
Expressway シリーズ	LIC-EXP-SERIES	116341E00-m-########	Expressway-C Expressway-E	Expressway シリーズのシステムを有効にします（Cisco Webex ハイブリッドサービスを除く）

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
リッチ メディア セッション ライセンス	LIC-EXP-RMS	116341Yn-m-########	Expressway-C Expressway-E	

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
				Expressway がメディア ストリームを処理する（メディアを「トラバース」または「ハンドル」するとも言われる）必要がある場合に Expressway により有効にされたコール。 RMS ライセンスは次の機能が必要なコールで使用されます。 • IPv4-IPv6 インターワーキング • H.323-SIP インターワーキング • 別のエンティティに代わるメディアの暗号化 • Microsoft SIP から標準ベースの SIP へのインターワーキング **注**：両方のエンドポイントがシスコインフラストラクチャに登録されている場合は、RMS ライセンスは不要です。 RMS ライセンスは CMR クラウド

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
				のコールでは使用されません
トラバーサル コール ライセンス	シラミ-VCSE-n	116341Wnm########	VCS 制御 VCS Expressway	VCS がメディア ストリームを処理する（メディアを「トラバース」または「ハンドル」するとも言われる）必要がある場合に VCS により有効にされたコール。 トラバーサル コール ライセンスは次の機能が必要なコールで使用されます。 • IPv4-IPv6 インターワーキング • H.323-SIP インターワーキング • 別のエンティティに代わるメディアの暗号化 • Microsoft SIP から標準ベースの SIP へのインターワーキング トラバーサル コール ライセンスは CMR クラウドのコールでは使用されません

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
非トラバーサル コール ライセンス	シラミ-VCS-n	116341Vn-m-########	VCS 制御 VCS Expressway	メディア トラバーサルを必要としない（シグナリングのみ）VCS により有効にされたコール
登録ライセンス	ライセンス・アンド・ス・アンド・グ	116341Rn-m-########	VCS 制御 VCS Expressway	VCS への発信者の登録
ルーム システムの登録ライセンス	LIC-EXP-ルーム	116341An-m-########	Expressway-C Expressway-E	Expressway-C への TelePresence ルーム登録
デスクトップ システム ライセンス登録	リック・エップ・ド・スク	116341Bn-m-########	Expressway-C Expressway-E	Expressway-C へのデスクトップ エンドポイント登録
TURN リレー ライセンスが必要です（TURN relay licenses）	LIC-EXP-TURN	116341In-m-########	VCS Expressway Expressway-E	Jabber Guest、Microsoft 相互運用性（オフサイト MS クライアント）
トラバーサル サーバ機能 （X12.6 以降では使用されません）	LIC-EXP-E	116341T00-m-########	VCS Expressway Expressway-E	ファイアウォール トラバーサル：MRA、B2B、CMR クラウド、CMR Hybrid、プロキシ登録、Jabber Guest、MS 相互運用性（オフサイト MS クライアント）
FindMe 機能	LIC-VCS-FINDME	116341U00-m-########	VCS 制御 Expressway-C	Cisco TMS で管理する複数のエイリアス。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。

機能、ライセンスオプション	製品ID（PID）	キー パターン	適用対象	目的
SIP 機能のインターワーキング H.323	LIC-EXP-GW	116341G00-m-########	VCS 制御 VCS Expressway Expressway-C Expressway-E	このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
デバイスのプロビジョニング機能	リック・VCS-デヴプロヴ	116341P00-m-########	VCS 制御 Expressway-C	Cisco TMS の設定および電話帳を使用したエンドポイントのプロビジョニング。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
高度なネットワーク機能	LIC-EXP-AN	116341L00-m-########	VCS Expressway Expressway-E	2 つ目の NIC とスタティック NAT の有効化。 このキーは明示的に必須ではありませんが、ロードされても動作に影響しません。
高度なアカウントのセキュリティ機能	LIC-VCS-JITC	116341J00-m-########	VCS 制御 VCS Expressway	FIPS140-2 暗号化モードの有効化（高度にセキュアな環境） 高度なアカウントセキュリティモードの有効化
高度なアカウントのセキュリティ機能	LIC-EXP-JITC =	116341J00-m-########	Expressway-C Expressway-E	FIPS140-2 暗号化モードの有効化（高度にセキュアな環境） 高度なアカウントセキュリティモードの有効化

機能、ライセンス オプション	製品ID（PID）	キー パターン	適用対象	目的
Microsoft 相互運用性	LIC-EXP-MSFT	116341C00-m-########	VCS 制御 Expressway-C	次を含む Expressway と Microsoft インフラストラクチャ間のすべての統合：A/V コールのインターワーキング、Microsoft クライアントからのデスクトップ共有、チャットおよびプレゼンス フェデレーションと IM&P。

n - このキーで提供されるライセンス数。この位置に 00 が含まれる場合、キーは複数のライセンス用ではなく 1 つの機能用であることを意味します。

m - キー、通常1.のインデックス。

~ #十六進数。

許可リストによるファイル参照の決定

CSVファイルを使用してルールを定義できます。この項では、各ルールの引数に許容されるデータへの参照を提供し、CSV 形式のルールを示します。

表 *1:* リストルールの引数を許可する

引数インデックス	パラメータ名	必須/任意	サンプル値
0	Url	必須	protocol://host[:port][/path] それぞれの説明は次のとおりです。 • protocol は http または https です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。：の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます（例：:8443 ポートが指定されて、Expresswayはプロビジョニングされたプロトコルのデフォルトポートを使用します（80または443） • /path はオプションです。HTTP 仕様に準拠する必要があります。
1	導入	任意	このルールを使用する導入の名前。複数の導入がある場合は必須です。それ以外の場合は空白の引数を入力します。

引数インデックス	パラメータ名	必須/任意	サンプル値
2	HttpMethods	任意	HTTP メソッドのカンマ区切りリスト。必要に応じて二重引用符で囲います。 例：`"GET,PUT"`
3	MatchType	任意	`exact` または `prefix`。 デフォルト：`prefix`
4	説明（Description）	任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。

CSV ファイルの例

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,,"First Rule"
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- ファイルの最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのルール、ルールごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、ルール値は正しい順序にします
- スペースを含む値は二重引用符で囲みます

許可リスト テスト ファイル リファレンス

CSV ファイルを使用してテストを定義できます。この項では、各テストの引数に許容されるデータへの参照を提供し、CSV 形式のテストを示します。

表 *2:* リストテスト引数の許可

引数インデックス	パラメータ名	必須/任意	サンプル値
0	Url	必須	`protocol://host[:port][/path]` それぞれの説明は次のとおりです。 • protocol は `http` または `https` です。 • host には DNS 名または IP アドレスを指定できます。 • :port はオプションです。：の後に 0 ～ 65535 の範囲の 1 つの数値のみが続きます。 • /path はオプションです。HTTP 仕様に準拠する必要があります。
1	ExpectedResult	必須	`allow` または `block`。テストで、指定した URL をルールによって許可またはブロックする必要があると前提するかどうかを指定します。
2	Deployment	任意	この URL を使用してテストする導入の名前。この引数を省略すると、テストはデフォルトの導入を使用します。
3	Description	任意	ルールの説明。スペースを含む場合は二重引用符で囲みます。

引数インデックス	パラメータ名	必須/任意	サンプル値
4	HttpMethod	任意	テストする HTTP メソッドを 1 つ指定します。例：`PUT` 指定しない場合、デフォルトで `GET` に設定されます。

CSV ファイルの例

```
Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST
```

- 最初の行にパラメータ名（記載のとおり）をリストします
- 1 行ごとに 1 つのテスト、テストごとに 1 行
- カンマで引数を区切ります
- 上記の表に示すように、テスト値は正しい順序にします
- スペースを含む値は二重引用符で囲みます

Expressway マルチテナンシーの概要

Expressway の製品ラインは、Cisco Hosted Collaboration Solution で次のようなさまざまなエッジアクセス機能を提供するために使用されます。

- Mobile & Remote Access（MRA）を使用すると、Cisco Jabber などのエンドポイントは、エンタープライズ ネットワーク外のエンドポイントに対して Cisco Unified Communications Manager によって提供される登録、コール制御、プロビジョニング、メッセージング、プレゼンス サービスを設定することができます。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。
- ビジネス ツー ビジネス（B2B）によって、インターネット経由で到達可能な Cisco Hosted Collaboration Solution を利用しない企業との間でダイヤルできるセキュアな接続オプションが可能になります。
- Cisco Webex ハイブリッド サービスは、オンプレミスの機器と Cisco Collaboration Cloud を関連付けて統合された Cisco Webex エクスペリエンスを実現します。

これらのサービスを導入するには、Cisco Expressway-E クラスタと Expressway-C クラスタを顧客ごとに設定および管理する必要があります。小規模のお客様の場合は、これが非効率的なリソースの使用や管理上の負担の増大の原因になる可能性があります。

このオーバーヘッドを軽減するために、マルチテナント構成を導入することができます。これにより、パートナーは最大 50 の顧客間で Expressway-E クラスタを共有しながら、専用の Expressway-C クラスタを顧客ごとに展開できます。

この専用 Expressway-C クラスタは、MRA、B2B、およびハイブリッドの 3 つのサービスすべてに使用できます。この設定は、顧客あたり最大約 500 のユーザがいる小規模な顧客をサポートすることを目的としています。

大規模なお客様の場合は、シングルテナント（専用の）Expressway-E クラスタを使用して、顧客の規模とパフォーマンスの要件を満たすことを推奨します。

マルチテナント Expressway の制限

マルチテナント Expressway には、標準の Expressway 製品に関連していくつかの制限があります。次の機能は、マルチテナント モードでサポートされません。

- Jabber Guest
- 以下を含むさまざまなモードにおける H323
  - H323/SIP インターワーキング
  - ビジネス ツー ビジネス H323
  - H323 ゲートキーパー
- Lync の相互運用
- Skype for Business の相互運用
- IPv6
- Cisco Meeting Server（CMS）

詳細情報

マルチテナント機能の詳細については、「Cisco Hosted Collaboration Solution ドキュメント」ページに用意されている次のドキュメントを参照してください。

- Cisco Hosted Collaboration Solution Reference Network Design Guide
- Cisco Hosted Collaboration Customer Onboarding Guide
- Cisco Hosted Collaboration Solution Capacity Planning Guide
- Cisco Hosted Collaboration Solution Troubleshooting Guide

マルチテナント Expressway のサイジング

以前の Expressway リリースでは、Expressway-E および Expressway-C クラスタ展開は、一致するクラスタと OVA のサイズに制限されていました。Expressway-E クラスタ内のノード数は、Expressway-C クラスタ内のノード数と一致する必要があります。各ノードは、両方のクラスタで同じ OVA サイズでなければなりません。

マルチテナント展開オプションを使用すると、その制限が緩和されます。推奨される展開は、共有の 6 ノード大規模 OVA Expressway-E クラスタと、顧客ごとに専用の 2 ノード中規模 OVA Expressway-C クラスタです。

2 ノード中規模 OVA クラスタが提供する容量を超える容量が必要な顧客の場合は、要件を満たす専用の Expressway-E クラスタを導入することをお勧めします。

全体的なサイジングの推奨事項については、『*Cisco Hosted Collaboration Solution* 参照 ネットワーク 設計ガイド』の「コラボレーション ソリューション サイジング ガイダンス」の章を参照してください。特に、この章の「Expressway」の項では、Expressway クラスタのサイジングと容量について説明しています。

マルチテナント展開では、Expressway-E の容量はすべての顧客で共有されますが、Expressway-C クラスタの容量はその顧客専用です。次の表に、顧客ごとの推奨容量を示します。ビデオおよびオーディオのみのコールの数値は、いずれかのコールタイプのものであることに注意してください。両方ではありません。

共有 Expressway-E クラスタのサイジング

クラスタ サイズ	プロキシ実施済みMRA登録	ビデオ コール	音声専用コール
6 ノード、大規模 OVA N+2 の配置であるため、容量は 4 ノード用であり、2 ノードで障害が発生しても容量の損失はありません。	10,000	2,000	4,000
顧客ごとの最大（50 の顧客に対し）	200	40	80

専用の Expressway-C クラスタのサイジング

クラスタ サイズ	プロキシ実施済みMRA登録	ビデオ コール	音声専用コール
2 ノード、中規模OVA N+1 の配置であるため、容量は単一ノードであり、1 ノードで障害が発生しても容量の損失はありません。	2,500	100	200

上記の表では、ビデオ通話と音声のみの通話は、MRA コール、B2B コール、およびハイブリッド コールの合計を占めています。共有の Expressway-E クラスタごとに推奨される最大顧客数 50 において、顧客あたりの平均同時 MRA 登録の最大数は 200 であり、Expressway-C クラスタの容量をはるかに下回ります。

同様に、顧客あたりの平均同時ビデオ通話の最大数は 40 であり、これもまた Expressway-C クラスタの容量を下回ります。Expressway-C クラスタのこの空き容量は、プロキシされた登録またはコール キャパシティに影響を与えることなく、共存するハイブリッド コネクタによって使用されます。

Expressway-E を共有している顧客の規模を計画する際に考慮すべき 2 つの使用例があります。これらの両方の使用例では、Expressway-E クラスタが制限要因です。Expressway-C には多くの容量があります。

使用例 1

ほとんどの顧客は、社内接続に MPLS を使用しており、自宅やモバイルでは MRA のみを使用しています。この場合、常にごく一部のユーザ（10-20%）しか MRA に登録されていません。1 顧客あたりの最大ユーザ数は約 500 です。

使用例 2

ほとんどの顧客は MPLS を使用しておらず、すべての接続に MRA を使用しています。この場合、100% のユーザが MRA に登録されています。1 顧客あたりの最大ユーザ数は 200 を超えてはいけません。

次の表に、これらの展開オプションを要約します。

表 *3*：導入シナリオ

使用例	顧客あたりの平均最大ユーザ数	一度に MRA 経由で登録できるユーザのパーセンテージ	注意事項
1	500	40%	ほとんどの顧客が社内接続に MPLS を使用している場合に、これを使用します。

使用例	顧客あたりの平均最大ユーザ数	一度に MRA 経由で登録できるユーザのパーセンテージ	注意事項
2	200	100 %	ほとんどの顧客が社内接続に MRA を使用している場合に、これを使用します。

Cisco Hosted Collaboration Solution ページの『マルチテナントおよび *Cisco Expressway*』を参照してください。

アラーム参照

以下の表に、Expressway で発生する可能性のあるアラームのリストを示します。

- 表 4 : ハードウェア アラーム
- 表 5 : ソフトウェアアラーム
- 表 6 : クラスタアラーム
- 表 7 : ネットワークアラーム
- 表 8 : ライセンスアラーム
- 表 9 : 外部アプリケーション/サービスアラーム
- 表 10 : セキュリティアラーム
- 表 11 : 設定ミスアラーム
- 表 12 : バックツーバックユーザエージェントアラーム
- 表 13 : 管理コネクタアラーム
- 表 14 : カレンダーコネクタ アラーム
- 表 15 : コールコネクタアラーム
- 表 16 : 重要なイベントアラーム
- 表 17 : テレメトリーアラーム

表 *4*: ハードウェア アラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
10001	ハードウェア障害（Hardware failure）	ハードウェアで次の問題が発生したときに生成されます。 • しきい値を下回るファン速度。 • しきい値を上回るシステム温度。 • しきい値を下回るシステム入力電圧。 • しきい値を上回るシステム入力電圧。	Cisco RMA プロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール およびサービス ガイド』を参照してください。	クリティカル
10002	RAID の劣化（RAID degraded）	<problem description>	Cisco RMA プロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール およびサービス ガイド』を参照してください。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
10003	PSUの冗長性の損失（PSU redundancy lost）	<problem description>	Cisco RMAプロセスに従って交換部品を入手します。サーバ コンポーネントを交換する方法については、「Cisco UCS C220 M4 ラック サーバ」ページの『*Cisco UCS C220 M4* サーバーのインストール および サービス ガイド』を参照してください。	クリティカル
10004	RAIDの再構築（RAID rebuilding）	<problem description>	再構築が完了するまで待ちます。正常に完了すると、すべてのRAID関連のアラームが自動的に引き下げられます。	クリティカル
10005	不適切なハードウェアの警告（Unsuitable hardware warning）	現在のハードウェアが、このバージョンのExpressway でサポートされているVMの設定要件を満たしていません。	サポートされるハードウェアバージョンへのアップグレードについては、シスコの担当者にお問い合わせください。サポートされるバージョンについては、「Expressway インストール ガイド」ページの「*Cisco Expressway on Virtual Machine Installation Guide*」を参照 してください。	警告

表 *5:* ソフトウェアアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15004	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました	インシデント レポート ページを表示します。	エラー
15005	データベースの障害（Database Failure）	データベースを削除し、バックアップから復元した後でシステムをリブートしてください	システムを再起動します	警告
15006	再起動が必要です（Restart required）	言語パックがインストールされましたが、これを有効にするにはリスタートが必要です	システムを再起動します。	警告
15007	システムがビジー（The system is busy）	システムがシャットダウンするか、起動します		アラート
15008	データ ベースをロードできませんでした（Failed to restore database）	データ ベースをロードできませんでした。一部の設定データが失われました	システム データをバックアップから復旧します。	警告
15009	初期設定へのリセットが開始されました（Factory reset started）	初期設定へのリセットが開始されました		アラート
15010	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました	インシデント レポート ページを表示します。	エラー
15011	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが <module> で検出されました	インシデント レポート ページを表示します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15012	言語パッケージの不一致（Language pack mismatch）	一部のテキストラベルが変換できない可能性があります	シスコの担当者に連絡し、最新の言語パックが使用可能かどうかを確認します	警告
15013	初期設定へのリセットに失敗しました（Factory reset failed）	初期設定へのリセットに失敗しました		アラート
15014	再起動が必要です（Restart required）	コアダンプモードが変更されましたが、この変更を有効にするにはリスタートが必要です	システムを再起動します。	警告
15015	メンテナンスモード（Maintenance mode）	Expressway がメンテナンスモードになっており、コールや登録を受け入れなくなりました		警告
15016	ディレクトリサービスのデータベース障害（Directory service database failure）	ディレクトリサービスのデータベースが実行していません	システムを再起動します。	警告
15017	アプリケーションに障害が発生しました（Application failed）	OpenDS サービスが突然停止し、再起動しました	問題が解決しない場合は、シスコの担当者に連絡してください	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15018	ブートの選択の不一致（Boot selection mismatch）	ブートしたシステムが予期していた設定と一致しません。これは、ブート中のシリアルコンソールでのユーザ入力か、誤った文字によって発生した可能性があります（Booted system does not match expected configuration; this may be caused by user input or spurious characters on the serial console during the boot）	システムを再起動します	クリティカル
15019	アプリケーションに障害が発生しました（Application failed）	予期しないソフトウェア エラーが検出されました（An unexpected software error was detected） <details>	システムを再起動します。問題が解決しない場合はシスコのサポート担当者に連絡してください。	クリティカル
15021	Cisco XCP ルータの遅延再起動（Delayed Cisco XCP Router restart）	Cisco XCP ルータの遅延再起動機能が有効になっているため、Cisco XCP ルータ サービスは現在最新の設定では動作していません。	[Cisco XCP ルータの遅延再起動ページ（Delayed Cisco XCP Router restart）] でルータを再起動するか、またはスケジュールされた時間に再起動するように設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15022	再起動が必要です（Restart required）	ドメイン証明書設定が変更されました。これを有効にするには再起動が必要です。	システムを再起動します。	警告
15023	復元に失敗（Restore failed）	バックアップが復元されませんでした。システムは、以前の設定に復元されます。	エラー ログで詳細を確認して操作を再試行します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー
15024	暗号化デバイスの障害（Crypto device failure）	設定された暗号デバイスで暗号化/解読化サイクルをテスト中にエラーが検出されました。	HSM 設定 ページで詳細をご確認ください	クリティカル
15025	HSM 登録解除の障害（HSM disenrollment failure）	HSM へのピアの登録解除に失敗しました。	HSM 設定 ページで詳細をご確認ください	エラー
15026	HSM 登録の障害（HSM enrollment failure）	HSM へのピアの登録に失敗しました。	HSM 設定 ページで詳細をご確認ください	エラー
15027	HSMの障害（HSM failure）	HSM の障害には管理者の注意が必要です。	HSM 設定 ページで詳細をご確認ください	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15028	再起動が必要です（Restart required）	サーバ証明書と秘密キーが変更されましたが、この変更を適用するには再起動が必要です（Server certificate and private key have been changed, however a restart is required for this to take effect.）	変更を有効にするためにExpresswayを再起動します。	警告
15029	クラッシュレポートの送信に失敗しました（Failed to send Crash Report）	クラッシュレポートをサーバに送信できませんでした。	Expressway とクラッシュレポートサーバ間のネットワーク接続を確認します。クラッシュレポートサーバ証明書の有効期限が切れていないか、無効にされ、CA チェーン内の証明書が信頼ストアで更新されたのを確認します。	
15030	Unified CM データのクロスチェックの失敗（Unified CM data crosscheck failure）	Expressway の Unified CM 構成データは一貫していません。	すべての Unified CM サーバを削除してから、再度追加してください。詳細については、『Cisco Expressway 導入ガイドによるモバイルおよび Remote Access』の「Unified CM サーバの検出」セクションをご覧ください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
15031	HSM TLPがインストールされていません（HSM TLP not installed）	HSM の障害には管理者の注意が必要です。	詳細についてはアップグレードページを参照してください。	エラー
15022	Unified CM サーバーを使用できません（Unified CM server unavailable）	発行者のUnified CM設定に使用できないサーバが含まれています。	詳細については、イベントログを参照してください。問題を解決して更新します。詳細については、『Cisco Expressway 導入ガイドによるモバイルおよび Remote Access』の「Unified CM サーバの検出」セクションをご覧ください。	警告

表 *6:* クラスタアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20020	再起動が必要です（Restart required）	TLS 検証設定がアクティブなステータスと一致しません。	システムを再起動します。	警告
20021	クラスタ通信障害（Cluster communication failure）	<peers> との TCP 接続をポート <ports> で確立できません	ポート リファレンス ガイドを確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20003	無効なクラスタ設定（Invalid cluster configuration）	クラスタ設定が無効です（The cluster configuration is invalid）	「クラスタリング（Clustering）」ページをチェックして、このシステムの IP アドレスが含まれていること、および重複する IP がないことを確認します。	警告
20004	クラスタ通信障害（Cluster communication failure）	システムがクラスタ内のピアの 1 つまたは複数と通信できません（The system is unable to communicate with one or more of the cluster peers）	クラスタリング設定を確認します。	警告
20005	無効なピア アドレス（Invalid peer address）	無効なピア アドレスが 1 つ以上あります（One or more peer addresses are invalid）	「クラスタリング（Clustering）」ページをチェックし、すべての [ピア（Peer）] フィールドに有効な IP アドレスが使用されていることを確認します。	警告
20006	クラスタ データベース通信障害（Cluster database communication failure）	1 つ以上のクラスタ ピアでデータベースを複製できません（The database is unable to replicate with one or more of the cluster peers）	クラスタリング設定を確認し、再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20007	再起動が必要です（Restart required）	クラスタ設定が変更されました。これを有効にするには再起動が必要です（Cluster configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
20008	クラスタ複製エラー（Cluster replication error）	アップグレードが進行中のため、設定の自動レプリケーションが一時的に無効にされました（Automatic replication of configuration has been temporarily disabled because an upgrade is in progress）	アップグレードが完了するまで待ちます。	警告
20009	クラスタ複製エラー（Cluster replication error）	設定の自動レプリケーション中にエラーが発生しました（There was an error during automatic replication of configuration）	クラスタ レプリケーションの手順を表示します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20011	クラスタ複製エラー（Cluster replication error）	このピアの設定がプライマリの設定と競合しています。設定を手動で同期化する必要があります（This peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告
20012	クラスタ複製エラー（Cluster replication error）	このピアのクラスタ設定がプライマリ設定ピアの設定と一致しません（This peer's cluster configuration settings do not match the configuration primary peer's settings）	このピアのクラスタを設定します	警告
20014	クラスタ複製エラー（Cluster replication error）	プライマリまたはこのピアの設定ファイルが見つかりません。設定を手動で同期化する必要があります（Cannot find primary or this peer's configuration file, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20014	クラスタ複製エラー（Cluster replication error）	プライマリまたはこの下位のピア構成ファイルが見つかりません	ノードを再起動する	警告
20015	クラスタ複製エラー（Cluster replication error）	ピアのリストにローカル Expressway が表示されません（The local Expressway does not appear in the list of peers）	このクラスタのピアのリストを確認します。	警告
20016	クラスタ複製エラー（Cluster replication error）	プライマリ ピアに到達できません（The primary peer is unreachable）	このクラスタのピアのリストを確認します。	警告
20017	クラスタ複製エラー（Cluster replication error）	プライマリ設定 ID に一貫性がありません。設定を手動で同期する必要があります（Configuration primary ID is inconsistent, manual synchronization of configuration is required）	クラスタ レプリケーションの手順を表示します。	警告
20018	無効なクラスタリング設定（Invalid clustering configuration）	H.323 モードを有効にする必要があります。クラスタリングではピア間に H.323 通信を使用します（H.323 mode must be turned On - clustering uses H.323 communications between peers）	H.323 モードを設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
20019	クラスタ名が設定されていません（Cluster name not configured）	FindMe またはクラスタリングを使用している場合は、クラスタ名を定義する必要があります（IfFindMe or clustering are in use a cluster name must be defined.）	クラスタ名を設定します。	警告
20024	クラスタ構成エラー（Cluster configuration error）	クラスタが不整合状態	クラスタを再作成するには、『Cisco Expressway クラスタ作成およびメンテナンス導入ガイド』を参照してください。	警告
20025	データベースの同期に失敗した（Failed to synchronize database）	ノード <nodename> でデータベースの同期ができませんでした、CLI の <nodename> ノードを再起動してください この場合、<nodename> は、IP アドレスまたは、完全修飾ドメイン名（FQDN）です。	CLI（コマンドライン インターフェイス）から影響を受けるノードを再起動します。	重大
20026	ClusterDB ログサーバーの回復に失敗しました（Failed to recover ClusterDB log server）	ClusterDB ログサーバーが凍結され、CDB ログメッセージは処理されません。	問題が解決しない場合は、シスコの担当者に連絡してください。	重大

表 *7:* ネットワークアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25001	再起動が必要です（Restart required）	ネットワーク設定が変更されました。これを有効にするには再起動が必要です（Network configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25002	日時を確認できません（Date and time not validated）	システムは NTP サーバから正確な日時を取得できません（The system is unable to obtain the correct time and date from an NTP server）	時刻設定を確認します。	警告
25003	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv4 アドレスがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have any IPv4 addresses defined）	IP 設定を構成します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25004	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv4 ゲートウェイがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv4 gateway defined）	IP 設定を構成します。	警告
25006	再起動が必要です（Restart required）	高度なネットワークのオプションキーが変更されました。これを有効にするには再起動が必要です（Advanced Networking option key has been changed, however a restart is required for this to take effect）	必要な LAN 設定とスタティック NAT 設定を「IP」ページで構成してから、システムを再起動します。	警告
25007	再起動が必要です（Restart required）	QoS設定が変更されました。これを有効にするには再起動が必要です（QoS settings have been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25008	再起動が必要です（Restart required）	ポート設定が変更されました。これを有効にするには再起動が必要です（Port configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25009	再起動が必要です（Restart required）	イーサネット設定が変更されました。これを有効にするには再起動が必要です（Ethernet configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25010	再起動が必要です（Restart required）	IP 設定が変更されました。これを有効にするには再起動が必要です（IP configuration has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25011	再起動が必要です（Restart required）	HTTPS サービスが変更されました。これを有効にするには再起動が必要です（HTTPS service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25013	IP 設定の不一致（IP configuration mismatch）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、システムには定義されている IPv6 ゲートウェイがありません（IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv6 gateway defined）	IP 設定を構成します。	警告
25014	設定の警告（Configuration warning）	IP プロトコルは IPv4 と IPv6 の両方に設定されていますが、Expressway には定義されている IPv6 アドレスがありません（IP protocol is set to both IPv4 and IPv6, but the Expressway does not have any IPv6 addresses defined）	IP 設定を構成します。	警告
25015	再起動が必要です（Restart required）	SSH サービスが変更されました。これを有効にするには再起動が必要です（SSH service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25016	非推奨のイーサネット速度（Ethernet speed not recommended）	イーサネット インターフェイスの速度設定が 1000Mb/s 全二重または 100Mb/s 全二重以外の値にネゴシエートされています。これによりネットワーク上でパケット損失が発生する可能性があります（An Ethernet interface speed setting has been negotiated to a value other than 1000Mb/s full duplex or 100Mb/s full duplex; this may result in packet loss over your network）	イーサネット パラメータを設定します。	警告
25017	再起動が必要です（Restart required）	HTTP サービスが変更されました。これを有効にするには再起動が必要です（HTTP service has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25018	ポート競合（Port conflict）	<function> <port> と <function> <port> 間にポートの競合が発生しています（There is a port conflict between <function> <port> and <function> <port>）	ポート設定を「ローカル インバウンド ポート（Local inbound ports）」ページと「ローカル アウトバウンド ポート（Local outbound ports）」ページで確認します。	警告
25019	詳細なログ レベルを設定しました（Verbose log levels configured）	ネットワーク ログまたはサポート ログの 1 つ以上のモジュールが [デバッグ（Debug）] レベルまたは [トレース（Trace）] レベルに設定されています（One or more modules of the Network Log or Support Log are set to a level of Debug or Trace）	ネットワーク ログ モジュールとサポート ログ モジュールは、シスコのサポート担当者による別途のアドバイスがない限り、[情報（Info）] レベルに設定する必要があります。診断ロギングが進行中の場合は、診断ロギングが停止した時点で自動的にリセットされます。	警告
25020	NTP クライアント障害（NTP client failure）	システムが NTP クライアントを実行できません（The system is unable to run the NTP client）	キー設定や有効期限を含め、NTP のステータス情報を確認します。	警告
25021	NTP サーバが使用できません（NTP server not available）	システムは NTP サーバに接続できません（The system is unable to contact an NTP server）	時刻設定とステータスを確認します。また、DNS 設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25022	トラバーサル ゾーンの時刻が同期されていません（Time not synchronized over traversal zone）	このサーバのシステム時刻が、SIP トラバーサル ゾーンのもう一方のサーバのシステム時刻と異なっています（The system time of this server is different from that on a server on the other side of a SIP traversal zone）	システムの時刻設定が一貫していることを確認します。変更を行った場合は、それが有効になるまで時間がかかることがあります。	警告
25023	XMPP のフェデレーション設定警告（XMPP Federation configuration warning）	フェデレーション用の Expressway アドレスを使用した Unified CM IM and Presence サービス サーバの設定に失敗しました（Failed to configure Unified CM IM and Presence Service servers with Expressway address for XMPP federation）	IM and Presence サービス サーバが稼働していることを確認し、AXL サービスがそこで実行されていることを確認してから、サーバを更新します。	警告
25024	XMPP 設定エラー（XMPP configuration error）	XMPP ネットワーク アドレスの設定が無効です（Invalid configuration of XMPP network address）	IPv4 アドレスが正しいことを確認します。127.0.0.1（ループバック アドレス）を使用することができます	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25026	再起動が必要です（Restart required）	Web 管理ポート設定が変更されました。これを有効にするには再起動が必要です（Web administration port has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
25027	SSLH 障害（SSLH failure）	設定ファイルが書き込まれていないため、プロトコル多重化サービスを開始できません。Expressway-E が TCP 443 で TURN 要求と WebRTC 要求をリッスンできません（The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.）	TURN サービスを再設定します。	クリティカル
25028	HSM ボックスの接続の問題（HSM box connectivity issue）	一部の HSM モジュールに問題があります	HSM 設定 ページで詳細をご確認ください	アラート

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
25029	再起動が必要です（Restart required）	TURNプロトコルモードを UDP に変更されました。このため、TCP 443 TURN サービスはオフになっていますが、これを有効にする場合は再起動が必要です。	システムを再起動します。	
25030	DNS 逆引き検索に失敗（Reverse DNS Lookup failed）	アドレス <サーバの *IP* アドレス> の DNS 逆引き参照を実行できませんでした。これにより、MRA ログインが失敗する可能性があります。	DNS サーバが、そのアドレス <サーバの*IP*アドレス*&gt* に対して有効な PTR レコードで設定されていることを確認してください。	エラー
25031	証明書検証が失敗しました（Certificate verification failed）	アドレス <*IP Address of E server*> の PTR レコードの FQDN が、IP <*IP Address of E server*> を持つそのサーバの証明書に提示された SAN エントリと一致しません。	Expressway-E のサーバ証明書に SAN エントリとして存在する FQDN を持つアドレス <*IP Address of E server*> に対して、有効な PTR レコード (1 つだけ) が作成されていることを確認してください。	エラー

表 *8 :* ライセンスアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30001	キャパシティ警告（Capacity warning）	同時発生トラバーサル コールの数がライセンス供与されている上限に近づいています（The number of concurrent traversal calls has approached the licensed limit）	シスコの担当者にお問い合わせください。	警告
30002	キャパシティ警告（Capacity warning）	同時発生トラバーサル コールの数がユニットの物理的な上限に近づいています（The number of concurrent traversal calls has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告
30003	キャパシティ警告（Capacity warning）	同時発生非トラバーサル コールの数がユニットの物理的な上限に近づいています（The number of concurrent non-traversal calls has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告
30004	キャパシティ警告（Capacity warning）	非トラバーサルの同時コールの数がライセンス制限に近づきました	シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30005	キャパシティ警告（Capacity warning）	TURN リレーの使用率がユニットの物理的な上限に近づいています（TURN relays usage has approached the unit's physical limit）	シスコの担当者にお問い合わせください。	警告
30007	キャパシティ警告（Capacity warning）	TURN リレーの使用率がライセンス供与されている上限に近づいています（TURN relays usage has approached the licensed limit）	シスコの担当者にお問い合わせください。	警告
30009	TURN リレーをインストールしました（TURN relays installed）	TURN サービスは Expressway-E のみで使用できます。TURN のオプション キーは無視されました（TURN services are only available on Expressway-E; TURN option key ignored）	オプションキーの追加/削除	警告
30010	キャパシティ警告（Capacity warning）	同時登録の数がライセンス制限に近づきました	シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30011	TURN リレー ライセンスが必要です（TURN relay licenses required）	TURN サービスは有効になっていますが、TURN リレー ライセンスのオプション キーがインストールされていません（TURN services are enabled but no TURN relay license option keys are installed）	オプションキーを追加するかTURN サービスを無効化します	警告
30012	損失したクラスタ ピアのライセンス使用状況（License usage of lost cluster peer）	クラスタ ピア <n> は <n> 時間以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されます（Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30013	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	クラスタピアの一部が、<n>時間以上利用できない状態です。クラスタ全体で使用可能な合計からライセンスが次のように削除されます（Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows:）<details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30014	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	クラスタ ピア <n> は <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されます（Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30015	損失したクラスタピアのライセンス使用状況（License usage of lost cluster peer）	クラスタピアの一部が、<n> 日以上利用できない状態です。クラスタ全体で使用可能な合計からライセンスが次のように削除されます（Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows:）<details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30016	損失したクラスタピアのライセンスがライセンスプールから除去されました（Licenses of lost cluster peer have been taken off the license pool）	クラスタ ピア <n> は <n> 日以上、使用できない状態になっています。クラスタ全体で使用可能な合計から <date> にライセンスが削除されました（Cluster peer <n> has been unavailable for more than <n> days. Its licenses have been removed from the total available for use across the cluster on <date>.）。	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30017	損失したクラスタピアのライセンスがライセンスプールから除去されました（Licenses of lost cluster peer have been taken off the license pool）	クラスタピアの一部が、<n> 日以上利用できない状態です。クラスタ全体で使用可能な合計からライセンスが次のように削除されました（Several cluster peers have been unavailable for more than <n> days. Their licenses have been removed from the total available for use across the cluster as follows:）<details>.	このピアの問題を解決するか、このピアをクラスタ設定から削除します。	警告
30018	プロビジョニングライセンスの上限に到達しました（Provisioning licenses limit reached）	同時にプロビジョニングされたデバイスの数がライセンス供与された上限に到達しました（The number of concurrently provisioned devices has reached the licensed limit）	プロビジョニングの制限は Cisco TMS によって設定されます。追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告
30019	コール ライセンスの上限に到達しました（Call license limit reached）	同時発生非トラバーサルコールイセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent traversal call licenses）	問題が解決しない場合は、シスコの担当者に連絡し、コール ライセンスを追加購入してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30020	コール ライセンスの上限に到達しました（Call license limit reached）	同時発生トラバーサル コール ライセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent traversal call licenses）	問題が解決しない場合は、シスコの担当者に連絡し、コール ライセンスを追加購入してください。	警告
30021	TURN リレー ライセンスの上限に到達しました（TURN relay license limit reached）	同時発生 TURN リレー ライセンスのライセンス上限の <n> に到達しました（You have reached your license limit of <n> concurrent TURN relay licenses）	問題が解決しない場合は、シスコの担当者に連絡し、TURN リレー ライセンスを追加購入してください。	警告
30022	コール キャパシティの上限に到達しました（Call capacity limit reached）	同時非トラバーサル コール数がユニットの物理的上限に達しました（The number of concurrent non-traversal calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30023	コール キャパシティの上限に到達しました（Call capacity limit reached）	同時発生トラバーサル コールの数がユニットの物理的な上限に到達しました（The number of concurrent traversal calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30024	TURN リレー キャパシティの上限に到達しました（TURN relay capacity limit reached）	同時発生 TURN リレー コールの数がユニットの物理的な上限に到達しました（The number of concurrent TURN relay calls has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30025	再起動が必要です（Restart required）	オプション キーまたはタイプが変更されました。これを有効にするには再起動が必要です（An option key or the type has been changed, however a restart is required for this to take effect）	システムを再起動します。	警告
30026	ルーム システムのライセンスの上限に近づいています（Approaching room system license limit）	TelePresence Room システムの同時登録数がライセンスの上限に近づいています（The number of concurrent registered TelePresence room systems is approaching the license limit）	追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30027	キャパシティ警告（Capacity warning）	TelePresence Room システムとデスクトップ システムの同時登録数が、1 つ以上のピアで物理的な上限に達しました（The number of concurrent registered TelePresence room systems and registered desktop systems has reached the physical limit in one or more peer(s)）	すべてのピアに登録が均等に配分されていることを確認します。システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30028	ルーム システムの登録の上限に到達しました（Room system registrations limit reached）	TelePresence Room システムの登録数がライセンスの上限に到達しました（The number of registered TelePresence room systems has reached the license limit）	追加のルーム システム ライセンスを購入するには、シスコの担当者にお問い合わせください。	警告
30029	デスクトップ システムのライセンスの上限に近づいています（Approaching desktop system license limit）	デスクトップ システムの同時登録数がライセンスの上限に近づいています（The number of concurrent registered desktop systems is approaching the license limit）	追加ライセンスが必要な場合は、シスコの担当者にお問い合わせください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30030	キャパシティ警告（Capacity warning）	TelePresence Room システムとデスクトップ システムの登録数がユニットの物理的な上限に到達しました（The number of registered TelePresence room systems and registered desktop systems has reached the unit's physical limit）	システムに容量を追加します。シスコの担当者にお問い合わせください。	警告
30031	デスクトップ システムのライセンスの上限に到達しました（Desktop system license limit reached）	デスクトップ システムの登録数がライセンスの上限に到達しました（The number of registered desktop systems has reached the license limit）	デスクトップ システムのライセンスを購入するには、シスコの担当者にお問い合わせください。	警告
30035	Eval の Smart ライセンス（Smart license in Eval）	システムは 1 日、2 日、3 日、7 日、30 日後に期限切れになる評価モードで動作しています	Cisco Smart Software Manager または衛星にシステムを登録します	警告
30036	Smart ライセンスが過負荷状態でコンプライアンスに適合していません（Smart license in overage out of compliance）	ライセンス数が不足しているため、システムが動作しています	Cisco Smart Software Manager で追加のライセンスを設定します	アラート

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30037	Smart ライセンス準拠外のプロビジョニングはありません（Smart license no provision out of compliance）	ライセンス数が不足しているため、システムが動作しています	ユーザおよびデバイスのプロビジョニング機能を復元するには、Cisco Smart Software Manager で追加ライセンスを取得してください	クリティカル
30038	Smart ライセンスプロビジョニングなしEvalの有効期限が切れました（Smart license no provision Eval expired）	ライセンス評価期間が期限切れで、製品が適用モードになっています	ユーザおよびデバイスのプロビジョニング機能を回復するには、ネットワーク接続を確認して、ライセンス認証を更新してください。	クリティカル
30039	期限切れ承認の Smart ライセンスの有効期限が切れました（Smart license in overage authorization expired）	ライセンス認証の期限が切れました	ユーザとデバイスのプロビジョニングする機能が失われないよう、ネットワーク接続とライセンス認証の更新を確認してください	アラート
30040	Smart ライセンスプロビジョニング認証が期限切れです（Smart license no provision authorization expired）	ライセンス認証が期限切れで、製品が強制モードになっています	ユーザおよびデバイスのプロビジョニング機能を回復するには、ネットワーク接続を確認して、ライセンス認証を更新してください。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30041	Smart ライセンスの登録が期限切れです（Smart license registration expired）	ライセンス登録の有効期限が切れ、システムが Cisco Smart Software Manager または衛星の登録を解除されています	Cisco Smart Software Manager または衛星へのネットワーク接続を確認してください。また、システムクロックが正しいことを確認してから、システムを Cisco Smart Software Manager またはサテライトに登録します。問題が解決しない場合は、TAC ケースを上げてください。	エラー
30042	Smart ライセンス通信エラー（Smart license communication error）	システムがクラウドベースの Cisco Smart Software Manager または On-Prem との通信に失敗しました	クラウドベースの Cisco Smart Software Manager または On-Prem とのネットワーク接続を確認してください	エラー
30043	Smart ライセンス認証の有効期限が間もなく切れます（Smart license authorization expiring soon）	ライセンス認可期間が間もなく終了します	承認の更新を開始してください	警告
30044	Smart ライセンスの更新認証に失敗しました（Smart license renew auth failed）	ライセンス認証の更新に失敗しました	承認の更新を再試行してください。問題が解決しない場合は、TAC ケースを上げてください	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
30045	Smart ライセンスの更新登録に失敗しました（Smart license renew registration failed）	ライセンス登録の更新に失敗しました	登録の更新を再試行してください。問題が解決しない場合は、TAC ケースを上げてください	エラー
30046	Smart ライセンス登録の有効期限が間もなく切れます（Smart license registration expiring soon）	Cisco Smart Software Manager または衛星への登録はすぐに期限切れになります	ユーザまたはデバイスをプロビジョニングする機能が失われないように登録更新を開始してください	警告
30047	キャパシティ警告（Capacity warning）	システムが、エクスポート制御分類による暗号化シグナリングセッションのデバイス数をサポートするためのライセンス制限に達しました	シスコの担当者にお問い合わせください。	警告
30048	キャパシティワーニングに近づいています（Approaching Capacity warning）	システムが、エクスポート制御分類による暗号化シグナリングセッションのデバイス数をサポートするためのライセンス制限に近づいています	シスコの担当者にお問い合わせください。	警告

表 *9:* 外部アプリケーション/サービスアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35001	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、NDS ホスト名が設定されていません（Active Directory mode has been enabled but the DNS hostname has not been configured）	DNS ホスト名を設定します。	警告
35002	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、NTP サーバが設定されていません（Active Directory mode has been enabled but the NTP server has not been configured）	NTP サーバを設定します。	警告
35003	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、DNS サーバが設定されていません（Active Directory mode has been enabled but no DNS servers have been configured）	DNS サーバを設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35004	LDAP設定が必要です（LDAP configuration required）	管理者アカウントまたはFindMeアカウントにリモートログイン認証を使用していますが、有効なLDAPサーバアドレス、ポート、Bind_DN、およびBase_DNが設定されていません（Remote login authentication is in use for administrator accounts but a valid LDAP Server address, Port, Bind_DN and Base_DN have not been configured）	LDAPパラメータを設定します	警告
35005	設定の警告（Configuration warning）	Active Directoryモードは有効になっていますが、ドメインが設定されていません（Active Directory mode has been enabled but a domain has not been configured）	[Active Directoryサービス（Active Directory Service）]ページでドメインを設定します	警告
35007	設定の警告（Configuration warning）	Active Directory SPNEGOが無効になっています。SPNEGO設定を有効にすることを推奨します（Active Directory SPNEGO disabled; you are recommended to enable the SPNEGO setting）	SPNEGOを有効にします。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35008	設定の警告（Configuration warning）	Active Directory モードは有効になっていますが、ワークグループが設定されていません（Active Directory mode has been enabled but a workgroup has not been configured）	[Active Directory サービス（Active Directory Service）] ページでワークグループを設定します。	警告
35009	TMS プロビジョニング拡張サービスの通信障害（TMS Provisioning Extension services communication failure）	Expressway は TMS Provisioning Extension サービスと通信できません。TMS がこのクラスタに対してユーザのプロビジョニングを行っていない場合は、電話帳サービスの障害も発生している可能性があります（The VCS is unable to communicate with the TMS Provisioning Extension services. Phone book service failures can also occur if TMS does not have any users provisioned against this cluster.）	「TMS Provisioning Extension サービスのステータス（TMS Provisioning Extension service status）」ページに移動し、障害が発生したサービスを選択して問題に関する詳細を表示します	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35010	TMS プロビジョニング拡張サービス データのインポート障害（TMS Provisioning Extension services data import failure）	Expressway の内部テーブルの制限超過が発生するため、TMS Provisioning Extension サービスからのインポートがキャンセルされました（An import from the TMS Provisioning Extension services has been canceled as it would cause the Expressway to exceed internal table limits）	Expressway イベント ログで詳細を確認した後、TMS 内の対応するデータを確認します。TMS 内のデータを修正した後、完全同期を実行する必要があります。	警告
35011	TMS プロビジョニング拡張サービス データのインポート障害（TMS Provisioning Extension services data import failure）	TMS プロビジョニング拡張サービスからインポートしたレコードのうち 1 つ以上が認識できないデータ形式であったためドロップされました（One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format）	Expressway イベント ログで詳細を確認した後、TMS 内の対応するデータを確認します。TMS 内のデータを修正した後、完全同期を実行する必要があります。	警告
35012	LDAP サーバへの接続に失敗しました（Failed to connect to LDAP server）	H.350 デバイス認証用の LDAP サーバに接続できません（Failed to connect to the LDAP server for H.350 device authentication）	H.350 ディレクトリ サービスが正しく設定されていることを確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35013	ユニファイドコミュニケーションSSHトンネルの障害（Unified Communications SSH tunnel failure）	[このシステムは1つ以上のリモートホストと通信できません（This system cannot communicate with one or more remote hosts）]：<*Host 1, Host 2, ...*> ホストのリストは200文字に切り詰められます。	イベントログを確認し、Expressway-CとExpressway-E間のトラバーサルゾーンがアクティブであることを確認します。	警告
35014	ユニファイドコミュニケーションSSHトンネル通知の障害（Unified Communications SSH tunnel notification failure）	このシステムは、1つ以上のリモートホストと通信できません（This system cannot communicate with one or more remote hosts）	ファイアウォールがExpressway-Cのエフェメラルポートから Expressway-Eの2222 TCPへのトラフィックを許可することを確認します。	警告
35015	Unified CMのポート競合（Unified CM port conflict）	Unified CM <name> とユニファイドコミュニケーション間でUnified CM <name> にポート競合が発生しています（両方ともポート <number> を使用しています）	回線側（ユニファイドコミュニケーション）とSIPトランクトラフィックにUnified CM上の同じポートを使用できません。Unified CM上のポート設定を確認し、必要に応じて <zone> を再設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
35016	SAML メタデータが変更されました（SAML metadata has been modified）	設定変更によってローカル SAML メタデータが変更されました。ID プロバイダーのどのコピーとも異なっています。このメタデータはサーバ証明書または SSO 対応ドメインの変更によって、あるいはトラバーサル サーバ ピアの番号またはそれらのアドレスの変更によって変更された可能性があります（Configuration changes have modified the local SAML metadata, which is now different to any copies on Identity Provider(s). This metadata may have been modified by changing the server certificate or the SSO-enabled domains, or by changing the number of traversal server peers or their addresses）	アイデンティティ プロバイダーにインポートできるよう、SAML メタデータをエクスポートします。	警告

表 *10*：セキュリティアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40001	セキュリティ アラート（Security alert）	CRL 配布ポイントが自動更新用に定義されていません（No CRL distribution points have been defined for automatic updates）	CRL 設定を確認します。	警告
40002	セキュリティ アラート（Security alert）	CRL ファイルの自動更新に失敗しました（Automatic updating of CRL files has failed）	問題が解決しない場合は、シスコの担当者に連絡してください	警告
40003	安全でないパスワードが使用されています（Insecure password in use）	root ユーザにデフォルトのパスワードが設定されています（The root user has the default password set）	root パスワードの変更手順を表示します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40004	証明書ベースの認証が必要です（Certificate-based authentication required）	高度なアカウントセキュリティモードでは、システムのクライアント証明書ベースのセキュリティを[証明書ベースの認証（Certificate-based authentication）]に設定することを推奨します（Your system is recommended to have client certificate-based security set to Certificate-based authentication when in advanced account security mode）	クライアント証明書ベースのセキュリティを設定します	警告
40005	安全でないパスワードが使用されています（Insecure password in use）	admin ユーザにデフォルトのパスワードが設定されています（The admin user has the default password set）	admin パスワードを変更します。	エラー
40006	セキュリティ アラート（Security alert）	CRL の更新をダウンロードできません（Unable to download CRL update）	CRL 配布ポイントとイベント ログを確認します。	警告
40007	セキュリティ アラート（Security alert）	CRL 自動更新用の設定ファイルが見つかりませんでした（Failed to find configuration file for CRL automatic updates）	問題が解決しない場合は、シスコの担当者に連絡してください	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40008	セキュリティ アラート（Security alert）	SSHサービスがデフォルトのキーを使用しています（The SSH service is using the default key）	デフォルトのSSHキーの変更手順を表示します	警告
40009	再起動が必要です（Restart required）	HTTPS クライアント証明書の検証モードが変更されました。これを有効にするには再起動が必要です（HTTPS client certificates validation mode has changed, however a restart is required for this to take effect）	システムを再起動します。	警告
40011	アカウント単位のセッションの制限が必要です（Per-account session limit required）	高度なアカウントセキュリティモードでは、ゼロ以外のアカウント単位のセッションの制限が必要（A non-zero per-account session limit is required when in advanced account security mode）	アカウント単位のセッションの制限を設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40012	外部マネージャの接続にHTTPを使用しています（External manager connection is using HTTP）	高度なアカウントセキュリティモードでは、外部マネージャへの接続にHTTPSを使用することを推奨します（You are recommended to use HTTPS connections to the external manger when in advanced account security mode）	外部マネージャを設定します。	警告
40013	HTTPSクライアント証明書の検証が無効になっています（HTTPS client certificate validation disabled）	高度なアカウントセキュリティモードでは、HTTPS接続に対してクライアント側の証明書の検証を有効にすることを推奨します（You are recommended to enable client side certificate validation for HTTPS connections when in advanced account security mode）	HTTPSクライアント証明書の検証を設定します	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40014	タイムアウト時間が必要です（Time out period required）	高度なアカウントセキュリティモードでは、ゼロ以外のシステムセッション タイムアウト時間が必要です（A non-zero system session time out period is required when in advanced account security mode）	セッション タイムアウト時間を設定します。	警告
40015	システム セッションの制限が必要です（System session limit required）	高度なアカウントセキュリティモードでは、ゼロ以外のシステムセッションの制限が必要です（A non-zero system session limit is required when in advanced account security mode）	システム セッションの制限を設定します。	警告
40016	暗号化が必要です（Encryption required）	高度なアカウントセキュリティモードでは、ログイン アカウントのLDAPサーバ設定で暗号化を[TLS] に設定することを推奨します（Your login account LDAP server configuration is recommended to have encryption set to TLS when in advanced account security mode）	ログイン アカウントLDAPサーバを設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40017	インシデント レポートが有効になっています（Incident reporting enabled）	高度なアカウント セキュリティ モードでは、インシデント レポートを無効にすることを推奨します（You are recommended to disable incident reporting when in advanced account security mode）	インシデント レポートを設定します。	警告
40018	安全でないパスワードが使用されています（Insecure password in use）	1 人以上のユーザが厳密でないパスワードを使用しています（One or more users has a non-strict password）		警告
40019	外部マネージャの証明書チェックを無効にしました（External manager has certificate checking disabled）	高度なアカウント セキュリティ モードでは、外部マネージャの証明書チェックを有効にすることを推奨します（You are recommended to enable external manager certificate checking when in advanced account security mode）	外部マネージャを設定します。	警告
40020	セキュリティ アラート（Security alert）	Active Directory サービスへの接続に TLS 暗号化を使用していません（The connection to the Active Directory Service is not using TLS encryption）	Active Directory サービスの接続設定を行います	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40021	リモート ロギングが有効になっています（Remote logging enabled）	高度なアカウント セキュリティ モードでは、リモート syslog サーバを無効にすることを推奨します（You are recommended to disable the remote syslog server when in advanced account security mode）	リモート ロギングを設定します。	警告
40022	セキュリティ アラート（Security alert）	Active Directory セキュア チャネルが無効になっています。セキュア チャネル設定を有効にすることを推奨します（Active Directory secure channel disabled; you are recommended to enable the secure channel setting）	セキュア チャネルを有効にします。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40024	CRL チェックが必要です（CRL checking required）	高度なアカウントセキュリティモードでは、ログイン アカウントのLDAP サーバ設定で証明書失効リスト（CRL）のチェックを [すべて（All）] に設定することを推奨します（Your login account LDAP server configuration is recommended to have certificate revocation list (CRL) checking set to All when in advanced account security mode）	ログイン アカウント LDAP サーバを設定します。	警告
40025	SNMP が有効になっています（SNMP enabled）	高度なアカウントセキュリティモードでは、SNMP を無効にすることを推奨します（You are recommended to disable SNMP when in advanced account security mode）	SNMP モードを設定します。	警告
40026	リブートが必要です（Reboot required）	高度なアカウントセキュリティモードを変更しました。これを有効にするにはリブートが必要です（The advanced account security mode has changed, however a reboot is required for this to take effect）	Expressway をリブートします	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40027	セキュリティ アラート（Security alert）	TMS プロビジョニング拡張サービスへの接続に TLS 暗号化を使用していません（The connection to the TMS Provisioning Extension services is not using TLS encryption）	TMS プロビジョニング拡張サービスの接続を設定します。	警告
40028	安全でないパスワードが使用されています（Insecure password in use）	root ユーザのパスワードは MD5 を使用してハッシュされますが、これでは十分に安全といえません（The root user's password is hashed using MD5, which is not secure enough）	root パスワードの変更手順を表示します。	警告
40029	LDAP サーバの CA 証明書がありません（LDAP server CA certificate is missing）	LDAP データベースの有効な CA 証明書がアップロードされていません。これは TLS を介した接続に必要です（A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS）	有効な CA 証明書をアップロードします。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40030	セキュリティ アラート（Security alert）	ファイアウォール ルールのアクティブ化に失敗しました。ファイアウォール設定に少なくとも 1 つの拒否されたルールが含まれています（Firewall rules activation failed; the firewall configuration contains at least one rejected rule）	ファイアウォール ルールの設定を確認して拒否されたルールを修正し、再有効化を試みます。	警告
40031	セキュリティ アラート（Security alert）	以前のファイアウォール設定を復元できません（Unable to restore previous firewall configuration）	ファイアウォール ルールの設定を確認後、拒否されたルールを修正してルールをアクティブ化して、承認します。問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告
40032	セキュリティ アラート（Security alert）	ファイアウォールを初期化できません（Unable to initialize firewall）	システムを再起動します。問題が解決しない場合は、シスコの担当者にお問い合わせください	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40033	設定の警告（Configuration warning）	デフォルトのゾーン アクセス ルールは有効になっていますが、SIP over UDP または SIP over TCP を有効のままにしておくと、このセキュリティ機能を回避する手段を提供することになります（The Default Zone access rules are enabled, but leaving SIP over UDP or SIP over TCP enabled offers a way to circumvent this security feature）	[SIP] ページで UDP と TCP を無効にして TLS を使用した証明書アイデンティティ チェックを適用するか、またはデフォルト ゾーンに対するアクセス ルールを無効にします。	警告
40034	セキュリティ アラート（Security alert）	ファイアウォールのアクティブ化に失敗しました。ファイアウォール設定にプライオリティの重複があります（Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities）	ファイアウォール ルールの設定をチェックしてすべてのルールに一意のプライオリティがあることを確認してからアクティブ化を再試行します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40036	委任クレデンシャルチェックエラー（Delegated credential checking error）	SIPドメイン <domain> に関連付けられたトラバーサルサーバゾーンは、トラバーサルクライアントシステムに接続できません	ドメインとそれに関連付けられたトラバーサルサーバゾーンが正しく設定されていることを確認します。また、リモートトラバーサルクライアントシステムを確認する必要もあります	警告
40037	委任クレデンシャルチェックエラー（Delegated credential checking error）	委任クレデンシャルチェック要求の受信に使用するトラバーサルクライアントゾーン <zone> に通信の問題があります	そのトラバーサルクライアントゾーンが正しく設定されていることを確認します。また、リモートトラバーサルサーバ システムを確認する必要があります	警告
40038	委任クレデンシャルチェック設定エラー（Delegated credential checking configuration error）	SIPドメイン <domain>に関連付けられているトラバーサルサーバゾーンでTLS検証モードが有効になっていません	ドメインをチェックし、TLS 検証モードが関連付けられているトラバーサルサーバゾーンで有効になっていることを確認します	警告
40039	委任クレデンシャルチェック設定エラー（Delegated credential checking configuration error）	委任認証要求を受け入れるように設定されたトラバーサルクライアントゾーン (<zone>) でTLS検証モードが有効になっていません	TLS確認モードがトラバーサルクライアントゾーンで有効になっていることを確認します	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40040	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	TLS検証モードがユニファイド コミュニケーション サービス用に設定されたトラバーサル ゾーンで有効になっていません（TLS verify mode is not enabled on a traversal zone configured for Unified Communications services）	TLS検証モードがトラバーサル ゾーンで有効になっていることを確認します。また、リモート トラバーサル システムを確認する必要もあります。	警告
40041	セキュリティ アラート（Security alert）	自動化された侵入からの保護のルールが使用できません（Automated intrusion protection rules are not available）	失敗したサービスを無効にしてから、もう一度有効にします。	警告
40042	FIPS1 40-2 コンプライアンスの規制（FIPS140-2 compliance restriction）	一部のSIP設定がTLSトランスポートを使用していません。FIPS140-2に準拠するにはTLS が必要です（Some SIP configuration is not using TLS transport; FIPS140-2 compliance requires TLS）	[SIP] ページでTLSがシステム全体で対応する唯一のトランスポートであり、すべてのゾーンが TLS を使用していることを確認します。または、FIPS140-2に移行する場合は、FIPS 対応のデータのバックアップを復元できます。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40043	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	メディア暗号化がユニファイド コミュニケーション サービス用に設定されたトラバーサル ゾーンに適用されません（Media encryption is not enforced on a traversal zone configured for Unified Communications services）	メディア暗号化がトラバーサル ゾーンに対して [強制暗号化（Force encrypted）] に設定されていることを確認します。	警告
40044	システムのリセットが必要です（System reset required）	FIPS140-2 モードが有効化されています。システム リセットを実行するには、このプロセスを完了させる必要があります（FIPS140-2 mode has been enabled; a system reset is required to complete this process）	すべてのアラームがクリアされていることを確認してから、システムのリセットを実行する前にシステムのバックアップを実行します。	警告
40045	再起動が必要です（Restart required）	FIPS140-2 モードが無効化されています。システム リセットを実行するには、このプロセスを完了させる必要があります（FIPS140-2 mode has been disabled; a system restart is required to complete this process）	システムを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40046	FIPS1 40-2 コンプライアンスの規制（FIPS140-2 compliance restriction）	クラスタ化されたシステムが FIPS140-2 に準拠していません（Clustered systems are not FIPS140-2 compliant）	クラスタを解除します。	警告
40048	ユニファイド コミュニケーションの設定エラー（Unified Communications configuration error）	ユニファイド コミュニケーション サービスは有効になっていますが、SIP TLS が無効になっています（Unified Communications services are enabled but SIP TLS is disabled）	SIP TLS モードが [SIP の設定（SIP configuration）] ページで [オン（On）] に設定されていることを確認します。	警告
40049	クラスタ TLS の許容（Cluster TLS permissive）	クラスタ TLS 検証モードで無効な証明書が許容されています（Cluster TLS verification mode permits invalid certificates）	クラスタの TLS 検証モードを Enforcing に変更します	通知
40050	セキュリティ アラート（Security alert）	新しいファイアウォール設定をインストールできません（Unable to install new firewall configuration）	ファイアウォール設定とレート制限設定を確認し、拒否されたルールを修正します。システムを再起動しないでください。問題が解決しない場合は、シスコの担当者にお問い合わせください。	

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40051	サーバ証明書によって CMS が特定されません（CMS not Identified by Server Certificate）	CMS アドレス <*address*>は Expressway-C で入力されましたが、Expressway-E サーバ証明書で特定されません（CMS address <address> has been entered on the Expressway-C but is not identified by the Expressway-E server certificate）	Expressway-C の CMS アドレスが Expressway-E サーバの SAN エントリに一致することを確認します。CMS を SAN として含む新しいサーバ証明書の CSR を生成するか、Expressway-C 上の CMS を編集（または削除）します。	
40052	証明書エラー（Certificate error）	サーバ証明書には共通名（CN）属性がありません。一部のサービスは CN なしでは動作しません（Server certificate does not have a Common Name (CN) attribute. Some services do not work without the CN）	証明書を更新します。	
40053	無効な暗号化設定（Invalid Cipher config）	次のエントリには、FIPS140-2 モードで無効な暗号値 <*List*> があります（The following entries have cipher values that are invalid in FIPS140-2 mode: <List>）	暗号方式で影響を受ける暗号化エントリを再設定してください。	

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40054	トークンの復号の失敗（Token decryption failure）	Expressway-C は、Unified CM によって発行された OAuth トークンの復号化に失敗しました。これは、発行者の変更が原因である可能性があります（The Expressway-C failed to decrypt or decode an OAuth token issued by Unified CM. This could be caused by changes to the issuer.）。	Cisco Unified Communications Manager の設定を更新します。	警告
40055	キー ファイルの更新に失敗しました（Failed to update key file））	一貫性のない状態のためにシステム キー ファイルの更新に失敗しました（Failed to update system key file due to inconsistent state）	システムを再起動します。それでも問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告
40061	ACME 自動署名の障害（ACME auto-sign failure）	サーバ証明書の自動署名コマンドを実行中に障害が検出されました（A failure was detected while running the auto-sign command for the server certificate）	詳細については、サーバ証明書のページを参照してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40062	ACME 自動署名の障害（ACME auto-sign failure）	SNI ドメイン [<*domain*>] の自動署名コマンドを実行中に障害が検出されました（A failure was detected while running the auto-sign command for SNI domains [<domain>]）	詳細については、ドメイン証明書のページを参照してください。	警告
40063	ACME 自動展開の障害（ACME auto-deploy failure）	サーバ証明書の自動展開コマンドを実行中に障害が検出されました（A failure was detected while running the auto-deploy command for the server certificate）	詳細については、サーバ証明書のページを参照してください。	警告
40064	ACME 自動展開の障害（ACME auto-deploy failure）	SNI ドメイン [<domain>] の自動展開コマンドを実行中に障害が検出されました（A failure was detected while running the auto-deploy command for SNI domains [<domain>]）	詳細については、ドメイン証明書のページを参照してください。	警告
40066	HSM 証明書が使用されていません（HSM certificate is not used）	HSM 証明書がインストールされていますが、使用されていません	HSM 設定 ページで詳細をご確認ください	アラート
40068	サーバ証明書の有効性（Server certificate validity）	サーバ証明書の有効期限が切れた、またはサーバ証明書が本日期限切れです	新しいサーバ証明書を作成してアップロードします	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
40069	サーバ証明書の有効性（Server certificate validity）	<*n*>日でサーバ証明書の有効期限が切れます	新しいサーバ証明書を作成してアップロードすることをお勧めします	アラート
40100	セキュリティ アラート（Security alert）	ファイアウォール ルールがネットワーク インターフェイスと同期されていません（Firewall rules are not synchronized with network interfaces）	システムを再起動します。それでも問題が解決しない場合は、シスコの担当者にお問い合わせください。	警告
40101	タイムアウト絶対期間が必要です（Absolute Time out period required）	高度なアカウント セキュリティ モードでは、ゼロ以外のシステム セッション タイムアウト絶対時間が必要です	タイムアウト絶対期間の構成	警告

表 *11* : 設定ミスアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45001	コール ポリシー ファイルのロードに失敗しました（Failed to load Call Policy file）	<failure details>	コール ポリシーを設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45002	設定の警告（Configuration warning）	デフォルト サブゾーンとデフォルト ゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Default Zone is missing）	デフォルトのリンクを設定します。	警告
45003	設定の警告（Configuration warning）	H.323 モードと SIP モードがオフに設定されています。それらの一方または両方を有効にしてください（H.323 and SIP modes are set to Off; one or both of them should be enabled）	H.323 モードまたは SIP モードあるいはその両方を設定します。	警告
45006	設定の警告（Configuration warning）	デフォルト サブゾーンとクラスタ サブゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Cluster Subzone is missing）	デフォルトのリンクを設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45007	設定の警告（Configuration warning）	デフォルト サブゾーンとトラバーサル サブゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Default Subzone and the Traversal Subzone is missing）	デフォルトのリンクを設定します。	警告
45008	設定の警告（Configuration warning）	トラバーサル サブゾーンとデフォルト ゾーン間に予期していたデフォルト リンクがありません（Expected default link between the Traversal Subzone and the Default Zone is missing）	デフォルトのリンクを設定します。	警告
45009	設定の警告（Configuration warning）	プロビジョニングを正しく動作させるには、デフォルト ゾーンと、プロビジョニング要求を受信する関連ゾーンで認証ポリシーを有効にする必要があります（For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests）	各関連ゾーンの認証ポリシーを「[クレデンシャルの確認（Check credentials）]」または「[認証済みとして処理（Treat as authenticated）]」に設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45012	設定の警告（Configuration warning）	プレゼンス サービスが正しく動作するためには、デフォルト サブゾーンとそれに関連するすべてのサブゾーンが有効化されている必要があります。エンドポイントが登録されていない場合も、デフォルト ゾーンでの認証が有効化されていなければなりません。	デフォルトサブゾーンと各関連サブゾーンおよびゾーンの認証ポリシーを「[クレデンシャルの確認（Check credentials）]」または「[認証済みとして処理（Treat as authenticated）]」に設定します。	警告
45013	設定の警告（Configuration warning）	電話帳を正しく動作させるには、デフォルト サブゾーンとその他の関連サブゾーンで認証ポリシーを有効にする必要があります。また、エンドポイントが登録されていない場合は、デフォルト ゾーンで認証を有効にする必要もあります（For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered）	デフォルトサブゾーンと各関連サブゾーンおよびゾーンの認証ポリシーを「[クレデンシャルの確認（Check credentials）]」または「[認証済みとして処理（Treat as authenticated）]」に設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45014	設定の警告（Configuration warning）	SIP メディア暗号化モードが「Force encrypted」 または 「Force unencrypted」 の状態で、ゾーン内でH.323 が有効になっています。	関連するゾーンでH.323 を無効にするか、別のSIP メディア暗号化モードを選択します	警告
45016	設定の警告（Configuration warning）	ゾーンの SIP メディア暗号化モードは「[ベストエフォート（Best effort）]」 または「[強制暗号化（Force encrypted）]」 に設定されていますが、トランスポートが TLS ではありません。TLSは暗号化に必要です。（A zone has a SIP media encryption mode of "Best effort" or "Force encrypted" but the transport is not TLS. TLS is required for encryption.）	関連するゾーンでSIP トランスポートを TLS に設定するか、または別のSIP メディア暗号化モードを選択します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45017	設定の警告（Configuration warning）	サブゾーンの SIP メディア暗号化モードは 「[ベスト エフォート（Best effort）]」または 「[強制暗号化（Force encrypted）]」 に設定されていますが、TLS が有効になっていません。TLS は暗号化に必要です。（A zone has a SIP media encryption mode of "Best effort" or "Force encrypted" but the transport is not TLS. TLS is required for encryption.）	[SIP の設定（SIP configuration）] ページで TLS を有効にするか、または関連するサブゾーンまたはデフォルト サブゾーンに別の SIP メディア暗号化モードを選択します	警告
45018	設定の警告（Configuration warning）	DNS ゾーン（<zone_name>) など）の SIP のデフォルト トランスポート プロトコルが <protocol>) に設定されていますが、そのプロトコルはシステム全体にわたって無効になっています（DNS zones (including <zone_name>) have their SIP default transport protocol set to <protocol>), but that protocol is disabled system-wide.）。	DNS ゾーンの SIP のデフォルトのトランスポート プロトコルとシステム全体の SIP トランスポートの設定が一貫していることを確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45019	メディア ポートの不足（Insufficient media ports）	ライセンス供与されたコールの数をサポートするにはメディア ポートの数が足りません（There is an insufficient number of media ports to support the number of licensed calls）	メディア ポート範囲を拡大します。	警告
45021	HSMサーバ設定の問題	HSM サーバ構成に問題があります	HSM 設定 ページで詳細をご確認ください	アラート
45022	再起動が必要です（Restart required）	DMI 管理構成が変更されましたが、これを有効にするには再起動が必要です。	システムを再起動します。	警告
45023	設定エラー（Configuration error）	複数の接続間でホスト/ポートタプルを共有しようと試みます。	ゾーンを確認して、ホスト名またはポートの競合を修正します	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
45024	SSLH 障害（SSLH failure）	管理 *DMI* のみモードが設定され、Web Administration がポート 443 を使用している場合、プロトコル多重サービスは開始できません。Expressway が TCP 443 で TURN 要求と WebRTC 要求をリッスンできません（The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.）		クリティカル

表 *12 :* バックツーバックユーザエージェントアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55001	B2BUA サービス再起動が必要です（B2BUA service restart required）	一部の B2BUA サービス固有の設定が変更されました。これを有効にするには再起動が必要です（Some B2BUA service specific configuration has changed, however a restart is required for this to take effect）	B2BUAサービスをリスタートする	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55002	B2BUA の誤設定（B2BUA misconfiguration）	Expressway 通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for Expressway communications is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55003	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft デバイスの信頼できるホストの IP アドレスが無効です（Invalid trusted host IP address of Microsoft device）	設定されている信頼できるホストのアドレスを確認します	警告
55004	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft コール通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for Microsoft call communications is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55005	B2BUA の誤設定（B2BUA misconfiguration）	Microsoftの宛先アドレスが誤って設定されています（The Microsoft destination address is misconfigured）	B2BUA の設定を確認します。	警告
55006	B2BUA の誤設定（B2BUA misconfiguration）	Microsoftの宛先ポートが誤って設定されています（The Microsoft destination port is misconfigured）	B2BUA の設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55007	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft トランス ポート タイプの設定が誤っています（The Microsoft transport type is misconfigured）	B2BUA の設定を確認します。	警告
55008	B2BUA の誤設定（B2BUA misconfiguration）	サービスの FQDN がないか、または無効です（Missing or invalid FQDN of service）	Expressway のシステム ホスト名とドメイン名を確認します	警告
55009	B2BUA の誤設定（B2BUA misconfiguration）	サービスの IP アドレスが無効です（Invalid IP address of service）	Expressway の LAN 1 IPv4 アドレスを確認します	警告
55010	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA メディア ポート範囲の終了値の設定が誤っています（The B2BUA media port range end value is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55011	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA メディア ポート範囲の開始値の設定が誤っています（The B2BUA media port range start value is misconfigured）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55012	B2BUA の誤設定（B2BUA misconfiguration）	無効なMicrosoftの相互運用性モード（Invalid Microsoft interoperability mode）	B2BUA の設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55013	B2BUA の誤設定（B2BUA misconfiguration）	オプション キーが無効です（Invalid option key）	オプション キーを確認します	警告
55014	B2BUA の誤設定（B2BUA misconfiguration）	ホップ カウントが無効です（Invalid hop count）	[B2BUA の設定（B2BUA configuration）]（詳細設定）を確認します。	警告
55015	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの信頼できるホストの IP アドレスが無効です（Invalid trusted host IP address of transcoder）	設定されている信頼できるホストのアドレスを確認します	警告
55016	B2BUA の誤設定（B2BUA misconfiguration）	この B2BUA 用のトランスコーダを有効にする設定が誤っています（The setting to enable transcoders for this B2BUA is misconfigured）	B2BUA の設定（トランスコーダの設定）を確認します。	警告
55017	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダ通信用の B2BUA ポートの設定が誤っています（The port on B2BUA for transcoder communications is misconfigured）	B2BUA の設定（トランスコーダの設定）を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55018	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダアドレスまたはポートの詳細、あるいはその両方の設定が誤っています（Transcoder address and/or port details are misconfigured）	B2BUA 設定（トランスコーダの設定）と設定されている信頼できるホストのアドレスを確認します	警告
55019	B2BUA の誤設定（B2BUA misconfiguration）	TURN サーバのアドレスが無効です（Invalid TURN server address）	B2BUA の設定（TURN の設定）を確認します。	警告
55021	B2BUA の誤設定（B2BUA misconfiguration）	この B2BUA に TURN サービスを提供するための設定が誤っています（The setting to offer TURN services for this B2BUA is misconfigured）	B2BUA の設定（TURN の設定）を確認します。	警告
55026	B2BUA の誤設定（B2BUA misconfiguration）	TURN サービスは有効になっていますが、有効な TURN サーバが設定されていません（The B2BUA has been enabled to use transcoders, but there are no transcoders configured）	TURN サーバのアドレスを設定します	警告
55028	B2BUA の誤設定（B2BUA misconfiguration）	メディア ポート範囲の最初と最後の設定が誤っています（The start and end media port ranges are misconfigured）	B2BUA のメディア ポート範囲の設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55029	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA が使用するメディア ポート範囲が <module> で使用するメディア ポート範囲と重複しています	両方のサービスのポート設定を確認します。	警告
55030	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for Expressway communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告
55031	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft コールの通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for Microsoft call communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告
55032	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの通信に B2BUA が使用するポートは <module> も使用します（The port used by the B2BUA for transcoder communications is also used by <module>）	両方のサービスのポート設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55033	B2BUA の誤設定（B2BUA misconfiguration）	Microsoft の有効な信頼できるホストが設定されていません（No valid Microsoft trusted hosts have been configured）	少なくとも 1 つの信頼できるホストデバイスを設定します	警告
55034	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーダの有効な信頼できるホストが設定されていません（No valid transcoder trusted hosts have been configured）	少なくとも 1 つのトランスコーダの信頼できるホストを設定します。	警告
55035	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA がトランスコーダに接続できません（The B2BUA cannot connect to the transcoders）	B2BUAサービスをリスタートする	警告
55036	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA が Expressway に接続できません（The B2BUA cannot connect to the Expressway）	B2BUAサービスをリスタートする	警告
55037	B2BUA 接続の問題（B2BUA connectivity problem）	B2BUA が Microsoft 環境に接続できません（The B2BUA cannot connect to the Microsoft environment）	「Microsoft 相互運用性のステータス（Microsoft interoperability status）」ページで問題の詳細を確認します。設定変更を行った後に B2BUA サービスの再起動が必要になる場合があります	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55101	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の許可済みホスト IP アドレスが無効です（Invalid Expressway authorized host IP address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55102	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の連絡先アドレスの URI 形式が無効です（Invalid URI format of Expressway contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55103	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の暗号化モードが無効です（Invalid Expressway encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55104	B2BUA の誤設定（B2BUA misconfiguration）	Expressway ICE モードが無効です（Invalid Expressway ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55105	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップのホスト設定が無効です（Invalid Expressway next hop host configuration）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55106	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップの活性モードが無効です（Invalid Expressway next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55107	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップ モードが無効です（Invalid Expressway next hop mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55108	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップ ポートが無効です（Invalid Expressway next hop port）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55109	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のトランスポート タイプが無効です（Invalid Expressway transport type）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55110	B2BUA の誤設定（B2BUA misconfiguration）	B 側の連絡先アドレスの URI 形式が無効です（Invalid URI format of B side contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55111	B2BUA の誤設定（B2BUA misconfiguration）	B 側の暗号化モードが無効です（Invalid B side encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55112	B2BUA の誤設定（B2BUA misconfiguration）	B 側の ICE モードが無効です（Invalid B side ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55113	B2BUA の誤設定（B2BUA misconfiguration）	B 側のネクストホップの活性モードが無効です（Invalid B side next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55114	B2BUA の誤設定（B2BUA misconfiguration）	B 側のネクストホップ モードが無効です（Invalid B side next hop mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55115	B2BUA の誤設定（B2BUA misconfiguration）	コマンド リスニング ポートが無効です（Invalid command listening port）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55116	B2BUA の誤設定（B2BUA misconfiguration）	デバッグ ステータス パスが無効です（Invalid debug status path）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55117	B2BUA の誤設定（B2BUA misconfiguration）	サービスが無効です（Invalid service）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55118	B2BUA の誤設定（B2BUA misconfiguration）	ソフトウェア文字列が無効です（Invalid software string）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55119	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスの連絡先アドレスの URI 形式が無効です（Invalid URI format of transcoding service contact address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55120	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスの暗号化モードが無効です（Invalid transcoding service encryption mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55121	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスの ICE モードが無効です（Invalid transcoding service ICE mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55122	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスのネクスト ホップの活性モードが無効です（Invalid transcoding service next hop liveness mode）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55123	B2BUA の誤設定（B2BUA misconfiguration）	トランスコーディング サービスのトランス ポート タイプの設定が誤っています（The transcoding service transport type is misconfigured）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55124	B2BUA の誤設定（B2BUA misconfiguration）	必須 TURN サービスの設定が誤っています（The mandatory TURN server setting is misconfigured）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55125	B2BUA の誤設定（B2BUA misconfiguration）	Expressway のネクスト ホップのホスト設定が無効です（Invalid Expressway next hop host configuration）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55126	B2BUA の誤設定（B2BUA misconfiguration）	Expressway の許可済みホスト IP アドレスが無効です（Invalid Expressway authorized host IP address）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55127	B2BUA の誤設定（B2BUA misconfiguration）	FQDN 設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because FQDN configuration is missing）	**システムホスト名**と**ドメイン名**を [DNS] ページで設定してから B2BUA サービスを再起動します。	警告
55128	B2BUA の誤設定（B2BUA misconfiguration）	IPv4 インターフェイスのアドレス設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because IPv4 interface address configuration is missing）	LAN 1 IPv4 アドレスを「IP」ページで設定してから B2BUA サービスを再起動します	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55129	B2BUA の誤設定（B2BUA misconfiguration）	クラスタ名の設定がないため、B2BUA アプリケーションを起動できません（Cannot start B2BUA application because cluster name configuration is missing）	クラスタ名を [クラスタリング（Clustering）] ページで設定します。	警告
55130	B2BUA の誤設定（B2BUA misconfiguration）	クラスタ名が無効です（Invalid cluster name）	クラスタ名を確認してから B2BUA サービスを再起動します	警告
55131	B2BUA の誤設定（B2BUA misconfiguration）	セッション更新間隔が無効です（Invalid session refresh interval）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55132	B2BUA の誤設定（B2BUA misconfiguration）	コール リソース制限が無効です（Invalid call resource limit）	サービスを再起動します。問題が解決しない場合は、シスコの担当者に連絡してください。	警告
55133	B2BUA の誤設定（B2BUA misconfiguration）	B2BUA セッションの更新間隔が最小セッション更新間隔より小さくなっています（The B2BUA session refresh interval is smaller than the minimum session refresh interval）	両方の設定を [B2BUA の設定（B2BUA configuration）]（詳細設定）で確認してから B2BUA サービスを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55134	B2BUA の誤設定（B2BUA misconfiguration）	最小セッション更新間隔が無効です（Invalid minimum session refresh interval）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55135	B2BUA 設定の警告（B2BUA configuration warning）	Microsoft の信頼できるホスト デバイスが多数設定されています。そのため、パフォーマンスに影響を与える可能性があります。極端な場合は、コールが接続に十分なネットワーク リソースにアクセスできなくなる可能性があります（A large number of Microsoft trusted host devices have been configured; this may impact performance, or extreme cases it may prevent calls from accessing enough network resources to connect）	「B2BUA の信頼できるホスト（B2BUA trusted hosts）」ページでトポロジを確認し、信頼できるホスト デバイスの数を減らすようにします。	警告
55137	B2BUA の誤設定（B2BUA misconfiguration）	VCS マルチストリーム モードが無効です（Invalid VCS multistream mode）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告
55139	B2BUA の誤設定（B2BUA misconfiguration）	VCS マルチストリーム モードが無効です（Invalid VCS multistream mode）	B2BUA の設定（詳細設定）を確認してから B2BUA サービスを再起動します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
55142	RDP TCP/UDP ポートが不足しています（Insufficient RDP TCP/UDP ports）	RDP コールの最大数をサポートするには TCP/UDP ポートの数が足りません（There is an insufficient number of TCP/UDP ports to support the maximum number of RDP calls）	B2BUA 設定の RDP TCP/UDP ポート範囲を拡大します	警告

表 *13*：管理コネクタアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60050	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity error）	Cisco Collaboration Cloud のアドレス：<*string*> に到達できませんでした	<*string*> または <*string*> を確認するか、またはネットワーク ユーティリティ <*string*> を使用して、このアドレスを確認します。	エラー
60051	（ハイブリッドサービス）通信エラー（[Hybrid services] Communication error）	Cisco Collaboration Cloud からの HTTP エラー コード <*string*>（アドレス：<*string*>）	ハイブリッド サービスのステータスを確認します。問題が続くようであれば、Cisco Collaboration Cloud の管理者へお問い合わせください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60052	（ハイブリッドサービス）通信エラー（[Hybrid services] Communication error）	<*string*>	<*string*>、<*string*>、<*string*> のアドレスを確認してください。アドレスが問題の原因でない場合は、Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60053	（ハイブリッドサービス）アクセス エラー（[Hybrid services] Access error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60054	（ハイブリッドサービス）コネクタ インストール エラー（[Hybrid services] Connector install error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60055	（ハイブリッドサービス）証明書が無効なためダウンロードに失敗しました（[Hybrid services] Download failed because the certificate was not valid）	<*string*>	Expressway の信頼できる CA リストで、受信した証明書に署名した CA を確認します。	エラー
60056	（ハイブリッドサービス）証明書が無効なためアップグレードに失敗しました（[Hybrid services] Upgrade failed because certificate was not valid）	<*string*>	Expressway の信頼できる CA リストで、受信した証明書に署名した CA を確認します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60057	（ハイブリッドサービス）証明書名が一致しなかったためアップグレードに失敗しました（[Hybrid services] Upgrade failed because certificate name did not match）	<*string*>	<*string*>からの証明書の CN または SAN がホスト名と一致していることを確認します。	エラー
60058	（ハイブリッドサービス）CA 証明書が見つからなかったため接続に失敗しました（[Hybrid services] Connection failed because the CA certificate was not found）	<*string*> から証明書に署名したルート CA が Expressway の信頼できる CA リストにないため、Cisco Collaboration Cloud に安全に接続できません。	Expressway の信頼できる CA リストを更新し、受信した証明書に署名した CA を含めます。	エラー
60059	（ハイブリッドサービス）証明書名が一致しなかったため接続に失敗しました（[Hybrid services] Connection failed because the certificate name did not match）	<*string*> からの証明書に、ホスト名と一致する CN または SAN 属性がありませんでした。	リモート サーバからの証明書の CN または SAN がホスト名と一致していることを確認します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60060	（ハイブリッドサービス）証明書が検証されなかったため接続に失敗しました（[Hybrid services] Connection failed because the certificate was not validated）	Expressway が <*string*> からの証明書を検証できませんでした。これは、Expressway が CA を信頼していないか、または証明書が現在有効でないために発生する可能性があります。	Expressway <*string*> リストに、受信した証明書に署名した CA のルート証明書が含まれていることを確認します。CA 証明書が最新であり、失効していないことを確認します。<*string*> が設定されており、Expressway が同期していることを確認します。これらの潜在的原因を排除できる場合は、シスコにご連絡ください。送信したサーバ証明書が無効である可能性があります。	エラー
60061	（ハイブリッドサービス）ユーザの選択によりアップグレードが阻止されました（[Hybrid services] Upgrade prevented by user choice）	以前に、Cisco Collaboration Cloud によって現在アドバタイズされているコネクタのアップグレードが拒否されました。次のバージョンが利用可能になると、自動アップグレードが継続されます。アドバタイズされるバージョン：<*string*>	コネクタのバージョンを確認します。	アラート

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60062	（ハイブリッドサービス）コネクタ ディセーブル エラー（[Hybrid services] Connector disable error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60063	（ハイブリッドサービス）コネクタ イネーブル エラー（[Hybrid services] Connector enable error）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60064	（ハイブリッドサービス）コネクタが予期せず実行していません（[Hybrid services] Connector unexpectedly not running）	<*string*>	停止したコネクタを再起動します。そのコネクタが最近アップグレードされた場合は、以前のバージョンにロールバックしてください。エラーが解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー
60065	（ハイブリッドサービス）コネクタのバージョンの不一致（[Hybrid services] Connector version mismatch）	<*string*>	Cisco Collaboration Cloud 管理者にお問い合わせください。	エラー
60066	（ハイブリッドサービス）定期的な認証の更新に失敗しました（[Hybrid services] Routine authentication refresh failed）	Expressway は定期的に <*string*> を通じて認証を更新しますが、今回は成功しませんでした。Expressway は <*string*> 分以内に再試行します。	この問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60067	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity Error）	<*string*> にアクセスしようとしてエラーが発生しました。Expressway は約 <*string*> 秒後に再試行します。	<*string*> をチェックし、エラーが続く場合はネットワークの問題を確認してください。	エラー
60068	（ハイブリッドサービス）Cisco Collaboration Cloud からの無効な応答（[Hybrid services] Invalid responses from Cisco Collaboration Cloud）	<*string*> から無効なデータが受信されました。	Cisco Collaboration Cloud の予定されたアドレスがあるか確認します。	エラー
60069	（ハイブリッドサービス）サービス コネクタなし（[Hybrid services] No service connectors）	ハイブリッド サービスに登録されていますが、サービス コネクタがインストールされていません。管理コネクタがアクティブで、Cisco Collaboration Cloud への不要な接続を確立しています。	シスコ クラウド コラボレーション管理に移動し、組織が 1 つ以上のハイブリッド サービスを使用する権利があることを確認します。ハイブリッド サービスを使用していない場合は、この Expressway を <*string*> することを強く推奨します。	アラート
60070	（ハイブリッドサービス）HTTP 例外（[Hybrid services] HTTP exception）	<*string*> からの HTTP 応答を処理中に受信された例外：<*string*>	問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60071	（ハイブリッドサービス）キーエラー（[Hybrid services] Key error）	このシステムは、コネクタ ファイルのデータ エラーのために正しく登録できませんでした。関連するサービスは、正常に登録されているように見えても、期待どおりに機能しません。	再度登録を試みてください（最初に登録を解除する必要がある場合があります）。問題が解消されない場合は、Cisco Collaboration Cloud 管理者に連絡してください。	エラー
60072	（ハイブリッドサービス）サポートされていない Expressway バージョン（[Hybrid services] Unsupported Expressway version）	ご使用の Expressway のバージョンは、ハイブリッド サービスではサポートされなくなりました。ハイブリッド サービスを引き続き使用するには、新しいバージョンにアップグレードする必要があります。	cisco.com にある最新の Expressway バージョンにアップグレードしてください。	アラート

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60073	（ハイブリッドサービス）サポートされていない Expressway バージョン（[Hybrid services] Unsupported Expressway version）	Cisco Expressway の新バージョンがリリースされました。最新の機能を使用し、次の Expressway バージョンがリリースされたときにサポートされていないハイブリッドサービスの展開を避けるため、できるだけ早くこのバージョンにアップグレードすることをお勧めします。現在のバージョンは次の Expressway リリースまでサポートされます。	cisco.com にある最新の Expressway バージョンにアップグレードしてください。	アラート
60074	（ハイブリッドサービス）接続エラー（[Hybrid services] Connectivity error）	Cisco Collaboration Cloud に到達できません。	Teams Service のネットワーク要件を確認し、強調表示されているプロキシガイドラインに従います。	error

表 *14* : カレンダーコネクタ アラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60100	Microsoft Exchange サーバが到達不能（Microsoft Exchange Server unreachable）	Microsoft Exchange Server へのアクセス エラーが発生しました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Server とカレンダー コネクタ間のネットワークの接続性を確認します。Microsoft Exchange Server 上の負荷を確認します。	クリティカル
60101	Microsoft Exchange Server アクセスが拒否されました（Microsoft Exchange Server access denied）	Microsoft Exchange Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60102	Microsoft Exchange Server 証明書を検証できません（Microsoft Exchange Server certificate not validated）	Microsoft Exchange Server の証明書を検証できませんでした。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Server 証明書が有効なことを確認します。	クリティカル
60103	Microsoft Exchange Server のバージョンがサポートされていません（Microsoft Exchange Server version unsupported）	設定された Microsoft Exchange Server のバージョンがサポートされていません。詳細情報：<*string*>	Microsoft Exchange Server をサポートされているバージョンにアップグレードする必要があります。	クリティカル
60104	Microsoft Exchange Server が設定されていません（No Microsoft Exchange Server configured）	Microsoft Exchange Server の設定が構成されていないため、カレンダー コネクタが停止しました。	カレンダー コネクタに少なくとも 1 つの Microsoft Exchange Server を設定し、それを再度有効にします。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60110	Microsoft Exchange Autodiscover が到達不能（Microsoft Exchange Autodiscover unreachable）	ユーザの自動検出中に Microsoft Exchange Server へのアクセスでタイムアウトが発生しました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Autodiscover Server とカレンダー コネクタ間のネットワークの接続性を確認します。	クリティカル
60111	Microsoft Exchange Autodiscover のアクセスが拒否されました（Microsoft Exchange Autodiscover access denied）	ユーザの自動検出中に Microsoft Exchange Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60112	Microsoft Exchange Autodiscover 証明書を検証できません（Microsoft Exchange Autodiscover certificate not validated）	自動検出中に、Microsoft Exchange Server の証明書を検証できませんでした。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サーバ証明書が有効なことを確認します。	クリティカル
60113	リダイレクトされた Microsoft Exchange Autodiscovery URL が信頼されていません（Redirected Microsoft Exchange Autodiscovery URL not trusted）	リダイレクトされた Microsoft Exchange Autodiscovery URL が変更され、信頼されていません。詳細情報：<*string*>	Exchange サービス レコードを開き、再度レコードを保存します。新しいリダイレクション URL が信頼されることを確認します。	クリティカル
60120	Microsoft Exchange Autodiscover LDAP が到達不能（Microsoft Exchange Autodiscover LDAP unreachable）	自動検出中に Microsoft LDAP サーバへのアクセスでタイムアウトが発生しました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	Microsoft Exchange Autodiscover LDAP Server とカレンダー コネクタ間のネットワークの接続性を確認します。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60121	Microsoft Exchange Autodiscover LDAP のアクセスが拒否されました（Microsoft Exchange Autodiscover LDAP access denied）	自動検出中に Microsoft LDAP Server へのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：これには <*string*> が含まれます。最後の既知のエラー：<*string*>	サービス アカウントに有効なクレデンシャルと正しいアクセス許可があり、ロックされていないことを確認します。	クリティカル
60130	Microsoft Exchange Server のユーザ サブスクリプションの失敗（Microsoft Exchange Server user subscription failure）	;<*string*> ユーザが Microsoft Exchange Server に登録できませんでした（<string> users failed to subscribe to Microsoft Exchange Server(s).）詳細情報：ユーザには <*string*> が含まれています。	Microsoft Exchange Server がビジー状態でないこと、および Microsoft Exchange Server とカレンダー コネクタとの間のネットワークの接続性を確認します。	エラー
60131	SMTP アドレスにメールボックスがありません（SMTP address has no mailbox）	メールボックスが関連付けられていない複数の（<*string*>）SMTP アドレスが検出されました（Multiple (<string>) SMTP address(es) have been detected with no associated mailbox(es).）詳細情報：<*string*>	ターゲット メールボックスが完全に有効で、ターゲット サーバが正しいことを確認します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60132	サブスクリプションが動作していません（Subscription not operational）	カレンダー サービスが Microsoft Exchange Server から 1 人以上のユーザの通知を受信していません。これが対処されるまで、これらのユーザのカレンダー サービス要求および通知は処理されません。	Microsoft Exchange Server が正しく機能していることと、ネットワークに接続していることを確認します。この状態が続く場合は、カレンダー サービスの再起動を検討してください。	エラー
60140	会議通知の着信率が高すぎます（Meeting notification incoming rate too high）	<*string*> カレンダー サービス ユーザの着信会議通知率が高すぎます（The incoming meeting notification rate is too high for <string> Calendar Serviceuser(s).）詳細情報：ユーザには <*string*> が含まれています。	Microsoft Exchange Server でユーザのメールボックスを確認します。	エラー
60142	会議の処理時間が長すぎます（Meeting processing time too long）	カレンダー サービスの会議の処理時間が、少なくとも 1 人のユーザに対して 5 分のしきい値を超えています。	Microsoft Exchange Server とカレンダー サービスでユーザの通知率を確認します。	エラー
60150	Cisco Collaboration Cloud のモニタ サービスが到達不能（Cisco Collaboration Cloud Monitor Service unreachable）	現在必要なクラウド サービスに到達できません。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：<*string*>	インターネットへの接続を確認します。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60151	Cisco Collaboration Cloud のモニタ サービスへのアクセスが拒否されました（Cisco Collaboration Cloud Monitor Service access denied）	Cisco Collaboration Cloud サービスへのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：<*string*>	テクニカル サポートにお問い合わせください。	クリティカル
60152	Cisco Collaboration Cloud API サービスが到達不能（Cisco Collaboration Cloud API Service unreachable）	現在必要なクラウド サービスに到達できません。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：<*string*>	インターネットへの接続を確認します。	クリティカル
60153	Cisco Collaboration Cloud API サービスへのアクセスが拒否されました（Cisco Collaboration Cloud API Service access denied）	Cisco Collaboration Cloud サービスへのアクセスが拒否されました。これが解決されるまで、カレンダー サービス要求および通知は処理されません。詳細情報：<*string*>	テクニカル サポートにお問い合わせください。	クリティカル
60154	暗号化サービスからのキーの取得が失敗しました（Retrieving key from encryption service failed）	カレンダー コネクタが既存のキーを取得できなかったか、または暗号化サービスから新しいキーを生成する要求を失敗しました。詳細情報：暗号化サービスは <*string*> です。	暗号化サービスがオンになっていることを確認します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60155	Cisco Collaboration Cloud のモニタ メッセージ サービスが接続されていません（Cisco Collaboration Cloud Monitor message service not connected）	カレンダー コネクタが Cisco Collaboration Cloud のモニタ メッセージ サービスに接続できませんでした。詳細情報：クラウド サービス ルートは <*string*> です。	Cisco Collaboration Cloud のモニタ メッセージ サービスへのネットワーク接続を確認します。	クリティカル
60156	Cisco Collaboration Cloud API メッセージ サービスが接続されていません（Cisco Collaboration Cloud API message service not connected）	カレンダー コネクタが Cisco Collaboration Cloud API メッセージ サービスに接続できませんでした。詳細情報：クラウド サービス ルートは <*string*> です。	Cisco Collaboration Cloud API メッセージ サービスへのネットワーク接続を確認します。	クリティカル
60160	Cisco Collaboration Meeting Rooms（CMR）サービスに到達不能またはアクセスが拒否されました（Cisco Collaboration Meeting Rooms (CMR) service unreachable or access denied）	Cisco Collaboration Meeting Rooms（CMR）サービスに現在到達できないか、またはアクセスが拒否されました。これが解決されるまで、@webex 会議は処理されません。詳細情報：CMR サービスのサイト名には <*string*> が含まれています。	ネットワーク接続と CMR サービスに設定されているアカウント クレデンシャルを確認します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60161	WebEx ユーザ アカウントが使用できません（WebEx user account not available）	<*string*> Webex ユーザアカウントは利用できません。アカウントの問題が解決されるまで、これらのユーザの @webex 会議は処理されません。詳細情報：影響を受けるユーザには <*string*> が含まれています。	WebEx サービス アカウントとユーザ アカウントを確認します。ユーザに WebEx アカウントがあるか、アカウントがロックアウトされていないか、非アクティブ化されていないか、または Personal Room が無効になっているか確認します。	警告
60162	Cisco WebEx 管理者パスワードの有効期限が切れている、または無効です（Cisco WebEx administrator password has expired or invalid）	期限切れまたは無効な管理者パスワードが原因で Cisco WebEx サービスにアクセスできません。これが解決されるまで、影響を受けるサイトでの @webex 会議は処理されません。詳細情報：Webex サービス サイト名には <*string*> が含まれています。	影響を受ける WebEx サーバで、期限切れまたは無効な管理者パスワードを変更します。	エラー
60163	Cisco WebEx 管理者パスワードの有効期限が切れます（Cisco WebEx administrator password expiring）	<*string*> サイトの Cisco Webex 管理者パスワードの有効期限が間もなく切れます。詳細情報：管理者パスワードの期限が切れる Webex サービス サイトには <*string*> が含まれています。	影響を受ける WebEx サーバで、期限が切れる管理者パスワードを変更します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60164	Cisco WebEx 管理者アカウントがロックアウトされました（Cisco WebEx administrator account locked out）	管理者アカウントがロックアウトされているため、Cisco WebEx サービスにアクセスできません。これが解決されるまで、影響を受けるサイトでの @webex 会議は処理されません。詳細情報：Webex サービスサイト名には <*string*> が含まれています。	影響を受ける WebEx サーバで管理者アカウントをロック解除します。	エラー
60170	管理コネクタが実行されていません（Management Connector not running）	管理コネクタが実行されていないため、カレンダー コネクタが動作していません。	**[アプリケーション（Applications）]** > **[クラウド拡張（Cloud Extensions）]** > **[コネクタ管理（Connector Management）]** に移動して、管理コネクタを開始します。	エラー
60171	管理コネクタが動作していません（Management Connector not operational）	管理コネクタが動作していないため、カレンダー コネクタが動作していません。	管理コネクタのステータスを確認し、必要に応じて再起動します。	エラー
60190	カレンダー コネクタが動作していません（Calendar Connector not operational）	1 つ以上のクラウド サービスおよび/またはオンプレミス サービスが動作していないため、カレンダー コネクタが動作していません。	詳細については、カレンダー コネクタのステータスを確認してください。	クリティカル

表 *15* : コールコネクタアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60300	ユーザにはディレクトリ番号が設定されていません。（The user is not configured with any directory numbers.）	ユーザにディレクトリ番号が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM でユーザに関連付けられているデバイスに少なくとも 1 つの回線を追加します。	警告
60301	ユーザのコントロール リストに有効なデバイスがありません。（The user has no valid devices in the control list.）	ユーザのコントロール リストに有効なデバイスがありません（The user has no valid devices in the control list）：user[<*string*>]:<*string*>	回線が少なくとも 1 つある有効なデバイスを少なくとも 1 つ Unified CM のユーザに関連付けます。	警告
60302	ユーザにディレクトリ URI が設定されていません。（The user is not configured with a directory URI.）	ユーザにディレクトリ URI が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM のユーザのアカウント設定で、ディレクトリ URI の値を入力します。	警告
60303	この電子メールアドレスを持つユーザが見つかりませんでした（Could not find a user with this email address.）	この電子メールアドレスを持つユーザを見つけることができませんでした（Could not find a user with this email address）：user[<*string*>]:<*string*>	Unified CM でユーザの電子メールアドレスを入力します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60304	電子メールとディレクトリ URI の不一致（Email mismatch with directory URI）	ユーザの電子メールがディレクトリ URI と一致しません（The user's email does not match the directory URI）：user[<*string*>]: <*string*>	ユーザの電子メールとディレクトリ URI が Unified CM で同じであることを確認します。	警告
60305	ユーザのプライマリ ディレクトリ URI が、プライマリ回線用に設定されたディレクトリ URI と一致しません（The user's primary directory URI does not match the directory URI configured for the primary line.）	ユーザのプライマリ ディレクトリ URI が、プライマリ回線用に設定されたディレクトリ URI と一致しません（The user's primary directory URI does not match the directory URI configured for the primary line）：user[<*string*>]: <*string*>	Unified CM で、関連するデバイス上のユーザのディレクトリ URI と回線 URI が同一であることを確認します。	警告
60306	ユーザが有効な CTI リモート デバイスで構成されていません（The user is not configured with a valid CTI remote device.）	ユーザが有効な CTI リモート デバイスで構成されていません（The user is not configured with a valid CTI remote device）：user[<*string*>]: <*string*>	Unified CM で CTI リモート デバイスを設定し、ユーザのコントロール リストに追加します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60307	Webex SIP アドレスを Webex クラウドにルーティングできません（Webex SIP address cannot be routed to the Webex cloud.）	ユーザの Webex SIP アドレスを Webex クラウドにルーティングできません（The user's Webex SIP address cannot be routed to the Webex cloud）） : user[<*string*>]: <*string*>	Unified CM で再ルーティング コーリング サーチ スペースと、Webex SIP アドレス パターン用に設定されたパーティションを確認します。	エラー
60308	すでに使用中の Webex SIP アドレスです（Webex SIP address is already in use.）	ユーザの Webex SIP アドレスは別のユーザに割り当てられています（The User's Webex SIP address is assigned to another user） : user[<*string*>]: <*string*>	Cisco Unified CM Administration で、ユーザのリモート接続先がデバイスですでに使用されているかどうかを確認してください。	エラー
60309	ユーザのリモート接続先が削除されませんでした（The user's remote destination was not removed.）	ユーザがコール サービス接続で非アクティブ化されたときに、リモート接続先が削除されませんでした（When the user is deactivated for Call Service Connect, the remote destination was not removed. ） : user[<*string*>]: <*string*>	Cisco Unified CM Administration で、ユーザのリモート接続先がデバイスですでに使用されているかどうかを確認してください。Unified CM ユーザの CTI リモート デバイスからリモート接続先を削除します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60310	Unified CM でユーザの Webex SIP アドレスを追加できません（Unable to add the user's Webex Teams SIP address in Unified CM.）	Unified CM でユーザの Webex SIP アドレスを追加できません（Unable to add the user's Webex SIP address in Unified CM）：user[<*string*>]:<*string*>	Cisco Unified CM Administration で、手動で作成済みのリモート接続先が存在する場合はそれを削除します。これにより、コール コネクタによって自動的にリモート接続先が再作成されます。	エラー
60311	ユーザにプライマリ ディレクトリ番号が設定されていません。（The user is not configured with a primary directory number.）	ユーザにプライマリ ディレクトリ番号が設定されていません（The user is not configured with a primary directory number）：user[<*string*>]:<*string*>	Unified CM でユーザのプライマリ ディレクトリ番号を設定します。	警告
60315	自動 Spark リモート デバイスが省略された名前で作成されました（Automatic Spark Remote Device created with truncated name）	コールサービス接続のアクティベーション中に、自動 Spark リモート デバイス名が短縮されました。- ユーザ [<*string*>]<*string*> に nam <*string*>のデバイスがあります。	この問題を避けるには、ユーザ ID を 15 文字以下にする必要があります。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60316	Spark リモート デバイスを削除できません（Unable to delete Spark Remote Device）	コール コネクタは、コール サービス接続が非アクティブ化された後、Spark リモート デバイスを削除できません（Call connector cannot delete the Spark remote device after Call Service Connect was deactivated）：user[<*string*>]: <*string*>	Unified CM でエラー メッセージを確認します。	警告
60317	コール コネクタは、Unified CM に CTI リモートデバイスを作成できません（Call connector is unable to create a CTI Remote Device in Unified CM.）	コール コネクタは、Unified CM に CTI リモートデバイスを作成できません（Call connector is unable to create a CTI Remote Device in Unified CM）：user[<*string*>]: <*string*>	競合する可能性のあるデバイス名を確認します。	警告
60318	コール コネクタが CTI リモート デバイスを作成するには、ユーザはモビリティを有効にする必要があります（Users must have mobility enabled for call connector to create a CTI remote device.）	ユーザがモビリティを有効にしなければ、コールコネクタは Webex のリモート デバイスを作成できません（Users must have mobility enabled for call connector to create a Remote Device for Webex Teams）：user[<*string*>]: <*string*>	Unified CM ユーザがモビリティに対し有効になっているかどうか確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60319	Unified CM AXL への接続が失われました（Connectivity to Unified CM AXL Service lost）	Unified CM AXL サービスへの接続が失われました（Connectivity to Unified CM AXL Service lost）：Unified CM [<*string*>]	AXL サービスが Unified CM 上で動作しているかどうかを確認し、ネットワークの問題を解決します。	error
60320	Unified CM CTIManager サービスに接続できません（Cannot connect to Unified CM CTIManager Service.）	Unified CM CTIManager サービスに接続できません（Cannot connect to Unified CM CTIManager Service）：Unified CM [<*string*>]	CTIManager サービスが Unified CM 上で動作しているかどうかを確認し、ネットワークの問題を解決します。	エラー
60321	証明書検証が失敗しました（Certificate verification failed）	Webex クラウドから提供された証明書を検証できなかったため、コール コネクタが停止しました（Call Connector stopped as it could not verify the certificate provided by the Webex cloud.）	Expressway 登録プロセスの一環として証明書をダウンロードし、Expressway-C を登録します。それでもエラーが続く場合は、Expressway-C 信頼ストア内の Webex 証明書を更新します。	エラー
60322	完全修飾ドメイン名が無効です（Fully Qualified Domain Name is not valid）	完全修飾ドメイン名が空です（Fully Qualified Domain Name is Empty）：user[<*string*>]: <*string*>	Unified CM エンタープライズ パラメータに完全修飾ドメイン名を追加します。手順については、マニュアルを参照してください。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60323	完全修飾ドメイン名が無効です（Fully Qualified Domain Name is not valid）	完全修飾ドメイン名にワイルドカードが含まれています（Fully Qualified Domain Name contains wild card）：user[<*string*>]: <*string*>	Unified CM エンタープライズ パラメータにワイルドカードを含まない新しい完全修飾ドメイン名を追加します。	警告
60324	Unified CM AXL サーバに到達できません（Unable to reach the Unified CM AXL server.）	Unified CM AXL サーバに到達できません（Unable to reach the Unified CM AXL server）：server[<*string*>]	コール コネクタと Unified CM 間のネットワーク接続を確認します。	エラー
60325	Unified CM AXL サーバで認証できません（Unable to authenticate with Unified CM AXL server）	Unified CM AXL サーバで認証できません：[<*string*>]	コール コネクタの設定時に指定した Unified CM ユーザ クレデンシャルを確認します。	エラー
60326	Unified CM AXL 通信用に設定されたユーザが承認されていません（User configured for Unified CM AXL communication is not authorized）	Unified CM AXL 通信用に設定されたユーザが承認されていません（User configured for Unified CM AXL communication is not authorized）：server [<*string*>]	コール コネクタの UCM 設定で設定されているユーザのアクセス ロールを確認します。	エラー
60327	Unified CM が設定されていません（No Unified CM Configured）	Unified CM がコール コネクタに設定されていません。	コール コネクタに Unified CM を設定します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60328	ユーザが複数の Unified CM クラスタに対して設定されています。（The user is configured for more than one Unified CM cluster.）	ユーザが複数の Unified CM クラスタに対して設定されています：user[<*string*>]: <*string*>	このコール コネクタに設定されているすべての Unified CM でユーザのホーム クラスタ設定を確認します。	警告
60329	コール コネクタが無効な Webex SIP アドレスを受信しました。（Call connector received an invalid Webex SIP Address.）	無効な Spark SIP アドレス：user[<*string*>]: <*string*> の場合	ユーザおよびデバイス設定を確認します。マニュアルに従って再設定を行い、必要に応じて有効な Webex SIP アドレスを再設定します。	エラー
60330	ユーザが複数の CTI リモート デバイスで設定されています（The user is configured with more than one CTI remote device.）	ユーザが複数の CTI リモート デバイスで設定されています（The user is configured with more than one CTI remote device）：user[<*string*>]: <*string*>	Unified CM でユーザのコントロール リストから余分なデバイスを削除します。	警告
60331	CTI リモート デバイスには設定されたディレクトリ番号はありません。（The CTI remote device has no configured directory numbers.）	CTI リモート デバイスにディレクトリ番号が設定されていません（The CTI remote device has no configured directory numbers）：user[<*string*>]: <*string*>	Unified CM で、ユーザに関連付けられた CTI リモート デバイスに少なくとも 1 つの回線を追加します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60332	Unified CM CTIManager で、リモート接続先を更新する要求がタイムアウトしました。（In Unified CM CTIManager, a request timed out to update the remote destination.）	Unified CM CTIManager で、リモート接続先の更新要求がタイムアウトしました（In Unified CM CTIManager, a request timed out to update the remote destination）：user[<*string*>]: <*string*>	Unified CM CTIManager サービスが起動して実行していることを確認します。	警告
60333	Unified CM CTIManager に接続できません（Unable to connect to Unified CM CTIManager）	Unified CM CTIManager に接続できません。	コール コネクタと Unified CM 間のネットワーク接続を確認します。	エラー
60334	Unified CM CTIManager に設定されたユーザを認証できません（Unable to authenticate user configured for Unified CM CTIManager）	Unified CM CTIManager に設定されたユーザを認証できません。	コール コネクタの Unified CM 設定でユーザ クレデンシャルを確認します。	エラー
60335	Unified CM のデバイス所有権の競合（Conflict in Device Ownership on Unified CM.）	Unified CM がデバイスの所有者との競合を示しています（Unified CM shows a conflict with the owner of the device）：user[<*string*>]: <*string*>	Unified CM で設定を確認します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60336	ユーザ用に作成しようとしたCTIリモート デバイスと同じ名前のデバイスが存在します（A device exists with the same name as the CTI remote device tried to create for the user.）	作成しようとしたCTIリモートデバイスと同じ名前のデバイスが存在します（A device exists with the same name as the CTI remote device tried to create）：user[<*string*>]:<*string*>	Unified CMでデバイス名と設定を確認します。	警告
60337	CTIリモートデバイスがユーザ用に正常に作成されましたが、コールイベントを受信するデバイス サブスクリプションが失敗しました。（CTI remote device successfully created for the user, but the device subscription to receive call events failed.）	CTIリモートデバイスがユーザ用に正常に作成されましたが、コールイベントを受信するデバイス サブスクリプションが失敗しました（CTI remote device successfully created for the user, but the device subscription to receive call events failed）：user[<*string*>]:<*string*> の場合	Unified CMで設定を確認し、再試行します。	警告
60338	Unified CMの無効なリモート接続先（Invalid remote destination on Unified CM.）	Unified CMの無効なリモート接続先（Invalid remote destination on Unified CM）：user[<*string*>]:<*string*> の場合	マニュアルのユーザおよびリモートデバイスの設定手順に従って、有効なWebex SIPアドレスを作成します。	警告

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60339	このユーザのリモート接続先の制限を超えています（The user exceeds the remote destination limit.）	Webex SIP アドレスを作成できません。Cisco Unified CM でのこのユーザのリモート接続先の制限を超えています（Unable to create a Webex SIP address. The user exceeds the remote destination limit in Cisco Unified CM.）	未使用のリモート接続先を削除するか、制限を増やします。	エラー
60340	ユーザにホームクラスタが設定されていません。（The user is not configured with a home cluster.）	このユーザのホーム クラスタは設定されていません（The user is not configured with a home cluster）：user[<*string*>]: <*string*>	Unified CM でこのユーザのホーム クラスタを設定します。	警告
60341	コール コネクタの構成が無効です（Call connector invalid configuration）	無効な構成の理由（Invalid Configuration reason）=[<*string*>]	設定エラーを修正してから、コール コネクタを再起動します。	エラー
60342	コール コネクタのバージョンがWebex クラウドと一致しません（Call connector version mismatch with the Webex cloud）	[<*string*>] 状態の無効なメッセージを受信しました。Webex クラウドとバージョンが一致していない可能性があります（Invalid message received in state [<string>], potential version mismatch with the Webex cloud）	admin.webex.com にアクセスし、[サービス（Services）]>[ハイブリッド コール（Hybrid Call）]>[すべて表示（View all）] に移動してリソースを開き、最新のコール コネクタ ソフトウェアにアップグレードします。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60343	Webex SIP アドレスが 48 文字の制限を超えています（Webex SIP Address exceeds the 48 character limit.）	ユーザの Webex SIP アドレスを追加できません（Unable to add Webex SIP address for a user.）Unified CM は、48 文字を超えるリモート接続先をサポートしていません（Unable to add Webex SIP for a user. Unified CM does not support remote destinations that are longer than 48 characters.）	Webex SIP アドレスが 48 文字の制限を超えないようにデバイス名を変更します。	エラー
60344	ユーザのディレクトリ URI が組織の検証済みドメイン リストにありません（User's directory URI is not in the organization's verified domain list）	ユーザのディレクトリ URI が組織の検証済みドメイン リストにありません（User's directory URI is not in the organization's verified domain list）：user[<*string*>]: <*string*> にドメイン リスト = <*string*> があります。	ユーザのディレクトリ URI と、このユーザの検証済みドメインのリストを確認します。	警告
60345	Unified CM クラスタのデータキャッシュの構築に失敗しました（Failed to Build Unified CM Cluster Data-Cache）	Unified CM クラスタのデータキャッシュの構築に失敗しました（Failed to Build Unified CM Cluster Data-Cache）：server[<*string*>]	AXL サービスが Unified CM クラスタ ノード上で動作しているかどうかを確認し、ネットワークの問題を解決します。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60346	Cisco Collaboration Cloud サービスとの認証の失敗（Authentication Failure with Cisco Collaboration Cloud Services.）	Expressway で利用できる認証クレデンシャルが無効です。	Expressway に移動し、**[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[コネクタ管理（Connector Management）]** でクラウドに再登録します。	エラー
60347	Cisco Collaboration Cloud サービスとの承認の失敗（Authorization Failure with Cisco Collaboration Cloud Services.）	この Expressway が Cisco Collaboration Cloud サービスにアクセスするためのロールまたはアクセス範囲が無効です。	Expressway に移動し、**[アプリケーション（Applications）]** > **[ハイブリッドサービス（Hybrid Services）]** > **[コネクタ管理（Connector Management）]** でクラウドに再登録します。	エラー
60348	Cisco Collaboration Cloud からの接続がダウンしています（Connection from the Cisco Collaboration Cloud is down.）	Cisco Collaboration Cloud からの接続がダウンしています。	ネットワーク DNS またはプロキシ設定を確認してから、再度試してください。	エラー
60349	Cisco Collaboration Cloud への接続がダウンしています（Connection to the Cisco Collaboration Cloud is down.）	Cisco Collaboration Cloud への接続がダウンしています。	ネットワーク DNS またはプロキシ設定を確認してから、再度試してください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60350	組織のハイブリッド ボイスメールを有効にできません（Cannot enable hybrid voicemail for your organization.）	組織のハイブリッド ボイスメールを有効にできません。	このエラーが解消されない場合は、試用チームに連絡するか、または Cisco Spark アプリを通じてフィードバックを送信してサポートにお問い合わせください。	警告
60351	コール コネクタが無効なハイブリッド ボイスメール設定を検出しました（Call connector detected an invalid hybrid voicemail configuration.）	コール コネクタが無効なハイブリッド ボイスメール設定を検出しました。	ハイブリッド ボイスメールの展開手順を確認します。このエラーが解消されない場合は、試用チームに連絡するか、または Cisco Spark アプリを通じてフィードバックを送信してサポートにお問い合わせください。	エラー
60352	UCM にこのディレクトリ URI を持つディレクトリ番号が存在しません（No Directory Number exists in UCM with this directory URI）	UCM にこのディレクトリ URI を持つディレクトリ番号が存在しません。	このディレクトリ URI を使用して UCM にディレクトリ番号を設定します。	エラー
60353	Unified CM で AXL 変更通知が開始されません（AXL Change Notification is not started at Unified CM.）	Unified CM で AXL 変更通知が開始されません（AXL Change Notification is not started at Unified CM）：server[<*string*>]	Unified CM のエンタープライズ パラメータで AXL 変更通知を有効にします。	エラー

表 *16* : 重要なイベントアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
90001	緊急コール（Emergency call）	緊急コールは、ゾーン（ゾーン名）、送信元 IP（*IP* アドレス）から（*user@example.com*）によって実行されています。	NA	emergency

表 *17* : テレメトリーアラーム

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60800	CollectD サービスダウン（CollectD Service Down）	Core Telemetry Service が動作しない	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	クリティカル
60801	クラウドに接続された UC 接続のダウン（Cloud-Connected UC Connection Down）	クラウドに接続されている UC への接続が切断されている	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。問題が解決しない場合は、シスコのサポート担当者に連絡してください。	クリティカル

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60802	設定エラー（Configuration Error）	設定の更新または設定の取得の失敗	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。また、クラスタまたはノードが認証され、適切にオンボードされているかも確認します。それでも問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー
60803	認証エラー（Authentication Error）	1 つ以上のリモートコネクタ接続またはトランザクション処理で認証に失敗しました	テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。また、クラスタまたはノードが承認され、適切にオンボードされ、必要な証明書がインストールされているかも確認します。それでも問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60804	CA 証明書の読み取りエラー（CA Certificate Read Error）	CA 証明書の読み取りまたは組み込みに失敗しました	• また、クラスタまたはノードが承認され、適切にオンボードされ、必要な証明書がインストールされていることを確認します。 • 必要な証明書を再インストールします。 • テレメトリ―コネクタを無効にして有効にし、ネットワークの問題を確認します。 問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー

ID	タイトル	説明（Description）	ソリューション	シビラティ（重大度）
60805	無効な証明書エラー（Invalid Certificate Error）	無効な証明書がロードされている	• また、クラスタまたはノードが承認され、適切にオンボードされ、有効な証明書がインストールされていることを確認します。 • 正しい証明書および有効な証明書を再インストールします。 • テレメトリ—コネクタを無効にして有効にし、ネットワークの問題を確認します。 問題が解決しない場合は、シスコのサポート担当者に連絡してください。	エラー

コマンド リファレンス — xConfiguration

設定の個々の項目を設定および変更するには、`xConfiguration` グループのコマンドを使用します。各コマンドは、メインの要素と、その後に続く 1 つ以上のサブ要素から構成されます。

既存の設定に関する情報を取得するには、次のように入力します。

- `xConfiguration`：現在のすべての設定を返す場合。
- `xConfiguration <element>`：指定した要素とそのすべてのサブ要素を返す場合。
- そのサブ要素の設定を返す `xConfiguration <element> <subelement>`

各 xConfiguration コマンドの使用に関する情報を取得するには、次のように入力します。

- xConfiguration ? xConfiguration：コマンドで使用可能なすべての要素のリストを返す場合。
- xConfiguration ??xConfiguration ：コマンドで使用可能なすべての要素のリストと、各要素の値空間、説明、およびデフォルト値を返す場合。
- xConfiguration <element> ?：使用可能なすべてのサブ要素とそれらの値空間、説明、およびデフォルト値を返す場合。
- xConfiguration <element> <sub-element> ?：使用可能なすべてのサブ要素とそれらの値空間、説明、およびデフォルト値を返す場合

設定項目を設定するには、コマンドを次のように入力します。次の表記法を使用して、各コマンドに有効な値を山カッコ内に示し、その後に各コマンドを示します。

表 *18 : CLI* リファレンスで使用されるデータ表記規則

書式	意味
<0..63>	整数値が必要であることを示します。数値は最小値と最大値を示しています。この例では、0 ～ 63 の範囲内の値にする必要があります。
<S: 7,15>	**S** は引用符で囲まれた文字列値が必要であることを示します。数値は文字列の最小文字数と最大文字数を示します。この例では、文字列の長さを 7 ～ 15 文字にする必要があります。
<Off/Direct/Indirect>	コマンドの有効な一連の値を示します。値は引用符で囲まないでください。
[1..50]	角カッコはこの特定の項目を複数設定できることを示します。各項目には示された範囲内のインデックスが割り当てられます。 たとえば、IP Route [1..50] Address <S: 0,39> は最大 50 の IP ルートを指定でき、各ルートには最大 39 文字の長さのアドレスが必要であることを意味します。

xConfiguration コマンド

次の表に、使用可能なすべての **xConfiguration** コマンドを示します。

表 *19 : xConfiguration CLI* リファレンス

xConfiguration Administration DeviceProvisioning: <On/Off> Expressway Web ユーザインターフェイスで **[システム（System）] > [TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにアクセスさせるかどうかを指定します。アクセス可能な場合、このページから、Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）とユーザ、デバイス、FindMe、電話帳のプロビジョニング サービスに接続できます。デフォルト：Off *On*：**[システム（System）] > [TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにアクセス可能になり、この Expressway のプロビジョニングサービスを設定できます。 *Off*：**[システム（System）] > [TMS プロビジョニング拡張サービス（TMS Provisioning Extension services）]** ページにはアクセスできません。 例：`xConfiguration Administration DeviceProvisioning: On`
xConfiguration Administration HTTP Mode: <On/Off> HTTP コールを HTTPS ポートにリダイレクトするかどうかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 *On*：コールは HTTPS にリダイレクトされます。 *Off*：HTTP アクセスは使用できません。 例：`xConfiguration Administration HTTP Mode: On`
xConfiguration Administration HTTPS Mode: <On/Off> Web インターフェイス経由で Expressway にアクセスできるかどうかを決定します。Web インターフェイスと TMS アクセスの両方を有効にするには、これを On にする必要があります。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 例：`xConfiguration Administration HTTPS Mode: On`
xConfiguration Administration LCDPanel Mode: <On/Off> Expressway の前面の LCD パネルでシステムを識別するかどうかを制御します。デフォルトは On です。 *On*：システム名とアクティブな IP アドレスのうち最初のアドレスが表示されます。 *Off*：LCD パネルにはシステムに関する識別情報は表示されません。 例：`xConfiguration Administration LCDPanel Mode: On`
xConfiguration Administration SSH Mode: <On/Off> SSH と SCP を使用して Expressway にアクセスできるかどうかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトは On です。 例：`xConfiguration Administration SSH Mode: On`

xConfiguration Alarm Notification Email Custom Alarm ID: <String>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。カスタマイズまたは無効化された通知のアラーム ID。

xConfiguration Alarm Notification Email Custom Disable Notify: <Off>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。

xConfiguration Alarm Notification Email Custom Email: <String>

1 つ以上のカスタマイズされたアラーム通知が設定されている場合。選択したアラーム通知の送信に使用される電子メール ID（最大長 254）。

xConfiguration Alarm Notification Email Destination Alert: <S: 0, 254>

厳しい属性 「Alert」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Alert: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Critical: <S: 0, 254>

厳しい属性 「Critical」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Alert: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Debug: <S: 0, 254>

厳しい属性 「Debug」 を使用するアラームの電子メール通知先。

例：`Configuration Alarm Notification Email Destination Debug: 「uctech@example.com」`

xConfiguration Alarm Notification Email Destination Emergency: <S: 0, 254>

厳しい属性 「Emergency」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Emergency: 「ert@example.com」`

xConfiguration Alarm Notification Email Destination Error: <S: 0, 254>

厳しい属性 「Error」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Error: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Info: <S: 0, 254>

厳しい属性 「Info」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Info: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Notice: <S: 0, 254>

厳しい属性 「Notice」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Notice: 「ucadmin@example.com」`

xConfiguration Alarm Notification Email Destination Warning: <S: 0, 254>

厳しい属性 「Warning」 を使用するアラームの電子メール通知先。

例：`xConfiguration Alarm Notification Email Destination Warning: 「ucadmin@example.com」`

xConfiguration Alarm Notification SMTP Mode: <On/Off>

アラームベースの電子メール通知を使用するかどうかを決定します。デフォルトはオフです。

例：`xConfiguration Alarm Notification SMTP Mode: On`

xConfiguration Alarm Notification SMTP Server Email: <S: 0, 254>

アラームベースの電子メール通知が設定されている通知先アドレスに送信される送信元電子メール。

例：`Alarm Notification SMTP Server Email: 「ucadmin@example.com」`

xConfiguration Alarm Notification SMTP Server Host: <S: 0, 128>

アラームベースの電子メール通知の送信に使用するSMTPサーバのIPアドレスまたはFQDN。

例：`xConfiguration Alarm Notification SMTP Server Host: 「email.example.com」`

xConfiguration Alarm Notification SMTP Server Password: <Password>

アラームベースの電子メール通知の送信に使用される SMTP サーバのパスワード。

例：`xConfiguration Alarm Notification SMTP Server Password: 「{cipher}$NNxx1xxx-xxxx-xxxx-xxxn-fnxnxNNNxxxN$1$xX+xnXnnXxnnxxnnnXXXnxnXXxnxXxxx/XXxnxnxxxx=」`

xConfiguration アラーム通知 SMTP サーバポート：

アラームベースの電子メール通知の送信に使用する SMTP サーバのポート番号。デフォルトは 587 です。

例：`xConfiguration Alarm Notification SMTP Server Port: 587`

xConfiguration Alternates Cluster Name: <S: 0,128>

この Expressway クラスタ宛の SRV レコードに使用する完全修飾ドメイン名。たとえば、「「cluster1.example.com」」など。名前には、文字、数字、ハイフン、および下線のみ使用できます。

警告：このExpresswayでユーザアカウントを設定した後にクラスタ名を変更した場合は、その新しいクラスタ名を使用してユーザアカウントを再設定する必要がある場合があります。

例：`Configuration Alternates Cluster Name: 「Regional」`

xConfiguration Alternates ConfigurationPrimary: <1..6>

他のすべてのピアに設定を複製するプライマリがこのクラスタ内のどのピアかを指定します。クラスタは、ローカル Expressway を含む最大 6 つのピアで構成されます。

例：`xConfiguration Alternates ConfigurationPrimary: 1`

xConfiguration Alternates Peer [1..6] Address: <S: 0, 128>

この Expressway が所属するクラスタ内の 1 つのピアのアドレスを指定します。クラスタは、ローカル Expressway を含む最大 6 つのピアで構成されます。シスコはされたFQDNを使用することをお勧めします。これは、IPアドレスにすることができます。

例：`xConfigurationの 1つのピアアドレス:「「cluster1peer3.example.com」」`

xConfiguration ApacheModReqTimeOut

1 つの短縮コマンドを使用して、要求のタイムアウトに使用可能なすべてのプロパティを設定できます。

例：`xConfiguration ApacheModReqTimeout Apachehead:20 Apachebody:20 Status:On`

xConfiguration ApacheModReqTimeOut Apachebody: <0..120>

Apache Web サーバが要求の本文を待機する秒数を変更します。タイムアウトの期限が切れる前に要求の本文全体を受信しなかった場合、Apache はタイムアウト エラーを返します。デフォルト：20。

例：`xConfiguration ApacheModReqTimeout Apachebody:20`

xConfiguration ApacheModReqTimeOut Apacheheader: <0..120>

Apache Web サーバが要求のヘッダーを待機する秒数を変更します。タイムアウトの期限が切れる前に要求のヘッダー全体を受信しなかった場合、Apacheはタイムアウトエラーを返します。デフォルト：20。

例：`xConfiguration ApacheModReqTimeout Apacheheader:20`

xConfiguration ApacheModReqTimeOut Status: <On/Off>

カスタムの Apache 要求のタイムアウトを切り替えます。切り替えを省略した場合は、タイムアウトのステータスが表示されます。

On：デフォルトの Apache 要求タイムアウトよりも `Apachebody` と `Apacheheader` の設定（またはデフォルト）が優先されます。

Off：`Apachebody` と `Apacheheader` は影響を与えません。Apache 要求のタイムアウトはデフォルトで 300 秒に設定されています。

例：`xConfiguration ApacheModReqTimeout Status:On`

xConfiguration Applications ConferenceFactory Alias: <S:0,60>

Multiway 機能がアクティブになったときにエンドポイントがダイヤルするエイリアス。これは、Multiway 機能の開始に使用できるすべてのエンドポイントに事前に設定する必要があります。

例：`xConfiguration Applications ConferenceFactory Alias: 「multiway@example.com」`

xConfiguration Applications ConferenceFactory Mode: <On/Off>

Mode オプションを使用して Conference Factory アプリケーションを有効または無効にできます。デフォルト：Off

例：`xConfiguration Applications ConferenceFactory Mode: Off`

xConfiguration Applications ConferenceFactory Range End: <1..65535>

会議エイリアスの生成に使用するテンプレート内の %% を置き換える範囲の最後の数値。デフォルト：65535。

例：`xConfiguration Applications ConferenceFactory Range End: 30000`

xConfiguration Applications ConferenceFactory Range Start: <1..65535>

会議エイリアスの生成に使用するテンプレート内の %% を置き換える範囲の最初の数値。デフォルト：65535。

例：`xConfiguration Applications ConferenceFactory Range Start: 10000`

xConfiguration Applications ConferenceFactory Template: <S:0,60>

Multiway 会議を MCU に作成するためにダイヤルするよう Expressway がエンドポイントに通知するエイリアス。このエイリアスは、完全修飾 SIP エイリアスとして MCU にルーティングする必要があります。

例：`xConfiguration Applications ConferenceFactory Template: 「563%%@example.com」`

xConfiguration Applications External Status [1..10] Filename: <S:0,255>

外部アプリケーション用にアタッチするステータスが含まれている XML ファイル。

例：`xConfiguration Applications External Status 1 Filename: 「foo.xml」`

xConfiguration Applications External Status [1..10] Name: <S:0,64>

ステータスが参照される外部アプリケーションの記述名。

例：`xConfiguration Applications External Status 1 Name: 「foo」`

xConfiguration Authentication ADS ADDomain: <S: 0,255>

Expressway が AD ドメインに参加するときに使用する Kerberos レルム。注：このフィールドは大文字と小文字を区別します。

例：`xConfiguration Authentication ADS ADDomain: 「CORPORATION.INT」`

xConfiguration Authentication ADS Clockskew: <1..65535>

Kerberos メッセージが無効だと見なされる前に、Expressway と KDC 間で許可される最大クロック スキュー（秒単位）。デフォルトは 300 です。

例：`xConfiguration Authentication ADS Clockskew: 300`

xConfiguration Authentication ADS CipherSuite: <S:1,2048>

Expressway が AD ドメインに参加するために TLS 暗号化 LDAP 接続を実行するときに使用する暗号スイートを指定します。このコマンドは「OpenSSL 暗号」形式の文字列を受け入れます（https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

例：`xConfiguration Authentication ADS CipherSuite: 「HIGH:MEDIUM:!ADH:!aNULL:!eNULL:-AES128-SHA256:@STRENGTH」`

xConfiguration Authentication ADS DC [1..5] Address: <S: 0,39>

Expressway が AD ドメインに参加するときに使用できるドメイン コントローラのアドレス。特定の AD を指定しなかった場合は、AD の検出に DNS SRV クエリが使用されます。

例：`xConfiguration Authentication ADS DC 1 Address: 「192.168.0.0」`

xConfiguration Authentication ADS Encryption: <Off/TLS>

ADS サーバへの LDAP 接続に使用する暗号化を設定します。

（注） 無効な暗号を削除しましたが、保持された 1 つの暗号（eTYPE-アーク FOUR-HMAC-MD5）を削除して、後方互換性を確保しました。

デフォルトは TLS です。

Off：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Authentication ADS Encryption: TLS`

xConfiguration Authentication ADS KDC [1..5] Address: <S: 0,39>

AD ドメインへ接続するときに使用する Kerberos 配布センター（KDC）のアドレス。特定の KDC を指定しなかった場合は、KDC の検出に DNS SRV クエリが使用されます。

例：`xConfiguration Authentication ADS KDC 1 Address: 「192.168.0.0」`

xConfiguration Authentication ADS KDC [1..5] Port: <1..65534>

Expressway が AD ドメインに参加するときに使用できる KDC のポートを指定します。デフォルト：88。

例：`xConfiguration Authentication ADS KDC 1 Port: 88`

xConfiguration Authentication ADS MachineName: <S: 0..15>

Expressway が AD ドメインに参加するときに使用するデフォルトの NETBIOS マシン名を上書きします。

例：`xConfiguration Authentication ADS MachineName: 「short_name」`

xConfiguration Authentication ADS MachinePassword Refresh: <On/Off>

AD ドメインに参加するときに、この Samba クライアントがマシンのパスワードを 7 日おきに更新する必要があるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication ADS MachinePassword Refresh: On`

xConfiguration Authentication ADS Mode: <On/Off>

Expressway が AD との関係の形成を試行するかどうかを示します。デフォルト：Off

例：`xConfiguration Authentication ADS Mode: On`

xConfiguration Authentication ADS SPNEGO: <Enabled/Disabled>

クライアント（Expressway）がサーバ（AD ドメイン コントローラ）で認証するときに SPNEGO（Simple and Protected GSSAPI Negotiation Mechanism）を使用するかどうかを示します。デフォルト：有効.

例：`xConfiguration Authentication ADS SPNEGO: Enabled`

xConfiguration Authentication ADS SecureChannel: <Auto/Enabled/Disabled>

Expressway から AD ドメイン コントローラに送信されたデータをセキュア チャネル経由で送信するかどうかを示します。デフォルト：[Auto]

例：`xConfiguration Authentication ADS SecureChannel: Auto`

xConfiguration Authentication ADS Workgroup: <S: 0,15>

Expressway が AD ドメインに参加するときに使用するワークグループ。

例：`xConfiguration Authentication ADS Workgroup: 「corporation」`

xConfiguration Authentication Account Admin Account [1..n] AccessAPI: <On/Off>

このアカウントがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスと設定にアクセスできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 AccessAPI: On`

xConfiguration Authentication Account Admin Account [1..n] AccessWeb: <On/Off>

このアカウントが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 AccessWeb: On`

xConfiguration Authentication Account Admin Account [1..n] Enabled: <On/Off>

アカウントが有効になっているか、無効になっているかを示します。無効なアカウントへのアクセスは拒否されます。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Account 1 Enabled: On`

xConfiguration Authentication Account Admin Account [1..n] Name: <S: 0, 128>

管理者アカウントのユーザ名。

例：`xConfiguration Authentication Account Admin Account 1 Name: 「bob_smith」`

xConfiguration Authentication Account Admin Account [1..n] Password: <Password>

この管理者が Expressway へのログインに使用するパスワード。

例：`xConfiguration Authentication Account Admin Account 1 Password: 「abcXYZ_123」`

xConfiguration Authentication Account Admin Group [1..n] AccessAPI: <On/Off>

このグループのメンバーがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 AccessAPI: On`

xConfiguration Authentication Account Admin Group [1..n] AccessWeb: <On/Off>

このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 AccessWeb: On`

xConfiguration Authentication Account Admin Group [1..n] Enabled: <On/Off>

グループが有効になっているか、無効になっているかを示します。無効になっているグループのメンバーへのアクセスは拒否されます。デフォルトは On です。

例：`xConfiguration Authentication Account Admin Group 1 Enabled: On`

xConfiguration Authentication Account Admin Group [1..n] Name: <S: 0, 128>

管理者グループの名前。

例：`xConfiguration Authentication Account Admin Group 1 Name: 「administrators」`

xConfiguration Authentication Certificate Crlcheck: <None/Peer/All>

HTTPS クライアント証明書を証明書失効リスト（CRL）と照合して確認するかどうかを指定します。CRL データは CRL の管理ページを使用して Expressway にアップロードされます。デフォルトは All です。

None：CRL チェックは実行されません。

Peer：クライアントの証明書を発行した CA に関連付けられた CRL のみを確認します。

All：クライアントの証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。

例：`xConfiguration Authentication Certificate Crlcheck: All`

xConfiguration Authentication Certificate Crlinaccessible: <Ignore/Fail>

たとえば、失効の送信元に通信できない、または適切な失効リストが提示されないなど、失効ステータスを確立できない場合の失効リストの確認の動作を制御します。デフォルトは Ignore です。

Ignore：失効していないものとして証明書を処理します。

Fail：失効しているものとして証明書を処理します（したがって、TLS 接続は許可しません）。

例：`xConfiguration Authentication Certificate Crlinaccessible: Ignore`

xConfiguration Authentication Certificate Mode: <NotRequired/Validation/Authentication>

クライアント システム（通常は Web ブラウザ）が HTTPS を使用して Expressway と通信するために必要なセキュリティ レベルを制御します。デフォルトは NotRequired です。

NotRequired：クライアントシステムはどのような形式の証明書も提示する必要はありません。

Validation：クライアントシステムは、信頼できる認証局（CA）が署名した有効な証明書を提示する必要があります。Not required から Certificate validation に変更した場合は、再起動が必要です。

Authentication：クライアントシステムは、信頼できる CA が署名した有効な証明書を提示する必要があり、その証明書にはクライアントの認証クレデンシャルを含める必要があります。このモードを有効にすると、標準のログイン メカニズムは使用できなくなります。

例：`xConfiguration Authentication Certificate Mode: NotRequired`

xConfiguration Authentication Certificate UsernameRegex: <String>

Expressway に提示するクライアント証明書に適用する正規表現。(? regex) を使用してキャプチャ グループの名前を指定することで、照合するサブパターンを関連付けられたテンプレートで置き換えることができます。デフォルトは /Subject:.*CN= (? ([^,\]|(\,))*)/m

例：`xConfiguration Authentication Certificate UsernameRegex: 「/Subject:.*CN= (? ([^,\]|(\,))*)/m」`

xConfiguration Authentication Certificate UsernameTemplate: <String>

正規表現に使用する固定テキストとキャプチャしたグループ名の組み合わせを含んだテンプレート。各キャプチャ グループ名は # を使用して、たとえば prefix#Group1#suffix のように区切ります。各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。置換された文字列は、ユーザの認証クレデンシャル（ユーザ名）として使用されます。デフォルトは #captureCommonName# です。

例：`xConfiguration Authentication Certificate UsernameTemplate: 「#captureCommonName#」`

xConfiguration Authentication H350 BindPassword: <S: 0, 60>

LDAP サーバにバインドするときに使用するパスワードを設定します。

例：`xConfiguration Authentication H350 BindPassword: 「abcXYZ_123」`

xConfiguration Authentication H350 BindSaslMode: <None/DIGEST-MD5>

LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。デフォルトは DIGEST-MD5 です。

None：メカニズムを使用しません。

DIGEST-MD5：DIGEST-MD5 メカニズムを使用します。

例：`xConfiguration Authentication H350 BindSaslMode: DIGEST-MD5`

xConfiguration Authentication H350 BindUserDn: <S: 0, 500>

LDA Pサーバにバインドするときに使用するユーザの識別名を設定します。

例：`xConfiguration Authentication H350 BindUserDn: 「manager」`

xConfiguration Authentication H350 BindUserName: <S: 0, 500>

LDAP サーバにバインドするときに使用するユーザ名を設定します。SASL を使用する場合にのみ適用されます。

例：`xConfiguration Authentication H350 BindUserName: 「manager」`

xConfiguration Authentication H350 DirectoryBaseDn: <S: 0, 500>

LDAP サーバに接続するときに使用するユーザの識別名を設定します。

例：`xConfiguration Authentication H350 DirectoryBaseDn: 「dc=example,dc=company,dc=com」`

xConfiguration Authentication H350 LdapEncryption: <Off/TLS>

LDAP サーバへの接続に使用する暗号化を設定します。デフォルト：TLS。

Off：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Authentication H350 LdapEncryption: TLS`

xConfiguration Authentication H350 LdapServerAddress: <S: 0, 256>

デバイス認証のための LDAP クエリを実行するときに使用する LDAP サーバの IP アドレスまたは完全修飾ドメイン名

例：`xConfiguration Authentication H350 LdapServerAddress: 「ldap_server.example.com」`

xConfiguration Authentication H350 LdapServerAddressResolution: <AddressRecord/ServiceRecord>

LDAP サーバ アドレスが FQDN として指定されている場合の解決方法を定義します。デフォルトは AddressRecord です。

アドレス レコード（*Address record*）：DNS A レコードまたは AAAA レコード ルックアップ。

SRV レコード（*SRV record*）：DNS SRV レコード ルックアップ。

例：`xConfiguration Authentication H350 LdapServerAddressResolution: AddressRecord`

xConfiguration Authentication H350 LdapServerPort: <1..65535>

デバイス認証のための LDAP クエリを実行するときに使用する LDAP サーバの IP ポートを設定します。通常、セキュリティで保護されていない接続は 389 を使用します。デフォルト：389

例：`xConfiguration Authentication H350 LdapServerPort: 389`

xConfiguration Authentication H350 Mode: <On/Off>

デバイス認証への H.350 ディレクトリの使用を有効または無効にします。デフォルト：Off

例：`xConfiguration Authentication H350 Mode: Off`

xConfiguration Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

エイリアスの確認および登録方法を決定します。デフォルトは LDAP です。

LDAP：エンドポイントによって提示されたエイリアスを LDAP データベースのリストにあるエイリアスと照合して確認します。

Endpoint：エンドポイントによって提示されたエイリアスを使用します。LDAP データベースにあるエイリアスはすべて無視されます。

Combined：エンドポイントが提示したエイリアスのほかに LDAP データベースのリストにあるエイリアスも使用します。

例：`xConfiguration Authentication LDAP AliasOrigin: LDAP`

xConfiguration Authentication Password: <S: 0, 215>

別のシステムでの認証時に Expressway が使用するパスワード。プレーンテキストの最大長は 128 文字で、暗号化されます。注：トラバーサル クライアント ゾーンには適用されません。

例：`xConfiguration Authentication Password: 「password123」`

xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: <0..65535>

ダイジェスト認証のキャッシュ有効期限の秒単位の確認間隔。デフォルトは 600 です。

例：`xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: 600`

xConfiguration Authentication Remote Digest Cache Lifetime: <0..43200>

秒単位のダイジェスト認証暫定ハッシュのライフタイム。デフォルトは 600 です。

例：`xConfiguration Authentication Remote Digest Cache Lifetime: 600`

xConfiguration Authentication Remote Digest Cache Limit: <0..65535>

ダイジェスト認証のキャッシュ有効期限の秒単位の確認間隔。デフォルトは 10000 です。

例：`xConfiguration Authentication Remote Digest Cache Limit: 10000`

xConfiguration Authentication Remote Digest Cache Mode: <On/Off>

ダイジェスト認証キャッシュを有効にするかどうかを制御します。デフォルト：[オン（On）]

例：`xConfiguration Authentication Remote Digest Cache Mode: On`

xConfiguration Authentication StrictPassword Enabled: <On/Off>

ローカル管理者アカウントのパスワードは、それらが受け入れられる前に最小レベルの複雑性を満たしているかどうかを決定します。さらに、パスワードは「「abc」」や「「123」」などの連続する文字を多く含んでいたり、違う文字がほとんど含まれていないディクショナリの単語に基づいたものや、あるいは回文にはしないでください。デフォルトは Off です。

On：ローカル管理者パスワードは複雑度の要件を満たす必要があります。

Off：パスワードの複雑度は確認されません。

例：`xConfiguration Authentication StrictPassword Enabled: Off`

xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: <0..255>

同じ文字を連続して繰り返すことができる最大回数。値を 0 にするとこの確認が無効になります。デフォルト：0

例：`xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`

xConfiguration Authentication StrictPassword MinimumClasses: <0..4>

使用する必要がある文字クラスの最小数。文字クラスには、数字、大文字、小文字、特殊文字の 4 種類があります。これらすべての使用を求めずに 2 ～ 3 の異なる文字クラスを必須とする場合に、この設定を使用します。値を 0 にするとこの確認が無効になります。デフォルト：[0]。

例：`xConfiguration Authentication StrictPassword MinimumClasses: 0`

xConfiguration Authentication StrictPassword MinimumDigits: <0..255>

使用する必要がある数字の最小数。値を0にするとこの確認が無効になります。デフォルト：2。

例：`xConfiguration Authentication StrictPassword MinimumDigits: 2`

xConfiguration Authentication StrictPassword MinimumLength: <6..255>

パスワードの最小の長さ。デフォルトは 15 です。

例：`xConfiguration Authentication StrictPassword MinimumLength: 15`

xConfiguration Authentication StrictPassword MinimumLowerCase: <0..255>

使用する必要がある小文字の最小数。値を 0 にするとこの確認が無効になります。デフォルト：2。

例：`xConfiguration Authentication StrictPassword MinimumLowerCase: 2`

xConfiguration Authentication StrictPassword MinimumOther: <0..255>

使用する必要がある特殊文字の最小数。特殊文字は英字や数字ではない文字のことです。値を 0 にするとこの確認が無効になります。デフォルト：2

例：`xConfiguration Authentication StrictPassword MinimumOther: 2`

xConfiguration Authentication StrictPassword MinimumUpperCase: <0..255>

使用する必要がある大文字の最小数。値を 0 にするとこの確認が無効になります。デフォルト：2

例：`xConfiguration Authentication StrictPassword MinimumUpperCase: 2`

xConfiguration Authentication UserName: <S: 0, 128>

別のシステムでの認証時にExpresswayで使用するユーザ名。注：トラバーサルクライアントゾーンには適用されません。

例：`xConfiguration Authentication UserName: 「user123」`

xConfiguration Bandwidth Default: <64..65535>

エンドポイントで帯域幅が指定されていないExpresswayが管理するコールに使用する帯域幅（kbps 単位）。デフォルト：384。

例：`xConfiguration Bandwidth Default: 384`

xConfiguration Bandwidth Downspeed PerCall Mode: <On/Off>

要求を満たすために使用できるコール単位の帯域幅が不足している場合にExpresswayがコールのダウンスピードを試行するかどうかを決定します。デフォルトは On です。

On：Expressway はより低い帯域幅でのコールの発信を試行します。

Off：コールは拒否されます。

例：`xConfiguration Bandwidth Downspeed PerCall Mode: On`

xConfiguration Bandwidth Downspeed Total Mode: <On/Off>

要求を満たすために使用できる総帯域幅が不足している場合にExpresswayがコールのダウンスピードを試行するかどうかを決定します。デフォルトは On です。

On：Expressway はより低い帯域幅でのコールの発信を試行します。

Off：コールは拒否されます。

例：`xConfiguration Bandwidth Downspeed Total Mode: On`

xConfiguration Bandwidth Link [1..3000] Name: <S: 1, 50>

このリンクに名前を割り当てます。

例：`xConfiguration Bandwidth Link 1 Name: 「HQ to BranchOffice」`

xConfiguration Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>

このリンクを適用する最初のゾーンまたはサブゾーンを指定します。

例：`xConfiguration Bandwidth Link 1 Node1 Name: 「HQ」`

xConfiguration Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>

このリンクを適用する 2 番目のゾーンまたはサブゾーンを指定します。

例：`xConfiguration Bandwidth Link 1 Node2 Name: 「BranchOffice」`

xConfiguration Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>

このリンクと関連付ける最初のパイプを指定します。

例：`xConfiguration Bandwidth Link 1 Pipe1 Name: 「512Kb ASDL」`

xConfiguration Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>

このリンクと関連付ける 2 番目のパイプを指定します。

例：`xConfiguration Bandwidth Link 1 Pipe2 Name: 「2Gb Broadband」`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>

このパイプのコール単位の帯域幅の制限がある場合、どのコールにも使用可能な帯域幅の最大量（kbps 単位）を設定します。デフォルト：1920。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

このパイプで個々のコールの帯域幅を制限するかどうかを決定します。デフォルトはUnlimitedです。

NoBandwidth：使用可能な帯域幅はありません。コールは、このパイプで発信できません。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>

このパイプの帯域幅が制限されている場合にパイプで常に使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは 500000 です。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

このパイプで総帯域幅制限を適用するかどうかを決定します。デフォルトはUnlimitedです。

NoBandwidth：使用可能な帯域幅はありません。コールは、このパイプで発信できません。

例：`xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Name: <S: 1, 50>

このパイプに名前を割り当てます。

例：`xConfiguration Bandwidth Pipe 1 Name: 「512Kb ASDL」`

xConfiguration Call Loop Detection Mode: <On/Off>

Expressway がコール ループを確認するかどうかを指定します。デフォルトは On です。

例：`xConfiguration Call Loop Detection Mode: On`

xConfiguration Call Routed Mode: <Always/Optimal>

Expressway がコールにシグナリングをルーティングするかどうかを指定します。デフォルトは [Always] です。

Always：Expressway は常にコール シグナリングをルーティングします。

Optimal：可能な場合、Expressway はコール シグナリング パスからその Expressway 自体を削除します。つまり、コールはコール ライセンスを消費しない場合があります。

例：`xConfiguration Call Routed Mode: Always`

xConfiguration Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

Expressway またはそのネイバーの 1 つの登録されていないシステムに Expressway がコールを試行する方法。デフォルトは Indirect です。

Direct：Expressway がネイバーを照会することなく、エンドポイントが不明な IP アドレスにコールできます。端部がローカルシステムに直接登録されていたかのように、コール セットアップが実行されます。

Indirect：不明な IP アドレスへのコールを受信すると、Expressway はネイバーにそのリモートアドレスを照会し、許可されれば、ネイバーを通じてコールをルーティングします。

Off：Expressway に直接登録されたエンドポイントが Expressway に直接登録されたシステムの IP アドレスのみをコールする可能性があります。

例：`xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

xConfiguration Call Services Fallback Alias: <S: 0, 60>

Expressway の IP アドレスまたはドメイン名が指定されていても、コール エイリアスが指定されていないコールの場合に、着信メッセージを発信するエイリアスを指定します。

例：`xConfiguration Call Services Fallback Alias: 「reception@example.com」`

xConfiguration CollaborationEdge AllowEmbeddedSafari: <Yes/No>

これは、iOS 9 以降を使用している iPad または iPhone が OAuth トークンを使用して認可する場合に、それらの iPad または iPhone 上の Cisco Jabber 11.8 以降にのみ適用されます。

Yes を選択すると、iOS デバイス上の Jabber がネイティブ Safari ブラウザに認証ページを表示できるようになります。

No を選択すると、iOS デバイス上の Jabber は、Safari ブラウザではなく WebView ブラウザに認証ページを表示します。

（注） このオプションを切り替える場合は、Cisco Unified Communications Manager の **[iOS の SSO ログイン動作（SSO Login Behavior for iOS）]** についても対応する選択を行ってください。

例：`xConfiguration CollaborationEdge AllowEmbeddedSafari: No`

xConfiguration CollaborationEdge AllowList DefaultMethods: <String>

HTTP 許可リストに 1 つ以上のデフォルト HTTP メソッドを設定します。

設定パラメータ：

メソッド：<OPTIONS/GET/HEAD/POST/PUT/DELETE>：コンマ区切りの 1 つ以上の http メソッドのセット

例：`xConfiguration CollaborationEdge AllowList DefaultMethods: PUT,GET,POST`

xConfiguration CollaborationEdge AllowOnboardingOverMra: <On/Off>

MRA デバイスのアクティベーション コードによるオンボーディングを有効または無効にします。有効/無効にすると、その設定に応じて自動的に mTLS が MRA ポート上で有効または無効にされます。mTLS に必要な CA 証明書は自動生成されます。

例`xCo : nfiguration CollaborationEdge AllowOnboardingOverMra: On`

xConfiguration CollaborationEdge AllowRedirectUri: <On/Off>

リダイレクトURIを有効または無効にします。クライアントがOAuthフロー（およびMRA）に埋め込みブラウザを使用できるようにします。デフォルト値は*no*です。このオプションを有効にするには値を *[*はい（*Yes*）*]* に設定します。

例：`xConfiguration CollaborationEdge AllowRedirectUri: Off`

xConfiguration CollaborationEdge Enabled: <On/Off>

この Expressway の Mobile & Remote Access を有効または無効にします。

例：`xConfiguration CollaborationEdge Enabled: On`

xConfiguration CollaborationEdge InternalCheck: <No/Yes>

このスイッチは、使用可能な認証モードに関してExpressway-Cがユーザのホーム ノードを確認するかどうかを決定します。*No* を選択すると、Expresswayは、実際にホームノードを確認することなく、Expressway-C で有効になっている認証モードが使用可能であることをクライアントに通知します。その結果、通常、内部ネットワークのトラフィックが減少します。ただし、このオプションは、すべてのノードで同じ認証モードが使用可能であることが分かっている場合にのみ選択してください。

Expressway-E がクライアントに応答する前に Expressway-C がユーザのホームノードについて確認できるようにするには、*Yes* を選択します。

例：`xConfiguration CollaborationEdge InternalCheck: No`

xConfiguration CollaborationEdge JabbercEnabled: <On/Off>

この Expressway の Jabber Guest サービスを有効または無効にします。

例：`xConfiguration JabbercEnabled: Off`

xConfiguration CollaborationEdge JabbercProxyProtocol: <http/https>

Expressway を通じて Jabber Guest サービスをプロキシ送信するために使用するプロトコルを選択します。

例：`xConfiguration JabbercProxyProtocol: https`

xConfiguration CollaborationEdge LegacyCred: <On/Off>

MRA クライアントが Expressway に提供するユーザ名とパスワードに基づいて Unified Communications サービスが MRA クライアントを認可する場合は、On を選択します。

例：`xConfiguration CollaborationEdge LegacyCred: Off`

xConfiguration CollaborationEdge LegacySso: <On/Off/Exclusive>

MRA クライアントがExpresswayに提供するOAuthトークンに基づいてUnified Communicationsサービスが MRA クライアントを認可する場合は、On を選択します。これは自己記述 OAuth トークン タイプではありません。

例：`xConfiguration CollaborationEdge LegacySso: Off`

xConfiguration CollaborationEdge OauthLocal: <On/Off>

Unified Communications サービスへの Mobile & Remote Access の OAuth ローカル認証を有効または無効にします。

例：`xConfiguration CollaborationEdge OauthLocal: Off`

xConfiguration CollaborationEdge OauthSso: <On/Off>

Unified Communications サービスへの Mobile & Remote Access の OAuth シングル サインオンを有効または無効にします。

例：`xConfiguration CollaborationEdge OauthSso: Off`

xConfiguration CollaborationEdge RFC3327Enabled: <On/Off>

自動的に生成されたネイバー ゾーンを経由するレジスタの変更のパス ヘッダー サポート Unified CMノードを参照してください。

On：Expressway-Cは自身のアドレスをREGISTERメッセージのPathヘッダーおよびREGISTERメッセージへの応答に挿入します。

Off：Expressway-Cは、REGISTERメッセージのContactヘッダーのアドレスを上書きします。

例：`xConfiguration CollaborationEdge rfc3327Enabled: On`

xConfiguration CollaborationEdge SSO Scope: <PEER/CLUSTER>

Expressway ピアごとに、選択した IdP で SAML 合意を使用する場合は、PEER を指定します。クラスタに 1 つの SAML 合意を使用する場合は、CLUSTER を指定します。

例：`xConfiguration CollaborationEdge SSO Scope: CLUSTER`

xConfiguration CollaborationEdge SSO IdP <index> Digest: <sha1/sha256>

クライアントに渡す SAML 認証要求に署名するときに Expressway が使用するハッシュ アルゴリズムを変更します。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256`

xConfiguration CollaborationEdge SsoAlwaysAvailable: <On/Off>

Expressway-C がユーザのホーム ノードに使用可能な SSO があることを確認するかどうかを決定します。

On：Expressway-Eは、ホームノードを実際に確認せずに、SSOが使用可能であるとクライアントに常に通知します。

Off：Expressway-Eがクライアントに応答する前に、Expressway-Cが常にユーザのホームノードで SSO が使用できることを確認できるようにします。

例：`xConfiguration CollaborationEdge SsoAlwaysAvailable: Off`

（注） デフォルト値の *Off* は、Web UI で [内部 SSO のアベイラビリティの確認（**Check for internal SSO availability**）] をデフォルトの *[*はい（*Yes*）*]* に設定することと同じです。

xConfiguration CollaborationEdge SsoEnabled: <On/Off>

UC サービスへの Mobile & Remote Access のシングル サインオンを切り替えます。

例：`xConfiguration CollaborationEdge SsoEnabled: Off`

xConfiguration CollaborationEdge SsoSipTokenExtraTtl: <0..172800>

指定した秒数で SIP 認証のライフタイムを延長します。

重要　存続可能時間の拡張は、オンプレミスの UC クレデンシャルが期限切れになった後も、外部ユーザがエッジ経由で SIP を使用できることを意味します。これにより、（再認証が必要であることに気付かなかった場合でも）通話を受け入れることができる短いウィンドウがユーザに提供されますが、この利便性とセキュリティ リスクの増大のバランスをとる必要があります。

例：`xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0`

xConfiguration CollaborationEdgeDeployments <index> DeploymentId: <1..65535>

特定の導入の導入 ID を変更します。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5`

xConfiguration CollaborationEdgeDeployments <index> UserReadableName: <String>

この導入の名前を入力します。この Expressway を使用して提供するユニファイド コミュニケーション サービスを複数の導入を使用してパーティション化することができます。ユニファイドコミュニケーション サービスをパーティション化するための導入の使用を参照してください。

<*index*>は、Expressway に設定されているリストから特定の IdP を識別する整数です。

例：`xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment`

xConfiguration Ciphers SIPTLSCiphers Value: <S:0,2048>

SIP TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。この機能を有効にするには、再起動が必要です。また、aNULL 暗号方式はインバウンド接続ではサポートされません。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH`

例：`xConfiguration Ciphers SIPTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH」`

SIP TLS プロトコル値を変更するには、*SIP Advanced SipTlsVersions* を参照してください。

xConfiguration Ciphers HTTPSCiphers Value: <S:0,2048>

HTTPS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers HTTPSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers HTTPSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

HTTPS TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers HTTPSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers SMTPTLSCiphers Value: <S:0,2048>

「OpenSSL 暗号」形式で使用する SMTP TLS 暗号スイートを指定します（以下参照、https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers SMTPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers SMTPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

SMTP TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers SMTPTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers ReverseProxyTLSCiphers Value: <S:0,2048>

リバース プロキシ TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers ReverseProxyTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers ReverseProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

リバース プロキシ TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers ReverseProxyTLSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers UcClientTLSCiphers Value: <S:0,2048>

UC クライアント TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration CiphersUcClientTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers UcClientTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

UC クライアント TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers UcClientTLSProtocol Value: 「minTLSv1.2」`

xConfiguration Ciphers XCPTLSCiphers Value: <S:0,2048>

XCP TLS 暗号スイートを「OpenSSL 暗号方式」の形式で使用するように指定します（https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT を参照してください）。この機能を有効にするには、再起動が必要です。

デフォルト：`EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

例：`xConfiguration Ciphers XCPTLSCiphers Value: 「EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL」`

xConfiguration Ciphers XCPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

XCP TLS プロトコルの最小バージョンを指定します。

デフォルト：`minTLSv1.2`

例：`xConfiguration Ciphers XCPTLSProtocol Value: minTLSv1.2`

xConfiguration Ciphers sshd_ciphers Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）に利用可能な暗号方式を設定します。

デフォルト：
`aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`

例：`xConfiguration Ciphers sshd_ciphers Value: 「aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr」`

xConfiguration Ciphers sshd_kex Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）のキー交換アルゴリズムを設定します。

デフォルト：
`ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

例：`xConfiguration Ciphers sshd_kex Value: 「ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1」`

xConfiguration Ciphers sshd_macs Value: <S:0,2048>

「openssh」 形式の管理/ルート SSH 接続（TCP/22）のメッセージ認証コードダイジェストを設定します。

デフォルト：`hmac-sha2-512,hmac-sha2-256,hmac-sha1`

例：`xConfiguration Ciphers sshd_macs Value: 「hmac-sha2-512,hmac-sha2-256,hmac-sha1」`

xConfiguration Ciphers sshd_pfwd_ciphers Value: <S:0,2048>

順方向および逆方向の HTTP プロキシ（つまり、APNS および MRA HTTP トラフィック）に使用される SSH トンネルで使用できる暗号方式。

デフォルト：`aes256-ctr`

例：`xConfiguration Ciphers sshd_pfwd_ciphers Value: 「aes256-ctr」`

xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms

使用可能な公開キーアルゴリズムを構成します。

デフォルト値：
`「x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521」`

次の値のみが許可されます：
`x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521`

例：`xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms Value: "x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256"`

（注） **sshd_pfwd_pubkeyalgorithms** 構成（構成した公開キーの 4 つすべてのタイプ）のデフォルト値を使用する必要があります。

この構成をカスタマイズする場合は、このノードのサーバー証明書が使用するすべての公開キータイプを構成します。同様に、ssh トンネルを使用してこのノードに接続している他のすべてのノードを構成します。

たとえば、1 つのノード Expressway-C には 256 サイズの ECDSA を使用して作成されたサーバー証明書があり、これは 384 サイズの ECDSA を使用して作成されたサーバー証明書がある ssh トンネルを介して別のノード Expressway-E に接続しています。両方のノードで **sshd_pfwd_pubkeyalgorithms** を 値 `"x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384"` に構成します。

xConfiguration DNS PerDomainServer [1..5] Address: <S: 0, 39>

関連付けられたドメイン名のホスト名を解決するときのみに使用する DNS サーバの IP アドレス。

例：`xConfiguration DNS PerDomainServer 1 Address: 「192.168.12.1」`

xConfiguration DNS PerDomainServer [1..5] Domain1: <S: 0, 39>

この特定の DNS サーバで解決する最初のドメイン名。

例：`xConfiguration DNS PerDomainServer 1 Domain1: 「dept.example.com」`

xConfiguration DNS PerDomainServer [1..5] Domain2: <S: 0, 39>

この特定の DNS サーバで解決する 2 番目のドメイン名。

例：`xConfiguration DNS PerDomainServer 1 Domain2: 「other.example.com」`

xConfiguration DNS Server [1..5] Address: <S: 0, 39>

ドメイン名を解決するときに使用するデフォルトの DNS サーバの IP アドレス。最大で 5 のサーバを指定できます。デフォルトの DNS サーバは、ルックアップするドメインに定義されたドメイン単位の DNS サーバがない場合に使用します。

例：`xConfiguration DNS Server 1 Address: 「192.168.12.0」`

xConfiguration EdgeConfigServer CredentialTtl: <0..604800>

SSO 認証には適用されません。

Expressway がクライアントの認証に成功するために送信する認証トークンのライフタイムを指定します。正常に認証されたクライアントは、このトークンが期限切れになる前に更新を要求する必要があります。更新しないと、再認証が必要になります。

例：`xConfiguration EdgeConfigServer CredentialTtl: 28800`

xConfiguration EdgeConfigServer PurgeInterval: <0..604800>

SSO 認証には適用されません。

Expressway がキャッシュ クリアの動作の間に待機する時間を指定します。キャッシュがクリアされると、期限切れのトークンのみが削除されるため、この設定は期限切れトークンをキャッシュに保持できる最長時間となります。

例：`xConfiguration EdgeConfigServer PurgeInterval: 43200`

xConfiguration EdgeConfigServer RateLimitLogins: <0..100>

VCS を使用してユーザのクレデンシャルをレート コントロール期間ごとに許可する回数を制限します。同じユーザ クレデンシャルを使用しているデバイスは、この回数に対して考慮されます。

上限に到達すると、これらのクレデンシャルを使用するためのそれ以降の試行が現在のレート コントロールの期限が切れるまで拒否されます。

レート コントロール機能を無効にするには 0 を入力します。

例：`xConfiguration EdgeConfigServer RateLimitLogins: 3`

xConfiguration EdgeConfigServer RateLimitPeriod: <0..86400>

許可がカウントされる期間（秒単位）を定義します。レート コントロールが有効になっている場合は、ユーザの最初の許可でカウンタとタイマーが起動します。レート コントロールの期限が切れるとカウンターがリセットされ、ユーザの次の許可によって新しい期間が開始されます。

レート コントロール機能を無効にするには 0 を入力します。

例：`xConfiguration EdgeConfigServer RateLimitPeriod: 300`

xConfiguration ErrorReport Contact: <S: 0, 128>

必要に応じて、インシデント レポートでフォローアップするオプションの連絡先電子メール アドレス。

例：`xConfiguration ErrorReport Contact: 「bob smith」`

xConfiguration ErrorReport CoreDump: <On/Off>

診断コアダンプ ファイルを作成するかどうかを決定します。デフォルトは On です。

例：`xConfiguration ErrorReport CoreDump: On`

xConfiguration ErrorReport Mode: <On/Off>

アプリケーション機能の詳細情報を Web サービスに自動的に送信するかどうかを決定します。デフォルト：Off

例：`xConfiguration ErrorReport Mode: Off`

xConfiguration ErrorReport Proxy: <S: 0, 128>

インシデント レポート サーバへの HTTP/HTTPS 接続に使用するオプションのプロキシ サーバ。

例：`xConfiguration ErrorReport Proxy: https://proxy_address/submiterror/`

xConfiguration ErrorReport Url: <S: 0, 128>

アプリケーション障害の詳細情報を送信する Web サービスの URL。デフォルト：https://cc-reports.cisco.com/submitapplicationerror/

例：`xConfiguration ErrorReport Url: https://cc-reports.cisco.com/submitapplicationerror/`

xConfiguration Ethernet [1..2] IP V4 Address: <S: 7,15>

指定した LAN ポートの IPv4 アドレスを指定します。注：変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 Address: 「192.168.10.10」`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15>

Expressway がスタティック NAT モードで動作している場合、これによりそのスタティック NAT の外部パブリック IPv4 アドレスを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 StaticNAT Address: 「64.22.64.85」`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off>

Expressway をスタティック NAT の背後に配置するかどうかを指定します。変更を有効にするには、システムを再起動する必要があります。デフォルト：Off

例：`xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On`

xConfiguration Ethernet [1..2] IP V4 SubnetMask: <S: 7,15>

指定した LAN ポートの IPv4 サブネット マスクを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V4 SubnetMask: 「255.255.255.0」`

xConfiguration Ethernet [1..2] IP V6 Address: <S: 0, 39>

指定した LAN ポートの IPv6 アドレスを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Ethernet 1 IP V6 Address: 「2001:db8::1428:57ab」`

xConfiguration Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

指定した LAN ポートからのイーサネット リンクの速度を設定します。速度を自動的に設定するには Auto を使用します。変更を有効にするには、システムを再起動する必要があります。デフォルト：[Auto]

例：`xConfiguration Ethernet 1 Speed: Auto`

xConfiguration ExternalManager Address: <S: 0, 128>

外部マネージャの IP アドレスまたは完全修飾ドメイン名（FQDN）を設定します。

例：`xConfiguration ExternalManager Address: 「192.168.0.0」`

xConfiguration ExternalManager Path: <S: 0, 255>

外部マネージャの URL を設定します。デフォルトは tms/public/external/management/SystemManagementService.asmx です。

例：`xConfiguration ExternalManager Path: 「tms/public/external/management/SystemManagementService.asmx」`

xConfiguration ExternalManager Protocol: <HTTP/HTTPS>

外部マネージャに接続するために使用するプロトコル。デフォルトは HTTPS です。

例：`xConfiguration ExternalManager Protocol: HTTPS`

xConfiguration ExternalManager Server Certificate Verification Mode: <On/Off>

外部マネージャによって提供される証明書を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration ExternalManager Server Certificate Verification Mode: On`

xConfiguration H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Expressway がエンドポイントからのゲートキーパー検出要求に応答するかどうかを決定します。デフォルトは On です。

例：`xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

xConfiguration H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

コールの確立後に使用する範囲の上位ポートを指定します。デフォルト：19999。

例：`xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

xConfiguration H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

コールの確立後に使用する範囲の下位ポートを指定します。デフォルト：15000。

例：`xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

xConfiguration H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

H.323 コール シグナリングをリッスンするポートを指定します。デフォルト：1720。

例：`xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

xConfiguration H323 Gatekeeper CallTimeToLive: <60..65534>

Expressway がコール中のエンドポイントをポーリングし、まだコール中であることを確認するための間隔（秒単位）デフォルトは 120 です。

例：`xConfiguration H323 Gatekeeper CallTimeToLive: 120`

xConfiguration H323 Gatekeeper Registration RIPAllRequests: <On/Off>

Expresswayがリクエストを処理中グリーティングとH.323の登録要求に応答するかどうかを決定します。

リモートLDAPディレクトリ サービスの登録要求を認証するときに登録タイムアウトが発生したらこの設定を有効にします。デフォルト：Off

例:`xConfiguration H323のゲートキーパー登録RIPAllRequests:オフ`

xConfiguration H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

エンドポイントが別のIPアドレスから現在登録されているエイリアスの登録を試行する場合のシステムの動作。デフォルトは Reject です。

Reject：登録を拒否します。

Overwrite：元の登録を削除して、新しい登録に置き換えます。

例：`xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

xConfiguration H323 Gatekeeper Registration UDP Port: <1024..65534>

H.323 UDP 登録に使用するポートを指定します。デフォルト：1719。

例：`xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

xConfiguration H323 Gatekeeper TimeToLive: <60..65534>

H.323 エンドポイントが現在も機能していることを確認するために Expressway に再登録する必要がある間隔（秒単位）。デフォルト：1800。

例：`xConfiguration H323 Gatekeeper TimeToLive: 1800`

xConfiguration H323 Gateway CallerId: <IncludePrefix/ExcludePrefix>

ISDN ゲートウェイのプレフィックスを宛先のエンドポイントに提供される発信者の E.164 番号に挿入するかどうかを指定します。プレフィックスを含めると、受信者はコールを直接返せます。デフォルトは ExcludePrefix です。

IncludePrefix：ISDN ゲートウェイのプレフィックスを送信元の E.164 番号に挿入します。

ExcludePrefix：送信元の E.164 number のみを表示します。

例：`xConfiguration H323 Gateway CallerId: ExcludePrefix`

xConfiguration H323 Mode: <On/Off>

Expressway が H.323 ゲートキーパー機能を提供するかどうかを決定します。デフォルト：Off

例：`xConfiguration H323 Mode: On`

xConfiguration Interworking BFCP Compatibility Mode: <Auto/TAA/Draft>

H.323 インターワーキング BFCP コントロールに対する SIP の互換性設定を制御します。デフォルト：[Auto]

例：`xConfiguration Interworking BFCP Compatibility Mode: Auto`

xConfiguration Interworking Encryption KeySize2048: <On/Off>

H.323-SIP インターワーキングの暗号化に使用する 2048 ビットの Diffie-Hellman キーが Expressway に含まれるかどうかを決定します。デフォルトは On です。

*On:*Expressway は、1024 ビットと 2048 ビットの両方の暗号キー長を提供します。

Off：Expressway は 2048 ビットの暗号化キー長を提供しません。

例：`xConfiguration Interworking Encryption KeySize2048: On`

xConfiguration Interworking Encryption Mode: <Auto/Off>

Expressway が SIP エンドポイントと H.323 エンドポイント間の暗号化されたコールを許可するかどうかを決定します。デフォルト：[Auto]

Off：インターワーキングコールは暗号化されません。

Auto：エンドポイントが要求した場合はインターワーキング コールが暗号化されます。

例：`xConfiguration Interworking Encryption Mode: Auto`

xConfiguration Interworking Encryption Replay Protection Mode: <On/Off>

コールをインターワーキングするときに、着信 SRTP の再生保護を Expressway が実行するかどうかを制御します。デフォルト：Off

On：再生された SRTP パケットは Expressway でドロップされます。

Off：Expressway は再生された SRTP パケットを確認しません。

例：`xConfiguration Interworking Encryption Replay Protection Mode: Off`

xConfiguration Interworking Mode: <On/Off/RegisteredOnly>

Expressway を SIP コールと H.323 コール間のゲートウェイとして機能させるかどうかを決定します。デフォルトは RegisteredOnly です。

Off：Expressway は SIP-H.323 ゲートウェイとして機能しません。

On：Expressway は、エンドポイントがローカルに登録されているかどうかに関係なく、SIP-H.323 ゲートウェイとして機能します。

RegisteredOnly：Expressway は、少なくとも 1 つのエンドポイントがローカルに登録されている場合にのみ、SIP-H.323 ゲートウェイとして機能します。

例：`xConfiguration Interworking Mode: On`

xConfiguration Interworking Require Invite Header Mode: <On/Off>

SIP と H.323 インターワーキング機能がダイアログを構成する INVITE の必須ヘッダーで com.tandberg.sdp.duo.enable と com.tandberg.sdp.bfcp.udp を送信するかどうかを制御します。デフォルト：Off

例：`xConfiguration Interworking Require Invite Header Mode: Off`

xConfiguration IP DNS Domain Name: <S: 0, 128>

DNS サーバに照会する前に、非修飾ホスト名に追加する名前。NTP サーバ、LDAP サーバ、外部マネージャ サーバ、およびリモート ログ サーバの非修飾ドメイン名の解決を試行するときに使用します。また、**システム ホスト名**とともに使用して、SIP メッセージングでのこの Expressway への参照を識別します。

例：`xConfiguration IP DNS Domain Name: 「example.com」`

xConfiguration IP DNS Hostname : <S: 0, 63>

このシステムが認識している DNS ホスト名。これは完全修飾ドメイン名ではなく、ホストのラベル部分です。名前には、英字、数字、ハイフン、および下線のみを使用できます。最初の文字は英字、最後の文字は英字または数字にする必要があります。

例：`xConfiguration IP DNS Hostname: 「localsystem」`

xConfiguration IP DNS MaxPort: <1024..65535>

DNS クエリの送信に使用する範囲の上位送信元ポート。要求は、この範囲からランダムにポートを選択します。警告：設定したソース ポート範囲が狭いと、DNS スプーフィング攻撃に対する脆弱性が高まります。デフォルト：65535。

例：`xConfiguration IP DNS MaxPort: 65535`

xConfiguration IP DNS MinPort: <1024..65535>

DNS クエリの送信に使用する範囲の下位送信元ポート。要求は、この範囲からランダムにポートを選択します。警告：設定したソース ポート範囲が狭いと、DNS スプーフィング攻撃に対する脆弱性が高まります。デフォルト：1024。

例：`xConfiguration IP DNS MinPort: 1024`

xConfiguration IP DNS SearchDomains: <S: 0, 1024>

DNS サーバを照会するときに追加で検索するドメイン名のスペース区切りリスト。NTP サーバ、LDAP サーバ、外部マネージャ サーバ、およびリモート ログ サーバの非修飾ドメイン名の解決を試行するときに使用します。ローカル システム ホスト名とともに使用して、SIP メッセージングでこのシステムへの参照を識別することもできます。（ピア固有）

例：`xConfiguration IP DNS SearchDomains: 「example1.int」「" "example2.int」「example3.int」`

xConfiguration IP DNS UseEphemeralPortRange: <On/Off>

発信 DNS クエリがシステムの通常のエフェメラル ポート範囲を使用するか、設定可能なカスタム ポート範囲を使用するかを決定します。デフォルトは On です。

例：`xConfiguration IP DNS UseEphemeralPortRange: On`

xConfiguration IP Ephemeral PortRange End: <1024..65534>

Expressway コール処理によって禁止されていない限り、エフェメラル アウトバウンド接続に使用する範囲内の最上位のポート。デフォルト：35999。

例：`xConfiguration IP Ephemeral PortRange End: 35999`

xConfiguration IP Ephemeral PortRange Start: <1024..65534>

Expressway コール処理によって禁止されていない限り、エフェメラル アウトバウンド接続に使用する範囲内の最下位のポート。デフォルトは 30000 です。

例：`xConfiguration IP Ephemeral PortRange Start: 30000`

xConfiguration IP External Interface: <LAN1/LAN2>

外部に面している LAN インターフェイスを定義します。デフォルトは LAN1 です。

例：`xConfiguration IP External Interface: LAN1`

xConfiguration IP Gateway: <S: 7,15>

Expressway の IPv4 ゲートウェイを指定します。注：変更を有効にするには、システムを再起動する必要があります。デフォルトは 127.0.0.1 です。

例：`xConfiguration IP Gateway: "192.168.127.0"`

xConfiguration IP QoS Mode: <None/DiffServ>

すべてのシグナリングとメディア パケットに適用する QoS （Quality of Service）タグのタイプ。変更を有効にするには、システムを再起動する必要があります。デフォルト：[None]。

None：特定の QoS タグは適用されません。

DiffServ：指定したタグ値を IPv4 ヘッダーの TOS（サービスのタイプ）フィールドまたは IPv6 ヘッダーの TC（トラフィッククラス）フィールドに挿入します。

例：`xConfiguration IP QoS Mode: DiffServ`

重要 重要:このコマンドは、バージョン X8.9 から廃止されており、コマンド `QoS Audio`、`QoS Video`、`QoS XMPP`、および `QoS Signaling` に置き換わります。

xConfiguration IP QoS Value: <0..63>

システムを介してルーティングされるすべてのシグナリング トラフィックとメディア トラフィックにスタンプする値。変更を有効にするには、システムを再起動する必要があります。デフォルト：[0]。

例：`xConfiguration IP QoS Value: 16`

重要 重要:このコマンドは、バージョン X8.9 から廃止されており、コマンド `QoS Audio`、`QoS Video`、`QoS XMPP`、および `QoS Signaling` に置き換わります。

xConfiguration IP RFC4821 Mode: <Auto/Enabled/Disabled>

Expressway ネットワーク インターフェイスが RFC4821 Packetization Layer Path MTU Discovery をいつ使用するかを決定します。変更を有効にするには、システムを再起動する必要があります。デフォルトで、ディセーブルになっています。

Enabled：常にパケット化レイヤの MTU プロービングが実行されます。

Auto：デフォルトで無効になっていますが、ICMP ブラックホールが検出された場合に有効になります。

Disabled：パケット化レイヤの MTU プロービングは実行されません。

例：`xConfiguration IP RFC4821 Mode: Disabled`

xConfiguration IP Route [1..50] Address: <S: 0, 39>

このルートを適用するネットワークを決定するためにプレフィックス長とともに使用する IP アドレスを指定します。

例：`xConfiguration IP Route 1 Address: 「128.168.0.0」`

xConfiguration IP Route [1..50] Gateway: <S: 0, 39>

このルートのゲートウェイの IP アドレスを指定します。

例：`xConfiguration IP Route 1 Gateway: 「192.168.0.0」`

xConfiguration IP Route [1..50] Interface: <Auto/LAN1/LAN2>

このルーティングに使用するLANインターフェイスを指定します。Auto：使用に最適なインターフェイスを Expressway が選択します。デフォルト：[Auto]

例：`xConfiguration IP Route 1 Interface: Auto`

xConfiguration IP Route [1..50] PrefixLength: <0..128>

このルートを適用するネットワークを決定するときに一致する必要があるIPアドレスのビット数。デフォルト：32。

例：`xConfiguration IP Route 1 PrefixLength: 16`

xConfiguration IP V6 Gateway: <S: 0, 39>

ExpresswayのIPv6ゲートウェイを指定します。変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration IP V6 Gateway: 「3dda:80bb:6::9:144」`

xConfiguration IPProtocol: <Both/IPv4/IPv6>

Expressway が IPv4、IPv6、またはデュアル スタックのいずれのモードで実行するかを選択します。変更を有効にするには、システムを再起動する必要があります。デフォルトはIPv4です。

例：`xConfiguration IPProtocol: IPv4`

xConfiguration Language Default: <S: 0, 128>

Web インターフェイスで使用されるデフォルト言語。デフォルトは "en_US" です。

例：`xConfiguration Language Default: 「en_US」`

xConfiguration Log CDR Service: <off/serviceonly/serviceandlogging>

この Expressway によって生成されるコール詳細レコードを記録する方法を選択します。

Off：コール詳細レコードは記録されません。

serviceonly：コール詳細レコードは7日間ローカルに保存された後に削除されます。記録されたレコードにはユーザ インターフェイスからアクセスできません。

serviceandlogging：serviceonlyと同様ですが、CDRにはローカルイベントログからアクセスできます。syslog サーバのアドレスを追加した場合、それらのアドレスにレコードが情報メッセージとして送信されます。

デフォルト：*Off*

例：`xConfiguration Log CDR Service: serviceonly`

xConfiguration Log Level: <1..4>

イベントロギングの粒度を制御します。1は最も詳細度が低く、4が最も高くなります。注：この設定は過去に遡ることはできません。現時点以降のイベントログに書き込むイベントを決定します。デフォルトは 1 です。

例：`xConfiguration Log Level: 1`

xConfiguration Log MediaStats Logging: <On/Off>

メディア統計情報のロギングを切り替えます。デフォルト：Off

例：`xConfiguration Log MediaStats Logging: On`

xConfiguration Log SystemMetrics Interval: <30..600>

メトリック収集イベント間で待機する秒数を設定します。

重要 間隔が短いほどシステムのパフォーマンスに大きな影響を与え、長いほどメトリックが大まかになります。非常に高精度なメトリックが必要な場合以外は、最も長い間隔を使用することをお勧めします。

デフォルト：60

例：`xConfiguration Log SystemMetrics Interval: 60`

xConfiguration Log SystemMetrics Mode: <On/Off>

システム メトリック収集サービスを切り替えます。このシステムのメトリックの収集を開始するには、On と入力します。

デフォルトは *Off* です。

例：`xConfiguration Log SystemMetrics Mode: On`

xConfiguration Log SystemMetrics Network Address: <S: 0,1024>

リスニング サーバのアドレスを入力します。IP アドレス、ホスト名、または FQDN を使用できます。

デフォルト：空

例：`xConfiguration log SystemMetrics Network Address: 「192.168.0.5」`

LxConfiguration Log SystemMetrics Network Port: <1..65535>

システム メトリック トラフィックを予期するリスニング サーバのポートを入力します。

デフォルトは *25826* です。

例：`xConfiguration log SystemMetrics Network Port: 25826`

Configuration Logger Network [1..n] Level: <FATAL/ERROR/WARN/INFO/DEBUG/TRACE>

指定したモジュールのロギング レベル。デフォルト：INFO

例：`xConfiguration Logger Developer 1 Level: INFO`

xConfiguration Login Remote LDAP BaseDN Accounts: <S: 0,255>

管理者アカウントやユーザ アカウントの検索時にベースとして使用する識別名を設定します。

例：`xConfiguration Login Remote LDAP BaseDN Accounts: 「ou=useraccounts,dc=corporation,dc=int」`

xConfiguration Login Remote LDAP BaseDN Groups: <S: 0,255>

管理者グループやユーザ グループの検索時にベースとして使用する識別名を設定します。

例：`xConfiguration Login Remote LDAP BaseDN Groups: 「ou=groups,dc=corporation,dc=int」`

xConfiguration Login Remote LDAP CRLCheck: <None/Peer/All>

LDAP サーバとの TLS 接続を確立するときに証明書失効リスト（CRL）を確認するかどうかを指定します。CRL データは、信頼できる CA 証明書 PEM ファイルを使用して Expressway にアップロードされます。デフォルト：[None]。

None：CRL チェックは実行されません。

Peer：LDAP サーバの証明書を発行した CA に関連付けられた CRL のみを確認します。

All：LDAP サーバ証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。

例：`xConfiguration Login Remote LDAP CRLCheck: Peer`

xConfiguration Login Remote LDAP DirectoryType: <ActiveDirectory>

アクセスするLDAPディレクトリのタイプを定義します。デフォルトはActiveDirectoryです。

ActiveDirectory：ディレクトリは Windows Active Directory です。

例：`xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory`

xConfiguration Login Remote LDAP Encryption: <Off/TLS>

LDAP サーバへの接続に使用する暗号化を設定します。デフォルトは TLS です。

Off：暗号化は使用されません。

TLS：TLS 暗号化を使用します。

例：`xConfiguration Login Remote LDAP Encryption: Off`

xConfiguration Login Remote LDAP SASL: <None/DIGEST-MD5>

LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。デフォルトは DIGEST-MD5 です。

None：メカニズムを使用しません。

DIGEST-MD5：DIGEST-MD5 メカニズムを使用します。

例：`xConfiguration Login Remote LDAP SASL: DIGEST-MD5`

xConfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>

LDAP 認証のサブグループ検索深度レベルを設定します。デフォルト：16

例：`xConfiguration Login Remote LDAP SearchOptimize NestedDepth: "1"`

xConfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>

LDAP 認証用のグループを検索するときに、グループメンバールックアップをスキップするかどうかを定義します。デフォルト：[はい（Yes）]

例：`xConfiguration Login Remote LDAP SearchOptimize SkipMembers: "No"`

xConfiguration Login Remote LDAP Server Address: <S: 0,128>

LDAP クエリを実行するときに使用する LDAP サーバの IP アドレスまたは完全修飾ドメイン名を設定します。

例：`xConfiguration Login Remote LDAP Server Address: 「server.example.com」`

xConfiguration Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord>

LDAP サーバ アドレスが FQDN として指定されている場合の解決方法を定義します。デフォルトは AddressRecord です。

AddressRecord：DNS A レコードまたは AAAA レコード ルックアップ。

SRVRecord：DNS SRV レコード ルックアップ。SRV record：DNS SRV レコード ルックアップ。

例：`xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord`

xConfiguration Login Remote LDAP Server Port: <1..65534>

LDAP クエリを実行するときに使用する LDAP サーバの IP ポートを設定します。非セキュア接続は 389、セキュア接続は 636 を使用します。他のポートはサポートされていません。デフォルト：389。

例：`xConfiguration Login Remote LDAP Server Port: 389`

xConfiguration Login Remote LDAP VCS BindDN: <S: 0,255>

LDA Pサーバにバインドするときに使用するユーザの識別名を設定します。

例：`xConfiguration Login Remote LDAP VCS BindDN: 「systemmanager」`

xConfiguration Login Remote LDAP VCS BindPassword: <S: 0,122>

LDAP サーバにバインドするときに使用するパスワードを設定します。プレーン テキストの最大長は 60 文字で、暗号化されます。

例：`xConfiguration Login Remote LDAP VCS BindPassword: 「password123」`

xConfiguration Login Remote LDAP VCS BindUsername: <S: 0,255>

LDAP サーバにバインドするときに使用するユーザ名を設定します。SASL を使用する場合にのみ適用されます。

例：`xConfiguration Login Remote LDAP VCS BindUsername: 「systemmanager」`

Configuration Login Remote Protocol: <LDAP>

外部プロトコルに接続するために使用するプロトコル。デフォルトは LDAP です。

例：`xConfiguration Login Remote Protocol: LDAP`

xConfiguration Login Source Admin: <LocalOnly/RemoteOnly/Both>

アクセスが許可される前に管理者のログイン クレデンシャルを認証する場所を定義します。デフォルトは LocalOnly です。

LocalOnly：Expressway に保存されているローカルデータベースと照合してクレデンシャルを確認します。

RemoteOnly：Windows Active Directory などの外部クレデンシャルディレクトリと照合してクレデンシャルを確認します。これによって、デフォルトの admin アカウントを使用したログイン アクセスが無効になります。

Both：最初に Expressway に保存されているローカルデータベースと照合して確認し、一致するアカウントが見つからなかった場合は外部クレデンシャルディレクトリが代わりに使用されます。

例：`xConfiguration Login Source Admin: LocalOnly`

xConfiguration Login User [1..n] Name: <S: 0,60>

ローカル認証データベースにこのエントリの名前を定義します。

例：`xConfiguration Login User 1 Name: 「alice」`

xConfiguration Login User [1..n] Password: <S: 0,128>

ローカル認証データベースにこのエントリのパスワードを定義します。

例：`xConfiguration Login User 1 Password: 「abcXYZ_123」`

xConfiguration Management Interface HstsMode: <On/Off>

Web ブラウザがこのサーバへのアクセスにセキュアな接続のみを使用するように指示するかどうかを決定します。この機能を有効にすると、中間者（MITM）攻撃に対する保護が強化されます。デフォルトは On です。

On：Web サーバからのすべての応答は、有効期限が 1 年の Strict Transport Security ヘッダーが追加されて送信されます。

Off：Strict Transport Security ヘッダーは送信されず、ブラウザは通常どおりに動作します。
注：変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration Management Interface HstsMode: On`

xConfiguration Management Interface Port: <1..65535>

管理者が Expressway Web インターフェイスにアクセスするための https リスニング ポートを設定します。デフォルト：443。

例:`xConfiguration IPアドレス ポート:7443`

警告　ブラウザを使用して Expressway Web インターフェイスポートにアクセスできるかどうかを確認します。ブラウザが応答しない場合は、Webインターフェイスを使用して管理できないことを意味します。ネットワーク内のファイアウォールまたはその他のセキュリティ機器が指定されたポートをブロックしていないことを確認します。Webインターフェイスで提供されるポート（443、445、7443、9000）は、ほとんどのネットワークで機能する可能性があります。

xConfiguration Management Session InactivityTimeout: <0..65535>

管理セッション（シリアルポート、HTTPS、またはSSH）がタイムアウトになる前に、管理セッションが非アクティブになる期間（分）を設定します。セッション タイムアウトをオフにするには値を 0 に設定します。デフォルトは 30 です。

例：`xConfiguration Management Session InactivityTimeout: 30`

xConfiguration Management Session MaxConcurrentSessionsTotal: <0..65535>

システムで許可される同時管理者セッションの最大数。これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。値を 0 にすると、セッション制限はオフになります。デフォルト：[0]。

例：`xConfiguration Management Session MaxConcurrentSessionsTotal: 0`

xConfiguration Management Session MaxConcurrentSessionsUser: <0..65535>

個々の管理者アカウントがシステムで許可される同時セッションの数。これには、Web セッション、SSH セッション、およびシリアル セッションが含まれます。値を 0 にすると、セッション制限はオフになります。デフォルト：[0]。

例：`xConfiguration Management Session MaxConcurrentSessionsUser: 0`

xConfiguration NetworkLimits

機能を制限するまでレートを設定します。`xconfig networklimits ?` と入力して、ヘルプを確認する。

例：`xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5`

xConfiguration NTP Server [1..5] Address: <S: 0, 128>

システム時刻を同期するときに使用する最大 5 つの NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を設定します。

例：`xConfiguration NTP Server 1 Address: 「ntp.server.example.com」`

xConfiguration Option [1..64] Key: <S: 0, 90>

ソフトウェア オプションのオプション キーを指定します。これらのキーは、システムのキャパシティを引き上げるなど、特別な機能を追加するためにシステムに追加されます。詳細については、シスコのサポート担当者にお問い合わせください。

例：`xConfiguration Option 1 Key: 「1X4757T5-1-60BAD5CD」`

xConfiguration Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>

コール ポリシーの使用を有効または無効にします。デフォルト：Off

Off：コールポリシーを無効にします。

LocalCPL：アップロードした CPL ファイルのポリシーを使用します。

LocalService：グループポリシーの情報とローカルファイルを使用します。

PolicyService：外部ポリシーサービスを使用します。

例：`xConfiguration Policy AdministratorPolicy Mode: Off`

xConfiguration Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='403' reason='Service Unavailable'/> です。

例：`xConfiguration Policy AdministratorPolicy Service DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Policy AdministratorPolicy Service Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy AdministratorPolicy Service Password: 「password123」`

xConfiguration Policy AdministratorPolicy Service Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Policy AdministratorPolicy Service Path: 「service」`

xConfiguration Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Policy AdministratorPolicy Service Protocol: HTTPS`

xConfiguration Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy AdministratorPolicy Service Server 1 Address: 「service.server.example.com」`

xConfiguration Policy AdministratorPolicy Service Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Policy AdministratorPolicy Service Status Path: status`

xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On`

xConfiguration Policy AdministratorPolicy Service UserName: <S: 0,30>

リモート ポリシー サービスにログインして照会するために Expressway が使用するユーザ名を指定します。

例：`xConfiguration Policy AdministratorPolicy Service UserName: 「user123」`

xConfiguration Policy FindMe CallerID: <FindMeID/IncomingID>

着信コールの発信元が呼び出し先にどのように表示されるかを決定します。デフォルトは IncomingID です。

IncomingID：コールが発信されたエンドポイントのアドレスを表示します。

FindMeID：発信エンドポイントのアドレスに関連付けられた FindMe ID を表示します。

例：`xConfiguration Policy FindMe CallerId: FindMeID`

xConfiguration Policy FindMe Mode: <Off/On/ThirdPartyManager>

FindMe アプリケーションの動作方法を設定します。デフォルトは Off です。

Off：FindMe を無効にします。

On：FindMe を有効にします。

ThirdPartyManager：オフボックスのサードパーティ製 FindMe マネージャを使用します。

例：`xConfiguration Policy FindMe Mode: On`

xConfiguration Policy FindMe Server Address: <S: 0, 128>

リモート FindMe マネージャの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy FindMe Server Address: 「userpolicy.server.example.com」`

xConfiguration Policy FindMe Server Password: <S: 0, 82>

リモート FindMe マネージャにログインして照会するために Expressway が使用するパスワードを指定します。プレーンテキストの最大長は30文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy FindMe Server Password: 「password123」`

xConfiguration Policy FindMe Server Path: <S: 0, 255>

リモート FindMe マネージャの URL を指定します。

例：`xConfiguration Policy FindMe Server Path: 「service」`

xConfiguration Policy Services Service [1..20] DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='504' reason='Policy Service Unavailable'/> です。

例：`xConfiguration Policy Services Service 1 DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Policy Services Service [1..20] Description: <S: 0,64>

自由形式のポリシー サービスの説明。

例：`xConfiguration Policy Services Service 1 Description: 「Conference management service」`

xConfiguration Policy Services Service [1..20] HTTPMethod: <POST/GET>

リモート サービスに使用する HTTP 方式のタイプを指定します。デフォルトは POST です。

例：`xConfiguration Policy Services Service 1 HTTPMethod: POST`

xConfiguration Policy Services Service [1..20] Name: <S: 0,50>

このサービス ポリシーに名前を割り当てます。

例：`xConfiguration Policy Services Service 1 Name: 「Conference handler」`

xConfiguration Policy Services Service [1..20] Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Policy Services Service 1 Password: 「password123」`

xConfiguration Policy Services Service [1..20] Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Policy Services Service 1 Path: 「service」`

xConfiguration Policy Services Service [1..20] Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Policy Services Service 1 Protocol: HTTPS`

xConfiguration Policy Services Service [1..20] Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Policy Services Service 1 Server 1 Address: 「192.168.0.0」`

xConfiguration Policy Services Service [1..20] Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Policy Services Service 1 Status Path: status`

xConfiguration Policy Services Service [1..20] TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off`

xConfiguration Policy Services Service [1..20] TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Policy Services Service 1 TLS Verify Mode: On`

xConfiguration Policy Services Service [1..20] UserName: <S: 0,30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

例：`xConfiguration Policy Services Service 1 UserName: 「user123」`

xConfiguration QoS Audio <0..63>

音声トラフィックの QoS マーキング用の DSCP（Differentiated Service Code Point）の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のオーディオ メディア トラフィックに、IP パケット ヘッダーにそれを記述することによってスタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：46。

変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration QoS Audio: 30`

xConfiguration QoS Video <0..63>

ビデオ トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のビデオ メディア トラフィックに、IP パケット ヘッダーにそれを記述することによって スタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：34。

変更を有効にするには、システムを再起動する必要があります。

例:`xConfigurationのQoSのビデオ:43`

xConfiguration QoS XMPP <0..63>

IM & Presence トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる XMPP トラフィックに、IP パケット ヘッダーにそれを記述することによって スタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：24。

変更を有効にするには、システムを再起動する必要があります。

例:`xConfiguration QoS XMPP:34`

xConfiguration QoS Signaling <0..63>

シグナリング トラフィックの QoS マーキング用の DSCP の値を定義します。DSCP 値は、Expressway を介してルーティングされる SIP と H.323 のシグナリング トラフィックに、IP パケット ヘッダーにそれを記述することによってスタンプ（マーク）されます。IPv4 の場合は ToS フィールド、IPv6 の場合は TC フィールドに書き込まれます。値「「0」」は、標準のベストエフォートサービスを指定します。デフォルト：24。

変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration QoS Signaling: 34`

xConfiguration Registration AllowList [1..2500] Description: <S: 0,64>

自由形式の許可リスト ルールの説明。

例：`xConfiguration Registration AllowList 1 Description: "Everybody at @example.com"`

xConfiguration Registration AllowList [1..2500] Pattern String: <S: 0, 60>

許可リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが許可リストのパターンの 1 つと一致した場合に登録が許可されます。

例：`xConfiguration Registration AllowList 1 Pattern String: 「john.smith@example.com」`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

Prefix：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

Prefix：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration DenyList [1..2500] Description: <S: 0,64>

自由形式の拒否リスト ルールの説明。

例：`xConfiguration Registration DenyList 1 Description: 「Anybody at @nuisance.com」`

xConfiguration Registration DenyList [1..2500] Pattern String: <S: 0, 60>

拒否リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが拒否リストのパターンの 1 つと一致した場合は登録が許可されません。

例：`xConfiguration Registration DenyList 1 Pattern String: 「john.jones@example.com」`

xConfiguration Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

拒否リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。デフォルトは Exact です。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

Prefix：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Registration DenyList 1 Pattern Type: Exact`

xConfiguration Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService>

システムに登録できるエンドポイントを決定するときに使用するポリシーを指定します。デフォルト：[None]。

None：制限はありません。

AllowList：許可リストに設定されたエイリアスに登録しようとしているエンドポイントのみが登録できます。

DenyList：拒否リストに設定されたエイリアスに登録しようとしているエンドポイントを除くすべてのエンドポイントが登録できます。

Directory：ローカルディレクトリ内にあるエイリアスを登録するエンドポイントのみが登録できます。

PolicyService：ポリシーサービスで許可されている詳細で登録するエンドポイントのみが登録できます。

例：`xConfiguration Registration RestrictionPolicy Mode: None`

xConfiguration Registration RestrictionPolicy Service DefaultCPL: <S: 0,255>

リモート サービスが使用できない場合に Expressway が使用する CPL。デフォルトは <reject status='504' reason='Policy Service Unavailable'/> です。

例：`xConfiguration Registration RestrictionPolicy Service DefaultCPL: 「<reject status='403' reason='Service Unavailable'/>」`

xConfiguration Registration RestrictionPolicy Service Password: <S: 0,82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワードを指定します。プレーン テキストの最大長は 30 文字で、これらの文字は暗号化されます。

例：`xConfiguration Registration RestrictionPolicy Service Password: 「password123」`

Configuration Registration RestrictionPolicy Service Path: <S: 0,255>

リモート サービスの URL を指定します。

例：`xConfiguration Registration RestrictionPolicy Service Path: 「service」`

xConfiguration Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS>

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

例：`xConfiguration Registration RestrictionPolicy Service Protocol: HTTPS`

xConfiguration Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128>

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

例：`xConfiguration Registration RestrictionPolicy Service Server 1 Address: 「192.168.0.0」`

xConfiguration Registration RestrictionPolicy Service Status Path: <S: 0..255>

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

例：`xConfiguration Registration RestrictionPolicy Service Status Path: status`

xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: <On/Off>

ポリシー サービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

例：`xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: <On/Off>

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

例：`xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On`

xConfiguration Registration RestrictionPolicy Service UserName: <S: 0,30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

例：`xConfiguration Registration RestrictionPolicy Service UserName: 「user123」`

xConfiguration Remote Syslog [1..4] Address: <S: 0..128>

ログを書き込む最大 4 つのリモート syslog サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。これらのサーバは、BSD または IETF syslog プロトコルをサポートしている必要があります。

例：`xConfiguration Remote Syslog 1 Address: 「remote_server.example.com」`

xConfiguration Remote Syslog [1..4] Crlcheck: <On/Off>

syslog サーバが提供する証明書を証明書失効リスト（CRL）と照合して確認するかどうかを制御します。デフォルトは Off です。

例：`xConfiguration Remote Syslog 1 Crlcheck: Off`

xConfiguration Remote Syslog [1..4] Format: <bsd/ietf>

リモート syslog メッセージが作成される形式。デフォルトは bsd です。

例：`xConfiguration Remote Syslog 1 Format: bsd`

xConfiguration Remote Syslog [1..4] Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

この syslog サーバに送信するログ メッセージの最小シビラティ（重大度）を選択します。デフォルトは informational です。

例：`xConfiguration Remote Syslog 1 Loglevel: informational`

xConfiguration Remote Syslog [1..4] Mode: <bsd/ietf/ietf_secure/user_defined>

syslog サーバにメッセージを送信するときに使用する syslog プロトコルを選択します。または、user_defined を選択してトランスポート タイプ、ポート、および形式を個々に設定します。デフォルトは bsd です。

例：`xConfiguration Remote Syslog 1 Mode: bsd`

xConfiguration Remote Syslog [1..4] Port: <1..65535>

使用する UDP/TCP 宛先ポート。推奨されるポート：UDP=514 TCP/TLS=6514 デフォルト：514。

例：`xConfiguration Remote Syslog 1 Port: 514`

xConfiguration Remote Syslog [1..4] Transport: <udp/tcp/tls>

syslog サーバと通信するときに使用するトランスポート プロトコル。TLS 暗号化を使用する場合、適切な CA 証明書ファイルをアップロードする必要があります。デフォルトは UDP です。

例：`xConfiguration Remote Syslog 1 Transport: udp`

xConfiguration ResourceUsage Warning Activation Level: <0..100>

コール数または登録数がライセンス供与された最大キャパシティに到達していることを Expressway がいつどのような場合に警告するかを制御します。この数は、到達したときに警告をトリガーする最大数のパーセンテージを表します。0：警告は表示されません。デフォルト：90。

例：`xConfiguration ResourceUsage Warning Activation Level: 90`

xConfiguration SIP Advanced BibInviteDelay: <1..5000>

サーバーが処理する必要がある SIP BIB 招待メッセージの最大遅延を指定します（ミリ秒単位）。

デフォルト：0

例：`xConfiguration SIP Advanced BibInviteDelay: 1000`

xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>

SIP REFER メッセージの最大遅延を指定します。これには、サーバーが処理できる (ミリ秒単位で) 最初の通話ダイアログ中に DtLineBusyTone が含まれます (SIP メッセージが順番に処理されるようにします)。

Expressway は、SIP メッセージ（REFER には DtLineBusyTone パラメータと 183 Session Progress が含まれます）を処理して送信します。これにより、Jabber Over MRA が話中音の代わりに断続的に呼び出し音を再生します

デフォルト：0

遅延を 100 ～ 200 ミリ秒に調整することをお勧めします。

例：`xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>`

xConfiguration SIP Advanced SipMaxSize: <1..1048576>

サーバで処理できる SIP メッセージの最大サイズ（バイト単位）を指定します。デフォルトは `32768` です。

例：`xConfiguration SIP Advanced SipMaxSize: 32768`

xConfiguration SIP Advanced SipTcpConnectTimeout: <1..150>

発信 SIP TCP 接続が確立されるまで待機する最大秒数を入力します。デフォルトは 10 です。

例：`xConfiguration SIP Advanced SipTcpConnectTimeout: 10`

xConfiguration SIP Advanced SipTlsDhKeySize: <1024/2048/3072>

Diffie-Hellmanキー交換を使用する着信接続にデフォルト キーのサイズを指定します（ビット）。

デフォルト：1024。

（注）　変更を有効にするには、システムを再起動する必要があります。

例：`xConfiguration SIP Advanced SipTlsDhKeySize: 1024`

xConfiguration SIP Advanced SipTlsVersions: <TLSv1/TLSv1.1/TLSv1.2/TLSv1:TLSv1.1/TLSv1:TLSv1.2/TLSv1.1:TLSv1.2/TLSv1:TLSv1.1:TLSv1.2>

サポートされる SIP TLS プロトコル バージョンを指定します。デフォルト:TLSv1:TLSv1.1:TLSv1.2

例：`xConfiguration SIP Advanced SipTlsVersions: TLSv1.1:TLSv1.2`

xConfiguration SIP Authentication Digest Nonce ExpireDelta: <30..3600>

nonce を再利用できる最大時間（秒単位）を指定します。デフォルトは 300 です。

例：`xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300`

xConfiguration SIP Authentication Digest Nonce Length: <32..512>

SIP ダイジェスト認証で使用するために生成する nonce または cnonce の長さ。デフォルトは 60 です。

例：`xConfiguration SIP Authentication Digest Nonce Length: 60`

xConfiguration SIP Authentication Digest Nonce Limit: <1..65535>

保存する nonce の数の最大限度。デフォルト：10000。

例：`xConfiguration SIP Authentication Digest Nonce Limit: 10000`

xConfiguration SIP Authentication Digest Nonce Maximum Use Count: <1..1024>

Expressway が生成する nonce をクライアントが使用できる最大回数。デフォルト：128。

例：`xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`

xConfiguration SIP Authentication NTLM Mode: <On/Off/Auto>

NTLM プロトコルを使用して Expressway がエンドポイントにいつチャレンジするかを制御します。デフォルトは Auto です。

Off：Expressway は NTLM プロトコルを含むチャレンジを送信しません。

On：Expressway は常に NTLM をチャレンジに組み込みます。

Auto：Expressway はエンドポイントのタイプに基づいて NTLM でチャレンジするかどうかを決定します。

例：`xConfiguration SIP Authentication NTLM Mode: Auto`

xConfiguration SIP Authentication NTLM SA Lifetime: <30..43200>

NTLM セキュリティ アソシエーションのライフタイムを秒単位で指定します。デフォルト：28800。

例：`xConfiguration SIP Authentication NTLM SA Lifetime: 28800`

xConfiguration SIP Authentication NTLM SA Limit: <1..65535>

保存する NTLM セキュリティ アソシエーションの最大数。デフォルトは 10000 です。

例：`xConfiguration SIP Authentication NTLM SA Limit: 10000`

xConfiguration SIP Authentication Retry Limit: <1..16>

403 Forbidden 応答を受信する前に、認証の失敗によって SIP UA がチャレンジする回数。これが SIP ダイジェストのチャレンジ（NTLM 以外のチャレンジ）のみにみ適用されます。デフォルトは 3 です。

例：`xConfiguration SIP Authentication Retry Limit: 3`

xConfiguration SIP Domain [1..200] Authzone: <S: 0,128>

このドメインの SIP メッセージのクレデンシャル チェックを委任するときに使用するトラバーサル ゾーン。

例：`xConfiguration SIP Domain 1 Authzone: 「traversalzone」`

xConfiguration SIP Domain [1..200] Edge: <On/Off>

リモートおよびモバイルのコラボレーション機能が有効かどうか。デフォルトは Off です。

例：`xConfiguration SIP Domain 1 Edge: On`

xConfiguration SIP Domain [1..200] Name: <S: 0,128>

この Expressway が権限を持つドメインを指定します。ドメイン名は複数のレベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。有効なドメインの例としては、「100.example-name.com」 などがあります。

例：`xConfiguration SIP Domain 1 Name: 「100.example-name.com」`

xConfiguration SIP Domain [1..200] Sip: <On/Off>

Expressway はこのドメインの SIP レジストラとして機能し、このドメインを含むエイリアスで登録を試みるすべての SIP エンドポイントの登録要求を受け入れるかどうかを指定します。デフォルトは On です。

例：`xConfiguration SIP Domain 1 Sip: On`

xConfiguration SIP GRUU Mode: <On/Off>

GRUU（RFC5627）サポートがアクティブかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP GRUU Mode: On`

xConfiguration SIP MediaRouting ICE Mode: <On/Off>

ICE 参加者が NAT デバイスの背後まで通過する場合に ICE から ICE 以外のコールのメディアを Expressway が取得するかどうかを制御します。デフォルトは Off です。

例：`xConfiguration SIP MediaRouting ICE Mode: Off`

xConfiguration SIP Mode: <On/Off>

Expressway が SIP レジストラと SIP プロキシの機能を提供するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP Mode: On`

xConfiguration SIP PreRoutedRouteHeader: <S:0,128>

事前にルーティングした新しいルートヘッダーパスの通過を許可する要求メッセージを制御します。

X12.5 と同様に、このフラグは SIP REGISTER メッセージに対してのみ使用できます。

例：`xConfiguration SIP PreRoutedRouteHeader: 「REGISTER」`

xConfiguration SIP Registration Call Remove: <Yes/No>

SIP 登録の期限が切れか、または削除されたときに、関連付けられたコールをドロップするかどうかを指定します。デフォルトは No です。

例：`xConfiguration SIP Registration Call Remove: No`

xConfiguration SIP Registration Mode: <Off/On>

Expressway が SIP 登録を提供するかどうかを決定します。デフォルトは On です。

例：`xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Outbound Flow Timer: <0..600>

アウトバウンド登録応答内の Flow-Timer ヘッダーの値を指定します。ユーザエージェントがキープアライブを送信していない場合に、サーバが登録フローが終了したと見なした後の秒数を定義します。デフォルトは 0 です（ヘッダーは追加されません）。

例：`xConfiguration SIP Registration Outbound Flow Timer: 0`

xConfiguration SIP Registration Outbound Refresh Maximum: <30..7200>

アウトバウンド登録の SIP 登録更新期間の最大許容値。これよりも大きな値の要求には、小さな値（[アウトバウンド登録更新戦略（Outbound registration refresh strategy）] に従って計算されます）が返されることになります。デフォルトは 3600 秒です。

例：`xConfiguration SIP Registration Outbound Refresh Maximum: 3600`

xConfiguration SIP Registration Outbound Refresh Minimum: <30..7200>

アウトバウンド登録についての SIP 登録更新期間の最小許容値。この値よりも小さな値の要求は、「423 Interval Too Brief」応答で登録が拒否されます。デフォルトは 300 秒です。

例：`xConfiguration SIP Registration Outbound Refresh Minimum: 300`

onfiguration SIP Registration Outbound Refresh Strategy: <Maximum/Variable>

アウトバウンド登録についての SIP 登録有効期限の生成に使用する方法。デフォルトは Variable です。

Maximum：設定した最大更新値と登録で要求された値のうちの小さいほうを使用します。

Variable：設定した最小更新値と、設定した最大更新値と登録で要求された値のいずれか小さいほうの値の間でランダム値を生成します。

例：`xConfiguration SIP Registration Outbound Refresh Strategy: Variable`

xConfiguration SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

プロキシ登録をどのように処理するかを指定します。デフォルトは Off です。

Off：登録要求はプロキシ経由で送信されません。

ProxyToKnownOnly：登録要求はプロキシ経由でネイバーのみに送信されます。

ProxyToAny：登録要求は、Expressway の既存のコール処理ルールに従ってプロキシ経由で送信されます。

例：`xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Standard Refresh Maximum: <30..7200>

標準的な登録についての SIP 登録更新期間の最大許容値。これよりも大きな値の要求では小さな値が返されることになります。その値は、標準的な登録更新戦略に従って計算されます。デフォルトは 60 秒です。

例：`xConfiguration SIP Registration Standard Refresh Maximum: 60`

xConfiguration SIP Registration Standard Refresh Minimum: <30..3600>

標準的な登録についての SIP 登録更新期間の最小許容値。この値よりも小さな値の要求は、「423 Interval Too Brief」応答で登録が拒否されます。デフォルトは 45 秒です。

例：`xConfiguration SIP Registration Standard Refresh Minimum: 45`

xConfiguration SIP Registration Standard Refresh Strategy: <Maximum/Variable>

標準的な登録についての SIP 登録有効期限の生成に使用する方法。デフォルトは Maximum です。

Maximum：設定した最大更新値と登録で要求された値のうちの小さいほうを使用します。

Variable：設定した最小更新値と、設定した最大更新値と登録で要求された値のいずれか小さいほうの値の間でランダム値を生成します。

例：`xConfiguration SIP Registration Standard Refresh Strategy: Maximum`

xConfiguration SIP Require Duo Video Mode: <On/Off>

Expressway でサポートするエンドポイントに com.tandberg.sdp.duo.enable 拡張子を使用する必要があるかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP Require Duo Video Mode: On`

xConfiguration SIP Require UDP BFCP Mode: <On/Off>

Expressway でサポートするエンドポイントに com.tandberg.udp.bfcp 拡張子を使用する必要があるかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP Require UDP BFCP Mode: On`

xConfiguration SIP Routes Route [1..20] Address: <S:0,39>

一致している SIP 要求が転送されるこのルートのネクスト ホップの IP アドレスを指定します。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`

xConfiguration SIP Routes Route [1..20] Authenticated: <On/Off>

認証した要求を転送するかどうか。デフォルトは Off です。注：このコマンドは、開発者のみが使用できます。

On：着信メッセージが認証されている場合にのみ、要求をルートに転送します。

Off：このルートに一致するメッセージを常に転送します。

例：`xConfiguration SIP Routes Route 1 Authenticated: On`

xConfiguration SIP Routes Route [1..20] Header Name: <S:0,64>

照合する SIP ヘッダー フィールドの名前（Event など）。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Header Name: "Event"`

xConfiguration SIP Routes Route [1..20] Header Pattern: <S:0,128>

指定した SIP ヘッダー フィールドと照合する正規表現。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Header Pattern: 「(my-event-package)(.*)」`

xConfiguration SIP Routes Route [1..20] Method: <S:0,64>

このルートを選択するために照会する SIP メソッド（INVITE、SUBSCRIBE など）。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Method: 「SUBSCRIBE」`

xConfiguration SIP Routes Route [1..20] Port: <1..65534>

一致している SIP 要求がルーティングされるこのルートのネクスト ホップ上のポートを指定します。デフォルトは 5060 です。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Port: 22400`

xConfiguration SIP Routes Route [1..20] Request Line Pattern: <S:0,128>

SIP 要求の行と照合する正規表現。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Request Line Pattern: 「.*@(%localdomains%|%ip%)」`

xConfiguration SIP Routes Route [1..20] Tag: <S:0,64>

作成するルートを識別するために外部アプリケーションが指定したタグ値。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Tag: 「Tag1」`

xConfiguration SIP Routes Route [1..20] Transport: <UDP/TCP/TLS>

このルートに転送された SIP メッセージに使用するトランスポート タイプを決定します。デフォルトは TCP です。注：このコマンドは、開発者のみが使用できます。

例：`xConfiguration SIP Routes Route 1 Transport: TCP`

xConfiguration SIP Service SipRegistrationMode: <Off/On>

Expressway が SIP サービス登録を提供するかどうかを決定します。デフォルトは On です。

例：`xConfiguration SIP Service SipRegistrationMode: Off`

重要　次のコマンドは、バージョン X14.0.1 で廃止されました。

`xConfiguration SIP Registration Mode: <Off/On>`

xConfiguration SIP Session Refresh Minimum: <90..7200>

SIP コールのセッション更新間隔を Expressway がネゴシエートする最小値。詳細については、RFC 4028 の Min-SE ヘッダーの定義を参照してください。デフォルトは 500 です。

例：`xConfiguration SIP Session Refresh Minimum: 500`

xConfiguration SIP Session Refresh Value: <90..86400>

SIP コールのセッション更新要求間に許容される最大時間。詳細については、RFC 4028 の Session-Expires の定義を参照してください。デフォルトは 1800 です。

例：`xConfiguration SIP Session Refresh Value: 1800`

xConfiguration SIP TCP Mode: <On/Off>

TCP プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP TCP Mode: On`

xConfiguration SIP TCP Outbound Port End: <1024..65534>

アウトバウンド TCP/TLS SIP 接続で使用する範囲内の上位ポートを指定します。デフォルトは 29999 です。

例：`xConfiguration SIP TCP Outbound Port End: 29999`

xConfiguration SIP TCP Outbound Port Start: <1024..65534>

アウトバウンド TCP/TLS SIP 接続で使用する範囲内の下位ポートを指定します。デフォルトは 25000 です。

例：`xConfiguration SIP TCP Outbound Port Start: 25000`

xConfiguration SIP TCP Port: <1024..65534>

着信 SIP TCP コールのリスニング ポートを指定します。デフォルトは 5060 です。

例：`xConfiguration SIP TCP Port: 5060`

xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: <On/Off>

証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。CRL は Expressway に手動でダウンロードするか、または事前に設定された URI から自動的にダウンロードするか、あるいは X.509 証明書に含まれた CRL 配布ポイント（CDP）URI から自動的にダウンロードすることができます。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: <On/Off>

X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Mode: <On/Off>

失効確認が SIP TLS 接続の確立時に交換された証明書に対し実行されるかどうかを制御します。デフォルトは Off です。

例：`xConfiguration SIP TLS Certificate Revocation Checking Mode: Off`

xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: <On/Off>

Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。OCSP を使用するには、チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。デフォルトは On です。

例：`xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: <Ignore/Fail>

失効の送信元に接続できない場合の失効確認動作を制御します。デフォルトは Fail です。

Fail：失効しているものとして証明書を処理します（したがって、TLS 接続は許可しません）。

Ignore：失効していないものとして証明書を処理します。

例：`xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: Fail`

xConfiguration SIP TLS Mode: <On/Off>

TLS プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは On です。

例：`xConfiguration SIP TLS Mode: On`

xConfiguration SIP TLS Port: <1024..65534>

着信 SIP TLS コールのリスニング ポートを指定します。デフォルトは 5061 です。

例：`xConfiguration SIP TLS Port: 5061`

xConfiguration SIP UDP Mode: <On/Off>

UDP プロトコルを使用した着信 SIP コールと発信 SIP コールを許可するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration SIP UDP Mode: On`

xConfiguration SIP UDP Port: <1024..65534>

着信 SIP UDP コールのリスニング ポートを指定します。デフォルト：5060。

例：`xConfiguration SIP UDP Port: 5060`

xConfiguration SNMP CommunityName: <S: 0, 16>

Expressway の SNMP コミュニティ名。デフォルト：public

例：`xConfiguration SNMP CommunityName: 「public」`

xConfiguration SNMP SystemContact: <S: 0, 70>

Expressway の問題についての問い合わせが可能な担当者の名前。デフォルトは Administrator です。

例：`xConfiguration SNMP SystemContact: Administrator`

xConfiguration SNMP SystemLocation: <S: 0, 70>

The physical location of the system.

例：`xConfiguration SNMP SystemLocation: 「Server Room 128」`

xConfiguration SNMP V1Mode: <On/Off>

SNMP バージョン 1 のサポートを有効または無効にします。デフォルトは Off です。

例：`xConfiguration SNMP V1Mode: Off`

xConfiguration SNMP V2cMode: <On/Off>

SNMP バージョン 2c のサポートを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V2cMode: On`

xConfiguration SNMP V3AuthenticationMode: <On/Off>

SNMP バージョン 3 の認証を有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V3AuthenticationMode: On`

xConfiguration SNMP V3AuthenticationPassword: <S: 0,215>

SNMP バージョン 3 の認証パスワードを設定します。パスワードは 8 文字以上にする必要があります。

例：`xConfiguration SNMP V3AuthenticationPassword: 「password123」`

xConfiguration SNMP V3Mode: <On/Off>

SNMP バージョン 3 のサポートを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMPV3 Mode: On`

xConfiguration SNMP V3PrivacyMode: <On/Off>

SNMP バージョン 3 のプライバシーを有効または無効にします。デフォルトは On です。

例：`xConfiguration SNMP V3PrivacyMode: On`

xConfiguration SNMP V3PrivacyPassword: <S: 0,215>

SNMP バージョン 3 のプライバシー パスワードを設定します。パスワードは 8 文字以上にする必要があります。

例：`xConfiguration SNMP V3PrivacyPassword: 「password123」`

xConfiguration SNMP V3PrivacyType: <AES>

SNMP バージョン 3 のプライバシー タイプを設定します。デフォルトは AES です。

例：`xConfiguration SNMP V3PrivacyType: AES`

xConfiguration SNMP V3UserName: <S: 0,70>

SNMP V3 を使用するときに使用するユーザ名を設定します。

例：`xConfiguration SNMP V3UserName: 「user123」`

xConfiguration SystemUnit Maintenance Mode: <On/Off>

メンテナンスモードにExpresswayを設定します。新しいコールと登録は拒否され、既存のコールと登録は期限切れにできます。デフォルトは Off です。

例：`xConfiguration SystemUnit Maintenance Mode: Off`

xConfiguration SystemUnit Name: <S:, 0, 50>

Expresswayの名前を定義します。システム名は Web インターフェイスのさまざまな場所やユニットの前面パネルに表示されます。システムを一意に識別する名前を選択します。

例：`xConfiguration SystemUnit Name: 「MainHQ」`

xConfiguration TimeZone Name: <S: 0, 64>

Expressway のローカル タイム ゾーンを設定します。タイム ゾーンの名前は、POSIX 命名規則（Europe/London や America/New_York など）に従います。デフォルトは GMT です。

例：`xConfiguration TimeZone Name: 「GMT」`

xConfiguration Transform [1..100] Description: <S: 0,64>

自由形式のトランスフォーメーションの説明。

例：`xConfiguration Transform [1..100] Description: 「Change example.net to example.com」`

xConfiguration Transform [1..100] Pattern Behavior: <Strip/Replace>

エイリアスをどのように変更するかを示します。デフォルトは Strip です。

Strip：一致しているプレフィックスまたはサフィックスをエイリアスから削除します。

Replace：置換文字列内のテキストでエイリアスの一致している部分を置換します。

AddPrefix：エイリアスの前に置換文字列を追加します。

AddSuffix：エイリアスの後ろに置換文字列を追加します。

例：`xConfiguration Transform 1 Pattern Behavior: Replace`

xConfiguration Transform [1..100] Pattern Replace: <S: 0, 60>

選択したパターン動作とともに使用するテキスト文字列。

例：`xConfiguration Transform 1 Pattern Replace: 「example.com」`

xConfiguration Transform [1..100] Pattern String: <S: 0, 60>

エイリアスと比較するパターン。

例：`xConfiguration Transform 1 Pattern String: 「example.net」`

Configuration Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

適用するトランスフォーメーションで、パターン文字列をエイリアスとどのように照合するか。デフォルトは Prefix です。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Transform 1 Pattern Type: Suffix`

xConfiguration Transform [1..100] Priority: <1..65534>

指定したトランスフォーメーションにプライオリティを割り当てます。トランスフォーメーションはプライオリティ順に着信メッセージと比較されます。また、プライオリティはトランスフォーメーションごとに一意である必要があります。デフォルトは 1 です。

例：`xConfiguration Transform 1 Priority: 10`

xConfiguration Transform [1..100] State: <Enabled/Disabled>

トランスフォーメーションが有効になっているか、無効になっているかを示します。無効になっているトランスフォーメーションは無視されます。

例：`xConfiguration Transform 1 State: Enabled`

xConfiguration Traversal Media Port End: <1025..65533>

トラバーサル コールでは（Expressway がシグナリングとともにメディアも取得する）、メディアに使用する範囲の上位ポートを指定します。ポートはこの範囲からペアで割り当てられ、各ペアの最初は偶数になります。したがって、この範囲は奇数で終了する必要があります。デフォルトは 59999 です。

例：`xConfiguration Traversal Media Port End: 59999`

xConfiguration Traversal Media Port Start: <1024..65532>

トラバーサル コールでは（Expressway がシグナリングとともにメディアも取得する）、メディアに使用する範囲の下位ポートを指定します。ポートはこの範囲からペアで割り当てられ、各ペアの最初は偶数になります。したがって、この範囲は偶数で始まる必要があります。デフォルトは 36000 です。

例：`xConfiguration Traversal Media Port Start: 36000`

xConfiguration Traversal Server H323 Assent CallSignaling Port: <1024..65534>

Assent シグナリングに使用する Expressway 上のポート。デフォルトは 2776 です。

例：`xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

xConfiguration Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

H460.18 シグナリングに使用する Expressway 上のポート。デフォルトは 2777 です。

例：`xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`

xConfiguration Traversal Server TURN Authentication Realm: <S: 1,128>

認証チャレンジでサーバが送信するレルム。デフォルトは TANDBERG です。

例：`xConfiguration Traversal Server TURN Authentication Realm: 「TANDBERG」`

xConfiguration Traversal Server TURN Authentication Remote Mode: <On/Off>

サーバが要求を認証する必要があるかどうかを決定します。有効にすると、サーバはその応答も認証します。デフォルトは On です。

例：`xConfiguration Traversal Server TURN Authentication Remote Mode: On`

xConfiguration Traversal Server TURN Media Port End: <1024..65534>

TURN リレーに使用する範囲の上位ポート。デフォルトは 61799 です。

例：`xConfiguration Traversal Server TURN Media Port End: 61799`

xConfiguration Traversal Server TURN Media Port Start: <1024..65534>

TURN リレーに使用する範囲の下位ポート。デフォルトは 60000 です。

例：`xConfiguration Traversal Server TURN Media Port Start: 60000`

xConfiguration Traversal Server TURN Mode: <On/Off>

Expressway が TURN サービスをトラバーサル クライアントに提供するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration Traversal Server TURN Mode: Off`

xConfiguration Traversal Server TURN Port: <1024..65534>

TURN 要求のリスニング ポート。デフォルトは 3478 です。

例：`xConfiguration Traversal Server TURN Port: 3478`

xConfiguration Traversal Server TURN PortRangeEnd: <1024..65534>

TURN 要求に使用する範囲の上位ポート。デフォルトは 3483 です。

例：`xConfiguration Traversal Server TURN PortRangeEnd: 3483`

xConfiguration Traversal Server TURN PortRangeStart: <1024..65534>

TURN 要求に使用する範囲の下位ポート。デフォルトは 3478 です。

例：`xConfiguration Traversal Server TURN PortRangeStart: 3478`

Configuration Traversal Server TURN ProtocolMode: <TCP/UDP/Both>

TURN 要求に許可されたプロトコル。デフォルトは [両方（Both）] です。

例：`xConfiguration Traversal Server TURN ProtocolMode: Both`

xConfiguration xConfiguration Traversal Server TURN Authentication Mode: <On/Off>>

サーバで要求の認証を必要とするかどうかを指定します。有効にすると、サーバはその応答も認証します。デフォルトは On です。

例：`xConfiguration Traversal Server TURN Authentication Mode: On`

xConfiguration XCP Config FcmService: <On/Off>

MRA を使用した Jabber Android デバイスの FCM プッシュ通知を有効にするかどうかを制御します。デフォルトは Off です。

例：`xConfiguration XCP Config FcmService: On`

xConfiguration XCP DelayedRestart EnableDelayedRestart: <On/Off>

Cisco XCP ルータの遅延再起動機能が有効かどうかを制御します。デフォルトは Off です。

例：`xConfiguration DelayedRestart EnableDelayedRestart: On`

xConfiguration XCP DelayedRestart EnableScheduledRestart: <On/Off>

Cisco XCP ルータのスケジュール設定された再起動が有効かどうかを制御します。デフォルトは Off です。

例：`xConfiguration XCP DelayedRestart EnableScheduledRestart: On`

xConfiguration XCP DelayedRestart MultitenancyEnabled: <On/Off>

マルチテナンシーをオンにして、Cisco XCP ルータの遅延再起動を設定します。デフォルトは Off です。

例：`xConfiguration XCP DelayedRestart MultitenancyEnabled: On`

xConfiguration XCP DelayedRestart ScheduledTime:

スケジュール設定された再起動が実行される毎日の時刻。

例：`xConfiguration XCP DelayedRestart ScheduledTime: 01.00`

xConfiguration XCP DelayedRestartNotify RestartTime:

再起動時間の通知を設定します。

例：`xConfiguration DelayedRestartNotify RestartTime: 01.00`

xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: <On/Off>

証明書失効リスト（CRL）を XCP TLS 接続の証明書失効確認を実行するために使用するかどうかを制御します。OCSP の使用に加えて、CRL は Expressway に手動でダウンロードするか、または事前に設定された URI から自動的にダウンロードするか、あるいは X.509 証明書に含まれた CRL 配布ポイント（CDP）URI から自動的にダウンロードすることができます。デフォルトは Off です。

例：`xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: Off`

xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: <On/Off>

Expressway が証明書の確認のために自動的に XCP ピアの IP アドレスを FQDN に変換するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On`

xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off>

Expressway にその X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: On`

xConfiguration XCP TLS Certificate CVS EnableCvs: <On/Off>

XCP TLS 接続時に XCP ピアの証明書を確認するかどうかを制御します。*Off* にすると、そのほかすべての XCP TLS 証明書 CVS の設定オプションが無効になります。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS EnableCvs: On`

xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: <On/Off>

失効の送信元に接続できない場合の証明書の確認動作を制御します。

On：失効しているものとして証明書を処理します（したがって、TLS接続は許可しません）。

Off：失効していないものとして証明書を処理します。

デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: On`

xConfiguration XCP TLS Certificate CVS UseCrl: <On/Off>

XCP TLS 接続の確立時に交換される証明書の失効について、Expressway が自身の CRL を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS UseCrl: On`

xConfiguration XCP TLS Certificate CVS UseOcsp: <On/Off>

証明書が失効しているかどうかを確認するために、Expressway が OCSP を使用して証明書失効チェックを実行できるかどうかを制御します。OCSP を使用するには、チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS UseOcsp: On`

xConfiguration XCP TLS Certificate CVS VerifyHostname: <On/Off>

Expressway が自身のピアの設定に対し、XCP ホストの証明書を確認するかどうかを制御します。デフォルトは On です。

例：`xConfiguration XCP TLS Certificate CVS VerifyHostname: On`

xConfiguration Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto`

xConfiguration Zones DefaultZone SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones DefaultZone SIP Media ICE Support: On`

xConfiguration Zones DefaultZone SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones DefaultZone SIP Multistream Mode: Off`

xConfiguration Zones DefaultZone SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones DefaultZone SIP Record Route Address Type: IP`

xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: <On/Off>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: Off`

xConfiguration Zones DefaultZone SIP TLS Verify Mode: <On/Off>

外部サービスによって提供される証明書に記載されているホスト名を Expressway で検証するかどうかを制御します。有効にすると、証明書のホスト名（共通名とも呼ぶ）は、デフォルト ゾーンのアクセス ルールで指定されたパターンと照合されます。デフォルトは Off です。

例：`xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのサブゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

デフォルト サブゾーン内のエンドポイントで送受信するすべてのコールの帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920`

Configuration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーン内のエンドポイントで送受信するすべてのコールの帯域幅に制限を設けるかどうかを制御します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーンとの間でコールを行うことはできません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

デフォルト サブゾーン内の 2 つのエンドポイント間のすべてのコールの帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーン内の 2 つのエンドポイント間のいずれかのコールの帯域幅に制限を設けるかどうかを制御します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーン内ではコールを発信できません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

デフォルト サブゾーンの総帯域幅制限を設定します（モードが Limited に設定されている場合にのみ適用）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

デフォルト サブゾーンにエンドポイントが常に使用する総帯域幅の制限を設けるかどうかを決定します。

NoBandwidth：使用可能な帯域幅はありません。デフォルト サブゾーン内ではコールを送受信できません。

デフォルトは Unlimited です。

例：`xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Registrations: <Allow/Deny>

デフォルト サブゾーンに割り当てられている登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow`

xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このサブゾーンで送受信されるSIPコール（インターワーキングコールを含む）にExpresswayによって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: <On/Off>

このゾーン内のデバイスでICEをサポートするかどうかを制御します。デフォルトはOffです。

On：このゾーンではICEをサポートします。

Off：このゾーンではICEをサポートしません。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: On`

xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトはOnです。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: <On/Off>

このゾーンでSIP UPDATEメッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP*セッションを更新するために、このゾーンから*SIP UPDATE*メッセージを送信します。

Off：このゾーンでは*SIP*セッション更新用の*SIP UPDATE*メッセージを送信しません。

デフォルトはOffです。

例：`xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: On`

xConfiguration Zones LocalZone SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones LocalZone SIP Record Route Address Type: IP`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64>

自由形式のメンバーシップ ルールの説明。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: 「Office-based staff」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50>

このメンバーシップ ルールに名前を割り当てます。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: 「Office Workers」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60>

エイリアスを比較するパターンを指定します。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: 「@example.com」`

nfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex>

パターンとエイリアスを照合する方法。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534>

エンドポイントのアドレスが複数のルールを満たす場合に、ルールを適用する順序（および、そのために、エンドポイントを割り当てるサブゾーン）を決定します。最もプライオリティの高いルール（1、次が 2、その次が 3 など）が最初に適用されます。複数のサブネット ルールが同じプライオリティの場合、最も大きなプレフィックス長を持つルールが最初に適用されます。エイリアス パターン マッチ ルールで同じプライオリティのものは、設定順に検索されます。デフォルトは 100 です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled>

メンバーシップ ルールが有効になっているか、無効になっているかを示します。無効になっているメンバーシップ ルールは無視されます。デフォルトは Enabled です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50>

アドレスがこのルールを満たす場合にエンドポイントを割り当てるサブゾーン。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: 「Branch Office」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39>

このサブネットを識別するために（プレフィクス長とともに）使用する IP アドレス指定します。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: 「192.168.0.0」`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128>

このサブネットに所属するために IP アドレスと一致する必要があるサブネット アドレスのビット数。デフォルトは 32 です。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch>

このルールに適用するアドレスのタイプ。

*[*サブネット（*Subnet*）*]*：IP アドレスが設定した IP アドレス サブネットに含まれる場合は、デバイスを割り当てます。

AliasPatternMatch：エイリアスが設定したパターンと一致する場合は、デバイスを割り当てます。

例：`xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのサブゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。詳細については、『Administrator Guide』を参照してください。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000>

このサブゾーン内のエンドポイントで送受信するいずれかのコールに帯域幅制限（kbps 単位）（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

サブ ゾーン内のエンドポイントで送受信するいずれかのコールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンではコールを送受信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000>

このサブゾーン内の 2 つのエンドポイントのいずれかのコールに帯域幅制限（モードが Limited に設定されている場合にのみ適用）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

このサブゾーン内の 2 つのエンドポイントで送受信するいずれかのコールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンではコールを発信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000>

このサブゾーンの総帯域幅制限を設定します（モードが Limited に設定されている場合にのみ適用）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

このサブゾーンにエンドポイントが常に使用するコールの総帯域幅の制限を設けるかどうかを制御します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。このサブゾーンから、またはこのサブゾーン内でコールを発信できません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50>

このサブゾーンに名前を割り当てます。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Name: 「BranchOffice」`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny>

このサブゾーンに割り当てられている登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このサブゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones LocalZone SubZones SubZone 1 SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones LocalZone SubZones Subzone 1 SIP Media ICE Support: On`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones LocalZone SubZones Subzone 1 SIP Multistream Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Assent Mode: <On/Off>

ファイアウォール トラバーサルに Assent モードを使用する H.323 コールを許可するかどうかを決定します。Expressway に直接登録されているトラバーサル対応エンドポイントに適用します。デフォルトは On です。

例：`xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

ファイアウォール トラバーサルに H460.18 モードを使用する H.323 コールを許可するかどうかを決定します。Expressway に直接登録されているトラバーサル対応エンドポイントに適用します。デフォルトは On です。

例：`xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Expresswayに直接登録されているトラバーサル対応のエンドポイントからのコールにExpresswayが逆多重化モードで動作するかどうかを制御します。デフォルトは Off です。

On：すべてのコールに同じ 2 つのポートを使用できるようにします。

Off：各コールが個別のポートペアをメディアに使用します。

例：`xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Preference: <Assent/H46018>

Expressway に直接登録されているエンドポイントが Assent プロトコルと H460.18 プロトコルの両方をサポートしている場合は、この設定で使用する Expressway を決定します。デフォルトは Assent です。

例：`xConfiguration Zones LocalZone Traversal H323 Preference: Assent`

xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

ファイアウォールの NAT バインドを有効に保つため、コールが確立した後に Expressway に直接登録されているトラバーサル対応エンドポイントが TCP プローブを送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Expressway に直接登録されているトラバーサル対応エンドポイントが TCP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Expressway に直接登録されているトラバーサル対応エンドポイントが TCP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`

xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

ファイアウォールの NAT バインドを有効に保つため、コールが確立した後に Expressway に直接登録されているトラバーサル対応エンドポイントが UDP プローブを送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Expressway に直接登録されているトラバーサル対応エンドポイントが UDP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Expressway に直接登録されているトラバーサル対応エンドポイントが UDP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

Expressway が処理するトラバーサル コールのいずれかに適用する帯域幅制限（kbps 単位）（モードが Limited に設定されている場合のみ）。デフォルトは 1920 です。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Expressway が処理するいずれかのトラバーサル コールの帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。トラバーサル コールは発信できません。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

Expressway が処理するすべてのトラバーサル コールに許可する総帯域幅制限（kbps 単位）（モードが Limited に設定されている場合のみ）。デフォルトは 500000 です。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Expressway が処理するすべてのトラバーサル コールの総帯域幅に制限を設けるかどうかを決定します。デフォルトは Unlimited です。

NoBandwidth：使用可能な帯域幅はありません。トラバーサル コールは発信できません。

例：`xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones Policy Mode: <SearchRules/Directory>

宛先の検索を試行するときに使用するモード。デフォルトは SearchRules です。

SearchRules：クエリするゾーンとその順序を決定する設定済みの検索ルールを使用します。

Directory：要求を正しいゾーンに送信するためにディレクトリ サービスの機能を使用します。

例：`xConfiguration Zones Policy Mode: SearchRules`

xConfiguration Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No>

この検索ルールを認証された検索要求にのみ適用するかどうかを指定します。デフォルトは No です。

例：`xConfiguration Zones Policy SearchRules Rule 1 Authentication: No`

ration Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64>

自由形式の検索ルールの説明。

例：`xConfiguration Zones Policy SearchRules Rule 1 Description: 「Send query to the DNS zone」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress>

クエリをターゲットゾーンに送信するかどうかを決定します。デフォルトはAnyAliasです。

AliasPatternMatch：エイリアスが対応するパターン タイプと文字列とが一致する場合にのみ照会します。

AnyAlias：いずれかのエイリアス（IP アドレスではない）のゾーンを照会します。

AnyIPAddress：指定した IP アドレス（エイリアスではない）のゾーンを照会します。

例：`xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias`

xConfiguration Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50>

検索ルールの記述名。

例：`xConfiguration Zones Policy SearchRules Rule 1 Name: 「DNS lookup」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace>

ターゲットゾーンに送信する前に、エイリアスの一致した部分を変更するかどうかを決定します（エイリアス パターン マッチ モードにのみ適用します）。デフォルトは Strip です。

*[*変更しない（*Leave*）*]*：エイリアスは変更されません。

*[*除去（*Strip*）*]*：一致するプレフィックスまたはサフィックスをエイリアスから削除します。

*[*置換（*Replace*）*]*：エイリアスの一致部分が [置換文字列（Replace string）] のテキストで置き換えられます。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60>

パターンに一致するエイリアスの部分を置き換える文字列（置換パターン動作にのみ適用します）。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: 「@example.net」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60>

エイリアスと比較するパターン（エイリアス パターン マッチ モードにのみ適用します）。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern String: 「@example.com」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex>

適用するルールで、パターン文字列をどのようにエイリアスと照合するか（エイリアス パターン マッチ モードにのみ適用します）。デフォルトは Prefix です。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

例：`xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones Policy SearchRules Rule [1..2000] Priority: <1..65534>

他の検索ルールのプライオリティと比較したときに、このルールを適用する検索プロセスの順序。プライオリティ 1 のすべてのルールが最初に適用され、次にプライオリティ 2 のすべてのルールが適用されます。デフォルトは 100 です。

例：`xConfiguration Zones Policy SearchRules Rule 1 Priority: 100`

xConfiguration Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop>

エイリアスがこの検索ルールと一致する場合の進行中の検索動作を指定します。「Stop」を選択した場合、このルールと同じプライオリティのルールは適用されます。デフォルトは Continue です。

*[*続行（*Continue*）*]*：エイリアスが特定したエンドポイントが検出されるまで、残りの検索ルールを（プライオリティ順に）適用します。

*[*停止（*Stop*）*]*：エイリアスで特定されたエンドポイントがターゲット ゾーンで検出されない場合でも、これ以上は検索ルールを適用しません。

例：`xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue`

xConfiguration Zones Policy SearchRules Rule [1..2000] Protocol: <Any/H323/SIP>

照会するルールに必要な送信元のプロトコル。

例：`xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Mode: <Any/AllZones/LocalZone/Named>

このルールを適用する要求のソース。デフォルトは Any です。

Any：ローカル登録されたデバイス、ネイバーまたはトラバーサルゾーン、および登録されていないデバイス。

All Zones：ローカルに登録されたデバイスとネイバーまたはトラバーサルゾーン。

Local Zone：ローカル登録されたデバイスのみ。

Named：特定のゾーンまたはサブゾーン。

例：`xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Name: <S: 0..50>

このルールを適用する送信元（サブ）ゾーンの名前。

例：`xConfiguration Zones Policy SearchRules Rule 1 Source Name: 「Local Office」`

xConfiguration Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled>

検索ルールが有効になっているか、無効になっているかを示します。無効になっている検索ルールは無視されます。デフォルトは Enabled です。

例：`xConfiguration Zones Policy SearchRules Rule 1 State: Enabled`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50>

エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。

例：`xConfiguration Zones Policy SearchRules Rule 1 Target Name: 「Sales Office」`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService>

この検索ルールを適用するターゲットのタイプ。

例：`xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone`

xConfiguration Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off>

NAPTR（SIP）レコードまたは SRV（SIP と H.323）レコードがこのゾーンを介してダイヤルされたエイリアスで検出されなかった場合は、Expressway が A および AAAA DNS レコードを照会するかどうかを決定します。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Audio DefaultCodec:

`<G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>`

空の INVITE を許可しない場合に使用する音声コーデックを指定します。デフォルトは G711u です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off>

Expressway がこのゾーンに送信する SIP INVITE メッセージを SDP を使用せずに生成するかどうかを制御します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。デフォルトは On です。

On：SDP を使用していない SIP INVITE が生成され、このネイバーに送信されます。

Off：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535>

空の INVITE を許可しない場合に使用するビデオ ビット レートを指定します。デフォルトは 384 です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

空の INVITE を許可しない場合に使用するビデオ コーデックを指定します。デフォルトは H263 です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

空の INVITE を許可しない場合に使用すビデオ解像度を指定します。デフォルトは CIF です。

例：`xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: <UDP/TCP/TLS>

DNS NAPTR レコードと SIP URI パラメータによって必要なトランスポート情報が得られないときに DNS ゾーンからの SIP コールに使用するトランスポート タイプを決定します。RFC 3263 では、UDP を使用する必要があると提案しています。デフォルトは UDP です。

例：`xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: UDP`

xConfiguration Zones Zone [1..1000] DNS SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 1 DNS SIP Media ICE Support: Off`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 1 DNS SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを決定します。デフォルトは Off です。

On：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] DNS SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>

H.323 検索としてこのゾーン宛に発信された SIP 検索を Expressway が受信したときの動作を制御します。デフォルトは Off です。

Off：SIP OPTION メッセージはこのゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>

DNS ルックアップにより返されたこの Expressway と宛先システム サーバ間の X.509 証明書チェックを制御します。有効になっている場合は、DNS ルックアップに送信されたドメイン名（サブジェクト共通名の属性かサブジェクト代替名の属性）がサーバの X.509 証明書に含まれている必要があります。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128>

トラバーサル クライアントの X.509 証明書で検索する証明書の所有者の名前（サブジェクト共通名の属性またはサブジェクト代替名の属性のいずれかに含まれている必要があります）。空の場合は、解決された URI のドメインの部分が使用されます。

例：`xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: 「example.com」`

xConfiguration Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>

このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。

On：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。

Off：INVITE 要求は変更されません。

例：`xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone [1..1000] DNS ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

ゾーンの詳細な設定方法を決定します。

Default：工場出荷時の初期設定を使用します。

Custom：各設定を個別に行うことができます。

Preconfigured profiles：事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。

例：`xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>

変換された E.164 番号に追加する DNS ゾーン。これにより、このゾーンで照会する ENUM ホスト名が作成されます。

例：`xConfiguration Zones Zone 2 ENUM DNSSuffix: 「e164.arpa」`

xConfiguration Zones Zone [1..1000] H323 Mode: <On/Off>

このゾーンでの H.323 コールの送受信を許可するかどうかを決定します。デフォルトは On です。

例：`xConfiguration Zones Zone 2 H323 Mode: On`

xConfiguration Zones Zone [1..1000] HopCount: <1..255>

エイリアス検索要求をこのゾーンに送信するときに使用するホップ カウントを指定します。注：別のゾーンから受信した検索要求にすでにホップ カウントが割り当てられている場合は、2 つの値のうちの小さいほうが使用されます。デフォルトは 15 です。

例：`xConfiguration Zones Zone 2 HopCount: 15`

xConfiguration Zones Zone [1..1000] Name: <S: 1, 50>

このゾーンに名前を割り当てます。

例：`xConfiguration Zones Zone 3 Name: 「UK Sales Office」`

xConfiguration Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534>

この Expressway で送受信する H.323 コールに使用するネイバーのポート。デフォルトは 1720 です。

例：`xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`

xConfiguration Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>

この Expressway で送受信する H.323 検索に使用するネイバーのポート。デフォルトは 1719 です。

例：`xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`

xConfiguration Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>

Expressway がこのゾーン宛の H323 検索を受信したときの動作を決定します。デフォルトは Off です。

Off：LRQ メッセージがゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec:

`<G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>`

空の INVITE を許可しない場合に使用する音声コーデックを指定します。デフォルトは G711u です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>

Expressway がこのゾーンに送信する SIP INVITE メッセージを SDP を使用せずに生成するかどうかを決定します。SDP を使用していない INVITE は、宛先デバイスがコーデックの選択を開始するよう求められることを意味し、コールが H.323 からローカルにインターワーキングされていた場合に使用されます。デフォルトは On です。

On：SDP を使用していない SIP INVITE が生成され、このネイバーに送信されます。

Off：SIP INVITE が生成され、事前設定された SDP が挿入されてから INVITE が送信されます。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No>

Expressway はこのゾーンへのコールで暗号化された SRTCP を提供するかどうかを制御します。Expressway は INFO 要求を送信します。デフォルトは No です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>

H.323 コールとインターワーキングするときに Expressway が SIP エンドポイントをどのように検索するかを決定します。デフォルトは Options です。

Options：Expressway は OPTIONS 要求を送信します。

Info：Expressway は INFO 要求を送信します。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>

空の INVITE を許可しない場合に使用するビデオ ビット レートを指定します。デフォルトは 384 です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

空の INVITE を許可しない場合に使用するビデオ コーデックを指定します。デフォルトは H263 です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

空の INVITE を許可しない場合に使用すビデオ解像度を指定します。デフォルトは CIF です。

例：`xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] Neighbor Monitor: <Yes/No>

ゾーンがそのネイバー ピアをモニタするかどうかを指定します。LQR H323、または SIP OPTIONS、あるいはその両方がピアに定期的に送信されます。いずれかのピアが応答に失敗すると、そのピアは非アクティブとマークされます。どのピアも応答を管理していない場合、そのゾーンは非アクティブとマークされます。デフォルトは Yes です。

例：`xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

xConfiguration Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>

ネイバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。ネイバー ゾーンが Expressway クラスタの場合、これはそのクラスタ ピアの 1 つになります。

例：`xConfiguration Zones Zone 3 Neighbor Peer 1 Address: 「192.44.0.18」`

xConfiguration Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 3 Neighbor Registrations: Allow`

xConfiguration Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>

形式が不正な、または破損した SIP メッセージに対するシステムの許容度を制御します。

Drop All：システムは、形式が不正な、または破損した SIP メッセージを受信した時点で SIP 接続を閉じます。

RetainSome：システムは、形式が不正でも必須ではないヘッダーが設定された SIP メッセージを受信した場合、SIP 接続を維持します。必須のヘッダーの形式が不正な場合は、接続を閉じます。

Retain All: システムは、(必須ヘッダーを含む) 形式が不正なヘッダーを持つ SIP メッセージを受信しても SIP 接続を維持します。

デフォルトは DropAll です。

（注）
- *Content-Length* ヘッダーは例外です。設定されているモードにかかわらず、このヘッダーが存在しないか形式が不正な場合、接続は常に閉じられます。
- Expressway が不正な形式のメッセージを 11 個以上続けて受信した場合も、モードにかかわらず接続が閉じられます。
- CMR Cloud 導入環境では、RetainAll モードを設定することをお勧めします。

例：`xConfiguration Zones Zone 3 RetainConnectionOnParseErrorMode: RetainSome`

xConfiguration Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>

このゾーンからの認証された SIP メッセージ（P-Asserted-Identity ヘッダーを含んでいるもの）を信頼できるかどうかを制御します。デフォルトは Off です。

On：それ以上のチャレンジを行うことなく、メッセージが信頼されます。

Off：認証のため、メッセージにチャレンジが実行されます。

例：`xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Refer Mode: <Forward/Terminate>

SIP REFER 要求の処理方法を決定します。

Forward：SIP REFER 要求がターゲットに転送されます。

Terminate：SIP REFER 要求は Expressway によって終了されます。

デフォルトは Forward です。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Refer Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Replaces Mode: <Forward/Terminate>

Meeting Server コール ブリッジ グループからの INVITE メッセージに対して、Expressway でロード バランシングを処理できるようにします。デフォルトは Forward です。

Terminate：Expressway B2BUA が Meeting Server からの INVITE を処理します。この Expressway に登録されているエンドポイント、あるいは隣接する VCS または Expressway に登録されているエンドポイントに対してロード バランシングを有効にする必要があります。

Forward：Expressway は Meeting Server からの INVITE をプロキシします。エンドポイントが Unified CM に登録されている場合、Unified CM で代わりにこれらの INVITE を処理できるため、このオプションを使用できます。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Replaces Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64>

ローカル SIP Back-to-Back User Agent サービスのインスタンスを表す識別子。

例：`xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`

xConfiguration Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No>

ネイバー ピアからのクラス 5 の SIP 応答により、ゾーンが使用についてアライブであると見なされるようになるかどうかを指定します。デフォルトは Yes です。

例：`xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`

xConfiguration Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>

Expressway によるこのゾーンで暗号化された SIP コールの処理方法を決定します。デフォルトは Auto です。

Auto：セキュア SIP トランスポート（TLS）が使用されている場合、SIP コールが暗号化されます。

[Microsoft]：SIP コールは MS-SRTP を使用して暗号化されます。

[オフ（Off）]：SIP コールは暗号化されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>

複数の MIME ストリッピングをこのゾーンからの要求上で実行するかどうかを制御します。Microsoft Office Communications Server 2007 に接続する場合は、On に設定する必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 Neighbor SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 3 Neighbor SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching>

このネイバーで送受信するコールのメディアの Expressway による処理方法と、このネイバー宛のメディアを転送する場所。デフォルトは Auto です。.

Signaled：このネイバーで送受信されるコールのメディアは常に取得されます。このネイバーから受信した SDP でシグナリングされたとおりに転送されます。

Latching：このネイバーで送受信されるコールのメディアは常に取得されます。メディアは、このネイバーからのメディアを受信する IP アドレスとポートに転送されます。

Auto：コールがトラバーサルコールの場合にのみ、メディアが取得されます。このネイバーが NAT の背後にある場合、Expressway はこのゾーンからのメディアを受信するメディアを IP アドレスとポートに転送されます（ラッチング）。または、SDP でシグナリングされた IP アドレスとポートにメディアが転送されます（シグナリング）。

例：`xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 Neighbor SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

On：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Port: <1024..65534>

この Expressway で送受信する SIP コールに使用するネイバーのポートを指定します。デフォルトは 5061 です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Port: 5061`

xConfiguration Zones Zone [1..1000] Neighbor SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255>

このゾーンから受信した SIP 要求の Proxy-Require ヘッダーを検索し、そのヘッダーから削除するオプション タグのカンマ区切りのリスト。デフォルトでは、オプションタグは指定されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: 「com.example.something,com.example.somethingelse」`

xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No>

このゾーンに REGISTER メッセージがプロキシ転送されるときに Expressway が RFC3327 Path ヘッダーを挿入するかどうかを制御します。無効にすると、Expressway が代わりに連絡先ヘッダーを書き換えて、RFC3327 をサポートしない SIP レジストラとのインターワーキングを許可します。デフォルトは Yes です。

例：`xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: Yes`

（注） バージョン X8.9 で、MRA に使用するネイバー ゾーンの自動作成機能を制御するトグルを導入しました。このバージョンのこれらのゾーンでは、デフォルトは No です。`xConfiguration CollaborationEdge RFC3327Enabled` を参照してください。

xConfiguration Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname>

Expressway がその IP アドレスを使用するか、このゾーンへの発信 SIP 要求の Record-Route または Path ヘッダーのホスト名を使用するかを制御します。注：ホスト名にこの値を設定すると、有効な DNS システム ホスト名も Expressway で設定する必要があります。デフォルトは IP です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>

H.323 検索としてこのゾーン宛に発信された SIP 検索を Expressway が受信したときの動作を制御します。デフォルトは Off です。

Off：SIP OPTION メッセージはこのゾーンに送信されます。

On：検索に自動的に応答します。検索が転送されることはありません。

例：`xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP SipUpdateRefresh Support: <On/Off>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP SipUpdateRefresh Support: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>

この Expressway とネイバー システム間のインバウンド接続とアウトバンド接続の X.509 証明書チェックと相互認証を制御します。有効になっている場合は、ピア アドレス フィールドで指定したネイバー システムの FQDN または IP アドレスがネイバーの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>

このネイバーで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>

このゾーンに送信された INVITE 要求から UDP/BFCP をフィルタリングにより除去するかどうかを決定します。UDP/BFCP プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。

On：UDP/BFCP プロトコルを参照しているメディア回線が TCP/BFCP で置き換えられ、無効になります。

Off：INVITE 要求は変更されません。

例：`xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone 1 Neighbor SIP UDP IX Filter Mode: <On/Off>

このゾーンに送信された INVITE 要求から UDP/UDT/IX または UDP/DTLS/UDT/IX をフィルタリングにより除去するかどうかを決定します。

UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルをサポートしない SIP デバイスとの相互運用性を有効にするためにこのオプションが必要な場合があります。デフォルトは Off です。

On：UDP/UDT/IX プロトコルまたは UDP/DTLS/UDT/IX プロトコルを参照するメディア回線を RTP/AVP に置き換えて無効にします。

Off：INVITE 要求は変更されません。

例：`xConfiguration Zones Zone 1 neighbor SIP UDP IX Filter Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off>

このゾーンで送受信するすべての要求と応答の Allow ヘッダーから Expressway が UPDATE メソッドを削除するかどうかを制御します。デフォルトは Off です。

例：`xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always>

このネイバーで送受信するコールのシグナリングを Expressway がどのように処理するかを指定します。デフォルトは Auto です。

Auto：コールルーテッドモードの設定に従ってシグナリングを取得します。

Always：コールルーテッド モードの設定に関係なく、ネイバーで送受信するコールのシグナリングを常に取得します。

例：`xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SRV MaxPeers: <1..30>

所定のネイバーゾーンが SRV レコードルックアップで構成されている場合に、Expressway が登録できるピアの最大数を指定します。

例：`xConfiguration Zones Zone 1 Neighbor SRV MaxPeers: 30`

xConfiguration Zones Zone [1..1000] Neighbor ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

ゾーンの詳細な設定方法を決定します。

Default：工場出荷時の初期設定を使用します。

[カスタム（Custom）]：各設定を個別に行うことができます。

Preconfigured profiles：事前設定されたプロファイルのいずれかを選択して、そのタイプのシステムへの接続に必要な適切な設定を自動的に使用します。

例：`xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] SIP Mode: <On/Off>

このゾーンでの SIP コールの送受信を許可するかどうかを決定します。デフォルトは On です。

例：`xConfiguration Zones Zone 3 SIP Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>

トラバーサル サーバに接続するときに Expressway で使用するパスワード。プレーン テキストの最大長は 128 文字で、暗号化されます。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication Password: 「password123」`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>

トラバーサル サーバに接続するときに Expressway で使用するユーザ名。

例：`xConfiguration Zones Zone 4 TraversalClient Authentication UserName: 「clientname」`

xConfiguration Zones Zone [1..1000] TraversalClient DisconnectOnFailInterval: <10>

ピアが OPTIONS ping に応答できない場合、トラバーサル クライアントゾーンはエラー状態になります。DISCONNECT_ON_FAIL_INTERVAL が構成されている場合、エラー状態の間、Expressway ノードは接続を切断してから OPTIONS ping を送信し、接続の堅牢性を確保します。切断は、DISCONNECT_ON_FAIL_INTERVAL に従った間隔で発生します。

デフォルトでは、フラグは無効です。有効にするには、値の範囲を 0 ー 3600 秒に設定します

最小値 = *0*。

最大値 = 3600。

デフォルト：0（無効）

例：`xConfiguration Zones Zone 1 TraversalClient DisconnectOnFailInterval: 「10」`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>

この Expressway からの H.323 ファイアウォール トラバーサル コールに使用するトラバーサル サーバのポート。トラバーサル サーバが Expressway-E の場合、この Expressway に関連付けられた Expressway-E のトラバーサル ゾーンで設定されているポート番号にする必要があります。

例：`xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>

2 つのファイアウォール トラバーサル プロトコルのうちのどちらをトラバーサル サーバで送受信するコールに使用するかを決定します。注：このトラバーサル クライアントで送受信するコールのサーバに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>

トラバーサル サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。トラバーサル サーバが Expressway-E クラスタの場合、これはそのクラスタ ピアの 1 つになります。

例：`xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: 「10.192.168.1」`

xConfiguration Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>

トラバーサル サーバへの接続の確立に失敗した試行を再度試す間隔（秒単位）。デフォルトは 120 です。

例：`xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

xConfiguration Zones Zone [1..1000] TraversalClient SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalClient SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalClient SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルトは Auto です。

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On>

Expressway がこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 TraversalClient SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

On：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>

この Expressway からの SIP コールに使用するトラバーサル サーバのポートを指定します。トラバーサル サーバが Expressway-E の場合、この Expressway のトラバーサル ゾーンで設定されているポート番号にする必要があります。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalClient SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>

どのファイアウォール トラバーサル プロトコルをトラバーサル サーバで送受信する SIP コールに使用するかを決定します。注：このトラバーサル クライアントで送受信するコールのサーバに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>

この Expressway とトラバーサル サーバ間での X.509 証明書チェックと相互認証を制御します。有効になっている場合は、ピア アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>

トラバーサル サーバで送受信する SIP コールに使用するトランスポート タイプを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Expressway がこのゾーンからの着信メッセージをどのように認証するかを制御し、それらのメッセージを認証または未認証として処理するか、あるいは拒否するかを制御します。H.323 メッセージ、ローカル ドメインから発信される SIP メッセージか非ローカル ドメインから発信される SIP メッセージかによって動作が異なります。デフォルトは DoNotCheckCredentials です。

例：`xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>

トラバーサル サーバで認証するときに、トラバーサル クライアントが使用する名前。トラバーサル クライアントが Expressway の場合は、その Expressway の認証ユーザ名にする必要があります。トラバーサル クライアントがゲートキーパーの場合は、そのゲートキーパーのシステム名にする必要があります。

例：`xConfiguration Zones Zone 5 TraversalServer Authentication UserName: 「User123」`

xConfiguration Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

トラバーサル クライアントからのコールに対して、Expressway が逆多重化モードで動作するかどうかを決定します。デフォルトは Off です。

On：すべてのコールに同じ 2 つのポートを使用できるようにします。

Off：各コールが個別のポートペアをメディアに使用します。

例：`xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>

このトラバーサル クライアントからの H.323 ファイアウォール トラバーサルに使用する Expressway のポートを指定します。デフォルトは 6001 です（新しいゾーンごとに 1 ずつ増加）。

例：`xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>

2 つのファイアウォール トラバーサル プロトコルのうちのどちらをトラバーサル クライアントで送受信するコールに使用するかを決定します。注：このトラバーサル サーバで送受信するコールのクライアントに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny>

このゾーンを通じてルーティングされたプロキシ経由で送信される SIP 登録を受け入れるかどうかを制御します。デフォルトは Allow です。

例：`xConfiguration Zones Zone 5 TraversalServer Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalServer SIP SipUpdateRefresh Support: <Off/On>

このゾーンで SIP UPDATE メッセージによるセッション更新をサポートするかどうかを指定します。

On：*SIP* セッションを更新するために、このゾーンから *SIP UPDATE* メッセージを送信します。

Off：このゾーンでは *SIP* セッション更新用の *SIP UPDATE* メッセージを送信しません。

デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalServer SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media AesGcm Support: <Off/On>

このゾーンを通過するメディアの AES GCM アルゴリズムによる暗号化/復号化を有効にします。デフォルトは Off です。

例：`xConfiguration Zones Zone 1 TraversalServer SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

このゾーンで送受信される SIP コール（インターワーキング コールを含む）に Expressway によって適用されるメディア暗号化ポリシー。デフォルト： [Auto]

On：すべてのメディアを暗号化する必要があります。

Off：すべてのメディアの暗号化を解除する必要があります。

BestEffort：使用可能な場合は暗号化を使用します。使用できない場合は暗号化されていないメディアにフォールバックします。

Auto：メディア暗号化ポリシーは適用されません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICE Support: <On/Off>

このゾーン内のデバイスで ICE をサポートするかどうかを制御します。デフォルトは Off です。

On：このゾーンでは ICE をサポートします。

Off：このゾーンでは ICE をサポートしません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICEPassThrough Support: <On/Off>

このゾーン内のデバイスで ICE パススルーをサポートするかどうかを制御します。デフォルト：Off

On：このゾーンでは ICE パススルーをサポートします。

Off：このゾーンでは ICE パススルーをサポートしません。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On>

Expresswayがこのゾーンのデバイス間のマルチストリームを許可するかどうかを制御します。デフォルトは On です。

On：マルチストリームを許可します。

Off：マルチストリームを拒否します。

例：`xConfiguration Zones Zone 1 TraversalServer SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>

ローカル Expressway が再度受信した場合は拒否するように、このゾーンに送信された SIP 要求を「ポイゾニング」するかどうかを制御します。デフォルトは Off です。

On：このゾーンを介して送信され、このExpressway が再度受信する SIP 要求は拒否されます。

Off：このゾーンを介して送信され、この Expressway が再度受信する SIP 要求は通常どおりに処理されます。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>

このトラバーサル クライアントからの SIP ファイアウォール トラバーサルに使用する Expressway のポート。デフォルトは 7001 です（新しいゾーンごとに 1 ずつ増加）。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalServer SIP PreloadedSipRoutes Accept: <Off/On>

[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オン（On）] に切り替えて、Route ヘッダーを含んだ SIP INVITE 要求をこのゾーンで処理できるようにします。このヘッダーを含んでいる SIP INVITE 要求をゾーンで拒否するには、[プリロードされた SIP ルートのサポート（Preloaded SIP routes support）] を [オフ（Off）] に切り替えます。

例：`xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>

どのファイアウォール トラバーサル プロトコルをトラバーサル クライアントで送受信する SIP コールに使用するかを決定します。注：このトラバーサル サーバで送受信するコールのクライアントに同じプロトコルを設定する必要があります。デフォルトは Assent です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>

この Expressway とトラバーサル クライアント間での X.509 証明書チェックと相互認証を制御します。有効にした場合は、TLS 検証サブジェクト名を指定する必要があります。デフォルトは Off です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>

トラバーサル クライアントの X.509 証明書で検索する証明書の所有者の名前（サブジェクト共通名の属性またはサブジェクト代替名の属性のいずれかに含まれている必要があります）。

例：`xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: 「myclientname」`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>

トラバーサル クライアントと Expressway 間の SIP コールに 2 つのトランスポート タイプのどちらを使用するかを決定します。デフォルトは TLS です。

例：`xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

コールが確立した後、ファイアウォールのNATバインドを有効にしておくために、トラバーサル クライアントが TCP プローブを Expressway に送信する間隔（秒単位）を設定します。デフォルト：20。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>

トラバーサル クライアントが Expressway への TCP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>

トラバーサル クライアントが Expressway に TCP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

コールが確立した後、ファイアウォールのNATバインドを有効にしておくために、トラバーサル クライアントが UDP プローブを Expressway に送信する間隔（秒単位）を設定します。デフォルトは 20 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>

トラバーサル クライアントが Expressway への UDP プローブの送信を試行する回数を設定します。デフォルトは 5 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>

トラバーサル クライアントが Expressway に UDP プローブを送信する頻度（秒単位）を設定します。デフォルトは 2 です。

例：`xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

ローカル Expressway に関連して、指定したゾーンの特性を決定します。

Neighbor：新しいゾーンはローカル Expressway のネイバーになります。

TraversalClient：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサルクライアントになります。

TraversalServer：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサルサーバになります。

ENUM：ゾーンに ENUM ルックアップで検出されたエンドポイントが含まれます。

DNS：ゾーンに DNS ルックアップで検出されたエンドポイントが含まれます。

例：`xConfiguration Zones Zone 3 Type: Neighbor`

xConfiguration license smart debug: <error/trace/debug/all>

スマートライセンシングのデバッグを有効します。デフォルト：エラー

Error：スマートライセンシングで発生したエラーをログに記録します。

Trace：通常のスマートライセンシング操作中にトレースメッセージをログに記録します。

Debug：デバッグメッセージをログに記録します。

All：3 つのレベルをすべて有効します。（ピア固有）

例：`xConfiguration license smart debug: all`

xConfiguration license smart deregister: <On/Off>

評価期間が満了していなければ、製品は評価モードに戻ります。製品で使用されるすべてのライセンス付与がバーチャルアカウントにすぐに戻されて、他の製品インスタンスで使用できるようになります。（ピア固有）

例：`xConfiguration license smart deregister: On`

xConfiguration license smart privacy: <none/all/hostname/version>

この製品インスタンスのホスト名と IP アドレスを Cisco Smart Software Manager または Cisco Smart Software Manager Satellite と交換する必要がない場合に使用します。（ピア固有）

例：`xConfiguration license smart privacy: all`

xConfiguration license smart register idtoken: <String>

Smart Software Manager または Smart Software Manager サテライトから生成した製品インスタンス登録トークンを使用して製品を登録します。（ピア固有）

例：`xConfiguration license smart register idtoken: <Token>`

xConfiguration license smart renew ID: <On/Off>

Cisco Smart Software Manager のネットワーク接続の問題が原因で自動登録の更新に失敗した場合は、この操作を実行します。（ピア固有）

例：`xConfiguration license smart renew ID: On`

xConfiguration license smart renew auth: <On/Off>

Cisco Smart Software Manager によるネットワーク接続の問題が原因で、自動認証ステータスの更新に失敗した場合は、この操作を実行します。（ピア固有）

例：`xConfiguration license smart renew auth: On`

xConfiguration license smart transport: <direct/satellite>

この製品インスタンスが Cisco Smart Software Manager と通信して使用情報を送受信する方法を決定します。

Direct：Cisco Smart Software Manager とインターネットを介して直接通信します。

Satellite：オンプレミスに導入された Smart Software Manager のサテライトを介して通信します。

例：`xConfiguration license smart transport: direct`

xConfiguration license smart reregister: <String>

次の場合に、この操作を実行して製品インスタンスを再登録します（この製品インスタンスの以前の登録の試行が、ネットワーク接続の問題によって失敗し、この問題を解決した後に再登録する必要があります）。仮想アカウントにすでに登録されている製品インスタンスを別の仮想アカウントに再登録するには。（ピア固有）

例：`xConfiguration license smart reregister: <Token>`

xConfiguration license smart url: <String>

Cisco Smart Software Manager のサテライトサーバの URL を入力します。（ピア固有）

例：`xConfiguration license smart url: http://www.alpha.crate.cisco.com/Transport gateway`

コマンド リファレンス — xCommand

項目を追加または削除し、システム コマンドを発行するには、**xCommand** グループのコマンドを使用します。

ここでは、現在利用可能なすべての **xCommand** コマンドを記載します。

コマンドを発行するには、示されているとおりにコマンドを入力した後、1 つまたは複数の所定のパラメータと値を入力します。次の表記法を使用して、各パラメータの有効な値を山かっこ内に示し、その後に各パラメータを示します。

書式	意味
<0..63>	整数値が必要であることを示します。数値は最小値と最大値を示しています。 この例では、0 ～ 63 の範囲内の値にする必要があります。
<S: 7,15>	**S** は引用符で囲まれた文字列値が必要であることを示します。数値は文字列の最小文字数と最大文字数を示します。 この例では、文字列の長さを 7 ～ 15 文字にする必要があります。
<Off/Direct/Indirect>	コマンドの有効な一連の値を示します。値は引用符で囲まないでください。
(r)	これが必須パラメータであることを示します。(r) はコマンド自体の一部ではないことに注意してください。

各 **xCommand** コマンドの使用に関する情報を CLI 内から取得するには、次のように入力します。

- **xCommand**または **xCommand ?** ：使用可能なすべての **xCommand** コマンドを取得する場合。
- **xCommand ??** ：現在のすべての **xCommand** コマンドと、各コマンドの説明、パラメータのリスト、各パラメータの値空間と説明を取得する場合。
- **xCommand <command> ?**：特定のコマンドとそのパラメータ、各パラメータの値空間と説明を返す場合。

set-access コマンド（試験版）について

set-access コマンドを使用すると、Expressway の内部システム コマンドにアクセスできます。**これらのコマンドは、シスコのサポートおよび開発チームのみが使用するために存在するものです。**シスコのサポート担当者のアドバイスや指示がない限り、これらのコマンドにはアクセスしないでください。

⚠

注意 これらのコマンドを誤って使用すると、システムの動作が不安定になったり、パフォーマンス上の問題が発生したり、システム設定が永続的に破損したりする可能性があります。

set-access を使用するには、次の手順に従います。

1. CLI に管理者としてログインします。
2. `set-access qwertsys` と入力します。

   これにより、set-access に関連付けられているシステム コマンド（名前が「「sys-」」で始まるコマンド）が有効になります。
3. 使用可能なコマンドをリストするには、? と入力します。

xCommand コマンド

次の表に、使用可能なすべての **xCommand** コマンドを記載します。

表 20 : xCommand CLI リファレンス

xCommand ACME Delete Pending Cert
保留中の証明書を削除します。 *Domain*：<文字列> 保留中の証明書とは、ACME プロバイダーにより署名された後、Expressway にまだ導入されていないか、導入されていない可能性がある証明書を意味します。 引数を渡さずに、または空の文字列を渡してこのコマンドを実行すると、保留中のサーバ証明書が削除されます。引数を渡して実行すると、指定したドメインに対して保留中になっている証明書が削除されます。 例：`xCommand ACME Delete Pending Cert` `xCommand ACME Delete Pending Cert Domain:「example.com」`

xCommand ACME Deploy

保留中の証明書を導入します。

Domain：<文字列>

ReloadCerts：<*On/Off*>

引数を渡さずにこのコマンドを実行すると、保留中のサーバ証明書が導入され、必要なプロセスに対して証明書がリロードされます。

引数を渡すと、指定したドメインの証明書が導入されます。また、ReloadCerts パラメータで指定されている場合は証明書のリロードも行われます。

例：`xCommand ACME Deploy`

```
xCommand ACME Deploy Domain:「example.com」 ReloadCerts:「On」
```

xCommand ACME Get Pending Cert

保留中の証明書を取得します。

Domain：<文字列>

保留中の証明書とは、ACME プロバイダーにより署名された後、Expressway にまだ導入されていないか、導入されていない可能性がある証明書を意味します。

引数を渡さずにこのコマンドを実行すると、保留中のサーバ証明書が取得されます。引数を渡して実行すると、指定したドメインの保留中の証明書が返されます。

例：`xCommand ACME Get Pending Cert`

```
xCommand ACME Get Pending Cert Domain:「example.com」
```

xCommand ACME Providers Read

ACME プロバイダーに関する情報を読み取ります。

ProviderUuid: <「*Default*」*/String*>

引数を渡さずにこのコマンドを実行すると、データベース内のすべてのプロバイダーに関する情報が返されます。文字列「Default」を渡すと、デフォルトのプロバイダーに関する情報が返されます。特定のプロバイダーに関する情報を返すには、そのプロバイダーの UUID を指定します。

例：`xCommand ACME Providers Read`

```
xCommand ACME Providers Read ProviderUuid: 「Default」
xCommand ACME Providers Read ProviderUuid: 「Provider-UUID」
```

xCommand ACME Providers Write

プロバイダーに関する情報を更新します。

Default：<*On/Off*>

Email(r)：<文字列>

Name：<文字列>

ProviderUuid(r): <「*Default*」*/String*>

TermsOfService(r): <Accepted>

Url：<*String*>

ProviderUuid、Email、TermsOfService の各引数を指定する必要があります。このコマンドでは、特定のプロバイダーの電子メールアドレスとサービス利用規約のみを更新できます。ほかの引数を指定しても、すべて無視されます。

例：`xCommand ACME Providers Write ProviderUuid: 「Default」 Email: new-email@example.com 「 TermsOfService: 」「Accepted」`

xCommand ACME Reset

Expressway-E 上の ACME サービスをリセットし、CLI、REST API、または Web インターフェイスを使用して実行されたすべての設定を削除します。

Action：<*execute*>

このコマンドは Expressway-E 上でのみ呼び出すことができます。SIGN、DISCARD、または DEPLOY コマンドの実行中は、このコマンドを実行できません。Acmereset を実行できるのは、すべてのドメイン証明書とサーバ証明書に対して ACME サービスが無効にされている場合のみです。

例：`xCommand ACME Reset execute`

```
xCommand ACME Reset Action: 「execute」
```

xCommand ACME Revoke

ACME 証明書を取り消します。

CertPath：<文字列>

Provider：<文字列>

ACME 証明書を取り消すには、その前に、取り消す証明書内のドメイン名/SAN エントリの管理権限を持っていることをプロバイダーに証明する必要があります。

これを証明するには、通常の送信および署名プロセスに従って、元の証明書と同じドメイン名/SAN エントリが含まれる新しい証明書を生成する必要があります。

この新しい証明書を受け取った後、古い証明書のパスを指定した `acmerevoke` を使用して古い証明書を取り消します。

デフォルトの ACME プロバイダーを使用した例：`xCommand ACME Revoke 「/path_to_cert_to_be_revoked」`

特定の ACME プロバイダーを使用した例：`xCommand ACME Revoke CertPath: 「/path_to_cert_to_be_revoked」 Provider:「ACME_Provider_Name」`

xCommand ACME Settings Read

ACME の設定を読み取ります。

Domain：<文字列>

サーバ証明書の ACME 設定を読み取るに、パラメータを指定せずにこのコマンドを入力します。特定のドメインの ACME 設定を読み取る場合は、そのドメインを指定します。

例：`xCommand ACME Settings Read`

`xCommand ACME Settings Read 「example.com」`

xCommand ACME Settings Write

ACME の設定を書き込みます。

AcmeManaged(r): < 無効化/手動または自動 >

Domain：<文字列>

ProviderUuid：<文字列>

RenewKey：<*Retain/Rotate*>

RenewalSchedule：<文字列>

ドメインを指定しない場合、このコマンドにより、サーバ証明書を管理しているACMEサービスの設定が書き込まれます。ドメインを指定すると、そのドメインの設定が書き込まれます。

指定したドメインにまだACMEが設定されていない場合、このコマンドはデフォルトプロバイダーの UUID を使用してそのドメインの ACME 設定を書き込みます。

指定したドメインにすでにACMEが設定されている場合、このコマンドは指定された設定だけを更新し、指定されていない設定は変更しません。

AcmeManaged パラメータを指定する必要があります。AcmeManaged を Automated に設定する場合は、RenewalSchedule と RenewKey も指定する必要があります。

例：`xCommand ACME Settings Write AcmeManaged: 「Manual」`

```
xCommand ACME Settings Write AcmeManaged: 「Automated」 Domain: 「example.com」
RenewalSchedule: 「{ 「DaysOfWeek」:[ 「Mon」 ],「TimeOfDay」:「04:00」 }」 RenewKey: 「Rotate」
```

xCommand ACME Sign

CSR に署名します。

Domain：<文字列>

NumSanEntries：<*-2147483648..2147483647*>

サーバ証明書の CSR を該当する ACME プロバイダーに送信する場合は、パラメータを指定せずにコマンドを入力します。ドメイン証明書の CSR を該当する ACME プロバイダーに送信する場合は、ドメインを指定します。

`NumSanEntries`パラメータは指定しないでください。これはユーザが変更するためのものではありません。

例：`xCommand Acme Sign`

```
xCommand ACME Sign Domain: 「example.com」
```

xCommand Admin Account Add

ローカル管理者アカウントを追加します。

Name(r): <S: 0, 128>

このアカウントのユーザ名。

Password(r)：<パスワード>

この アカウントのパスワード。

AccessAPI：*<On/Off>*

このアカウントが API を使用してシステムのステータスと設定にアクセスできるかどうか。デフォルトは On です。

AccessWeb：*<On/Off>*

このアカウントが Web インターフェイスを使用してシステムにログインできるかどうか。デフォルトは On です。

Enabled：*<On/Off>*

アカウントが有効になっているか、無効になっているかを示します。無効なアカウントへのアクセスは拒否されます。デフォルトは On です。

例：`xCommand Admin Account Add Name: 「bob_smith」Password: 「abcXYZ_123」 AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Account Delete

ローカル管理者アカウントを削除します。

Name(r): <S: 0, 128>

削除するアカウントのユーザ名。

例：`xCommand Admin Account Delete: 「bob_smith」`

xCommand Admin Group Add

Name(r): <S: 0, 128>

管理者グループの名前。

AccessAPI：*<On/Off>*

このグループのメンバーが API を使用してシステムのステータスと設定にアクセスできるかどうか。デフォルトは On です。

AccessWeb：*<On/Off>*

このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうか。デフォルトは On です。

Enabled：*<On/Off>*

グループが有効であるか無効であるかを示します。無効なグループのメンバーへのアクセスは拒否されます。デフォルトは On です。

例：`xCommand Admin Group Add Name: 「administrators」AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Group Delete

管理者グループを削除します。

Name(r): <S: 0, 128>

削除するグループの名前。

例：`xCommand Admin Group Delete: 「administrators」`

xCommand Allow List Add

許可リストにエントリを追加します。

PatternString(r)：*<S: 1, 60>*

許可リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが許可リストのパターンの 1 つと一致した場合に登録が許可されます。

PatternType：*<Exact/Prefix/Suffix/Regex>*

許可リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

デフォルトは Exact です。

Description: <S: 0,64>

自由形式の許可リスト ルールの説明。

例：`xCommand Allow List Add PatternString: 「John.Smith@example.com」 PatternType: Exact Description: 「Allow John Smith」`

xCommand Allow List Delete

許可リストからエントリを削除します。

AllowListId(r)：*<1..2500>*

削除するエントリのインデックス。

例：`xCommand Allow List Delete AllowListId: 2`

xCommand Boot

Expresswayをリブートします。

このコマンドにはパラメータがありません。

例：`xCommand Boot`

xcommand Certs Command for Server CSR

Server 証明書署名要求（CSR）生成を許可

Publickeyalgorithm パラメータのデフォルト値は 「RSA」 です

でサポートされているキーサイズは次のとおりです。

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

例：`xcommand Certs Command csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA`

xcommand Certs Command for Domain CSR

ドメイン証明書署名要求（CSR）生成を許可

Publickeyalgorithm パラメータのデフォルト値は 「RSA」 です

でサポートされているキーサイズは次のとおりです。

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

例： `xcommand Certs Command: csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA Domain: cisco.com`

xCommand Check Bandwidth

指定したタイプと帯域幅のコールが 2 つのノード間で取得するステータスとルート（ノードとリンクのリスト）を返す診断ツール。このコマンドは、既存のシステム設定を変更しません。

Node1(r)：*<S: 1, 50>*

コールを発信するサブゾーンまたはゾーン。

Node2(r)：*<S: 1, 50>*

コールが終端されるサブゾーンまたはサブゾーン。

Bandwidth(r)：*<1..100000000>*

コールの要求された帯域幅（kbps 単位）。

CallType(r)：*<Traversal/NonTraversal>*

コール タイプがトラバーサルか非トラバーサルか。

例：`xCommand Check Bandwidth Node1: 「DefaultSubzone」 Node2: 「UK Sales Office」 Bandwidth: 512 CallType: nontraversa`

xCommand Check Pattern

システムにエイリアス トランスフォーメーションを設定する前にそのトランスフォーメーション（ローカルまたはゾーン）の結果を確認できる診断ツール。

Target(r)：*<S: 1, 60>*

パターン マッチまたはトランスフォーメーションのテストに使用するエイリアス。

Pattern(r)：*<S: 1, 60>*

エイリアスと比較するパターン。

Type(r)：*<Exact/Prefix/Suffix/Regex>*

適用するパターン動作のエイリアスとパターン文字列をどのように照合するか。

Behavior(r)：*<Strip/Leave/Replace/AddPrefix/AddSuffix>*

エイリアスをどのように変更するかを示します。

Replace：*<S: 0, 60>*

選択したパターン動作とともに使用するテキスト文字列。

例：`xCommand Check Pattern Target: 「bob@a.net」 Pattern:「@a.net」 Type: 「suffix」 Behavior: replace Replace: 「@a.com」`

xCommand Clear All Status

システムのすべてのステータスと履歴をクリアします。

例：`xCommand Clear All Status`

xCommand Cluster Address Mapping Add

Fqdn(r)：<値>

IpAddress(r)：<値>

FQDN/IP マッピング エントリをクラスタ アドレス マッピング テーブルに追加します。

xCommand Cluster Address Mapping Delete

Fqdn(r)：<値>

IpAddress(r)：<値>

FQDN/IP マッピング エントリをクラスタ アドレス マッピング テーブルから削除します。

xCommand CMS Add

Cisco Meeting Server Web ブリッジを管理します。ゲスト アカウント クライアント URI を追加します。

Name: <値>

例：`xCommand CMS Add name: 「join.example.com」`

xCommand CMS Delete

Cisco Meeting Server Web ブリッジを管理します。ゲスト アカウント クライアント URI を削除します。

Name: <値>

例：`xCommand CMS Delete name: 「join.example.com」`

xCommand Credential Add

ローカル認証データベースにエントリを追加します。

Name(r)：<文字列>

ローカル認証データベースにこのエントリの名前を定義します。

Password(r)：<パスワード>

ローカル認証データベースにこのエントリのパスワードを定義します。

プレーン テキストの最大長は 128 文字で、これらの文字は暗号化されます。

例：`xCommand Credential Add Name: 「alice」 Password: 「abcXYZ_123」`

xCommand Credential Delete

ローカル認証データベースからエントリを削除します。

Name(r)：<文字列>

削除するエントリの名前。

例：`xCommand Credential Delete Name: 「alice」`

xCommand CUCM Config Add

Unified CM パブリッシャでルックアップを実行します。

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

Axlpassword(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するパスワード。

Axlusername(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するユーザ名。

CertValidationDisabled：*<On/Off>*

Unified CM パブリッシャが提示した証明書と照合する X.509 証明書の確認を制御します。デフォルトは On です。

例：`xCommand CUCM Config Add Address: 「cucm.example.com」 Axlpassword: 「xyz」 Axlusername: 「abc」`

xCommand CUCM Config Delete

Unified CM パブリッシャの詳細情報を削除します。

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

例：`xCommand CUCM Config delete Address: 「cucm.example.com」`

xCommand CUCM Mixed Mode Check

Address(r)：<値>

Unified CM パブリッシャの FQDN または IP アドレス。

Axlpassword(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するパスワード。

Axlusername(r)：<値>

Unified CM パブリッシャにアクセスするために Expressway が使用するユーザ名。

Command Custom Notification Add

アラームベースの電子メール通知用にカスタマイズされたエントリを追加します。アラーム ID ごとに、アラーム ID の通知を無効にするか、指定された電子メールアドレスに送信します。

alarm_id：<String> 通知をカスタマイズまたは無効化するアラーム ID を入力します。

custom_email：<S:0,254>通知が「カスタム」の場合は、選択したアラーム通知の送信に使用する電子メール ID を入力します。

disable_notify：<on/off> 選択したアラームに対するアクションを選択します。

- On：選択したアラームに関する通知は送信されません。
- Off：選択したアラームに関する通知が電子メールフィールドに入力された電子メール ID に送信されます。

デフォルトは On です。

カスタム通知を追加するには、disable_notify を 「[オフ（Off）]」 に指定します。

カスタム通知が追加された後は、xconfiguration コマンドの 「[アラーム通知電子メール（Alarm Notification Email）]」にリストされます。

xCommand Custom Notification Delete

アラームベースの電子メール通知用にカスタマイズされたエントリを削除します。

alarm_id(r): <String>：通知をカスタマイズまたは無効化するアラーム ID を入力します。

xCommand Default Links Add

デフォルトのサブゾーン、トラバーサルサブゾーン、およびデフォルトゾーン間のリンクを復元します。

このコマンドにはパラメータがありません。

例：`xCommand Default Links Add`

xCommand Default Values Set

システム パラメータをデフォルト値にリセットします。レベル 1 は、レベル 2 とレベル 3 の項目を除き、ほとんどの設定項目をデフォルト値にリセットします。レベル 2 は、リモート認証関連の設定項目とレベル 1 の項目をデフォルト値にリセットします。レベル 3 は、重大なすべての設定項目と、レベル 1 および レベル 2 の項目をデフォルト値にリセットします。

Level(r)：*<1..3>*

リセットするシステム パラメータのレベル。

例：`xCommand Default Values Set Level: 1`

xCommand Deny List Add

拒否リストにエントリを追加します。

PatternString(r)：*<S: 1, 60>*

拒否リストに追加するエントリを指定します。エンドポイントのエイリアスの 1 つが拒否リストのパターンの 1 つと一致した場合は登録が許可されません。

PatternType：*<Exact/Prefix/Suffix/Regex>*

拒否リスト内のエントリがプレフィックスか、サフィックスか、正規表現か、または完全一致かを指定します。

Exact：文字列は 1 文字も違うことなくエイリアスと一致する必要があります。

[プレフィックス（Prefix）]：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。

デフォルトは Exact です。

Description: <S: 0, 64>

自由形式の拒否リスト ルールの説明。

例：`xCommand Deny List Add PatternString: 「sally.jones@example.com」 PatternType: exact Description: 「Deny Sally Jones」`

xCommand Deny List Delete

拒否リストからエントリを削除します。

DenyListId(r)：*<1..2500>*

削除するエントリのインデックス。

例：`xCommand Deny List Delete DenyListId: 2`

xCommand Disconnect Call

コールを切断します。

Call：*<1..1000>*

切断するコールのインデックス。

CallSerialNumber：*<S: 1, 255>*

切断するコールのシリアル番号。コールインデックスかコールシリアル番号かのいずれかを指定する必要があります。

例：`xCommand Disconnect Call CallSerialNumber: 「6d843434-211c-11b2-b35d-0010f30f521c」`

xCommand DNS Lookup

指定したホスト名について DNS を照会します。

Hostname：<値>

照会するホストの名前。

RecordType：*<all/a/aaaa/srv/naptr>*

検索するレコードのタイプ。指定しない場合は、すべてのレコード タイプが返されます。

例：`xCommand DNS Lookup Hostname: 「example.com」 RecordType: all`

xCommand DNS Per Domain Server Add

特定のドメインのホスト名を解決するためのみに使用する DNS サーバを追加します。

Address(r)：<値>

関連付けられたドメイン名のホスト名を解決するときに使用する DNS サーバの IP アドレス。

Domain1(r)：<値>

特定の DNS サーバに関連付けるドメイン。

Domain2(r)：<値>

特定の DNS サーバに関連付けるオプションの 2 番目のドメイン。

Index：*<0..5>*

追加するサーバのインデックス。

例：`xCommand DNS Server Add Address: 「192.168.12.0」 Index: 1`

xCommand DNS Per Domain Server Delete

特定のドメインのホスト名を解決するために使用する DNS サーバを削除します。

Address：<値>

削除する DNS サーバの IP アドレス。

例：`xCommand DNS Per Domain Server Delete Address: 「192.168.12.0」`

xCommand DNS Server Add

デフォルトのDNSサーバを追加します。デフォルトのサーバは、ルックアップするドメインに定義されたドメイン単位の DNS サーバがない場合に使用します。

Address(r)：<値>

ドメイン名を解決するときに使用するデフォルトの DNS サーバの IP アドレス。

Index：*<0..5>*

追加するサーバのインデックス。

例：`xCommand DNS Server Add Address: 「192.168.12.0」 Index: 1`

xCommand DNS Server Delete

DNS サーバを削除します。

Address：<値>

削除する DNS サーバの IP アドレス。

例：`xCommand DNS Server Delete Address: 「192.168.12.0」`

xCommand Domain Add

この Expressway が権限を持つドメインを追加します。

Name(r): <S: 1, 128>

ドメイン名。複数のレベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。

Edgesip：*<On/Off>*

Unified CM がエンドポイントの登録、コール制御、およびプロビジョニングのサービスを提供します。デフォルトは Off です。

Edgexmpp：*<On/Off>*

Unified CM IM&P サービスがこの SIP ドメインのインスタント メッセージングとプレゼンスのサービスを提供します。デフォルトは Off です。

Sip：*<On/Off>*

Expressway がこのドメインに権限を持つかどうかを制御します。Expressway は、ドメインの SIP レジストラおよびプレゼンスサーバーとして機能し、このドメインを含むエイリアスで登録を試みるすべての SIP エンドポイントの登録要求を受け入れます。デフォルトは On です。

Xmppfederation：*<On/Off>*

XMPP フェデレーションにドメインを使用できるかどうかを制御します。デフォルトは Off です。

例：`xCommand Domain Add Name: 「100.example-name.com」 Authzone: 「Traversal zone」 Edge: Off Sip: On`

xCommand Domain Delete

ドメインを削除します。

ドメイン *Id(r): <1..200>*

削除するドメインのインデックス。

例：`xCommand Domain Delete DomainId: 2`

xCommand Domain Certs

サーバ名指定（SNI）のマルチドメイン証明書を管理します。

各ドメイン証明書 xCommand には、実行する操作を指定する「command」パラメータと、その後に特定のコマンドに必要な追加パラメータが必要です。

ドメイン証明書コマンドと関連するパラメータ：

domain_list：SNI の証明書を管理するドメインを一覧表示します。

パラメータ：（なし）

例：`xCommand Domain Certs command: domain_list`

domain_create：SNI の証明書を管理するための新しいドメインを作成します。

パラメータ：domain

例：`xCommand Domain Certs command: domain_create domain: a.com`

domain_delete：指定した証明書ドメインを削除します。

パラメータ：domain

例：`xCommand Domain Certs command: domain_delete domain: a.com`

is_csr_pending：ドメインの証明書署名要求が保留中の場合は true を返します。

パラメータ：domain

例：`xCommand Domain Certs command: is_csr_pending domain: a.com`

csr_create：ドメインの証明書署名要求を作成します。

パラメータ：domain、subjectfields、sans、digestalgorithm、keysize

例：
```
xCommand Domain Certs command: csr_create domain: a.com keysize: 4096
digestalgorithm: sha256 sans: 'DNS:host1.a.com, DNS:host2.a.com' subjectfields: '{ 「CN」
「www.a.com」, 「C」: 「US」, 「ST」: 「North Carolina」, 「L」:「RTP」, 「O」: 「a」, 「OU」:
「example org unit」, 「emailAddress」: 「admin@a.com」 }'
```

（注）
- xCommand パラメーター値は、スペースを含めることができるように、単一引用符で囲むことができます。
- sans はオプションのカンマで区切られたホスト名のリストです。各ホスト名の先頭には「DNS:」が追加されています（RFC5280 参照）。
- subjectfields は、各 [サブジェクト名（Subject Name）] フィールドの名前と値のペアのリストを含む JSON オブジェクトです（RFC5280 参照）。
- JSON の名前と値は、次のように二重引用符で囲む必要があります。
- keysize は、CSR 用に生成された秘密キーのビットの長さです。
- digestalgorithm は、CSR に署名するために使用されるメッセージ ダイジェスト アルゴリズムの名前です（「openssl dgst」を参照）。

csr_get：保留中の証明書署名要求を PEM 形式で返します。

パラメータ：domain

例：`xCommand Domain Certs command: csr_get domain: a.com`

csr_delete：保留中の証明書署名要求を削除します。

パラメータ：domain

例：`xCommand Domain Certs command: csr_delete domain: a.com`

is_cert_set：ドメインに対して証明書が設定されている場合は true を返します。

パラメータ：domain

例：`xCommand Domain Certs command: is_cert_set domain: a.com`

cert_put：証明書と秘密キーをアップロードします。

パラメータ：domain、certpath、keypath

例：`xCommand Domain Certs command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`

（注）
- 証明書とキーがまだアップロードされていない場合は、両方を指定する必要があります。
- 証明書署名要求が進行中の場合は、証明書のみをアップロードできます。

cert_get：ドメインの証明書を PEM 形式で返します。

パラメータ：domain

例：`xCommand Domain Certs command: cert_get domain: a.com`

cert_delete：ドメインの証明書と秘密キーを削除します。

パラメータ：domain

例：`xCommand Domain Certs command: cert_delete domain: a.com`

default command help："

Certpath：<文字列>

Command：
<domain_list/domain_create/domain_delete/csr_create/csr_get/csr_delete/cert_put/cert_get/cert_delete/is_csr_pending/is_cert_set>

Digestalgorithm：*</sha256/sha384/sha512>*

Domain：<文字列>

Keypath：<文字列>

Keysize：<値>

San：<文字列>

Subjectfields：<文字列>

xCommand Edge SSO Delete Tokens

特定のユーザに対して発行されたすべてのトークンを削除します。

Username(r)：<文字列>

削除するユーザのトークンを指定します。

例：`xCommand Edge SSO Delete Tokens Username: 「APerson」`

xCommand Edge SSO Purge Tokens

すべてのユーザに発行したすべてのトークンを削除します。

例：`xCommand Edge SSO Purge Tokens`

xCommand Edge SSO Status Clear

SSO 要求/応答カウンタを 0 にリセットします。

例：`xCommand Edge SSO Status Clear`

xCommand Feedback Deregister

特定のフィードバック要求を非アクティブ化します。

ID：*<1..3>*

非アクティブ化するフィードバック要求のインデックス。

例：`xCommand Feedback Deregister ID: 1`

xCommand Feedback Register

式で記述されたイベントまたはステータス変更に関する通知をアクティブ化します。通知は、指定された URL に XML 形式で送信されます。最大 15 の式を 3 のフィードバック ID に登録できます。

ID：*<1..3>*

この特定のフィードバック要求の ID。

URL(r): <S: 1, 256>

通知が送信される URL。

Expression.1..15：*<S: 1, 256>*

通知するイベントまたはステータス変更。有効な式は次のとおりです。

```
Status/Ethernet   Event/RegistrationFailure  Event/AuthenticationFailure
Event/    Status/Calls    Event/CallDisconnected
Event/CallFailure   Status/NTP    Status/LDAP
Status/Zones   Event/Bandwidth    Event/Locate
Status/Feedback   Event/CallAttempt   Event/CallConnected
Event/ResourceUsage   Status/ExternalManager
```

例：`xCommand Feedback Register ID: 1 URL: 「http://192.168.0.1/feedback/」 Expression.1: 「Status/Calls」 Expression.2: 「Event/CallAttempt」`

xCommand Find Registration

指定したエイリアスに関連付けられた登録に関する情報を返します。エイリアスはコマンドが発行された Expressway に登録されている必要があります。

Alias(r)：*<S: 1, 60>*

検出する必要があるエイリアス。

例：`xCommand Find Registration Alias: 「john.smith@example.com」`

重要 このコマンドは、Cisco TelePresence Video Communication Server（VCS）**のみ**に適用されます。

xCommand Fips

FIPS140-2暗号化モードを設定します。

Command：*<leave/enter/status>*

システムの FIPS140-2 暗号化モードの現在のステータスを入力、維持、または提供します。

例：`xCommand Fips Command: enter`

xCommand Force Config Update

このピアの関連設定を強制的に更新し、クラスタ プライマリの設定と一致するようにします。

このコマンドにはパラメータがありません。

例：`xCommand Force Config Update`

重要 HSM 機能は、Expressway ソフトウェアバージョンに応じて、プレビュー機能のみ使用できます。たとえば、バージョン X12.6 のプレビュー機能です。

Expressway バージョンのリリースノートを確認してから使用する前、またそのステータスがソフトウェアバージョンのプレビューである場合は、**プレビュー機能として実装する場合、および Expressway リリースノートに含まれるプレビューの免責事項に従って、そのステータスがソフトウェアバージョンのプレビューである場合に限り 、この 2 つのコマンドを使用してください。**

xCommand HSM Mode Read

Expressway に設定されている現在の HSM モードに戻します。

例：`xCommand HSM Mode Read`

xCommand HSM Mode Write

Expressway の HSM モードを変更します。Expressway で HSM 設定と少なくとも 1 つの HSM モジュールがすでに構成されている場合にのみ使用できます。

Mode：<enabled, disabled>

例：`xCommand HSM Mode Write Mode: enabled`

xCommand HSM Module Add

Expressway 構成に新しい HSM モジュールを追加します。このコマンドを使用する前に、HSM プロバイダーの設定を構成する必要があります。

Ip(r): <S: 0, 1024>

追加する HSM デバイスの IP アドレス。

Port：*<1..65535>*

nShield HSM との通信に使用されているポート。オプション。デフォルトは 9004 です。

Esn: <S: 0, 1024>

nShield HSM のシリアル番号。必須。

Kneti: <S: 0, 1024>

nShield HSM の検証に使用されるセキュリティハッシュ。必須。

例：`xCommand HSM Module Add Ip: 1.1.1.1 Port: 9004 Esn: abcd-abcd-abcd Kneti: abcd1234abcd1234a`

xCommand HSM Module Remove

Expressway で使用されるモジュールのリストから HSM モジュールを削除します。

Ip(r): <S: 0, 1024>

このコマンドには、すでに設定されている HSM モジュールの IP アドレスが必要です。

例：`xCommand HSM Module Remove Ip: 1.1.1.1`

xCommand HSM Modules

Expressway により使用されるすべての HSM モジュールの一覧を返します。

例：`xCommand HSM Modules`

xCommand HSM Settings Read

現在設定されている HSM 設定を返します。

例：`xCommand HSM settings Read`

xCommand HSM Settings Write

使用する HSM プロバイダーを設定します（サポートされているプロバイダーの詳細については、*Expressway* リリースノートを参照してください。サポートはプレビューベースのみである可能性があります）。

Provider(r): <nShield>

設定する HSM プロバイダー。

Rfsip: <S: 0, 1024>

Thales RFS（リモートファイルシステム）の IP アドレス。HSM を使用する場合は必須です。

Rfsport: <1..65535>

RFS との通信に使用されるポート。HSM を使用する場合は必須です。デフォルト 9004

例：`xCommand HSM Settings Write Provider: 「nShield」 Rfsip: 「1.1.1.1」 Rfsport: 「9004」`

xCommand HTTP Allow List Export

HTTP 許可リストのルールをデータベースから CSV 形式でエクスポートします。

File: <S>

ルールが CSV 形式でエクスポートされるファイルへのパスを指定します。ファイルパスは、'/tmp/' から始まります。

Deployment： *<S>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

xCommand HTTP Allow List Export Test

HTTP 許可リストのテストをデータベースから CSV 形式でエクスポートします。

File: <S>

テストが CSV 形式でエクスポートされるファイルへのパスを指定します。ファイルパスは、'/tmp/' から始まります。

Deployment： *<S>*

URL と共に使用し、どの導入でこのテストを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

xCommand HTTP Allow List Rule Add

HTTP の許可リストに 1 つまたは複数のルールを追加します。少なくとも URL または URLFile を指定する必要があります。

URL(r)： *<S>*

HTTP クライアントにアクセスを許可するリソースの URL を指定します。IPv6 アドレスには RFC 2732 形式を使用する必要があります。

例：`https://[2001:DB8::1]:8443/path` または `https://www.example.com:8443/resource`

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とするとクライアントは `http://hostname.SystemDNSDomain:80` に含まれるすべてにアクセスできます。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

複数のルールを含むCSVファイルへのパスを指定します。許可リストによるファイル参照の決定を参照してください。

URL を指定する場合は URLFile を指定しないでください。

MatchType:<exact/starts-with/startswith/prefix>

URL と共に使用し、ルールが URL に含まれるものに正確に一致するか、またはプレフィックス一致の基本としてそれを使用するかを指定します。指定しない場合、デフォルトで `exact` に設定されます。そのほかの選択肢はすべて同等です。

Deployment：*<S:* 「*Your Deployment 1*」/「*Your Deployment 2*」*>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

Description: <S: 128>

ルールを説明するテキスト。

HttpMethods:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

このルールで許可する一連のメソッドをカンマで区切って指定します。メソッドを指定しない場合、ルールでは **[設定（Configuration）] > [ユニファイドコミュニケーション（Unified Communications）] > [HTTP 許可リスト（HTTP allow list）] > [編集可能なインバウンドルール（Editable inbound rules）]** に設定されたデフォルトのメソッドが使用されます。

例：`xCommand HTTP Allow List Rule Add URLfile: 「tmp/rules.csv」`

例 2：`xCommand HTTP Allow List Rule Add URL: 「https://cucm2.example.com:8443/partial/path」 MatchType: starts-with Description: 「https access to read everything below partial/path/ on cucm2.example.com」 HttpMethods: 「OPTIONS,GET」`

xCommand HTTP Allow List Rule Delete

HTTP の許可リストから 1 つまたは複数のルールを削除します。少なくとも URL または URLFile を指定する必要があります。シングル ホストの複数のルールがあればそのほかのパラメータを指定する必要があります。

URL(r)： *<S>*

削除するルールのURLを指定します。

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とすると `http://hostname.SystemDNSDomain:80` のルールを削除します。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

削除する複数のルールを含む CSV ファイルへのパスを指定します。

URL を指定する場合は URLFile を指定しないでください。

MatchType:<exact/starts-with/startswith/prefix>

URL と共に使用し、ルールが URL に含まれるものに正確に一致するか、またはプレフィックス一致の基本としてそれを使用するかを指定します。指定しない場合、デフォルトで `exact` に設定されます。そのほかの選択肢はすべて同等です。

Deployment： *<S>*

URL と共に使用し、どの導入でこのルールを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合、導入を指定しなければ、ルールではデフォルトの導入が使用されます。

Description: <S: 128>

ルールを説明するテキスト。

HttpMethods:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

このルールで許可する一連のメソッドをカンマで区切って指定します。メソッドを指定しない場合、ルールでは **[設定（Configuration）]** > **[ユニファイドコミュニケーション（Unified Communications）]** > **[HTTP 許可リスト（HTTP allow list）]** > **[編集可能なインバウンドルール（Editable inbound rules）]** に設定されたデフォルトのメソッドが使用されます。

例 1：`xCommand HTTP Allow List Rule Delete URLfile: 「tmp/rules.csv」`

例 2：`xCommand HTTP Allow List Rule Delete URL: 「https://cucm2.example.com:8443/partial/path」 MatchType: starts-with Description: 「https access to read everything below partial/path/ on cucm2.example.com」 HttpMethods: 「OPTIONS,GET」`

xCommand HTTP Allow List Rules Test

(Experimental)

（CSV ファイルに定義されている）ルールのリストに対して（CSV ファイルに定義されている）URL のコレクションをテストします。このコマンドを使用して、ルールを適用する前にテストしたり、既存のルールが正常に機能しているかどうかテストしたりできます。

テスト、またはルール、あるいはその両方を CSV ファイルとして指定できます。両方を指定すると、Tests CSV ファイル内のテストが、Rules CSV ファイル内にルールに対して実行されます。1 つまたは両方のパラメータを除外する場合、このコマンドは、Expressway に既にあるルールまたはテスト（あるいはその両方）を使用します。（Workflow ルールを確認するには、`xstatus collaborationedge httpallowlist` を使用してください）。

Tests： <*S*>

複数のテストを含む CSV ファイルへのパス（たとえば `/tmp/tests.csv`）を指定します。許可リスト テスト ファイル リファレンスを参照してください。

Rules： <*S*>

ユーザがテストする複数のルールを含むCSVファイルへのパスを指定します。たとえば`/tmp/rules.csv`許可リストによるファイル参照の決定を参照してください。

例：`xCommand HTTP Allow List Rules Test Tests: 「/tmp/tests.csv」 Rules: 「/tmp/rules.csv」`

xCommand HTTP Allow List Test Add

(試験版)

HTTP 許可リストに対してテストする 1 つ以上の URL を追加します。少なくとも URL または URLFile を指定する必要があります。URL を指定する場合は、ExpectedResult を指定する必要があります。

URL(r)： *<S>*

テスト URL を指定します。IPv6 アドレスには RFC 2732 形式を使用する必要があります。

例：`https://[2001:DB8::1]:8443/path` または `https://www.example.com:8443/resource`

URLFile を指定する場合は URL を指定しないでください。

URL にはプロトコル（`http://` または `https://`）とホスト名を含める必要があります。また、URL をより限定的なものにするには、ドメイン、ポート、パスも含めます。URL の一部を省略すると、Expressway はデフォルトを指定します。たとえば `http://hostname` とすると `http://hostname.SystemDNSDomain:80` の URL をテストします。http のデフォルト ポートは 80、https のデフォルト ポートは 443 です。

URLFile(r)： *<S>*

複数のテストを含む CSV ファイルへのパスを指定します。許可リスト テスト ファイル リファレンスを参照してください。

URL を指定する場合は URLFile を指定しないでください。

ExpectedResult （R）:<allow/block>

許可リストに従って URL を許可またはブロックするかどうかを指定するには、URL と共に指定する必要があります。

Deployment： *<S>*

URL と共に使用し、どの導入でこのテストを使用するかを指定します。複数の導入がない場合は必要ありません。複数の導入がある場合は、導入を指定しなければテストはデフォルトの導入を使用します。

Description: <S: 128>

テストを説明するテキスト。

HttpMethod:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

テストする 1 つのメソッドを指定します。メソッドを指定しないと、テストでは GET が使用されます。

例 1：`xCommand HTTP Allow List Test Add URLfile: 「/tmp/tests.csv」`

例 2：`xCommand MRA Allow List Test Add URL:「https://cucm2.example.com:8443/partial/path」 ExpectedResult: block Description: 「https access to write to partial/path/ on cucm2.example.com」 HttpMethod: 「POST」`

xCommand HTTP Allow List Test Delete

(試験版)

HTTP の許可リストから 1 つまたは複数のテスト URL を削除します。少なくとも URL または URLFile を指定する必要があります。URL を指定する場合は、ExpectedResult を指定する必要があります。

URL(r)： *<S>*

削除するテスト URL を指定します。

URLFile を指定する場合は URL を指定しないでください。

URLFile(r)： *<S>*

削除する複数のテストを含む CSV ファイルへのパスを指定します。

URL を指定する場合は URLFile を指定しないでください。

ExpectedResult （R）:<allow/block>

削除するテストで期待される成果を指定します。テストを削除するには、必要。

Deployment： *<S>*

削除するテストを使用している導入を指定します。複数の導入がない場合は必要ありません。

Description: <S: 128>

テストを説明するテキスト。相互に区別できない複数のテストがある場合以外、テストを削除する必要はありません。

HttpMethod:<OPTIONS/GET/HEAD/POST/PUT/DELETE>

削除するテストで使用されているメソッドを指定します。メソッドを省略すると、Expressway はこのコマンドで現在のデフォルトのメソッドを使用します。これは、テストが対応するメソッドで作成されていないと削除が失敗する可能性があることを意味します。

例 1：`xCommand HTTP Allow List Test Delete URLfile: 「/tmp/tests.csv」`

例 2：`xCommand HTTP Allow List Test Delete URL: 「https://cucm2.example.com:8443/partial/path」 ExpectedResult: allow HttpMethod: 「get」`

xCommand HTTP Proxy Jabber CTargets Add

Jabber Guest サーバを設定して Jabber Guest ドメインと関連付けます。

DomainIndex(r)：*<0..200>*

この Jabber Guest サーバが関連付けられたドメインのインデックス。

Host(r)：*<S:1,1024>*

選択したドメインに使用する Jabber Guest サーバの FQDN。これは、非修飾ホスト名または IP アドレスではなく、FQDN である必要があります。

同じドメインに別のプライオリティで代替アドレスを指定できます。

Priority：*<0..9>*

このドメインに対してこのホスト名への接続を試行する順序。ドメインのプライオリティ 1 のすべてのホスト名が最初に試行され、次にプライオリティ 2 のすべてのホスト名という順で実行されます。

例：`xCommand HTTP Proxy Jabber CTargets Add DomainIndex: 2 Host: jabberguest.example.com`

Command HTTP Proxy Jabber CTargets Delete

設定された Jabber Guest サーバを Expressway から削除します。

*Host(r): <S:1,1024>*削除する Jabber Guest サーバの FQDN。

xCommand IMP Server Add

Microsoft SIP Simple メッセージをルーティングする外部のメッセージング サーバを追加します。

IMP(r): <値> *configuration/b2bua/imp/imp*

xCommand IMP Server Delete

外部メッセージング サーバを削除します。

IMP(r): <値> *configuration/b2bua/imp/imp*

xCommand License Smart Deregister

評価期間が満了していなければ、製品は評価モードに戻ります。製品で使用されるライセンス付与がバーチャル アカウントにすぐに戻されて、他の製品インスタンスで使用できるようになります。

xCommand License Smart Register Idtoken: <String>

Smart Software Manager または Smart Software Manager サテライトから生成した製品インスタンス登録トークンを使用して製品を登録します。

xCommand License Smart Renew Auth

Cisco Smart Software Manager によるネットワーク接続の問題が原因で、自動認証ステータスの更新に失敗した場合は、この操作を実行します。

xCommand License Smart Renew ID

Cisco Smart Software Manager のネットワーク接続の問題が原因で自動登録の更新に失敗した場合は、この操作を実行します。

xCommand License Smart Reregister: <String>

次の場合、この操作を実行して製品インスタンスを再登録します。

- この製品インスタンスの以前の登録の試行は、ネットワーク接続の問題のために失敗しました。この問題を解決した後に再登録する必要があります。
- 仮想アカウントにすでに登録されている製品インスタンスを別の仮想アカウントに再登録するには。

xCommand Link Add

新しいリンクを追加して設定します。

LinkName(r)：*<S: 1, 50>*

このリンクに名前を割り当てます。

Node1：*<S: 1, 50>*

このリンクを適用する最初のゾーンまたはサブゾーンを指定します。

Node2：*<S: 1, 50>*

このリンクを適用する 2 番目のゾーンまたはサブゾーンを指定します。

Pipe1：*<S: 1, 50>*

このリンクと関連付ける最初のパイプを指定します。

Pipe2：*<S: 1, 50>*

このリンクと関連付ける 2 番目のパイプを指定します。

例：`xCommand Link Add LinkName: 「Subzone1 to UK」 Node1: 「Subzone1」 Node2: 「UK Sales Office」 Pipe1: 「512Kb ASDL」`

xCommand Link Delete

リンクを削除します。

LinkId(r)：*<1..3000>*

削除するリンクのインデックス。

例：`xCommand Link Delete LinkId: 2`

xCommand Locate

Expressway のロケーション アルゴリズムを実行し、指定したエイリアスによって識別されたエンドポイントをローカルに検索し、指定した「ホップ」の回数内にネイバー上や DNS システムを通じて検出されたシステム上で見つけます。結果は xFeedback を通じて報告されます。そのため、このコマンド（xFeedback register event/locate）を発行する前にこのメカニズムをアクティブにする必要があります。

Alias(r)：*<S: 1, 60>*

見つけるエンドポイントに関連付けられたエイリアス。

HopCount(r)：*<0..255>*

検索で使用するホップ カウント。

Protocol(r)：*<H323/SIP>*

検索を開始するために使用するプロトコル。

SourceZone：*<S: 1, 50>*

検索要求をシミュレートするためのゾーン。デフォルトゾーン（不明なリモート システム）、ローカル ゾーン（ローカルに登録されたエンドポイント）、またはその他の設定済みのネイバー、トラバーサル クライアントまたはトラバーサル サーバ ゾーンから選択します。

Authenticated：*<Yes/No>*

検索要求を認証済みとして処理するかどうか。

SourceAlias：*<S: 0, 60>*

検索要求に使用する送信元エイリアス。デフォルトは xcom-locate です。

例：`xCommand Locate Alias: 「john.smith@example.com」 HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com`

xCommand Network Interface

LAN 2 ポートが管理およびコール シグナリングに有効になっているかどうかを制御します。

DualInterfaces(r)：*<enable/disable/status>*

LAN 2 ポートの現在のステータスの設定またはレポート。

例：`xCommand Networkinterface DualInterfaces: enable`

DedicatedManagementInterface: <enable/disable/status>

有効にすると、専用管理インターフェイス（DMI）が管理トラフィックに LAN3 ポートを使用します。（DMI を無効にしようとして、管理サービスがインターフェイスとしてのみ使用している場合、コマンドは失敗します。）

例：`xCommand Network Interface DedicatedManagementInterface: enable`

xCommand Network Limits

機能を制限するまでレートを制御します。

ヘルプを読むには、`xCommand Network Limits ?`を入力します。

xCommand NTP Server Add

システム時刻を同期するときに使用する NTP サーバを追加します。

Address(r)：<値>

追加する NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand NTP Server Add Address: ntp.server.example.com`

xCommand NTP Server Delete

Address(r)：<値>

削除する NTP サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand NTP Server Delete Address: 「ntp.server.example.com」`

xCommand Option Key Add

Expressway に新しいオプション キーを追加します。これらのキーは、Expressway のキャパシティを引き上げるなど、特別な機能を追加するために Expressway に追加されます。詳細については、シスコの担当者にお問い合わせください。

Key(r): <S: 0, 90>

ソフトウェア オプションのオプション キーを指定します。

例：`xCommand Option Key Add Key: 「1X4757T5-1-60BAD5CD」`

xCommand Option Key Delete

Expressway からソフトウェア オプション キーを削除します。

OptionKeyId(r)：*<1..64>*

削除するソフトウェア オプションの ID を指定します。

例：`xCommand Option Key Delete OptionKeyId: 2`

xCommand Ping

特定のホスト システムが接続可能であることを確認します。

Hostname：<値>

接続を試みるホスト システムの IP アドレスまたはホスト名。

例：`xCommand Ping Hostname: 「example.com」`

xCommand Pipe Add

新しいパイプを追加して設定します。

PipeName(r)：*<S: 1, 50>*

このパイプに名前を割り当てます。

TotalMode：*<Unlimited/Limited/NoBandwidth>*

パイプの総帯域幅の制限を制御します。

NoBandwidth：このパイプを使用してコールを発信できません。デフォルトはUnlimitedです。

Total：*<1..100000000>*

このパイプの帯域幅が制限されている場合にパイプで常に使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは500000です。

PerCallMode：*<Unlimited/Limited/NoBandwidth>*

個々のコールの帯域幅制限を制御します。

NoBandwidth：このパイプを使用してコールを発信できません。デフォルトはUnlimitedです。

PerCall：<1..100000000> 制限付きのコール単位モードでは、コールごとに使用可能な最大帯域幅（kbps単位）を設定します。デフォルトは1920です。

例：`xCommand Pipe Add PipeName: 「512k ADSL」 TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`

xCommand Pipe Delete

パイプを削除します。

PipeId(r)：*<1..1000>*

削除するパイプのインデックス。

例：`xCommand Pipe Delete PipeId: 2`

xCommand Policy Service Add

ポリシー サービスを追加します。

Name(r): <S: 0, 50>

このサービス ポリシーに名前を割り当てます。

Description: <S: 0, 64>

自由形式のポリシー サービスの説明。

Protocol：*<HTTP/HTTPS>*

リモートサービスに接続するために使用するプロトコルを指定します。デフォルトはHTTPSです。

Verify：*<On/Off>*

X.509 証明書のチェック、およびこの Expressway とポリシー サービス間の相互認証を制御します。有効になっている場合は、アドレス フィールドで指定したサーバの FQDN または IP アドレスがサーバの X.509 証明書内（サブジェクト共通名またはサブジェクト代替名のどちらかの属性）に含まれている必要があります。デフォルトは On です。

CRLCheck：*<On/Off>*

ポリシーサービスによって提供された証明書の証明書失効リストのチェックを制御します。有効になっている場合は、サーバの X.509 証明書が、その証明書の証明書発行機関の失効リストと照合して確認されます。デフォルトは Off です。

Address：*<S: 0, 128>*

リモート サービスの IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

Path：*<S: 0, 255>*

リモート サービスの URL を指定します。

StatusPath：*<S: 0..255>*

リモート サービス ステータスを取得するためのパスを指定します。デフォルトは status です。

UserName: <S: 0, 30>

リモートサービスにログインして照会するためにExpresswayが使用するユーザ名を指定します。

Password: <S: 0, 82>

リモートサービスにログインして照会するためにExpresswayが使用するパスワード。プレーンテキストの最大長は 30 文字です。

DefaultCPL：*<S: 0, 255>*

リモート サービスが使用できない場合に使用する CPL。デフォルトは <reject status='403' reason='Service Unavailable'/> です。

例：`xCommand PolicyServiceAdd Name: 「Conference」 Description: 「Conference service」`

```
Protocol: HTTPS Verify: On CRLCheck: On Address: 「service.example.com」 Path: 「service」
StatusPath: 「status」 UserName: 「user123」 Password: 「password12」3 DefaultCPL: 「<reject
status='403' reason='Service Unavailable'/>」
```

xCommand Policy Service Delete

ポリシー サービスを削除します。

PolicyServiceId(r)：*<1..20>*

削除するポリシー サービスのインデックス。

例：`xCommand Policy Service Delete PolicyServiceId: 1`

xCommand Remote Syslog Add

リモート syslog サーバのアドレスを追加します。

Address(r)：<値>

リモート syslog サーバの IP アドレスまたは FQDN。

Crlcheck：*<On/Off>*

syslog サーバが提供する証明書を証明書失効リスト（CRL）と照合して確認するかどうかを制御します。デフォルト：Off

Format：*<bsd/ietf>*

リモート syslog メッセージが作成される形式。デフォルト：bsd

Loglevel：*<emergency/alert/critical/error/warning/notice/informational/debug>*

この syslog サーバに送信するログ メッセージの最小シビラティ（重大度）。デフォルトは informational です。

Mode：*<bsd/ietf/ietf_secure/user_defined>*

syslog サーバにメッセージを送信するときに使用する syslog プロトコル。デフォルトは bsd です。

Port：*<1..65535>*

使用する UDP/TCP 宛先ポート。推奨されるポート：UDP=514 TCP/TLS=6514 デフォルト：514

Transport：*<udp/tcp/tls>*

syslog サーバと通信するときに使用するトランスポート プロトコル。デフォルトは udp です。

例：`xCommand RemoteSyslogAdd Address: 「remote_server.example.com」 Crlcheck: Off Format: bsd Loglevel: warning Mode: bsd Port: 514 Transport: udp`

xCommand Remote Syslog Delete

Address(r)：<値>

削除するリモート syslog サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

Port(r)：*<1..65535>*

削除するリモート syslog サーバが使用するポート。

Transport(r)：*<udp/tcp/tls>*

削除するリモート syslog サーバが使用するトランスポート プロトコル。

例：`xCommand RemoteSyslogDelete Address: 「remote_server.example.com」 Port: 514 Transport: udp`

xCommand Remove Registration

Expressway から登録を削除します。

Registration：*<1..3750>*

削除する登録のインデックス。

RegistrationSerialNumber：*<S: 1, 255>*

削除する登録のシリアル番号。

例：`xCommand RemoveRegistration RegistrationSerialNumber: 「a761c4bc-25c9-11b2-a37f-0010f30f521c」`

xCommand Restart

完全なシステム リブートを実行せずに Expressway を再起動します。

このコマンドにはパラメータがありません。

例：`xCommand Restart`

xCommand Route Add

新しい IP ルーティング（スタティック ルートとも呼ぶ）を追加して設定します。

Address(r)：*<S: 1, 39>*

このルートを適用するネットワークを決定するためにプレフィックス長とともに使用する IP アドレスを指定します。デフォルトは 32 です。

PrefixLength(r)：*<1..128>*

このルートを適用するネットワークの決定時に一致する必要がある IP アドレスのビット数を指定します。

Gateway(r)：*<S: 1, 39>*

このルートのゲートウェイの IP アドレスを指定します。

Interface：*<Auto/LAN1/LAN2>*

このルーティングに使用する LAN インターフェイス。*Auto*：使用に最適なインターフェイスを Expressway が選択します。デフォルトは Auto です。

例：`xCommand RouteAdd Address: 「10.13.8.0」 PrefixLength: 32 Gateway: 「192.44.0.1」`

xCommand Route Delete

ルートを削除します。

RouteId(r)：*<1..50>*

削除するルートのインデックス。

例：`xCommand Route Delete RouteId: 1`

重要　このコマンドは、Cisco TelePresence Video Communication Server（VCS）**のみ**に適用されます。

xCommand Secure Mode

高度なアカウント セキュリティのオプションを制御します。

Command(r)：*<on/off/status>*

削除するルートのインデックス。

例：`xCommand Secure Mode Command: off`

xCommand Search Rule Add

ゾーンまたはポリシー サービスに検索やコールをルーティングする新しい検索ルールを追加します。

Name(r): <S: 0, 50>

検索ルールの記述名。

ZoneName: <S: 0, 50>

エイリアスが検索ルールと一致するかどうかを照会するゾーンまたはポリシー サービス。

Description: <S: 0, 64>

自由形式の検索ルールの説明。

例：`xCommand SearchRuleAdd Name: 「"DNS lookup」ZoneName: 「Sales Office" Description」: 「Send query to the DNS zone」`

xCommand Search Rule Delete

検索ルールを削除します。

SearchRuleId(r)：*<1..2000>*

削除する検索ルールのインデックス。

例：`xCommand Search Rule Delete SearchRuleId: 1`

xCommand Trace Path

特定の宛先ホスト システムに送信されたネットワーク パケットが取得したパスを検出します。

Hostname：<値>

パスをトレースするホスト システムの IP アドレスまたはホスト名。

例：`xCommand Tracepath Hostname: 「example.com」`

xCommand Trace Route

特定の宛先ホスト システムに送信されたネットワーク パケットが取得したルートを検出します。また、パスの各ルータの詳細と、各ルータが要求への応答にかかった時間を報告します。

Hostname：<値>

ルートをトレースするホスト システムの IP アドレスまたはホスト名。

例：`xCommand Traceroute Hostname: 「example.com」`

xCommand Transform Add

新しいトランスフォーメーションを追加して設定します。

Pattern(r)：*<S: 1, 60>*

エイリアスを比較するパターンを指定します。

Type：*<Exact/Prefix/Suffix/Regex>*

適用するトランスフォーメーションで、パターン文字列をエイリアスとどのように照合するか。

*[*完全一致（*Exact*）*]*：文字列全体がエイリアスと 1 文字も違うことなく完全に一致する必要があります。

*[*プレフィックス（*Prefix*）*]*：文字列がエイリアスの先頭に表示される必要があります。

Suffix：文字列がエイリアスの末尾に表示される必要があります。

Regex：文字列は正規表現として処理されます。デフォルトは Prefix です。

Behavior：*<Strip/Replace/AddPrefix/AddSuffix>*

エイリアスをどのように変更するかを示します。

Strip：一致しているプレフィックスまたはサフィックスをエイリアスから削除します。

Replace：置換文字列内のテキストでエイリアスの一致している部分を置換します。

AddPrefix：エイリアスの前に置換文字列を追加します。

AddSuffix：エイリアスの後ろに置換文字列を追加します。デフォルトは Strip です。

Replace：*<S: 0, 60>*

選択したパターン動作とともに使用するテキスト文字列。

Priority：*<1..65534>*

指定したトランスフォーメーションにプライオリティを割り当てます。トランスフォーメーションはプライオリティ順に着信メッセージと比較されます。また、プライオリティはトランスフォーメーションごとに一意である必要があります。デフォルトは 1 です。

Description: <S: 0, 64>

自由形式のトランスフォーメーションの説明。

State：*<Enabled/Disabled>*

トランスフォーメーションが有効になっているか、無効になっているかを示します。無効になっているトランスフォーメーションは無視されます。デフォルトは Enabled です。

例：`xCommand TransformAdd Pattern: 「example.net」Type: suffix Behavior: replace Replace: 「example.com」Priority: 3 Description: 「Change example.net to example.com」State: Enabled`

xCommand Transform Delete

トランスフォーメーションを削除します。

TransformId(r)：*<1..100>*

削除されるトランスフォーメーションのインデックス。

例：`xCommand Transform Delete TransformId: 2`

xCommand Ucxn Config Add

Mobile & Remote Access で使用できるように Cisco Unity Connection サーバへのリンクを設定します。

Address(r)：*<S:0,1024>*

Unity Connection パブリッシャの FQDN または IP アドレス。

CertValidationDisabled：*<On/Off>*

CertValidationDisabled がオフ になっている場合、Cisco Unity Connection システムの FQDN または IP アドレスはそのシステムが提示する X.509 証明書内（証明書のサブジェクト共通名またはサブジェクト代替名のいずれか）に含まれている必要があります。証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

DeploymentId：*<1..65535>*

この Unity Connection パブリッシャは、選択した導入環境に関連付けられ、選択した導入環境の他のメンバーのみと通信できます。そのほかの導入環境のメンバーとは通信できません。

Password(r): <S: 1,1024>

Expressway-C が Cisco Unity Connection パブリッシャにアクセスするために使用するパスワード。

Username(r)：*<S:1,1024>*

Unified Connection パブリッシャにアクセスするために Expressway で使用されるユーザ名。たとえば、UC パブリッシャにおけるシステム管理者のロール。

xCommand Ucxn Config Delete

VCS から Cisco Unity Connection サーバへのリンクを削除します。

Address(r)：*<S:0,1024>*

Unity Connection パブリッシャの FQDN または IP アドレス。

xCommand XMPP Delete

IM and Presence サーバの詳細情報を削除します。

Address(r)：<値>

削除するリモート IM and Presence サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

例：`xCommand XMPP Delete Address: 「imp_server.example.com」`

xCommand XMPP Discovery

IM and Presence サーバの詳細情報を検出します。

Address(r)：<値>

検出するリモート IM and Presence サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）。

Axlpassword(r)：<パスワード>

IM and Presence パブリッシャへのアクセスに使用するパスワード。

Axlusername(r)：<文字列>

IM and Presenceパブリッシャにアクセスするためのユーザ名。

CertValidationDisabled：*<On/Off>*

IM and Presence パブリッシャが提示した証明書と照合した X.509 証明書の確認を制御します。デフォルトは On です。

例：`xCommand Xmppdiscovery Address: 「imp.example.com」 Axlpassword: 「xyz」 Axlpassword: 「abc」`

xCommand Zone Add

新しいゾーンを追加して設定します。

ZoneName(r)：*<S: 1, 50>*

このゾーンに名前を割り当てます。

Type(r)：*<Neighbor/TraversalClient/TraversalServer/ENUM/DNS>*

ローカル Expressway に関連して、指定したゾーンの特性を決定します。

Neighbor：新しいゾーンはローカル Expressway のネイバーになります。

TraversalClient：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサル クライアントです。

TraversalServer：ゾーン間にファイアウォールがあり、ローカル Expressway が新しいゾーンのトラバーサル サーバです。

ENUM：ゾーンに ENUM ルックアップで検出されたエンドポイントが含まれます。

DNS：ゾーンに DNS ルックアップで検出されたエンドポイントが含まれます。

例：`xCommand ZoneAdd ZoneName: 「UK Sales Office」 Type: Neighbor`

xCommand Zone Delete

ゾーンを削除します。

ZoneId(r)：*<1..1000>*

削除するゾーンのインデックス。

例：`xCommand Zone Delete ZoneId: 2`

xCommand Zone List

指定したエイリアスの検索で、照会されるゾーンと適用されるトランスフォーメーションのリスト（プライオリティ別にグループ化）を返します。

このコマンドは、既存のシステム設定を変更しません。

Alias(r)：*<S: 1, 60>*

検索するエイリアス。

例：`xCommand ZoneList Alias: 「john.smith@example.com」`

コマンド リファレンス - xStatus

システムの現在のステータスに関する情報を返すには、**xStatus** グループのコマンドを使用します。各 **xStatus** の要素は 1 つ以上のサブ要素に関する情報を返します。

ここでは、現在使用可能な **xStatus** コマンドと、各コマンドによって返される情報を記載します。

既存のステータスに関する情報を取得するには、次のように入力します。

- **xStatus**：すべてのステータス要素の現在のステータスを返す場合。
- **xStatus <element>**：特定の要素とそのすべてのサブ要素の現在のステータスを返す場合
- **xStatus <element> <sub-element>**そのグループのサブ要素の現在のステータスを返す場合。

xStatus コマンドに関する情報を取得するには、次のように入力します。

- **xStatus ?**：**xStatus**コマンドで使用可能なすべての要素のリストを返す場合。

xStatus の要素

現在の xStatus の要素は次のとおりです。

- Alarm
- Alternates
- Applications
- Authentication
- Authzkeys
- B2BUACalls
- B2buapresencerelayservice
- B2buapresencerelayuser
- CDR

- Cafe
- Calls
- Cloud
- Cluster
- CollaborationEdge
- Edgeauth
- Edgecmsserver
- EdgeConfigProvisioning
- Edgeconfigprovisioning
- Edgedomain
- Edgeexternalfqdn
- Edgeauthcodecache
- Edgesso
- ExternalManager
- Fail2ban
- Feedback
- Fips
- Firewall
- Gwtunnels
- H323
- HTTPProxy
- Hardware
- IntrusionProtection
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- MicrosoftContent
- MicrosoftIMP
- NetworkInterface
- NetworkLimits（試験版）

- Ntpcertificates
- Options
- PhonebookServer
- Pipes
- Policy
- PortUsage
- Registrations
- ResourceUsage
- Resourceusage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemMetrics
- SystemUnit
- TURN
- Teststatus
- Time
- Traversalserverresourceusage
- Tunnels
- Warnings
- XMPP
- Xcps2s
- Zones

外部ポリシーの概要

Cisco Expressway（Expressway）には、登録ポリシーとコール ポリシー設定のサポートが組み込まれています。また、より複雑なポリシー決定を実行するためのCPL（コール処理言語）もサポートします。CPLはマシン生成言語として設計されていて、特に直感的ではありません。Expressway は高度なコール ポリシー決定を行うために CPL をロードできますが、複雑な CPL は作成とメンテナンスが困難です。

Expressway外部ポリシー機能では、ポリシー決定を外部システムで行うことができ、実行するアクションの過程で Expressway に指示できます（たとえば、登録を承認するか、コールを分岐するかなど）。コール ポリシーは Expressway とは別に管理でき、Expressway では使用でき

ない機能を実行できます。外部ポリシー サーバは、ポリシー サーバがアクセスできる任意のソースからのデータに基づいてルーティングを決定できます。したがって、企業は特定の要件に基づいてルーティングを決定できます。

外部ポリシー サーバを使用するよう Expressway を設定すると、Expressway は外部ポリシー サーバにサービス要求を送信します（HTTP または HTTPS 経由で）。サービスは Expressway が次に実行する CPL スニペットを含む応答を返信します。

外部ポリシー サーバの使用

外部ポリシー サーバを使用するよう Expressway を設定できる主なエリアは次のとおりです。

- 登録ポリシー：登録を許可または拒否します。
- コール ポリシー（別名、管理ポリシー）：許可、拒否、ルーティング（コールに失敗した場合は、フォールバックで）およびコールの分岐をコントロールします。
- 検索ルール（ポリシーは、特定のダイヤル プランの検索ルールに適用にできます）。

これらのエリアごとに、ポリシー サービスを使用するかしないかを独自に設定できます。ポリシー サービスを使用する場合は、ポリシー サービスによる決定によって、Expressway による決定が置き換えられます（補完ではない）。

ポリシー サービスを設定するときは、次の点を考慮します。

- 最大 3 つの外部ポリシー サーバを指定して、復元力を提供できます（ロード バランシングではない）。
- サービスが使用できない場合に、デフォルト CPL をフォールバックとして Expressway で処理するように設定できます。
- サービスのステータスおよび到達可能性をステータス パスを使用して問い合わせることができます。

ポリシー サービスの詳細（CPL の例を含む）については、『*Expressway* 外部ポリシーの導入ガイド.』を参照してください。

外部ポリシー要求のパラメータ

Expressway は、ポリシー サービスを使用するときに、コール要求または登録要求に関する情報を POST メッセージでそのサービスに送信します。その際、名前と値のペアで構成される一連のパラメータを使用します。サービスは、これらのパラメータと、それ自体のポリシー決定のロジックおよび裏付けとなるデータに基づいて決定を行うことができます（たとえば、LDAP データベースや他の情報源などの外部データ ルックアップを介した登録やコールの発着信を許可するエイリアスのリストなど）。

サービス応答は、CPL が本文に含まれている 200 OK メッセージである必要があります。

次の表に、要求に含まれている可能性があるパラメータのリストを示し、そのパラメータが含まれている要求タイプを √ で示します。また、状況に応じて、許容される値の範囲を示します。

パラメータ名	値	登録 **policy**	検索 ルール	コール ポリシー
ALIAS		√		
ALLOW_INTERWORKING	TRUE / FALSE		√	√
AUTHENTICATED	TRUE / FALSE		√	√
AUTHENTICATED_SOURCE_ALIAS			√	√
AUTHENTICATION_USER_NAME			√	√
CLUSTER_NAME		√	√	√
DESTINATION_ALIAS			√	√
DESTINATION_ALIAS_PARAMS			√	√
GLOBAL_CALL-SERIAL_NUMBER	GUID		√	√
LOCAL_CALL_SERIAL_NUMBER	GUID		√	√
METHOD	INVITE / ARQ / LRQ / OPTIONS / SETUP / REGISTER	√	√	√
NETWORK_TYPE	IPV4 / IPV6		√	√
POLICY_TYPE	REGISTRATION / SEARCH / ADMIN	√	√	√
PROTOCOL	SIP/H323	√	√	√
REGISTERED_ALIAS			√	√
SOURCE_ADDRESS		√	√	√
SOURCE_IP		√	√	√
SOURCE_PORT		√	√	√

パラメータ名	値	登録 policy	検索 ルール	コール ポリシー
TRAVERSAL_TYPE	TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSERVER / TURNCLIENT / ICE]		√	√
UNAUTHENTICATED_SOURCE_ALIAS			√	√
UTCTIME		√	√	√
ZONE_NAME			√	√

暗号化のサポート

外部ポリシー サーバは TLS および AES-256/AES-128/3DES-168 をサポートする必要があります。

SHA-1 は MAC および Diffie-Hellman/Elliptic Curve Diffie-Hellman キー交換に必要です。Expressway は MD5 をサポートしません。

ポリシー サービスのデフォルト CPL

ポリシー サービスを設定するときは、サービスが使用できない場合に、Expressway が使用する**デフォルト CPL** を指定できます。

登録とコール ポリシーの**デフォルト CPL** は次のとおりです。

<reject status='403' reason='Service Unavailable'/>

これは、要求を拒否します。

検索ルールが使用するポリシー サービスの**デフォルト CPL** は次のとおりです。

<reject status='504' reason='Policy Service Unavailable'/>

これは、その特定の検索ルールによって検索を停止します。

このデフォルト CPL は、ポリシー サーバとの接続が切断された場合に、すべてのコール要求と登録要求が拒否されることを意味します。この動作が不要な場合は、代替のデフォルト CPL を指定することを推奨します。

コールまたは登録が拒否される場合に、どのサービスがなぜ要求を拒否するのかが明確になるように、サービスの各タイプにそれぞれ一意の理由値を使用することを推奨します。

フラッシュ ステータス ワード参照テーブル

フラッシュ ステータス ワードは、NTP サーバの同期の問題を診断するために使用されます。

これは、*ntpq* プログラムの *rv* コマンドで表示されます。これは、以下のように、16進数でコーディングされた多数のビットで構成されています。

コード	タグ	メッセージ	説明（Description）
0001	TEST1	pkt_dup	重複パケット
0002	TEST2	pkt_bogus	偽造パケット
0004	TEST3	pkt_unsync	サーバが同期していない
0008	TEST4	pkt_denied	アクセス拒否
0010	TEST5	pkt_auth	認証エラー
0020	TEST6	pkt_stratum	無効な飛びまたはストラタム
0040	TEST7	pkt_header	ヘッダー距離超過
0080	TEST8	pkt_autokey	Autokey シーケンスのエラー
0100	TEST9	pkt_crypto	Autokey プロトコルのエラー
0200	TEST10	peer_stratum	無効なヘッダーまたはストラタム
0400	TEST11	peer_dist	距離のしきい値超過
0800	TEST12	peer_loop	同期ループ
1000	TEST13	peer_unreach	到達不能または選択なし

サポートされている RFC

Expressway は次の RFC をサポートしています。

表 *21* : サポートされている *RFC*

RFC	説明
791	Internet Protocol
1213	『Management Information Base for Network Management of TCP/IP-based internets』
1305	『Network Time Protocol (Version 3) Specification, Implementation and Analysis』
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	『Transmission of IPv6 Packets over Ethernet Networks』
2560	『X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP』
2782	「A DNS RR for specifying the location of services (DNS SRV)」
2833	「RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals」
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2976	SIP INFO 方式
3164	『The BSD syslog Protocol』
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	「Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks」
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification

RFC	説明
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	「The Session Initiation Protocol (SIP) Refer Method」
3550	『RTP: A Transport Protocol for Real-Time Applications』
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	『DNS Extensions to Support IP Version 6』
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	『IP Version 6 Addressing Architecture』
4443	『Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification』
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)

RFC	説明
4787	『Network Address Translation (NAT) Behavioral Requirements for Unicast UDP』
4861	『Neighbor Discovery for IP version 6 (IPv6)』
5095	『Deprecation of Type 0 Routing Headers in IPv6』
5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF): Temporary Maximum Media Stream Bit Rate Request (TMMBR)
5245	Interactive Connectivity Establishment (ICE)
5389	Session Traversal Utilities for NAT (STUN)
5424	The Syslog Protocol
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)。この RFC については一部のみをサポートしています。パブリック GRUU はサポートしていますが、一時 GRUU はサポートしていません。
5766	『Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)』
5806	Diversion Indication in SIP
6156	Traversal Using Relays around NAT (TURN) Extension for IPv6

ソフトウェア バージョン履歴

ここでは、バージョン X8.7 以降のソフトウェア リリースで行われた機能の更新の概要を示します。特定の機能については、該当するソフトウェア バージョンのリリース ノートを参照してください。

ソフトウェア バージョン X 12.5 以降の新機能は、Cisco VCS ではサポートされておらず、Cisco Expressway 製品のみに適用されます。VCS システムの場合、このバージョンはメンテナンスおよびバグ修正のみを目的として VCS に用意されています。

X12.6 機能

表 *22 :* リリース番号別の機能履歴 - *Cisco Expressway* シリーズ

機能/変更	ステータス
MRA を介したウィスパーコーチング/ウィスパーアナウンスメント	X12.6.2 以降でサポート
カスタマイズ可能なアラームベースの電子メール通知	X12.6.2 以降でサポート
MRA を介したエージェント グリーティング	X12.6.2 以降でサポート
アクティブな MRA 登録数の表示	X12.6.1 以降でサポート
MRA を介したサイレント モニタリング	X12.6.1 以降でサポート
セキュリティ機能の拡張	X12.6 以降でサポート
スマート ライセンス	X12.6 以降でサポート
オプション キーではなく UI 設定による、タイプおよびシリーズの設定	X12.6 以降でサポート
アラームベースの電子メール通知	X12.6 以降でサポート
ハードウェア セキュリティ モジュール（HSM）のサポート	プレビュー
IM&P 用の Android プッシュ通知パブリッシャー	プレビュー（X12.6.2 からはデフォルトで無効）
Cisco Contact Center のヘッドセット機能	プレビュー
MRA での複数のプレゼンスドメイン	プレビュー
Expressway 転送プロキシ	X12.6.2 から削除
Smart Call Home	X12.6.2 から削除
Advanced Media Gateway	X12.6 から削除

X12.5 機能

表 *23 :* リリース番号別の機能履歴 - *Cisco Expressway* シリーズ

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
「Kari の法律」の直通 911 番（該当する B2B 導入の場合）	該当なし	該当なし	該当なし	X12.5.7 以降でサポートされています。
仮想化システム - ESXi 認定およびバージョンのサポート	詳細については 、仮想マシン設置ガイドの *Cisco Expressway* を 参照してください。			
Expressway-E での ACME (Automated Certificate Management Environment) サポート	サポート対象	サポート対象	サポート対象	サポート対象
クラスタ用の単一 SAML	サポート対象	サポート対象	サポート対象	サポート対象
複数の Meeting Server 会議ブリッジに対する SIP プロキシ - Cisco Meeting Server ロードバランシングのサポート（X12.5 では最新になっていません）以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	サポート対象	サポート対象	サポート対象

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
MRA: ICE 用メディア パス最適化	サポート対象	サポート対象	サポート対象	サポート対象
MRA: スプリット DNS のない改善されたデュアル ネットワーク ドメイン処理	サポート対象	サポート対象	サポート対象	サポート対象
MRA：Unified CM SIP 回線での更新（自己記述）による OAuth	プレビュー	サポート対象	サポート対象	サポート対象
MRA: アクティベーション コードを使用したデバイス オンボーディング	プレビュー	プレビュー	プレビュー	対応
MRA: 暗号化 iX のサポート	プレビュー	プレビュー	プレビュー	対応
MRA: ヘッドセット管理のサポート	プレビュー	プレビュー	プレビュー	対応
X12.5 の新機能ではなく、以前のプレビューステータスによる情報が含まれている機能は次のとおりです。				
Cisco Meeting App アプリでは Expressway-E TURN サーバを使用可能	プレビュー	サポート対象	サポート対象	サポート対象
MRA での複数のプレゼンスドメイン	プレビュー	プレビュー	プレビュー	プレビュー

機能/変更	X12.5	X12.5.1	X 12.5.2、X 12.5.3	X12.5.4、 X12.5.5、 X12.5.6、 X12.5.9 （X12.5.7 & X12.5.8 の再設定）
Smart Call Home	非推奨およびプレビュー	非推奨およびプレビュー	非推奨およびプレビュー	非推奨およびプレビュー

X8.11 の機能

表 *24 :* リリース番号別の機能履歴

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
アプライアンスのシステムサイズの選択	—	—	—	サポート対象	サポート対象
MRA での Finesse エージェントのサポート	—	—	サポート対象	サポート対象	サポート対象
CE1200 アプライアンス用ソフトウェアの最初のリリース	—	サポート対象	サポート対象	サポート対象	サポート対象
Expressway E へのデバイス登録（SIP および H.323）	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Cisco TMS プロビジョニング アクセスに対する変更	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
Cisco Expressway シリーズでの Multiway 会議	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
複数の Meeting Server 会議ブリッジに対する SIP プロキシ（Cisco Meeting Server ロード バランシングのサポート）	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
複数の Meeting Server Web ブリッジに対する Web プロキシ	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Cisco Meeting App アプリでは Expressway-E TURN サーバを使用可能	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
TCP 443 での TURN	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
大規模 Expressway-E での TURN ポート多重化	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
保存中のデータのセキュリティ強化	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
コモン クライテリアの準備	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
バックアップ時の必須パスワード	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
カスタム ドメイン検索	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
MRA での組み込みブリッジの録音（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました） MRA を介した BiB に関する情報が、*Cisco Expressway* を使用したモバイルおよびリモート アクセス ガイドに記載されました	サポート対象（以前はプレビュー版）	サポート対象	サポート対象	サポート対象	サポート対象
MRA でのアクセス ポリシーのサポート（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました）	サポート対象（以前はプレビュー版） Cisco Jabber 12.0 が必要です	X8.11 関連	X8.11 関連	X8.11 関連	X8.11 関連

機能/変更	X8.11（破棄）	X8.11.1（破棄）	X8.11.2（破棄）	X8.11.3（破棄）	X 8.11.4
MRA での複数のプレゼンスドメイン（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
ライセンス キーの統合	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
クラスタから離脱したピアの初期設定へのリセット	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Smart Call Home（X8.11 での新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
SRV 接続テスト ツール	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
REST API 拡張	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象

X8.10 の機能

表 *25 :* リリース番号別の機能履歴

機能/変更	X8.10	X 8.10.1	X 8.10.2	X8.10.3（変更なし）	X8.10.4（変更なし）
MRA での組み込みブリッジの録音	サポート対象外	サポート対象外	プレビュー	プレビュー	プレビュー
MRA のプッシュ通知のサポートの強化	プレビュー	サポート対象	サポート対象	サポート対象	サポート対象
MRA の自己記述トークンのサポート（更新を伴う OAuth トークン）	プレビュー	サポート対象	サポート対象	サポート対象	サポート対象
MRA のアクセス制御設定の変更	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
MRA のアクセス ポリシーのサポート	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー
TLS および暗号スイートのデフォルトへの変更	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
メディア暗号化の AES-GCM 暗号モード	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
マルチテナンシーの Cisco XCP ルータの遅延再起動	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
マルチテナンシーのサーバ名指定	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象

機能/変更	X8.10	X 8.10.1	X 8.10.2	X8.10.3（変更なし）	X8.10.4（変更なし）
セッション識別子のサポート	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
REST API 拡張	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Smart Call Home（X8.10 の新機能ではありません。以前はプレビュー ステータスであったため参照用に含めました)	プレビュー	プレビュー	プレビュー	プレビュー	プレビュー

X8.9 の機能

表 *26 :* リリース番号別の機能履歴

機能/変更	X8.9	X8.9.1	X8.9.2
Apple Push Notification サービスの Cisco Jabber for iPhone and iPad へのパススルー	サポート対象外	サポート対象	サポート対象
Cisco Meeting Server 用の Microsoft SIP トラフィックのエッジトラバーサル	サポート対象	サポート対象	サポート対象
Meeting Server の Web プロキシ	サポート対象外	サポート対象外	サポート対象
Skype for Business または Office 365 組織との IM and Presence サービス フェデレーション	プレビュー	サポート対象	サポート対象
H.323 ゲートキーパーとしての Cisco Expressway	サポート対象	サポート対象	サポート対象

機能/変更	X8.9	X8.9.1	X8.9.2
REST API 拡張	サポート対象	サポート対象	サポート対象
MRA での SSO のために Jabber for iPhone and iPad に Safari の使用を許可	サポート対象	サポート対象	サポート対象
MRA エンドポイントの共有回線および複数回線のサポート	プレビュー	サポート対象	サポート対象
Smart Call Home	プレビュー	プレビュー	プレビュー
セキュアなインストール ウィザード	サポート対象	サポート対象	サポート対象
DiffServ コード ポイント マーキング	サポート対象	サポート対象	サポート対象
MRA のメンテナンス モード	サポート対象	サポート対象	サポート対象

X8.8 機能

表 *27*：リリース番号別の機能履歴

機能/変更	X8.8
Expresswayの登録	サポートあり
ビジネス2016年のSkype for Businessとビジネス モバイル サポートにSkype for Business	サポートあり
Microsoft SIPトラフィック用に仲介国	サポートあり
マルチストリーム サポート	サポートあり
セットアップ ウィザードを選択できます	サポートあり
MRA 許可リストの改善	サポートあり
MRAのリモート設定のAPI	サポートあり
減少VM、CPU予約	サポートあり
最高レベルの環境	サポートあり

機能/変更	X8.8
ソフトウェア パッケージのサインイン	サポートあり
制限されたSSL/TLSサポート	サポート対象

X8.7 機能

表 *28 :* リリース番号別の機能履歴

機能/変更	X8.7
Office-Reverse（DVO-R）によるダイヤル	サポートあり
ゲートウェイ クラスタによる Lync 画面の共有	サポートあり
サポートされている Cisco IP Phone を使用したモバイルおよびリモート アクセス	サポートあり
ハイブリッド サービスと Expressway/VCS のブランド変更	サポートあり
VMWare vSphere® 6.0 でのホスティング	サポートあり
syslog 出力のキーワード フィルタ	サポート対象

法的通知

知的財産権

この管理者ガイドおよび関連する製品には、TANDBERG およびそのライセンサーの専有情報が含まれています。製品に関する情報は、下記の**著作権情報**および**特許情報**の項に記載されています。

TANDBERG® は Tandberg ASA に帰属する登録商標です。本書で使用されているその他の商標は、それぞれの所有者に帰属します。本書は、著作権と知的財産権の情報を含めて、すべて複製することができますが、この製品の使用に関連付けられている数量に制限されます。前の文に記載されている制限付き例外を除いて、本書のいかなる部分も、電子的、機械的、複写などの形式や手段を問わず、事前に書面で TANDBERG の許可を得ることなく、複製、検索システムへの保管、または伝送することはできません。

著作権情報

The product that is covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

TANDBERG はシスコの一部です。Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

この製品には、他者からライセンス付与された著作権付きソフトウェアが含まれています。A list of the licenses and notices for open source software used in this product can be found at: http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-licensing-information-listing.html

この製品には、カーネギーメロン大学（http://www.cmu.edu/computing）のコンピュータサービスによって開発されたソフトウェアが含まれています。

This product includes software developed by the University of California, Berkeley and its contributors.

重要：この製品の使用は、いかなる場合においても、前述した著作権、条項、および使用条件に従うものとします。USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

AVC Video のライセンス

各 AVC/H.264 製品に関し、シスコには次の通知を提供する義務があります。

この製品は、AVC 特許ポートフォリオ ライセンスに基づいて消費者の個人的な使用、または報酬を受けないその他の利用方法が認められています。報酬を受けないその他の利用方法とは、（i）AVC 標準に従ったビデオのエンコード、（ii）個人的な活動に従事する消費者がエンコードした AVC ビデオ、または AVC ビデオの供給が許されたビデオ プロバイダーから入手した AVC ビデオの復号化、あるいはその両方のことをいいます。その他のいかなる使用に対してもライセンスは供与されず、それが示唆されることもありません。追加情報は MPEG LA, L.L.C.でご確認いただけます。

参照先。http://www.mpegla.com

そのため、サービスプロバイダー、コンテンツプロバイダー、および放送事業者は、AVC/H.264 のエンコーダまたはデコーダ、あるいはその両方の使用については、使用する前に MPEG LA から別途ライセンスを取得する必要があります。

特許情報

この製品は、次の特許の 1 つ以上の対象になっています。

- US7,512,708
- EP1305927
- EP1338127

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。