



**Cisco Unified SIP Proxy Release 8.5 CLI コン  
フィギュレーション ガイド**  
**CLI Configuration Guide for Cisco Unified SIP Proxy Release 8.5**

2010 年 11 月 4 日

**【注意】シスコ製品をご使用になる前に、安全上の注意**  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊  
社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

**FCC クラス A 準拠装置に関する記述：**この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

**FCC クラス B 準拠装置に関する記述：**このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に準拠しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコシステムズの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

- 干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。
- テレビまたはラジオの左右どちらかの側に装置を移動させます。
- テレビまたはラジオから離れたところに装置を移動させます。
- テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うこととなります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任は一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

*Cisco Unified SIP Proxy Release 8.5 CLI コンフィギュレーション ガイド*

© 2010 Cisco Systems, Inc.

All rights reserved.

Copyright © 2010–2011, シスコシステムズ合同会社.

All rights reserved.



## CONTENTS

<b>Cisco Unified SIP Proxy Release 8.5 の概要</b>	<b>1</b>
このマニュアルについて	1
管理インターフェイス	1
コマンドライン インターフェイス	1
グラフィカル ユーザ インターフェイス	2
商用オープン ソース ライセンス	2
マニュアルの入手方法およびテクニカル サポート	2
シスコのテクニカル サポート	3
<b>Cisco Unified SIP Proxy Release 8.5 のマニュアル ロードマップ</b>	<b>5</b>
主なマニュアル リスト	5
リリース情報と一般情報	5
ライセンス情報	5
リリース ノート	5
リファレンス ガイド	6
コマンド リファレンス	6
インストールおよびアップグレード	6
インストールおよびアップグレード ガイド	6
メンテナンスおよび操作	6
メンテナンスおよび操作ガイド	6
Cisco DocWiki に関するトラブルシューティング情報	7
マーケティング資料	7
ソフトウェアのダウンロード	7
<b>初期設定タスク</b>	<b>9</b>
バックアップ パラメータの設定	9
バックアップ パラメータとは	9
前提条件	9
手順の概要	10
手順の詳細	10
例	11
NTP サーバの設定	11
NTP サーバの追加	11

NTP サーバの追加とは	11
手順の概要	12
手順の詳細	12
NTP サーバの追加例	13
NTP サーバの削除	13
手順の概要	13
手順の詳細	13
NTP サーバ情報の表示	14
NTP サーバ情報を表示するコマンド	14
NTP サーバ情報の表示例	14
時間帯の設定	15
時間帯の設定例	15
<b>Cisco Unified SIP Proxy モジュールの設定</b>	<b>17</b>
論理ネットワークの設定	17
手順の概要	17
手順の詳細	18
例	18
トリガー条件の設定	18
手順の概要	18
手順の詳細	19
例	20
サーバグループの設定	20
サーバグループについて	20
手順の概要	20
手順の詳細	21
例	21
ルート テーブルの設定	22
ルート テーブルについて	22
手順の概要	22
手順の詳細	22
例	23
正規化ポリシーの設定	23
手順の概要	23
手順の詳細	24
例	24
ルックアップ ポリシーの設定	25
手順の概要	25
手順の詳細	25

例	26	
ルーター トリガーの設定	26	
手順の概要	27	
手順の詳細	27	
例	27	
正規化トリガーの設定	27	
手順の概要	28	
手順の詳細	28	
例	28	
リッスン ポートとレコードルート ポートの設定	29	
手順の概要	29	
手順の詳細	29	
例	30	
ホスト名の設定	30	
手順の概要	30	
手順の詳細	30	
例	31	
トランスポート レイヤ セキュリティ (TLS) の設定	31	
署名付き証明書の作成とインポート	31	
前提条件	31	
手順の概要	31	
手順の詳細	32	
署名付き証明書の作成例	32	
Cisco Unified SIP Proxy 上での TLS の作成	33	
手順の概要	33	
手順の詳細	33	
TLS の設定例	34	
設定の確定	34	
データのバックアップおよび復元	35	
データのバックアップおよび復元について	35	
データのバックアップおよび復元に関する制約事項	35	
ファイルのバックアップ	36	
ファイルのバックアップについて	36	
手順の概要	36	
手順の詳細	37	
例	37	
ファイルの復元	38	

ファイルの復元について	38
手順の概要	38
手順の詳細	39
関連項目	39
<b>Cisco Unified SIP Proxy システムのメンテナンス</b>	<b>41</b>
設定のコピー	41
ハード ディスクから別の場所へのスタートアップ コンフィギュレーションのコピー	41
ネットワーク FTP サーバから別の場所へのスタートアップ コンフィギュレーションのコピー	42
ハード ディスクから別の場所への実行コンフィギュレーションのコピー	42
ネットワーク TFTPサーバから別の場所への実行コンフィギュレーションのコピー	43
ハード ディスク メモリの装着アクティビティの確認	43
トラブルシューティング	45
CLI コマンドを使用したシステムのトラブルシューティング	45
ログについて	45
Log コマンド	46
ログ出力の例	46
Trace コマンドの使用	46
Show コマンドの使用	47
コンフィギュレーションの変更のトラブルシューティング	47
関連項目	47
<b>設定例</b>	<b>49</b>



# Cisco Unified SIP Proxy Release 8.5 の概要

- [「このマニュアルについて」 \(P.1\)](#)
- [「管理インターフェイス」 \(P.1\)](#)
- [「商用オープンソースライセンス」 \(P.2\)](#)
- [「マニュアルの入手方法およびテクニカルサポート」 \(P.2\)](#)
- [「シスコのテクニカルサポート」 \(P.3\)](#)

## このマニュアルについて

このマニュアルには、CLI を使用した、Cisco Unified SIP Proxy システムの設定方法に関する情報が記載されています。すべての CLI コマンドの一覧が記載されている『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』と併せて使用してください。

## 管理インターフェイス

Cisco Unified SIP Proxy Release 8.5 では、Command-Line Interface (CLI; コマンドライン インターフェイス) と Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) の両方が使用されます。

- [「コマンドライン インターフェイス」 \(P.1\)](#)
- [「グラフィカル ユーザ インターフェイス」 \(P.2\)](#)

## コマンドライン インターフェイス

CLI はテキストベースのインターフェイスであり、Cisco Unified SIP Proxy をホストするルータとの Telnet セッションを介してアクセスできます。Cisco IOS コマンド構造およびルータに馴染みのあるユーザには、類似点を確認できるでしょう。

Cisco Unified SIP Proxy コマンドは、Cisco IOS CLI コマンドの構造によく似ています。ただし、Cisco Unified SIP Proxy CLI コマンドは Cisco IOS の設定に影響を及ぼしません。Cisco Unified SIP Proxy にログインすると、コマンド環境は、Cisco IOS 環境ではなくなります。

CLI は、IP ネットワーク内の任意の場所にある PC またはサーバからアクセス可能です。

## グラフィカル ユーザ インターフェイス

Cisco Unified SIP Proxy Release 8.5 では、Cisco Unified SIP Proxy システムの設定および操作に使用できる GUI が導入されました。

GUI の使用方法については、アプリケーションのオンライン ヘルプまたは『[GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。

GUI に関する情報は、このマニュアルの対象外です。

## 商用オープンソースライセンス

Cisco Unified SIP Proxy Release 8.5 用に作成されたソフトウェア コンポーネントの一部は、オープンソースライセンスまたは商用ライセンスによって提供されています。これらのコンポーネントおよび関連する著作権情報は、

[http://www.cisco.com/en/US/products/ps10475/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps10475/products_licensing_information_listing.html) で確認できます。

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



## シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"><li>• テクニカル サポートを受ける</li><li>• ソフトウェアをダウンロードする</li><li>• セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける</li><li>• ツールおよびリソースへアクセスする<ul style="list-style-type: none"><li>– Product Alert の受信登録</li><li>– Field Notice の受信登録</li><li>– BugToolkit を使用した既知の問題の検索</li></ul></li><li>• Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する</li><li>• トレーニング リソースへアクセスする</li><li>• TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する</li></ul> <p>この Web サイト上のツールにアクセスする際は、Cisco.com のユーザ名およびパスワードが必要です。</p>	<p><a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a></p>
<p>Cisco Feature Navigator Web サイトを使用して、プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を入手します。Cisco.com のアカウントは不要です。</p>	<p><a href="http://www.cisco.com/go/cfn">http://www.cisco.com/go/cfn</a></p>





# Cisco Unified SIP Proxy Release 8.5 のマニュアル ロードマップ

---

## 主なマニュアル リスト

- 『[Release Notes for Cisco Unified SIP Proxy Release 8.5](#)』
- 『[Open Source Licensing for Cisco Unified SIP Proxy Release 8.5](#)』
- 『[Install Guide for Cisco Unified SIP Proxy Release 8.5](#)』
- 『[CLI Configuration Guide for Cisco Unified SIP Proxy Release 8.5](#)』
- 『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』
- 『[GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5](#)』

## リリース情報と一般情報

### ライセンス情報

#### 『[Open Source Licensing for Cisco Unified SIP Proxy Release 8.5](#)』

この製品で使用されるオープンソース ソフトウェアに関する情報が記載されています。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps10475/products_licensing_information_listing.html)

### リリース ノート

#### 『[Release Notes for Cisco Unified SIP Proxy Release 8.5](#)』

システム要件、ライセンス情報、新機能、制限事項、および参考資料について記載されています。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps10475/prod_release_notes_list.html)

# リファレンス ガイド

## コマンド リファレンス

### 『*Command Reference for Cisco Unified SIP Proxy Release 8.5*』

Command-Line Interface (CLI; コマンドライン インターフェイス) を使用した Cisco Unified SIP Proxy Release 8.5 ソフトウェアの設定に関するヒントを紹介し、使用できる CLI コマンドおよび構文の一覧を示します。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps10475/prod_command_reference_list.html)

## インストールおよびアップグレード

### インストールおよびアップグレード ガイド

#### 『*Installation Guide for Cisco Unified SIP Proxy Release 8.5*』

Cisco Unified SIP Proxy Release 8.5 のインストール方法およびライセンスのインストール方法に関する情報が記載されています。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10475/prod_installation_guides_list.html)

## メンテナンスおよび操作

### メンテナンスおよび操作ガイド

#### 『*CLI Configuration Guide for Cisco Unified SIP Proxy Release 8.5*』

Command-Line Interface (CLI; コマンドライン インターフェイス) を使用して Cisco Unified SIP Proxy システムのセットアップ、設定、操作、およびメンテナンスを行う方法について説明します。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html)

#### 『*GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5*』

このマニュアルは、Cisco Unified SIP Proxy の Graphical User Interface (GUI; グラフィカル ユーザー インターフェイス) で表示できるオンライン ヘルプと同一です。GUI を使用して Cisco Unified SIP Proxy システムのセットアップ、設定、操作、およびメンテナンスを行う方法について説明します。

このマニュアルは、次の URL から入手できます。

[http://www.cisco.com/en/US/products/ps10475/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html)

## Cisco DocWiki に関するトラブルシューティング情報

Cisco Unified SIP Proxy のトラブルシューティング情報は、次の URL の Cisco DocWiki で確認できます。

[http://docwiki.cisco.com/wiki/Cisco\\_Unified\\_SIP\\_Proxy](http://docwiki.cisco.com/wiki/Cisco_Unified_SIP_Proxy)

DocWiki 上の情報は、Cisco.com ユーザ ID およびパスワードを持っているユーザであれば誰でも更新できます。このように、トラブルシューティング情報はシスコとお客様とのコラボレーションです。

## マーケティング資料

次の URL にあるデータシートなど Cisco Unified SIP Proxy Release 8.5 に関するマーケティング資料を参照してください。

<http://www.cisco.com/en/US/products/ps10140/index.html>

## ソフトウェアのダウンロード

Cisco Unified SIP Proxy Release 8.5 ソフトウェアをダウンロードするには、次の URL に移動してください。

<http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=282713225>.





## 初期設定タスク

---

- [「バックアップパラメータの設定」 \(P.9\)](#)
- [「NTP サーバの設定」 \(P.11\)](#)
- [「時間帯の設定」 \(P.15\)](#)

## バックアップパラメータの設定

- [「バックアップパラメータとは」 \(P.9\)](#)
- [「前提条件」 \(P.9\)](#)
- [「手順の概要」 \(P.10\)](#)
- [「手順の詳細」 \(P.10\)](#)
- [「例」 \(P.11\)](#)

## バックアップパラメータとは

Cisco Unified SIP Proxy のバックアップ機能および復元機能は、FTP サーバを使用してデータの保存および取得を行います。バックアップ機能によって、ファイルは Cisco Unified SIP Proxy から FTP サーバにコピーされます。復元機能によって、ファイルは FTP サーバから Cisco Unified SIP Proxy にコピーされます。FTP サーバは、バックアップ機能および復元機能が IP アドレスまたはホスト名を使用して FTP サーバにアクセスできる限り、ネットワークの任意の場所に配置できます。

すべての Cisco Unified SIP Proxy バックアップ ファイルは、指定したサーバに保存されます。バックアップ ファイルは、必要に応じて他の場所またはサーバにコピーできます。

バックアップパラメータは、Cisco Unified SIP Proxy バックアップ ファイルの保存に使用する FTP サーバ、および最も古いファイルが上書きされるまでに保存されるバックアップの数を指定します。

## 前提条件

- FTP 管理者または FTP サーバにログインできる他のユーザが、ファイルおよびディレクトリに対する読み取り、書き込み、上書き、作成、および削除の権限など FTP サーバに関するフル権限を持っていることを確認します。
- FTP サーバの URL、FTP サーバログインのユーザ名およびパスワードを用意します。
- 最も古いバックアップが上書きされるまで保存されるリビジョンの番号を決めます。

## 手順の概要

1. `configure terminal`
2. `backup server url backup-ftp-url username backup-ftp-usrname password backup-ftp-password`
3. `backup revisions number number`
4. `end`
5. `show backup`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>configure terminal</code>  se-10-0-0-0# <code>config terminal</code>	コンフィギュレーション モードを開始します。
ステップ2	<code>backup server url ftp-url username ftp-username password ftp-password</code>  例： se-10-0-0-0(config)> <code>backup server url ftp://main/backups username "admin" password "wxyz"</code>  se-10-0-0-0(config)> <code>backup server url ftp://192.0.2.15/backups username "admin" password "wxyz"</code>	バックアップ パラメータを設定します。  (注) バックアップ サーバを設定しなければ、バックアップ リビジョンを設定できません。  <ul style="list-style-type: none"> <li>• <b>server url</b> : <i>ftp-url</i> 値は、バックアップ ファイルの保存先である、ネットワーク FTP サーバの URL です。</li> <li>• <i>ftp-username</i> 値は、ネットワーク FTP サーバのユーザ名です。<i>ftp-password</i> 値は、ネットワーク FTP サーバのパスワードです。</li> </ul> この例では、 <b>main</b> は FTP サーバのホスト名で、 <b>backups</b> はバックアップ ファイルの保存先ディレクトリです。
ステップ3	<code>backup revisions number</code>  例： se-10-0-0-0(config)> <code>backup revisions 5</code>	保存されるバックアップ ファイルの数を設定します。このバックアップの数に達すると、システムは、保存されている最も古いファイルを削除します。
ステップ4	<code>end</code>  例： se-10-0-0-0(config)> <code>end</code>	コンフィギュレーション モードを終了します。
ステップ5	<code>show backup</code>  例： se-10-0-0-0> <code>show backup</code>	FTP サーバの URL、利用可能なバックアップ ファイルの最大数などバックアップ サーバの設定情報を表示します。



## 例

次の例では、バックアップサーバを設定し、**show backup** の出力を表示する方法を示します。

```
se-10-0-0-0> enable
se-10-0-0-0# configure terminal
se-10-0-0-0 (config)> backup revisions 5
se-10-0-0-0 (config)> backup server url ftp://10.12.0.1/ftp username "admin" password
"wxzy"
se-10-0-0-0 (config)> end
se-10-0-0-0> show backup
Server URL:                               ftp://10.12.0.1/ftp
User Account on Server:
Number of Backups to Retain:              5
se-10-0-0-0>
```

### 関連項目

- CLI コマンドについては、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。
- 設定のバックアップおよび復元については、『[データのバックアップおよび復元](#)』を参照してください。

## NTP サーバの設定

Cisco Unified SIP Proxy ソフトウェアのインストール時には、最大 2 つの Network Time Protocol (NTP; ネットワーク タイム プロトコル) サーバを追加することもできます。追加の NTP サーバ (システムは、最大 3 つの NTP サーバをサポート) を追加し、1 つ以上の NTP サーバを削除するか、CLI を使用して NTP サーバ情報を表示できます。

- [「NTP サーバの追加」 \(P.11\)](#)
- [「NTP サーバの削除」 \(P.13\)](#)
- [「NTP サーバ情報の表示」 \(P.14\)](#)

## NTP サーバの追加

- [「NTP サーバの追加とは」 \(P.11\)](#)
- [「手順の概要」 \(P.12\)](#)
- [「手順の詳細」 \(P.12\)](#)
- [「NTP サーバの追加例」 \(P.13\)](#)

## NTP サーバの追加とは

NTP サーバは、このサーバの IP アドレスまたはホスト名を使用して指定できます。

Cisco Unified SIP Proxy は、DNS サーバを使用してホスト名を IP アドレスに解決し、NTP サーバとして IP アドレスを保存します。DNS がホスト名を複数の IP アドレスに解決した場合、Cisco Unified SIP Proxy は NTP サーバとしてまだ指定されていない IP アドレスの 1 つをランダムに選択します。ランダムに選択しない場合は、1 つのサーバに対して **prefer** 属性を設定します。

## ■ NTP サーバの設定

1 つのホスト名に対して複数の IP アドレスを持つ NTP サーバを設定するには、同じホスト名を使用して設定手順を繰り返します。手順を繰り返すごとに、NTP サーバが残りの IP アドレスに割り当てられます。

## 手順の概要

1. `configure terminal`
2. `ntp server {hostname | ip-address} [ prefer ]`
3. `end`
4. `show ntp status`
5. `show ntp configuration`
6. `copy running-config startup-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code>  例： <code>se-10-0-0-0# config terminal</code>	コンフィギュレーション モードを開始します。
ステップ 2	<code>ntp server {hostname   ip-address} [ prefer ]</code>  例： <code>se-10-0-0-0(config)&gt; ntp server 192.0.2.14</code> <code>se-10-0-0-0(config)&gt; ntp server 192.0.2.17 prefer</code>	NTP サーバのホスト名または IP アドレスを指定します。  複数のサーバが設定されている場合、 <b>prefer</b> 属性を持つサーバが他のサーバよりも先に使用されます。
ステップ 3	<code>end</code>  例： <code>se-10-0-0-0(config)&gt; exit</code>	コンフィギュレーション モードを終了します。
ステップ 4	<code>show ntp status</code>  例： <code>se-10-0-0-0&gt; show ntp status</code>	NTP サーバに関する統計情報を表示します。
ステップ 5	<code>show ntp configuration</code>  例： <code>se-10-0-0-0&gt; show ntp configuration</code>	設定された NTP サーバを表示します。
ステップ 6	<code>copy running-config startup-config</code>  例： <code>se-10-0-0-0&gt; copy running-config startup-config</code>	コンフィギュレーションの変更部分をスタートアップのコンフィギュレーション ファイルにコピーします。

## NTP サーバの追加例

次のコマンドで、NTP サーバが設定されます。

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)# ntp server 192.0.2.14
se-10-0-0-0(config)# exit
se-10-0-0-0>
```

**show ntp status** コマンドの出力は、次のように表示されます。

```
se-10-0-0-0> show ntp status

NTP reference server 1:      192.0.2.14
Status:                     sys.peer
Time difference (secs):     3.268110099434328E8
Time jitter (secs):         0.1719226837158203
```

## NTP サーバの削除

NTP サーバは、このサーバの IP アドレスまたはホスト名を使用して削除できます。

- [「手順の概要」 \(P.13\)](#)
- [「手順の詳細」 \(P.13\)](#)

### 手順の概要

1. **configure terminal**
2. **no ntp server {hostname | ip-address}**
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例: se-10-0-0-0# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	<b>no ntp server {hostname   ip-address}</b>  例: se-10-0-0-0(config)# <b>no ntp server 192.0.2.14</b> se-10-0-0-0(config)# <b>no ntp server myhost</b>	削除する NTP サーバのホスト名または IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 3	<code>exit</code>  例： se-10-0-0-0(config)> <code>exit</code>	コンフィギュレーション モードを終了します。
ステップ 4	<code>show ntp status</code>  例： se-10-0-0-0> <code>show ntp status</code>	NTP サーバに関する統計情報を表示します。
ステップ 5	<code>show ntp configuration</code>  例： se-10-0-0-0> <code>show ntp status</code>	設定された NTP サーバを表示します。
ステップ 6	<code>copy running-config startup-config</code>  例： se-10-0-0-0> <code>copy running-config startup-config</code>	コンフィギュレーションの変更部分をスタートアップのコンフィギュレーション ファイルにコピーします。

## NTP サーバ情報の表示

- 「[NTP サーバ情報を表示するコマンド](#)」 (P.14)
- 「[NTP サーバ情報の表示例](#)」 (P.14)

## NTP サーバ情報を表示するコマンド

次のコマンドを使用することで、NTP サーバの設定情報およびステータスを表示できます。

- `show ntp associations`
- `show ntp servers`
- `show ntp source`
- `show ntp status`

## NTP サーバ情報の表示例

次の例は、`show ntp associations` コマンドの出力例です。

```
se-10-0-0-0> show ntp associations

ind assID status  conf reach auth condition  last_event cnt
=====
  1 61253  8000   yes  yes  none    reject
```

次の例は、`show ntp servers` コマンドの出力例です。

```
se-10-0-0-0> show ntp servers

remote          refid          st t when poll reach  delay  offset  jitter
=====
1.100.6.9       0.0.0.0       16 u   - 1024   0    0.000   0.000 4000.00
space reject,   x falsetick,  . excess,    - outlier
```

```
+ candidate,          # selected,          * sys.peer,          o pps.peer
```

次の例は、**show ntp source** コマンドの出力例です。

```
se-10-0-0-0> show ntp source
```

```
127.0.0.1: stratum 16, offset 0.000013, synch distance 8.67201
0.0.0.0:          *Not Synchronized*
```

次の例は、**show ntp status** コマンドの出力例です。

```
se-10-0-0-0> show ntp status
```

```
NTP reference server :      10.100.6.9
Status:                   reject
Time difference (secs):    0.0
Time jitter (secs):       4.0
```

### 関連項目

- CLI コマンドについては、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。
- Cisco Unified SIP Proxy システムの初期インストールおよびインストール後の設定ツールについては、『[Installation Guide for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。
- コピーおよび設定については、「[設定のコピー](#)」(P.41) を参照してください。

## 時間帯の設定

Cisco Unified SIP Proxy ソフトウェアのインストール時には、時間帯の設定を求めるプロンプトが表示されます。時間帯の変更が必要な場合は、Cisco Unified SIP Proxy コンフィギュレーション モードで **clock timezone** コマンドを使用します。

時間帯を表示するには、モジュール EXEC モードで **show clock detail** コマンドを使用します。

### 時間帯の設定例

```
se-10-0-0-0# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
se-10-0-0-0(config)# clock timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                4) Arctic Ocean        7) Australia            10) Pacific Ocean
2) Americas              5) Asia                8) Europe
3) Antarctica           6) Atlantic Ocean     9) Indian Ocean
>? 2
Please select a country.
1) Anguilla              18) Ecuador            35) Paraguay
2) Antigua & Barbuda    19) El Salvador       36) Peru
3) Argentina            20) French Guiana     37) Puerto Rico
4) Aruba                 21) Greenland         38) St Kitts & Nevis
5) Bahamas              22) Grenada           39) St Lucia
6) Barbados             23) Guadeloupe       40) St Pierre & Miquelon
7) Belize               24) Guatemala        41) St Vincent
8) Bolivia              25) Guyana            42) Suriname
9) Brazil               26) Haiti             43) Trinidad & Tobago
10) Canada              27) Honduras         44) Turks & Caicos Is
11) Cayman Islands      28) Jamaica          45) United States
```

- |                        |                          |                         |
|------------------------|--------------------------|-------------------------|
| 12) Chile              | 29) Martinique           | 46) Uruguay             |
| 13) Colombia           | 30) Mexico               | 47) Venezuela           |
| 14) Costa Rica         | 31) Montserrat           | 48) Virgin Islands (UK) |
| 15) Cuba               | 32) Netherlands Antilles | 49) Virgin Islands (US) |
| 16) Dominica           | 33) Nicaragua            |                         |
| 17) Dominican Republic | 34) Panama               |                         |

>? **45**

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Standard Time - Indiana - most locations
- 6) Eastern Standard Time - Indiana - Crawford County
- 7) Eastern Standard Time - Indiana - Starke County
- 8) Eastern Standard Time - Indiana - Switzerland County
- 9) Central Time
- 10) Central Time - Michigan - Wisconsin border
- 11) Central Time - North Dakota - Oliver County
- 12) Mountain Time
- 13) Mountain Time - south Idaho & east Oregon
- 14) Mountain Time - Navajo
- 15) Mountain Standard Time - Arizona
- 16) Pacific Time
- 17) Alaska Time
- 18) Alaska Time - Alaska panhandle
- 19) Alaska Time - Alaska panhandle neck
- 20) Alaska Time - west Alaska
- 21) Aleutian Islands
- 22) Hawaii

>? **16**

The following information has been given:

```

United States
Pacific Time

```

Therefore TZ='America/Los\_Angeles' will be used.

Local time is now: Mon Aug 27 17:23:54 PDT 2007.

Universal Time is now: Tue Aug 28 00:23:54 UTC 2007.

Is the above information OK?

- 1) Yes
- 2) No

>? **1**

Save the change to startup configuration and reload the module for the new time zone to take effect.

se-10-0-0-0(config)>



# Cisco Unified SIP Proxy モジュールの設定

- 「論理ネットワークの設定」 (P.17)
- 「トリガー条件の設定」 (P.18)
- 「サーバグループの設定」 (P.20)
- 「ルートテーブルの設定」 (P.22)
- 「正規化ポリシーの設定」 (P.23)
- 「ロックアップポリシーの設定」 (P.25)
- 「ルーティングトリガーの設定」 (P.26)
- 「正規化トリガーの設定」 (P.27)
- 「リッスンポートとレコードルートポートの設定」 (P.29)
- 「ホスト名の設定」 (P.30)
- 「トランスポートレイヤセキュリティ (TLS) の設定」 (P.31)
- 「設定の確定」 (P.34)

## 論理ネットワークの設定

Cisco Unified SIP Proxy 上の各インターフェイスは、論理ネットワークと関連付けられます。論理ネットワークは、サーバグループ、リッスンポイント、その他のプロパティの編成に使用されます。SIP メッセージは、メッセージが到達するネットワークと関連付けられます。

- 「手順の概要」 (P.17)
- 「手順の詳細」 (P.18)
- 「例」 (P.18)

## 手順の概要

1. `cusps`
2. `configure`
3. `sip network network`
4. `end network`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>culp</code>  例： <code>se-10-0-0-0&gt; culp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<code>configure</code>  例： <code>se-10-0-0-0 (culp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ 3	<code>sip network network</code>  例： <code>se-10-0-0-0 (culp-config)&gt; sip network service-provider</code>	ネットワークを作成し、ネットワーク コマンドモードにします。この場合、作成されるネットワークの名前は「service provider」です。
ステップ 4	<code>end network</code>  例： <code>se-10-0-0-0 (culp-config-network)&gt; end network</code>	ネットワーク コマンドモードを終了します。

## 例

次の例では、「service-provider」という名前のネットワークを作成する方法を示します。

```
se-10-0-0-0> culp
se-10-0-0-0 (culp)> configure
se-10-0-0-0 (culp-config)> sip network service-provider
se-10-0-0-0 (culp-config-network)> end network
```

## トリガー条件の設定

トリガー条件を作成すると、Cisco Unified SIP Proxy はさまざまな呼び出しフローに対して適切な動作で応答できます。一般的に、呼び出しフローが複雑であるほど複雑なトリガーが必要です。

- 「手順の概要」(P.18)
- 「手順の詳細」(P.19)
- 「例」(P.20)

## 手順の概要

1. `culp`
2. `configure`
3. `trigger condition trigger-condition-name`



4. `sequence sequence-number`
5. (オプション) `in-network network-name`
6. (オプション) `mid-dialog`
7. `end sequence`
8. `end trigger condition`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>culp</code>  例: <code>se-10-0-0-0&gt; culp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<code>configure</code>  例: <code>se-10-0-0-0 (culp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ 3	<code>trigger condition trigger-condition-name</code>  例: <code>se-10-0-0-0 (culp-config)&gt; trigger condition call-from-service-provider</code>	トリガー条件を作成し、トリガー コマンド モードにします。この場合、作成されるトリガーの名前は「call-from-service-provider」です。
ステップ 4	<code>sequence sequence-number</code>  例: <code>se-10-0-0-0 (culp-config-trigger)&gt; sequence 1</code>	指定した数字のシーケンスを作成し、トリガー シーケンス コマンド モードにします。この数字は、トリガーが評価される順番を示します。この場合、作成されるトリガーのシーケンス番号は 1 です。
ステップ 5	<code>in-network network-name</code>  例: <code>se-10-0-0-0 (culp-config-trigger-seq)&gt; in-network service-provider</code>	オプション。トリガー条件の着信ネットワーク名を指定します。この場合、着信ネットワークは「service-provider」ネットワークです。
ステップ 6	<code>mid-dialog</code>  例: <code>se-10-0-0-0 (culp-config-trigger-seq)&gt; mid-dialog</code>	オプション。 <code>mid-dialog</code> メッセージのルーティングポリシーをバイパスする特殊なトリガーです。
ステップ 7	<code>end sequence</code>  例: <code>se-10-0-0-0 (culp-config-trigger-seq)&gt; end sequence</code>	トリガー シーケンス コマンド モードを終了します。
ステップ 8	<code>end trigger condition</code>  例: <code>se-10-0-0-0 (culp-config-trigger)&gt; end trigger condition</code>	トリガー コマンド モードを終了します。

## 例

このサンプルでは、Cisco Unified SIP Proxy は呼び出しが入ってきたネットワークに基づいて対処を行うだけなので、トリガーは単純です。

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> trigger condition call-from-service-provider
se-10-0-0-0 (cusp-config-trigger)> sequence 1
se-10-0-0-0 (cusp-config-trigger-seq)> in-network service-provider
se-10-0-0-0 (cusp-config-trigger-seq)> end sequence
se-10-0-0-0 (cusp-config-trigger)> end trigger condition

se-10-0-0-0 (cusp-config)> trigger condition mid-dialog
se-10-0-0-0 (cusp-config-trigger)> sequence 1
se-10-0-0-0 (cusp-config-trigger-seq)> mid-dialog
se-10-0-0-0 (cusp-config-trigger-seq)> end sequence
se-10-0-0-0 (cusp-config-trigger)> end trigger condition
```

## サーバグループの設定

- 「サーバグループについて」 (P.20)
- 「手順の概要」 (P.20)
- 「手順の詳細」 (P.21)
- 「例」 (P.21)

## サーバグループについて

サーバグループは、Cisco Unified SIP Proxy が各ネットワークで通信を行う要素を定義します。使用されるサーバグループ名は、発信要求の SIP URI に挿入されます。Cisco Unified Communications Manager などの一部のデバイスでは、処理を行う前に要求の URI を検証します。つまり、これを利用できるようにするには、場合によって完全修飾ドメイン名 (FQDN) を使ってエンドデバイスを設定する必要があります。

個別の各要素の 2 つのフィールド (q-value および weight) は、要素のプライオリティとロードバランシングを指定するために使用されるので重要です。呼び出しは q-value に基づいて特定の要素にルーティングされます。最も高い q-value を持つ要素は、そのサーバグループにルーティングされたすべてのトラフィックを受信します。複数の要素が同じ q-value を持つ場合、トラフィックは、使用されているロードバランシングオプションに基づいて各要素に分散されます。デフォルトでは call-id に基づいてロードバランシングが行われますが、weight も使用できます。weight を使用する場合、ある要素が受信するトラフィックの割合は、その要素の weight を、q-value の weight が同じ稼働中の要素の合計で割った割合に等しくなります。これらの weight の合計は 100 に等しい必要はありません。weight と q-value を変えることで、さまざまなプライオリティやロードバランシング方式を設定できます。

## 手順の概要

1. cusp
2. configure
3. server-group sip group *server-group-name* *network*

4. `element ip-address ipaddress port {udp | tcp | tls} [q-value q-value] [weight weight]`
5. `lb-type {global | highest-q | request-uri | call-id | to-uri | weight }`
6. `end server-group`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>cusp</code>  例: <code>se-10-0-0-0&gt; cusp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ2	<code>configure</code>  例: <code>se-10-0-0-0 (cusp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ3	<code>server-group sip group server-group-name network</code>  例: <code>se-10-0-0-0 (cusp-config)&gt; server-group sip group sp.example.com service-provider</code>	SIP サーバグループを作成し、サーバグループコマンドモードを開始します。この場合、作成されるサーバグループの名前は「sp.example.com」です。「sp.example.com」は、「service-provider」という名前のネットワークを使用します。
ステップ4	<code>element ip-address ipaddress port {udp   tcp   tls} [q-value q-value] [weight weight]</code>  例: <code>se-10-0-0-0 (cusp-config-sg)&gt; element ip-address 192.168.10.3 5060 tls q-value 1.0 weight 100</code>	SIP サーバグループの IP 要素を作成し、この SIP サーバグループの特性を決定します。  (注) このコマンドは、複数回入力できます。
ステップ5	<code>lb-type {global   highest-q   request-uri   call-id   to-uri   weight }</code>  例: <code>se-10-0-0-0 (cusp-config-sg)&gt; lb-type weight</code>	SIP サーバグループのロードバランシングアルゴリズムを設定します。この例では、同じ q-value を持つ他の要素の重みに対して、その重みに比例して要素が選択されることを指定します。
ステップ6	<code>end server-group</code>  例: <code>se-10-0-0-0 (cusp-config-sg)&gt; end server-group</code>	サーバグループコマンドモードを終了します。

## 例

```

se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> server-group sip group sp.example.com service-provider
se-10-0-0-0 (cusp-config-sg)> element ip-address 192.168.10.3 5060 tls q-value 1.0 weight 100
se-10-0-0-0 (cusp-config-sg)> element ip-address 192.168.10.4 5060 tls q-value 1.0 weight 50

```

```

se-10-0-0-0(cusp-config-sg)> element ip-address 192.168.10.5 5060 tls q-value 1.0 weight
50
se-10-0-0-0(cusp-config-sg)> lb-type weight
se-10-0-0-0(cusp-config-sg)> end server-group

```

## ルート テーブルの設定

- 「ルート テーブルについて」 (P.22)
- 「手順の概要」 (P.22)
- 「手順の詳細」 (P.22)
- 「例」 (P.23)

## ルート テーブルについて

SIP 要求を適切な宛先へ送るには、ルート テーブルを設定する必要があります。各ルート テーブルは、ルックアップ ポリシーに基づいて照合するキーのセットで構成されています。たとえば、各キーはダイヤルされた電話番号の市外局番を表す場合があります。

## 手順の概要

1. **cusp**
2. **configure**
3. **route table *table-name***
4. **key *key* response *response-code***
5. **key *key* target-destination *target-destination network***
6. **end route table**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>cusp</b>  例： se-10-0-0-0> <b>cusp</b>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<b>configure</b>  例： se-10-0-0-0(cusp)> <b>configure</b>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ3	<code>route table table-name</code>  例: se-10-0-0-0 (cusp-config)> <code>route table service-provider-table</code>	ルートテーブルを作成し、ルートテーブルコマンドモードを開始します。この場合、「service-provider-table」という名前のルートテーブルが作成されます。
ステップ4	<code>key key response response-code</code>  例: se-10-0-0-0 (cusp-config-rt)> <code>key * response 404</code>	応答コードを検索キーに割り当てます。この例では、「404」の応答がすべてに割り当てられます。
ステップ5	<code>key key target-destination target-destination network</code>  例: se-10-0-0-0 (cusp-config-rt)> <code>key 510 target-destination cube-sp.example.com cube-sp</code>	宛先要素の key 部分を指定した値に置き換えます。 (注) このコマンドは、複数回入力できます。
ステップ6	<code>end route table</code>  例: se-10-0-0-0 (cusp-config-rt)> <code>end route table</code>	ルートテーブルコマンドモードを終了します。

## 例

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> route table service-provider-table
se-10-0-0-0 (cusp-config-rt)> key * response 404
se-10-0-0-0 (cusp-config-rt)> key 510 target-destination cube-sp.example.com cube-sp
se-10-0-0-0 (cusp-config-rt)> end route table
```

## 正規化ポリシーの設定

正規化ポリシーは、互換性がないネットワークを考慮して SIP メッセージを変更します。この場合、サービスプロバイダーがエスケープシーケンスの「91」を処理できないため、request-uri と TO ヘッダーからシーケンスを削除する必要があります。

- [「手順の概要」 \(P.23\)](#)
- [「手順の詳細」 \(P.24\)](#)
- [「例」 \(P.24\)](#)

## 手順の概要

1. `cusp`
2. `configure`
3. `policy normalization policy_name`

4. `uri-component update request-uri {user | host | host-port | phone | uri} {all | match-string} replace-string`
5. `uri-component update header {first | last | all} {user | host | host-port | phone | uri} {all | match-string} replace-string`
6. `end policy`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>cusp</code>  例： <code>se-10-0-0-0&gt; cusp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<code>configure</code>  例： <code>se-10-0-0-0 (cusp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ 3	<code>policy normalization policy-name</code>  例： <code>se-10-0-0-0 (cusp-config)&gt; policy normalization outgoing-norm-policy</code>	正規化ポリシーを作成し、ポリシー正規化コマンドモードを開始します。この例では、正規化ポリシーの名前を「outgoing-norm-policy」にします。
ステップ 4	<code>uri-component update request-uri {user   host   host-port   phone   uri} {all   match-string} replace-string</code>  例： <code>se-10-0-0-0 (cusp-config-norm)&gt; uri-component update request-uri user ^91 ""</code>	request-URI に含まれる URI コンポーネントフィールドを更新する正規化ポリシー手順を設定します。
ステップ 5	<code>uri-component update header {first   last   all} {user   host   host-port   phone   uri} {all   match-string} replace-string</code>  例： <code>se-10-0-0-0 (cusp-config-norm)&gt; uri-component update TO all user ^91 ""</code>	ソースメッセージのヘッダーに含まれる URI コンポーネントフィールドを更新する正規化ポリシー手順を設定します。
ステップ 6	<code>end policy</code>  例： <code>se-10-0-0-0 (cusp-config-norm)&gt; end policy</code>	ポリシー正規化コマンドモードを終了します。

## 例

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> policy normalization outgoing-norm-policy
```

```

se-10-0-0-0 (cusp-config-norm)> uri-component update request-uri user ^91 ""
se-10-0-0-0 (cusp-config-norm)> uri-component update TO all user ^91 ""
se-10-0-0-0 (cusp-config-norm)> end policy

```

## ルックアップ ポリシーの設定

ルックアップ ポリシーによって、ルート テーブル内のキーの使われ方が決まります。各キーは、ダイヤルされる電話番号の先頭を表します。これは、各ポリシーが、`request-uri` のユーザ コンポーネントをルート テーブル内のキーに対して照合するための記述であるためです。`request-uri` のユーザ コンポーネントは、呼び出される電話番号です。照合に使用されるルールはプレフィックスで、これはルート テーブル内の最も長いプレフィックス マッチが使用されることを意味します。したがって、ダイヤルされた番号が `510-1XX-XXXX` である場合、呼び出しは `cme.example.com` サーバグループへ送られます。ダイヤルされた番号が `510-XXX-XXXX` である場合、呼び出しは `cucm.example.com` サーバグループへ送られます。以下のサンプルの 4 つのポリシーは、それぞれが特定のテーブルを参照することを除いて同一です。

- 「手順の概要」 (P.25)
- 「手順の詳細」 (P.25)
- 「例」 (P.26)

## 手順の概要

1. `cusp`
2. `configure`
3. `policy lookup policy-name`
4. `sequence sequence-number`
5. `rule {exact | prefix | subdomain | subnet | fixed length} [case-insensitive]`
6. `end sequence`
7. `end policy`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>cusp</code>  例： <code>se-10-0-0-0&gt; cusp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<code>configure</code>  例： <code>se-10-0-0-0 (cusp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<code>policy lookup policy-name</code>  例： se-10-0-0-0(cusp-config)> <b>policy lookup service-provider-policy</b>	指定した名前のポリシーを作成し、ポリシー ルックアップ コマンド モードを開始します。この場合、作成されるポリシーの名前は「service-provider-policy」です。
ステップ 4	<code>sequence sequence-number</code>  例： se-10-0-0-0(cusp-config-lookup)> <b>sequence 1</b>	指定した数字のシーケンスを作成し、ポリシー ルックアップ シーケンス コマンド モードを開始します。シーケンスは、その数字の順番に従って実行されます。
ステップ 5	<code>rule {exact   prefix   subdomain   subnet   fixed length} [case-insensitive]</code>  例： se-10-0-0-0(cusp-config-lookup-seq)> <b>rule prefix</b>	ルックアップ ポリシーのルーティング アルゴリズムを決定するルールを作成します。  この場合、最も長いプレフィクスの一致をルックアップ ポリシーで検索することを指定するルールが作成されます。
ステップ 6	<code>end sequence</code>  例： se-10-0-0-0(cusp-config-lookup-seq)> <b>end sequence</b>	ポリシー ルックアップ シーケンス コマンド モードを終了します。
ステップ 7	<code>end policy</code>  例： se-10-0-0-0(cusp-config-lookup)> <b>end policy</b>	ポリシー ルックアップ コマンド モードを終了します。

## 例

```

se-10-0-0-0> cusp
se-10-0-0-0(cusp)> configure
se-10-0-0-0(cusp-config)> policy lookup service-provider-policy
se-10-0-0-0(cusp-config-lookup)> sequence 1 service-provider-table request-uri
uri-component user
se-10-0-0-0(cusp-config-lookup-seq)> rule prefix
se-10-0-0-0(cusp-config-lookup-seq)> end sequence
se-10-0-0-0(cusp-config-lookup)> end policy

```

## ルーティング トリガーの設定

ルーティング トリガーは、トリガー条件をルックアップ ポリシーと相互に関連付けます。照合される対応条件によって、単一のポリシーが選択されます。条件はシーケンス番号の昇順で評価されます。ポリシー ステップが `mid-dialog` メッセージでスキップされるように、`mid-dialog` 条件が最初に評価されます。以下の設定に基づき、INVITE メッセージが正常にルーティングされた後、それに続くすべてのメッセージ (`mid-dialog`) はルーティング ポリシーをバイパスします。

- 「手順の概要」 (P.27)
- 「手順の詳細」 (P.27)
- 「例」 (P.27)



## 手順の概要

1. `culp`
2. `configure`
3. `trigger routing sequence sequence-number {by-pass | policy policy} [condition trigger-condition]`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>culp</code>  例: <code>se-10-0-0-0&gt; culp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ2	<code>configure</code>  例: <code>se-10-0-0-0 (culp)&gt; configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ3	<code>trigger routing sequence sequence-number {by-pass   policy policy} [condition trigger-condition]</code>  例: <code>se-10-0-0-0 (culp-config)&gt; trigger routing sequence 2 policy service-provider-policy condition call-from-service-provider</code>	ルーティング ポリシーをトリガー条件と関連付けます。  この例では、2番目のシーケンスは、以前に作成した「service-provider-policy」というポリシーと、以前に作成した「call-from-service-provider」というトリガーに従います。

## 例

```
se-10-0-0-0> culp
se-10-0-0-0 (culp)> configure
se-10-0-0-0 (culp-config)> trigger routing sequence 1 by-pass condition mid-dialog
se-10-0-0-0 (culp-config)> trigger routing sequence 2 policy service-provider-policy
condition call-from-service-provider
se-10-0-0-0 (culp-config)> trigger routing sequence 3 policy cube-sp-policy condition
call-from-cube-sp
se-10-0-0-0 (culp-config)> trigger routing sequence 4 policy cube-es-policy condition
call-from-cube-es
se-10-0-0-0 (culp-config)> trigger routing sequence 5 policy enterprise-policy condition
call-from-enterprise
```

## 正規化トリガーの設定

正規化トリガーは、トリガー条件を正規化ポリシーと相互に関連付けます。トリガーには、ルーティングの前に発生する pre-normalization と、ルーティングの後に発生する post-normalization の 2 種類があります。ルーティング ポリシーと同様に、特殊なポリシーは mid-dialog メッセージでの正規化をバイパスします。

- 「手順の概要」(P.28)

- 「手順の詳細」 (P.28)
- 「例」 (P.28)

## 手順の概要

1. **cusp**
2. **configure**
3. **trigger pre-normalization sequence** *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>cusp</b>  例： se-10-0-0-0> <b>cusp</b>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<b>configure</b>  例： se-10-0-0-0 (cusp)> <b>configure</b>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ 3	<b>trigger pre-normalization sequence</b> <i>sequence-number</i> { <b>by-pass</b>   <b>policy</b> <i>policy</i> } [ <b>condition</b> <i>trigger-condition</i> ]  例： se-10-0-0-0 (cusp-config)> <b>trigger pre-normalization sequence 2 policy outgoing-norm-policy condition call-from-cube-sp</b>	着信 SIP メッセージの正規化前アルゴリズムを正規化ポリシーに設定します。  この例では、2 番目のシーケンスは、以前に作成した「outgoing-norm-policy」というポリシーと、以前に作成した「call-from-cube-sp」というトリガーに従います。

## 例

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> trigger pre-normalization sequence 1 by-pass condition
mid-dialog
se-10-0-0-0 (cusp-config)> trigger pre-normalization sequence 2 policy outgoing-norm-policy
condition call-from-cube-sp
```

## リッスンポートとレコードルートポートの設定

各ネットワークのリッスンポートとレコードルートポートを設定する必要があります。リッスンポートとレコードルートポートでは、Cisco Unified SIP Proxy モジュールの実際のアドレスが使用されません。**sip record-route** コマンドは、発信要求内に record-route ヘッダーを挿入します。**sip listen** コマンドは、Cisco Unified SIP Proxy がそのポートで受信要求を受け付けられるようにします。

- 「手順の概要」 (P.29)
- 「手順の詳細」 (P.29)
- 「例」 (P.30)

### 手順の概要

1. **cusp**
2. **configure**
3. **sip record-route** *network\_name* {**tcp** | **tls** | **udp**} *ip\_address* [*port*]
4. **sip listen** *network\_name* {**tcp** | **tls** | **udp**} *ip\_address* *port*

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>cusp</b>  例: se-10-0-0-0> <b>cusp</b>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ2	<b>configure</b>  例: se-10-0-0-0 (cusp)> <b>configure</b>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。
ステップ3	<b>sip record-route</b> <i>network_name</i> { <b>tcp</b>   <b>tls</b>   <b>udp</b> } <i>ip_address</i> [ <i>port</i> ]  例: se-10-0-0-0 (cusp-config)> <b>sip record-route</b> <b>service-provider</b> <b>udp</b> 10.10.10.99 5060	SIP ネットワークのレコードルーティングをイネーブルにします。  この例では、「service-provider」ネットワークはレコードルート コンフィギュレーションに関連付けられ、Record-Route ヘッダー フィールドに入力される IP アドレスは「10.10.10.99」、Record-Route ヘッダー フィールドに入力されるポートは 5060 です。
ステップ4	<b>sip listen</b> <i>network_name</i> { <b>tcp</b>   <b>tls</b>   <b>udp</b> } <i>ip_address</i> <i>port</i>  例: se-10-0-0-0 (cusp-config)> <b>sip listen</b> <b>service-provider</b> <b>udp</b> 10.10.10.99 5060	特定の SIP ネットワーク、ホスト、およびポート上の SIP トラフィックをリッスンするリスナーを作成します。

## 例

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> sip record-route service-provider udp 10.10.10.99 5060
se-10-0-0-0 (cusp-config)> sip listen service-provider udp 10.10.10.99 5060
```

## ホスト名の設定

アップストリーム要素がネットワーク内の 2 つの Cisco Unified SIP Proxy をルーティングするために DNS SRV を使用している場合、この 2 つの Cisco Unified SIP Proxy が同じ FQDN を持つように設定する必要があります。これを行うには、両方の Cisco Unified SIP Proxy の Cisco Unified SIP Proxy コンフィギュレーション モードで **sip alias** コマンドを入力します。

- 「手順の概要」 (P.30)
- 「手順の詳細」 (P.30)
- 「例」 (P.31)

## 手順の概要

1. **cusp**
2. **configure**
3. **sip alias hostname**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>cusp</b>  例： se-10-0-0-0> <b>cusp</b>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ 2	<b>configure</b>  例： se-10-0-0-0 (cusp)> <b>configure</b>	Cisco Unified SIP Proxy コンフィギュレーション モードを開始します。
ステップ 3	<b>sip alias hostname</b>  例： se-10-0-0-0 (cusp-config)> <b>sip alias myhost</b>	このインスタンスのホスト名を設定します。

## 例

```
se-10-0-0-0> cusp
se-10-0-0-0 (cusp)> configure
se-10-0-0-0 (cusp-config)> sip alias myhost
```

## トランスポート レイヤ セキュリティ (TLS) の設定

- 「署名付き証明書の作成とインポート」(P.31)
- 「Cisco Unified SIP Proxy 上での TLS の作成」(P.33)

## 署名付き証明書の作成とインポート

Cisco Unified SIP Proxy では、TLS、伝送制御プロトコル (TCP)、およびユーザ データグラム プロトコル (UDP) がサポートされています。TLS 接続の確立には署名付き証明書による認証が必要なため、いくつか追加の手順が必要です。

- 「前提条件」(P.31)
- 「手順の概要」(P.31)
- 「手順の詳細」(P.32)
- 「署名付き証明書の作成例」(P.32)

## 前提条件

証明書要求をエクスポートするには、FTP サーバか HTTP が必要です。

## 手順の概要

1. **configure terminal**
2. **crypto key generate [rsa {label label-name | modulus modulus-size} | default]**
3. **crypto key certreq label label-name url {ftp: | http:}**
4. **crypto key import rsa label label-name {der url {ftp: | http: } | pem {terminal | url {ftp: | http: }} [default]**
5. **crypto key import cer label mykey url ftp:**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code>  例: <code>se-10-0-0-0# configure terminal</code>	コンフィギュレーション モードを開始します。
ステップ 2	<code>crypto key generate [rsa {label label-name   modulus modulus-size}   default]</code>  例: <code>se-10-0-0-0(config)&gt; crypto key generate rsa label mykey modulus 512 default</code>	RSA 秘密キーを作成します。
ステップ 3	<code>crypto key certreq label label-name url {ftp:   http:}</code>  例: <code>se-10-0-0-0(config)&gt; crypto key certreq label mykey url ftp:</code>	署名する証明書要求を作成します。
ステップ 4	<code>crypto key import rsa label label-name {der url {ftp:   http: }   pem { terminal   url {ftp:   http: } } [default]</code>  例: <code>se-10-0-0-0(config)&gt; crypto key import trustcacert label rootCA url ftp:</code>	証明書要求に署名した後、要求への署名に使用した信頼済み認証局 (CA) をインポートします。
ステップ 5	<code>crypto key import rsa label label-name {der url {ftp:   http: }   pem { terminal   url {ftp:   http: } } [default]</code>  例: <code>se-10-0-0-0(config)&gt; crypto key import cer label mykey url ftp:</code>	ルート CA をインポートした後、署名付き証明書をインポートします。

## 署名付き証明書の作成例

```

se-10-0-0-0# configure terminal
se-10-0-0-0(config)> crypto key generate rsa label mykey modulus 512 default
Key generation in progress. Please wait...
The label name for the key is mykey

se-10-0-0-0(config)> crypto key certreq label mykey url ftp:
Address or name of remote host? 192.168.202.216
Username (ENTER if none)? anonymous
Password (not shown)?
Destination path? netmod/mykey.csr
Uploading CSR file succeed

se-10-0-0-0(config)> crypto key import trustcacert label rootCA url ftp:
Import certificate file...
Address or name of remote host? 192.168.202.216
Source filename? netmod/rootCA/cacert.pem
1212 bytes received.

```

```

se-10-0-0-0(config)> crypto key import cer label mykey url ftp:
Import certificate file...
Address or name of remote host? 192.168.202.216
Source filename? netmod/mycert.cer
952 bytes received.
Import succeeded

```

#### 次の作業

- TLS ピア要素のいずれかに使用する、信頼済み CA 証明書をインポートします。

## Cisco Unified SIP Proxy 上での TLS の作成

証明書をインポートしたら、TLS 接続を有効にする必要があります。セキュリティを強化する場合は、信頼済みピアのリストを作成できます。このリストを作成すると、指定したピアからの接続だけを受け付けます。ピアのホスト名エントリは、証明書内にあるピアの `subjectAltName` である必要があります。subjectAltName が証明書内で使用されていない場合は、ピアのホスト名エントリは CN である必要があります。

- [「手順の概要」 \(P.33\)](#)
- [「手順の詳細」 \(P.33\)](#)
- [「TLS の設定例」 \(P.34\)](#)

### 手順の概要

1. `cusp`
2. `configure`
3. `sip tls`
4. `sip tls trusted-peer {peer ' s-hostname}`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>cusp</code>  例: se-10-0-0-0> <code>cusp</code>	Cisco Unified SIP Proxy EXEC モードを開始します。
ステップ2	<code>configure</code>  例: se-10-0-0-0 (cusp)> <code>configure</code>	Cisco Unified SIP Proxy コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<pre>sip tls</pre> <p>例:</p> <pre>se-10-0-0-0(cusp-config)&gt; sip tls</pre>	インターネット経由のセキュアな通信を提供する、他の SIP エンティティによる SIP TLS 接続の使用をイネーブルにします。
ステップ 4	<pre>sip tls trusted-peer {peer's-hostname}</pre> <p>例:</p> <pre>se-10-0-0-0(cusp-config)&gt; sip tls trusted-peer example.com</pre>	信頼済みピアのリストを作成します。

## TLS の設定例

```
se-10-0-0-0> cusp
se-10-0-0-0(cusp)> configure
se-10-0-0-0(cusp-config)> sip tls
se-10-0-0-0(cusp-config)> sip tls trusted-peer example.com
```

## 設定の確定

ここで設定を確定する必要があります。設定を確定する目的は 2 つあります。設定をアクティブにすることとその保持のためです。

- 現在有効な設定を表示するには、**show configuration active** コマンドを入力します。
- 変更を確定した後で有効になる設定を表示するには、**show configuration candidate** コマンドを入力します。
- このサンプルの設定を確定するには、次のコマンドを入力します。

```
se-10-0-0-0(cusp-config)> commit
```





## データのバックアップおよび復元



(注) バックアップ サーバの設定は、初期設定のプロセスで行います。まだ行っていない場合は、「[バックアップパラメータの設定](#)」(P.9) を参照してください。

- 「[データのバックアップおよび復元について](#)」(P.35)
- 「[データのバックアップおよび復元に関する制約事項](#)」(P.35)
- 「[ファイルのバックアップ](#)」(P.36)
- 「[ファイルの復元](#)」(P.38)
- 「[関連項目](#)」(P.39)

## データのバックアップおよび復元について

Cisco Unified SIP Proxy のバックアップ機能および復元機能は、FTP サーバを使用してデータの保存および取得を行います。バックアップ機能によって、ファイルは Cisco Unified SIP Proxy モジュールから FTP サーバにコピーされます。復元機能によって、ファイルは FTP サーバから Cisco Unified SIP Proxy アプリケーションにコピーされます。FTP サーバは、バックアップ機能および復元機能が IP アドレスまたはホスト名を使用して FTP サーバにアクセスできる限り、ネットワークの任意の場所に配置できます。

システム ファイルやアプリケーション ファイルに変更を加えた場合は、設定ファイルを常にバックアップすることを推奨します。コンフィギュレーション データを保持するためにバックアップを定期的に行ってください。

システムでは、次のタイプのバックアップがサポートされています。

- すべて：すべてのファイルおよびデータをバックアップします。
- 設定：システムおよびアプリケーションの設定だけをバックアップします。
- データ：ルートおよびアプリケーション データだけをバックアップします。

## データのバックアップおよび復元に関する制約事項

- システムのバックアップおよび復元を行うときは、オフライン モードになっている必要があります。そのため、コールトラフィックに最も影響を与えないときにこれらのタスクを実行することを推奨します。オフライン モードでは、すべてのコールが終了します。
- Cisco Unified SIP Proxy では、次のバックアップおよび復元機能はサポートされていません。

- バックアップ操作および復元操作のスケジュール。バックアップおよび復元の手順は、適切なコマンドを入力したときに開始されます。
- メッセージ格納域の配置の一元化。Cisco Unified SIP Proxy バックアップ ファイルをその他のメッセージストアと併用または統合することはできません。
- 選択的なバックアップおよび復元。完全バックアップ機能と完全復元機能のみが使用できません。個々のメッセージやその他の特定のデータを格納または取得することはできません。

## ファイルのバックアップ

- 「ファイルのバックアップについて」 (P.36)
- 「手順の概要」 (P.36)
- 「手順の詳細」 (P.37)
- 「例」 (P.37)

## ファイルのバックアップについて

Cisco Unified SIP Proxy は、各バックアップにバックアップ ID を自動的に割り当てます。バックアップには 3 種類ありますが、システムでバックアップ ID が生成されるときにバックアップの種類は考慮されません。したがって、2 つのバックアップが、一方がコンフィギュレーション ファイルで、他方がデータ ファイルであるとしても、同じバックアップ ID を持つということはありません。

復元するファイルのバックアップ ID を判別するには、EXEC モードまたはオフライン モードで **show backup server** コマンドまたは **show backup history** コマンドを使用します。これらのコマンドによって、リモート バックアップ サーバにあるすべての使用可能なバックアップのコピーと、それぞれのバックアップ ID が表示されます。

## 手順の概要

1. **offline**
2. **backup category {all | configuration | data}**
3. **continue**
4. **show backup history**
5. **show backup server**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<b>offline</b>  <b>例 :</b> se-10-0-0-0# <b>offline</b> !!!WARNING!!!: Putting the system offline will terminate all active calls. Do you wish to continue[n]? : <b>y</b>	オフライン モードを開始します。すべてのコールが終了します。  <b>(注)</b> Cisco Unified SIP Proxy は引き続きオフライン モードでコールをルーティングします。
ステップ2	<b>backup category {all   configuration   data}</b>  <b>例 :</b> se-10-0-0-0 (offline)# <b>backup category all</b> se-10-0-0-0 (offline)# <b>backup category configuration</b> se-10-0-0-0 (offline)# <b>backup category data</b>	バックアップして保存するデータのタイプを指定します。
ステップ3	<b>continue</b>  <b>例 :</b> se-10-0-0-0 (offline)# <b>continue</b>	オフライン モードを終了し、システムを以前のオンライン モードに戻します。システムは、新しいコールおよびボイス メッセージの処理を開始します。
ステップ4	<b>show backup history</b>  <b>例 :</b> se-10-0-0-0> <b>show backup history</b>	各バックアップ ファイル、そのバックアップ ID、ファイルに保存されているデータのタイプ、およびバックアップ手順の成否を表示します。
ステップ5	<b>show backup server</b>  <b>例 :</b> se-10-0-0-0> <b>show backup server</b>	バックアップ サーバで使用できるバックアップ ファイルの一覧を表示します。ファイルはカテゴリ別にグループ化され、バックアップの日付とバックアップ ファイル ID がそれぞれ表示されます。

## 例

次の例では、**show backup history** コマンドおよび **show backup server** コマンドの出力を示します。

```
se-10-0-0-0> show backup history

blade522> show backup history
#Start Operation
Category: Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation: Backup
Backupid: 1
Date: Tue Oct 21 06:14:30 EDT 2008
Result: Success
Reason:
#End Operation

#Start Operation
Category: Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation: Restore
Backupid: 1
```

```
Restoreid: 1
Date: Tue Oct 21 06:17:21 EDT 2008
Result: Success
Reason:
#End Operation
```

```
se-10-0-0-0> show backup server
```

```
Category: Data
Details of last 5 backups
Backupid: 1
Date: Tue Jul 22 10:55:52 PDT 2008
Description:
Backupid: 2
Date: Tue Jul 29 18:06:33 PDT 2008
Description:
Backupid: 3
Date: Tue Jul 29 19:10:32 PDT 2008
Description:
Category: Configuration
Details of last 5 backups
Backupid: 1
Date: Tue Jul 22 10:55:48 PDT 2008
Description:
Backupid: 2
Date: Tue Jul 29 18:06:27 PDT 2008
Description:
Backupid: 3
Date: Tue Jul 29 19:10:29 PDT 2008
Description:
```

```
se-10-0-0-0>
```

## ファイルの復元

- 「ファイルの復元について」(P.38)
- 「手順の概要」(P.38)
- 「手順の詳細」(P.39)

## ファイルの復元について

バックアップ ファイルを作成した後は、必要に応じてファイルを復元できます。復元はオフラインモードで行います。これによってすべてのコールが終了します。したがって、コールトラフィックに最も影響を与えないときにファイルを復元する必要があります。

復元するファイルのバックアップ ID を判別するには、EXEC モードまたはオフラインモードで **show backup server** コマンドまたは **show backup history** コマンドを使用します。

## 手順の概要

1. **show backup server**
2. **offline**
3. **restore id backup\_ID category {all | configuration | data}**

4. show backup history
5. reload

## 手順の詳細

	コマンドまたはアクション	目的
ステップ1	<pre>show backup server</pre> <p>例:</p> <pre>se-10-0-0-0&gt; show backup server</pre>	データおよび設定のバックアップ ファイルを一覧表示します。復元するファイルのリビジョン番号は、バックアップ ID フィールドで確認します。
ステップ2	<pre>offline</pre> <p>例:</p> <pre>se-10-0-0-0# offline !!!WARNING!!!: Putting the system offline will terminate all active calls. Do you wish to continue[n]? : y</pre>	オフライン モードを開始します。すべてのコールが終了します。 <b>(注)</b> Cisco Unified SIP Proxy は引き続きオフライン モードでコールをルーティングします。
ステップ3	<pre>restore id backup_ID category {all   configuration   data}</pre> <p>例:</p> <pre>se-10-0-0-0 (offline) # restore id 22 category all</pre>	バックアップ ID の値と復元するファイルのタイプを指定します。
ステップ4	<pre>show backup history</pre> <p>例:</p> <pre>se-10-0-0-0&gt; show backup history</pre>	バックアップおよび復元手順の成否とバックアップ ID を表示します。
ステップ5	<pre>reload</pre> <p>例:</p> <pre>se-10-0-0-0 (offline) # reload</pre>	アップロードされたファイル情報をアクティブにして、Cisco Unified SIP Proxy システムを再起動します。

## 関連項目

- 初期設定のプロセスで行うバックアップ サーバの設定については、「[バックアップ パラメータの設定](#)」(P.9) を参照してください。
- コンフィギュレーションのバックアップおよび復元に使用される CLI コマンドについては、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。





# Cisco Unified SIP Proxy システムのメンテナンス

- 「設定のコピー」 (P.41)
- 「ハードディスク メモリの装着アクティビティの確認」 (P.43)

## 設定のコピー

スタートアップ コンフィギュレーションおよび実行コンフィギュレーションを Cisco Unified SIP Proxy モジュール上のハードディスク、ネットワーク FTP サーバ、およびネットワーク TFTP サーバにコピーしたり、これらからコピーしたりするには、モジュール EXEC コマンドを使用します。



(注)

使用している特定の TFTP サーバによっては、TFTP サーバ上で同じ名前のファイルを作成し、ファイルが正しい許可を持っていることを確認してから、実行コンフィギュレーションを TFTP サーバへ転送する必要があります。

- 「ハードディスクから別の場所へのスタートアップ コンフィギュレーションのコピー」 (P.41)
- 「ネットワーク FTP サーバから別の場所へのスタートアップ コンフィギュレーションのコピー」 (P.42)
- 「ハードディスクから別の場所への実行コンフィギュレーションのコピー」 (P.42)
- 「ネットワーク TFTP サーバから別の場所への実行コンフィギュレーションのコピー」 (P.43)

## ハードディスクから別の場所へのスタートアップ コンフィギュレーションのコピー

モジュール EXEC モードで、次のコマンドを使用して、ハードディスク上のスタートアップ コンフィギュレーションを別の場所にコピーします。

```
copy startup-config {ftp: user-id:password@ftp-server-url | tftp:tftp-server-url}
```

## 構文の説明

<b>ftp:</b> <i>user-id:password@</i>	FTP サーバのユーザ名およびパスワード。エントリに、コロン (:) とアットマーク (@) を含めます。
<i>ftp-server-url</i>	ディレクトリおよびファイル名を含む FTP サーバの URL。たとえば、 <code>ftps://server/dir/filename</code> です。
<b>tftp:</b> <i>tftp-server-url</i>	ディレクトリおよびファイル名を含む TFTP サーバの URL。たとえば、 <code>tftps://server/dir/filename</code> です。

このコマンドはインタラクティブであり、ユーザに情報の入力を求めます。パラメータは 1 行では入力できません。この例では、スタートアップ コンフィギュレーションが FTP サーバにコピーされます。FTP サーバは、ファイルを転送するためのユーザ名およびパスワードを要求します。スタートアップ コンフィギュレーション ファイルは、「start」というファイル名で FTP サーバ上に保存されます。

```
se-10-0-0-0> copy startup-config ftp
Address or name of remote host? admin:messaging@ftps://server/dir/start
Source filename? temp_start
```

次の例では、スタートアップ コンフィギュレーションが TFTP サーバにコピーされます。TFTP サーバは、ユーザ名およびパスワードを要求します。このコマンドは、「configs」という名前の TFTP ディレクトリに「temp\_start」という名前のファイルとしてスタートアップ コンフィギュレーションを保存します。

```
se-10-0-0-0> copy startup-config tftp
Address or name of remote host? tftps://server/dir/temp_start
Source filename? temp_start
```

## ネットワーク FTP サーバから別の場所へのスタートアップ コンフィギュレーションのコピー

モジュール EXEC モードで、次のコマンドを使用して、ネットワーク FTP サーバ上のスタートアップ コンフィギュレーションを別の場所にコピーします。

```
copy ftp: {nvram:startup-config | running-config | startup-config | system:running-config}
```

このコマンドの詳細については、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。

このコマンドはインタラクティブであり、ユーザに情報の入力を求めます。パラメータは 1 行では入力できません。次の例は、このプロセスを示しています。この例では、FTP サーバはユーザ名およびパスワードを要求します。このコマンドは、「congifs」という名前の FTP サーバ ディレクトリに存在する「start」という名前のファイルをスタートアップ コンフィギュレーションにコピーします。

```
se-10-0-0-0> copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? admin:messaging@tftps://server/configs
Source filename? start
```

## ハード ディスクから別の場所への実行コンフィギュレーションのコピー

モジュール EXEC モードで、次のコマンドを使用して、ハード ディスク上の実行コンフィギュレーションを別の場所にコピーします。

```
copy running-config {ftp: user-id:password@ftps://server/dir/filename | startup-config | tftp:tftps://server/dir/filename }
```



このコマンドの詳細については、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。

このコマンドは、コマンドのコピー先に応じて双方向に機能します。

- 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーする場合、次の例のように 1 行でコマンドを入力します。

```
se-10-0-0-0> copy running-config startup-config
```

- 実行コンフィギュレーションを FTP サーバまたは TFTP サーバにコピーする場合、このコマンドはインタラクティブになり、ユーザに情報の入力を求めます。パラメータは 1 行では入力できません。次の例では、実行コンフィギュレーションが FTP サーバにコピーされます。FTP サーバはユーザ名とパスワードを要求します。実行コンフィギュレーションは、「configs」という名前のディレクトリに「saved\_start」という名前のファイルとしてコピーされます。

```
se-10-0-0-0> copy running-config ftp:
Address or name of remote host? admin:messaging@ftps://server/configs
Source filename? saved_start
```

## ネットワーク TFTP サーバから別の場所への実行コンフィギュレーションのコピー

モジュール EXEC モードで、次のコマンドを使用して、ネットワーク TFTP サーバから別の場所に実行コンフィギュレーションをコピーします。

```
copy tftp: {running-config | startup-config} tftps://server/dir/filename
```

### 構文の説明

<b>running-config</b>	ハードディスク上のアクティブ コンフィギュレーション。
<b>startup-config</b>	ハードディスク上のスタートアップ コンフィギュレーション。
<i>tftp-server-url</i>	TFTP サーバの URL。

このコマンドはインタラクティブであり、ユーザに情報の入力を求めます。パラメータは 1 行では入力できません。次の例は、このプロセスを示しています。この例では、TFTP サーバ上の「configs」という名前のディレクトリに存在する「start」という名前のファイルが、スタートアップ コンフィギュレーションにコピーされます。

```
se-10-0-0-0> copy tftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? tftps://server/configs
Source filename? start
```

## ハードディスクメモリの装着アクティビティの確認

Cisco Unified SIP Proxy は、ハードディスクメモリの使用および装着をログとして追跡します。追跡データは、モジュールに保存されます。このデータを表示するには、モジュール EXEC モードで **show interfaces** コマンドを使用します。

次の例は、出力例です。

```
se-10-0-0-0> show interfaces
GigabitEthernet 0 is up, line protocol is up
Internet address is 10.10.1.20 mask 255.255.255.0 (configured on router)
```

## ■ ハード ディスク メモリの装着アクティビティの確認

```
25629 packets input, 1688582 bytes
0 input errors, 0 dropped, 0 overrun, 0 frame errors
25634 packets output, 1785015 bytes
0 output errors, 0 dropped, 0 overrun, 0 collision errors
0 output carrier detect errors
IDE hd0 is up, line protocol is up
2060 reads, 32704512 bytes
0 read errors
489797 write, 2520530944 bytes
0 write errors
```



## トラブルシューティング

---

- 「CLI コマンドを使用したシステムのトラブルシューティング」 (P.45)
- 「コンフィギュレーションの変更のトラブルシューティング」 (P.47)
- 「関連項目」 (P.47)

## CLI コマンドを使用したシステムのトラブルシューティング

問題のトラブルシューティング時に、シスコのテクニカル サポート担当者がこれらのコマンドを複数実行することをお願いする場合があります。シスコのテクニカル サポート担当者はそのときに、コマンドに関する追加情報をお伝えします。



注意

これらのコマンドの一部は、システムのパフォーマンスに影響を与える場合があります。Cisco Technical Support による指示がない限り、これらのコマンドを使用しないことを強く推奨します。

- 「ログについて」 (P.45)
- 「Log コマンド」 (P.46)
- 「ログ出力の例」 (P.46)
- 「Trace コマンドの使用」 (P.46)
- 「Show コマンドの使用」 (P.47)

## ログについて

システムの問題をデバッグするために、ログ メッセージを使用できます。ログ メッセージは、`messages.log` ファイルに保存されます。

デフォルトでは、ハード ディスクに対するログおよびトレースはオフになっています。`log trace boot` コマンドを実行すると、ログおよびトレース機能がすぐに開始されます。

ハード ディスクにあるログ ファイルおよびトレース ファイルを確認するには、Cisco Unified SIP Proxy EXEC モードで `show logs` コマンドを使用します。このコマンドにより、使用可能なログのリスト、ログのサイズ、および最新の変更が行われた日付が表示されます。

各ファイルは 10 MB の固定長で、この長さに達すると、トレースおよびロギングは自動的に停止します。古いファイルは、新しいファイルによって上書きされます。



ヒント

ログ ファイルの内容を表示できない場合は、ログ ファイルを Cisco Unified SIP Proxy から外部サーバへコピーして、**vi** などのテキスト エディタを使用して内容を表示します。

## Log コマンド

Cisco Unified SIP Proxy には、次の log コマンドがあります。

- **log console** コマンド
- **log console monitor** コマンド
- **log server** コマンド
- **log trace boot** コマンド
- **log trace buffer save** コマンド
- **show logs** コマンド
- **show trace log** コマンド

## ログ出力の例

次に、ログ出力の例を示します。

```
se-Module (exec-mping) > show logs

SIZELAST_MODIFIED_TIMENAME
28719Mon Dec 22 14:15:06 EST 2008linux_session.log
2573Fri Dec 19 08:28:13 EST 2008install.log
8117Fri Dec 19 08:27:51 EST 2008dmesg
2274Fri Dec 19 08:27:55 EST 2008syslog.log
10455Thu Dec 18 16:38:13 EST 2008sshd.log.prev
1268Fri Dec 19 08:28:09 EST 2008atrace.log
384 Fri Dec 19 08:27:55 EST 2008debug_server.log
10380Thu Dec 18 16:06:58 EST 2008postgres.log.prev
1361Fri Dec 19 08:28:14 EST 2008sshd.log
5598Fri Dec 19 08:30:13 EST 2008postgres.log
1014Fri Dec 19 08:27:57 EST 2008klog.log
2298494Sun Dec 21 23:30:00 EST 2008messages.log
85292Fri Dec 19 08:25:33 EST 2008shutdown_installer.log
```

## Trace コマンドの使用

Cisco Unified SIP Proxy のネットワーク コンフィギュレーションのトラブルシューティングを実行するには、Cisco Unified SIP Proxy EXEC モードで **trace enable** コマンドを実行します。

Cisco Unified SIP Proxy には、次の trace コマンドがあります。

- **log trace boot** コマンド
- **log trace buffer save** コマンド
- **show trace log** コマンド
- **show trace options** コマンド
- **trace disable** コマンド

- `trace enable` コマンド
- `trace level` コマンド

## Show コマンドの使用

Cisco Unified SIP Proxy コンフィギュレーションのトラブルシューティングを実行するために、標準の show コマンドに加えて次のコマンドを使用します。

- `show status queue`
- `show status server-group radius [server-group-name]`
- `show status server-group sip [server-group-name]`
- `show status sip`

## コンフィギュレーションの変更のトラブルシューティング

**問題** コンフィギュレーション データの一部が失われました。

**推奨処置** 変更内容を実行コンフィギュレーションに頻繁にコピーします。「[設定のコピー](#)」(P.41) を参照してください。

**問題** システムを再起動したときにコンフィギュレーション データが失われました。

**説明** 再起動する前にデータを保存していませんでした。

**推奨処置** `copy running-config startup-config` コマンドを使用して、変更内容を実行コンフィギュレーションからスタートアップ コンフィギュレーションにコピーします。Cisco Unified SIP Proxy の再起動時に、スタートアップ コンフィギュレーションがリロードされます。「[設定のコピー](#)」(P.41) を参照してください。



**(注)** メッセージはアプリケーション データと見なされて、スタートアップ コンフィギュレーションのディスクに直接保存されます (停電の場合や、新規にインストールする場合は、別のサーバにバックアップする必要があります)。これ以外のコンフィギュレーションの変更をスタートアップ コンフィギュレーションに保持するには、明示的に「コンフィギュレーションの保存」操作を行う必要があります。

## 関連項目

- CLI コマンドについては、『[CLI Command Reference for Cisco Unified SIP Proxy Release 8.5](#)』を参照してください。
- コンフィギュレーションのコピーについては、「[設定のコピー](#)」(P.41) を参照してください。





## 設定例

---

次の例では、Cisco Unified SIP Proxy システムの設定後、**show configuration active verbose** コマンドを入力すると表示される内容を示します。

```
se-10-0-0-0 (cusp-config)> show configuration active verbose
Building CUSP configuration...
!
server-group sip global-load-balance call-id
server-group sip retry-after 0
server-group sip element-retries udp 3
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
sip alias myhostname
sip dns-srv
  enable
  no naptr
  end dns
!
no sip header-compaction
no sip logging
!
sip max-forwards 70
sip network cube-es standard
  no non-invite-provisional
  allow-connections
  retransmit-count invite-server-transaction 9
  retransmit-count non-invite-client-transaction 9
  retransmit-count invite-client-transaction 5
  retransmit-timer clientTn 64000
  retransmit-timer serverTn 64000
  retransmit-timer T4 5000
  retransmit-timer T2 4000
  retransmit-timer T1 500
  retransmit-timer TU2 32000
  retransmit-timer TU1 5000
  end network
!
sip network cube-sp standard
  no non-invite-provisional
  allow-connections
  retransmit-count invite-server-transaction 9
  retransmit-count invite-client-transaction 5
  retransmit-count non-invite-client-transaction 9
  retransmit-timer T4 5000
  retransmit-timer T2 4000
  retransmit-timer T1 500
  retransmit-timer TU2 32000
  retransmit-timer TU1 5000
  retransmit-timer clientTn 64000
```

```
retransmit-timer serverTn 64000
end network
!
sip network enterprise standard
no non-invite-provisional
allow-connections
retransmit-count invite-client-transaction 5
retransmit-count invite-server-transaction 9
retransmit-count non-invite-client-transaction 9
retransmit-timer serverTn 64000
retransmit-timer T4 5000
retransmit-timer T2 4000
retransmit-timer T1 500
retransmit-timer TU2 32000
retransmit-timer TU1 5000
retransmit-timer clientTn 64000
end network
!
sip network service-provider standard
no non-invite-provisional
allow-connections
retransmit-count invite-server-transaction 9
retransmit-count non-invite-client-transaction 9
retransmit-count invite-client-transaction 5
retransmit-timer serverTn 64000
retransmit-timer TU1 5000
retransmit-timer TU2 32000
retransmit-timer T1 500
retransmit-timer T2 4000
retransmit-timer T4 5000
retransmit-timer clientTn 64000
end network
!
sip overload reject retry-after 0
!
no sip peg-counting
!
sip privacy service
sip queue message
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue radius
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue request
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue response
drop-policy head
low-threshold 80
size 2000
thread-count 20
```



```
end queue
!
sip queue st-callback
drop-policy head
low-threshold 80
size 2000
thread-count 10
end queue
!
sip queue timer
drop-policy none
low-threshold 80
size 2500
thread-count 8
end queue
!
sip queue xcl
drop-policy head
low-threshold 80
size 2000
thread-count 2
end queue
!
route recursion
!
sip tcp connection-timeout 240
sip tcp max-connections 256
sip tls
!
trigger condition call-from-cube-es
sequence 1
in-network cube-es
end sequence
end trigger condition
!
trigger condition call-from-cube-sp
sequence 1
in-network cube-sp
end sequence
end trigger condition
!
trigger condition call-from-enterprise
sequence 1
in-network enterprise
end sequence
end trigger condition
!
trigger condition call-from-service-provider
sequence 1
in-network service-provider
end sequence
end trigger condition
!
trigger condition mid-dialog
sequence 1
mid-dialog
end sequence
end trigger condition
!
accounting
no enable
no client-side
no server-side
end accounting
```

```

!
server-group sip group cme.example.com enterprise
element ip-address 192.168.10.6 5060 tls q-value 1.0 weight 0
failover-resp-codes 503
lbtype global
ping
end server-group
!
server-group sip group cube-es.example.com cube-es
element ip-address 192.168.20.4 5060 tls q-value 1.0 weight 0
element ip-address 192.168.20.3 5060 tls q-value 1.0 weight 0
failover-resp-codes 503
lbtype global
ping
end server-group
!
server-group sip group cube-sp.example.com cube-sp
element ip-address 10.10.20.3 5060 tls q-value 1.0 weight 0
element ip-address 10.10.20.4 5060 tls q-value 1.0 weight 0
failover-resp-codes 503
lbtype global
ping
end server-group
!
server-group sip group cucm.example.com enterprise
element ip-address 192.168.10.4 5060 tls q-value 1.0 weight 50
element ip-address 192.168.10.5 5060 tls q-value 1.0 weight 50
element ip-address 192.168.10.3 5060 tls q-value 1.0 weight 100
failover-resp-codes 503
lbtype weight
ping
end server-group
!
server-group sip group sp.example.com service-provider
element ip-address 10.10.10.3 5060 udp q-value 1.0 weight 0
failover-resp-codes 503
lbtype global
ping
end server-group
!
route table cube-es-table
key * response 404
key 5101 target-destination cme.example.com enterprise
key 510 target-destination cucm.example.com enterprise
end route table
!
route table cube-sp-table
key * target-destination sp.example.com service-provider
end route table
!
route table enterprise-table
key * response 404
key 5101 target-destination cme.example.com enterprise
key 91 target-destination cube-es.example.com cube-es
key 510 target-destination cucm.example.com enterprise
end route table
!
route table service-provider-table
key * response 404
key 510 target-destination cube-sp.example.com cube-sp
end route table
!
policy normalization outgoing-norm-policy
uri-component update TO all user ^91 ""

```

```
    uri-component update request-uri user ^91 ""
  end policy
!
policy lookup cube-es-policy
  sequence 1 cube-es-table request-uri uri-component user
  rule prefix
  end sequence
end policy
!
policy lookup cube-sp-policy
  sequence 1 cube-sp-table request-uri uri-component user
  rule prefix
  end sequence
end policy
!
policy lookup enterprise-policy
  sequence 1 enterprise-table request-uri uri-component user
  rule prefix
  end sequence
end policy
!
policy lookup service-provider-policy
  sequence 1 service-provider-table request-uri uri-component user
  rule prefix
  end sequence
end policy
!
trigger routing sequence 5 policy enterprise-policy condition call-from-enterpri
se
trigger routing sequence 4 policy cube-es-policy condition call-from-cube-es
trigger routing sequence 3 policy cube-sp-policy condition call-from-cube-sp
trigger routing sequence 2 policy service-provider-policy condition
call-from-service-provider
trigger routing sequence 1 by-pass condition mid-dialog
trigger pre-normalization sequence 2 policy outgoing-norm-policy condition
call-from-cube-sp
trigger pre-normalization sequence 1 by-pass condition mid-dialog
!
no server-group sip global-ping
!
sip listen service-provider udp 10.10.10.99 5060
sip listen cube-sp tls 10.10.20.99 5060
sip listen cube-es tls 192.168.20.99 5060
sip listen enterprise tls 192.168.10.99 5060
!
sip record-route cube-es tls 192.168.20.99 5060
sip record-route service-provider udp 10.10.10.99 5060
sip record-route cube-sp tls 10.10.20.99 5060
sip record-route enterprise tls 192.168.10.99 5060
!
end
se-10-0-0-0(cusp-config)>
```





## INDEX

---

### B

- backup category コマンド [36](#)
- backup revisions number コマンド [10](#)
- backup server url コマンド [10](#)

---

### C

- Cisco Unified Communications Manager [20](#)
- clock timezone コマンド [15](#)
- configure terminal コマンド [10, 12, 13, 15, 31](#)
- configure コマンド [17, 18, 20, 22, 23, 25, 27, 28, 29, 30, 33](#)
- continue コマンド [36](#)
- copy ftp コマンド [42](#)
- copy running-config startup-config コマンド [12, 13, 47](#)
- copy running-config コマンド [42](#)
- copy startup-config コマンド [41](#)
- copy tftp コマンド [43](#)
- crypto key certreq label コマンド [31](#)
- crypto key generate コマンド [31](#)
- crypto key import cer label コマンド [31](#)
- crypto key import rsa label コマンド [31](#)
- cusp コマンド [17, 18, 20, 22, 23, 25, 27, 28, 29, 30, 33](#)

---

### D

- DNS サーバ
  - ホスト名を IP アドレスに解決 [11](#)

---

### E

- element ip-address コマンド [21](#)

- end network コマンド [17](#)
- end policy コマンド [24, 25](#)
- end route table コマンド [22](#)
- end sequence コマンド [19, 25](#)
- end server-group コマンド [21](#)
- end trigger condition コマンド [19](#)
- end コマンド [10, 12](#)
- exit コマンド [13](#)

---

### F

- FTP サーバ
  - スタートアップ コンフィギュレーションのコピー [42](#)
  - バックアップおよび復元 [9, 35](#)

---

### I

- in-network コマンド [19](#)

---

### K

- key response コマンド [22](#)
- key target-destination コマンド [22](#)

---

### L

- lb-type コマンド [21](#)
- log console monitor コマンド [46](#)
- log console コマンド [46](#)
- log server コマンド [46](#)
- log trace boot コマンド [45, 46](#)
- log trace buffer save コマンド [46](#)

**M**

messages.log、ファイル サイズ **45**  
 mid-dialog コマンド **19**

**N**

ntp server コマンド **12, 13**  
 NTP サーバ  
   削除 **13**  
   設定 **11**  
   表示 **14**  
 NTP サーバの削除 **13**

**O**

offline コマンド **36, 38**

**P**

policy lookup コマンド **25**  
 policy normalization コマンド **23**

**Q**

q-value **20**

**R**

reload コマンド **39**  
 restore id コマンド **38**  
 route table コマンド **22**  
 rule コマンド **25**

**S**

sequence コマンド **19, 25**  
 server-group sip group コマンド **20**

show backup history コマンド **36, 39**  
 show backup server コマンド **36, 38**  
 show backup コマンド **10**  
 show clock detail コマンド **15**  
 show configuration active コマンド **34**  
 show configuration candidate コマンド **34**  
 show interfaces コマンド **43**  
 show logs コマンド **45, 46**  
 show ntp associations コマンド **14**  
 show ntp configuration コマンド **12, 13**  
 show ntp servers コマンド **14**  
 show ntp source コマンド **14**  
 show ntp status コマンド **12, 13, 14**  
 show status queue コマンド **47**  
 show status server-group radius コマンド **47**  
 show status server-group sip コマンド **47**  
 show status sip コマンド **47**  
 show trace log コマンド **46**  
 show trace options コマンド **46**  
 show コマンド **47**  
 sip alias コマンド **30**  
 sip listen コマンド **29**  
 sip network コマンド **17**  
 sip record-route コマンド **29**  
 sip tls trusted-peer コマンド **33**  
 sip tls コマンド **33**

**T**

TFTP サーバ、コンフィギュレーションのコピー **43**  
 TLS、設定 **31**  
 trace disable コマンド **46**  
 trace enable コマンド **47**  
 trace level コマンド **47**  
 trace コマンド **46**  
 trigger condition コマンド **18**  
 trigger pre-normalization sequence コマンド **28**  
 trigger routing sequence コマンド **27**

---

**U**

uri-component update header コマンド [24](#)  
 uri-component update request-uri コマンド [24](#)

---

**お**

オフライン モード [38](#)

---

**か**

完全修飾ドメイン名、設定 [20](#)

---

**<**

グラフィカル ユーザ インターフェイス  
 概要 [1, 2](#)

---

**こ**

コピー

設定 [41](#)

コマンド

backup category [36](#)  
 backup revisions number [10](#)  
 backup server url [10](#)  
 clock timezone [15](#)  
 configure [17, 18, 20, 22, 23, 25, 27, 28, 29, 30, 33](#)  
 configure terminal [10, 12, 13, 15, 31](#)  
 continue [36](#)  
 copy ftp [42](#)  
 copy running-config [42](#)  
 copy running-config startup-config [12, 13, 47](#)  
 copy startup-config [41](#)  
 copy tftp [43](#)  
 crypto key certreq label [31](#)  
 crypto key generate [31](#)  
 crypto key import cer label [31](#)

crypto key import rsa label [31](#)  
 cusp [17, 18, 20, 22, 23, 25, 27, 28, 29, 30, 33](#)  
 element ip-address [21](#)  
 end [10, 12](#)  
 end network [17](#)  
 end policy [24, 25](#)  
 end route table [22](#)  
 end sequence [19, 25](#)  
 end server-group [21](#)  
 end trigger condition [19](#)  
 exit [13](#)  
 in-network [19](#)  
 key response [22](#)  
 key target-destination [22](#)  
 lb-type [21](#)  
 log console [46](#)  
 log console monitor [46](#)  
 log server [46](#)  
 log trace boot [45, 46](#)  
 log trace buffer save [46](#)  
 mid-dialog [19](#)  
 ntp server [12, 13](#)  
 offline [36, 38](#)  
 policy lookup [25](#)  
 policy normalization [23](#)  
 reload [39](#)  
 restore id [38](#)  
 route table [22](#)  
 rule [25](#)  
 sequence [19, 25](#)  
 server-group sip group [20](#)  
 show backup [10](#)  
 show backup history [36, 39](#)  
 show backup server [36, 38](#)  
 show clock detail [15](#)  
 show configuration active [34](#)  
 show configuration candidate [34](#)  
 show interfaces [43](#)  
 show logs [45, 46](#)

show ntp associations [14](#)  
 show ntp configuration [12, 13](#)  
 show ntp servers [14](#)  
 show ntp source [14](#)  
 show ntp status [12, 13, 14](#)  
 show status queue [47](#)  
 show status server-group radius [47](#)  
 show status server-group sip [47](#)  
 show status sip [47](#)  
 show trace log [46](#)  
 show trace options [46](#)  
 sip alias [30](#)  
 sip listen [29](#)  
 sip network [17](#)  
 sip record-route [29](#)  
 sip tls [33](#)  
 sip tls trusted-peer [33](#)  
 trace disable [46](#)  
 trace enable [47](#)  
 trace level [47](#)  
 trigger condition [18](#)  
 trigger pre-normalization sequence [28](#)  
 trigger routing sequence [27](#)  
 uri-component update header [24](#)  
 uri-component update request-uri [24](#)

コマンドライン インターフェイス

概要 [1](#)

---

## さ

サーバ グループ

概要 [20](#)

設定 [20](#)

---

## し

時間帯 [15](#)

証明書、作成 [31](#)

初期設定タスク

NTP サーバの設定 [11](#)

時間帯の設定 [15](#)

バックアップ パラメータの設定 [9](#)

---

## せ

正規化トリガー、概要 [27](#)

正規化トリガー、設定 [27](#)

正規化ポリシー

概要 [23](#)

設定 [23](#)

制約事項

バックアップおよび復元 [35](#)

設定

確定 [34](#)

コピー [41](#)

設定タスク

NTP サーバの設定 [11](#)

TLS の設定 [31](#)

サーバ グループの設定 [20](#)

正規化トリガーの設定 [27](#)

正規化ポリシーの設定 [23](#)

トリガー条件の設定 [18](#)

ホスト名の設定 [30](#)

リッスンポートとレコードルートポートの設定 [29](#)

ルーティング トリガーの設定 [26](#)

ルート テーブルの設定 [22](#)

バックアップ ポリシーの設定 [25](#)

論理ネットワークの設定 [17](#)

設定の確定 [34](#)

---

## て

データの損失、トラブルシューティング [47](#)

伝送制御プロトコル [31](#)



**と**

- トラブルシューティング **45**
  - show コマンドの使用 **47**
  - trace コマンドの使用 **46**
    - データの損失 **47**
- トランスポート レイヤ セキュリティ、設定 **31**
- トリガー条件
  - 設定 **18**

**は**

- ハード ディスク
  - コンフィギュレーションのコピー **42**
  - スタートアップ コンフィギュレーションのコピー **41**
  - 装着 **43**
  - ログ **45**
- バックアップ
  - FTP サーバ **9, 35**
  - 制約事項 **35**
  - 設定 **9**
  - パラメータ **9**
- パラメータ
  - バックアップ **9**

**ひ**

- 表示
  - NTP サーバ **14**

**ふ**

- ファイル サイズ
  - messages.log **45**
- 復元
  - FTP サーバ **9, 35**
  - 制約事項 **35**
  - 手順 **38**

**ほ**

- ホスト名、概要 **30**
- ホスト名、設定 **30**
- ホスト名を IP アドレスに解決 **11**

**も**

- モジュール
  - 使用 **43**
  - 装着 **43**

**ゆ**

- ユーザ データグラム プロトコル **31**

**ら**

- ライセンス
  - インストール **5**

**り**

- リッスン ポートとレコードルート ポート、設定 **29**

**る**

- ルーティング トリガー
  - 概要 **26**
  - 設定 **26**
- ルート テーブル
  - 概要 **22**
  - 設定 **22**
- バックアップ ポリシー
  - 概要 **25**
  - 設定 **25**

---

## れ

レコードルート

    ポートについて **29**

    ポートの設定 **29**

---

## ろ

ログ、概要 **45**

ログ メッセージ **45**