



# ディザスタ リカバリ システム アドミニストレーション ガイド for Cisco Unity Connection Release 8.x

Disaster Recovery System Administration Guide for Cisco Unity Connection Release 8.x

**【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。

このマニュアルでは、ディザスタ リカバリ システムの概要を紹介し、ディザスタ リカバリ システムの使用方法を説明し、さまざまなバックアップ関連のタスクおよび復元関連のタスクを完了するための手順を示します。このマニュアルは、Cisco Unified Communications Manager をはじめとする Cisco IP テレフォニ アプリケーションのユーザを対象としたリファレンス ガイドであり、さまざまな手順を参照するためのガイドとなるものです。

このマニュアルは、次の内容で構成されています。

- 「ディザスタ リカバリ システムの概要」 (P.2)
- 「Cisco Unity Connection のバックアップおよび復元を行うためのタスク リスト」 (P.3)
- 「システム要件」 (P.4)
- 「ディザスタ リカバリ システムへのアクセス方法」 (P.5)
- 「マスター エージェントの役割とアクティブ化」 (P.5)

- 「ローカル エージェント」 (P.6)
- 「バックアップ デバイスの管理」 (P.6)
- 「バックアップ スケジュールの作成と編集」 (P.8)
- 「スケジュールの有効化、無効化、および削除」 (P.10)
- 「手動バックアップの開始」 (P.10)
- 「バックアップ ステータスの確認」 (P.11)
- 「復元による Cisco Unity Connection ボイス メッセージへの影響について」 (P.12)
- 「Cisco Unity Connection サーバの復元または変更」 (P.12)
- 「復元ステータスの表示」 (P.15)
- 「バックアップ履歴および復元履歴の表示」 (P.16)
- 「トレース ファイル」 (P.17)
- 「コマンドライン インターフェイス」 (P.17)
- 「アラームおよびメッセージ」 (P.18)
- 「関連資料」 (P.20)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.20)
- 「シスコ製品のセキュリティ」 (P.20)

## ディザスタ リカバリ システムの概要

Disaster Recovery System (DRS; ディザスタ リカバリ システム) は、Cisco Unity Connection の管理から呼び出すことができるシステムで、データをバックアップして復元するための機能をすべて備えています。ディザスタ リカバリ システムでは、スケジュールリングした自動またはユーザ起動のデータバックアップを定期的に行うことができます。

DRS は、プラットフォーム バックアップ/復元の一環として、独自の設定 (バックアップ デバイス設定およびスケジュール設定) を復元します。DRS は、`drfDevice.xml` ファイルおよび `drfSchedule.xml` ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要はありません。



### 注意

Cisco Unity Connection を復元する場合は事前に、サーバにインストールされている Cisco Unity Connection バージョンが復元するバックアップ ファイルのバージョンに一致することを確認してください。ディザスタ リカバリ システムは、Cisco Unity Connection のバージョンが一致する場合に限り、復元をサポートします。たとえばディザスタ リカバリ システムでは、バージョン 6.1(1).1000-1 からバージョン 6.1(2).1000-1 への復元や、バージョン 6.1(2).1000-1 からバージョン 6.1(2).1000-2 への復元は行えません。



### 注意

Cisco Unity Connection を復元する場合は、事前に、復元のホスト名、IP アドレス、バージョン、および配置タイプが、復元するバックアップ ファイルのホスト名、IP アドレス、バージョン、および配置タイプに一致することを確認してください。

ディザスタ リカバリ システムには、次の機能が含まれています。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス

- バックアップおよび復元機能を実行するための分散システム アーキテクチャ
- バックアップのスケジューリング
- 物理的なテープ ドライブまたはリモート SFTP サーバへのバックアップのアーカイブ

ディザスタ リカバリ システムには、Master Agent (MA; マスター エージェント) と Local Agent (LA; ローカル エージェント) という 2 つの主要な機能が含まれています。マスター エージェントは、ローカル エージェントと協調してバックアップおよび復元アクティビティを調整します。



**注意**

DRS 暗号化は、クラスタ セキュリティ パスワードによって異なります。コマンドライン インターフェイスまたは新規インストールでこのセキュリティ パスワードを変更した場合は、すぐに新規バックアップを作成するか、または古いセキュリティ パスワードを記憶することを推奨します。



**(注)**

Cisco Unity Connection クラスタ処理が設定されている場合、ディザスタ リカバリ システムは、マスター エージェントとローカル エージェントとの間で SSL ベースの通信を使用して、パブリッシャ サーバとサブスクライバ サーバとの間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー / 秘密キーの暗号化を行います。証明書管理ページから IPSEC 信頼ストア (hostname.pem) ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。IPSEC 信頼ファイルを手動で削除する場合は、IPSEC 証明書を IPSEC 信頼に必ずアップロードしてください。



**注意**

コール処理が中断してサービスに影響が及ぶことがないように、バックアップはオフピーク時間にスケジューリングしてください。

## Cisco Unity Connection のバックアップおよび復元を行うためのタスク リスト

次の表は、Cisco Unity Connection のバックアップおよび復元に関するタスク リストです。



**(注)**

DRS は、バックアップ デバイス設定およびバックアップ スケジュール設定のバックアップと復元を行うので、復元後に DRS を再設定する必要はありません。

## Cisco Unity Connection のバックアップに関するタスク リスト

表 1 は、ディザスタ リカバリ システムを使用して Cisco Unity Connection のバックアップを行うためのタスク リストです。

表 1 Cisco Unity Connection のバックアップに関するタスク リスト

アクション	参照先
データのバックアップ先となるバックアップ デバイスを作成する。	「バックアップ デバイスの管理」(P.6)
スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成および編集する。	「バックアップ スケジュールの作成と編集」(P.8)
データをバックアップするためのバックアップ スケジュールを有効または無効にする。	「スケジュールの有効化、無効化、および削除」(P.10)
手動バックアップを実行する (任意)。	「手動バックアップの開始」(P.10)
バックアップのステータスを確認する: バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。	「バックアップ ステータスの確認」(P.11)

## Cisco Unity Connection の復元に関するタスク リスト

表 2 は、ディザスタ リカバリ システムを使用して Cisco Unity Connection の復元を行うためのタスク リストです。

表 2 Cisco Unity Connection の復元に関するタスク リスト

アクション	参照先
保管場所、バックアップ ファイル、機能、およびノードを選択する。	「Cisco Unity Connection サーバの復元または変更」(P.12)
復元のステータスを確認する: 復元プロセスの実行中、現在の復元ジョブのステータスを確認できます。	「復元ステータスの表示」(P.15)

## システム要件

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。シスコでは任意の SFTP サーバ製品を使用できますが、Cisco Technology Developer Partner Program (CTDP) を介してシスコが認定する SFTP 製品を使用することを推奨します。GlobalSCAPE などの CTDP パートナーは、特定のバージョンの Cisco Unity Connection での製品の使用を認定しています。お使いの Cisco Unity Connection バージョンを認定したベンダーに関する情報については、次の URL を参照してください。

<http://www.cisco.com/pcgi-bin/ctdp/Search.pl>

シスコでは社内テストに次のサーバを使用しています。いずれかのサーバを使用できますが、サポートについては各ベンダーにお問い合わせください。

- Open SSH (<http://sshwindows.sourceforge.net/> を参照)
- Cygwin (<http://www.cygwin.com/> を参照)
- Titan (<http://www.titanftp.com/> を参照)

シスコでは、SFTP 製品、freeFTPD の使用はサポートしません。この SFTP 製品では、ファイル サイズが 1 GB に制限されているためです。



(注) CTRDP プロセスでまだ認定されていないサードパーティ製品で問題が発生した場合、サポートについてはそのサードパーティ ベンダーに問い合わせてください。



(注) バックアップまたは復元の実行中、OS 管理タスクは実行できません。ディザスタ リカバリ システムではプラットフォーム API がロックされて、すべての OS 管理要求がブロックされるからです。一方、ほとんどの Command Line Interface (CLI; コマンドラインインターフェイス) コマンドはブロックされません。CLI ベースのアップグレード コマンドだけがプラットフォーム API ロッキング パッケージを使用するからです。



ヒント バックアップはネットワーク トラフィックが少なくなる時間帯にスケジューリングしてください。



(注) HP DL380-G6 サーバ (ソフトウェア専用) に移行すると、新規サーバに Cisco Unified Communications Manager の旧バージョン (5.x および 6.x) をインストールできなくなります。このため、DRS バックアップを実行できるようにするには、Cisco Unified Communications Manager の旧バージョンを古いパブリッシャ (すでにサポートされていない可能性があります) にインストールする必要があります。このバックアップが完了したら、HP DL380-G6 (ソフトウェア専用) パブリッシャにそれを復元できます。

## ディザスタ リカバリ システムへのアクセス方法

ディザスタ リカバリ システムにアクセスするには、[Cisco Unity Connection の管理 (Cisco Unity Connection Administration) ] ウィンドウの右上隅にある [ナビゲーション (Navigation) ] ドロップダウン リスト ボックスから、[ディザスタ リカバリ システム (Disaster Recovery System) ] を選択します。Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。



(注) 管理者ユーザ名とパスワードは Cisco Unity Connection のインストール時に設定したものであり、Command Line Interface (CLI; コマンドライン インターフェイス) を使用して、管理者パスワードを変更したり、新しい管理者アカウントを設定したりできます。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

## マスター エージェントの役割とアクティブ化

Master Agent (MA; マスター エージェント) はサーバ上で自動的にアクティブになります。

Master Agent (MA; マスター エージェント) は、次の役割を果たします。

- MA は、システム全体のコンポーネント登録情報を保管します。
- MA は、スケジュールされた一連のタスクを XML ファイルに保持します。MA は、ユーザ インターフェイスからスケジュール更新情報を受け取ると、このファイルを更新します。MA は、スケジュールに従って、該当するローカル エージェントに実行可能タスクを送信します (ローカル エージェントは、遅滞なくただちにバックアップ タスクを実行します)。

- ディザスタ リカバリ システム ユーザ インターフェイスから MA にアクセスすると、バックアップ デバイスの設定、バックアップ スケジュールの新規追加によるバックアップのスケジューリング、既存のスケジュールの表示または更新、実行したスケジュールのステータスの表示、システム復元の実行など、さまざまなアクティビティを実行できます。
- MA は、ローカルに接続されたテープ ドライブまたはリモート ネットワーク上の場所にバックアップ データを格納します。

## ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカル エージェントが搭載されています。

ローカル エージェントは、サーバ上でバックアップおよび復元スクリプトを実行します。



(注)

Cisco Unity Connection クラスタ処理が設定されている場合、ディザスタ リカバリ システムは、マスター エージェントとローカル エージェントとの間で SSL ベースの通信を使用して、パブリッシャ サーバとサブスクリバ サーバとの間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー / 秘密キーの暗号化を行います。この証明書交換は内部で処理されます。この交換のために設定に変更を加える必要はありません。

## バックアップ デバイスの管理

ディザスタ リカバリ システムを使用する場合は、事前に、バックアップ ファイルの保存先を設定する必要があります。最大 10 個のバックアップ デバイスを設定できます。バックアップ デバイスを設定するには、次の手順を実行します。



(注)

コマンドライン インターフェイスからデバイスを追加、削除、および一覧表示できます。DRS 用の CLI コマンドの詳細については、「[コマンドライン インターフェイス](#)」(P.17) を参照してください。

### 手順

- ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation)] リストの [ディザスタ リカバリ システム (Disaster Recovery System)] をクリックし、[移動 (Go)] をクリックします。



(注) Cisco Unity Connection クラスタ処理が設定されている場合、パブリッシャ サーバのみのバックアップを推奨します。

- [ディザスタ リカバリ システム (Disaster Recovery System)] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用すると同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [バックアップ (Backup)] > [バックアップ デバイス (Backup Device)] に移動します。[バックアップ デバイス リスト (Backup Device List)] ウィンドウが表示されます。
- ステップ 4** 新しいバックアップ デバイスを設定するには、[新規追加 (Add New)] をクリックします。
- ステップ 5** バックアップ デバイスを編集するには、[バックアップ デバイス (Backup Device)] リストでそのデバイスを選択します。次に、[選択項目の編集 (Edit Selected)] をクリックします。

[バックアップ デバイス (Backup Device) ] ウィンドウが表示されます。

**ステップ 6** [バックアップ デバイス名 (Backup device name) ] フィールドにバックアップ デバイス名を入力します。



(注) バックアップ デバイス名には、英数字、スペース ( )、ダッシュ (-)、およびアンダースコア ( \_ ) だけを使用できます。それ以外の文字は使用しないでください。

**ステップ 7** 次のいずれかのバックアップ デバイスを選択し、[バックアップ先の選択 (Select Destination) ] 領域で適切なフィールド値を入力します。

- [テープ デバイス (Tape Device) ] : ローカルに接続されたテープ ドライブにバックアップ ファイルを格納します。リストから目的のテープ デバイスを選択します。次の考慮事項に注意してください。
  - 1 つのバックアップに複数のテープは使用できません。データが 1 本のテープに収まらない場合は、ネットワーク ディレクトリにバックアップを保存する必要があります。あるいは 1 つのテープにコンポーネントをバックアップし、さらに 1 つ以上の別のテープにメールボックス ストアをバックアップする必要があります。
  - 1 本のテープに複数のバックアップは保存できません。バックアップするたびに前回のバックアップのデータが上書きされるため、最新のバックアップのデータだけが保持されます。サーバのバックアップを複数作成する場合は (たとえば、コンポーネントのバックアップと、メールボックス ストアのバックアップ)、バックアップごとに異なるテープを使用する必要があります。そうしないと、最後にバックアップしたデータだけが保持されます。



(注) VMware 仮想マシンからログインした場合は、テープへのバックアップはできません。テープ デバイス オプションが、VMware ユーザには無効になっているからです。

- [ネットワーク ディレクトリ (Network Directory) ] : バックアップ ファイルを SFTP 接続でアクセスできるネットワーク ドライブに格納します。次の必須情報を入力します。
  - [サーバ名 (Server name) ] : ネットワーク サーバの名前または IP アドレス
  - [パス名 (Path name) ] : バックアップ ファイルの保存先となるディレクトリのパス名
  - [ユーザ名 (User name) ] : リモート システム上のアカウントの有効なユーザ名
  - [パスワード (Password) ] : リモート システム上のアカウントの有効なパスワード
  - [ネットワーク ディレクトリに保存するバックアップ数 (Number of backups to store on Network Directory) ] : このネットワーク ディレクトリに保存するバックアップの数

複数の Connection サーバをバックアップする場合、各 Connection サーバに対して別々のディレクトリをネットワーク ドライブに作成することを推奨します。また、他のアプリケーション (Cisco Unified Communications Manager、Cisco Unified Presence) をバックアップするために DRS を使用する場合、サーバごとに別々のディレクトリを作成することを推奨します。ここで指定した値は、1 つのサーバのバックアップだけではなく、ディレクトリ内のすべてのバックアップに適用されます。たとえば、Connection サーバ用に 3 つのバックアップおよび Cisco Unified Communications Manager サーバ用に 3 つのバックアップを保持する場合を考えます。両方のサーバに同じネットワーク ディレクトリを指定し、両方のサーバについてディレクトリに保管するバックアップ数を 3 と指定した場合、ディレクトリには、直近 3 回分のバックアップしか表示されません。直近 3 回のバックアップが Connection サーバのバックアップである場合、Cisco Unified Communications Manager のバックアップは保管されません。

保持するバックアップが上書きされないように十分に大きい数値を指定してください。Connection サーバのフル バックアップを行うために 3 つの別々のバックアップ (MailboxStore1 コンポーネントおよび MailboxStore2 コンポーネント) を必要とするように

DRS を設定している場合で、直近 2 回分のフルバックアップを保持するときは、この項目に 6 を選択します。ディザスタリカバリシステムでは、小さい数値を選択すると、保持したいバックアップが上書きされることがあります。

[パス名 (Path name)] フィールドで指定された保管場所には、ここで指定したバックアップ数プラス 1 個を保持できる十分なスペースが必要です。ネットワークドライブに最大許容数のバックアップが保管されている場合、DRS は最新のバックアップデータを保存し、古いものから削除します。



(注) ネットワーク上に格納先を設定するには、SFTP サーバにアクセスする必要があります。バックアップに先立って SFTP パスが存在する必要があります。SFTP サーバへのアクセスに使用するアカウントには、選択したパスに対する書き込み権限が必要です。

**ステップ 8** これらの設定を更新するには、[保存 (Save)] をクリックします。



(注) [保存 (Save)] ボタンをクリックすると、選択したバックアップデバイスが、DRS マスターエージェントによって検証されます。ユーザ名、パスワード、サーバ名、またはディレクトリパスが無効である場合、保存操作は失敗します。

**ステップ 9** バックアップデバイスを削除するには、[バックアップデバイス (Backup Device)] リストでそのデバイスを選択します。次に、[選択項目の削除 (Delete Selected)] をクリックします。



(注) バックアップスケジュールにバックアップデバイスとして設定されているバックアップデバイスは削除できません。

## バックアップスケジュールの作成と編集

最大 10 個のバックアップスケジュールを作成できます。各バックアップスケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保管場所など、独自のプロパティがあります。



(注) コマンドラインインターフェイスからバックアップスケジュールを一覧表示および追加できます。DRS 用の CLI コマンドの詳細については、「[コマンドラインインターフェイス](#)」(P.17) を参照してください。



(注) バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されることに注意してください。このパスワードは、クラスタセキュリティパスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティパスワードは忘れないように記憶しておくか、またはセキュリティパスワードを変更/リセットしたらすぐにバックアップを作成する必要があります。

バックアップスケジュールを管理するには、次の手順を実行します。

## 手順

**ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation)] リストの [ディザスタ リカバリ システム (Disaster Recovery System)] をクリックし、[移動 (Go)] をクリックします。

[ディザスタ リカバリ システム (Disaster Recovery System)] ログイン ウィンドウが表示されます。

**ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。

**ステップ 3** [バックアップ (Backup)] > [スケジューラ (Scheduler)] に移動します。

[スケジュール リスト (Schedule List)] ウィンドウが表示されます。

**ステップ 4** 次のいずれかの手順を実行して、新規スケジュールを追加するか、または既存のスケジュールを編集します。

a. 新規スケジュールを作成するには、[新規追加 (Add New)] をクリックします。

b. 既存のスケジュールを設定するには、[スケジュール リスト (Schedule List)] 列でその名前をクリックします。

[スケジューラ (Scheduler)] ウィンドウが表示されます。

**ステップ 5** スケジュール名を [スケジュール名 (Schedule Name)] フィールドに入力します。



**(注)** デフォルトのスケジュールの名前は変更できません。

**ステップ 6** [バックアップ デバイスの選択 (Select Backup Device)] 領域で、バックアップ デバイスを選択します。

**ステップ 7** [機能の選択 (Select Features)] 領域で、バックアップする機能を選択します。少なくとも 1 つの機能を選択する必要があります。

次の機能のバックアップは必須です。

- 録音済みのグリーティングおよびボイス名 (CONNECTION\_GREETINGS\_VOICENAMES)。
- データベース (CONNECTION\_DATABASE)。
- その他の Connection 固有のデータ (CUC)。

メッセージのバックアップ (CONNECTION\_MESSAGES\_<データベース名>) はオプションです。

**ステップ 8** [バックアップの開始時刻 (Start Backup at)] 領域で、バックアップを開始する日付と時刻を選択します。次の点に注意してください。

- システム パフォーマンスへの影響を回避するために、バックアップはオフピーク時間にスケジューリングしてください。
- データベース統計情報更新タスクの実行時間帯にバックアップをスケジューリングすることは避けてください。デフォルトでは、このタスクは毎日午前 3 時 30 分に実行されます。

**ステップ 9** [頻度 (Frequency)] 領域で、バックアップを行う頻度を選択します。[一度 (Once)]、[日次 (Daily)]、[週次 (Weekly)]、[月次 (Monthly)] のいずれかになります。[週次 (Weekly)] を選択した場合は、バックアップを行う週の曜日も選択できます。



**ヒント** バックアップ頻度を火曜日から土曜日までの [週次 (Weekly)] に設定するには、[デフォルトの設定 (Set Default)] をクリックします。

**ステップ 10** これらの設定を更新するには、[保存 (Save)] をクリックします。

**ステップ 11** スケジュールを有効にするには、[スケジュールの有効化 (Enable Schedule)] をクリックします。

設定した時刻になると、自動的に次のバックアップが発生します。

**ステップ 12** スケジュールを無効にするには、[スケジュールの無効化 (Disable Schedule)] をクリックします。

## スケジュールの有効化、無効化、および削除

### 手順



(注)

コマンドライン インターフェイスからバックアップ スケジュールを有効化、無効化、および削除できます。DRS 用の CLI コマンドの詳細については、「[コマンドライン インターフェイス](#)」(P.17) を参照してください。

- ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation)] リストの [ディザスタ リカバリ システム (Disaster Recovery System)] をクリックし、[移動 (Go)] をクリックします。
- [ディザスタ リカバリ システム (Disaster Recovery System)] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用すると同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [バックアップ (Backup)] > [スケジューラ (Scheduler)] に移動します。
- [スケジュール リスト (Schedule List)] ウィンドウが表示されます。
- ステップ 4** 変更するスケジュールの横にあるチェックボックスをオンにします。
- すべてのスケジュールを選択するには、[すべて選択 (Select All)] をクリックします。
  - すべてのチェックボックスをオフにするには、[すべてクリア (Clear All)] をクリックします。
- ステップ 5** 選択したスケジュールを有効にするには、[選択されたスケジュールの有効化 (Enable Selected Schedules)] をクリックします。
- ステップ 6** 選択したスケジュールを無効にするには、[選択されたスケジュールの無効化 (Disable Selected Schedules)] をクリックします。
- ステップ 7** 選択したスケジュールを削除するには、[選択項目の削除 (Delete Selected)] をクリックします。

## 手動バックアップの開始

手動バックアップを開始するには、次の手順を実行します。



(注)

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。このパスワードは、クラスタ セキュリティ パスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティ パスワードは忘れないように記憶しておくか、またはセキュリティ パスワードを変更/リセットしたらすぐにバックアップを作成する必要があります。

## 手順

- ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation)] リストの [ディザスタ リカバリ システム (Disaster Recovery System)] をクリックし、[移動 (Go)] をクリックします。
- [ディザスタ リカバリ システム (Disaster Recovery System)] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [バックアップ (Backup)] > [手動バックアップ (Manual Backup)] に移動します。[手動バックアップ (Manual Backup)] ウィンドウが表示されます。
- ステップ 4** [バックアップ デバイスの選択 (Select Backup Device)] 領域で、バックアップ デバイスを選択します。
- ステップ 5** [機能の選択 (Select Features)] 領域で、バックアップする機能を選択します。
- 次の機能のバックアップは必須です。
- 録音済みのグリーティングおよびボイス名 (CONNECTION\_GREETINGS\_VOICENAMES)。
  - データベース (CONNECTION\_DATABASE)。
  - その他の Connection 固有のデータ (CUC)。
- メッセージのバックアップ (CONNECTION\_MESSAGES\_<データベース名>) はオプションです。
- ステップ 6** 手動バックアップを開始するには、[バックアップの開始 (Start Backup)] をクリックします。

## バックアップステータスの確認

現在のバックアップ ジョブのステータスを確認し、現在のバックアップ ジョブをキャンセルできます。バックアップ履歴を表示するには、「[バックアップ履歴および復元履歴の表示](#)」(P.16) を参照してください。


**注意**

リモート サーバへのバックアップが 20 時間以内に完了しないと、バックアップ セッションがタイムアウトします。その場合は、新規バックアップを開始する必要があります。

## 現在のバックアップ ジョブのステータスの確認

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

## 手順

- ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation)] リストの [ディザスタ リカバリ システム (Disaster Recovery System)] をクリックし、[移動 (Go)] をクリックします。
- [ディザスタ リカバリ システム (Disaster Recovery System)] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [バックアップ (Backup)] > [現在のステータス (Current Status)] に移動します。[バックアップ ステータス (Backup Status)] ウィンドウが表示されます。

- ステップ 4** バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。
- ステップ 5** 現在のバックアップをキャンセルするには、[バックアップのキャンセル (Cancel Backup)] をクリックします。



**(注)** 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

## 復元による Cisco Unity Connection ボイス メッセージへの影響について

Connection のバックアップを実行し、1 つ以上のメールボックス ストアを作成した後で、新規メールボックス ストアをバックアップせずに復元を実行した場合、新規メールボックス ストアは削除されます。

Connection ディレクトリのみバックアップおよび復元を実行し、Connection ボイス メッセージのバックアップおよび復元をしなかった場合、次の関連機能をユーザが使用することによってユーザフォルダの一部が削除される可能性があります。

- 下書きメッセージを最初に保存するときに、下書きフォルダが作成されるように設定できます (接続を切断するか電話を切るときに下書きメッセージが自動的に保存されるように、またはユーザが任意で下書きメッセージを保存できるように Connection を設定する必要があります)。
- メッセージに「時間指定送信」のマークを最初に付けたときに、時間指定送信フォルダが作成されます (時間指定送信フォルダは設定可能ではありません)。
- 送信済みのメッセージをリコールできる送信済みアイテムのフォルダは、メッセージのリコールを設定してから最初にボイス メッセージを送信するときに作成されます (Cisco Unity Connection の管理 では、[送信済みメッセージ: 保持期間 (日) (Sent Messages: Retention Period (in Days))] の値を変更する必要があります。[システム設定 (System Settings)] > [詳細設定 (Advanced)] > [メッセージング (Messaging)] ページで、0 より大きな値に設定します)。

ユーザ フォルダにメッセージが残っている場合、そのメッセージは「配信できないメッセージ」のフォルダに移動します。

## Cisco Unity Connection サーバの復元または変更

既存のサーバまたは Cisco Unity Connection クラスターの両方のサーバで Cisco Unity Connection データを復元する場合は、この項の手順を実行します。

Cisco Unity Connection サーバを変更、または Connection サーバ (Cisco Unity Connection クラスターのどちらかまたは両方のサーバ) のハード ディスクを変更する場合は、『*Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 8.x*』の「Replacing Cisco Unity Connection 8.x Servers or Hard Disks」の章にある該当するタスク リストを参照してください。このガイドは、[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/8x/upgrade/guide/8xcucrugx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/upgrade/guide/8xcucrugx.html) にあります。データの復元に関しては、この項の手順を実行してください。

## 手順

- ステップ 1** サーバまたは Cisco Unity Connection クラスタにソフトウェアを再インストールした場合は、適宜次の手順を実行します。
- a. サーバの IP アドレスおよびホスト名がサーバをバックアップしたときの IP アドレスおよびホスト名に一致することを確認します。一致しない場合、復元は失敗します。  
 また、Cisco Unity Connection が仮想マシンで動作している場合、次の設定がサーバをバックアップしたときの値と一致することを確認します。この設定は Connection 仮想マシンのライセンス MAC の値を作成するために使用します。これらの設定のいずれかを後から変更する場合は、仮想マシンの新しいライセンス ファイルを取得する必要があります。
    - 時間帯 (Time zone)
    - NTP サーバ
    - NIC (速度/デュプレックス) 設定
    - DHCP 設定
    - プライマリ DNS 設定
    - SMTP ホスト名
    - X.509 証明書情報 (組織、部門、ロケーション、都道府県、および国)
  - b. バックアップを作成したときにインストールされた Connection のバージョンが、サーバにインストールする Cisco Unity Connection のバージョンと完全に一致することを確認します。  
 たとえば、ディザスタ リカバリ システムではバージョン 8.5.(1).1000-1 からバージョン 8.5.(2).1000-1 への復元や、バージョン 8.5.(2).1000-1 からバージョン 8.5.(2).1000-2 への復元は行えません (バージョンの末尾の数字はサービス リリースまたはエンジニアリング スペシャルをインストールするごとに変わります)。
  - c. Cisco Unity Connection サーバがバックアップされたときに有効だったセキュリティ パスワードがあることを確認します。  
 DRS はセキュリティ パスワードを暗号キーとして使用し、バックアップ データを暗号化します。直近のバックアップの後にセキュリティ パスワードを変更した場合、DRS は古いセキュリティ パスワードを要求します。
  - d. サーバに元々インストールされていたライセンスを再インストールします。
  - e. 接続言語を以前にインストールした場合は、その同じ言語を再インストールします。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、Cisco Unity Connection サーバの [ディザスタ リカバリ システム (Disaster Recovery System)] にログインします。
- ステップ 3** [復元 (Restore)] > [復元ウィザード (Restore Wizard)] に移動します。[復元ウィザード ステップ 1 (Restore Wizard Step 1)] ウィンドウが表示されます。
- ステップ 4** [バックアップ デバイスの選択 (Select Backup Device)] 領域で、復元元となるバックアップ デバイスを選択します。次に、[次へ (Next)] をクリックします。  
 [復元ウィザード ステップ 2 (Restore Wizard Step 2)] ウィンドウが表示されます。
- ステップ 5** 復元するバックアップ ファイルを選択します。



(注) バックアップ ファイル名は、システムがバックアップ ファイルを作成した日時を示します。

**ステップ 6** [次へ (Next) ] をクリックします。[復元ウィザード ステップ 3 (Restore Wizard Step 3) ] ウィンドウが表示されます。

**ステップ 7** 次の機能の復元は必須です。

- 録音済みのグリーティングおよびボイス名 (CONNECTION\_GREETINGS\_VOICENAMES)。
- データベース (CONNECTION\_DATABASE)。
- その他の Connection 固有のデータ (CUC)。

メッセージの復元 (CONNECTION\_MESSAGES\_<データベース名 >) はオプションです。



**(注)** バックアップされた機能だけが表示されます。

**ステップ 8** [次へ (Next) ] をクリックします。[復元ウィザード ステップ 4 (Restore Wizard Step 4) ] ウィンドウが表示されます。

**ステップ 9** ファイル整合性チェックを実行する場合は、[SHA1 メッセージ ダイジェストを使用したファイル整合性チェックの実行 (Select the Perform file integrity check using SHA1 Message Digest) ] チェックボックスをオンにします。



**(注)** ファイル整合性チェックは任意で、SFTP バックアップの場合にだけ必要です。テープおよびローカル デバイス バックアップから復元するときには、ファイル整合性チェックを実行する必要はありません。



**(注)** ファイル整合性チェックの処理は CPU およびネットワーク帯域幅を大量に消費するため、復元プロセスの処理速度が大きく低下します。

**ステップ 10** 復元するノードを選択するよう求められた場合は、**ステップ 7** で選択したものと同一機能を選択し、[次へ (Next) ] をクリックします。



**注意**

選択した機能の既存のデータが上書きされます。

**ステップ 11** データの復元を開始するには、[復元 (Restore) ] をクリックします。



**(注)** **ステップ 7** で [SHA1 メッセージ ダイジェストを使用したファイル整合性チェックの実行 (Select the Perform file integrity check using SHA1 Message Digest) ] チェックボックスをオンにした場合、[復元 (Restore) ] をクリックすると、DRS が各ファイルに対してファイル整合性チェックを実行します。チェック中に .tar ファイルに不一致が見つかり、復元プロセスは整合性チェックに失敗したコンポーネントをエラーとし、次の .tar ファイル (つまり、次のコンポーネント) の復元に進みます。

**ステップ 12** 復元のステータスを表示するには、「復元ステータスの表示」(P.15) を参照してください。

**ステップ 13** サーバを再起動します。再起動の詳細については、『Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 8.x』の「System Restart」の章を参照してください。このガイドは、[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/8x/os\\_administration/guide/8xcucosagx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosagx.html) にあります。

**ステップ 14** Connection スタンドアロン サーバを復元する場合は、**ステップ 15** に進みます。

Connection クラスタを復元する場合、パブリッシャ サーバからサブスライバ サーバへのデータのコピーを Connection に実行させます。

- a. パブリッシャ サーバの再起動が終了したら、サブスライバ サーバのコマンドライン インターフェイスにログインします。
- b. コマンドラインで次のコマンドを実行し、パブリッシャ サーバからサブスライバ サーバへのデータのコピーを Connection に実行させます。

```
utils cuc cluster overwrittenb
```

- c. サブスライバ サーバで Connection クラスタのステータスをチェックします。コマンドラインで、次のコマンドを実行します。

```
show cuc cluster status
```

- d. パブリッシャ サーバのコマンドライン インターフェイスにログインします。
- e. パブリッシャ サーバで Connection クラスタのステータスをチェックします。コマンドラインで、次のコマンドを実行します。

```
show cuc cluster status
```

**ステップ 15** オフピーク時間中に、各電話システムのメッセージ待機インジケータを再同期します。

- a. Cisco Unity Connection の管理 で、[テレフォニー インテグレーション (Telephony Integrations) ] を展開し、[電話システム (Phone System) ] をクリックします。
- b. 最初の電話システムの名前をクリックします。
- c. [この電話システムのすべての MWI を同期する (Synchronize All MWIs on This Phone System) ] で [実行 (Run) ] をクリックします。
- d. 残りの電話システムについて手順 a. ~ c. を繰り返します。

**ステップ 16** サーバまたはハードディスクについては、『*Reconfiguration and Upgrade Guide for Cisco Unity Connection Release 8.x*』の「Replacing Cisco Unity Connection 8.x Servers or Hard Disks」の章にある該当するタスク リストを参照してください。このガイドは、[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/8x/upgrade/guide/8xcucrugx.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/upgrade/guide/8xcucrugx.html) にあります。

## 復元ステータスの表示

現在の復元ジョブのステータスを確認するには、次の手順を実行します。

### 手順

- ステップ 1** Cisco Unity Connection の管理で、[ナビゲーション (Navigation) ] リストの [ディザスタ リカバリ システム (Disaster Recovery System) ] をクリックし、[移動 (Go) ] をクリックします。  
[ディザスタ リカバリ システム (Disaster Recovery System) ] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [復元 (Restore) ] > [ステータス (Status) ] に移動します。[復元ステータス (Restore Status) ] ウィンドウが表示されます。

[ 復元ステータス (Restore Status) ] ウィンドウの [ ステータス (Status) ] 列に、復元手順の完了率など、進行中の復元のステータスが表示されます。

**ステップ 4** 復元ログ ファイルを表示するには、ログファイル名リンクをクリックします。

## バックアップ履歴および復元履歴の表示

次の手順を使用すると、最新の 20 個のバックアップおよび復元ジョブを表示できます。

- 「[バックアップ履歴](#)」
- 「[復元履歴](#)」

### バックアップ履歴

バックアップ履歴を参照するには、次の手順を実行します。

#### 手順

- ステップ 1** Cisco Unity Connection の管理で、[ ナビゲーション (Navigation) ] リストの [ ディザスタ リカバリ システム (Disaster Recovery System) ] をクリックし、[ 移動 (Go) ] をクリックします。
- [ ディザスタ リカバリ システム (Disaster Recovery System) ] ログイン ウィンドウが表示されます。
- ステップ 2** Cisco Unified Communications Operating System 管理に使用すると同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [ バックアップ (Backup) ] > [ 履歴 (History) ] に移動します。[ バックアップ履歴 (Backup History) ] ウィンドウが表示されます。
- ステップ 4** [ バックアップ履歴 (Backup History) ] ウィンドウから、ファイル名、バックアップ デバイス、完了日、結果、バックアップされている機能など、これまでに実行したバックアップの情報を参照できます。



**(注)** [ バックアップ履歴 (Backup History) ] ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

### 復元履歴

復元履歴を参照するには、次の手順を実行します。

#### 手順

- ステップ 1** Cisco Unity Connection の管理で、[ ナビゲーション (Navigation) ] リストの [ ディザスタ リカバリ システム (Disaster Recovery System) ] をクリックし、[ 移動 (Go) ] をクリックします。
- [ ディザスタ リカバリ システム (Disaster Recovery System) ] ログイン ウィンドウが表示されます。

- ステップ 2** Cisco Unified Communications Operating System 管理に使用するのと同じ管理者ユーザ名とパスワードを使用して、ディザスタ リカバリ システムにログインします。
- ステップ 3** [復元 (Restore) ] > [履歴 (History) ] に移動します。[復元履歴 (Restore History) ] ウィンドウが表示されます。
- ステップ 4** [復元履歴 (Restore History) ] ウィンドウから、ファイル名、バックアップ デバイス、完了日、結果、復元した機能など、これまでに実行した復元の情報を参照できます。



(注) [復元履歴 (Restore History) ] ウィンドウには、最新の 20 個の復元ジョブだけが表示されます。

## トレース ファイル

ディザスタ リカバリ システムのこのリリースでは、マスター エージェント、GUI、および各ローカル エージェントのトレース ファイルが次の場所書き込まれます。

- マスター エージェントの場合、トレース ファイルは `platform/drf/trace/drfMA0*` にあります。
- 各ローカル エージェントの場合、トレース ファイルは `platform/drf/trace/drfLA0*` にあります。
- GUI の場合、トレース ファイルは `platform/drf/trace/drfConfLib0*` にあります。

トレース ファイルを表示するには、コマンドライン インターフェイスを使用します。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

## コマンドライン インターフェイス

また、ディザスタ リカバリ システムでは表 3 に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの内容とコマンドライン インターフェイスの使用法の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

表 3 ディザスタ リカバリ システム コマンドライン インターフェイス

コマンド	説明
<code>utils disaster_recovery backup</code>	ディザスタ リカバリ システム インターフェイスに設定されている機能を使用して、手動バックアップを開始します。
<code>utils disaster_recovery restore</code>	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するために、パラメータが必要です。
<code>utils disaster_recovery status</code>	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
<code>utils disaster_recovery show_backupfiles</code>	既存のバックアップ ファイルを表示します。
<code>utils disaster_recovery cancel_backup</code>	進行中のバックアップ ジョブをキャンセルします。
<code>utils disaster_recovery show_registration</code>	現在設定されている登録を表示します。

表 3 ディザスタ リカバリ システム コマンドライン インターフェイス (続き)

コマンド	説明
utils disaster_recovery show_tapeid	テープ識別情報を表示します。
utils disaster_recovery device add	ネットワーク デバイスまたはテープ デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。

## アラームおよびメッセージ

ディザスタ リカバリ システム (DRS) は、バックアップ手順または復元手順の実行中にエラーなどの条件が発生すると、アラームなどのメッセージを発行します。表 4 に、シスコ DRS アラームの一覧を示します。

表 4 ディザスタ リカバリ システム アラームおよびメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアッププロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアップ プロセスでデバイスへのアクセス中にエラーが発生しました。
DRFBackupFailure	シスコ DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセスでエラーが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRS は、別のバックアップの実行中は新規バックアップを開始できません。
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS 内部プロセスでエラーが発生しました。
DRFLA2MAFailure	DRF ローカル エージェントが、マスター エージェントに接続できません。	DRS ローカル エージェントが、マスター エージェントに接続できません。
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェントがダウンしている可能性があります。
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェントがローカル エージェントに接続できません。

表 4 ディザスタ リカバリ システム アラームおよびメッセージ (続き)

アラーム名	説明	説明
DRFMABackupComponent Failure	DRF は、少なくとも 1 つのコンポーネントをバックアップできません。	DRS はコンポーネントのデータをバックアップするように要求しましたが、バックアッププロセス中にエラーが発生し、コンポーネントはバックアップされませんでした。
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスター エージェントから切断されました。	DRS マスター エージェントが Cisco Unity Connection ノードでバックアップ操作を実行しているときに、そのノードが、バックアップ操作が完了する前に切断されました。
DRFMARestoreComponent Failure	DRF は、少なくとも 1 つのコンポーネントを復元できません。	DRS はコンポーネントのデータを復元するように要求しましたが、復元プロセス中にエラーが発生し、コンポーネントは復元されませんでした。
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスター エージェントから切断されました。	DRS マスター エージェントが Cisco Unity Connection ノードで復元操作を実行しているときに、そのノードが、復元操作が完了する前に切断されました。
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェントがダウンしている可能性があります。
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコンポーネントがないため、DRS バックアップが失敗しました。
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能が選択されませんでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、デバイスから読み取ることができません。
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーが発生しました。
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーが発生しています。
DRFSecurityViolation	DRF システムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセージには、コードインジェクションやディレクトリトラバーサルなど、セキュリティ違反となる可能性がある悪意のあるパターンが含まれています。DRF ネットワーク メッセージはブロックされました。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストアが見つかりません。DRF ローカル エージェントが、マスター エージェントに接続できません。

表 4 ディザスタ リカバリ システム アラームおよびメッセージ (続き)

アラーム名	説明	説明
DRFUnknownClient	パブリッシャの DRF マスター エージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。	パブリッシャの DRF マスター エージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。
DRFLocalDeviceError	DRF は、ローカル デバイスにアクセスできません。	DRF は、ローカル デバイスにアクセスできません。
DRFBackupCompleted	DRF バックアップが正常に完了しました。	DRF バックアップが正常に完了しました。
DRFRestoreCompleted	DRF の復元が正常に完了しました。	DRF の復元が正常に完了しました。
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行または新規インストール後に、現在のシステムの有効なバックアップが見つかりませんでした。

## 関連資料

Cisco.com にある Cisco Unity Connection のマニュアルの説明と URL については、『*Documentation Guide for Cisco Unity Connection Release 8.x*』を参照してください。このマニュアルは Connection に同梱されており、次の URL から入手できます。

[http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/connection/8x/roadmap/8xcucdg.html](http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/roadmap/8xcucdg.html)

## 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。

## シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。

[http://www.access.gpo.gov/bis/ear/ear\\_data.html](http://www.access.gpo.gov/bis/ear/ear_data.html)

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 アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワークトポロジ図、およびその他の図は、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および電話番号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。

© 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.

