CHAPTER 7

Cisco Emergency Responder 8.5 向け Cisco Unified オペレーティング システムの設定

次のトピックで、Cisco Emergency Responder（Cisco ER）8.5 に付属の Cisco Unified Communications オペレーティング システムの設定および使用方法を説明します。

Cisco Unified Communications Operating System の管理へのログイン

Cisco Unified Communications Operating System の管理にアクセスしてログインするには、次の手順に従います。

（注） Cisco Unified Communications Operating System の管理を使用する場合、ブラウザのコントロール（[Back] ボタンなど）は使用しないでください。

手順

ステップ 1 Cisco ER にログインします。

ステップ 2 [Cisco ER Administration] ページの上部右隅の [Navigation] メニューから、[Cisco Unified OS Administration] を選択して [Go] をクリックします。

[Cisco Unified Communications Operating System Administration Logon] ウィンドウが表示されます。

（注）　また、次の URL を入力して Cisco Unified Communications Operating System の管理に直接アクセスすることもできます。
http://*server-name***/cmplatform**

ステップ 3　管理者ユーザ名とパスワードを入力します。

（注）　管理者ユーザ名とパスワードは、インストール時に決めるか、コマンドライン インターフェイスを使用して作成します。

ステップ 4　[Submit] をクリックします。

[Cisco Unified Communications Operating System Administration] ウィンドウが表示されます。

管理者パスワードとセキュリティ パスワードの復旧

管理者パスワードやセキュリティ パスワードがわからなくなった場合、次の手順に従ってパスワードをリセットします。

パスワードを復旧するには、システム コンソール経由でシステムに接続している必要があります。つまり、キーボードとモニタをサーバに接続している必要があります。システムにセキュア シェル接続している状態でパスワードを復旧できません。

注意　サーバ グループのすべてのサーバのセキュリティ パスワードが一致する必要があります。すべてのマシンのセキュリティ パスワードを変更してください。変更しないと、互いに通信できなくなります。

注意　セキュリティ パスワードを変更した後に、サーバ グループ内の各サーバをリセットする必要があります。サーバの再起動に失敗すると、システム サービスとサブスクライバ サーバの [Cisco ER Administration] ページに問題が発生します。

（注）　この手順中、物理的にシステムにアクセスできるか確認するため、有効な CD または DVD をディスク ドライブから取り出し、再挿入する必要があります。

手順

ステップ 1　次のユーザ名とパスワードを使用してシステムにログインします。

- ユーザ名：**pwrecovery**
- パスワード：**pwreset**

[Welcome to platform password reset] ウィンドウが表示されます。

ステップ 2　任意のキーを押して続行します。

ステップ 3　ディスク ドライブに CD または DVD が入っている場合は、ここで取り出します。

ステップ 4　任意のキーを押して続行します。

CD または DVD がディスク ドライブから取り出してあるかが確認されます。

ステップ 5　有効な CD または DVD をディスク ドライブに挿入します。

（注）　このテストでは、音楽 CD ではなくデータ CD を使用する必要があります。

ディスクを挿入したかが確認されます。

ステップ 6　ディスクが挿入されていることをシステムが確認した後、次のいずれかのオプションを入力して続行するよう要求されます。

- **a** を入力して、管理者パスワードをリセットする。
- **s** を入力して、セキュリティ パスワードをリセットする。
- **q** を入力して、終了する。

ステップ 7　選択したタイプの新しいパスワードを入力します。

ステップ 8　新しいパスワードを再入力します。

パスワードには 6 文字以上が必要です。システムが新しいパスワードの有効性を確認します。パスワードが有効性テストに合格しない場合、新しいパスワードを入力するよう要求されます。

ステップ 9　新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するよう指示されます。

Cisco Unified OS 情報の表示

Cisco Unified OS の管理の Web ページを使用して、オペレーティング システム、プラットフォーム ハードウェア、ネットワークのステータスを表示できます。次のトピックで、この情報の表示方法を説明します。

- 「ServerGroup 情報の表示」（P.7-3）
- 「ハードウェア ステータスの表示」（P.7-4）
- 「ネットワーク ステータスの表示」（P.7-4）
- 「インストールされているソフトウェアの表示」（P.7-4）
- 「システム ステータスの表示」（P.7-4）

ServerGroup 情報の表示

クラスタ情報を表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Cisco Unified OS Administration] Web ページで、[Show]>[ServerGroup] を選択します。

[ServerGroup] ページが表示されます。

ステップ 2　[ServerGroup] ページのフィールドの説明については、表 C-1（P.C-2）を参照してください。

ハードウェア ステータスの表示

ハードウェア ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Cisco Unified OS Administration] Web ページから、[Show]>[Hardware] を選択します。

[Hardware Status] ページが表示されます。

ステップ 2　[Hardware Status] ページのフィールドの説明については、表 C-2（P.C-2）を参照してください。

ネットワーク ステータスの表示

表示されるネットワーク ステータス情報は、ネットワークの耐障害性がイネーブルになっているかどうかによって異なります。ネットワークの耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。ネットワークの耐障害性がイネーブルになっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。ネットワークの耐障害性がイネーブルになっていない場合、イーサネット 0 のステータス情報のみが表示されます。

ネットワーク ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[Network] を選択します。

[Network Settings] ページが表示されます。

ステップ 2　[Network Settings] ページのフィールドの説明については、表 C-3（P.C-3）を参照してください。

インストールされているソフトウェアの表示

ソフトウェア バージョンとインストールされているソフトウェア オプションを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[Software] を選択します。

[Software Packages] ページが表示されます。

ステップ 2　[Software Packages] ページのフィールドの説明については、表 C-4（P.C-4）を参照してください。

システム ステータスの表示

システム ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[System] を選択します。

[System Status] ページが表示されます。

ステップ 2　[System Status] ページのフィールドの説明については、表 C-5（P.C-5）を参照してください。

IP 設定の表示

IP 設定を表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[IP Preference] を選択します。

[IP Preferences] ページが表示されます。

ステップ 2　データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

（注）　検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加した場合、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 3　[Find] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

Cisco Unified OS 設定の表示と変更

IP 設定、ホスト設定、および Network Time Protocol（NTP; ネットワーク タイム プロトコル）設定を表示および変更するには、設定オプションを使用します。次のトピックで、Cisco Unified OS 設定の表示および変更方法について説明します。

- 「時刻設定の設定」（P.7-9）
- 「ソフトウェア バージョンの再起動、シャット ダウン、切り替え」（P.7-10）

イーサネット設定の設定

[Ethernet Settings] オプションで、Dynamic Host Configuration Protocol（DHCP）、ポート、ゲートウェイ情報を表示および変更できます。

[Ethernet Configuration] ページで、DHCP を有効または無効にでき、イーサネット ポートの IP アドレスとサブネットマスクを指定し、ネットワーク ゲートウェイの IP アドレスを指定できます。

（注）　イーサネット設定はすべて Eth0 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルトは 1500 です。

イーサネット設定を表示または変更するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[IP]>[Ethernet] を選択します。

[Ethernet Configuration] ページが表示されます。

ステップ 2　イーサネット設定を変更するには、目的のフィールドに新しい値を入力します。[Ethernet Configuration] ウィンドウのフィールドの説明については、表 C-7（P.C-6）を参照してください。

（注）　DHCP を有効にすると、[Port Information] および [Gateway Information] 設定は無効になり、変更できません。

ステップ 3　変更を保存するには、[Save] をクリックします。

CER サーバの IP アドレスの変更

Cisco ER パブリッシャと Cisco ER サブスクライバのいずれか、または両方の IP アドレスを変更できます。

次のセクションで、Cisco ER サーバで IP アドレスを変更する方法について説明します。

- 「Cisco ER パブリッシャ サーバの IP アドレスの変更」（P.7-6）
- 「Cisco ER サブスクライバ サーバの IP アドレスの変更」（P.7-7）
- 「Cisco ER パブリッシャおよびサブスクライバ サーバ両方の IP アドレスの変更」（P.7-8）

Cisco ER パブリッシャ サーバの IP アドレスの変更

インストール後に Cisco ER パブリッシャの IP アドレスを変更するには、次の手順を実行します。

（注）　サーバの IP アドレスを変更する前に、DNS サーバの IP アドレス情報を更新してください。

1. 次のオプションのいずれかを使用して、Cisco ER パブリッシャの IP アドレスを変更します。
   - Cisco Unified オペレーティング システムの管理の [Settings] > [IP] > [Ethernet] で新しい IP アドレスを入力します。「Ethernet Configuration」（P.C-6）を参照してください。
   - Command-line Interface（CLI; コマンドライン インターフェイス）で、**set network ip** コマンドを使用して新しい IP アドレスを設定します。「set network ip」（P.F-22）を参照してください。
2. Cisco ER パブリッシャを再起動します。
3. Cisco ER パブリッシャが完全に動作したら、Cisco ER サブスクライバで Cisco Unified オペレーティング システムの管理にログインします。
4. [Settings] > [IP] > [Publisher] を選択します。Cisco Unified オペレーティング システムの管理に、パブリッシャの古い IP アドレスが表示されます。[Edit] ボックスにパブリッシャの新しい IP アドレスを入力して [Save] をクリックします。
5. Cisco ER パブリッシャと Cisco ER サブスクライバの通信が維持されるよう、ただちに Cisco ER サブスクライバを再起動します。
6. 「utils dbreplication status」（P.F-57）で説明しているように、utils dbreplication status CLI コマンドを使用して複製を確認します。各サーバの値が 2 と等しくなるようにしてください。
7. CTI ポートが Cisco ER パブリッシャ サーバで登録されているか確認します。CTI ポートが登録されていない場合、ポートを削除し、再度追加して CTI ポートを再作成してください。「必要な CTI ポートの作成」（P.3-8）を参照してください。

Cisco ER サブスクライバ サーバの IP アドレスの変更

インストール後に Cisco ER サブスクライバの IP アドレスを変更するには、次の手順を実行します。

（注）　サーバの IP アドレスを変更する前に、DNS サーバの IP アドレス情報を更新してください。

1. 次のオプションのいずれかを使用して、Cisco ER サブスクライバの IP アドレスを変更します。
   - Cisco Unified オペレーティング システムの管理の [Settings] > [IP] > [Ethernet] で新しい IP アドレスを入力します。「Ethernet Configuration」（P.C-6）を参照してください。
   - Command-line Interface（CLI; コマンドライン インターフェイス）で、**set network ip** コマンドを使用して新しい IP アドレスを設定します。「set network ip」（P.F-22）を参照してください。
2. Cisco ER サブスクライバを再起動します。
3. Cisco ER サブスクライバが完全に動作したら、Cisco ER パブリッシャを再起動します。
4. 「utils dbreplication status」（P.F-57）で説明しているように、utils dbreplication status CLI コマンドを使用して複製を確認します。各サーバの値が 2 と等しくなるようにしてください。

Cisco ER パブリッシャおよびサブスクライバ サーバ両方の IP アドレスの変更

パブリッシャとサブスクライバ両方の IP アドレスを変更する場合、サーバの IP アドレスを続けて変更し、最初にサブスクライバを起動する必要があります。

注意　サブスクライバで IP アドレスの変更作業が完了してから、パブリッシャ サーバの IP アドレスの変更を開始してください。

Cisco ER パブリッシャとサブスクライバの IP アドレスを変更するには、次の手順を実行します。

1. Cisco ER パブリッシャ サーバの IP アドレスの変更方法の詳細は、「Cisco ER パブリッシャ サーバの IP アドレスの変更」（P.7-6）を参照してください。
2. Cisco ER サブスクライバ サーバの IP アドレスの変更方法の詳細は、「Cisco ER サブスクライバ サーバの IP アドレスの変更」（P.7-7）を参照してください。

NTP サーバの設定

外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。外部 NTP サーバの追加、削除、または変更を行うには、次の手順を実行します。

（注）　パブリッシャ上では NTP サーバ設定しか構成することができません。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[NTP Servers] を選択します。

[NTP Server List] ページが表示されます。[NTP Server List] ページの詳細は、「NTP Server List」（P.C-8）を参照してください。

ステップ 2　NTP サーバの追加、削除、または変更ができます。

- NTP サーバを削除するには、当該のサーバの前にあるチェックボックスをオンにしてから [Delete Selected] をクリックします。
- NTP サーバを追加するには、[Add] をクリックします。[NTP Server Configuration] ページが表示されます。ホスト名または IP アドレスを入力して [Save] をクリックします。
- NTP サーバを変更するには、IP アドレスをクリックします。[NTP Server Configuration] ページが表示されます。ホスト名または IP アドレスを変更して [Save] をクリックします。

（注）　NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。NTP サーバを変更した場合は、必ず、ページを更新して正しいステータスを表示する必要があります。

ステップ 3　[NTP Server Settings] ページを更新して正しいステータスを表示するには、[Settings]>[NTP Servers] を選択します。

（注）　NTP サーバの削除、変更、追加が終わったら、変更を有効にするためにパブリッシャとサブスクライバの両方をすべて再起動する必要があります。

SMTP 設定の設定

[SMTP Settings] ウィンドウでは、SMTP ホスト名の表示や設定ができ、SMTP ホストがアクティブであるかどうかが表示されます。

SMTP ホスト設定を行うには、次の手順を実行します。

ヒント　システムから E メールを送信する場合は、SMTP ホストを設定する必要があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[SMTP] を選択します。

[SMTP Settings] ページが表示されます。[SMTP Settings] ページの詳細は、「SMTP Settings」（P.C-9）を参照してください。

ステップ 2　SMTP ホストのホスト名または IP アドレスを入力します。

ステップ 3　[Save] をクリックします。

時刻設定の設定

時刻を手動で設定するには、次の手順を実行します。

（注）　サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。NTP サーバの削除については、「NTP サーバの設定」（P.7-8）を参照してください。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページで、[Settings]>[Time] を選択します。[Time Settings] ページが表示されます。[Time Settings] ページの詳細は、「Time Settings」（P.C-10）を参照してください。

ステップ 2　システムの日付と時刻を入力します。

ステップ 3　[Save] をクリックします。

ソフトウェア バージョンの再起動、シャット ダウン、切り替え

新しいソフトウェア バージョンにアップグレードした場合と古いソフトウェア バージョンに戻す必要がある場合の両方で、このオプションを使用できます。

Cisco ソフトウェア バージョンを再起動、シャットダウン、切り替えるには、次の手順を実行します。

注意　この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[Version] を選択します。[Version Settings] ページが表示されます。[Version Settings] ページの詳細は、「Version Settings」（P.C-10）を参照してください。

ステップ 2　アクティブなパーティションで実行しているバージョンを再起動するには、[Restart] をクリックします。

[Restart] をクリックすると、現在のパーティションのシステムが、バージョンを切り替えずに再起動します。

ステップ 3　システムをシャット ダウンするには、[Shutdown] をクリックします。

[Shutdown] をクリックすると、すべてのプロセスが中断され、システムがシャット ダウンします。

（注）　ハードウェアの電源は自動的には切れません。

注意　サーバの電源ボタンを押すと、システムがただちにシャット ダウンします。

ステップ 4　アクティブ ディスク パーティションで実行中のシステムをシャット ダウンし、その後非アクティブ パーティションのソフトウェア バージョンを使用してシステムを自動的に再起動するには、[Switch Versions] をクリックします。

[Switch Version] をクリックするとシステムが再起動し、現在非アクティブであるパーティションがアクティブになります。

（注）　[Switch Version] ボタンは、非アクティブのパーティションにソフトウェアがインストールされている場合にのみ表示されます。

（注）　新しいソフトウェア バージョンにアップグレードした場合や古いソフトウェア バージョンに戻す必要がある場合に、このオプションを使用できます。

セキュリティの管理

次のトピックで、セキュリティと IPSec 管理の作業を行う方法について説明します。

- 「Internet Explorer のセキュリティ オプションの設定」（P.7-11）

- 「証明書と Certificate Trust List の管理」（P.7-11）
- 「IPSEC 管理」（P.7-17）

Internet Explorer のセキュリティ オプションの設定

サーバから証明書がダウンロードできるよう、Internet Explorer のセキュリティ設定が正しく設定されているか確認するには、次の手順を実行します。

手順

ステップ 1　Internet Explorer を起動します。

ステップ 2　[Tools]>[Internet Options] を選択します。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　[Advanced] タブの [Security] セクションまでスクロール ダウンします。

ステップ 5　必要に応じて、[Do not save encrypted pages to disk] チェックボックスをオフにします。

ステップ 6　[OK] をクリックします。

証明書と Certificate Trust List の管理

次のトピックで、[Certificate Management] メニューを使用して実行できる機能について説明します。

- 「証明書の表示」（P.7-11）
- 「証明書または CTL のダウンロード」（P.7-12）
- 「証明書の削除と再作成」（P.7-12）
- 「証明書または証明書信頼リストのアップロード」（P.7-13）
- 「サード パーティ製の CA 証明書の使用」（P.7-15）
- 「証明書の有効期限日の監視」（P.7-16）

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。

[Certificate List] ページが表示されます。[Certificate List] ページの詳細は、「Certificate List」（P.C-11）を参照してください。

ステップ 2　証明書のリストをフィルタリングするには、[Find] コントロールを使用します。

ステップ 3　証明書または信頼ストアの詳細を表示するには、表示するファイル名をクリックします。

[Certificate Configuration] ページに該当の証明書の情報が表示されます。

ステップ 4　[Certificate List] ページに戻るには、[Related Links] リストで [Back To Find/List] を選択し、[Go] をクリックします。

証明書または CTL のダウンロード

証明書または CTL を Cisco ER からローカル システムにダウンロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。
[Certificate List] ページが表示されます。証明書または CTL のファイル名をクリックします。

ステップ 2　証明書のリストをフィルタリングするには、[Find] コントロールを使用します。

ステップ 3　証明書または CTL のファイル名をクリックします。
[Certificate Configuration] ページが表示されます。

ステップ 4　[Download] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除と再作成

次の各項では、証明書の削除と再作成について説明します。

- 「証明書の削除」（P.7-12）
- 「証明書の再作成」（P.7-13）

証明書の削除

信頼できる証明書を削除するには、次の手順を実行します。

注意　証明書を削除すると、システムの動作に影響する場合があります。[Certificate List] で選択する証明書については、システムから既存の CSR がすべて削除されるため、新しい CSR を生成する必要があります。詳細については、「証明書署名要求の作成」（P.7-15）の手順を参照してください。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2　証明書のリストをフィルタリングするには、[Find] コントロールを使用します。

ステップ 3　証明書または CTL のファイル名をクリックします。
[Certificate Configuration] ページが表示されます。

ステップ 4　[Delete] をクリックします。

証明書の再作成

証明書を再作成するには、次の手順を実行します。

注意　証明書を再作成すると、システムの動作に影響する場合があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Generate New] をクリックします。

[Generate Certificate] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。表示される証明書の名前の説明については、表 7-1 を参照してください。

ステップ 4　[Generate New] をクリックします。

表 7-1　証明書の名前と説明

名前	説明
tomcat	この自己署名ルート証明書は、HTTPS サーバのインストール中に作成されます。
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。

証明書または証明書信頼リストのアップロード

注意　新しい証明書ファイルまたは Certificate Trust List（CTL）ファイルをアップロードすると、システムの動作に影響する場合があります。新しい tomcat 証明書または証明書信頼リストをアップロードした後、CLI コマンドの **utils service restart Cisco Tomcat** を入力して、Cisco Tomcat サービスを再起動する必要があります。

（注）　信頼証明書は他のクラスタ サーバに配布されません。複数のサーバで同じ証明書が必要な場合は、証明書を各サーバに個々にアップロードする必要があります。

次の各項では、CA ルート証明書、アプリケーション証明書、または CTL ファイルをサーバにアップロードする方法について説明します。

- 「証明書のアップロード」（P.7-14）
- 「信頼できる証明書のアップロード」（P.7-14）

証明書のアップロード

CA ルート証明書、アプリケーション証明書、CTL ファイルをサーバにアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Upload Certificate] をクリックします。

[Upload Certificate] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　サード パーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキストボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。

信頼できる証明書のアップロード

信頼できる証明書をアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Upload CTL] をクリックします。

[Upload Certificate Trust List] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　サード パーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキストボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。

サード パーティ製の CA 証明書の使用

Cisco Unified OS は、サード パーティ製の Certificate Authority（CA; 認証局）が PKCS # 10 Certificate Signing Request（CSR; 証明書署名要求）によって発行した証明書をサポートしています。次の表に、このプロセスの概要および参考となる文書を示します。

	作業	参考となる文書
ステップ 1	サーバに CSR を作成する。	「証明書署名要求の作成」（P.7-15）を参照してください。
ステップ 2	CSR を PC にダウンロードする。	「証明書または CTL のダウンロード」（P.7-12）を参照してください。
ステップ 3	CSR を使用して、CA からアプリケーション証明書を取得する。	アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」（P.7-16）を参照してください。
ステップ 4	CA ルート証明書を取得する。	ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」（P.7-16）を参照してください。
ステップ 5	CA ルート証明書をサーバにアップロードする。	「証明書または証明書信頼リストのアップロード」（P.7-13）を参照してください。
ステップ 6	アプリケーション証明書をサーバにアップロードする。	「証明書または証明書信頼リストのアップロード」（P.7-13）を参照してください。
ステップ 7	新しい証明書に影響されるサービスを再起動する。	すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat の証明書を更新した場合は Tomcat サービスを再起動します）。さらに、CAPF または Cisco Unified CM の証明書を更新した場合は、TFTP サービスも再起動します。 サービスの再起動の詳細については、「Control Center の使用」（P.6-1）を参照してください。

証明書署名要求の作成

Certificate Signing Request（CSR; 証明書署名要求）を作成するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Generate CSR] をクリックします。

[Generate Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

証明書署名要求をダウンロードするには、次の手順を実行します。

ステップ 4　[Generate CSR] をクリックします。

証明書署名要求のダウンロード

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Download CSR] をクリックします。

[Download Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　[Download CSR] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

サードパーティ製の CA 証明書の取得

サード パーティの CA が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA から取得する必要があります。これらの証明書の取得に関する情報は、CA から入手してください。入手の手順は、CA によって異なります。

CAPF および Cisco ER の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、CSR 作成プロセスの最後のページに表示される X.509 拡張を有効にする必要があります。

Cisco Unified OS では、証明書は DER および PEM 符号化フォーマットで、CSR は PEM 符号化フォーマットで作成されます。また、DER および DER 符号化フォーマットの証明書を受け入れます。

証明書の有効期限日の監視

証明書の有効期限日が近づいたときに、システムから自動的に E メールを送信できます。

Certificate Expiry Monitor の表示と設定をするには、次の手順を実行します。

（注）　[Certificate Expiration Monitor] ページの情報を更新するには、Cisco Certificate Expiry Monitor サービスが実行している必要があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Monitor] を選択します。

[Certificate Monitor] ページが表示されます。

ステップ 2　必要な設定情報を入力します。[Certificate Monitor Expiration] フィールドの説明については、表 C-21（P.C-15）を参照してください。

ステップ 3　変更内容を保存するには、[Save] をクリックします。

IPSEC 管理

次のトピックで、IPSec の管理方法について説明します。

- 「既存の IPSec ポリシーの表示または変更」（P.7-17）
- 「新しい IPSec ポリシーの設定」（P.7-17）

（注） IPSec は、インストール中にサーバ グループのサーバ間で自動的に設定されるわけではありません。

既存の IPSec ポリシーの表示または変更

既存の IPSec ポリシーを表示または変更するには、次の手順を実行します。

（注） システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。

注意 IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[IPSEC Configuration] を選択します。

[IPSEC Policy Configuration] ページが表示されます。

注意 既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

ステップ 2　[Display Detail] リンクをクリックします。[Association Details] ページが表示されます。このページのフィールドの説明については、表 C-23（P.C-16）を参照してください。

新しい IPSec ポリシーの設定

新しい IPSec ポリシーとアソシエーションを設定するには、次の手順を実行します。

（注） システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。

注意 IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[IPSEC Configuration] を選択します。

[IPSEC Policy List] ページが表示されます。

ステップ 2　[Add New] をクリックします。

[IPSEC Policy Configuration] ページが表示されます。

ステップ 3　[Next] をクリックします。

[Setup IPSEC Policy and Association] ページが表示されます。

ステップ 4　[IPSEC Policy Configuration] ページに適切な情報を入力します。このページのフィールドの説明については、表 C-23（P.C-16）を参照してください。

ステップ 5　新しい IPSec ポリシーを設定するには、[Save] をクリックします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、イネーブル/ディセーブル、または削除するには、次の手順を実行します。

（注）　システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを作成したり変更したりしないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

注意　既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1　[Security] > [IPSEC Configuration] を選択します。

（注）　[Security] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications Operating System の管理に再ログインする必要があります。

[IPSEC Policy List] ウィンドウが表示されます。

ステップ 2　ポリシーを表示、イネーブル、またはディセーブルにするには、次の手順を実行します。

a.　ポリシー名をクリックします。

[IPSEC Policy Configuration] ウィンドウが表示されます。

b.　ポリシーをイネーブルまたはディセーブルにするには、[Enable Policy] チェックボックスを使用します。

c.　[Save] をクリックします。

ステップ 3　1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a.　削除するポリシーの隣にあるチェックボックスをオンにします。

[Select All] をクリックしてすべてのポリシーを選択することも、[Clear All] をクリックしてすべてのチェックボックスをオフにすることもできます。

b. [Delete Selected] をクリックします。

ソフトウェア アップグレードの実行

次のトピックで、ソフトウェア アップグレードの実行方法について説明します。

ソフトウェアのアップグレードとインストール

システムの動作中に、サーバにアップグレード ソフトウェアをインストールできます。システムにはアクティブで起動可能なパーティションと、非アクティブで起動可能なパーティションの 2 つのパーティションがあります。システムのブートと動作はすべてアクティブ パーティションとしてマークされているパーティションで実行されます。

アップグレード ソフトウェアをインストールする場合は、アクティブでないパーティションにインストールします。ソフトウェアのインストール中もシステムは通常通り動作します。準備ができたら、非アクティブ パーティションをアクティブにして、アップグレードしたソフトウェアでシステムをリブートします。現在アクティブなパーティションは、システムの再起動後に非アクティブ パーティションとして認識されます。現在のソフトウェアは、次のアップグレードまで、非アクティブのパーティションに保持されます。設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

[Software Upgrade] ページで、Cisco ER ソフトウェアをローカルまたはリモート ソースのいずれかからアップグレードできます。

ソフトウェア アップグレードの手順で、問題が発生した場合にアップグレードを取り消すこともできます。システムの非アクティブなパーティションにアップグレード用のソフトウェアをインストールし、再起動してシステムを新しいバージョンのソフトウェアに切り替えます。この処理で、アップグレードされたソフトウェアがアクティブなパーティションになり、現在のソフトウェアが非アクティブなパーティションになります。設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

何らかの理由でアップグレードから元の状態に戻す場合、ソフトウェアの以前のバージョンがある非アクティブ パーティションでシステムを再起動できます。しかし、ソフトウェアのアップグレード後に行った設定の変更はすべて失われます。

（注） Cisco ER 8.5 から新しいバージョンにアップグレードする場合、パブリッシャを最初にアップグレードし、次にサブスクライバをアップグレードする必要があります。

アップグレード ファイルの取得

アップグレード プロセスを開始する前に、適切なアップグレード ファイルを Cisco.com から取得する必要があります。詳細は、該当する『Cisco ER Release Notes』の「Installation and Upgrade」の項を参照してください。

（注） インストールする前に、パッチ ファイルの名前を変更しないでください。システムでそれが有効なファイルだと認識されなくなります。

（注）　ファイルを解凍または展開しないでください。解凍や展開をすると、アップグレード ファイルを読み込めなくなる場合があります。

インストール プロセス中も、アップグレード ファイルにはローカル DVD かリモートの FTP または SFTP サーバからアクセスできます。アップグレード ファイルにアクセスする際に入力するディレクトリ名とファイル名は、大文字と小文字が区別されるため、注意してください。

ローカル ソースからのインストールとアップグレード

ローカル ディスク ドライブにセットした DVD からソフトウェアをインストールしてアップグレード処理を開始できます。

（注）　ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。詳細については、「Cisco Emergency Responder 8.5 Disaster Recovery System の設定」の章を参照してください。

ソフトウェアを DVD からインストールまたはアップグレードするには、次の手順を実行します。

手順

ステップ 1　適切なアップグレード ファイルを Cisco.com からダウンロードします。

ステップ 2　DVD を焼くための .iso ファイルを使用して DVD を作成します。.iso ファイルには、元の DVD ディスクの完全なイメージが含まれます。DVD に .iso ファイルをコピーしただけでは、正しく動作しません。DVD 作成ソフトウェアを使用して、イメージに含まれているファイルを解凍し、それを DVD に焼く必要があります。これにより、DVD ディスクの正確な複製が作成されます。

ステップ 3　DVD をアップグレードするローカル サーバのディスク ドライブに挿入します。

ステップ 4　[Cisco Unified OS Administration] Web ページから、[Software Upgrades]>[Install/Upgrade] を選択します。

[Software Installation/Upgrade] ページが表示されます。

ステップ 5　[Source] リストから [DVD/CD] を選択します。

ステップ 6　[Directory] フィールドに、DVD のパッチファイルのパスを入力します。

ファイルがルート ディレクトリにある場合は、スラッシュ（/）を入力します。

ステップ 7　[Next] をクリックしてアップグレード プロセスを続行します。

ステップ 8　インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 9　次のページで、ダウンロードの進捗を確認します。この進捗には、転送中のファイル名とメガバイト数が表示されます。

ステップ 10　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Reboot to upgraded partition] を選択します。システムが再起動され、アップグレードされたソフトウェアが起動されます。

ステップ 11　アップグレードをインストールして、後でアップグレードされたパーティションに手動で再起動するには、次のいずれかの手順を実行します。

a.　[Do not reboot after upgrade] を選択します。

b.　[Next] をクリックします。

[Upgrade Status] ウィンドウにアップグレード ログが表示されます。

c. インストールが完了したら、[Finish] をクリックします。

d. システムを再起動して、アップグレードをアクティブにするには、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

システムが再起動され、アップグレードされたソフトウェアが起動されます。

リモート ソースからのインストールとアップグレード

ソフトウェアをネットワーク ドライブまたはリモート サーバからインストールするには、次の手順を実行します。

（注） ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。詳細については、「Cisco Emergency Responder 8.5 Disaster Recovery System の設定」の章を参照してください。

（注） Cisco Unified オペレーティング システムの管理にアクセスしている間は、ブラウザの制御機能（表示の更新や再読み込みなど）を使用しないでください。代わりに、インターフェイスに用意されているナビゲーション制御を使用します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Software Upgrades]>[Install/Upgrade] を選択します。

[Software Installation/Upgrade] ページが表示されます。

ステップ 2　[Source] リストから [Remote Filesystem] を選択します。

ステップ 3　[Directory] フィールドに、リモート システムのパッチファイルのパスを入力します。

アップグレード ファイルが Linux または UNIX サーバ上にある場合は、ディレクトリ パスの先頭にフォワード スラッシュを入力する必要があります。たとえば、アップグレード ファイルが patches ディレクトリにあるにある場合は、**/patches** と入力する必要があります。

アップグレード ファイルが Windows サーバ上に配置されている場合は、FTP サーバまたは SFTP サーバに接続することになるため、次のような適切な構文を使用するよう注意してください。

- パスの記述はフォワード スラッシュ（/）で開始し、パスの区切り文字には常にフォワード スラッシュを使用します。
- パスの先頭部分は、サーバ上の FTP または SFTP ルート ディレクトリにする必要があります。したがって、C: などのドライブ文字で開始される Windows 絶対パスは入力できません。

ステップ 4　[Server] フィールドにサーバ名を入力します。

ステップ 5　[User Name] フィールドにユーザ名を入力します。

ステップ 6　[User Password] フィールドにパスワードを入力します。

ステップ 7　[Transfer Protocol] フィールドで、転送プロトコルを選択します。

ステップ 8　[Next] をクリックしてアップグレード プロセスを続行します。

ステップ 9　インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 10　次のページで、ダウンロードの進捗を確認します。この進捗には、転送中のファイル名とメガバイト数が表示されます。

ステップ 11　ダウンロードが完了したら、ダウンロードしたファイルのチェックサム値と、Cisco.com に表示されているチェックサム値を確認します。

注意　アップグレード ファイルの認証と整合性を保証するため、2 つのチェックサム値は一致している必要があります。チェックサム値が一致しない場合、Cisco.com から新しいバージョンのファイルをダウンロードして、再度アップグレードを試みてください。

（注）　アップグレード プロセスの進行中にサーバとの接続を失った場合、またはブラウザを閉じた場合は、[Software Upgrades] メニューに再度アクセスしようとすると、次のメッセージが表示されることがあります。

Warning: Another session is installing software, click Assume Control to take over the installation.

セッションを引き継ぐ場合は、[Assume Control] をクリックします。

[Assume Control] が表示されない場合は、Real Time Monitoring Tool でアップグレードを監視することもできます。

ステップ 12　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Reboot to upgraded partition] を選択します。システムが再起動され、アップグレードされたソフトウェアが起動されます。

ステップ 13　アップグレードをインストールして、後でアップグレードされたパーティションに手動で再起動するには、次のいずれかの手順を実行します。

a. [Do not reboot after upgrade] を選択します。

b. [Next] をクリックします。

[Upgrade Status] ウィンドウにアップグレード ログが表示されます。

c. インストールが完了したら、[Finish] をクリックします。

d. システムを再起動して、アップグレードをアクティブにするには、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

システムが再起動され、アップグレードされたソフトウェアが起動されます。

アップグレードの途中停止

アップグレード ソフトウェアのインストール中に、アップグレードが途中停止したように見える場合があります。アップグレード ログには新しいログ メッセージが表示されなくなります。アップグレードが途中停止した場合は、アップグレードをキャンセルし、I/O スロットリングを無効にして、アップグレード手順を初めからやり直す必要があります。正常にアップグレードが完了した場合は、I/O スロットリングを再度有効にする必要はありません。

I/O スロットリングを無効にするには、CLI コマンドの **utils iothrottle disable** を入力します。

I/O スロットリングのステータスを表示するには、CLI コマンドの **utils iothrottle status** を入力します。

I/O スロットリングを有効にするには、CLI コマンドの **utils iothrottle enable** を入力します。デフォルトでは、iothrottle は有効になっています。

システムがキャンセルに応答しない場合、サーバを再起動し、I/O スロットリングを無効にし、アップグレード処理の手順を再度開始してください。

以前のバージョンへの復帰

アップグレード後、ソフトウェア バージョンをアップグレードの実行前に戻すことができます。システムを再起動し、次の作業を実行して非アクティブなパーティションのソフトウェア バージョンに切り替えます。

	作業	詳細情報の参照先
1.	パブリッシャ ノードを以前のバージョンに戻します。	「パブリッシャ サーバの以前のバージョンへの復帰」（P.7-23）
2.	すべてのバックアップ サブスクライバ ノードを以前のバージョンに戻します。	「サブスクライバ サーバの以前のバージョンへの復帰」（P.7-24）

パブリッシャ サーバの以前のバージョンへの復帰

パブリッシャ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications Operating System の管理を表示します。

https://*server-name*/**cmplatform**

server-name は、Cisco ER サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　[Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[Switch Versions] ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a.　開いている Cisco Unified Communications Operating System の管理に再度ログインします。

b.　[Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

c.　アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d.　アクティブにしたサービスがすべて動作していることを確認します。

e.　次の URL を入力し、ユーザ名とパスワードを入力して Cisco ER にログインします。

https://*server-name*/**ccmadmin**

f. ログインできること、および設定データが存在することを確認します。

サブスクライバ サーバの以前のバージョンへの復帰

サブスクライバ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications Operating System の管理を表示します。

https://*server-name*/**cmplatform**

server-name は、Cisco ER サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　[Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[Switch Versions] ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a. 開いている Cisco Unified Communications Operating System の管理に再度ログインします。

b. [Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

c. アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d. アクティブにしたサービスがすべて動作していることを確認します。

ブリッジ アップグレード

ブリッジ アップグレードは、製造中止されたサーバから CER-8.5(1) をサポートするサーバに移行するユーザに移行パスを提供します。

サポートが中止されたサーバは、ブリッジ アップグレード サーバとして機能することが許可され、アップグレードおよび起動できますが、Cisco Emergency Responder は正しく機能しません。

CER-8.5(1) に正常にアップグレードすると、コンソールに、新しいバージョンの Cisco Emergency Responder では DRS バックアップのみしかできないことを通知する警告が表示されます （この警告は、CLI と GUI セッションの両方に表示されます)。

ステップ 1　製造中止されたサーバで CER-8.5(1) バージョンにアップグレードします。

ステップ 2　製造中止されたサーバにある新しい CER バージョンを使用して、DRS バックアップを実行します。

（注） Cisco Emergency Responder および Cisco Phone Tracking エンジンは、製造中止されたサーバでのブリッジ アップグレード後は、使用可能として表示されません。

ステップ 3　新しいサポートされているサーバに、CER-8.5(1) バージョンを、製造中止されたサーバと同じホスト名でインストールします。

ステップ 4　CER-8.5(1) を実行している新しくサポートされたサーバで、最初のノードで DRS の復元を実行します。

（注）　ブリッジ アップグレード可能なサーバの一覧については、『Cisco ER 8.5(1) Release Notes』を参照してください。

カスタマイズされたログオン メッセージ

Cisco Unified Communications オペレーティング システムの管理、Cisco Unified CM の管理、コマンド ライン インターフェイスに表示するカスタマイズされたログオン メッセージを含むテキスト ファイルをアップロードできます。

カスタマイズされたログオン メッセージをアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Upgrades] > [Customized Logon Message] の順に選択します。

[Customized Logon Message] ウィンドウが表示されます。

ステップ 2　アップロードするテキスト ファイルを選択して、[Browse] をクリックします。

ステップ 3　[Upload File] をクリックします。

（注）　アップロードできるファイルは 10KB 以内です。

システムにカスタマイズされたログオン メッセージが表示されます。

ステップ 4　デフォルトのログオン メッセージに戻すには、[Delete] をクリックします。

カスタマイズされたログオン メッセージが削除され、システムにデフォルトのログオン メッセージが表示されます。

Cisco Unified OS のサービスの使用

次のトピックで、Cisco Unified OS のサービスの使用方法を説明します。

- 「ping ユーティリティの使用」（P.7-25）
- 「リモート サポートの設定」（P.7-26）

ping ユーティリティの使用

[Ping Configuration] ページで、他のシステムがネットワーク経由でアクセスできるかを確認するため、ping 要求を送信できます。

他のシステムに ping を送信するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Services]>[Ping] を選択します。

[Ping Configuration] ページが表示されます。[Ping Configuration] ページの詳細は、「Ping Configuration」（P.C-19）を参照してください。

ステップ 2　ping の送信先となるシステムの IP アドレスまたはネットワーク名を入力します。

ステップ 3　ping 間隔を秒で入力します。

ステップ 4　パケット サイズを入力します。

ステップ 5　ping 回数（システムに ping を送信する回数）を入力します。

（注）　複数回の ping を指定した場合は、**ping** コマンドを入力してもリアルタイムでは ping の日時が表示されません。**ping** コマンドがデータを表示するのは、指定した回数だけ ping を送信した後です。

ステップ 6　IPSec を検証するかどうかを選択します。

ステップ 7　[Ping] をクリックします。

[Ping Results] テキスト ボックスに ping の統計情報が表示されます。

リモート サポートの設定

[Remote Support] ページで、シスコのサポート担当者が指定日時に Cisco ER システムにアクセスできるようにするためのリモート アカウントを設定できます。

リモート サポート処理が次のように動作します。

1. ユーザがリモート サポート アカウントを設定します。このアカウントには、シスコの担当者がアクセスできる、設定可能な制限時間が含まれます。
2. リモート サポート アカウントの設定が完了すると、パス フレーズが生成されます。
3. ユーザはシスコのサポートに電話し、リモート サポート アカウント名とパス フレーズを伝えます。
4. シスコのサポート担当者はパスフレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。
5. シスコのサポート担当者はデコードしたパスワードを使用して、お客様のシステムにリモート サポート アカウントでログインします。
6. アカウントの制限時間が経過すると、シスコのサポート担当者はリモート サポート アカウントにアクセスできなくなります。

リモート サポートを設定するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Services]>[Remote Support] を選択します。

[Remote Access Configuration] ページが表示されます。

ステップ 2　リモート サポート アカウントが設定されていない場合、[Add] をクリックします。

ステップ 3　リモート アカウントのアカウント名と、アカウントの期限を、日単位で入力します。

（注）　アカウント名の長さが 6 文字以上で、すべて小文字のアルファベットであることを確認します。

ステップ 4　[Save] をクリックします。

[Remote Access Configuration] ページが再度表示されます。[Remote Access Configuration] ページのフィールドの説明については、表 C-27（P.C-21）を参照してください。

ステップ 5　生成されたパス フレーズを使用してシステムにアクセスする方法については、シスコの担当者にお問い合わせください。