CHAPTER 1

Cisco CP Express ウィザード

ここでは、Cisco Configuration Professional Express（Cisco CP Express）ウィザードについて紹介し、このウィザードで実行可能な設定と各 Cisco CP Express 画面に必要な情報について説明します。

この章の内容は、次のとおりです。

Cisco CP Express を使用する前に

Cisco CP Express ウィンドウがルータの初期設定を誘導します。
Cisco CP Express を使用すれば、ルータに対して次の設定を行うことができます。

- Local Area Network（LAN; ローカル エリア ネットワーク）設定
- DHCP サーバ設定
- Wide Area Network（WAN; ワイドエリア ネットワーク）
- ファイアウォール
- セキュリティ設定
- ルータ プロビジョニング

Cisco CP Express ウィザードを完了して、ルータに設定を配信したら、必要に応じて、Cisco CP Express で設定を変更できます。

Cisco CP Express インターフェイス

Cisco CP Express には 3 種類のウィンドウがあります。

- [概要（Overview）] 画面：このウィンドウには、基本的なルータ情報のスナップショットが表示され、設定画面に移動しなくても、その場で情報を確認できます。
- ウィザード画面：Cisco CP Express を初めて起動すると、ウィザード画面が表示されます。この画面は、ルータ設定の必須部分を誘導して、ルータがネットワーク上で機能できるようにします。ルータとそれが接続されている LAN を保護するために、ファイアウォールとセキュリティの設定が含まれています。各画面の左ペインに、実行中の設定部分が表示されます。右ペインには、設定フィールドが表示されます。画面の詳細を確認する場合は、画面上部の疑問符（?）アイコンをクリックしてください。
- 編集画面：初期設定が完了したら、Cisco CP Express に戻って、必要に応じて、ルータ設定を変更できます。

Cisco CP Express と CCP

Cisco CP Express を使用すれば、ルータがネットワーク上で機能するために欠かせない設定を実行できます。Cisco Configuration Professional（Cisco CP）を使用すれば、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）設定、Intrusion Prevention System（IPS; 侵入防御システム）設定、ネットワークなどのより詳細な設定をルータ上で実行できます。PC 上に Cisco CP がインストールされている場合は、それを起動して設定するルータの IP アドレスを入力できます。

画面について

次のトピックで、ルータ情報を表示したり、Cisco CP Express を起動したりしたときに使用する画面とダイアログボックスについて説明します。

- ウェルカム
- 概要

ウェルカム

このウィザードは、次のような操作を支援する基本設定を誘導します。

- ルータ名を指定する。
- ユーザ名とパスワードを指定する。
- Cisco CP Express ウィザードを使用して手動でルータを設定することも、USB トークンまたは USB フラッシュ デバイスからロードされたコンフィギュレーション ファイル、Secure Device Provisioning（SDP）、または Cisco Network Services（ご使用の Cisco IOS リリースでサポートされている場合）を使用して、ルータをプロビジョニングすることもできます。

  Cisco Network Services を使用してルータを設定する場合は、ルータが Cisco Network Services サーバに接続して設定を取得できるように Cisco Network Services パラメータを入力できます。
- 工場出荷時設定の LAN IP アドレスを変更する。

  ルータのプロビジョニング用として SDP または Cisco Network Services が選択されている場合は、このタスクが省略されます。

- LAN 用の DHCP アドレス プールを作成する。

  ルータのプロビジョニング用として SDP または Cisco Network Services が選択されている場合は、このタスクが省略されます。

- DNS サーバと組織のドメイン名を特定する。この情報については、ネットワーク管理者またはインターネット サービス プロバイダーにお問い合わせください。

  ルータのプロビジョニング用として SDP または Cisco Network Services が選択されている場合は、このタスクが省略されます。

- WAN 接続を構築する。
- LAN および WAN 接続用のファイアウォールを構築する。
- ネットワークのセキュリティとパフォーマンスを向上させる設定を実行する。

追加のインターフェイスを設定したり、より詳細な設定を実行したりするには、Cisco CP を使用します。詳細については、「Cisco Configuration Professional」を参照してください。

ルータの基本設定

基本設定では、ルータ名を指定したり、ユーザ アカウントとパスワードを作成したり、Enable Secret パスワードを作成したりします。詳細については、次の項を参照してください。

基本設定について

次のトピックで、[基本設定（Basic Configuration）] 画面について説明します。

基本設定（Basic Configuration）

[基本設定（Basic Configuration）] ウィンドウでは、設定中のルータに名前を付けたり、組織のドメイン名を入力したり、Cisco CP Express、Cisco Configuration Professional（Cisco CP）、および CLI へのアクセスを制御したりできます。

ホスト名（Hostname）

ルータの名前を入力します。

ドメイン名（Domain Name）

組織のドメイン名を入力します。*cisco.com* はドメイン名の例ですが、サフィクスが *.org* や *.net* などのドメイン名もあります。

ユーザ名とパスワード

Cisco CP Express ユーザと Telnet ユーザ用のユーザ名とパスワードを設定する必要があります。

（注）　このウィンドウで設定したユーザ名とパスワードは、それを変更しないかぎり、次回以降に Cisco CP Express を起動したときに使用します。パスワードは推測されにくく、覚えやすいものにします。

ユーザ名（Username）

ユーザ名を入力します。

新しいパスワードの入力（Enter New Password）

新しいパスワードを入力します。パスワードは 6 文字以上にする必要があります。

新しいパスワードの再入力（Reenter New Password）

確認のために新しいパスワードを再入力します。

Enable Secret パスワード（Enable Secret Password）

Enable Secret パスワードは、Telnet またはコンソール ポート経由でルータにアクセスしているユーザの特権 EXEC モードへのアクセスを制御します。特権 EXEC モードでは、ユーザが設定を変更したり、このモード以外では使用できないコマンドにアクセスしたりできます。[新しいパスワードの入力（Enter Password）] フィールドに Enable Secret パスワードを入力して、確認のために同じパスワードを [新しいパスワードの再入力（Reenter Password）] フィールドに再入力する必要があります。パスワードは 6 文字以上にする必要があります。

（注）　あなたにとっては覚えやすいが、他人にとっては推測しにくい Enable Secret パスワードを選択してください。このパスワードは暗号化形式で保存されるため、コンフィギュレーション ファイルを表示しても読み取ることはできません。

ルータのプロビジョニング

Cisco CP Express を使用すれば、ネットワーク サーバまたは USB フラッシュ デバイス/トークンからコンフィギュレーション ファイルを取り出して、ルータのメモリにロードできます。

次のトピックで、Cisco CP Express のプロビジョニング画面について説明します。

- ルータ プロビジョニング（Router Provisioning）
- USB トークンからのプロビジョニング（Provision From USB Token）
- USB フラッシュからのプロビジョニング（Provision From USB Flash）
- ファイルの選択（File Selection）
- CNS サーバ情報（CNS Server Information）

ルータ プロビジョニング（Router Provisioning）

このウィンドウには、ルータのプロビジョニングに使用可能なオプションが一覧表示されます。これらのオプションの一部は、ご使用の Cisco IOS リリースでサポートされている場合にのみ表示されます。

Cisco CP Express

このオプションは、Cisco CP Express を使用してルータを手動でプロビジョニングする場合に選択します。

USB トークン（USB Token）/USB フラッシュ（USB Flash）

このオプションは、USB トークンまたは USB フラッシュ デバイスがルータに接続されており、それに該当するコンフィギュレーション ファイルが保存されている場合に選択します。

（注）　USB トークンと USB フラッシュ デバイスの両方がルータに接続されている場合は、Cisco CP Express で USB トークンが使用されます。ルータに接続された USB フラッシュ デバイスを使用する場合は、Cisco CP Express を起動する前に、すべての USB トークンをルータから取り外す必要があります。

Secure Device Provisioning（Secure Device Provisioning）

ネットワーク管理者から SDP を使用したルータのプロビジョニングに関する情報が提供されている場合は、[Secure Device Provisioning（Secure Device Provisioning）] を選択します。

SDP オプションを選択する前に、次の内容を確認してください。

- ルータと SDP サーバが IP 接続されている。
- Web ブラウザが JavaScript をサポートしている。

SDP を選択した場合は、Cisco CP Express ウィザードの完了後に、新しいブラウザ ウィンドウが自動的に開きます。新しいブラウザ ウィンドウには、SDP を使用したルータのプロビジョニングを誘導するウィザードが表示されます。

SDP の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

CNS サーバ（CNS Server）

サービス プロバイダーから Cisco Network Services サーバ情報が提供されている場合は、このオプションを選択します。詳細については、「Cisco Network Services」をクリックしてください。

USB トークンからのプロビジョニング（Provision From USB Token）

このウィンドウを使用すれば、ルータに接続された USB トークンからロードされた CCCD コンフィギュレーション ファイルを使用してルータをプロビジョニングできます。CCCD ファイルは、TMS ソフトウェアを使用して USB トークン上にロード可能なブート コンフィギュレーション ファイルです。

（注） このウィンドウは、USB トークンがルータに接続されている場合にのみ表示されます。USB トークンと USB フラッシュ デバイスの両方がルータに接続されている場合は、Cisco CP Express で USB トークンが使用されます。ルータに接続された USB フラッシュ デバイスを使用する場合は、Cisco CP Express を起動する前に、すべての USB トークンをルータから取り外す必要があります。

CCCD コンフィギュレーション ファイルを使用してルータをプロビジョニングした場合は、そのファイルが実行コンフィギュレーションとマージされ、スタートアップ コンフィギュレーションの一部にもなります。

注意 Cisco CP は、ルータのプロビジョニングに使用されるコンフィギュレーション ファイルの妥当性をチェックしません。使用するコンフィギュレーション ファイルに適切な設定が保存されていることを確認してください。

USB トークンからルータをプロビジョニングするには、次の手順を実行します。

ステップ 1　[トークン名（Token Name）] ドロップダウン メニューから、USB トークンを選択します。

ステップ 2　デフォルトの PIN を使用して USB トークンにログイン*しない*場合は、[デバイスと PIN を指定（Specify device and PIN）] を選択して、[トークンの PIN（Token PIN）] フィールドに PIN を入力します。

[デバイスとデフォルト PIN を指定（Specify device and default PIN）] を選択した場合は、デフォルト PIN の 1234567890 が USB トークンのログインに使用されます。

ステップ 3　[ログイン（Login）] をクリックして、USB トークンにログインします。

USB トークンにログインできなければ、USB トークンからルータをプロビジョニングすることができません。[戻る（Back）] ボタンをクリックして、ルータをプロビジョニングする別の方法を選択します。

ステップ 4　[CCCD のプレビュー（Preview CCCD）] をクリックして、下側のペインにファイルの内容を表示します。

USB フラッシュからのプロビジョニング（Provision From USB Flash）

このウィンドウを使用すれば、ルータに接続された USB フラッシュ デバイスからロードされたコンフィギュレーション ファイルを使用して、ルータをプロビジョニングできます。このウィンドウは、USB フラッシュ デバイスがルータに接続されている場合にのみ表示されます。

コンフィギュレーション ファイルを使用してルータをプロビジョニングした場合は、そのファイルが実行コンフィギュレーションとマージされ、スタートアップ コンフィギュレーションの一部にもなります。

注意　Cisco CP は、ルータのプロビジョニングに使用されるコンフィギュレーション ファイルの妥当性をチェックしません。使用するコンフィギュレーション ファイルに適切なデータが保存されていることを確認してください。

USB フラッシュ デバイスからルータをプロビジョニングするには、次の手順を実行します。

ステップ 1　[ファイル名（File Name）] フィールドにコンフィギュレーション ファイルの名前をフル パスで入力するか、[参照（Browse）] をクリックして選択ウィンドウを開きます。

ファイルに拡張子の .cfg を付けるか、ファイル名を CCCD ファイルにする必要があります。CCCD ファイルはブート コンフィギュレーション ファイルです。

ステップ 2　[ファイルのプレビュー（Preview File）] をクリックして、下側のペインにファイルの内容を表示します。

ファイルの選択（File Selection）

このウィンドウを使用すれば、ルータからファイルをロードできます。DOSFS ファイル システム以外はこのウィンドウに表示できません。

ウィンドウの左側には、Cisco ルータ フラッシュ メモリと、ルータに接続された USB デバイス上のディレクトリ システムを示す展開可能なツリーが表示されます。

ウィンドウの右側には、ウィンドウの左側で指定されたディレクトリで見つかったファイルとディレクトリの名前が一覧表示されます。また、各ファイルのバイト単位のサイズと、各ファイルとディレクトリが最後に修正された日付と時刻も表示されます。

ウィンドウの右側のリストでロードするファイルを選択できます。ファイル リストの下は、指定されたファイルのフル パスを含む [ファイル名（Filename）] フィールドです。

（注）　ルータをプロビジョニングするコンフィギュレーション ファイルを選択している場合は、ファイルを CCCD ファイルにするか、.cfg という拡張子を付ける必要があります。

名前（Name）

[名前（Name）] をクリックすると、名前に基づいてファイルとディレクトリがアルファベット順に並べ替えられます。再度 [名前（Name）] をクリックすると、順序が反転します。

サイズ（Size）

[サイズ（Size）] をクリックすると、ファイルとディレクトリがサイズ順に並べ替えられます。ディレクトリは、それが空でない場合でも、必ず、0 のサイズが割り当てられます。再度 [サイズ（Size）] をクリックすると、順序が反転します。

修正時刻（Time Modified）

[修正時刻（Time Modified）] をクリックすると、修正日時に基づいてファイルとディレクトリが並べ替えられます。再度 [修正時刻（Time Modified）] をクリックすると、順序が反転します。

CNS サーバ情報（CNS Server Information）

このウィンドウは、WAN 接続の設定が完了し、Cisco Network Services オプションを使用してルータをプロビジョニングすることにした場合に表示されます。このウィンドウでは、サービス プロバイダーから提供された Cisco Network Services サーバ情報を入力できます。Cisco Network Services サーバの IP アドレスとログイン情報を入力して、Cisco CP Express がルータに関する情報を取り出せるようにします。

CNS サーバの IP アドレス / ホスト名の入力（Enter the CNS Server IP Address /Hostname）

ネットワーク上の Cisco Network Services サーバの IP アドレスとホスト名のどちらかを入力する必要があります。ホスト名を入力した場合は、ホスト名を IP アドレスに解決可能な DNS サーバの IP アドレスを入力する必要があります。

CNS ID 文字列の入力（Enter the CNS ID String）

Cisco Network Services サーバからコンフィギュレーション ファイルを取得するためのデバイス ID を入力する必要があります。

CNS パスワードの入力（Enter the CNS Password）

上で入力したユーザ ID と一緒に Cisco Network Services サーバへのログインに使用するパスワードを入力します。

プライマリ DNS（Primary DNS）

ルータで使用されるプライマリ Domain Name Server（DNS; ドメイン ネーム サーバ）の IP アドレスを入力します。この IP アドレスは、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。

プライマリ DNS サーバは、ルータが IP アドレスを解決しようとして最初にアクセスするサーバです。

（注）　[CNS サーバの IP アドレス/ホスト名の入力（Enter the CNS Server IP Address /Hostname）] フィールドに Cisco Network Services サーバを特定するホスト名を入力した場合は、[プライマリ DNS（Primary DNS）] フィールドに DNS サーバの IP アドレスを入力する必要があります。

セカンダリ DNS（Secondary DNS）

ルータで使用されるセカンダリ ドメイン ネーム サーバの IP アドレスを入力します（使用可能な場合）。この IP アドレスは、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。

セカンダリ DNS サーバは、プライマリ サーバが使用できない場合にルータからアクセスされるサーバです。

ワイヤレス インターフェイスの設定

Cisco CP Express を使用すれば、ルータのワイヤレス インターフェイスとルータの LAN インターフェイスをブリッジできます。加えて、Cisco CP Express からワイヤレス管理アプリケーションを起動できます。

次のトピックで、[ワイヤレス インターフェイスの設定（Wireless Interface Configuration）] 画面について説明します。

- ワイヤレス インターフェイスの設定（Wireless Interface Configuration）

ワイヤレス インターフェイスの設定（Wireless Interface Configuration）

ルータのワイヤレス インターフェイスを設定するには、[はい（Yes）] をクリックします。Cisco CP Express は、ワイヤレス トラフィックを LAN インターフェイスにブリッジするようにルータを設定します。ワイヤレス インターフェイスを設定しない場合は、[いいえ（No）] をクリックします。[いいえ（No）] をクリックした場合でも LAN インターフェイスを設定できます。

Cisco CP Express では、1 つのワイヤレス インターフェイスしか設定することができません。ルータ上に複数のワイヤレス インターフェイスが存在する場合は、ワイヤレス アプリケーションを使用して設定します。

LAN インターフェイスの設定

Cisco CP Express ウィザードを使用すれば、LAN インターフェイスを IP アドレスを使用して設定したり、DHCP サーバとして設定したり、DHCP サーバで使用される IP アドレス範囲を指定したりできます。

次のトピックで、LAN インターフェイス画面について説明します。

- LAN インターフェイスの設定（LAN Interface Configuration）
- DHCP サーバ設定

LAN インターフェイスの設定（LAN Interface Configuration）

このウィンドウでは、LAN イーサネット インターフェイスの IP アドレスとサブネット情報を設定できます。

Cisco CP Express ウィザードの完了後に、LAN イーサネット インターフェイスの IP アドレスとサブネット情報を変更するには、再度 Cisco CP Express を起動して、[LAN（LAN）] をクリックし、必要なアドレスを編集します。

[インターフェイス（Interface）] リストまたは [ブリッジとインターフェイス間（Bridge-to-Interface）] リスト

ルータに複数の LAN インターフェイスが実装されている場合は、このリストにそれらのインターフェイスが表示されます。設定する LAN インターフェイスを選択します。

ルータにワイヤレス インターフェイスが 1 つしかなく、[ワイヤレス インターフェイスの設定（Wireless Interface Configuration）] ウィンドウで [はい（Yes）] をクリックした場合は、このリストのラベルが [ブリッジとインターフェイス間（Bridge-to Interface）] に変わります。ワイヤレス トラフィックをブリッジするインターフェイスを選択します。

IP アドレス（IP Address）

LAN インターフェイスの IP アドレスをドット区切り形式で入力します。Network Address Translation（NAT; ネットワーク アドレス変換）または Port Address Translation（PAT; ポート アドレス変換）を使用する予定の場合は、プライベート IP アドレスにすることができます。

（注）　このアドレスを書き留めてください。Cisco CP Express ウィザードを完了してルータを再起動するときに、このアドレスを使用して Cisco CP Express を実行します。ルータのクイック スタート ガイドで指定されているアドレスは使用しないでください。

サブネット マスク（Subnet Mask）

ネットワークのサブネット マスクを入力します。この値は、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。サブネット マスクを使用すれば、ルータで、ネットワークとアドレスのサブネット部分の定義に使用される IP アドレス数を特定できます。サブネット マスクの値は、このルータが接続されている LAN 上に設置可能なホスト数にも影響します。

サブネット ビット（Subnet Bits）

または、ネットワークと IP アドレスのサブネット部分の定義に使用されるビット数を入力します。この形式のサブネット マスク情報については、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。

ワイヤレス パラメータ

ルータにワイヤレス インターフェイスが 1 つしかなく、[ワイヤレス インターフェイスの設定（Wireless Interface Configuration）] ウィンドウで [はい（Yes）] をクリックした場合は、初期設定中に、これらのフィールドが表示されます。初期設定中にワイヤレス設定を実行した場合は、設定の編集中に、これらのフィールドが表示されます。ワイヤレス トラフィックがこの LAN インターフェイスにブリッジされます。

このワイヤレス トラフィックの Service Set Identifier（SSID）を入力します。SSID は、ワイヤレス ネットワーキング デバイスでワイヤレス接続を確立して維持するために使用される固有識別情報です。

（注）　設定された SSID 値を変更すると、ワイヤレス接続がダウンします。

Cisco CP Express ウィザードを完了して LAN 設定の編集中に詳細ワイヤレス パラメータを設定する場合は、カテゴリ バーの [ワイヤレス（Wireless）] をクリックします。

[更新（Refresh）] ボタン、[変更の適用（Apply Changes）] ボタン、[変更の破棄（Discard Changes）] ボタン

初期設定を編集中に表示されます。詳細については、「Cisco CP Express のボタン」をクリックしてください。

DHCP サーバ設定

Dynamic Host Configuration Protocol（DHCP）は、スタティック アドレス指定が不要な場合や特定のサービスに対してポート番号を使用する必要がない場合に使用される単純な形式のアドレス指定です。DHCP は、ネットワークへのログイン時にホストに IP アドレスを動的に割り当て、ログオフ時にそのアドレスを回収します。この方法では、ホストで不要になったアドレスを再利用できます。DHCP は、内部ネットワーク上のリソース（PC など）にアドレスを割り当てるために使用します。

[LAN インターフェイスに対して DHCP サーバを有効にする（Enable DHCP server on the LAN interface）] チェックボックス

ルータで LAN 上のデバイスにプライベート IP アドレスを割り当てられるようにする場合にオンにします。このウィンドウで有効にした場合は、1 日の間、DHCP サーバからホストに IP アドレスがリースされます。このチェックボックスをオンにした場合は、[開始 IP アドレス（Starting IP Address）] フィールドと [終了 IP アドレス（Ending IP Address）] フィールドに値を入力する必要があります。

開始 IP アドレス（Starting IP Address）

Cisco CP Express は、LAN インターフェイスに設定された IP アドレスとサブネット マスクに基づいて、このフィールドに IP アドレス範囲の中でもっとも小さいアドレスを入力します。DHCP アドレス プールを縮小したいが、LAN インターフェイスと同じサブネット内のアドレスを入力する必要がある場合、または、Cisco CP Express にアドレスが無効であることを伝えるメッセージが表示された場合は、この値をより高い値に変更できます。

終了 IP アドレス（Ending IP Address）

Cisco CP Express は、LAN インターフェイスに設定された IP アドレスとサブネット マスクに基づいて、このフィールドに IP アドレス範囲の中でもっとも大きい有効なアドレスを入力します。DHCP アドレス プールを縮小したいが、LAN インターフェイスと同じサブネット内のアドレスを入力する必要がある場合、または、Cisco CP Express にアドレスが無効であることを伝えるメッセージが表示された場合は、この値をより低い値に変更できます。

ドメイン名（Domain Name）

初期設定の完了後に表示されます。組織のドメイン名を入力できます。*cisco.com* はドメイン名の例ですが、サフィクスが *.org* や *.net* などのドメイン名もあります。

[すべての DHCP オプション パラメータを DHCP サーバ データベースにインポートする（Import all DHCP option parameters to the DHCP server database）] チェックボックス

初期設定の完了後に表示されます。DHCP オプション パラメータを DHCP サーバ データベースにインポートして、その情報を IP アドレスを要求している LAN 上の DHCP クライアントに送信する場合にこのオプションをオンにします。

プライマリ ドメイン ネーム サーバ（Primary Domain Name Server）

ルータで使用されるプライマリ DNS サーバの IP アドレスを入力します。この IP アドレスは、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。

プライマリ DNS サーバは、ルータが IP アドレスを解決しようとして最初にアクセスするサーバです。

セカンダリ ドメイン ネーム サーバ（Secondary Domain Name Server）

ルータで使用されるセカンダリ DNS サーバの IP アドレスを入力します（使用可能な場合）。この IP アドレスは、ネットワーク管理者またはサービス プロバイダーにお問い合わせください。

セカンダリ DNS サーバは、プライマリ サーバが使用できない場合にルータからアクセスされるサーバです。

[これらの DNS 値を DHCP クライアントに使用する（Use these DNS values for DHCP clients）] チェックボックス

DHCP サーバが LAN インターフェイス上で有効になっている場合に使用できます。このウィンドウで入力した IP アドレスの DNS サーバをルータの DHCP クライアントで使用できるようにする場合にオンにします。

[更新（Refresh）] ボタン、[変更の適用（Apply Changes）] ボタン、[変更の破棄（Discard Changes）] ボタン

初期設定を編集中に表示されます。詳細については、「Cisco CP Express のボタン」をクリックしてください。

ワイヤレス アクセス ポイントの設定

ルータにワイヤレス アクセス ポイントがインストールされている場合は、Cisco CP Express ウィザードを使用して設定できます。Cisco CP Express は、アクセス ポイント ハードウェアを検出して、該当する設定画面を表示します。

ワイヤレス アクセス ポイント設定画面については、次のトピックで説明します。

- 自律型ワイヤレス設定（Autonomous Wireless Configuration）
- ワイヤレス LWAPP ホスト ルータの設定（Wireless-LWAPP Host Router Configuration）

自律型ワイヤレス設定（Autonomous Wireless Configuration）

自律型ワイヤレス設定をサポートするイメージがルータ アクセス ポイント コントローラ上にインストールされている場合は、Cisco CP Express に [自律型ワイヤレス設定（Autonomous Wireless Configuration）] 画面が表示されます。

フィールドについて

表 1-1　自律型ワイヤレス設定（Autonomous Wireless Configuration）

要素	説明
自律型ワイヤレス設定（Autonomous Wireless Configuration）	自律モードで動作するようにワイヤレス アクセス ポイント コントローラを設定するには、[自律型ワイヤレス設定（Autonomous Wireless Configuration）] をオンにします。 **（注）** このフィールドは、Cisco CP Express ウィザードを使用している場合に表示されます。
ホスト名（Hostname）	アクセス ポイント コントローラのホスト名を入力します。「800-accesspoint」などを入力します。
パスワード（Password）/パスワードの確認（Confirm Password）	アクセス ポイント コントローラ用として設定するパスワードを入力してから、再度同じパスワードを入力して正しいかどうかを確認します。
スタティック IP アドレス フィールド	[IP アドレス（IP Address）] リストから [スタティック IP アドレス（Static IP Address）] を選択した場合は、[IP アドレス（IP Address）] フィールドと [サブネット マスク（Subnet Mask）] フィールドが表示されます。
IP アドレス（IP Address）	アクセス ポイント コントローラの BVI インターフェイスに設定する IP アドレスを入力します。この IP アドレスは使用されるサブネット マスクに対して有効になっている必要があります。たとえば、ネットワーク アドレスが 192.168.0.0 で、サブネット マスクが 255.255.255.248 の場合は、IP アドレスを 192.168.0.1 ～ 192.168.0.6 の範囲から選択する必要があります。
サブネット マスク（Subnet Mask）/サブネット ビット（Subnet Bits）	使用するサブネット マスクを指定するには、[サブネット マスク（Subnet Mask）] にマスクを入力するか、[サブネット ビット（Subnet Bits）] フィールドでサブネット ビットを選択します。サブネット ビットを選択した場合は、Cisco CP Express によって自動的にマスクが入力されます。たとえば、[サブネット ビット（Subnet Bits）] フィールドで 29 を選択した場合は、Cisco CP Express によって [サブネット マスク（Subnet Mask）] フィールドに 255.255.255.248 が入力されます。

表 1-1　自律型ワイヤレス設定（Autonomous Wireless Configuration）（続き）

要素	説明
ダイナミック IP アドレス フィールド	[IP アドレス（IP Address）] リストで [ダイナミック IP アドレス（Dynamic IP Address）] を選択すると、[ホスト名（Hostname）] フィールドが表示されます。
ホスト名（Hostname）	Internet Service Provider（ISP; インターネット サービス プロバイダー）から DHCP サーバの名前が提供されている場合は、それを [ホスト名（Hostname）] フィールドに入力します。
IP アドレスなし（No IP Address）	[IP アドレス（IP Address）] リストで [IP アドレスなし（No IP Address）] を選択した場合は、どの IP アドレスもルータ インターフェイス上に設定されず、どのフィールドも [IP アドレス（IP Address）] ボックスに表示されません。
[SSID] フィールドと [暗号化（Encryption）] フィールド	コントローラ設定で設定済みの SSID が検出されなかった場合は、[SSID] フィールドと [暗号化（Encryption）] フィールドが表示されます。
SSID	SSID（無線 SSID とも呼ばれる）は、クライアントで、アクセス ポイント ラジオに関連付けるために使用される固有識別情報です。この SSID は、大文字と小文字が区別される 2 ～ 32 文字の任意のアルファベットにすることができます。このフィールドに SSID を入力します。
暗号化（Encryption）	アクセス ポイントへの接続に使用する暗号化のタイプを選択します。次の暗号化タイプがサポートされています。 • Wired Equivalent Privacy（WEP; 有線と同等のプライバシー）: WEP は、元々、有線 LAN 上と同じプライバシー レベルを提供するように設計された 802.11 標準の暗号化アルゴリズムです。この標準では、サイズが 40 ビットまたは 104 ビットの WEP ベース キーが規定されています。 • Wi-Fi Protected Access（WPA）: WPA は、認証サーバのサービスを通して、データベースに照らして認証されたユーザにワイヤレス アクセスを許可し、WEP で使用されるものよりも強力なアルゴリズムを使用して IP トラフィックを暗号化します。
キー（Key）	アクセス ポイントで暗号化に使用されるキーを入力します。

表 1-1　自律型ワイヤレス設定（Autonomous Wireless Configuration）（続き）

要素	説明
注意	この画面でアクセス ポイント アプリケーションを起動することによって、アクセス ポイントの追加の設定を実行できます。
内部アクセス ポイントの詳細設定については、内部アクセス ポイント アプリケーションを起動するリンクをクリックします。（For advanced configuration of the internal access point, click on the link to launch the internal access point application.）	内部アクセス ポイント アプリケーションを起動するには、アクセス ポイントの IP アドレスを示すリンクをクリックします。このアプリケーションを使用して、追加の設定タスクを実行できます。内部アクセス ポイントの詳細設定については、『*Cisco 860 and Cisco 880 Series Integrated Services Router Software Configuration Guide*』を参照してください。このガイドは次のリンクから入手できます。 http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/860-880-890SCG.html

ワイヤレス LWAPP ホスト ルータの設定（Wireless-LWAPP Host Router Configuration）

自律型ワイヤレス Lightweight Access Point Protocol 設定をサポートする Cisco IOS イメージがルータ アクセス ポイント コントローラ上にインストールされている場合は、Cisco CP Express にワイヤレス LWAPP の設定画面が表示されます。

（注）　内部アクセス ポイントの詳細設定を実行する必要がある場合は、コントローラに関連付けられたワイヤレス LAN コントローラ管理アプリケーションを使用する必要があります。

フィールドについて

表 1-2　ワイヤレス LWAPP ホスト ルータ

要素	説明
ワイヤレス LWAPP ホスト ルータの設定（Wireless-LWAPP Host Router Configuration）	WLAN コントローラの IP アドレスをルータの DHCP サーバに設定するには、[ワイヤレス LWAPP ホスト ルータの設定（Wireless-LWAPP Host Router Configuration）] をオンにします。

表 1-2　ワイヤレス LWAPP ホスト ルータ（続き）

要素	説明
コントローラ IP アドレス（Controller IP Address）	DHCP オファーを受信するワイヤレス LAN コントローラの IP アドレスを入力します。
注：内部アクセス ポイントの詳細設定については～（Note: For advanced configuration of the internal access point.....）	Cisco CP Express を使用すれば、この画面でカバーされている設定タスクを実行できます。アクセス ポイントの追加の設定を実行するには、指定された手順を使用して、関連するワイヤレス管理アプリケーションを使用します。

WAN インターフェイスの設定

Cisco CP Express を使用すれば、WAN インターフェイスを設定できます。ルータに複数の WAN インターフェイスが実装されている場合は、設定するインターフェイスを選択できます。Cisco CP Express は、さまざまな WAN インターフェイスの設定をサポートします。

詳細については、「WAN について」を参照してください。

WAN について

- ケーブル モデム接続の追加（Add Cable Modem Connection）
- 認証（Authentication）

WAN インターフェイスの選択（WAN Interface Selection）

Cisco CP Express では、1 つの WAN 接続しか設定することができません。ルータに複数の WAN インターフェイスが実装されている場合は、このウィンドウで設定するインターフェイスを選択できます。リストから設定するインターフェイスを選択して、[接続の追加（Add Connection）] をクリックし、表示されたダイアログで接続を設定します。

（注）　WAN 接続を設定しなかった場合は、ファイアウォール、ルーティング、Cisco Network Services、または SDP を設定できなくなります。

[接続の追加（Add Connection）] ボタン、[編集（Edit）] ボタン、[削除（Delete）] ボタン

[接続の追加（Add Connection）] ボタンは、どの WAN 接続もまだ設定されていない場合に有効になります。[編集（Edit）] ボタンと [削除（Delete）] ボタンは、1 つ以上の WAN 接続が設定されている場合に有効になります。

インターフェイスを設定するには、インターフェイスを選択して、[接続の追加（Add Connection）] をクリックします。このボタンが無効になっている場合は、Cisco CP を使用して追加の WAN 接続を設定することも、設定済みの接続を削除して別の接続を設定することもできます。

既存の設定を編集するには、インターフェイスを選択して [編集（Edit）] をクリックします。

設定を削除するには、インターフェイスを選択して [削除（Delete）] をクリックします。

[有効（Enable）] ボタンまたは [無効（Disable）] ボタン

Cisco CP Express を使用して初期設定を編集している場合に使用できます。選択したインターフェイスが有効になっている場合は、[無効（Disable）] ボタンを使用してそのインターフェイスをシャットダウンできます。選択したインターフェイスがシャットダウンしている場合は、[有効（Enable）] ボタンを使用してそのインターフェイスを有効にできます。

[インターフェイス（Interface）] リスト

すべての WAN インターフェイスの名前、IP アドレス、およびタイプが表示されます。インターフェイスに対してどの IP アドレスも設定されていない場合は、「IP アドレスなし（no IP address）」というテキストが表示されます。

（注）　[LAN インターフェイスの設定（LAN Interface Configuration）] ウィンドウでデフォルト LAN インターフェイスを新しい IP アドレスを使用して設定しなかった場合は、それがこのウィンドウに表示され、WAN インターフェイスとして設定できます。

[更新（Refresh）] ボタン

初期設定を編集中に表示されます。詳細については、「Cisco CP Express のボタン」をクリックしてください。

インターネット（WAN）：イーサネット インターフェイス（Internet (WAN): Ethernet Interface）

このウィンドウは、イーサネット WAN インターフェイスを設定するために使用します。

[PPPoE を有効にする（Enable PPPoE）] チェックボックス

サービス プロバイダーがルータで PPPoE を使用するように要求している場合は、オンにして PPPoE カプセル化を有効にします。サービス プロバイダーが PPPoE を使用していない場合は、オフにします。ルータで PPPoE カプセル化をサポートしていない Cisco IOS リリースが実行されている場合は、このチェックボックスが使用できません。

[アドレス タイプ（Address Type）] リスト

次のいずれかを選択します。

[スタティック IP アドレス（Static IP Address）] オプション

スタティック IP アドレスを選択した場合は、表示されたフィールドに IP アドレスとサブネット マスクまたはサブネット ビットを入力します。

[ダイナミック（DHCP クライアント）（Dynamic (DHCP Client)）] オプション

[ダイナミック（Dynamic）] を選択した場合は、ルータでリモート DHCP サーバから IP アドレスがリースされます。アドレスを割り当てる DHCP サーバの名前を入力します。

[IP アンナンバード（IP Unnumbered）] オプション

インターフェイス間で IP アドレスを共有する場合は、[IP アンナンバード（IP Unnumbered）] を選択します。その後で、使用するために設定しているインターフェイスに必要な IP アドレスが設定されたインターフェイスを選択します。[PPPoE を有効にする（Enable PPPoE）] を選択しなかった場合は、このオプションが使用できません。

Easy IP（ネゴシエート済みの IP）（Easy IP (IP Negotiated)）

ルータで PPP/IPCP アドレス ネゴシエーションを通して IP アドレスが取得される場合は、[Easy IP（ネゴシエート済みの IP）（Easy IP (IP Negotiated)）] を選択します。[PPPoE を有効にする（Enable PPPoE）] を選択しなかった場合は、このオプションが使用できません。

[認証タイプ（Authentication Type）] チェックボックス

サービス プロバイダーが使用する認証のタイプに対応するボックスをオンにします。サービス プロバイダーが使用するタイプが不明の場合は、両方のボックスをオンにできます。ルータでは、両方のタイプの認証が試され、どちらかが成功します。

CHAP 認証は PAP 認証よりも安全です。

ユーザ名（Username）

インターネット サービス プロバイダーまたはネットワーク管理者から付与され、CHAP または PAP 認証用のユーザ名として使用されます。

パスワード（Password）

サービス プロバイダーから付与されたパスワードを正確に入力します。パスワードは大文字と小文字が区別されます。たとえば、パスワードの「test」と「Test」は同じではありません。

パスワードの確認（Confirm Password）

上のボックスに入力したパスワードを再入力します。

[更新（Refresh）] ボタン、[変更の適用（Apply Changes）] ボタン、[変更の破棄（Discard Changes）] ボタン

初期設定を編集中に表示されます。詳細については、「Cisco CP Express のボタン」をクリックしてください。

インターネット（WAN）：カプセル化の自動検出（Internet (WAN): Autodetect Encapsulation）

Cisco CP Express にカプセル化タイプの検出を指示する場合は [自動検出（Autodetect）] ボタンをクリックします。Cisco CP Express の処理が成功すると、検出されたカプセル化タイプとその他の設定パラメータが自動的に表示されます。

Cisco CP Express でカプセル化タイプが検出されなかった場合は、[ユーザ指定（User Specified）] をクリックして、カプセル化タイプと認証タイプを指定する必要があります。

[ステータス（Status）] アイコンと [有効（Enable）] または [無効（Disable）] ボタン

[ステータス（Status）] アイコンは、Cisco CP Express を使用して初期設定を編集しているときに表示されます。上矢印アイコンはインターフェイスがアップしていることを示します。下矢印アイコンはインターフェイスがダウンしていることを示します。

[有効（Enable）] または [無効（Disable）] ボタンは、Cisco CP Express を使用して初期設定を編集しているときに使用できます。選択したインターフェイスが有効になっている場合は、[無効（Disable）] ボタンを使用してそのインターフェイスをシャットダウンできます。選択したインターフェイスがシャットダウンしている場合は、[有効（Enable）] ボタンを使用してそのインターフェイスを有効にできます。

インターネット（WAN）：ユーザ指定のカプセル化（Internet (WAN): User Specified Encapsulation）

このウィンドウは、カプセル化を指定しているときに WAN インターフェイスを設定するために使用します。

[ステータス（Status）] アイコンと [有効（Enable）] または [無効（Disable）] ボタン

[ステータス（Status）] アイコンは、Cisco CP Express を使用して初期設定を編集しているときに表示されます。上矢印アイコンはインターフェイスがアップしていることを示します。下矢印アイコンはインターフェイスがダウンしていることを示します。

[有効（Enable）] または [無効（Disable）] ボタンは、Cisco CP Express を使用して初期設定を編集しているときに使用できます。選択したインターフェイスが有効になっている場合は、[無効（Disable）] ボタンを使用してそのインターフェイスをシャットダウンできます。選択したインターフェイスがシャットダウンしている場合は、[有効（Enable）] ボタンを使用してそのインターフェイスを有効にできます。

カプセル化

ADSL、G.SHDSL、または ADSL over ISDN インターフェイスが実装されている場合に、次の表に示すカプセル化を使用できます。

カプセル化	説明
PPPoE	Point-to-Point Protocol over Ethernet カプセル化を提供します。ATM インターフェイス上で PPPoE を設定すると、ATM サブインターフェイスとダイヤラ インターフェイスが作成されます。これらの論理インターフェイスは [要約（Summary）] ウィンドウに表示されます。 ルータで PPPoE カプセル化をサポートしていない Cisco IOS ソフトウェアが実行されている場合は、PPPoE オプションが無効になります。
PPPoA	Point-to-Point Protocol over ATM カプセル化（AAL5 SNAP と AAL5 MUX）を提供します。ルータで PPPoA カプセル化をサポートしていない Cisco IOS ソフトウェアが実行されている場合は、PPPoA オプションが無効になります。

カプセル化	説明
AAL5 SNAP を使用した RFC 1483 ルーティング	このオプションは、ATM インターフェイスを選択したときに使用できます。RFC 1483 接続を設定すると、ATM サブインターフェイスが作成されます。このサブインターフェイスは [要約（Summary）] ウィンドウに表示されます。
AAL5 MUX を使用した RFC 1483 ルーティング	このオプションは、ATM インターフェイスを選択したときに使用できます。RFC 1483 接続を設定すると、ATM サブインターフェイスが作成されます。このサブインターフェイスは [要約（Summary）] ウィンドウに表示されます。

仮想パス識別子（Virtual Path Identifier）

サービス プロバイダーまたはシステム管理者から提供された Virtual Path Identifier（VPI; 仮想パス識別子）の値を入力します。VPI は、ATM のスイッチングとルーティングで複数の接続に使用されたパスを特定するために使用されます。

仮想回線識別子（Virtual Circuit Identifier）

サービス プロバイダーまたはシステム管理者から提供された Virtual Circuit Identifier（VCI; 仮想回線識別子）の値を入力します。VCI は、ATM のスイッチングとルーティングで他の接続と共有されているパス内の特定の接続を区別するために使用されます。

[アドレス タイプ（Address Type）] リスト

次のいずれかを選択します。

- [スタティック IP アドレス（Static IP Address）] : [スタティック IP アドレス（Static IP Address）] を選択した場合は、表示されたフィールドに IP アドレスとサブネットまたはサブネット ビットを入力します。
- [ダイナミック（DHCP クライアント）（Dynamic (DHCP Client)）] : [ダイナミック（Dynamic）] を選択した場合は、ルータでリモート DHCP サーバから IP アドレスがリースされます。アドレスを割り当てる DHCP サーバの名前を入力します。
- [IP アンナンバード（IP Unnumbered）] : インターフェイス間で IP アドレスを共有する場合は、[IP アンナンバード（IP Unnumbered）] を選択します。その後で、使用するために設定しているインターフェイスに必要な IP アドレスが設定されたインターフェイスを選択します。

- [Easy IP（ネゴシエート済みの IP）（Easy IP (IP Negotiated)）] : ルータで PPP/IPCP アドレス ネゴシエーションを通して IP アドレスが取得される場合は、[Easy IP（ネゴシエート済みの IP）（Easy IP (IP Negotiated)）] を選択します。

中央オフィス内のリモート接続用の IP アドレス（IP Address for Remote Connection in Central Office）

G.SHDSL 接続を設定している場合は、このリンクが接続されるゲートウェイの IP アドレスを入力します。この IP アドレスは、サービス プロバイダーまたはネットワーク管理者から提供されます。ゲートウェイは、インターネットまたは社内の WAN にアクセスするためにルータから接続する必要のあるシステムです。

マルチリンク PPP を有効にする（Enable Multilink PPP）

このインターフェイスと一緒に Multilink Point-to-Point Protocol（MLP）を使用する場合は、このチェックボックスをオンにします。MLP は、ロード バランシング機能、パケット フラグメンテーション、オンデマンド帯域幅などの機能を使用して、複数の WAN に接続されたネットワークの性能を向上させます。

[認証タイプ（Authentication Type）] チェックボックス

サービス プロバイダーが使用する認証のタイプに対応するボックスをオンにします。サービス プロバイダーが使用するタイプが不明の場合は、両方のボックスをオンにできます。ルータでは、両方のタイプの認証が試され、どちらかが成功します。

CHAP 認証は PAP 認証よりも安全です。

ユーザ名（Username）

インターネット サービス プロバイダーまたはネットワーク管理者から付与され、CHAP または PAP 認証用のユーザ名として使用されるユーザ名を入力します。

パスワード（Password）

サービス プロバイダーから付与されたパスワードを正確に入力します。パスワードは大文字と小文字が区別されます。たとえば、パスワードの「test」と「Test」は同じではありません。

パスワードの確認（Confirm Password）

上のボックスに入力したパスワードを再入力します。

[更新（Refresh）] ボタン、[変更の適用（Apply Changes）] ボタン、[変更の破棄（Discard Changes）] ボタン

初期設定を編集中に表示されます。詳細については、「Cisco CP Express のボタン」をクリックしてください。

シリアル接続（Serial Connection）

このウィンドウでシリアル接続を作成または編集します。

[カプセル化（Encapsulation）] リスト

この接続用のカプセル化を選択します。接続を編集している場合は、このウィンドウでカプセル化タイプを変更できません。接続を削除してから、必要なカプセル化タイプで新しい接続を作成する必要があります。

- [フレーム リレー（Frame Relay）] : 接続されたデバイス間の HDLC カプセル化を使用して複数の仮想回線を処理するスイッチド データ リンク層プロトコルです。
- [HDLC] : High-Level Data Link Control（ハイレベル データリンク コントロール）。International Organization for Standardization（ISO; 国際標準化機構）によって策定された、ビット指向の同期型データ リンク層プロトコルです。HDLC は、フレーム キャラクタとチェックサムを使用して、同期シリアル リンクでのデータのカプセル化方法を指定します。
- [PPP] : Point-to-Point Protocol（ポイントツーポイント プロトコル）。

認証の詳細

PPP カプセル化を選択した場合は、インターネット サービス プロバイダーから要求される可能性のある認証情報を入力できます。

- [ユーザ名（Username）] : インターネット サービス プロバイダーまたはネットワーク管理者から付与され、CHAP または PAP 認証用のユーザ名として使用されるユーザ名を正確に入力します。
- [パスワード（Password）] : サービス プロバイダーから付与されたパスワードを正確に入力します。パスワードは大文字と小文字が区別されます。たとえば、パスワードの「test」と「Test」は同じではありません。

- [パスワードの確認（Confirm Password）]：上のボックスに入力したパスワードを再入力します。

[アドレス タイプ（Address Type）] リスト

- [スタティック IP アドレス（Static IP address）]：フレーム リレー、PPP、および HDLC のカプセル化タイプと一緒に使用できます。スタティック IP アドレスを選択した場合は、表示されたフィールドに IP アドレスとサブネット マスクまたはサブネット ビットを入力します。
- [IP アンナンバード（IP Unnumbered）]：フレーム リレー、PPP、および HDLC のカプセル化タイプと一緒に使用できます。インターフェイス間で IP アドレスを共有する場合は、[IP アンナンバード（IP Unnumbered）] を選択します。その後で、使用するために設定しているインターフェイスに必要な IP アドレスが設定されたインターフェイスを選択します。
- [ネゴシエート済みの IP（IP Negotiated）]：PPP カプセル化タイプと一緒にのみ使用できます。ルータで PPP/IPCP アドレス ネゴシエーションを通して IP アドレスが取得される場合は、[Easy IP（ネゴシエート済みの IP）（Easy IP (IP Negotiated)）] を選択します。

IP アドレス（IP Address）/サブネット マスク（Subnet Mask）

スタティック IP アドレスを選択した場合は、これらのフィールドに IP アドレスとサブネット マスクを入力します。

フレーム リレー設定に関するリンク

[DLCI]、[LMI]、および [IETF フレーム リレーのカプセル化を使用する（Use IETF Frame Relay Encapsulation）] フィールドについては、「フレーム リレー設定」をクリックしてください。

フレーム リレー設定

フレーム リレー接続を設定するために次の設定を実行します。

DLCI

このフィールドに、Data Link Connection Identifier（DLCI）を入力します。この番号は、このインターフェイス上で使用されるすべての DLCI で一意にする必要があります。DLCI は、この接続に対して一意のフレーム リレー識別子を提供します。

既存の接続を編集している場合は、[DLCI] フィールドが無効になります。DLCI を変更する必要がある場合は、接続を削除して再度作成します。

LMI タイプ（LMI Type）

次の Local Management Interface（LMI）タイプの中でどれを使用すべきかをサービス プロバイダーに問い合わせてください。LMI タイプは、接続のモニタに使用されるプロトコルを指定します。

[ANSI] オプション

American National Standards Institute（ANSI）標準 T1.617 で規定された Annex D

[Cisco] オプション

シスコと他の 3 社が共同で規定した LMI タイプ

[ITU-T Q.933] オプション

ITU-T Q.933 Annex A

[自動検出（Autosense）] オプション

デフォルト。この設定を使用すれば、ルータで、スイッチとの接続に使用されている LMI タイプを検出して使用できます。自動検出に失敗した場合は、ルータで Cisco LMI タイプが使用されます。

[IETF フレーム リレーのカプセル化を使用する（Use IETF Frame Relay Encapsulation）] チェックボックス

Internet Engineering Task Force（IETF）カプセル化を使用する場合にオンにします。このオプションは、シスコ製以外のルータに接続している場合に使用します。このインターフェイスを使用してシスコ製以外のルータに接続している場合は、このチェックボックスをオンにします。

インターネット（WAN）：詳細オプション（Internet (WAN): Advanced Options）

このウィンドウを使用すれば、デフォルトのスタティック ルートを指定したり、ルータ上で NAT を有効にしたりできます。

[デフォルト ルートの作成（Create Default Route）] チェックボックス

デフォルトのスタティック ルートは、ルータが学習していないネットワークに対してトラフィックがバインドされた場合に、ルータがトラフィックを送信する IP アドレスまたはインターフェイスを示します。[転送先インターフェイスとしてこのインターフェイスを使用する（Use This Interface as the Forwarding Interface）] がオンになっている場合は、ルータがこのようなトラフィックのすべてを接続されている WAN インターフェイスに送信します。[ネクスト ホップ IP アドレス（Next Hop IP address）] をオンにした場合は、ルータからこのようなトラフィックを送信するアドレスを指定します。

ダイナミック IP アドレスを使用する WAN インターフェイスを選択した場合は、これらのフィールドが表示されません。

インターネット（WAN）：ケーブル モデム（Internet (WAN): Cable Modem）

この画面を使用すれば、ルータ上でケーブル モデム インターフェイスを設定できます。Cisco CP Express は、デフォルトのケーブル モデム設定を表示し、DHCP サーバから IP アドレスを受信する DHCP クライアントとしてインターフェイスを設定します。

DHCP クライアントとしてケーブル モデム インターフェイスを設定する場合は、[このウィザードでは、選択されたケーブル モデム インターフェイス上のダイナミック IP アドレス（DHCP クライアント）を設定します（This wizard will configure a dynamic IP address (DHCP client) on the selected cable modem interface）] をオンにします。

ケーブル モデム接続の追加（Add Cable Modem Connection）

ケーブル モデム インターフェイスの設定を選択すると、Cisco CP Express にこのメッセージ画面が表示されます。インターフェイスが DHCP クライアントとして設定されることが表示されます。DHCP クライアントとして設定された WAN インターフェイスは、ISP または組織から提供された DHCP サーバから IP アドレスを取得する必要があります。

フィールドについて

表 1-3　ケーブル モデム設定メッセージ ボタン

要素	説明
OK	Cisco CP Express でケーブル モデム インターフェイスをデフォルト設定にし、DHCP サーバからダイナミック IP アドレスを取得する DHCP クライアントにするには、[OK] をクリックします。
キャンセル（Cancel）	インターフェイスを Cisco CP Express で使用される値に設定しない場合は、[キャンセル（Cancel）] をクリックします。

認証（Authentication）

このページは、次の要素を有効にした、または設定している場合に表示されます。

- シリアル接続用の Point-to-Point Protocol（PPP）
- ATM 接続用の Point-to-Point Protocol over Ethernet（PPPoE）または Point-to-Point Protocol over ATM（PPPoA）カプセル化
- イーサネット接続用の PPPoE または PPPoA カプセル化
- ISDN BRI またはアナログ モデム接続

サービス プロバイダーまたはネットワーク管理者は、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）パスワードまたは Password Authentication Protocol（PAP; パスワード認証プロトコル）パスワードを使用して、デバイス間の接続を保護できます。このパスワードは、着信アクセスと発信アクセスの両方を保護します。

フィールドについて

表 1-4　[認証（Authentication）] 画面

要素	説明
認証タイプ（Authentication Type）	サービス プロバイダーが使用する認証のタイプに対応するボックスをオンにします。サービス プロバイダーが使用するタイプが不明の場合は、両方のボックスをオンにできます。ルータでは、両方のタイプの認証が試され、どちらかが成功します。 CHAP 認証は PAP 認証よりも安全です。
ユーザ名（Username）	ユーザ名は、インターネット サービス プロバイダーまたはネットワーク管理者から付与され、CHAP または PAP 認証用のユーザ名として使用されます。
パスワード（Password）	サービス プロバイダーから付与されたパスワードを正確に入力します。パスワードは大文字と小文字が区別されます。たとえば、パスワードの「cisco」と「Cisco」は同じではありません。
パスワードの確認（Confirm Password）	上のボックスに入力したパスワードを再入力します。

ファイアウォールの設定

Cisco CP Express を使用すれば、ルータ上で WAN インターフェイスが設定されている場合にデフォルト設定を使用するようにファイアウォールを設定できます。

（注） Cisco CP Express を使用してファイアウォールを設定するためには、ルータ上の Cisco IOS イメージがファイアウォール フィーチャ セットをサポートしている必要があります。

ファイアウォールは、次の方法でネットワークを保護します。

- 内部インターフェイスと外部インターフェイスにデフォルト アクセス ルールを適用します。
- 外部インターフェイスにデフォルト インスペクション ルールを適用します。Cisco CP Express がデフォルト インスペクション ルールを作成して適用します。

- 外部インターフェイス上で IP Unicast Reverse-Path Forwarding（RPF）を有効にします。

Cisco CP Express にファイアウォールの設定を任せることにした場合は、後から、Cisco CP を使用してファイアウォールの設定を変更できます。ファイアウォールを設定しないことにした場合は、後から、Cisco CP Express または Cisco CP を使用してファイアウォールを設定できます。

トピックの「ファイアウォールの設定（Firewall Configuration）」でこの画面について説明します。

ファイアウォールの設定（Firewall Configuration）

[ファイアウォールの設定（Firewall Configuration）] ウィンドウでは、Cisco CP Express に WAN インターフェイスと LAN インターフェイス上のファイアウォールの設定を任せるオプションが提供されます。初期セットアップ中にファイアウォールを起動できます。

Cisco CP Express にファイアウォールの設定を任せる場合は、後から、Cisco CP のファイアウォール ポリシー設定機能を使用して、ファイアウォールの設定を変更できます。

（注）

- この機能は、ルータ上で動作している Cisco IOS リリースがファイアウォール フィーチャ セットをサポートしている場合に使用できます。
- WAN インターフェイスを設定しなかった場合は、[ファイアウォールの設定（Firewall Configuration）] ウィンドウが表示されません。

ファイアウォールは、次の方法でネットワークを保護します。

- 内部インターフェイスと外部インターフェイスにデフォルト アクセス ルールを適用します。Cisco CP Express が、DNS トラフィックと HTTP トラフィックを許可し、プライベート IP アドレス空間を拒否するなどのデフォルト アクセス ルールのリストを作成して適用します。
- 外部インターフェイスにデフォルト インスペクション ルールを適用します。Cisco CP Express がデフォルト インスペクション ルールのリストを作成して適用します。

- 外部インターフェイス上で IP Unicast Reverse-Path Forwarding（RPF）を有効にします。IP Unicast RPF は、ルータに、パケットが到着したインターフェイスに照らしてすべてのパケットの送信元アドレスをチェックさせる機能です。ルーティング テーブルに照らして、入力インターフェイスが送信元アドレスへのパスとして不適切な場合は、パケットがドロップされます。この送信元アドレス検証は、IP スプーフィングを阻止するために使用されます。

Cisco CP Express にファイアウォールの設定を任せることにした場合は、後から、Cisco CP を使用してファイアウォールの設定を変更できます。ファイアウォールを設定しないことにした場合は、後から、Cisco CP Express または Cisco CP を使用してファイアウォールを設定できます。詳細については、「Cisco Configuration Professional」をクリックしてください。

セキュリティの設定

ルータとネットワークのセキュリティを侵害する可能性のある一部の設定が、デフォルトで、有益なサービスを提供するという理由で有効になっています。たとえば、[Cisco ディスカバリ プロトコル（CDP）（Cisco Discovery Protocol (CDP)）] を使用すれば、管理者は、ネットワーク上で隣接しているルータに関する情報を簡単に表示できます。ただし、CDP は、その情報が悪意のある人物の手に渡った場合にセキュリティ リスクになるおそれがあります。
Cisco CP Express に、セキュリティ リスクを招く一般的な設定が一覧表示されます。ルータとネットワークを保護する目的でそれらを無効にできます。

デフォルトで無効になっているが、有効にするとネットワークを攻撃から保護したり、トラブルシューティングを支援したりできる [TCP Syn Wait 時間（TCP Syn Wait time）] などの設定やロギングもあります。Cisco CP Express に、これらの設定が一覧表示されます。それらを有効と無効のどちらかに設定できます。

[セキュリティ設定（Security Setting）] 画面については、次のトピックで説明します。

- セキュリティ設定（Security Settings）

以降のセクションに列挙されたトピックで、この画面で実行可能なセキュリティ設定について説明します。

セキュリティ リスク

これらのトピックでは、一般的なセキュリティ リスクを低減するために実行可能な設定について説明します。

- Finger サービスが無効（Disable Finger Service）
- PAD サービスが無効（Disable PAD Service）
- TCP スモール サーバ サービスが無効（Disable TCP Small Servers Service）
- UDP スモール サーバ サービスが無効（Disable UDP Small Servers Service）
- IP bootp サーバ サービスが無効（Disable IP BOOTP Server Service）
- IP 識別サービスが無効（Disable IP Identification Service）
- CDP が無効（Disable CDP）
- IP ソース ルートが無効（Disable IP Source Route）
- IP Gratuitous ARP が無効（Disable IP Gratuitous ARPs）
- IP リダイレクトが無効（Disable IP Redirects）
- IP Proxy ARP が無効（Disable IP Proxy ARP）
- IP ダイレクト ブロードキャストが無効（Disable IP Directed Broadcast）
- MOP サービスが無効（Disable MOP Service）
- IP アンリーチャブルが無効（Disable IP Unreachables）
- IP マスク応答が無効（Disable IP Mask Reply）

ルータとネットワーク用の拡張セキュリティ

これらのトピックでは、ルータとネットワークのセキュリティを拡張するために実行可能な設定について説明します。

- Netflow スイッチングが有効（Enable Netflow Switching）
- インバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Inbound Telnet Sessions）
- アウトバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Outbound Telnet Sessions）
- デバッグのシーケンス番号とタイム スタンプが有効（Enable Sequence Numbers and Time Stamps on Debugs）
- IP CEF が有効（Enable IP CEF）
- スケジューラ間隔の設定（Set Scheduler Interval）
- スケジューラ割り当ての設定（Set Scheduler Allocate）
- TCP Synwait 時間の設定（Set TCP Synwait Time）

- ロギングが有効（Enable Logging）
- すべての外部インターフェイスに対するユニキャスト RPF が有効（Enable Unicast RPF on All Outside Interfaces）

ルータ アクセス用の拡張セキュリティ

これらのトピックでは、ルータ アクセスのセキュリティを拡張するために実行可能な設定について説明します。

- パスワードの最小文字数を 6 文字以上に設定（Set Minimum Password Length to Less Than 6 Characters）
- 認証失敗率を再試行回数 3 回未満に設定（Set Authentication Failure Rate to Less Than 3 Retries）
- バナーの設定（Set Banner）
- Telnet 設定が有効（Enable Telnet Settings）
- ルータ アクセスに対する SSH が有効（Enable SSH for Access to the Router）

パスワードの暗号化

これらのトピックでは、パスワードの暗号化を有効にするために実行可能な設定について説明します。

- パスワード暗号化サービスが有効（Enable Password Encryption Service）.

セキュリティ設定（Security Settings）

このウィンドウを使用すれば、Cisco IOS ソフトウェア内のデフォルトでオンになっている機能や、セキュリティ リスクを招いたり、ルータに使用可能なメモリを使い果たすほどの大量のメッセージを送信させたりする可能性のある機能を無効にできます。特別な要件がなければ、このチェックボックスはオンのままにしてください。このヘルプ トピックは、Cisco CP Express で行うそれぞれのセキュリティ設定の説明にリンクしています。

Cisco CP Express を使用すれば、初期設定後にこのウィンドウで行ったセキュリティ設定を変更できます。このヘルプ ページで説明した設定グループに属している個別の設定のいずれかを変更する場合は、Cisco CP を使用します。詳細については、「Cisco Configuration Professional」をクリックしてください。

[ルータの SNMP サービスを無効にする（Disable SNMP Services on Your Router）] チェックボックス

ルータ上で SNMP サービスを無効にする場合にオンにします。SNMP を無効にする理由については、ヘルプ トピックの「SNMP が無効（Disable SNMP）」を参照してください。

[セキュリティ リスクを伴うサービスを無効にする（Disable Services that Involve Security Risks）] チェックボックス

ルータ上で次のサービスを無効にする場合にオンにします。これらのサービスを無効にする理由については、下のリンクをクリックしてください。

- Finger サービスが無効（Disable Finger Service）
- PAD サービスが無効（Disable PAD Service）
- TCP スモール サーバ サービスが無効（Disable TCP Small Servers Service）
- UDP スモール サーバ サービスが無効（Disable UDP Small Servers Service）
- IP bootp サーバ サービスが無効（Disable IP BOOTP Server Service）
- IP 識別サービスが無効（Disable IP Identification Service）
- CDP が無効（Disable CDP）
- IP ソース ルートが無効（Disable IP Source Route）
- IP Gratuitous ARP が無効（Disable IP Gratuitous ARPs）
- IP リダイレクトが無効（Disable IP Redirects）
- IP Proxy ARP が無効（Disable IP Proxy ARP）
- IP ダイレクト ブロードキャストが無効（Disable IP Directed Broadcast）
- MOP サービスが無効（Disable MOP Service）
- IP アンリーチャブルが無効（Disable IP Unreachables）
- IP マスク応答が無効（Disable IP Mask Reply）

[ルータ / ネットワーク上の拡張セキュリティのサービスを有効にする（Enable Services for Enhanced Security on the Router/Network）] チェックボックス

ルータ上で次のセキュリティ拡張機能とサービスを有効にする場合にオンにします。これらのサービスと機能の説明については、下のリンクをクリックしてください。

- Netflow スイッチングが有効（Enable Netflow Switching）
- インバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Inbound Telnet Sessions）
- アウトバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Outbound Telnet Sessions）
- デバッグのシーケンス番号とタイム スタンプが有効（Enable Sequence Numbers and Time Stamps on Debugs）
- IP CEF が有効（Enable IP CEF）
- スケジューラ間隔の設定（Set Scheduler Interval）
- スケジューラ割り当ての設定（Set Scheduler Allocate）
- TCP Synwait 時間の設定（Set TCP Synwait Time）
- ロギングが有効（Enable Logging）
- すべての外部インターフェイスに対するユニキャスト RPF が有効（Enable Unicast RPF on All Outside Interfaces）

[ルータ アクセスのセキュリティを強化する（Enhance Security on Router Access）] チェックボックス

ルータ上で次のセキュリティ拡張設定を実行する場合にオンにします。これらのサービスと機能の説明については、下のリンクをクリックしてください。

- パスワードの最小文字数を 6 文字以上に設定（Set Minimum Password Length to Less Than 6 Characters）
- 認証失敗率を再試行回数 3 回未満に設定（Set Authentication Failure Rate to Less Than 3 Retries）
- バナーの設定（Set Banner）
- Telnet 設定が有効（Enable Telnet Settings）
- ルータ アクセスに対する SSH が有効（Enable SSH for Access to the Router）

[パスワードの暗号化（Encrypt Passwords）] チェックボックス

パスワードの暗号化を有効にする場合にオンにします。詳細については、ヘルプトピックの「パスワード暗号化サービスが有効（Enable Password Encryption Service）」を参照してください。

[ルータの日付と時刻をローカル PC の設定に同期させる（Synchronize the router date and time with my local PC settings）] チェックボックス

デフォルトでオンになっています。Cisco CP Express を実行している PC の現在の設定を使用してルータの日付と時刻を設定しない場合は、このチェックボックスをオフにします。

概要

[要約（Summary）] ウィンドウに、ルータ設定に加えた変更が表示されます。設定を変更する場合は、[戻る（Back）] をクリックして変更を加えたウィンドウに戻ります。

[完了（Finish）] をクリックすると、入力したデータがルータ コンフィギュレーション ファイルに保存されます。

（注）　LAN インターフェイスに推奨されている新しい IP アドレスを付与した場合は、[完了（Finish）] をクリックするとルータへの接続が失われます。ルータに再接続できるようにするには、PC がルータと同じサブネット上に存在することを確認してから、LAN インターフェイスに付与した新しい IP アドレスを入力する必要があります。詳細については、「初期設定後のルータへの再接続」をクリックしてください。

テレワーカー サポート

Cisco CP Express を使用してテレワーカー サポート機能を設定する方法については、次の URL にあるスクリーンキャストを参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional_express/scrcst/screencast/ccp_express_sc.html

（注）　スクリーンキャストを表示するには、インターネットにアクセスできる必要があります。

補足ヘルプ

次のヘルプ トピックでは、追加情報を提供します。

Cisco Configuration Professional

Cisco CP Express を使用したルータの基本設定が完了したら、Cisco Configuration Professional（Cisco CP）を使用して、追加の接続を設定したり、Cisco CP Express を使用して完了した設定を微調整したり、VPN やデジタル証明書などの詳細機能を設定したりできます。

Cisco CP がルータ上にインストールされている場合と、Cisco CP を PC またはルータ上にインストールするための CD が貼付されている場合があります。Cisco CP を Cisco.com からダウンロードした場合は、セットアップ プログラムを使用して Cisco CP を PC またはルータ上にインストールできます。

Cisco CP を起動するには、[ツール（Tools）] メニューで [CCP] をクリックします。

Cisco Network Services

サービス プロバイダーから Cisco Network Services サーバ情報が提供されている場合は、このオプションを選択します。このオプションを選択すると、Cisco CP Express ウィザードを通して Cisco Network Services サーバに関する情報が収集され、WAN 設定ウィンドウに表示されるため、Cisco Network Services サーバに接続してその設定を取得する WAN 接続を設定できます。サー

ビス プロバイダーから Cisco Network Services サーバ情報が提供されなかった場合、または、Cisco CP Express を使用してルータを設定する場合は、このオプションを選択しないでください。

次の場合は、Cisco Network Services を使用できません。

- ルータに WAN インターフェイスがインストールされていない、または、ルータに Cisco CP Express でサポートされていない WAN インターフェイスがインストールされている。Cisco CP Express では、ルータで Cisco Network Services 設定ファイルが取得されるように WAN インターフェイスを設定できる必要があります。Cisco CP Express で WAN インターフェイスが設定できないと判断された場合は、Cisco Network Services が使用できないことを伝えるエラー メッセージが表示されます。ルータ上に WAN インターフェイスがインストールされていないが、Cisco Network Services を使用する場合は、[キャンセル（Cancel）] をクリックして、スタートアップ ウィザードを終了し、Cisco CP Express を閉じます。その後で、Cisco CP Express でサポートされている WAN インターフェイス カードをインストールして、Cisco CP Express を再起動し、スタートアップ ウィザードで [CNS サーバ（CNS Server）]（Cisco Network Services サーバ）を選択します。

  サポートされているインターフェイス カードのリストについては、次の URL で Cisco CP のリリース ノートを参照してください。

  http://www.cisco.com/go/ciscocp

- このオプションを選択せずに、Cisco CP Express を使用して LAN インターフェイスと WAN インターフェイスを設定し、[ルータのプロビジョニング（Router Provisioning）] ウィンドウに戻って、[CNS サーバ（CNS Server）] を選択した。Cisco Network Services を使用する場合は、[キャンセル（Cancel）] をクリックしてスタートアップ ウィザードを終了し、Cisco CP Express を閉じます。その後で、Cisco CP Express を再起動して、[ルータのプロビジョニング（Router Provisioning）] ウィンドウで [CNS サーバ（CNS Server）] を選択します。

セキュリティ設定

次のトピックでは、Cisco CP Express で実行可能なセキュリティ設定について説明します。

SNMP が無効（Disable SNMP）

Cisco CP Express は、可能な場合はいつでも、Simple Network Management Protocol（SNMP）を無効にします。SNMP は、ネットワークのパフォーマンスとプロセスに関するデータの送受信を容易にするネットワーク プロトコルです。ルータのモニタや、特に、ルータ設定の変更によく使用されます。ただし、最も一般に使用されている SNMP のバージョン 1 は、次の理由からセキュリティ リスクになる可能性があります。

- プレーン テキストで保存されたり、ネットワーク経由で送信されたりする *コミュニティ ストリング*と呼ばれる認証文字列（パスワード）を使用する。
- ほとんどの SNMP 実装が定期ポーリングの一部としてこのような文字列を繰り返し送信する。
- なりすましが容易なデータグラム ベースのトランザクション プロトコルである。

SNMP はネットワーク ルーティング テーブルや機密扱いのネットワーク情報のコピーを取得するために使用できるため、ネットワークで必要がなければ SNMP を無効にすることを推奨します。Cisco CP Express は、最初に、SNMP を無効にするように要求します。

SNMP を無効にするためにルータに配信される設定は次のとおりです。

```
no snmp-server
```

Finger サービスが無効（Disable Finger Service）

Cisco CP Express は、可能な場合はいつでも、Finger サービスを無効にします。Finger は、ネットワーク デバイスにログインしているユーザを学習するために使用されます。この情報の多くは機密性が高くありませんが、攻撃者にとって有益な場合があります。

加えて、Finger サービスは、「Finger of death」と呼ばれる特定のタイプの Denial of Service（DoS; サービス妨害）攻撃に使用される可能性があります。この攻撃は、特定のコンピュータに 1 分おきに Finger 要求を送信し、決して切断しません。

Finger サービスを無効にするためにルータに配信される設定は次のとおりです。

```
no service finger
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方について、詳しくは「Cisco Configuration Professional」をクリックしてください。

PAD サービスが無効（Disable PAD Service）

Cisco CP Express は、可能な場合はいつでも、すべての Packet Assembler/Disassembler（PAD; パケット組立分解装置）コマンドと、PAD デバイスとアクセス サーバ間の接続を無効にします。

PAD を無効にするためにルータに配信される設定は次のとおりです。

```
no service pad
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

TCP スモール サーバ サービスが無効（Disable TCP Small Servers Service）

Cisco CP Express は、可能な場合はいつでも、スモール サービスを無効にします。Cisco IOS Release 11.3 以前を実行しているシスコ デバイスは、デフォルトで、スモール サービス（echo、chargen、および discard）を提供します（Cisco IOS ソフトウェア リリース 12.0 以降では、スモール サービスがデフォルトで無効になっています）。これらのサービス、特に、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）バージョンはあまり正当な目的には使用されませんが、パケット フィルタリングで阻止されるはずの DoS などの攻撃を仕掛けるために使用される可能性があります。

たとえば、攻撃者は、送信元アドレスを実際には到達できない DNS サーバに改ざんした DNS パケットや、送信元ポートを DNS サービス ポート（ポート 53）に改ざんした DNS パケットを送信できます。このようなパケットがルータの UDP エコー ポートに到着すると、ルータから問題のサーバに DNS パケットが送信されます。どの発信アクセス リスト チェックもこのパケットには適用されません。これは、このパケットがルータ内でローカルに生成されたと見なされるためです。

スモール サービスの不正使用のほとんどが、なりすまし対策リストによって阻止または危険性が緩和されますが、ファイアウォールの一部になっている、または、ネットワークのセキュリティ上重要な部分に設置されているルータでは、ほとんどの場合、このサービスを無効にしておく必要があります。このサービスはほとんど使用されることがないため、種類に関係なく、すべてのルータ上で無効にしておくことを推奨します。

TCP スモール サーバを無効にするためにルータに配信される設定は次のとおりです。

```
no service tcp-small-servers
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

UDP スモール サーバ サービスが無効（Disable UDP Small Servers Service）

Cisco CP Express は、可能な場合はいつでも、スモール サービスを無効にします。Cisco IOS Release 11.3 以前を実行しているシスコ デバイスは、デフォルトで、スモール サービス（echo、chargen、および discard）を提供します（Cisco IOS ソフトウェア リリース 12.0 以降では、スモール サービスがデフォルトで無効になっています）。これらのサービス、特に、UDP バージョンはあまり正当な目的には使用されませんが、パケット フィルタリングで阻止されるはずの DoS などの攻撃を仕掛けるために使用される可能性があります。

たとえば、攻撃者は、送信元アドレスを実際には到達できない DNS サーバに改ざんした DNS パケットや、送信元ポートを DNS サービス ポート（ポート 53）に改ざんした DNS パケットを送信できます。このようなパケットがルータの UDP エコー ポートに到着すると、ルータから問題のサーバに DNS パケットが送信されます。どの発信アクセス リスト チェックもこのパケットには適用されません。これは、このパケットがルータ内でローカルに生成されたと見なされるためです。

スモール サービスの不正使用のほとんどが、なりすまし対策リストによって阻止または危険性が緩和されますが、ファイアウォールの一部になっている、または、ネットワークのセキュリティ上重要な部分に設置されているルータでは、ほとんどの場合、このサービスを無効にしておく必要があります。このサービスはほとんど使用されることがないため、種類に関係なく、すべてのルータ上で無効にしておくことを推奨します。

UDP スモール サーバを無効にするためにルータに配信される設定は次のとおりです。

```
no service udp-small-servers
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP bootp サーバ サービスが無効（Disable IP BOOTP Server Service）

Cisco CP Express は、可能な場合はいつでも、Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）サービスを無効にします。BOOTP を使用すれば、ルータとコンピュータの両方で、起動時に、Cisco IOS ソフトウェアのダウンロードなど、中央で管理されたサーバから必要なインターネット情報を自動的に設定できます。そのため、BOOTP は、攻撃者によって、ルータの Cisco IOS ソフトウェアのコピーをダウンロードするために使用される可能性があります。

加えて、BOOTP サービスは、DoS 攻撃に対して脆弱です。そのため、無効にするか、ファイアウォールでフィルタする必要があります。

BOOTP を無効にするためにルータに配信される設定は次のとおりです。

```
no ip bootp server
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP 識別サービスが無効（Disable IP Identification Service）

Cisco CP Express は、可能な場合はいつでも、識別サポートを無効にします。識別サポートを使用すれば、識別に関して TCP ポートに問い合わせることができます。この機能は、安全ではないプロトコルで、TCP 接続を開始するクライアントとその接続に応答するホストの ID を報告可能にします。識別サポートを使用すれば、ホスト上の TCP ポートに接続して、情報を要求する単純なテキスト文字列を発行し、単純なテキスト文字列の応答を受け取ることができます。

セグメントに直接接続された任意のシステムで、ルータがシスコ デバイスであることを学習したり、モデル番号や実行している Cisco IOS ソフトウェア リリースを特定したりできると危険な場合があります。この情報は、ルータに対する攻撃の設計に使用される可能性があります。

IP 識別サービスを無効にするためにルータに配信される設定は次のとおりです。

```
no ip identd
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

CDP が無効（Disable CDP）

Cisco CP Express は、可能な場合はいつでも、Cisco Discovery Protocol を無効にします。Cisco Discovery Protocol は、LAN セグメント上で Cisco ルータがお互いに識別し合うために使用される独自仕様のプロトコルです。このプロトコルは、セグメントに直接接続された任意のシステムで、ルータがシスコ デバイスであることを学習したり、モデル番号や実行している Cisco IOS ソフトウェア リリースを特定したりできる点で危険です。この情報は、ルータに対する攻撃の設計に使用される可能性があります。

Cisco Discovery Protocol を無効にするためにルータに配信される設定は次のとおりです。

```
no cdp run
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP ソース ルートが無効（Disable IP Source Route）

Cisco CP Express は、可能な場合はいつでも、IP ソース ルーティングを無効にします。IP プロトコルは、IP データグラムの送信者が、データグラムが最終目的地に到達するまでに通過するルートと、すべての応答が通過する一般的なルートを制御できるようにするソース ルーティング オプションをサポートします。これらのオプションがネットワーク内の正当な目的に使用されることはほとんどありません。一部の旧式の IP 実装では、ソース ルーティングされたパケットが

正しく処理されないため、ソース ルーティング オプションを使用してこれらのデータグラムを送信すると、このような実装を実行しているマシンがクラッシュする可能性があります。

IP ソース ルーティングを無効にすると、Cisco ルータから、ソース ルーティング オプションを伝送する IP パケットが転送されなくなります。

IP ソース ルーティングを無効にするためにルータに配信される設定は次のとおりです。

```
no ip source-route
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

パスワード暗号化サービスが有効（Enable Password Encryption Service）

Cisco CP Express は、可能な場合はいつでも、パスワード暗号化を有効にします。パスワード暗号化は、Cisco IOS ソフトウェアに、パスワード、CHAP シークレット、およびコンフィギュレーション ファイルに保存された同様のデータを暗号化するように指示します。これは、部外者が、偶然、管理者の肩越しにパスワードを見てしまうといったケースを避けるのに役立ちます。

パスワード暗号化を有効にするためにルータに配信される設定は次のとおりです。

```
service password-encryption
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

Netflow スイッチングが有効（Enable Netflow Switching）

Cisco CP Express は、可能な場合はいつでも、Netflow スイッチングを有効にします。Netflow スイッチングは、Access Control List（ACL; アクセス コントロール リスト）使用時のルーティング性能と、ネットワーク セキュリティを構築または拡張するその他の機能を向上させる Cisco IOS 機能です。Netflow は、

送信元と宛先の IP アドレスと TCP ポート番号に基づいて、ネットワーク パケットのフローを識別します。そのため、Netflow は、ネットワーク フロー内のすべてのパケットを使用するのではなく、フローの初期パケットだけを使用して、ACL との比較やその他のセキュリティ チェックを実行できます。これにより、パフォーマンスが向上するため、すべてのルータ セキュリティ機能を利用できます。

Netflow を有効にするためにルータに配信される設定は次のとおりです。

```
ip route-cache flow
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

インバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Inbound Telnet Sessions）

Cisco CP Express は、可能な場合はいつでも、インバウンド Telnet セッションとアウトバウンド Telnet セッションの両方の TCP キープアライブ メッセージを有効にします。TCP キープアライブを有効にすると、ルータで、定期的にキープアライブ メッセージが生成され、切断された Telnet 接続が検出されるとドロップされます。

インバウンド Telnet セッションの TCP キープアライブを有効にするためにルータに配信される設定は次のとおりです。

```
service tcp-keepalives-in
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

アウトバウンド telnet セッションの TCP キープアライブが有効（Enable TCP Keepalives for Outbound Telnet Sessions）

Cisco CP Express は、可能な場合はいつでも、インバウンド Telnet セッションとアウトバウンド Telnet セッションの両方の TCP キープアライブ メッセージを有効にします。TCP キープアライブを有効にすると、ルータで、定期的にキープアライブ メッセージが生成され、切断された Telnet 接続が検出されるとドロップされます。

アウトバウンド Telnet セッションの TCP キープアライブを有効にするためにルータに配信される設定は次のとおりです。

```
service tcp-keepalives-out
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

デバッグのシーケンス番号とタイム スタンプが有効（Enable Sequence Numbers and Time Stamps on Debugs）

Cisco CP Express は、可能な場合はいつでも、すべてのデバッグ メッセージとログ メッセージ上のシーケンス番号とタイム スタンプを有効にします。デバッグ メッセージとログ メッセージ上のタイム スタンプは、そのメッセージが生成された時刻と日付を表します。シーケンス番号は、同じタイム スタンプを持つメッセージが生成された順序を表します。メッセージが生成されるタイミングとシーケンスを理解しておくことは、攻撃の可能性を診断するうえで重要です。

タイム スタンプとシーケンス番号を有効にするためにルータに配信される設定は次のとおりです。

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

IP CEF が有効（Enable IP CEF）

Cisco CP Express は、可能な場合はいつでも、Cisco Express Forwarding または Distributed Cisco Express Forwarding を有効にします。トラフィックが新しい宛先に初めて到着したときはキャッシュ エントリを作成する必要がないため、Cisco Express Forwarding は、大量のトラフィックが複数の宛先に送られる他の

モードよりも予測可能な振る舞いをします。Cisco Express Forwarding 用に設定されたルートは、従来のキャッシュを使用しているルータよりも SYN 攻撃に有効です。

Cisco Express Forwarding を有効にするためにルータに配信される設定は次のとおりです。

```
ip cef
```

スケジューラ間隔の設定（Set Scheduler Interval）

Cisco CP Express は、可能な場合はいつでも、ルータ上でスケジューラ間隔を設定します。ルータが大量のパケットを高速で切り替えているときは、ネットワーク インターフェイスからの割り込みに対する応答に時間がかかるため、他の処理を実行できない可能性があります。一部の超高速パケット フラッドがこの状態を引き起こす可能性があります。この状態ではルータへの管理アクセスが停止される可能性があるため、デバイスが攻撃を受けたときは非常に危険です。スケジューラ間隔を調整すれば、CPU の使用率が 100% に達した場合でも指定された時間間隔後にルータでシステム プロセスが実行されることによって、ルータへの管理アクセスがいつでも使用できることが保証されます。

スケジューラ間隔を調整するためにルータに配信される設定は次のとおりです。

```
scheduler interval 500
```

スケジューラ割り当ての設定（Set Scheduler Allocate）

scheduler interval コマンドをサポートしていないルータ上では、Cisco CP Express が、可能な場合はいつでも、**scheduler allocate** コマンドを設定します。ルータが大量のパケットを高速で切り替えているときは、ネットワーク インターフェイスからの割り込みに対する応答に時間がかかるため、他の処理を実行できない可能性があります。一部の超高速パケット フラッドがこの状態を引き起こす可能性があります。この状態は、ルータへの管理アクセスを停止させる可能性があるため、デバイスが攻撃を受けたときは非常に危険です。**sheduler allocate** コマンドは、管理プロセスなどのネットワーク スイッチング以外の活動に対するルータ CPU プロセスの割合を保証します。

スケジューラ割り当てを設定するためにルータに配信される設定は次のとおりです。

```
scheduler allocate 4000 1000
```

TCP Synwait 時間の設定（Set TCP Synwait Time）

Cisco CP Express は、可能な場合はいつでも、TCP synwait 時間を 10 秒に設定します。TCP synwait 時間は、DoS 攻撃の 1 形態である SYN フラッディング攻撃を阻止するのに有効な値です。TCP 接続は、初めて接続を確立するまでに 3 段階ハンドシェークが必要です。接続要求が送信側から送信され、確認応答が受信側から送信され、確認応答の承認が送信側から送信されます。この 3 段階ハンドシェークの完了後に、接続が確立され、データ転送が開始可能になります。SYN フラッディング攻撃は、ホストに接続要求を繰り返し送信して、接続を完了させる確認応答の承認を送信しないため、ホスト上に完了していない接続がどんどん溜まって行きます。通常は、完了していない接続用のバッファの方が、完了した接続用のバッファよりも容量が少ないため、バッファが使い果たされ、ホストが停止する可能性があります。TCP synwait 時間を 10 秒に設定した場合は、ルータで 10 秒後に完了していない接続がシャットダウンされるため、ホスト上の完了していない接続の蓄積が阻止されます。

TCP synwait 時間を 10 秒に設定するためにルータに配信される設定は次のとおりです。

```
ip tcp synwait-time <10>
```

ロギングが有効（Enable Logging）

Cisco CP Express は、可能な場合はいつでも、タイム スタンプとシーケンス番号を使用したロギングを有効にします。ロギングはネットワーク イベントに関する詳細情報を提供することから、セキュリティ イベントの認識と応答に不可欠です。タイム スタンプとシーケンス番号は、ネットワーク イベントが発生した日付、時刻、および順序に関する情報を提供します。

ロギングを有効にして設定するためにルータに配信される設定は次のとおりです。*<log buffer size>* と *<logging server ip address>* は、Cisco CP Express に入力された値に置き換えられます。

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

すべての外部インターフェイスに対するユニキャスト RPF が有効（Enable Unicast RPF on All Outside Interfaces）

Cisco CP Express は、可能な場合はいつでも、インターネットに接続するすべてのインターフェイス上でユニキャスト Reverse Path Forwarding（RPF）を有効にします。RPF は、ルータに、パケットが到着したインターフェイスに照らしてすべてのパケットの送信元アドレスをチェックさせる機能です。ルーティング テーブルに照らして、入力インターフェイスが送信元アドレスへのパスとして不適切な場合は、パケットがドロップされます。この送信元アドレス検証は、IP スプーフィングを阻止するために使用されます。

この機能は、ルーティングが対称型の場合にのみ動作します。ネットワークが、ホスト A からホスト B へのトラフィックが辿るパスとホスト B からホスト A へのトラフィックが辿るパスが異なるように設計されている場合は、必ず、チェックが失敗し、2 台のホスト間の通信ができなくなります。この種の非対称ルーティングは、インターネット コアでは一般的です。この機能を有効にする前に、ネットワークで非対称ルーティングが使用されていないことを確認してください。

加えて、ユニキャスト RPF は、IP Cisco Express Forwarding が有効になっている場合にしか有効にすることができません。Cisco CP Express は、ルータの設定をチェックして、IP Cisco Express Forwarding が有効になっているかどうかを確認します。IP Cisco Express Forwarding が有効になっていない場合は、Cisco CP Express が IP Cisco Express Forwarding を有効にするように推奨し、その推奨が受け入れられた場合に有効にします。IP Cisco Express Forwarding が Cisco CP Express または別の方法で有効になっていない場合は、ユニキャスト RPF が有効になりません。

ユニキャスト RPF を有効にするために、次の設定が、プライベート ネットワークの外部に接続されているインターフェイスごとにルータに配信されます。<*outside interface*> はインターフェイス識別子に置き換えられます。

```
interface <outside interface>
ip verify unicast reverse-path
```

IP Gratuitous ARP が無効（Disable IP Gratuitous ARPs）

Cisco CP Express は、可能な場合はいつでも、IP gratuitous Address Resolution Protocol（ARP; アドレス解決プロトコル）要求を無効にします。不当 ARP とは、送信元と宛先の MAC アドレスが同じ ARP ブロードキャストのことです。このような ARP は、主に、ホストがその IP アドレスをネットワークに通知する

ときに使用されます。スプーフィングされた不当 ARP メッセージは、ネットワーク マッピング情報を不正に保存することによって、ネットワーク障害を引き起こすおそれがあります。

不当 ARP を無効にするために、次の設定がルータに配信されます。

```
no ip gratuitous-arps
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP リダイレクトが無効（Disable IP Redirects）

Cisco CP Express は、可能な場合はいつでも、Internet Message Control Protocol（ICMP; インターネット コントロール メッセージ プロトコル）リダイレクト メッセージを無効にします。ICMP は、パス、ルート、およびネットワークの状態に関する情報を中継することによって、IP トラフィックをサポートします。ICMP リダイレクト メッセージは、エンド ノードに、特別な宛先へのパスとして特定のルータを使用するように指示します。正常に機能している IP ネットワークでは、ルータは自分が所属するローカル サブネット上のホストにしかリダイレクトを送信しないうえ、どのエンド ノードもリダイレクトを送信しないため、リダイレクトが複数のネットワーク ホップを通過することはありません。ただし、攻撃者はこのようなルールを破ることができます。事実、一部の攻撃はこれに基づいています。ICMP リダイレクトを無効にすると、ネットワークに影響を及ぼすことができなくなり、この種の攻撃方法が排除されます。

ICMP リダイレクト メッセージを無効にするためにルータに配信される設定は次のとおりです。

```
no ip redirects
```

IP Proxy ARP が無効（Disable IP Proxy ARP）

Cisco CP Express は、可能な場合はいつでも、プロキシ ARP を無効にします。ARP は、ネットワーク上で IP アドレスを MAC アドレスに変換するために使用されます。通常、ARP は単一の LAN に限定されますが、ルータが ARP 要求のプロキシとして機能することによって、ARP クエリーを複数の LAN セグメント

全体で使用可能にできます。プロキシ ARP は LAN のセキュリティ バリアを越えるため、セキュリティ レベルが同じ 2 つの LAN の間で必要な場合にだけ使用するようにしてください。

プロキシ ARP を無効にするためにルータに配信される設定は次のとおりです。

```
no ip proxy-arp
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP ダイレクト ブロードキャストが無効（Disable IP Directed Broadcast）

Cisco CP Express は、可能な場合はいつでも、IP ダイレクト ブロードキャストを無効にします。IP ダイレクト ブロードキャストは、送信マシンが直接接続されていないサブネットのブロードキャスト アドレスに送信されるデータグラムです。ダイレクト ブロードキャストは、ネットワーク上をユニキャスト パケットとして転送され、ターゲット サブネットに到着します。そこで、リンク層ブロードキャストに変換されます。IP アドレッシング アーキテクチャの特性により、ターゲット サブネットに直接接続された、チェーン内の最後のルータのみが、ダイレクト ブロードキャストを確定できます。ダイレクト ブロードキャストが正当な目的で使用されることもありますが、このような使用は金融サービス業界以外ではあまり見られません。

IP ダイレクト ブロードキャストは、よく見かける「集中」DoS 攻撃や関連する攻撃にも使用されます。「集中」攻撃では、攻撃者が、ICMP エコー要求を嘘の送信元アドレスからダイレクト ブロードキャスト アドレスに送信することによって、ターゲット サブネット上のすべてのホストが嘘の送信元に応答を返すことになります。このような要求の連続ストリームを送信することによって、攻撃者は、アドレスが偽装されたホストを完全にダウンさせるほど大量の応答ストリームを発生させることができます。

IP ダイレクト ブロードキャストを無効にすると、そうしなかった場合に、インターフェイスのリンク層ブロードキャストに発展しかねないダイレクト ブロードキャストがドロップされます。

IP ダイレクト ブロードキャストを無効にするためにルータに配信される設定は次のとおりです。

```
no ip directed-broadcast
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

MOP サービスが無効（Disable MOP Service）

Cisco CP Express は、可能な場合はいつでも、すべてのイーサネット インターフェイス上の Maintenance Operations Protocol（MOP）を無効にします。MOP は、DECNet ネットワークとの通信時に設定情報をルータに提供するために使用されます。MOP はさまざまな攻撃に対して脆弱です。

イーサネット インターフェイス上で MOP サービスを無効にするためにルータに配信される設定は次のとおりです。

```
no mop enabled
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP アンリーチャブルが無効（Disable IP Unreachables）

Cisco CP Express は、可能な場合はいつでも、ICMP ホスト到達不能メッセージを無効にします。ICMP は、パス、ルート、およびネットワークの状態に関する情報を中継することによって、IP トラフィックをサポートします。ICMP ホスト到達不能メッセージは、ルータが、未知のプロトコルを使用している非ブロードキャスト パケットを受信した場合、または、ルータが、宛先アドレスまでのルートが不明なために最終目的地に配信できないパケットを受信した場合に送出されます。このメッセージは、攻撃者がネットワーク マッピング情報を取得するために使用されるおそれがあります。

ICMP ホスト到達不能メッセージを無効にするためにルータに配信される設定は次のとおりです。

```
int <all-interfaces>
no ip unreachables
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

IP マスク応答が無効（Disable IP Mask Reply）

Cisco CP Express は、可能な場合はいつでも、ICMP マスク応答メッセージを無効にします。ICMP は、パス、ルート、およびネットワークの状態に関する情報を中継することによって、IP トラフィックをサポートします。ICMP マスク応答メッセージは、ネットワーク デバイスが、インターネットワーク内の特定のサブネットワークに関するサブネット マスクを認識している必要がある場合に送信されます。また、ICMP マスク応答メッセージは、要求された情報を持っているデバイスから、情報を要求したデバイスに送信されます。このメッセージは、攻撃者がネットワーク マッピング情報を取得するために使用されるおそれがあります。

ICMP マスク応答メッセージを無効にするためにルータに配信される設定は次のとおりです。

```
no ip mask-reply
```

Cisco CP のセキュリティ監査機能を使用して、この修正を取り消すことができます。やり方については、Cisco CP のセキュリティ監査に関するオンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」をクリックしてください。

パスワードの最小文字数を 6 文字以上に設定（Set Minimum Password Length to Less Than 6 Characters）

Cisco CP Express は、可能な場合はいつでも、6 文字以上のパスワードを要求するようにルータを設定します。攻撃者がパスワードを盗むために使用する方法の 1 つは、パスワードが見つかるまで可能性のあるすべての文字の組み合わせを試すという方法です。パスワードが長いほど、可能性のある文字の組み合わせが急激に増加するため、この種の攻撃がより困難になります。

この設定変更では、ユーザ、Enable Secret、コンソール、AUX、tty、vty などのルータ上のパスワードをすべて 6 文字以上にする必要があります。この設定変更は、ルータ上で実行している Cisco IOS のバージョンが最小パスワード長機能をサポートしている場合にのみ実施されます。

ルータに配信される設定は次のとおりです。

```
security passwords min-length <6>
```

認証失敗率を再試行回数 3 回未満に設定（Set Authentication Failure Rate to Less Than 3 Retries）

Cisco CP Express は、可能な場合はいつでも、ログインの試みが 3 回失敗したらアクセスをロックするようにルータを設定します。「辞書」攻撃と呼ばれるパスワードを盗むための方法の 1 つは、辞書内のすべての単語を使用してログインを試みるソフトウェアを使用する方法です。この設定では、ログイン試行に 3 回失敗すると、ルータへのアクセスが 15 秒間ロックされ、辞書攻撃ができなくなります。ルータへのアクセスをロックすることに加えて、この設定では、ログイン試行が 3 回失敗すると、ログ メッセージが生成され、失敗したログイン試行が管理者に報告されます。

ログイン試行が 3 回失敗したらルータ アクセスをロックするためにルータに配信される設定は次のとおりです。

```
security authentication failure rate <3>
```

バナーの設定（Set Banner）

Cisco CP Express は、可能な場合はいつでも、テキスト バナーを設定します。一部の管轄区では、実際には利用が許可されていない無許可ユーザを示すバナーを提供すれば、システムに侵入したユーザの民事または刑事訴訟が非常に簡単になります。それ以外の管轄区では、自分の意志を通知する手段を講じていなければ、たとえ無許可ユーザであってもその活動をモニタすることが許可されない場合があります。テキスト バナーは、この通知を実行する方法の 1 つです。

テキスト バナーを作成するためにルータに配信される設定は次のとおりです。*<company name>*、*<administrator email address>*、および *<administrator phone number>* は、Cisco CP Express に入力された値に置き換えられます。

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Telnet 設定が有効（Enable Telnet Settings）

Cisco CP Express は、可能な場合はいつでも、次の設定を実行することによって、コンソール、AUX、vty、および tty 回線を保護します。

- **tansport input** コマンドと **transport output** コマンドを設定して、これらの回線への接続に使用可能なプロトコルを定義する。
- コンソール回線と AUX 回線上の exec-timeout 値を 10 分に設定して、管理ユーザが 10 分間何も操作をしなければ、これらの回線からログアウトされるようにする。

コンソール、AUX、vty、および tty 回線を保護するためにルータに配信される設定は次のとおりです。

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

ルータ アクセスに対する SSH が有効（Enable SSH for Access to the Router）

ルータ上で実行している Cisco IOS リリースが機密イメージ（56 ビット Data Encryption Standard（DES; データ暗号化規格）暗号化を使用し、輸出規制がかけられているイメージ）の場合は、Cisco CP Express が、可能な場合はいつでも、次の設定を実行して Telnet アクセスを保護します。

- Telnet アクセス用の Secure Shell（SSH; セキュア シェル）を有効にする。SSH は Telnet アクセスの安全性を非常に高めます。
- SSH タイムアウト値を 60 秒に設定して、60 秒後に完了していない SSH 接続をシャットダウンする。
- ルータへのアクセスをロックする SSH ログインの失敗回数を 2 に設定する。

アクセス機能とファイル転送機能を保護するためにルータに配信される設定は次のとおりです。

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Cisco CP Express のボタン

[ヘルプ（Help）] ボタン

クリックすると、新しいブラウザ ウィンドウが開いて、表示されている Cisco CP Express ウィンドウに関する情報が表示されます。

[バージョン情報（About）] ボタン

[バージョン情報（About）] をクリックすると、Cisco CP Express バージョン情報を含むウィンドウが表示されます。このウィンドウで [ハードウェアの詳細（Hardware Details）] と [ソフトウェアの詳細（Software Details）] をクリックすると、次の情報が表示されます。

[ハードウェアの詳細（Hardware Details）]：

- ルータ モデル タイプ
- ルータ内のメモリの合計
- ルータ内のフラッシュの合計容量
- ルータの起動元（フラッシュなど）

ハードウェア設定図も表示されます。

[ソフトウェアの詳細（Software Details）]：

- ルータが実行している Cisco IOS ソフトウェアの名前
- Cisco IOS ソフトウェアのリリース
- ファイアウォールや VPN などの Cisco IOS ソフトウェアがサポートしているフィーチャ セット
- Cisco CP Express のバージョン

[終了（Exit）] ボタン

初期設定を完了したら、[終了（Exit）] をクリックして Cisco CP Express を閉じます。

[更新（Refresh）] ボタン

初期設定を編集中に表示されます。[更新（Refresh）] をクリックすると、Cisco CP Express 内のルータ データが更新されます。

[変更の適用（Apply Changes）] ボタン

初期設定を編集中に表示されます。[変更の適用（Apply Changes）] をクリックすると、ルータに対する変更が配信されます。

[変更の破棄（Discard Changes）] ボタン

初期設定を編集中に表示されます。[変更の破棄（Discard Changes）] をクリックすると、加えた変更のウィンドウがクリアされます。

初期設定後のルータへの再接続

ルータの LAN インターフェイスに、推奨されている新しい IP アドレスを設定した場合は、設定の配信後にルータへの接続が失われます。

Cisco CP Express を使用した初期設定後にルータに再接続するには、次の手順を実行します。

ステップ 1　ルータの LAN インターフェイスと同じサブネット上に PC を配置します。

- ルータを DHCP サーバとして設定した場合は、IP アドレスを自動的に取得するように PC を設定してから、コマンド ウィンドウを開いて、**ipconfig /release** コマンドの次に **ipconfig /renew** コマンドを入力します。
- ルータが DHCP サーバとして設定されていない場合は、PC にルータと同じサブネット内のスタティック IP アドレスを設定する必要があります。たとえば、255.255.255.224 のサブネット マスクを使用して LAN の IP アドレスを 10.20.20.1 に変更した場合は、PC に 10.20.20.2 ～ 10.20.20.30 の IP アドレスを設定し、同じサブネット値を使用します。

ステップ 2　デフォルト インターフェイスとは異なる LAN インターフェイスを設定した場合は、PC が、設定した LAN インターフェイスに接続されていることを確認します。たとえば、LAN インターフェイスとして FE 0/0 ではなく、FE 0/1 を設定した場合は、PC が FE 0/1 に接続されていることを確認します。

ステップ 3　PC の準備が完了したら、ルータの LAN インターフェイスに設定した新しい IP アドレスをブラウザに入力する（http:// *新しい IP アドレス*）ことによって、PC をルータに再接続します。たとえば、LAN の IP アドレスを 10.20.20.1 に変更した場合は、Web ブラウザに「http://10.20.20.1」と入力してルータに再接続します。

ステップ 4　再接続後は、WAN 接続をテストして、インターネットに接続できることを確認します。

詳細については、「WAN（インターネット）接続のテスト」をクリックしてください。

WAN（インターネット）接続のテスト

インターネットへの接続は、ブラウザでリモート Web サイト（www.cisco.com など）にアクセスすることによってテストできます。入力したリモート Web サイトに接続できれば、WAN 設定が正しく機能しています。

リモート Web サイトに接続できなかった場合は、Cisco CP を使用して、次の手順を実行し、接続の問題を解決できます。

ステップ 1　[ツール（Tools）] メニューで **Cisco CP** をクリックして、Cisco CP を起動します。

ステップ 2　Cisco CP にログインして、[インターフェイスと接続（Interfaces and Connections）] をクリックします。

ステップ 3　[編集（Edit）] タブをクリックして、テストする WAN 接続を選択します。

ステップ 4　[接続のテスト（Test Connection）] をクリックして、表示された指示に従います。Cisco CP は、可能性のある問題を報告して、対策を推奨します。

SDP トラブルシューティングのヒント

この情報は、Secure Device Provisioning（SDP）の使用を登録する前に、ルータと証明書サーバ間の接続を準備するために使用します。登録中に問題が発生した場合は、これらのタスクを見直すことによって、問題の場所を特定できます。

SDP が起動したら、このヘルプ トピックが表示されているブラウザ ウィンドウを最小化しないと、SDP Web アプリケーションが表示できません。

トラブルシューティングのヒント

これらの推奨事項には、ローカル ルータと Certificate Authority（CA; 認証機関）サーバ上の準備も含まれています。これらの要件を CA サーバの管理者に伝える必要があります。次の状態を確認してください。

- ローカル ルータと CA サーバが IP 接続されている。ローカル ルータは証明書サーバを問題なく ping できる必要があり、証明書サーバはローカル ルータを問題なく ping できる必要があります。
- CA サーバの管理者が使用している Web ブラウザで JavaScript がサポートされている。
- CA サーバの管理者がローカル ルータに対して有効な権限を持っている。
- ローカル ルータ上のファイアウォールが証明書サーバとやり取りされるトラフィックを許可している。
- ファイアウォールがペティショナまたはレジスタラ上で設定されている場合は、そのファイアウォールが、SDP を呼び出した PC からの HTTP または HTTPS トラフィックを許可することを保証する必要があります。

SDP の詳細については、次の Web ページを参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html