CHAPTER 1

Cisco CP Express ウィザード

このヘルプ トピックでは、Cisco Configuration Professional Express（Cisco CP Express）ウィザードの概要を示し、このウィザードで実行できる設定と各 Cisco CP Express 画面で必要となる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。

はじめに

Cisco CP Express のウィンドウに表示される指示に従って、ルータの初期設定を行うことができます。Cisco CP Express では、ルータの以下の設定を指定できます。

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

Cisco CP Express ウィザードを完了して設定をルータに転送した後でも、必要に応じて、引き続き Cisco CP Express を使用して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、次の 3 つのタイプのウィンドウがあります。

- 概要画面 — このウィンドウにはルータの基本情報のスナップショットが表示され、設定画面を入力しなくても一目で情報を確認することができます。
- ウィザード画面 — Cisco CP Express を初めて実行したときは、ウィザード画面を使用します。ウィザード画面の指示に従ってルータの基本設定を完了すると、ネットワークでルータの使用を開始できるようになります。基本設定には、ルータとそのルータが機能する LAN を保護するためのファイアウォールとセキュリティ設定も含まれています。各画面の左側のペインには、現在作業中の設定が表示されます。右側のペインには、各設定フィールドが表示されます。それぞれの画面の詳細を確認するには、画面上部の疑問符（?）のアイコンをクリックしてください。
- 編集画面 — 初期設定の完了後に、必要に応じて Cisco CP Express に戻ってルータの設定を変更することができます。

Cisco CP Express と CCP

Cisco CP Express では、ネットワークでルータを機能させるための基本設定を行うことができます。Cisco Configuration Professional（CCP）では、仮想プライベート ネットワーク（VPN）設定、侵入防止システム（IPS）設定、ネットワークなどのより詳細な設定を行えます。CCP が PC にインストールされている場合は、PC 上で CCP を起動し、設定対象のルータの IP アドレスを指定します。

画面のリファレンス

次の各トピックでは、ルータ情報を参照するときと、Cisco CP Express の使用を開始するときに使用する次の画面およびダイアログ ボックスについて説明します。

- ようこそ
- 概要

ようこそ

このウィザードの指示に従うと、次の操作に必要な基本設定を行うことができます。

- ルータに名前を付ける。
- 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ルータを手動で設定できます。また、USB トークンまたは USB フラッシュ デバイスからロードしたコンフィギュレーション ファイルや、Secure Device Provisioning（SDP）、または Cisco Network Services を使用してルータをプロビジョニングできます（使用している Cisco IOS リリースでこれらがサポートされている場合）。

  Cisco Network Services を使用してルータを設定すると、ルータをサーバに接続させ、そのルータの設定を取得する働きをする Cisco Network Services パラメータを指定できます。
- 出荷時のデフォルトの LAN IP アドレスを変更する。

  ルータのプロビジョニングで SDP または Cisco Network Services が選択されると、このタスクは行われません。

- LAN 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で SDP または Cisco Network Services が選択されると、このタスクは行われません。
- DNS サーバとドメイン名を設定する。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 プロバイダにお問い合わせください。

  ルータのプロビジョニングで SDP または Cisco Network Services が選択されると、このタスクは行われません。
- WAN 接続を作成する。
- LAN および WAN 接続のファイアウォールを作成する。
- 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行う。

追加インタフェースの設定や、より詳細な設定を行うには、CCP 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、ルータ名の指定、ユーザ アカウントとパスワードの作成、および enable secret パスワードの作成を行います。詳細については、次のセクションを参照してください。

- 基本設定のリファレンス

基本設定のリファレンス

次のトピックでは、［基本設定］画面について説明します。

- 基本設定

基本設定

［基本設定］ウィンドウでは、設定する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（CCP）、およびコマンドライン インターフェイス（CLI）へのアクセスを制御したりできます。

ホスト名

ルータに付ける名前を入力します。

ドメイン名

組織のドメイン名を入力します。ドメイン名の例として *cisco.com* を挙げることができますが、これとは異なるサフィックス（*.org* や *.net* など）が付くドメイン名を指定することもできます。

ユーザ名 / パスワード

Cisco CP Express ユーザおよび Telnet ユーザのユーザ名とパスワードを設定する必要があります。

（注）　次回以降に Cisco CP Express を使用する際には、このウィンドウで設定したユーザ名とパスワードを使用します（設定を変更しない場合）。他の人に推測されにくく、自分では思い出しやすいパスワードを設定してください。

ユーザ名

ユーザ名を入力します。

新しいパスワードの入力

新しいパスワードを入力します。パスワードは 6 文字以上でなければなりません。

新しいパスワードの再入力

確認のため、新しいパスワードを再入力します。

Enable Secret パスワード

enable secret パスワードは、Telnet またはコンソール ポートを使用してルータにアクセスするユーザに対して、特権 EXEC モードへのアクセスを許可するかどうかを制御します。特権 EXEC モードでは、設定を変更したり、このモード以外では利用できない他のコマンドを実行したりできます。パスワード入力 のフィールドに enable secret パスワードを入力します。確認のため、［新しいパスワードの再入力］フィールドに同じパスワードをもう一度入力してください。パスワードは 6 文字以上でなければなりません。

（注）　enable secret パスワードは、自分では思い出しやすく、他の人に推測されにくいものを選択してください。パスワードは暗号化されて格納されるため、コンフィギュレーション ファイルを表示しても読むことはできません。

ルータのプロビジョニング

Cisco CP Express を使用して、ネットワーク サーバや、USB フラッシュ デバイスまたはトークンからコンフィギュレーション ファイルを取得して、ルータのメモリにロードすることができます。

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

ルータのプロビジョニング

このウィンドウでは、ルータのプロビジョニングに使用できるオプションが表示されます。一部のオプションは、Cisco IOS リリースによってサポートされている場合のみ表示されます。

Cisco CP Express

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には、このオプションを選択します。

USB トークンまたは USB フラッシュ

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、そのトークンまたはフラッシュ デバイスに適切なコンフィギュレーション ファイルが格納されている場合は、このオプションを選択します。

（注）　USB トークンと USB フラッシュ デバイスが両方ともルータに接続されている場合は、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、すべての USB トークンをルータから外してから Cisco CP Express を実行してください。

Secure Device Provisioning

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

次の点を確認してから、SDP オプションを選択してください。

- ルータと SDP サーバ間が IP 接続可能である。
- Web ブラウザが JavaScript をサポートしている。

SDP を選択した場合、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 ウィンドウでは、SDP でルータをプロビジョニングするウィザードが表示されます。

SDP の詳細については、次のサイトを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

CNS サーバ

サービス プロバイダから 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」を参照してください。

USB トークンからのプロビジョニング

このウィンドウでは、ルータに接続されている USB トークンからロードした 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 トークンにロードできるブート 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のみ表示されます。USB トークンと USB フラッシュ デバイスが両方ともルータに接続されている場合は、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、すべての USB トークンをルータから外してから Cisco CP Express を実行してください。

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すると、このファイルが現在の設定とマージされ、スタートアップ コンフィギュレーションの一部になります。

注意 CCP は、ルータのプロビジョニング時に使用するコンフィギュレーション ファイルが有効なものかをチェックしません。使用するコンフィギュレーション ファイルに記述されている設定内容が適切であ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、次の手順に従ってください。

ステップ 1　［トークン名］ドロップダウン メニューから USB トークン名を選択します。

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 を指定してください］を選択し、［トークンの PIN］フィールドに PIN を入力します。

［デバイスとデフォルトの PIN を指定してください］を選択すると、USB トークンへのログイン時にデフォルトの PIN 1234567890 が使用されます。

ステップ 3　［ログイン］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い場合、ルータは USB トークンからプロビジョニングされません。［戻る］ボタンをクリックして、別のルータのプロビジョニング方法を選択します。

ステップ 4　［CCCD のプレビュー］をクリックします。CCCD ファイルの内容が下部のペインに表示されます。

USB フラッシュからのプロビジョニング

このウィンドウでは、ルータに接続されている USB フラッシュ デバイスからロードし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、ルータに USB フラッシュ デバイスが接続されている場合のみ表示されます。

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すると、このファイルが現在の設定とマージされ、スタートアップ コンフィギュレーションの一部になります。

注意　CCP は、ルータのプロビジョニング時に使用するコンフィギュレーション ファイルが有効なものかをチェックしません。使用するコンフィギュレーション ファイルのデータが適切であ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、次の手順に従ってください。

ステップ 1　［ファイル名］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 パスで入力します。または、［参照］をクリックしてファイル選択ウィンドウを開きます。

拡張子が .cfg のファイル、または名前が CCCD のファイルを選択してください。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］をクリックします。選択したファイルの内容が下部のペインに表示されます。

ファイルの選択

このウィンドウでは、ルータからファイルをロードできます。このウィンドウで表示できるのは DOSFS ファイル システムだけです。

ウィンドウの左側には、拡張可能なツリーが表示されます。このツリーは、Cisco ルータのフラッシュ メモリおよびそのルータに接続されている USB デバイスにあるディレクトリ システムを表します。

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内にあるファイルおよびディレクトリの名前のリストが表示されます。また、各ファイルのサイズ（バイト単位）と、各ファイルおよびディレクトリの最終修正日時も表示されます。

ウィンドウの右側に表示されたリストで、ロードするファイルを選択できます。ファイル リストの下にある［ファイル名］フィールドには、指定したファイルのフル パスが表示されます。

（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 ファイルには、CCCD ファイルまたは拡張子が .cfg のファイルを選択してください。

名前

ファイルとディレクトリを名前のアルファベット順に並べ替える場合は、［名前］をクリックします。［名前］をもう一度クリックすると、順序が逆になります。

サイズ（バイト）

ファイルとディレクトリをサイズ順に並べ替える場合は、［サイズ（バイト）］をクリックします。ディレクトリのサイズは、空でなくても常にゼロ バイトと表示されます。［サイズ （バイト）］をもう一度クリックすると、順序が逆になります。

修正時刻

ファイルとディレクトリを修正日時の順に並べ替える場合は、［修正日時］をクリックします。［修正日時］をもう一度クリックすると、順序が逆になります。

CNS サーバ情報

このウィンドウは、WAN 接続を設定し、Cisco Network Services オプションを使用したルータのプロビジョニングを選択した場合に表示されます。このウィンドウでは、サービス プロバイダから提供された Cisco Network Services サーバ情報を入力します。Cisco CP Express がルータの設定情報を取得できるように、Cisco Network Services サーバの IP アドレスとログイン情報を入力してください。

CNS サーバの IP アドレス / ホスト名の入力

ネットワーク上の Cisco Network Services サーバの IP アドレスまたはホスト名を入力します。ホスト名を入力する場合は、ホスト名を IP アドレスに解決できる DNS サーバの IP アドレスを指定する必要があります。

CNS ID 文字列の入力

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に必要なデバイス ID を入力します。

CNS パスワードの入力

入力したユーザ ID で Cisco Network Services サーバにログインする際に使用するパスワードを入力します。

プライマリ DNS

ルータで使用するプライマリ DNS 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 プロバイダから提供されます。

プライマリ DNS サーバは、ルータが IP アドレスを解決するときに最初に接続するサーバです。

（注） ［CNS サーバ IP アドレス / ホスト名の入力］フィールドで Cisco Network Services を識別するためのホスト名を入力する場合、［プライマリ DNS］フィールドで 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

ルータで使用するセカンダリ DNS 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 プロバイダから提供されます。

セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合にルータが接続するサーバです。

ワイヤレス インターフェイスの設定

Cisco CP Express では、ルータのワイヤレス インターフェイスとルータの LAN インターフェイス間のブリッジを設定できます。また、Cisco CP Express からワイヤレス管理アプリケーションを起動することもできます。

次のトピックでは、［ワイヤレス インターフェイスの設定］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

ワイヤレス インターフェイスの設定

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］をクリックします。Cisco CP Express によって、ワイヤレス トラフィックを LAN インターフェイスへブリッジするようにルータが設定されます。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］をクリックします。［いいえ］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、ワイヤレス インターフェイスを 1 つ設定できます。ルータ上に他のワイヤレス インターフェイスがある場合は、ワイヤレス アプリケーションを使用して設定できます。

LAN インターフェイスの設定

Cisco CP Express ウィザードでは、IP アドレスを指定して LAN インターフェイスを設定した後、そのインターフェイスを DHCP サーバとして指定し、その DHCP サーバが使用する IP アドレスの範囲を指定できます。

次の各トピックでは、LAN インターフェイスの画面について説明します。

- LAN インターフェイスの設定
- DHCP サーバの設定

LAN インターフェイスの設定

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 ウィザードを完了した後で 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場合は、Cisco CP Express を再起動し、［LAN］をクリックして必要なアドレスを編集します。

インターフェイス / ブリッジ間インターフェイス リスト

ルータに複数の LAN インターフェイスがある場合は、このリストに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あり、［ワイヤレス インターフェイスの設定］ウィンドウで［はい］をクリックした場合、このリストには［ブリッジ間インターフェイス］というラベルが表示されます。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

LAN インターフェイスの IP アドレスをドット（.）で区切った 10 進表記で入力します。ネットワーク アドレス変換（NAT）またはポート アドレス変換（PAT）を使用する場合は、プライベート IP アドレスを指定できます。

（注）　このアドレスを書き留めておいてください。Cisco CP Express ウィザードを終了してルータを再起動したら、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』に記載されているアドレスを使用しないでください。

サブネット マスク

ネットワークのサブネット マスクを入力します。この値については、ネットワーク管理者またはサービス プロバイダに確認してください。サブネット マスクを指定すると、IP アドレスのうち、ネットワーク部およびサブネット部を定義するために何ビットが使用されているかをルータが判断できるようになります。サブネット マスクの値によって、このルータが接続される LAN 上に配置できるホスト数も決まります。

サブネット ビット

サブネット マスクの代わりに、IP アドレスのネットワークおよびサブネット部の定義に使用す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 プロバイダに確認してください。

ワイヤレス パラメータ

初期設定時、ルータにワイヤレス インターフェイスがあり、[ワイヤレス インターフェイスの設定] ウィンドウで [はい] をクリックした場合、これらのフィールドが表示されます。設定を編集する場合、初期設定時にワイヤレス設定を行うと、これらのフィールドが表示されます。この LAN インターフェイスにワイヤレス トラフィックがブリッジされます。

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 ネットワーク デバイスでワイヤレス接続を確立して維持するときに使用する一意の識別子です。

（注）　設定された SSID 値を変更すると、ワイヤレス接続が切断されます。

Cisco CP Express ウィザードの終了後に LAN 設定を編集し、詳細なワイヤレス 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］をクリックします。

変更 / 変更の適用 / 変更の破棄ボタン

初期設定の編集時に表示されます。詳細については、「Cisco CP Express のボタン」を参照してください。

DHCP サーバの設定

DHCP は、スタティック アドレス指定が必要ない場合に使用する簡単なアドレス指定形式です。DHCP は、ホストがネットワークに接続されると IP アドレスを一定時間ダイナミックに割り当てます。この方法では、ホストで IP アドレスが不要になると、そのアドレスを再利用することができます。内部ネットワークのリソース（PC など）にアドレスを割り当てるには、DHCP を使用してください。

LAN インターフェイスに対して DHCP サーバを有効にするチェック ボックス

このチェック ボックスを選択すると、ルータは LAN 上のデバイスにプライベート IP アドレスを割り当てることができます。このウィンドウで DHCP サーバを有効にすると、IP アドレスはホストに 1 日リースされます。このチェック ボックスを選択した場合は、［開始 IP アドレス］フィールドと［終了 IP アドレス］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

LAN インターフェイスに設定した IP アドレスとサブネット マスクに基づいて、Cisco CP Express によってこのフィールドに IP アドレス範囲の最小アドレスが入力されます。DHCP アドレス プールを小さくする場合は大きいアドレスに変更できますが、LAN インターフェイスのアドレスと同じサブネット内のアドレスを入力する必要があります。そうでないと、アドレスが無効であることを通知するメッセージが表示されます。

終了 IP アドレス

LAN インターフェイスに設定した IP アドレスとサブネット マスクに基づいて、Cisco CP Express によってこのフィールドに IP アドレス範囲の最大有効アドレスが入力されます。DHCP アドレス プールを小さくする場合は小さいアドレスに変更できますが、LAN インターフェイスのアドレスと同じサブネット内のアドレスを入力する必要があります。そうでないと、アドレスが無効であることを通知するメッセージが表示されます。

ドメイン名

初期設定を完了すると表示されます。組織のドメイン名を入力します。ドメイン名の例として *cisco.com* を挙げることができますが、これとは異なるサフィックス（*.org* や *.net* など）が付くドメイン名を指定することもできます。

すべての DHCP オプションを DHCP サーバ データベースにインポートするチェック ボックス

初期設定を完了すると表示されます。DHCP オプション パラメータを DHCP サーバのデータベースにインポートし、LAN 上の DHCP クライアントが IP アドレスを要求したときにこの情報も送信する場合は、このオプションをクリックします。

プライマリ DNS

ルータで使用するプライマリ 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 プロバイダから提供されます。

プライマリ DNS サーバは、ルータが IP アドレスを解決するときに最初に接続するサーバです。

セカンダリ DNS

ルータで使用するセカンダリ DNS サーバ（利用可能な場合）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 プロバイダから提供されます。

セカンダリ DNS サーバは、プライマリ DNS サーバが利用できない場合にルータが接続するサーバです。

これらの DNS 値を DHCP クライアントに使用するチェック ボックス

このチェック ボックスは、LAN インターフェイス上で DHCP サーバが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は、このチェック ボックスを選択します。

変更 / 変更の適用 / 変更の破棄ボタン

初期設定の編集時に表示されます。詳細については、「Cisco CP Express のボタン」を参照してください。

ワイヤレス アクセス ポイントの設定

ワイヤレス アクセス ポイントがルータに組み込まれている場合は、Cisco CP Express ウィザードを使用してそのアクセス ポイントを設定できます。Cisco CP Express によりアクセス ポイント ハードウェアが検出され、対応する設定画面が表示されます。

次の各トピックでは、ワイヤレス アクセス ポイントの設定画面について説明します。

- Autonomous ワイヤレス設定
- Wireless-LWAPP ホスト ルータの設定

Autonomous ワイヤレス設定

ルータのアクセス ポイント コントローラに Autonomous ワイヤレス設定をサポートするイメージがインストールされている場合は、[Autonomous ワイヤレス設定] 画面が表示されます。

フィールド リファレンス

表 1-1　Autonomous ワイヤレス設定

要素	説明
Autonomous ワイヤレス設定	アクセス ポイント コントローラを Autonomous モードで動作するように設定するには、[Autonomous ワイヤレス設定] を選択します。 **（注）** このフィールドは、Cisco CP Express ウィザードの使用時に表示されます。
ホスト名	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（たとえば、800-accesspoint）。
パスワードおよび確認	アクセス ポイント コントローラに設定するパスワードを入力し、その後、間違いがないか確認するため同じパスワードを再入力します。

表 1-1　Autonomous ワイヤレス設定（続き）

要素	説明
スタティック IP アドレス フィールド	IP アドレス リストからスタティック IP アドレスを選択すると、[IP アドレス] フィールドと［サブネット マスク］フィールドが表示されます。
IP アドレス	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割り当てる IP アドレスを入力します。この IP アドレスは使用するサブネット マスクに対して有効なものでなければなりません。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、192.168.0.1 ～ 192.168.0.6 の範囲に含まれる IP アドレスを使用する必要があります。
サブネット マスクとサブネット ビット	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］フィールドにマスクを入力するか、または［サブネット ビット] フィールドでサブネット ビット数を選択します。サブネット ビット数を選択すると、マスクが自動的に入力されます。たとえば、［サブネット ビット］フィールドで 29 を選択すると、［サブネット マスク］フィールドに 255.255.255.248 という値が自動的に入力されます。
ダイナミック IP アドレス フィールド	IP アドレス リストでダイナミック IP アドレスを選択すると、［ホスト名］フィールドが表示されます。
ホスト名	インターネット サービス プロバイダ（ISP）から DHCP サーバ名を通知されている場合は、［ホスト名］フィールドにその名前を入力します。
IP アドレスなし	IP アドレス リストで［IP アドレスなし］を選択すると、ルータのインターフェイスで IP アドレスは設定されず、[IP アドレス］ボックスにフィールドは何も表示されません。
SSID および暗号化フィールド	コントローラの設定で既存の SSID が検出されなかった場合、［SSID］フィールドと［暗号化］フィールドが表示されます。

表 1-1　Autonomous ワイヤレス設定（続き）

要素	説明
SSID	Service Set Identifier（SSID）は、無線 SSID とも呼ばれ、アクセス ポイントの無線に関連付けるためにクライアントで使用される一意の識別子です。SSID は、2 ～ 32 文字の任意の英数字（大文字 / 小文字の区別あり）で構成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	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。 • WEP — WEP（Wired Equivalent Privacy）は、802.11 標準暗号化アルゴリズムで、元来は有線 LAN でのプライバシー レベルを設定するために設計されたものです。この標準では、40 ビットまたは 104 ビット のサイズの WEP ベース キーが定義されています。 • WPA — WPA（Wi-Fi Protected Access）は、認証サーバのサービスを介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強力なアルゴリズムを使用してそのユーザの IP トラフィックを暗号化します。
キー	アクセス ポイントで暗号化に使用するキーを入力します。
詳細設定に関する注意	
注意:内部アクセスポイントの詳細設定について ...	Cisco CP Express では、この画面に含まれる設定タスクを実行することができます。内部アクセス ポイントの詳細設定を指定する必要がある場合は、『Cisco 860 and Cisco 880 Series Integrated Services Router Software Configuration Guide』を参照してください。

Wireless-LWAPP ホスト ルータの設定

ルータのアクセス ポイント コントローラに Autonomous Wireless-LWAPP（Wireless Lightweight Access Point Protocol）設定をサポートするイメージがインストールされている場合は、［Wireless-Unified (LWAPP) ホストルータの設定］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指定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 リファレンス

表 1-2　Wireless-LWAPP ホスト ルータ

要素	説明
Wireless-Unified(LWAPP) ホストルータの設定	ルータの DHCP サーバに対して WLAN コントローラの IP アドレスを設定するには、［Wireless-Unified (LWAPP) ホストルータの設定］を選択します。
WLAN コントローラの IP アドレス	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。
注意 : 内部アクセスポイントの詳細設定について ...	Cisco CP Express では、この画面に含まれる設定タスクを実行することができます。アクセス ポイントの追加の設定を行うには、画面の指示に従って、関連するワイヤレス管理アプリケーションを使用してください。

ワイドエリア ネットワーク インターフェイスの設定

Cisco CP Express では、ワイドエリア ネットワーク（WAN）インターフェイスを 1 つ設定することができます。ルータに複数の WAN インターフェイスがある場合は、設定するインターフェイスを選択できます。Cisco CP Express では、さまざまな WAN インターフェイスの設定をサポートしています。

詳細については、「WAN のリファレンス」を参照してください。

WAN のリファレンス

- WAN インターフェイスの選択
- インターネット（WAN）：イーサネット インターフェイス
- インターネット（WAN）：カプセル化タイプの自動検出
- インターネット（WAN）：ユーザ指定のカプセル化タイプ
- シリアル接続
- フレーム リレー設定
- インターネット（WAN）：詳細オプション
- インターネット（WAN）：ケーブル モデム
- ケーブルモデム接続の追加
- 認証

WAN インターフェイスの選択

Cisco CP Express では、WAN 接続を 1 つ設定できます。ルータに複数の WAN インターフェイスがある場合は、このウィンドウで設定するインターフェイスを選択します。設定するインターフェイスをリストから選択します。［接続の追加］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 接続を設定しないと、ファイアウォール、ルーティング、Cisco Network Services、SDP の設定はいずれも行えません。

接続の追加 / 編集 / 削除ボタン

WAN 接続が設定されていない場合は、［接続の追加］ボタンが有効になります。WAN 接続が 1 つ以上設定されている場合は、［編集］ボタンと［削除］ボタンが有効になります。

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］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、CCP を使用して他の WAN 接続を設定したり、設定された接続を削除して別の接続を設定したりできます。

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］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］をクリックします。

有効 / 無効ボタン

このボタンは、Cisco CP Express を使用して初期設定を編集す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ときは、［無効］ボタンを使用して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ときは、［有効］ボタンを使用してインターフェイスを有効にできます。

インターフェイス リスト

インターフェイス リストには、すべての WAN インターフェイスのインターフェイス名、IP アドレス、およびインターフェイス タイプが表示されます。インターフェイスに IP アドレスが設定されていないと、「IP アドレスがありません。」というメッセージが表示されます。

（注） ［LAN インターフェイス設定］ウィンドウでデフォルトの LAN インターフェイスを選択せずに、新しい IP アドレスを使用して設定した場合、このウィンドウにはその LAN インターフェイスが表示されます。これを WAN インターフェイスとして設定できます。

更新ボタン

初期設定の編集時に表示されます。詳細については、「Cisco CP Express のボタン」を参照してください。

インターネット（WAN）：イーサネット インターフェイス

このウィンドウでは、イーサネット WAN インターフェイスを設定します。

PPPoE を有効にするチェック ボックス

ルータで PPPoE を使用するようにサービス プロバイダから要求されている場合は、このチェック ボックスを選択して PPPoE カプセル化を有効にします。サービス プロバイダが PPPoE を使用しない場合は、このチェック ボックスを選択解除します。ルータが PPPoE カプセル化をサポートしていない Cisco IOS リリースを実行している場合、このチェック ボックスは使用できません。

アドレス タイプ 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 オプション

スタティック IP アドレスを選択した場合は、IP アドレスとサブネット マスクまたはサブネット ビットをそれぞれのフィールドに入力します。

ダイナミック（DHCP クライアント）オプション

このオプションを選択した場合、ルータはリモート DHCP サーバから IP アドレスをリースします。アドレスの割り当てを行う DHCP サーバの名前を入力します。

IP アンナンバード オプション

別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。設定中のインターフェイスと IP アドレスを共有するインターフェイスを選択します。［PPPoE を有効にする］を選択していない場合は、このオプションを使用できません。

Easy IP（ネゴシエート済みの IP）

ルータで PPP/IPCP アドレス ネゴシエーションによって IP アドレスを取得する場合は、［Easy IP（ネゴシエート済みの IP）］を選択します。［PPPoE を有効にする］を選択していない場合は、このオプションを使用できません。

認証タイプ チェック ボックス

サービス プロバイダが使用する認証タイプのチェック ボックスを選択します。認証タイプがわからない場合は、両方のチェック ボックスを選択できます。その場合、ルータは両方の認証タイプを試行して、成功した方を使用します。

CHAP 認証は PAP 認証より安全です。

ユーザ名

ユーザ名はインターネット サービス プロバイダまたはネットワーク管理者によって割り当てられ、CHAP、PAP、またはこれら両方の認証のユーザ名として使用されます。

パスワード

サービス プロバイダから割り当てら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を区別します。たとえば、test というパスワードは Test と同じではありません。

パスワードの確認

［パスワード］ボックスに入力したパスワードを再度入力します。

変更 / 変更の適用 / 変更の破棄ボタン

初期設定の編集時に表示されます。詳細については、「Cisco CP Express のボタン」を参照してください。

インターネット（WAN）：カプセル化タイプの自動検出

Cisco CP Express を使用してカプセル化のタイプを検出するには、［自動検出］ボタンをクリックします。自動検出に成功すると、Cisco CP Express は、カプセル化のタイプと、検出したその他の設定パラメータを自動的に設定します。

Cisco CP Express がカプセル化のタイプを検出できない場合、［ユーザ指定］をクリックしてカプセル化と認証のタイプを指定する必要があります。

ステータス アイコンおよび有効 / 無効ボタン

Cisco CP Express での初期設定の編集時にはステータス アイコンが表示されます。上向き矢印のアイコンは、インターフェイスが稼働していることを示します。下向き矢印のアイコンは、インターフェイスが停止していることを示します。

［有効］/［無効］ボタンは、Cisco CP Express での初期設定の編集時に使用することができます。選択したインターフェイスが有効になっているときは、［無効］ボタンを使用して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ときは、［有効］ボタンを使用して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タイプ

このウィンドウを使用して、カプセル化タイプの指定時に WAN インターフェイスを設定します。

ステータス アイコンおよび有効 / 無効ボタン

Cisco CP Express での初期設定の編集時にはステータス アイコンが表示されます。上向き矢印のアイコンは、インターフェイスが稼働していることを示します。下向き矢印のアイコンは、インターフェイスが停止していることを示します。

［有効］/［無効］ボタンは、Cisco CP Express での初期設定の編集時に使用することができます。選択したインターフェイスが有効になっているときは、［無効］ボタンを使用して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ときは、［有効］ボタンを使用して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 のいずれかのインターフェイスが装備されている場合に使用できるカプセル化は、次の表のとおりです。

カプセル化	説明
PPPoE	PPP over Ethernet カプセル化。ATM インターフェイス上に 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］ウィンドウに表示されます。 ルータが PPPoE カプセル化をサポートしていない Cisco IOS ソフトウェアのリリースを実行している場合、PPPoE オプションは無効になります。
PPPoA	ATM を介したポイントツーポイント プロトコルのカプセル化（AAL5 SNAP および AAL5 MUX）。ルータが PPPoA カプセル化をサポートしていない Cisco IOS ソフトウェアのリリースを実行している場合、PPPoA オプションは無効になります。
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場合に使用できます。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］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場合に使用できます。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］ウィンドウに表示されます。

仮想パス識別子

サービス プロバイダまたはシステム管理者から取得した仮想パス識別子（VPI）値を入力します。VPI は、ATM スイッチングとルーティングにおいて、多数の接続で使用されるパスを識別するために使用されます。

仮想回線識別子

サービス プロバイダまたはシステム管理者から取得した仮想回線識別子（VCI）値を入力します。仮想回線識別子（VCI）は、ATM スイッチングとルーティングにおいて、VCI によって識別される他の接続と共有するパス内で、特定の VCI 接続を識別するために使用されます。

アドレス タイプ 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］— このオプションを選択した場合は、IP アドレスとサブネット マスクまたはサブネット ビットをそれぞれのフィールドに入力します。
- ［ダイナミック（DHCP クライアント）］— このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。アドレスの割り当てを行う DHCP サーバの名前を入力します。
- ［IP アンナンバード］— 別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。設定中のインターフェイスと IP アドレスを共有する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）］— ルータで PPP/IPCP アドレス ネゴシエーションによって IP アドレスを取得する場合は、このオプションを選択します。

中央オフィス内のリモート接続用の IP アドレス

G.SHDSL 接続を設定する場合は、このリンクの接続先ゲートウェイの 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。ゲートウェイとは、インターネットまたは組織の WAN にアクセスする際、ルータが接続する必要があるシステムです。

マルチリンク PPP を有効にする

このインターフェイスで Multilink Point-to-Point Protocol（MLP）を有効にする場合はこのチェック ボックスを選択します。MLP では、負荷分散機能、パケットのフラグメンテーション、Bandwidth On Demand、およびその他の機能を使用することにより、複数の WAN 接続を持つネットワークのパフォーマンスが向上します。

認証タイプ チェック ボックス

サービス プロバイダが使用する認証タイプのチェック ボックスを選択します。認証タイプがわからない場合は、両方のチェック ボックスを選択できます。その場合、ルータは両方の認証タイプを試行して、成功した方を使用します。

CHAP 認証は PAP 認証より安全です。

ユーザ名

インターネット サービス プロバイダまたはネットワーク管理者によって割り当てられ、CHAP、PAP、またはこれら両方の認証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

サービス プロバイダから割り当てら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を区別します。たとえば、test というパスワードは Test と同じではありません。

パスワードの確認

［パスワード］ボックスに入力したパスワードを再度入力します。

変更 / 変更の適用 / 変更の破棄ボタン

初期設定の編集時に表示されます。詳細については、「Cisco CP Express のボタン」を参照してください。

シリアル接続

このウィンドウでは、シリアル接続を作成または編集します。

カプセル化リスト

この接続のカプセル化を選択します。接続を編集する場合は、このウィンドウでカプセル化のタイプを変更することはできません。接続を削除し、必要なカプセル化のタイプを使用して新しい接続を作成してください。

- ［フレーム リレー］— 接続されたデバイス間で HDLC カプセル化を使用して複数の仮想回線を処理する、スイッチ型データリンク層プロトコルです。
- ［HDLC］— ハイレベル データリンク コントロール。ISO（国際標準化機構）が標準化したビット指向の同期データ リンク層プロトコルです。フレーム文字とチェックサムを使用した同期シリアル リンク上でのデータ カプセル化方式を指定します。
- ［PPP］— ポイントツーポイント プロトコル。

認証の詳細

PPP カプセル化を選択すると、インターネット サービス プロバイダが必要とする認証情報を提供できます。

- ［ユーザ名］— インターネット サービス プロバイダまたはネットワーク管理者によって割り当てられ、CHAP、PAP、またはこれら両方の認証のユーザ名として使用されているユーザ名を正確に入力します。
- ［パスワード］— サービス プロバイダから割り当てら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を区別します。たとえば、test というパスワードは Test と同じではありません。
- ［パスワードの確認］—［パスワード］ボックスに入力したパスワードを再度入力します。

アドレス タイプ リスト

- ［スタティック IP アドレス］— フレーム リレー、PPP、および HDLC カプセル化タイプで使用できます。スタティック IP アドレスを選択した場合は、IP アドレスとサブネット マスクまたはサブネット ビットをそれぞれのフィールドに入力します。
- ［IP アンナンバード］— フレーム リレー、PPP、および HDLC カプセル化タイプで使用できます。別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。設定中のインターフェイスと IP アドレスを共有するインターフェイスを選択します。
- ［ネゴシエート済みの IP］— PPP カプセル化タイプでのみ使用できます。ルータで PPP/IPCP アドレス ネゴシエーションによって IP アドレスを取得する場合は、［Easy IP（ネゴシエート済みの IP）］を選択します。

IP アドレスおよびサブネット マスク

［スタティック IP アドレス］を選択する場合は、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 リレー設定のリンク

［DLCI］、［LMI］、および［IETF フレーム リレーのカプセル化を使用する］フィールドの説明については、「フレーム リレー設定」を参照してください。

フレーム リレー設定

フレーム リレー接続を設定するには、以下の設定を行います。

DLCI

DLCI（データリンク接続識別子）を入力します。この番号は、このインターフェイスで使用されるすべての DLCI の中で一意である必要があります。DLCI によって、この接続に一意のフレームリレー識別子が割り当てられます。

既存の接続を編集する場合、DLCI フィールドは無効になります。DLCI を変更する必要がある場合は、接続を一度削除して再度作成します。

LMI タイプ

使用する LMI（Local Management Interface）タイプについては、サービス プロバイダに確認してください。LMI タイプでは、接続の監視に使用するプロトコルを指定します。

ANSI オプション

ANSI（American National Standards Institute）標準 T1.617 で定義されている Annex D

Cisco オプション

Cisco と他の 3 社で共同定義した LMI タイプ

ITU-T Q.933 オプション

ITU-T Q.933 Annex A

自動検出オプション

デフォルト。ルータはスイッチと通信することによって、使用されている LMI タイプを検出し、そのタイプを使用します。自動検出に失敗した場合は、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チェック ボックス

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）のカプセル化方式を使用する場合は、このチェック ボックスを選択します。このオプションは、Cisco 製以外のルータに接続するときに使用されます。このインターフェイスで Cisco 製以外のルータに接続する場合は、このチェック ボックスを選択してください。

インターネット（WAN）：詳細オプション

このウィンドウでは、デフォルトのスタティック ルートを指定し、ルータ上の NAT を有効にできます。

デフォルト ルートを作成チェック ボックス

デフォルトのスタティック ルートは、ルータが認識していないネットワーク先のトラフィックの場合に、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。［このインターフェイスを転送インターフェイスとして使用］を選択すると、設定している WAN インターフェイスに、該当するすべてのトラフィックがルータによって送信されます。［ネクスト ホップの IP アドレス］をクリックした場合は、該当するトラフィックの転送先アドレスを指定します。

これらのフィールドは、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ている場合は表示されません。

インターネット（WAN）：ケーブル モデム

この画面では、ルータのケーブル モデム インターフェイスを設定できます。Cisco CP Express によって、デフォルトのケーブル モデム設定が提供され、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が設定されます。

［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。］を選択すると、ケーブル モデム インターフェイスが DHCP クライアントとして設定されます。

ケーブルモデム接続の追加

ケーブル モデム インターフェイスの設定を選択すると、このメッセージ画面が表示されます。インターフェイスを DHCP クライアントとして設定することを通知するメッセージが表示されます。WAN インターフェイスを DHCP クライアントとして設定する場合、そのインターフェイスは ISP または社内で準備された 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 リファレンス

表 1-3　ケーブル モデム設定メッセージの各ボタン

要素	説明
OK	Cisco CP Express のデフォルト設定でケーブル モデム インターフェイスを設定し、そのインターフェイスを、DHCP サーバからダイナミック IP アドレスを取得する DHCP クライアントとして設定するには、［OK］をクリックします。
キャンセル	Cisco CP Express が使用する設定でインターフェイスを設定しない場合は、［キャンセル］をクリックします。

認証

このページは、次の設定を有効にした場合、またはその設定中に表示されます。

- シリアル接続に対する PPP（ポイントツーポイント プロトコル）
- ATM 接続に対する PPPoE（PPP over Ethernet）または PPPoA（PPP over ATM）カプセル化
- イーサネット接続に対する 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 プロバイダまたはネットワーク管理者は、CHAP（Challenge Handshake Authentication Protocol）パスワードまたは PAP（Password Authentication Protocol）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。このパスワードはインバウンド アクセスとアウトバウンド アクセスの両方を保護します。

フィールド リファレンス

表 1-4　［認証］画面

要素	説明
認証タイプ	サービス プロバイダが使用する認証タイプのチェック ボックスを選択します。認証タイプがわからない場合は、両方のチェック ボックスを選択できます。その場合、ルータは両方の認証タイプを試行して、成功した方を使用します。 CHAP 認証は PAP 認証より安全です。
ユーザ名	ユーザ名はインターネット サービス プロバイダまたはネットワーク管理者によって割り当てられ、CHAP または PAP 認証のユーザ名として使用されます。
パスワード	サービス プロバイダから割り当てら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を区別します。たとえば、cisco というパスワードは Cisco と同じではありません。
パスワードの確認	［パスワード］ボックスに入力したパスワードを再度入力します。

ファイアウォールの設定

ルータに WAN インターフェイスを設定した場合は、Cisco CP Express でデフォルトの設定を使用するファイアウォールを設定できます。

（注）　Cisco CP Express でファイアウォールを設定するには、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。

- デフォルトのアクセス　ルールを内部および外部のインターフェイスに適用する。
- デフォルトのインスペクション　ルールを外部インターフェイスに適用する — デフォルトのインスペクション ルールのリストが Cisco CP Express によって作成され、適用されます。
- 外部インターフェイスでの IP ユニキャスト RPF（逆方向パス転送）を有効にする。

Cisco CP Express でファイアウォールを設定した場合、後で CCP を使用してファイアウォール設定を変更できます。Cisco CP Express でファイアウォールを設定しない場合でも、後で Cisco CP Express または CCP を使用してファイアウォールを設定できます。

画面については、「ファイアウォール設定」で説明しています。

ファイアウォール設定

［ファイアウォール設定］ウィンドウでは、WAN および LAN インターフェイスにファイアウォールを設定できます。初期セットアップ時にファイアウォールを適用したり、ルータを初期設定した後に Cisco CP Express を使用してファイアウォールを適用したりできます。

Cisco CP Express のファイアウォール設定をそのまま適用しても、後で CCP のファイアウォール ポリシー機能を使用してファイアウォール設定を変更できます。

（注）

- この機能は、ルータで実行されている 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。
- ［ファイアウォール設定］ウィンドウは、WAN インターフェイスを設定していない場合に表示されます。

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。

- デフォルトのアクセス　ルールを内部および外部のインターフェイスに適用する — DNS と HTTP の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、デフォルトのアクセス ルール リストが Cisco CP Express によって作成され、適用されます。
- デフォルトのインスペクション　ルールを外部インターフェイスに適用する — デフォルトのインスペクション ルールのリストが Cisco CP Express によって作成され、適用されます。
- 外部インターフェイスでの IP ユニキャスト RPF（逆方向パス転送）を有効にする — IP ユニキャスト RPF 機能により、ルータはパケットを受信したインターフェイスとパケットの送信元アドレスをチェックします。入力インターフェイスがルーティング テーブルに指定されている送信元アドレスへの適切なパスでない場合、パケットは廃棄されます。この送信元アドレスの検証は IP スプーフィングの防止に使用されます。

Cisco CP Express でファイアウォールを設定した場合、後で CCP を使用してファイアウォール設定を変更できます。Cisco CP Express でファイアウォールを設定しない場合でも、後で Cisco CP Express または CCP 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」を参照してください。

セキュリティ設定

ルータとネットワークのセキュリティを低下させる可能性がある設定でも、有用なサービスを提供することから、デフォルトで有効な場合があります。たとえば、CDP（Cisco ディスカバリ プロトコル）により、管理者はネットワーク上の隣接ルータに関する情報を簡単に参照できます。しかし、CDP によって提供される情報が不適切な人物に渡った場合、セキュリティ リスクが発生するおそれがあります。Cisco CP Express では、セキュリティ リスクを引き起こす一般的な設定のリストを参照できます。必要に応じて、これらの設定を無効にし、ルータおよびネットワークのセキュリティを確保することができます。

また、デフォルトで無効な設定の中には、有効にした場合、ネットワークを攻撃から保護するとともにトラブルシューティングにも役立つ、TCP 時間やロギングなどの設定があります。これらの設定のリストについても Cisco CP Express で参照し、有効にするかどうかを選択することができます。

［セキュリティ設定］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

以降のセクションの各トピックでは、この画面で指定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

次の各トピックでは、一般的なセキュリティ リスクを緩和するための設定について説明します。

- Finger サービスを無効にする
- PAD サービスを無効にする
- TCP スモール サーバ サービスを無効にする
- UDP スモール サーバ サービスを無効にする
- IP BOOTP サーバ サービスを無効にする
- IP ident サービスを無効にする
- CDP を無効にする
- IP ソース ルートを無効にする
- IP Gratuitous ARP を無効にする

- IP リダイレクトを無効にする
- IP プロキシ ARP を無効にする
- IP ダイレクト ブロードキャストを無効にする
- MOP サービスを無効にする
- IP アンリーチャブル メッセージを無効にする
- IP マスク応答を無効にする

ルータおよびネットワークの拡張セキュリティ

次の各トピックでは、ルータおよびネットワークのセキュリティを強化するための設定について説明します。

- NetFlow スイッチングを有効にする
- 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
- 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
- デバッグのシーケンス番号とタイム スタンプを有効にする
- IP CEF を有効にする
- スケジューラ インターバルを設定する
- スケジューラ アロケートを設定する
- TCP Synwait 時間を設定する
- ロギングを有効にする
- すべての外部インターフェイスに対してユニキャスト RPF を有効にする

ルータ アクセスの拡張セキュリティ

次の各トピックでは、ルータへのアクセスのセキュリティを強化するための設定について説明します。

- パスワードの最小文字数を 6 文字以上に設定する
- 認証失敗回数を再試行回数 3 回未満に設定する
- バナーを設定する
- Telnet 設定を有効にする
- ルータ アクセスに対して SSH を有効にする

パスワード暗号化

次の各トピックでは、パスワードを暗号化するための設定について説明します。

- パスワード暗号化サービスを有効にする

セキュリティ設定

Cisco IOS ソフトウェアの機能の中でデフォルトで有効になっているものが原因で、セキュリティ リスクが生じたり、ルータが大量のメッセージを送信するためにメモリを使い果たしてしまう可能性がある場合は、このウィンドウでその機能を無効にすることができます。必要がない限り、これらのチェック ボックスの選択はデフォルトのままとしてください。このヘルプ トピックは、Cisco CP Express で行う各セキュリティ設定の説明にリンクします。

初期設定が完了したら、Cisco CP Express を使用してこのウィンドウのセキュリティ設定を変更できます。このヘルプ ページに記載された設定グループの下に表示されている個々の設定を変更する場合は、CCP 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 SNMP サービスを無効にするチェック ボックス

このチェック ボックスを選択すると、ルータ上の SNMP サービスが無効になります。SNMP を無効にする理由については、ヘルプ トピック「SNMP を無効にする」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チェック ボックス

このチェック ボックスを選択すると、ルータ上の次のサービスが無効になります。これらのサービスを無効にする理由については、次の各リンクをクリックしてください。

- Finger サービスを無効にする
- PAD サービスを無効にする
- TCP スモール サーバ サービスを無効にする
- UDP スモール サーバ サービスを無効にする
- IP BOOTP サーバ サービスを無効にする

- IP ident サービスを無効にする
- CDP を無効にする
- IP ソース ルートを無効にする
- IP Gratuitous ARP を無効にする
- IP リダイレクトを無効にする
- IP プロキシ ARP を無効にする
- IP ダイレクト ブロードキャストを無効にする
- MOP サービスを無効にする
- IP アンリーチャブル メッセージを無効にする
- IP マスク応答を無効にする

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チェック ボックス

このチェック ボックスを選択すると、ルータ上の次のセキュリティ拡張機能とサービスが有効になります。これらのサービスと機能の詳細については、次の各リンクをクリックしてください。

- NetFlow スイッチングを有効にする
- 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
- 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
- デバッグのシーケンス番号とタイム スタンプを有効にする
- IP CEF を有効にする
- スケジューラ インターバルを設定する
- スケジューラ アロケートを設定する
- TCP Synwait 時間を設定する
- ロギングを有効にする
- すべての外部インターフェイスに対してユニキャスト RPF を有効にする

ルータ アクセスのセキュリティを強化するチェック ボックス

このチェック ボックスを選択すると、ルータに次のセキュリティ拡張設定が実装されます。これらのサービスと機能の詳細については、次の各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 文字以上に設定する
- 認証失敗回数を再試行回数 3 回未満に設定する
- バナーを設定する
- Telnet 設定を有効にする
- ルータ アクセスに対して SSH を有効にする

パスワードの暗号化チェック ボックス

このチェック ボックスを選択すると、パスワードの暗号化が有効になります。詳細については、ヘルプ トピック「パスワード暗号化サービスを有効にする」を参照してください。

ルータの日付および時刻の設定と PC の設定の同期をとるチェック ボックス

このチェック ボックスは、デフォルトで選択されています。ルータの日付と時刻を、Cisco CP Express を実行している PC の現在の設定に合わせない場合は、このチェック ボックスを選択解除してください。

要約

［要約］ウィンドウには、ルータの設定内容の変更が表示されます。設定を変更する場合は、［戻る］をクリックし、変更を行うウィンドウに戻ります。

入力したデータをルータのコンフィギュレーション ファイルに保存するには、［完了］をクリックします。

（注） LAN インターフェイスに推奨する新しい IP アドレスが割り当てられている場合、［完了］をクリックすると、ルータとの接続が切断されます。ルータに再接続するには、PC がルータと同じサブネット内にあることを確認し、LAN インターフェイスに割り当てた新しい IP アドレスを入力する必要があります。詳細については、「初期設定後にルータに再接続する」を参照してください。

追加のヘルプ

次のヘルプ トピックには追加情報が記載されています。

Cisco Configuration Professional

Cisco CP Express を使用してルータの基本設定を行った後に、Cisco Configuration Professional（CCP）を使用して、追加の接続の設定、Cisco CP Express を使用して行った設定の調整、仮想プライベート ネットワーク（VPN）やデジタル証明書などの高度な機能の設定を行うことができます。

CCP はルータにインストールされていることがあります。また、PC またはルータに CCP をインストールするときに使用する CD として配信されている場合もあります。Cisco.com から CCP を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 PC またはルータに CCP をインストールできます。

CCP を起動するには、［ツール］メニューの［CCP］をクリックします。

Cisco Network Services

サービス プロバイダから 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 ウィザードによって Cisco Network Services サーバの情報が収集され、WAN 設定のウィンドウが表示されます。これらのウィンドウを使用して、Cisco Network Services サーバへの WAN 接続を設定したり設定を取得したりできます。サービス プロバイダから Cisco Network Services サーバ情報が提供されていない場合、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か、またはルータにインストールされている WAN インターフェイスが Cisco CP Express でサポートされていない場合。ルータで Cisco Network Services コンフィギュレーション ファイルを取得するには、Cisco CP Express で 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 は WAN インターフェイスを設定できないと判断すると、Cisco Network Services が使用できないことを通知するエラー メッセージを表示します。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場合、Cisco Network Services を使用するには、［キャンセル］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。次に、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（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 から CCP リリース ノートを参照してください。

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

- このオプションを選択しないで、Cisco CP Express を使用して LAN および 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］ウィンドウに戻って、［CNS サーバ］を選択した場合。Cisco Network Services を使用する必要がある場合は、［キャンセル］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。次に、Cisco CP Express を再起動して［ルータのプロビジョニング］ウィンドウで［CNS サーバ］を選択してください。

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 を無効にする

Cisco CP Express は、可能であれば、簡易ネットワーク管理プロトコル（SNMP）サービスを無効にします。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を取得およびポストする機能を提供します。ルータの監視に広く使用されており、ルータの設定変更にもよく使用されます。ただし、最も普及している SNMP のバージョン 1 は、次の理由からセキュリティリスクの原因となることがよくあります。

- 「コミュニティ文字列」と呼ばれる認証文字列（パスワード）を使用しているが、この文字列は平文で保存されておりネットワーク上を平文で送信される。
- 多くの SNMP 実装では、これらの文字列を定期的なポーリングの際に繰り返し送信する。
- 簡単にスプーフィングできる、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 テーブルのコピーやネットワーク機密情報を取得するときに使用できるため、ネットワークで必要でない限り、SNMP を無効にすることをお勧めします。Cisco CP Express は、初期設定で SNMP を無効にするよう要求します。

SNMP 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 snmp-server
```

Finger サービスを無効にする

Cisco CP Express は、可能であれば 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確認するために使用します。通常、これらの情報はそれほど機密性の高いものではありませんが、攻撃者にとって有用な情報になることもあります。

Finger サービスは、"Finger of death" と呼ばれる特殊なタイプのサービス拒否（DoS）攻撃に悪用される可能性があります。これは、毎分 1 つの Finger 要求を特定のコンピュータに送り続け、決してコネクションを切断しない攻撃です。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

PAD サービスを無効にする

Cisco CP Express は、可能であれば、すべてのパケット アセンブラ / ディスアセンブラ（PAD）コマンド、および 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 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 pad
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

TCP スモール サーバ サービスを無効にする

Cisco CP Express は、可能であれば、スモール サービスを無効にします。Cisco IOS リリース 11.3 以前が稼働している Cisco デバイスでは、デフォルトで、echo、chargen、discard の各サービスが有効になっています（Cisco IOS リリース 12.0 以降では、スモール サービスはデフォルトで無効になりました）。これらのサービス、特に UDP（User Datagram Protocol）版のサービスは、正当な目的で使用されることはほとんどなく、サービス拒否（DoS）などの攻撃で利用される可能性があります。ただし、ルータでパケットをフィルタリングしていればほとんどの攻撃を防ぐことができます。

たとえば、攻撃者は、通常なら到達不可エラーになるはずの DNS サーバのアドレスを送信元アドレスに設定し、DNS サービス ポート（53 番ポート）を送信元ポートに設定した、偽造 DNS パケットを送信する可能性があります。このようなパケットがルータの UDP echo ポートに送信されると、ルータは DNS パケットを不正なサーバに送信することになります。アウトバウンド アクセス制限リストはこのパケットには適用されません。なぜなら、このパケットはルータが自分で生成したものと見なされるからです。

こうしたスモール サービスの悪用はほとんどの場合、スプーフィング防止アクセス リストによって回避（または少なくとも危険度を軽減）できるものの、ファイアウォールの一部であるルータや、ネットワーク上の厳重なセキュリティを要する部分に設置されたルータでは、これらのサービスをほぼ無条件で無効にするべきです。これらのサービスはほとんど使用されないため、すべてのルータ上で無効にすることが得策と言えます。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

UDP スモール サーバ サービスを無効にする

Cisco CP Express は、可能であれば、スモール サービスを無効にします。Cisco IOS リリース 11.3 以前が稼働している Cisco デバイスでは、デフォルトで、echo、chargen、discard の各サービスが有効になっています（Cisco IOS リリース 12.0 以降では、スモール サービスはデフォルトで無効になりました）。これらのサービス、特に UDP（User Datagram Protocol）版のサービスは、正当な目的に使用されることはほとんどなく、多くの場合、サービス拒否（DoS）などの攻撃に悪用されます。こうした攻撃は、パケットをフィルタリングすることによって防止できます。

たとえば、攻撃者は、通常であれば到達不可エラーになる DNS サーバのアドレスを送信元アドレスに設定し、送信元ポートには DNS サービス ポート（53 番ポート）を設定した、偽造 DNS パケットを送信する可能性があります。このようなパケットがルータの UDP echo ポートに送信されると、ルータは DNS パケットを不正なサーバに送信することになります。アウトバウンド アクセス制限リストはこのパケットには適用されません。なぜなら、このパケットはルータが自分で生成したものと見なされるからです。

こうしたスモール サービスの悪用はほとんどの場合、スプーフィング防止アクセス リストによって回避（または少なくとも危険度を軽減）できるものの、ファイアウォールの一部であるルータや、ネットワーク上の厳重なセキュリティを要する部分に設置されたルータでは、これらのサービスをほぼ無条件で無効にするべきです。これらのサービスはほとんど使用されないため、すべてのルータ上で無効にすることが得策と言えます。

UDP スモール 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 udp-small-servers
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP BOOTP サーバ サービスを無効にする

Cisco CP Express は、可能であれば、Bootstrap Protocol（BOOTP）サービスを無効にします。BOOTP を使用すると、ルータとコンピュータは、起動時に、集中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取得できます。これには、Cisco IOS ソフトウェアのダウンロードも含まれます。このため、BOOTP は、ルータの Cisco IOS ソフトウェアを不正にダウンロードするための手段として攻撃者に悪用される可能性があります。

BOOTP サービスは DoS 攻撃も受けやすいため、無効にするか、ファイアウォールでフィルタリングする必要があります。

BOOTP 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 bootp server
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP ident サービスを無効にする

Cisco CP Express は、可能であれば、ident サポート サービスを無効にします。ident サポートを稼働すると、TCP ポートに対して識別情報を問い合わせることができます。こうした問い合わせに対して、安全でないプロトコルは、TCP コネクションを開始したクライアントやそのコネクションに応答したホストの識別情報を返します。ident サポートを稼働していると、ホスト上の TCP ポートに接続し、簡単な文字列のコマンドを送信して情報を要求し、簡単な文字列で応答を受信できます。

ルータに直接接続されたネットワーク セグメント上のシステムから、ルータの製造元が Cisco であることを把握できたり、そのモデル番号および稼働している Cisco IOS ソフトウェアのリリースを確認できたりするという状況は危険と言えます。この情報を基にしてルータに対する攻撃方法を考え出すことができるためです。

IP ident 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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

CDP を無効にする

Cisco CP Express は、可能であれば、CDP（Cisco ディスカバリ プロトコル）を無効にします。Cisco ディスカバリ プロトコルは、1 つの LAN セグメント上で各 Cisco ルータが互いを特定するために使用する独自プロトコルです。ルータに直接接続されたネットワーク セグメント上のシステムから、ルータの製造元が Cisco であることを把握できたり、そのモデル番号および稼働している Cisco IOS ソフトウェアのリリースを確認できたりするという状況は危険と言えます。この情報を基にしてルータに対する攻撃方法を考え出すことができるためです。

Cisco ディスカバリ プロトコル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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP ソース ルートを無効にする

Cisco CP Express は、可能であれば、IP ソース ルーティングを無効にします。IP プロトコルは、ソース ルーティング オプションをサポートしています。このオプションを使用すると、IP データグラムの送信者が、データグラムの最終宛先までの通過経路、また通常は、その応答の通過経路を制御できます。しかし、このオプションがネットワーク上で正当な目的に使用されることはほとんどあり

ません。一部の古い IP 実装では、ソースルート指定されたパケットを正しく処理しないため、そうした実装を稼働しているマシンにソースルート指定されたデータグラムを送信することで、マシンをクラッシュさせることができます。

IP ソース ルーティングを無効にすると、ソースルートが指定された 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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

パスワード暗号化サービスを有効にする

Cisco CP Express は、可能であれば、パスワードの暗号化を有効にします。パスワード暗号化は、パスワード、Challenge Handshake Authentication Protocol（CHAP）secret、およびコンフィギュレーション ファイルに保存される同様のデータを暗号化するように、Cisco IOS ソフトウェアに指示します。このサービスを利用すれば、誰かが管理者の後ろからのぞくなど、パスワードをうっかり見られるのを防ぐことができます。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

NetFlow スイッチングを有効にする

Cisco CP Express は、可能であれば、NetFlow スイッチングを有効にします。NetFlow スイッチングを使用すると、アクセス コントロール リスト（ACL）およびネットワーク セキュリティを実現し、強化するその他の機能を使用しながら、同時にルーティングのパフォーマンスも高めることができます。NetFlow は、送信元 / 宛先 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 フローを特定します。特定のフローの先頭パケットだけを使用して、ACL との照合やその他のセキュリティ チェックを行うため、フロー内のすべてのパケットを使用してこれらの処理を行う必要はありません。これにより、パフォーマンスが向上するため、ルータのすべてのセキュリティ機能を利用できるようになります。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

インバウンド telnet セッションの TCP キープアライブを有効にする

Cisco CP Express は、可能であれば、インバウンドとアウトバウンド両方の telnet セッションについて、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、ルータが定期的にキープアライブ メッセージを生成するようになります。これにより、壊れた telnet 接続を検出し破棄することができます。

インバウンド telnet セッションで、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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

アウトバウンド telnet セッションの TCP キープアライブを有効にする

Cisco CP Express は、可能であれば、インバウンドとアウトバウンド両方の telnet セッションについて、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、ルータが定期的にキープアライブ メッセージを生成するようになります。これにより、壊れた telnet 接続を検出し破棄することができます。

インバウンド telnet セッションで、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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

デバッグのシーケンス番号とタイム スタンプを有効にする

Cisco CP Express は、可能であれば、すべてのデバッグ メッセージとログ メッセージで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 メッセージのタイム スタンプは、そのメッセージが生成された日時を示します。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番を示します。メッセージが生成された時刻と順番を知ることは、攻撃の可能性を診断する際に重要な情報となります。

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 を有効にする

Cisco CP Express は、可能であれば、Cisco Express Forwarding（CEF）または Distributed Cisco Express Forwarding（DCEF）を有効にします。Cisco Express Forwarding では、トラフィックの新しい宛先毎にキャッシュ エントリを作成する必要がないため、多くの宛先に向けて大量のトラフィックが送信されてきた場合に、他のモードよりもルータが想定範囲内で動作します。Cisco Express Forwarding 用に設定されたルータは、従来のキャッシュを使用したルータに比べて、SYN 攻撃の影響を受けにくくなります。

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 インターバルを設定する

Cisco CP Express は、可能であれば、ルータのスケジューラ インターバルを設定します。ルータは、大量のパケットをファースト スイッチングで処理していると、ネットワーク インターフェイスからのインタラプトに応答する時間がかかり過ぎて、他の処理ができなくなります。これは、大量のパケットが高速で送信されると発生します。このような状態になると管理者もルータにアクセスできなくなる可能性があるため、ルータが攻撃されている場合は非常に危険です。スケジューラ間隔を調整すると、ルータへの管理目的のアクセスがいつでも確実に行えるようになります。これは、指定された時間間隔が経過すると、たとえ CPU の使用率が 100% であっても、システム処理に強制的に CPU 時間が割り当てられるからです。

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 アロケートを設定する

Cisco CP Express は、可能であれば、**scheduler interval** コマンドをサポートしていないルータ上で **scheduler allocate** コマンドを設定します。ルータは、大量のパケットをファースト スイッチングで処理していると、ネットワーク インターフェイスからのインタラプトに応答する時間がかかり過ぎて、他の処理ができなくなります。これは、大量のパケットが高速で送信されると発生します。このような状態になると管理者もルータにアクセスできなくなる可能性があるため、ルータが攻撃されている場合は非常に危険です。**scheduler allocate** コマンドは、ルータの全 CPU 時間のうちの一定の割合を、管理処理などのネットワーク スイッチング以外の処理に割り当てることを保証します。

スケジューラ割り当ての割合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 時間を設定する

Cisco CP Express は、可能であれば、TCP Synwait 時間を 10 秒に設定します。TCP Synwait 時間を設定することは、サービス拒否（DoS）攻撃の手法の 1 つである SYN フラッド攻撃に対抗する方法として有用です。TCP で接続を確立するには、3 フェーズのハンドシェイクを行う必要があります。まず、開始側が接続要求を送信し、それに対して受信側が確認応答を返し、さらにそれに対して開始側が確認応答を受け取ったことを送信します。この 3 フェーズのハンドシェイクが完了したら、接続が確立され、データ転送を開始できます。SYN フラッド攻撃は、同じホストに接続要求を繰り返し送信します。そして、接続を完了させる確認応答の受け取りの送信を行わないことで、ホスト側に未完了の接続を増やし続けます。未完了の接続用のバッファ領域は通常、確立された接続用のバッファ領域よりも小さいため、未完了の接続数が増えるとバッファがいっぱいになり、ホストは機能停止状態になります。TCP Synwait 時間を 10 秒に設定すると、ルータは、ハンドシェイクの最後の確認応答の受信待ち状態になってから 10 秒後に未完了の接続を破棄するため、ホスト側に未完了の接続が溜まるのを阻止できます。

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>
```

ロギングを有効にする

Cisco CP Express は、可能であれば、シーケンス番号とタイム スタンプ付きのロギングを有効にします。ログは、ネットワーク イベントに関する詳細な情報を提供するので、セキュリティ イベントを認識して対策を施すには不可欠です。タイム スタンプとシーケンス番号は、ネットワーク イベントの発生した日時と順番に関する情報を提供します。

ロギングを有効化するために、ルータに配信される設定は次のとおりです。*<log buffer size>* および *<logging server ip address>* の部分は、Cisco CP Express で入力した情報で置き換えてください。

```
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してユニキャスト RPF を有効にする

Cisco CP Express は、可能であれば、インターネットに接続されているすべてのインターフェイス上で、ユニキャスト逆方向パス転送（RPF）を有効にします。RPF 機能により、ルータはパケットを受信したインターフェイスとパケットの送信元アドレスをチェックします。入力インターフェイスがルーティング テーブルに指定されている送信元アドレスへの適切なパスでない場合、パケットは廃棄されます。この送信元アドレスの検証は IP スプーフィングの防止に使用されます。

この方法が機能するのは、ルーティングが対称的に行われる場合だけです。ホスト A からホスト B へのトラフィックが、ホスト B からホスト A へのトラフィックと異なる経路をたどるようにネットワークが設計されている場合は、上のようなチェックを行うと常に失敗し、2 つのホスト間の通信は不可能となります。このような非対称的なルーティングは、インターネットのコア部分で一般的に行われています。この機能を有効にする前に、必ず、ネットワークが非対称的なルーティングを行っていないことを確認してください。

また、ユニキャスト RPF を有効にできるのは、IP Cisco Express Forwarding（CEF）が有効になっているときだけです。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、Cisco CP Express は、IP

Cisco Express Forwarding を有効にするように推奨し、推奨が承認されると実際に有効にします。Cisco CP Express、またはそれ以外の方法で IP Cisco Express Forwarding が有効になっていない場合は、ユニキャスト RPF を有効にすることはできません。

ユニキャスト RPF を有効にするために、プライベート ネットワークの外に接続されたルータの各インターフェイスに配信される設定は次のとおりです。<*outside interface*> の部分はインターフェイス識別子で置き換えてください。

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

IP Gratuitous ARP を無効にする

Cisco CP Express は、可能であれば、IP Gratuitous ARP 要求を無効にします。Gratuitous ARP とは、宛先の MAC アドレスが送信元の MAC アドレスと同じになるような ARP ブロードキャストのことです。これは元々、ホストが自分の IP アドレスをネットワーク全体に通知するためのプロトコルです。Gratuitous ARP メッセージが偽造されると、ネットワークのマッピング情報が間違って格納されるため、ネットワークの誤動作を引き起こします。

Gratuitous 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 gratuitous-arps
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP リダイレクトを無効にする

Cisco CP Express は、可能であれば、ICMP（インターネット制御メッセージ プロトコル）のリダイレクト 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条件に関する情報を伝達することによって 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、特定の宛先まで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、ルータはローカル サブネット上のホストだけにリダイレクトを送信し、エンド ノードはリダイレクトを送信しません。また、リダイレクトが 2 つ以上のネットワーク ホップを経由して転送されることもありません。ただし、これらのルールは攻撃者によって破られる可能性があります。実際、一部の攻撃では、ルール違反のリダイレクトを利用しています。ICMP リダイレクトを無効にしてもネットワークの運用に影響はありません。無効にすることで、こうした攻撃を防止できます。

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 プロキシ ARP を無効にする

Cisco CP Express は、可能であれば、プロキシ アドレス解決プロトコル（ARP）を無効にします。ARP は、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、ルータは ARP 要求のためのプロキシとして機能できます。これにより、複数の LAN セグメントにまたがって ARP 要求を送信できるようになります。ただし、これは LAN というセキュリティ防護壁を破ることになるため、プロキシ ARP は同じセキュリティ レベルを持つ 2 つの LAN 間のみに限定して、必要な場合に限って使用してください。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP ダイレクト ブロードキャストを無効にする

Cisco CP Express は、可能であれば、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、送信側のマシンが直接接続し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、送信先サブネットに到達するまでユニキャスト パケットとして伝送され、送信先サブネットでリンク層ブロードキャストに変換されます。IP のアドレス指定アーキテクチャの性質により、ダイレクト ブロードキャストを最終的に識別できるのは、チェーン内の最後のルータ、つまり送信先サブネットに直接接続されているルータだけです。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場合もありますが、そのような使用法は金融サービス業界以外では一般的ではありません。

IP ダイレクト ブロードキャストは、よく知られている「smurf」というサービス拒否攻撃で悪用され、他の同じような攻撃でも悪用される場合があります。「smurf」攻撃では、攻撃者が偽装された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 ICMP エコー要求を送信します。その結果、送信先サブネット上のすべてのホストが偽装された送信元アドレスに応答を送信します。このような要求を連続的に送信することによって、攻撃者は大量の応答を生成し、偽装されたアドレスを持つホストを完全な過負荷状態にすることができます。

IP ダイレクト ブロードキャストを無効にすると、そのインターフェイスでリンク層ブロードキャストに大量に変換されるはずのダイレクト ブロードキャストが廃棄されます。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

MOP サービスを無効にする

Cisco CP Express は、可能であれば、すべてのイーサネット インターフェイス上で Maintenance Operations Protocol（MOP）を無効にします。MOP は、DECNet ネットワークと通信するとき、ルータに設定情報を送信するために使用されます。MOP は、さまざまな攻撃を受けやすいプロトコルです。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP アンリーチャブル メッセージを無効にする

Cisco CP Express は、可能であれば、インターネット制御メッセージ プロトコル（ICMP）のホスト アンリーチャブル 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条件に関する情報を伝達することによって IP トラフィックをサポートします。ICMP ホストのアンリーチャブル メッセージは、ルータが、不明なプロトコルを使用する非ブロードキャスト パケットを受信した場合、または宛先アドレスまでのルートがないために最終的な宛先に配信できないパケットを受信した場合に送信されます。これらのメッセージは、ネットワーク マッピング情報を取得するために攻撃者に悪用される可能性があります。

ICMP ホスト アンリーチャブル 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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

IP マスク応答を無効にする

Cisco CP Express は、可能であれば、インターネット制御メッセージ プロトコル（ICMP）の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条件に関する情報を伝達することによって 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のサブネット マスクを認識する必要がある場合に送信されます。このメッセージは、必要な情報を持っているデバイスによって、情報を要求したデバイスに送信されます。これらのメッセージは、ネットワーク マッピング情報を取得するために攻撃者に悪用される可能性があります。

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
```

CCP セキュリティ監査機能を使用して、この設定変更を元に戻すことができます。設定変更を元に戻す方法については、CCP のセキュリティ監査機能オンライン ヘルプを参照してください。詳細については、「Cisco Configuration Professional」を参照してください。

パスワードの最小文字数を 6 文字以上に設定する

Cisco CP Express は、可能であれば、最低 6 文字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解読するときに使用する方法の 1 つに、パスワードが見つかるまで考えられる文字の組み合わせをすべて試すという方法があります。パスワードが長くなると考えられる文字の組み合わせが指数関数的に増加するため、この攻撃方法が成功する確率は大幅に低下します。

この設定を変更すると、ルータに設定されているすべてのパスワード（user、enable、secret、console、AUX、tty、vty など）の長さを 6 文字以上にする必要があります。この設定変更が実施されるのは、お使いのルータ上で稼働している Cisco IOS のバージョンでパスワードの最小長機能がサポートされている場合だけです。

ルータに配信される設定は次のとおりです。

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

認証失敗回数を再試行回数 3 回未満に設定する

Cisco CP Express は、可能であれば、3 回ログインに失敗するとアクセスをロックするようにルータを設定します。パスワード解読の手法の 1 つに「辞書」攻撃と呼ばれる方法があります。これは、辞書に書かれているすべての単語を使用してログインを試みるものです。この設定を使用すると、3 回ログインに失敗したら 15 秒間アクセスがロックされるようにルータが設定されます。これにより、辞書攻撃は使えなくなります。この設定では、ルータへのアクセスをロックするだけでなく、3 回ログインに失敗したらログ メッセージを生成し、ログインに失敗したユーザがいることを管理者に警告します。

3 回ログインに失敗した後、ルータへの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>
```

バナーを設定する

Cisco CP Express は、可能であれば、テキスト バナーを設定します。管轄区域によっては、不正ユーザに対して不正な侵入を警告するバナーを表示した方が、システムに侵入したクラッカーに対する民事または刑事起訴が容易になることがあります。また、監視することをあらかじめ本人に通知しない限り、たとえ不正ユーザであっても、その行動を監視することが禁止されている管轄区域もあります。テキスト バナーは、そうした通知を行うための手法の 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*>、<*administrator phone number*> の部分は、Cisco CP Express で入力した情報で置き換えてください。

```
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 設定を有効にする

Cisco CP Express は、可能であれば、以下の設定を実装することで、コンソール、AUX、vty、tty の各回線のセキュリティを強化します。

- **transport input** および **transport output** コマンドを設定して、上記の回線に接続する際に使用できるプロトコルを定義する。
- コンソールおよび AUX 回線の実行タイムアウト値を 10 分に設定する。これにより、10 分間作業していない状態が続くと、これらの回線にログインしている管理者が強制的にログアウトされる。

コンソール、AUX、vty、tty の各回線のセキュリティを強化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 アクセスに対して SSH を有効にする

ルータ上で実行されている Cisco IOS リリースが crypto イメージ（56 ビットの Data Encryption Standard（DES; データ暗号規格）暗号化を使用し、輸出制限の対象となるイメージ）の場合、Cisco CP Express は、可能であれば、次の設定を実装して Telnet アクセスのセキュリティを強化します。

- Telnet アクセス用に Secure Shell（SSH; セキュア シェル）を有効化する。SSH により Telnet アクセスのセキュリティは大幅に強化されます。
- SSH タイムアウト値を 60 秒に設定する。これにより、未完了の SSH 接続は 60 秒後にシャットダウンされる。
- SSH ログインの失敗回数を最大 2 回に設定し、3 回以上失敗するとルータへのアクセスをロックする。

アクセスとファイル転送機能のセキュリティを強化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 ボタン

［ヘルプ］をクリックすると、新しいブラウザ ウィンドウが開き、Cisco CP Express ウィンドウに関する情報が表示されます。

バージョン情報ボタン

［バージョン情報］をクリックすると、Cisco CP Express のバージョン情報を記載したウィンドウが表示されます。このウィンドウの［ハードウェア / ソフトウェアの詳細］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

- ルータのモデル タイプ
- ルータの合計メモリ
- ルータのフラッシュの合計容量
- ルータのブート元（フラッシュなど）

ハードウェアのダイアグラムも表示されます。

ソフトウェアの詳細

- ルータで実行する Cisco IOS ソフトウェアの名前
- Cisco IOS ソフトウェアのリリース
- Cisco IOS ソフトウェアでサポートされるファイアウォールや VPN などのフィーチャ セット
- Cisco CP Express のバージョン

終了ボタン

初期設定を完了後、［終了］をクリックして Cisco CP Express を終了します。

更新ボタン

初期設定の編集時に表示されます。［更新］をクリックすると、Cisco CP Express のルータ データが更新されます。

変更の適用ボタン

初期設定の編集時に表示されます。［変更の適用］をクリックすると、変更内容がルータに配信されます。

変更の破棄ボタン

初期設定の編集時に表示されます。［変更の破棄］をクリックすると、変更が行われたウィンドウがクリアされます。

初期設定後にルータに再接続する

推奨する新しい IP アドレスをルータの LAN インターフェイスに割り当てた場合は、設定を配信するとルータとの接続が切断されます。

Cisco CP Express を使用して初期設定を実行したら、次の手順に従ってルータに再接続します。

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 を設定する必要があります。コマンド ウィンドウを開き、**ipconfig /release** コマンドの後に **ipconfig /renew** コマンドを入力します。
- ルータを DHCP サーバとして設定しなかった場合は、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 PC に割り当てる必要があります。たとえば、LAN IP アドレスを 10.20.20.1（サブネット マスクは 255.255.255.224）に変更した場合は、10.20.20.2 ～ 10.20.20.30 の IP アドレスを PC に割り当て、同じサブネット値を使用します。

ステップ 2デフォルト以外の LAN インターフェイスを設定した場合は、設定した LAN インターフェイスに PC を接続します。たとえば、LAN インターフェイスに FE 0/0 ではなく FE 0/1 を設定した場合は、PC を FE 0/1 に接続します。

ステップ 3　PC の準備が完了したら、ルータの LAN インターフェイスを割り当てた新しい IP アドレスをブラウザ（http:// *新しい IP アドレス*）に入力して、PC をルータに再接続します。たとえば、LAN 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、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する必要があります。

詳細については、「WAN（インターネット）接続をテストする」を参照してください。

WAN（インターネット）接続をテストする

インターネットへの接続をテストするには、www.cisco.com などのリモート Web サイトにブラウザでアクセスしてみます。入力したリモート Web サイトに接続することができれば、WAN 設定は正常に機能しています。

リモート Web サイトに接続することができない場合は、CCP を使用して、次の手順で接続のトラブルシューティングを実行します。

ステップ 1　［ツール］メニューの［CCP］をクリックして CCP を起動します。

ステップ 2　CCP にログインし、［インターフェイスと接続］をクリックします。

ステップ 3　［編集］タブをクリックし、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］をクリックし、画面の指示に従います。CCP から問題点が報告され、推奨処置が提示されます。

SDP のトラブルシューティングのヒント

Secure Device Provisioning（SDP）を使用して登録を行う前に、このトピックの情報を参照してルータと証明書サーバの間の接続を準備してください。登録時に問題が発生した場合は、準備のために行ったタスクを見直すことで、問題のある場所を判断できます。

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て、SDP の Web アプリケーションが見えるようにします。

トラブルシューティングのヒント

ここに記載されている推奨事項は、ローカル ルータと認証機関（CA）サーバでの準備作業を必要とします。CA サーバの管理者に必要な作業を伝える必要があります。推奨される確認事項は次のとおりです。

- ローカル ルータと CA サーバが相互に IP 続可能であること。ローカル ルータは証明書サーバに ping を正常に実行できなければならず、また証明書サーバもローカル ルータに ping を正常に実行できなければなりません。
- CA サーバ管理者が JavaScript をサポートする Web ブラウザを使用していること。
- CA サーバ管理者がローカル ルータに対するイネーブル特権を持っていること。
- ローカル ルータ上のファイアウォールで、証明書サーバとの間で送受信されるトラフィックが許可されること。
- 申請者（Petitioner）と登録者（Registrar）の一方または両方でファイアウォールが設定されている場合は、SDP アプリケーションが起動された PC からの HTTP または HTTPS トラフィックがそのファイアウォールで許可されることを確認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/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332