Web ブラウザ インターフェイスの使用方法

この章では、アクセス ポイント / ブリッジの設定に使用できる Web ブラウザ インターフェイスについて説明します。この章の内容は、次のとおりです。

Web ブラウザ インターフェイスには、アクセス ポイント / ブリッジの設定の変更、ファームウェアのアップグレード、およびネットワーク上の他の無線デバイスの監視と設定に使用する管理ページが含まれます。

（注） アクセス ポイント / ブリッジの Web ブラウザ インターフェイスは、Windows 98、2000、および XP プラットフォーム上の Microsoft Internet Explorer バージョン 6.0、および Windows 98、Windows 2000、および Solaris プラットフォーム上の Netscape Navigator バージョン 7.0 と完全に互換性があります。

（注） Command-Line Interface（CLI; コマンドライン インターフェイス）および Web ブラウザ インターフェイスの両方を使用してアクセス ポイント / ブリッジを設定することは避けてください。設定にはどちらか一方を使用します。CLI を使用してアクセス ポイント / ブリッジを設定した場合、Web ブラウザ インターフェイスでは、その設定が正しく解釈されずに表示される場合があります。ただし、表示が正しくないからといって、アクセス ポイント / ブリッジが誤って設定されている訳ではありません。

初めて Web ブラウザ インターフェイスを使用する場合

アクセス ポイント / ブリッジの IP アドレスを使用して、管理システムを参照します。IP アドレスをアクセス ポイント / ブリッジに割り当てる方法の詳細は、「IP アドレスの取得と割り当て」の項（P. 2-3）を参照してください。

Web ブラウザ インターフェイスの使用を開始する手順は、次のとおりです。

ステップ 1　ブラウザを起動します。

ステップ 2　アクセス ポイント / ブリッジの IP アドレスをブラウザの **Location** フィールド（Netscape Communicator の場合）または **Address** フィールド（Internet Explorer の場合）に入力し、**Enter** キーを押します。

ステップ 3　管理者のユーザ名とパスワードを入力して **Enter** キーを押します。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。Summary Status ページが表示されます。

Web ブラウザ インターフェイスの管理ページの使用方法

システム管理ページでの設定情報の表示と保存には、一貫性のある手法が使用されています。ページの左側にはナビゲーション バーがあり、下部には設定アクション ボタンが表示されます。ナビゲーション バーは他の管理ページを参照する場合に使用し、設定アクション ボタンは設定の変更を保存またはキャンセルする場合に使用します。

（注）　ブラウザの **Back** ボタンをクリックすると前のページに戻りますが、変更内容は保存されないことに留意してください。**Cancel** をクリックすると、ページで行った変更はすべてキャンセルされ、ページは移動しません。変更は、**Apply** をクリックした場合にだけ適用されます。

図 3-1 は、Web ブラウザ インターフェイスのホーム ページを示しています。

図 3-1　Web ブラウザ インターフェイスのホーム ページ

アクション ボタンの使用方法

表 3-1 は、ほとんどの管理ページに表示されるページ リンクとボタンの一覧を示しています。

表 3-1　管理ページの共通ボタン

ボタン / リンク	説明
ナビゲーション リンク	
Home	アクセス ポイント / ブリッジにアソシエートされた無線デバイスの数、イーサネット インターフェイスと無線インターフェイスのステータス、および最近のアクセス ポイント / ブリッジのアクティビティ リストに関する情報を示す、アクセス ポイント/ブリッジのステータス ページを表示します。
Express Setup	システム名、IP アドレス、SSID などの基本的な設定を行う Express Setup ページを表示します。
Express Security	基本セキュリティ設定（No Security、Static WEP Key、EAP Authentication、または WPA）を選択できる Express Security ページを表示します。
Network Map	無線 LAN のインフラストラクチャ デバイスのリストを表示します。
Association	無線 LAN 上のすべてのデバイスのシステム名、ネットワークでの役割、および親とクライアントの関連性を示すリストを表示します。
Network Interfaces	イーサネットと無線のインターフェイスのステータスと統計を表示し、各インターフェイスの設定ページへのリンクを提示します。
Security	セキュリティ設定の要約を表示し、セキュリティ設定ページへのリンクを提示します。
Services	アクセス ポイント / ブリッジのいくつかの機能に関するステータスと、Telnet/SSH、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、ドメイン ネーム サーバ、フィルタ、プロキシ モバイル IP、QoS（Quality Of Service）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、SNTP、および Virtual Local Area Network（VLAN; バーチャル LAN ）の設定ページへのリンクを表示します。
Wireless Services	Wireless Domain Services Status ページを表示します。このページから AP および Wireless Domain Services（WDS）のページにアクセスできます。
System Software	アクセス ポイント / ブリッジで実行されているファームウェアのバージョン番号を表示し、ファームウェアのアップグレードおよび管理のための設定ページへのリンクを表示します。
Event Log	アクセス ポイント / ブリッジのイベント ログを表示し、トラップに含めるイベントの選択、イベントの重大度レベルの設定、通知方法の設定を行う設定ページへのリンクを表示します。
設定アクション ボタン	
Apply	そのページに加えた変更を保存し、ページをそのまま表示します。
Refresh	ページに表示されるステータス情報または統計を更新します。
Cancel	そのページに加えた変更を廃棄し、ページをそのまま表示します。
Back	そのページに加えた変更を廃棄し、直前のページに戻ります。

入力フィールドの文字制限

1300 シリーズのアクセス ポイント / ブリッジは Cisco IOS ソフトウェアを使用するため、Web ブラウザ インターフェイスの入力フィールドに使用できない文字がいくつかあります。入力フィールドに使用できない文字は次のとおりです。

“
]
+
/
タブ
後続のスペース

安全な参照のための HTTPS の有効化

HTTPS を有効にすることにより、アクセス ポイント / ブリッジの Web ブラウザ インターフェイスとの通信を保護できます。HTTPS では、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションが保護されます。

（注）　HTTPS を有効にすると、ブラウザからアクセス ポイント / ブリッジへの接続が解除されます。接続が解除された場合は、使用しているブラウザのアドレス入力用ボックスで、URL を http://*ip_address* から **https://*ip_address*** に変更して、アクセス ポイントに再度ログインします。

（注）　HTTPS を有効にすると、ほとんどのブラウザでは、ユーザが Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）のないデバイスを参照するたびに承認を求めるプロンプトが表示されます。このプロンプトを表示させないようにするには、次の ステップ 2 ～ ステップ 9 の設定を行って、アクセス ポイント用の FQDN を作成します。ただし、FQDN の作成を省略する場合は、ステップ 10 にスキップします。

FQDN を作成して HTTPS を有効にする手順は、次のとおりです。

ステップ 1　ブラウザでポップアップ ブロッキング ソフトウェアを使用している場合は、その機能を無効にします。

ステップ 2　Express Setup ページを参照します。図 3-2 は、Express Setup ページを示しています。

図 3-2　Express Setup ページ

ステップ 3　System Name フィールドにアクセス ポイント / ブリッジの名前を入力して、**Apply** をクリックします。

ステップ 4　Services – DNS ページを参照します。図 3-3 は、Services – DNS ページを示しています。

図 3-3　Services – DNS ページ

ステップ 5　Domain Name System で、**Enable** を選択します。

ステップ 6　Domain Name フィールドに、所属する会社のドメイン名を入力します。たとえば、シスコシステムズの場合、ドメイン名は *cisco.com* になります。

ステップ 7　Name Server IP Addresses 入力フィールドに、DNS サーバの IP アドレスを 1 つ以上入力します。

ステップ 8　**Apply** をクリックします。アクセス ポイント / ブリッジの FQDN は、システム名とドメイン名で構成されます。たとえば、システム名が *br 1310*、ドメイン名が *company.com* の場合、FQDN は *br1310.company.com* になります。

ステップ 9　DNS サーバで、FQDN を入力します。

ヒント　DNS サーバがない場合、アクセス ポイント / ブリッジの FQDN はダイナミック DNS サービスを使用して登録できます。インターネットで「*ダイナミック DNS*」を検索して、料金ベースの DNS サービスを見つけてください。

ステップ 10　Services: HTTP Web Server ページを表示します。図 3-4 は、HTTP Web Server ページを示しています。

図 3-4　Services: HTTP Web Server ページ

ステップ 11　Enable Secure (HTTPS) Browsing チェックボックスをオンにして、**Apply** をクリックします。

（注）　標準の HTTP および HTTPS を両方とも有効にできますが、シスコでは、どちらか一方を有効にすることをお勧めします。

警告ウィンドウが表示され、アクセス ポイントの参照に HTTPS を使用することが示されます。またこの警告ウィンドウでは、アクセス ポイント / ブリッジの参照に使用する URL について、*http* から *https* に変更するように指示されます。図 3-5 は、警告ウィンドウを示しています。

図 3-5　HTTPS の警告ウィンドウ

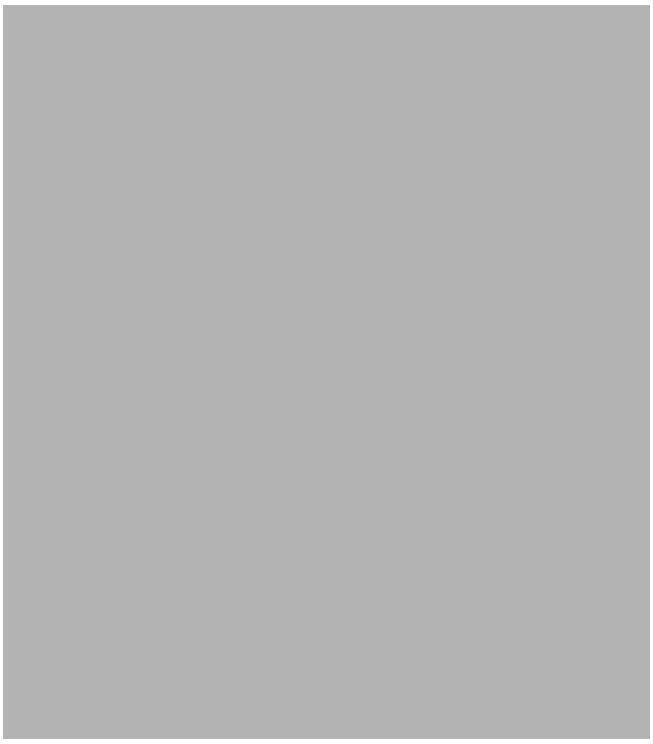
ステップ 12　**OK** をクリックします。ブラウザのアドレス入力用ボックスで、アドレスが **http://*ip-address*** から **https://*ip-address*** に変更されます。

ステップ 13　別の警告ウィンドウが表示され、アクセス ポイントのセキュリティ証明書が有効であること、およびその発行元が不明であることが示されます。ただし、対象となるサイトはユーザ自身のアクセス ポイントであるため、その証明書を受け入れても問題ありません。図 3-6 は、証明書の警告ウィンドウを示しています。

図 3-6　証明書の警告ウィンドウ

ステップ 14　**View Certificate** をクリックし、証明書を受け入れて処理を続けます（証明書を受け入れずに処理を続行するには、**Yes** をクリックして、ステップ 23 にスキップします）。図 3-7 は、Certificate ウィンドウを示しています。

図 3-7　Certificate ウィンドウ



ステップ 15　Certificate ウィンドウで、**Install Certificate** をクリックします。Microsoft Windows の Certificate Import Wizard が表示されます。図 3-8 は、Certificate Import Wizard ウィンドウを示しています。

図 3-8　Certificate Import Wizard ウィンドウ

ステップ 16 **Next** をクリックします。次のウィンドウでは、証明書の保存場所を指定するように求められます。シスコでは、システムのデフォルトの保存場所を使用するようにお勧めします。図 3-9 は、証明書の保存場所を指定するウィンドウを示しています。

図 3-9　証明書の保存場所の指定ウィンドウ

ステップ 17 **Next** をクリックして、デフォルトの保存場所を受け入れます。証明書が正常にインポートされたことを示すウィンドウが表示されます。図 3-10 は、インポートの完了ウィンドウを示しています。

図 3-10　証明書のインポート完了ウィンドウ

ステップ 18　**Finish** をクリックします。最後のセキュリティ警告ウィンドウが表示されます。図 3-11 は、セキュリティ警告を示しています。

図 3-11　証明書のセキュリティ警告

ステップ 19　**Yes** をクリックします。インストールが正常に完了したことを示す別のウィンドウが表示されます。図 3-12 は、インストールの完了ウィンドウを示しています。

図 3-12　インポート完了ウィンドウ

ステップ 20　**OK** をクリックします。

ステップ 21　継続して表示されている 図 3-7 の Certificate ウィンドウで、**OK** をクリックします。

ステップ 22　図 3-6 に示す Security Alert ウィンドウで、**Yes** をクリックします。

ステップ 23　アクセス ポイントのログイン ウィンドウが表示されるので、再度アクセス ポイントにログインする必要があります。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。どちらも大文字と小文字を区別して入力します。

CLI の設定例

次は、「オンライン ヘルプの使用方法」の項（P. 3-13）に記載された手順と同じ働きをする CLI コマンドの例を示しています。

```
ap# configure terminal
ap(config)# hostname br1310
ap(config)# ip domain name company.com
ap(config)# ip name-server 10.91.107.18
ap(config)# ip http secure-server
ap(config)# end
```

この例では、アクセス ポイントのシステム名は *br1310*、ドメイン名は *company.com*、DNS サーバの IP アドレスは 10.91.107.18 です。

この例で使用されているコマンドの詳細は、Cisco IOS Commands Master List, Release 12.3 を参照してください。次のリンクをクリックすると、コマンドのマスター リストを参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123mindx/index.htm

HTTPS 証明書の削除

HTTPS を有効にすると、アクセス ポイントで証明書が自動的に生成されます。ただし、アクセス ポイントの FQDN を変更する必要がある場合、あるいは HTTPS を有効にした後で FQSN 追加する必要がある場合は、証明書を削除しなければならないことがあります。その場合の手順は、次のとおりです。

ステップ 1　Services: HTTP Web Server ページを表示します。

ステップ 2　**Enable Secure (HTTPS) Browsing** チェックボックスをオフにして、HTTPS を無効にします。

ステップ 3　**Delete Certificate** をクリックして、証明書を削除します。

ステップ 4　HTTPS を再度有効にします。アクセス ポイントでは、新しい FQDN を使用して新しい証明書が生成されます。

オンライン ヘルプの使用方法

Web ブラウザ インターフェイスの各ページの上部に表示される Help アイコンをクリックすると、オンライン ヘルプが表示されます。図 3-13 に Print アイコンと Help アイコンを示します。

図 3-13　Print アイコンと Help アイコン

新しいブラウザ ウィンドウにヘルプ ページが表示された後、Select a topic ドロップダウン メニューを使用して、VLAN の設定などの共通の設定作業のヘルプ索引または手順を表示します。

ヘルプ ファイルの場所の変更

シスコの Web サイトには、アクセス ポイントおよびブリッジに関する最新の HTML ヘルプ ファイルがあります。デフォルトでは、アクセス ポイントの Web ブラウザ インターフェイスにある Help ボタンをクリックすると、アクセス ポイント / ブリッジで Cisco.com のヘルプ ファイルが開きます。ただし、ヘルプ ファイルをネットワークにインストールして、ユーザのデバイスからそれらにアクセスすることもできます。ヘルプ ファイルをローカルにインストールする手順は、次のとおりです。

ステップ 1　Cisco.com の Software Center からヘルプ ファイルをダウンロードします。次のリンクをクリックして、Software Center の Wireless Software ページを参照してください。

http://www.cisco.com/public/sw-center/sw-wireless.shtml

アクセス ポイントのソフトウェア バージョンに合ったヘルプ ファイルを選択します。

ステップ 2　ヘルプ ファイルを、使用するアクセス ポイント / ブリッジからアクセスできるネットワーク上のディレクトリへ解凍します。ヘルプ ファイルを解凍すると、ヘルプのバージョン番号とアクセス ポイントのモデル番号に従って名前が付けられたフォルダに、HTML ヘルプ ページが保存されます。

ステップ 3　アクセス ポイント Web ブラウザ インターフェイスで Services: HTTP Web Server ページを参照します。図 3-14 は、HTTP Web Server ページを示しています。

図 3-14　HTTP Web Server ページ

ステップ 4　デフォルトのヘルプ ルート URL 入力フィールドに、ヘルプ ファイルを解凍した場所への完全なパスを入力します。アクセス ポイントの Help ボタンをクリックすると、アクセス ポイントによって、ヘルプのバージョン番号とモデル番号が入力したパスに自動的に追加されます。

（注）　デフォルトのヘルプ ルート URL の入力フィールドには、ヘルプのバージョン番号とデバイスのモデル番号を追加しないでください。ヘルプのバージョンとモデル番号は、アクセス ポイントによって自動的に追加されます。

ヘルプ ファイルをユーザのネットワーク ファイル サーバ *//myserver/myhelp* に解凍した場合、デフォルトのヘルプ ルート URL は次のようになります。

http://myserver/myhelp

表 3-2 は、ヘルプ ファイルの場所と、1100 シリーズのアクセス ポイント用 Help Root URL の例を示しています。

表 3-2　Help Root URL とヘルプ ファイルの場所の例

ファイルの解凍場所	デフォルトのヘルプ ルート URL	ヘルプ ファイルの実際の場所
//myserver/myhelp	http://myserver/myhelp	//myserver/myhelp/123-02.JA/1100

ステップ 5　**Apply** をクリックします。

Web ブラウザ インターフェイスの無効化

Web ブラウザ インターフェイスの使用をすべて無効にするには、Services: HTTP-Web Server ページで **Disable Web-Based Management** チェックボックスをオンにして、**Apply** をクリックします。図 3-15 は、Services: HTTP Web Server ページを示しています。

図 3-15　Services: HTTP Web Server ページ

Web ブラウザ インターフェイスを再度有効にするには、アクセス ポイント CLI で次のグローバル コンフィギュレーション コマンドを入力します。

```
ap(config)# ip http server
```