# Web ブラウザ インターフェイスの使用方法

この章では、ワイヤレス デバイス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。

Web ブラウザ インターフェイスには、ワイヤレス デバイスの設定の変更、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モニタと設定に使用する管理ページが含まれます。

(注) ワイヤレス デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 および Mozilla Firefox バージョン 17 と完全に互換性があります。

(注) ワイヤレス デバイスの設定に、CLI と Web ブラウザ インターフェイスの両方を使用することは避けてください。CLI を使用してワイヤレス デバイスを設定した場合、Web ブラウザ インターフェイスでは、設定が正しく表示されない場合があります。しかし、正しく表示されない場合でも、ワイヤレス デバイスは正しく設定されていることがあります。

## 初めて Web ブラウザ インターフェイスを使用する場合

ワイヤレス デバイスの IP アドレスを使用して、管理システムを参照します。IP アドレスをワイヤレス デバイスに割り当てる方法は、「アクセス ポイントへのログイン」セクション（4-3 ページ）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** アドレス バーにワイヤレス デバイスの IP アドレスを入力し、**Enter** キーを押します。[Summary Status] ページが表示されます。

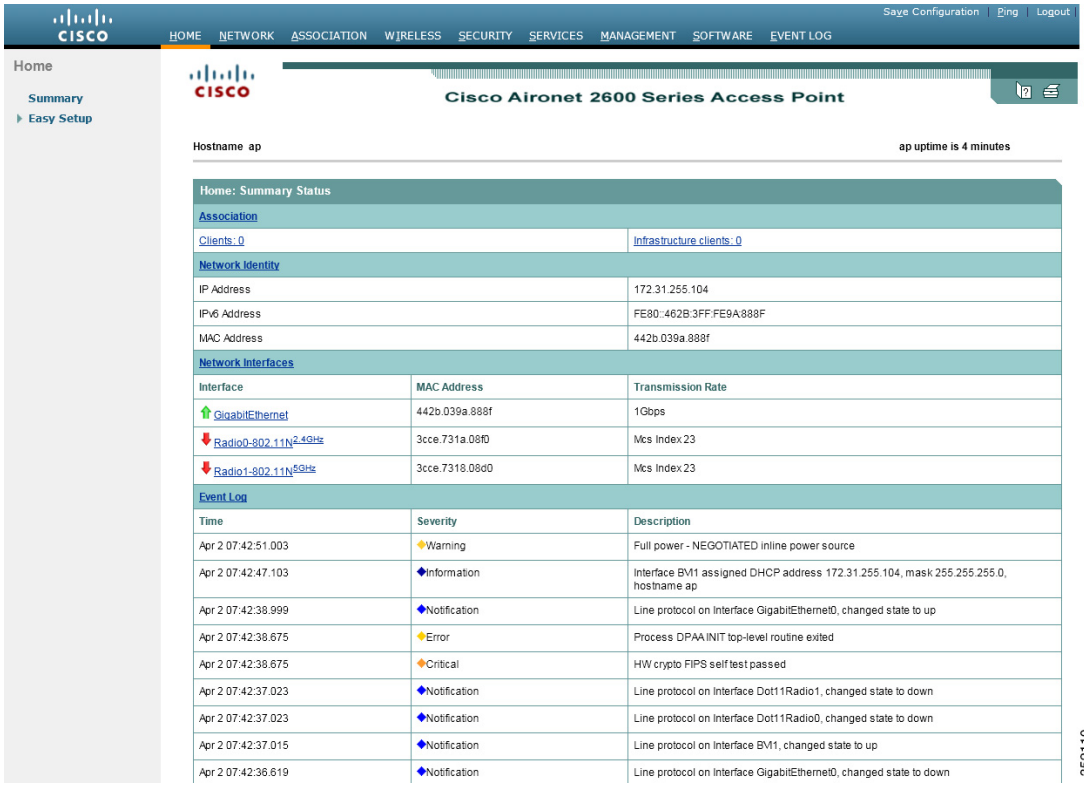
# Web ブラウザ インターフェイスの管理ページの使用方法

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。ページの上部にあるナビゲーション バーを使用して、メイン メニューのオプションを選択できます。ページの左側にもナビゲーション バーがあります。これは、サブ メニューをナビゲートするために使用します。ナビゲーション バーは他の管理ページへ移動する場合に使用し、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）　Web 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、ページの移動は行われません。変更は、[Apply] をクリックした場合にだけ適用されます。

図 2-1 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 2-1　　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 2-1は、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 2-1　管理ページのボタンとリンク*

| ボタン/リンク | 説明 |
|---|---|
| ナビゲーション リンク | |
| Home | ワイヤレス デバイスにアソシエートされた無線デバイスの数、イーサネットおよび無線インターフェイスのステータス、最近のワイヤレス デバイスの活動リストを示す、ワイヤレス デバイスのステータス ページを表示します。 |
| Easy Setup | システム名、IP アドレス、無線ネットワークでの役割などの基本的な設定を行う [Express Setup] ページを表示します。 |
| Network | 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。アクセス ポイント インターフェイス（無線とイーサネット）の設定サブメニューがあります。 |
| 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。 |
| Wireless | 無線ドメイン サービスの設定とデバイスの要約を表示し、WDS の設定ページへのリンクを示します。 |
| 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 | いくつかの無線デバイス機能のステータスを表示し、Telnet/SSH、CDP、ドメイン ネーム サーバ、フィルタ、QoS、SNMP、SNTP、および VLAN の設定ページへのリンクを示します。 |
| Management | 現在のゲスト ユーザのリストを表示し、ゲスト ユーザの設定ページおよび Web 認証ページへのリンクを示します。 |
| Software | 無線デバイス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、ファームウェアをアップグレードおよび管理するための設定ページへのリンクを示します。 |
| Event Log | 無線デバイスのイベント 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。 |
| Logout | AP 設定を保存せずに AP 設定 Web インターフェイスを終了します。 |
| ping | IPv4 または IPv6 アドレスへの ping を実行します。 |
| Save Configuration | AP の現在の設定を NVRAM に保存します。 |

# 入力フィールドの文字制限

Web ブラウザ インターフェイスの入力フィールドで、次の文字を使用することはできません。この制限は、Cisco IOS ソフトウェアを使用するアクセス ポイントのすべてに適用されます。

」
]
+
/

タブ

末尾のスペース

# 安全なブラウザ利用のための HTTPS の有効化

HTTPS を有効にすることで、アクセス ポイントの 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 は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。

（注）HTTPS を有効にすると、ブラウザとアクセス ポイントの接続が解除される可能性があります。接続が解除された場合は、ブラウザのアドレス入力用ボックスの URL を「http://*ip_address*」から「**https://*ip_address***」に変更し、アクセス ポイントに再びログインします。

（注）HTTPS を有効にした場合、大部分のブラウザでは、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を持た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。承認を求めるプロンプトが表示されないようにするには、次の手順の説明に従って、アクセス ポイントの FQDN を作成します。

FQDN を作成し、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、ポップアップ ブロッキング機能を無効にします。

**ステップ 2**　[Easy Setup] > [Network Configuration] を選択します。

[Network Configuration] ページが表示されます。

**ステップ 3**　[Host Name] フィールドにアクセス ポイントの名前を入力し、[Apply] をクリックします。

**ステップ 4**　[Services] > [DNS] ページを選択します。

[Services: DNS - Domain Name Service] ページが表示されます。

**ステップ 5**　[Domain Name System (DNS)] フィールドで、[Enable] オプション ボタンをクリックします。

**ステップ 6**　[Domain Name] フィールドに、会社のドメイン名を入力します。

**ステップ 7**　[Name Server IPv4/IPv6 Addresses] 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 ポイントの FQDN は、システム名とドメイン名を組み合わせたものです。たとえば、システム名が *ap3600*、ドメイン名が *company.com* の場合、FQDN は *ap3600.company.com* です。

**ステップ 9**　DNS サーバの FQDN を入力します。

ヒント　DNS サーバがない場合は、ダイナミック DNS サービスを使用してアクセス ポイントの FQDN を登録できます。インターネットで*ダイナミック DNS* を検索し、有料の DNS サービスを見つけてください。

**ステップ 10**　[Services] > [HTTP] を選択します。

[Services: HTTP - Web Server] ページが表示されます。

**ステップ 11**　[Web-based Configuration Management] フィールドで、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにします。

**ステップ 12**　[Domain Name] フィールドにドメイン名を入力し、[Apply] をクリックします。

（注）　HTTPS を有効にすると、自動的に HTTP が無効になります。HTTPS が有効にされた状態で HTTP アクセスを維持するには、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにしてから、[Enable Standard (HTTP) Browsing] チェックボックスをオンにします。標準 HTTP と HTTPS の両方を有効にできますが、いずれか一方のみを有効にすることを推奨します。

警告メッセージが表示され、以降はアクセス ポイントの参照にセキュア HTTP が使用されることが伝えられます。警告メッセージには、*https* を含む新しい URL も表示されます。アクセス ポイントを参照するには、この URL を使用する必要があります。

**ステップ 13**　警告メッセージ ボックスで [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のアドレスが、*http://*<ip-address> から *https://*<ip-address> に変更されます。

**ステップ 14**　別の警告メッセージが表示され、アクセス ポイントのセキュリティ証明書が、信頼できる認証局によって発行されたものではないことが伝えられます。ただし、この警告メッセージは無視できます。[Continue to this Website（not recommended）] をクリックします。

（注）　次の手順では、Microsoft Internet Explorer を使用していることを前提としています。そうでない場合は、自己署名証明書を使用した Web サイトへのアクセス方法の詳細について、ご使用のブラウザのマニュアルを参照してください。

**ステップ 15**　アクセス ポイントのログイン ウィンドウが表示されます。アクセス ポイントに再びログインします。デフォルトのユーザ名は *Cisco*（大文字小文字を区別）、デフォルトのパスワードは *Cisco*（大文字小文字を区別）です。

**ステップ 16**　アクセス ポイントのセキュリティ証明書を表示するには、アドレス バーの [Certificate error] アイコンをクリックします。

**ステップ 17**　[View Certificate] をクリックします。

**ステップ 18**　[Certificate] ウィンドウで、[Install Certificate] をクリックします。
Microsoft Windows の証明書のインポート ウィザードが表示されます。

**ステップ 19**　[Next] をクリックします。
次に表示される画面では、証明書を保管する場所を確認されます。システムのデフォルトの保管領域を使用することを推奨します。

**ステップ 20**　[Next] をクリックし、デフォルトの保管領域を承認します。
これで、正常に証明書がインポートされます。

**ステップ 21**　[Finish] をクリックします。
セキュリティ警告が表示されます。

**ステップ 22**　[Yes] をクリックします。
インストールが成功したことを示すメッセージ ボックスが表示されます。

**ステップ 23**　[OK] をクリックします。

### CLI の設定例

次の例は、「安全なブラウザ利用のための HTTPS の有効化」セクション（2-4 ページ）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# hostname ap3600
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 *ap3600*、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については、リリース 12.4 の『Cisco IOS Commands Master List』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/ios124/124mindx/124htnml.htm

## HTTPS 証明書の削除

HTTPS を有効にすると、アクセス ポイントは証明書を自動的に生成します。ただし、HTTPS を有効にした後でアクセス ポイントの完全修飾ドメイン名（FQDN）を変更したり、FQDN を追加したりする必要が生じた場合、証明書の削除が必要になることがあります。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、HTTPS を無効にします。

**ステップ 3**　[Delete Partial SSL certificate] をクリックして証明書を削除します。

**ステップ 4**　[Apply] をクリックします。アクセス ポイントは、新しい FQDN を使用して新しい証明書を生成します。

### HTTPS 証明書を削除する CLI コマンド

グローバル コンフィギュレーション モードでは、次のコマンドを使用して HTTPS 証明書を削除します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | **no ip http secure-server** | HTTPS を無効にします。 |
| ステップ 2 | **crypto key zeroize rsa** *name-of-rsa-key* | HTTP サーバ用の RSA キーを削除します。さらに、削除されるキーを使用して発行されたルータ証明書（HTTPS 証明書）もすべて削除されます。 |

# オンライン ユーザ ガイドの使用

Web ブラウザ インターフェイスで、ホーム ページの上部にあるヘルプ アイコンをクリックすると、このガイドのオンライン バージョン（『Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points』）にアクセスできます。ガイドをオンラインで表示することも、PDF バージョンのガイドをダウンロードしてオフラインで参照することもできます。オンライン ガイドは定期的に更新されるため、最新の情報を入手できます。

# 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中止するには、[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、[Apply] をクリックします。

Web ブラウザ インターフェイスを再び有効にするには、アクセス ポイントの 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
```