CHAPTER 3

セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューションについて説明します。この章の内容は、次のとおりです。

Cisco Unified Wireless Network Solution セキュリティ

Cisco Unified Wireless Network Solution セキュリティ ソリューションは、802.11 アクセス ポイントのセキュリティを構成する潜在的に複雑なレイヤ 1、レイヤ 2、およびレイヤ 3 を 1 つの単純なポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを無線 LAN ごとにカスタマイズできます。これは、単純で、統一された、体系的なセキュリティ管理ツールを提供します。

企業での無線 LAN 展開の最も大きな課題の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格なアクセス ポイントの登場も新たな問題で、企業ネットワークに接続して man-in-the-middle アタックおよび DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが無線 LAN セキュリティの最新技術を採用することをためらっています。

レイヤ 1 ソリューション

Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティ ソリューションによって、すべてのクライアントはアクセスの試行回数を、オペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、そのクライアントは、オペレータが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。そのオペレーティング システムは、無線 LAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X 動的キーや Wi-Fi Protected Access（WPA）動的キーなど業界標準のセキュリティ ソリューションも実装できます。Cisco Unified Wireless Network Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、または WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラとアクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP の問題の解決をさらに進めるには、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）などの業界標準のレイヤ 3 セキュリティ ソリューションを使用します。

Cisco Unified Wireless Network Solution では、ローカルおよび RADIUS Media Access Control（RADIUS MAC; RADIUS メディア アクセス制御）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カード MAC アドレスの既知のリストがある小規模のクライアント グループに適しています。Cisco Unified Wireless Network Solution は、ローカルおよび RADIUS ユーザ / パスワード認証もサポートします。この認証は、小規模から中規模のクライアント グループに適しています。

シングル ポイントでの設定ポリシー マネージャのソリューション

Cisco Unified Wireless Network Solution に WCS を装備した場合、システム全体のセキュリティ ポリシーを無線 LAN ごとに設定できます。スモール オフィス、ホームオフィス（SOHO）のアクセス ポイントでは、アクセス ポイントごとにセキュリティ ポリシーを個別に設定する必要があります。また、複数のアクセス ポイントにわたってセキュリティ ポリシーを設定するには、サードパーティのアプライアンスを使用する必要があります。Cisco Unified Wireless Network Solution セキュリティ ポリシーは WCS からシステム全体に適用できるため、エラーを除去することができ、全体的な作業量が大幅に減少します。

不正アクセス ポイントのソリューション

この項では、不正アクセス ポイントに対するセキュリティ ソリューションについて説明します。

不正アクセス ポイントの問題

不正アクセス ポイントは、正規のクライアントをハイジャックし、プレーン テキストまたは他の DoS 攻撃や man-in-the-middle アタックを使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正アクセス ポイントを使用して、パスワードやユーザ名などの機密情報を取得できるのです。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームはアクセス ポイントを模倣し、特定の無線 LAN クライアント アダプタに伝送して、他のすべてのアダプタには待機するように指示します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。したがって、無線 LAN サービス プロバイダーは、空間からの不正アクセス ポイントの締め出しに強い関心を持っています。

オペレーティング システムのセキュリティ ソリューションでは、「不正アクセス ポイントのタギングと阻止」の説明にあるように、Radio Resource Management（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的に監視し、不正アクセス ポイントを自動的に検出し、それらを特定します。

不正アクセス ポイントのタギングと阻止

WCS を使用して Cisco Unified Wireless Network Solution を監視している場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントが MAC アドレスで表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 つから 4 つのアクセス ポイントに対して、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらのクライアントに認証解除とアソシエート解除のメッセージを送信することによって阻止する）のいずれかを実行します。

統合されたセキュリティ ソリューション

Cisco Unified Wireless Network Solution では、次の統合されたセキュリティ ソリューションも用意されています。

- Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、認可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco Unified Wireless Network Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。

- コントローラおよびアクセス ポイントには、システム全体の認証および認可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが実現されています。
- オペレーティング システムのセキュリティ ポリシーは個別の無線 LAN に割り当てられ、アクセス ポイントは設定されたすべての無線 LAN（最大 16）に同時にブロードキャストします。このポリシーにより、干渉を増加し、システム スループットを低下するアクセス ポイントの追加が不要になる場合があります。
- オペレーティング システムのセキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間を監視し、それらを検出したときはオペレータに通知します。
- オペレーティング システムのセキュリティは、業界標準の AAA サーバで動作し、システム統合が単純で簡単です。
- Cisco Intrusion Detection System（CIDS; シスコ侵入検知システム）/Intrusion Protection System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、コントローラにそれらのクライアントの無線ネットワークへのアクセスをブロックするように指示します。
- オペレーティング システムのセキュリティ ソリューションは、通常、高い処理能力を必要とする、包括的なレイヤ 2 およびレイヤ 3 の暗号化アルゴリズムを実現します。コントローラに VPN/ 拡張セキュリティ モジュールを装備することで、高度なセキュリティ設定に必要なハードウェアとしての機能も実現でき、暗号化を別のサーバで行う必要はありません。

WCS を使用した Cisco Unified Wireless Network Solution のレイヤ 3 モードからレイヤ 2 モードへの変換

WCS ユーザ インターフェイスを使用して Cisco Unified Wireless Network Solution をレイヤ 3 モードからレイヤ 2 LWAPP 転送モードに変換する手順は、次のとおりです。

（注）　IOS ベースの Lightweight アクセス ポイントでは、レイヤ 2 LWAPP モードはサポートされません。このようなアクセス ポイントは、レイヤ 3 でしか実行できません。

（注）　この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1　コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

（注）　変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2　WCS ユーザ インターフェイスにログインします。LWAPP 転送モードをレイヤ 3 からレイヤ 2 に変換する手順は、次のとおりです。

a. **Configure > Controllers** の順にクリックし、All Controllers ページに移動します。
b. 目的のコントローラの IP アドレスをクリックして、*IP Address* > Controller Properties ページを表示します。
c. サイドバーで、**System > General** の順にクリックして、*IP Address* > General ページを表示します。
d. LWAPP 転送モードを **Layer2** に変更し、**Save** をクリックします。
e. WCS で次のメッセージが表示された場合、**OK** をクリックします。

```
Please reboot the system for the LWAPP Mode change to take effect.
```

ステップ 3　Cisco Unified Wireless Network Solution を再起動する手順は、次のとおりです。

a. *IP Address* > Controller Properties ページに戻ります。
b. **System > Commands** の順にクリックして、*IP Address* > Controller Commands ページを表示します。
c. Administrative Commands の下で、**Save Config To Flash** を選択し **GO** をクリックして、変更した設定をコントローラに保存します。
d. **OK** をクリックして、次に進みます。
e. Administrative Commands の下で、**Reboot** を選択し **GO** をクリックして、コントローラをリブートします。
f. **OK** をクリックし、保存して再度ブートすることを確認します。

ステップ 4　コントローラが再度ブートした後で LWAPP 転送モードがレイヤ 2 になっていることを確認する手順は、次のとおりです。

a. **Monitor > Devices** > **Controllers** の順にクリックし、Controllers > Search Results ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、Controllers > *IP Address* > Summary ページを表示します。

c. General の下で、現在の LWAPP 転送モードが Layer2 になっていることを確認します。

これで、レイヤ 3 からレイヤ 2 への LWAPP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

WCS に対するファイアウォールの設定

WCS サーバと WCS ユーザ インターフェイスがファイアウォールの同じ側にない場合、ファイアウォール上の次のポートが双方向のトラフィックに対してオープンになっていない限り、これらは通信できません。

- 80（初期 HTTP 用）
- ポート 69（TFTP）
- ポート 162（トラップ）
- ポート 443（HTTPS）

これらのポートをオープンにして、WCS サーバと WCS ユーザ インターフェイスとの間の通信を許可するようにファイアウォールを設定します。

アクセス ポイント認証

アクセス ポイントが認証に使用する証明書の種類に応じて、認可済みアクセス ポイントの一覧を表示できます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　IP Address 列で URL の 1 つをクリックします。

ステップ 3　左側のサイドバーのメニューから **Security > AP Authorization** の順に選択します。

ステップ 4　ウィンドウの AP Policies 部分に、アクセス ポイントの認証が有効かどうかが示されます。また、自己署名証明書（SSC AP）の承認が有効かどうかも示されます。通常は、アクセス ポイントは AAA または証明書によって認証されます。（SSC は 4400 コントローラおよび 200 コントローラのみに使用）。

これらの値を変更するには、Select a Command ドロップダウン メニューから **Edit AP Policies** を選択し、**GO** をクリックします。

ステップ 5　AP Authorization List 部分にアクセス ポイントの無線 MAC アドレス、証明書の種類、およびキー ハッシュが表示されます。別の認証エントリを追加するには、Select a Command ドロップダウン メニューから **Add AP Auth Entry** を選択し、**GO** をクリックします。

ステップ 6　ドロップダウン　メニューからこのコントローラに適用するテンプレートを選択して　**Apply**　をクリックします。アクセス ポイント認証の新しいテンプレートを作成するには、**click here** をクリックしてテンプレート作成ページにリダイレクトされるようにします。新しいテンプレートの作成手順については、「アクセス ポイント認証の設定」の項（P. 10-38）を参照してください。

Management Frame Protection （MFP; 管理フレーム保護）

Management Frame Protection（MFP）は、アクセス ポイントとクライアント間で受け渡される、無防備の 802.11 管理メッセージと暗号化されていない 802.11 管理メッセージにセキュリティを提供します。MFP では、インフラストラクチャとクライアントの両方がサポートされます。WCS ソフトウェア リリース 4.0 ではインフラストラクチャ MFP のみがサポートされている一方で、WCS ソフトウェア リリース 4.1 では、インフラストラクチャとクライアント MFP の両方がサポートされています。

- **インフラストラクチャ MFP —** DoS 攻撃を引き起こし、アソシエーションおよびプローブでネットワークを氾濫させ、不正アクセス ポイントをさしはさみ、QoS および無線測定フレームの攻撃によりネットワーク パフォーマンスに影響を与える敵対者を発見することにより、管理フレームを保護します。

  特に、インフラストラクチャ MFP では、アクセス ポイントによって送信される管理フレームに Message Integrity Check Information Element（MIC IE）を追加して、802.11 セッション管理機能を保護します。Message Integrity Check Information Element（MIC IE）はその後ネットワーク内のその他のアクセス ポイントにより検証されます。インフラストラクチャ MFP は、受動です。侵入を探知して報告できますが、侵入を阻止する手段がありません。

- **クライアント MFP —** スプーフされたフレームから認可済みクライアントを保護するので、無線 LAN に対する一般的な攻撃の多くが効果的でなくなります。認証解除攻撃などの大多数の攻撃は、有効なクライアントと競合することにより、単にパフォーマンスが低下します。

  特に、アクセス ポイントとクライアントの両方が、スプーフされたクラス 3 管理フレーム（つまり、認証済みでアソシエートが完了しているアクセス ポイントとクライアント間で受け渡される管理フレーム）をドロップして予防措置を講じることができるように、クライアント MFP ではアクセス ポイントと CCXv5 クライアント間で送信される管理フレームが暗号化されます。クライアント MFP では、クラス 3 ユニキャスト管理フレーム（アソシエーション解除、認証解除、および QoS (WMM) アクション）を保護するために、IEEE 802.11i で定義されるセキュリティ メカニズムを利用します。クライアント MFP はアクティブです。最も一般的な DoS 攻撃から、クライアントアクセス ポイント セッションを保護できます。セッションのデータ フレームで使用されるのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。アクセス ポイントまたはクライアントによって受信されるフレームを復号化できない場合、フレームはドロップされ、このイベントがコントローラに報告されます。

  クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしている必要があり、TKIP または AES-CCMP のいずれかを使用する WPA2 をネゴシエートする必要があります。PMK を取得するために、EAP または PSK を使用できます。アクセス ポイント間、またはレイヤ 2 とレイヤ 3 の高速ローミングでセッション キーを配信するために、CCKM およびコントローラ モビリティ管理が使用されます。

  ブロードキャスト フレームに対する攻撃を防ぐために、CCXv5 をサポートしているアクセス ポイントは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントとアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄します。

  クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足します。これは、インフラストラクチャ MFP が、無効なクラス 1 管理フレームとクラス 2 管理フレームだけでなく、クライアント MFP 対応ではないクライアントに送信される無効なユニキャスト フレームを検出して報告し続けるためです。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は、次の 3 つの主要なコンポーネントで構成されています。

- **Management frame protection**：アクセス ポイントは、各フレームに MIC IE を追加することにより、送信する管理フレームを保護します。フレームのコピー、変更、または再生を試みると、MIC が無効となり、MFP フレームを検出するように設定された受信アクセス ポイントはその矛盾を報告します。
- **Management frame validation**：インフラストラクチャ MFP でアクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。これにより、MC IE が存在し（発信側が MFP フレームを送信するよう設定されている場合）、管理フレーム

の中身が一致していることを確認できます。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID から有効な MIC IE が含まれていないフレームを受信した場合は、その矛盾がネットワーク管理システムに報告されます。タイムスタンプが適切に機能するには、すべてのコントローラで Network Time Protocol（NTP; ネットワーク タイム プロトコル）が同期されている必要があります。

- **イベント報告** : アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集積して、SNMP トラップ経由でネットワーク管理システムに結果を報告できます。

（注）　クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP はデフォルトで有効となり、グローバルに無効にできます。以前のソフトウェア リリースからアップグレードするときに、アクセス ポイント認証が有効にされている場合、インフラストラクチャ MFP はグローバルに無効にされます。これは、2 つの機能が相互に排他的であるためです。インフラストラクチャ MFP がグローバルに有効にされている場合、選択した WLAN に対してシグニチャ生成（送信フレームへの MIC の追加）を無効にし、選択したアクセス ポイントに対して検証を無効にできます。

WLAN テンプレートで MFP を設定します。「WLAN テンプレートの設定」の項（P. 10-11）を参照してください。

MFP の使用に関するガイドライン

MFP の使用に関するガイドラインは、次のとおりです。

- MFP では、1500 シリーズのメッシュ アクセス ポイントを除く、Cisco Aironet Lightweight アクセス ポイントの使用がサポートされています。
- Lightweight アクセス ポイントは、ローカル モードとモニタ モードでインフラストラクチャ MFP をサポートし、アクセス ポイントがコントローラに接続されているときには REAP モードとハイブリッド REAP モードをサポートします。ローカル モードではクライアント MFP をサポートし、ブリッジ モードではハイブリッド REAP モードをサポートします。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでのみ使用がサポートされています。
- CCXv5 以外のクライアントは、クライアント MFP が無効になっているかオプションの場合に、WLAN にアソシエートできます。

Intrusion Detection System（IDS; 侵入検知システム）の設定

Cisco Intrusion Detection System（CIDS; シスコ侵入検知システム）/Intrusion Protection System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、コントローラにそれらのクライアントの無線ネットワークへのアクセスをブロックするように指示します。このシステムにより、ワーム、スパイウェア / アドウェア、ネットワーク ウィルス、およびアプリケーションの不正使用などの脅威を検出し、分類し、阻止するための重要なネットワーク保護を実現できます。IDS で攻撃の検出に使用できる方法は 2 つあります。

- IDS センサー（レイヤ 3 用）
- IDS シグニチャ（レイヤ 2 用）

IDS センサーの表示

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから **Security > IDS Sensor Lists** の順に選択します。IDS Sensor ウィンドウが表示されます。このページには、このコントローラに設定されているすべての IDS センサーが一覧表示されます。

回避したクライアントの表示

IDS センサーが不審なクライアントを検出した場合は、このクライアントを回避するようにコントローラに警告します。回避するクライアントが現在モビリティ グループのアクセス ポイントおよびコントローラに関連付けられている場合は、回避エントリは同じモビリティ グループ内のすべてのコントローラに配信され、アンカー コントローラはこのクライアントを動的な除外リストに追加し、外部コントローラはクライアントを削除します。次回そのクライアントがコントローラに接続しようとしたときは、アンカー コントローラはハンドオフを拒否し、クライアントを除外している外部コントローラに知らせます。

IDS センサーに回避対象として識別されたクライアントの一覧を表示する手順は、次のとおりです。

ステップ 1　左側のサイドバーのメニューから **Monitor > Security** を選択します。

ステップ 2　**Shunned Clients** をクリックします。Shunned Client ウィンドウが表示されます。このページには、回避した各クライアントの IP アドレス、MAC アドレス、およびその不審クライアントを検出した IDS センサーの IP アドレスを表示します。

IDS シグニチャの設定

コントローラにおいて、*IDS シグニチャ*、または受信する 802.11 パケットのさまざまな種類の攻撃の識別に使用する、ビットパターンのマッチング ルールを設定できます。シグニチャが有効になっている場合は、コントローラに接続されたアクセス ポイントは受信した 802.11 データまたは管理フレームにおいてシグニチャ分析を実行し、矛盾をコントローラへ報告します。

シグニチャの設定方法は、次のとおりです。

IDS シグニチャのアップロード

コントローラから IDS シグニチャをアップロードする手順は、次のとおりです。

ステップ 1　シスコからシグニチャ ファイルを入手します（以降、*標準シグニチャ ファイル*）。「IDS シグニチャのダウンロード」の項（P. 3-12）に従い独自のシグニチャ ファイル（以降、*カスタム シグニチャ ファイル*）を作成することもできます。

ステップ 2　シグニチャのダウンロードに Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバを使用できることを確認します。TFTP サーバをセットアップするときのガイドラインは、次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポート経由でダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバはディストリビューション システム ネットワーク ポートと同じサブネットでも異なるサブネットでもかまいません。
- Cisco WCS の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを WCS と同じコンピュータ上で実行することはできません。

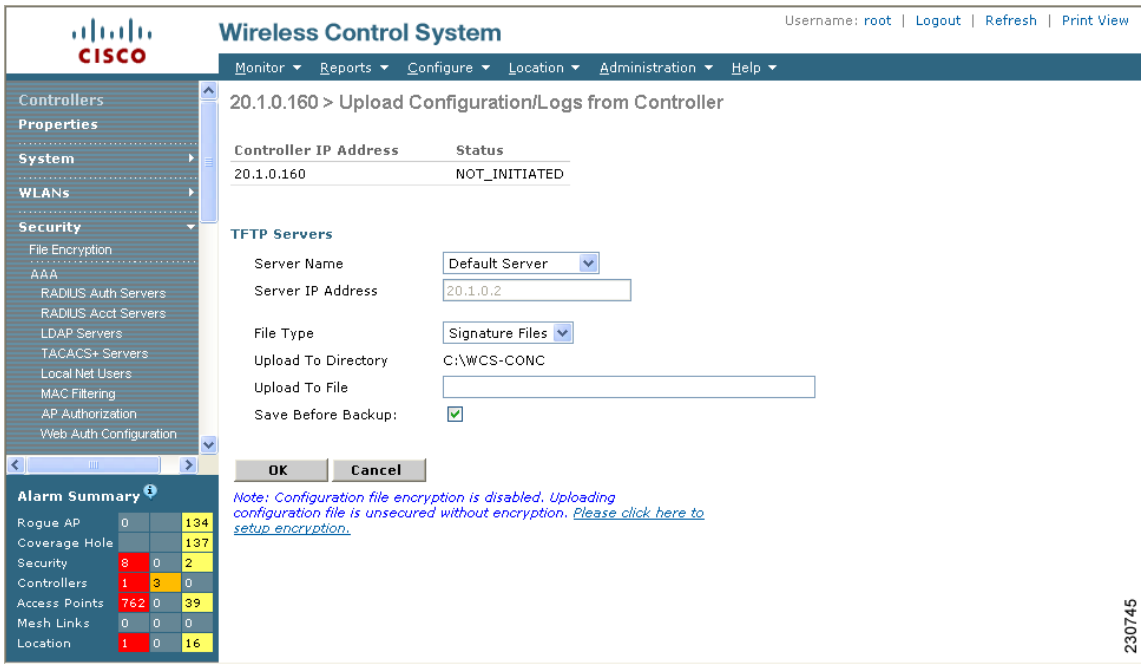
ステップ 3　**Configure > Controllers** の順に選択します。

ステップ 4　IP アドレスをクリックしてコントローラを選択します。

ステップ 5　左側のサイドバーのメニューから **Security** を選択し、**Standard Signatures** または **Custom Signatures** を選択します。

ステップ 6　Select a Command ドロップダウン メニューから、**Upload Signature Files from Controller** を選択します。図 3-1 は表示されるウィンドウを示しています。

図 3-1　シグニチャ ファイルのアップロード



ステップ 7　転送に使用している TFTP サーバ名を指定します。

ステップ 8　TFTP が新しい場合は、Server IP Address パラメータで TFTP IP アドレスを入力します。

ステップ 9　File Type ドロップダウン メニューから **Signature Files** を選択します。

ステップ 10　このシグニチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。Upload to File パラメータで別のディレクトリに変更できます（このパラメータは、Server Name がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグニチャ ファイルの拡張子として _std.sig を、カスタム シグニチャ ファイルの拡張子として _custom.sig を追加します。

ステップ 11　**OK** をクリックします。

IDS シグニチャのダウンロード

標準のシグニチャ ファイルが既にコントローラ上にあり、それにカスタマイズされたシグニチャをダウンロードする場合は、次の手順を実行します。

ステップ 1　**Configure** > **Controllers** の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　**System** > **Commands** の順に選択します。

ステップ 4　Upload/Download Commands ドロップダウン メニューから、**Download IDS Signatures** を選択し、**GO** をクリックします。

ステップ 5　シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6　File is Located On パラメータから **local machine** を選択します。ファイル名および、サーバのルート ディレクトリに対して相対的なパスが分かる場合は、TFTP サーバを選択することもできます。

ステップ 7　Maximum Retries パラメータに、シグニチャ ファイルのダウンロードを試みる最大時間を入力します。

ステップ 8　Timeout パラメータに、シグニチャ ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 9　シグニチャ ファイルは c:¥tftp ディレクトリにアップロードされます。そのディレクトリでのローカル ファイル名を指定し、Browse ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 10　何らかの理由で転送がタイムアウトした場合には、File Is Located On パラメータの TFTP サーバ オプションを選択すると、Server File Name が読み込まれ、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。まず、ローカル ファイルは管理者のワークステーションから WCS 自体の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の動作のため、ファイルはすでに WCS サーバの TFTP ディレクトリに配置され、ここでダウンロード Web ページが自動的にファイル名を読み込みます。

ステップ 11　**OK** をクリックします。

IDS シグニチャの有効化または無効化

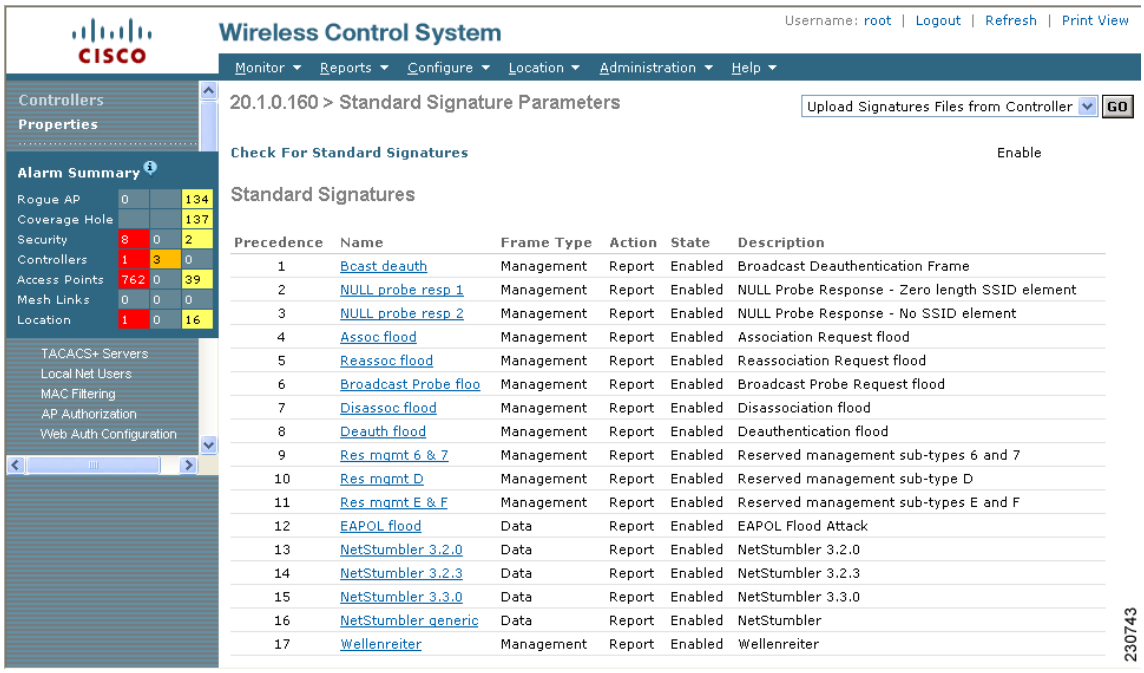
IDS シグニチャを有効化または無効化する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから **Security** を選択し、**Standard Signatures** または **Custom Signatures** を選択します。図 3-2 は表示される画面のサンプルを示しています。

図 3-2　標準シグニチャの確認

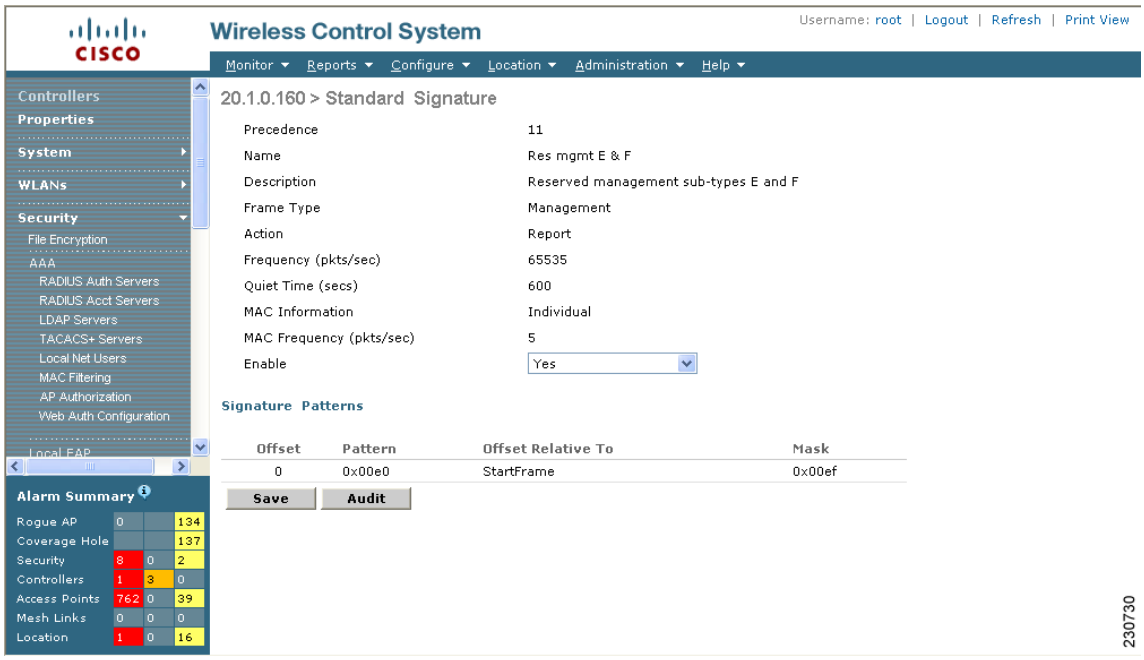


ステップ 4　個々のシグニチャを有効または無効にするには、有効または無効にしたい攻撃の種類の **Name** 列をクリックします。図 3-3 は詳細シグニチャ画面のサンプルを示しています。

Standard Signature Parameters ウィンドウには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。Custom Signatures ウィンドウには、現在コントローラ上にあるユーザ指定のシグニチャの一覧が表示されます。シグニチャ ウィンドウまたは詳細シグニチャ ウィンドウに次の情報が表示されます。

- Precedence：コントローラがシグニチャ チェックを実行する順序または優先順位
- Name：シグニチャによって検出を試みる攻撃の種類
- Description：シグニチャによって検出を試みる攻撃の種類についての詳細説明
- Frame Type：シグニチャによってセキュリティ攻撃を探す管理フレームまたはデータ フレームの種類
- Action：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。なにも処置をとらない場合は *None*、検出を報告する場合は *Report* となります。
- Frequency：シグニチャの周波数、または攻撃の検出前にアクセス ポイント レベルの検出において識別する必要のある、秒ごとの一致パケット数
- Quiet Time：攻撃が検出されなくなってからアラームを停止するまでの時間の長さ（秒）。この時間は MAC 情報がすべてまたは両方ある場合のみ表示されます。
- MAC Information：アクセス ポイント レベルの検出においてシグニチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。
- MAC Frequency：シグニチャの MAC の周波数、または攻撃の検出前にコントローラ レベルで識別する必要のある、秒ごとの一致パケット数
- Signature Patterns：セキュリティ攻撃の検出に使用するパターン

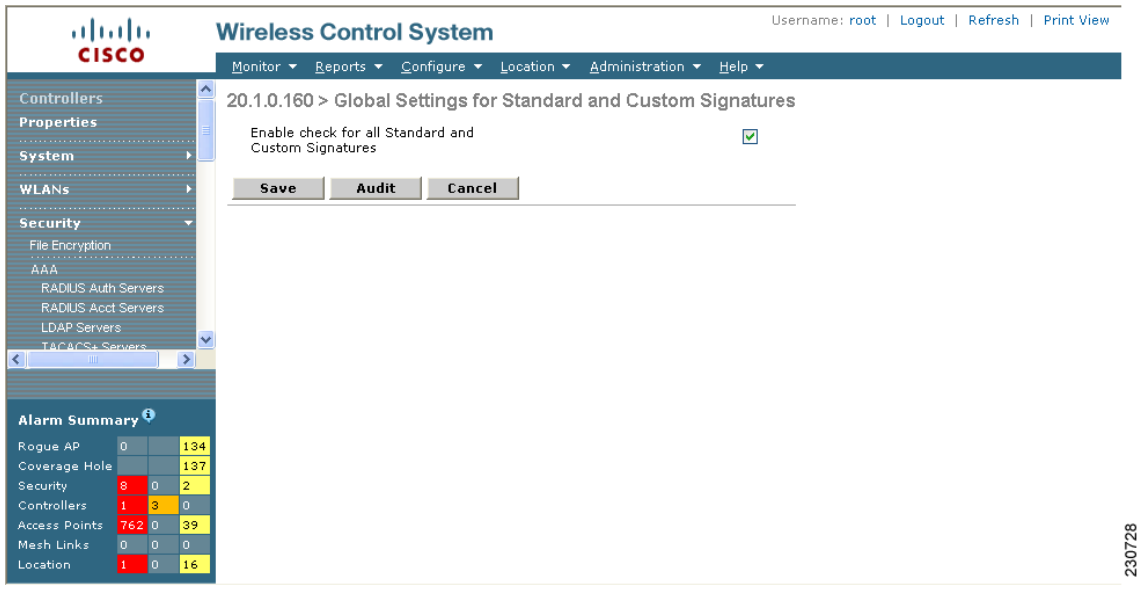
図 3-3　標準シグニチャ



ステップ 5　Enable ドロップダウン メニューで、**yes** を選択します。カスタマイズされたシグニチャをダウンロードしているため、_custom.sgi という名前のファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグニチャを無効にする必要があります。（たとえば、ブロードキャスト プローブの大量送信をカスタマイズしている場合に、ブロードキャスト プローブの大量送信を標準シグニチャでは無効にしたいがカスタム シグニチャでは有効にしたい場合がある）

ステップ 6　コントローラの現在の標準シグニチャとカスタム シグニチャをすべて有効にするには、Select a Command ドロップダウン リストから **Edit Signature Parameters**（図 3-2 の画面）を選択し、**GO** をクリックします。Global Settings for Standard and Custom Signature ウィンドウが表示されます（図 3-4 参照）。

図 3-4　標準シグニチャとカスタム シグニチャのグローバル設定



ステップ 7　**Enable Check for All Standard and Custom Signatures** チェックボックスをオンにします。これにより、ステップ 5 で有効にしたように、個々に選択したシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、前にステップ 5 で有効にしていても、すべてのファイルは無効になります。シグニチャが有効になっている場合は、コントローラに接続されたアクセス ポイントは受信した 802.11 データまたは管理フレームにおいてシグニチャ分析を実行し、矛盾をコントローラへ報告します。

ステップ 8　**Save** をクリックします。

IDS シグニチャのイベントの表示

有効なシグニチャに検出された攻撃の数を確認する手順は、次のとおりです。

ステップ 1　**Monitor > Events** または **Monitor > Alarms** の順に選択します。

ステップ 2　左側のサイドバーの Event Category ドロップダウン メニューから、**Security** を選択し、**Search** をクリックします。

Web ログインの有効化

Web 認証により、ゲストはブラウザを起動すると自動的に Web 認証ページにリダイレクトされます。ゲストは、この Web ポータルから WLAN にアクセスできます。この認証メカニズムを使用している無線 LAN 管理者は、暗号化されていないゲスト アクセスまたは暗号化されたゲスト アクセスを提供するオプションを用意する必要があります。ゲスト ユーザは、SSL で暗号化される有効なユーザ名とパスワードを使用して無線ネットワークにログインできます。Web 認証アカウントはローカルに作成するか、RADIUS サーバで管理できます。Cisco Wireless LAN Controller は Web 認証クライアントをサポートするように設定できます。コントローラで提供される Web 認証ページを置き換えるテンプレートを作成するには、「Web 認証テンプレートの設定」の項（P. 10-46）を参照してください。

ステップ 1　**Configure > Controller** の順に選択します。

ステップ 2　IP Address 列で IP アドレス URL をクリックして、Web 認証を有効にするコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから **Security > Web Auth Configuration** の順に選択します。

ステップ 4　ドロップダウン メニューから適切な Web 認証の種類を選択します。選択肢は、デフォルトの内部、カスタマイズ Web 認証、または外部です。

- デフォルトの内部を選択する場合でも、ページ　タイトル、メッセージ、およびリダイレクト URL を変更することや、ロゴを表示するかどうかを選択できます。手順 5 に進みます。
- カスタマイズされた Web 認証を選択する場合は、「カスタマイズされた Web 認証のダウンロード」の項（P. 3-18）に進んでください。
- 外部を選択する場合は、認証に成功した後でリダイレクトする URL を入力する必要があります。たとえば、このフィールドに入力した値が http://www.company.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 5　会社のロゴを表示する場合は、Logo Display チェックボックスをクリックします。

ステップ 6　Web 認証ページに表示するタイトルを入力します。

ステップ 7　Web 認証ページに表示するメッセージを入力します。

ステップ 8　認証に成功した後でユーザがリダイレクトされる URL を指定します。たとえば、このフィールドに入力した値が http://www.company.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 9　**Save** をクリックします。

カスタマイズされた Web 認証のダウンロード

前の項の手順 4 において、カスタマイズされた Web 認証オプションを選択した場合は、次の手順に従います。カスタマイズ Web 認証ページをコントローラにダウンロードできます。カスタマイズ Web ページは、ユーザ Web アクセス用のユーザ名とパスワードを設定するために作成されます。

カスタマイズ Web 認証をダウンロードする際は、次のガイドラインに従う必要があります。

- ユーザ名を指定する。
- パスワードを指定する。
- リダイレクト URL は、元の URL から引用した後、非表示の入力項目として保持する。
- 操作 URL は、元の URL から引用および設定する。
- 戻りステータス コードをデコードするスクリプトを含める。
- メイン ページで使用されるすべてのパスは相対パスとする。

ダウンロードの前に、次の手順を実行する必要があります。

ステップ 1　プレビュー画像の上でクリックして、サーバからサンプルの login.html バンドルをダウンロードします。login.html ファイルの例については、図 3-5 を参照してください。ダウンロードしたバンドルは .TAR ファイルとなります。

図 3-5　Login.html

ステップ 2　Login.html を開いて編集し、これを .tar または .zip ファイルとして保存します。

（注）　「承諾条件を読んで送信」するよう、任意のテキストまたは HTML エディタで Submit ボタンのテキストを編集できます。

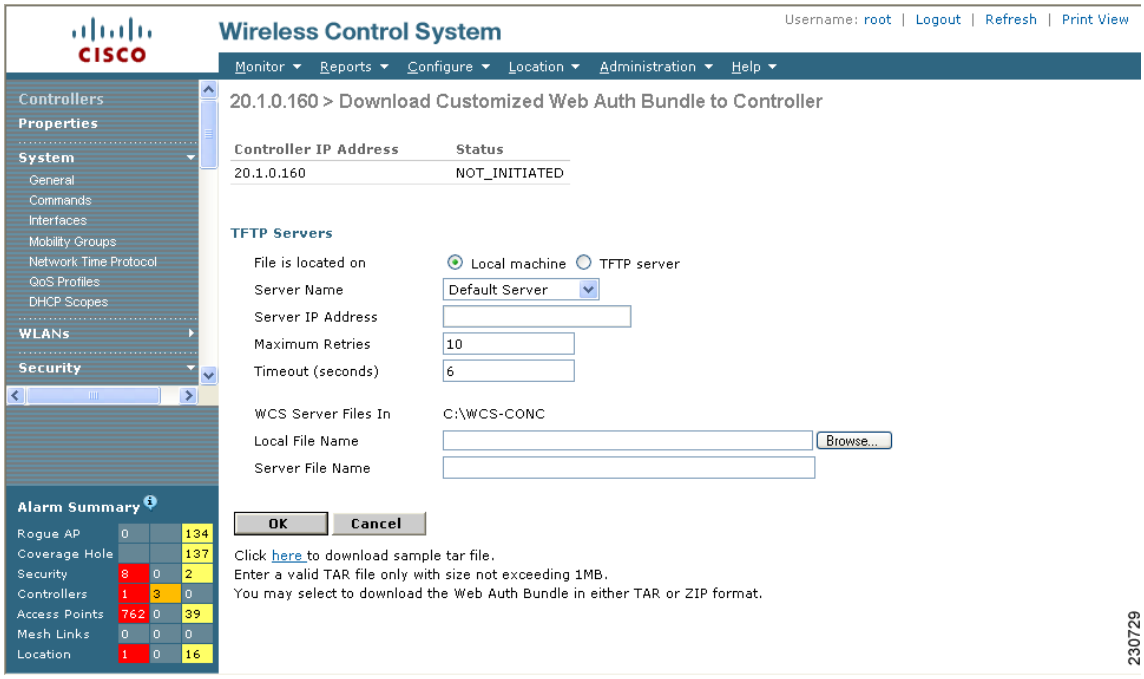
ステップ 3　ダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップするときのガイドラインは、次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポート経由でダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバはディストリビューション システム ネットワーク ポートと同じサブネットでも異なるサブネットでもかまいません。

- Cisco WCS の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを WCS と同じコンピュータ上で実行することはできません。

ステップ 4　リンク「After editing the HTML you may click **here** to redirect to the Download Web Auth Page」の **here** をクリックして、.tar ファイルまたは .zip ファイルをコントローラにダウンロードします。Download Customized Web Auth Bundle to Controller ウィンドウが表示されます（図 3-6 参照）。

図 3-6　カスタマイズ Web 認証バンドルのコントローラへのダウンロード



（注）　バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 5　File is Located On パラメータから **local machine** を選択します。ファイル名および、サーバのルートディレクトリに対して相対的なパスが分かる場合は、TFTP サーバを選択することもできます。

（注）　ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、WCS では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルのみを指定します。

ステップ 6　Timeout パラメータに、ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 7　WCS Server Files In パラメータには WCS サーバ ファイルを配置する場所を指定します。そのディレクトリでのローカル ファイル名を指定し、Browse ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 8　何らかの理由で転送がタイムアウトした場合には、File Is Located On パラメータの TFTP サーバ オプションを選択すると、Server File Name が読み込まれ、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。まず、ローカル ファイルは管理者のワークステーションから WCS 自体の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の動作のため、ファイルはすでに WCS サーバの TFTP ディレクトリに配置され、ここでダウンロード Web ページが自動的にファイル名を読み込みます。

ステップ 9　**OK** をクリックします。

何らかの理由で転送がタイムアウトした場合には、File Is Located On パラメータの TFTP サーバ オプションを選択すると、Server File Name が読み込まれ、再試行されます。

ステップ 10　ダウンロードが完了すると、新しいページに接続され、認証できます。

ゲスト WLAN への接続

ゲスト中央 WLAN に接続して Web 認証プロセスを実行する手順は、次のとおりです。ゲスト ユーザ アカウントの詳細については、「ゲスト ユーザ アカウントの作成」の項（P. 7-11）を参照してください。

ステップ 1　オープン認証の設定で接続されている場合は、仮想インターフェイスの IP アドレスを参照します（/1.1.1.1/login.html など）。

ステップ 2　WCS ユーザ インターフェイスに Login ウィンドウが表示されたら、ユーザ名とパスワードを入力します。

（注）　入力する文字はすべて、大文字と小文字が区別されます。

Lobby Ambassador は、ゲスト ユーザを追加する場合以外は、テンプレートにアクセスできません。

ステップ 3　**Submit** をクリックして、WCS にログインします。WCS ユーザ インターフェイスは、これでアクティブになり、使用可能になります。Guest Users Templates ページが表示されます。このページには作成したすべてのゲスト ユーザ テンプレートの概要が示されます。

（注）　WCS ユーザ インターフェイスを終了するには、ブラウザ ウィンドウを閉じるか、ページの右上の **Logout** をクリックします。WCS ユーザ インターフェイス セッションを終了しても、サーバ上では WCS は終了しません。

（注）　WCS セッション中にシステム管理者が WCS を停止すると、セッションが終了し、Web ブラウザに次のメッセージが表示されます。「The page cannot be displayed.」。サーバが再起動される際に、セッションは WCS に再アソシエートされません。WCS セッションを再開する必要があります。

ゲスト ユーザの削除

ゲスト WLAN とそのアカウントのユーザ名を使用してログインされるクライアント ステーションをすべて削除する手順は、次のとおりです。

ステップ 1　**Configure > Controller Templates** の順に選択します。

ステップ 2　Template Name 列からテンプレートを選択します。

ステップ 3　左側のサイドバーのメニューから **Security > Guest Users** の順に選択します。

ステップ 4　削除するユーザ名の前のチェックボックスをクリックします。WCS によって削除前に警告メッセージが表示されます。

ステップ 5　Select a command ドロップダウン メニューから、**Delete Templates** を選択します。削除が完了すると、ウィンドウに削除結果が表示されます。

（注）　トラップを呼び出して、ゲスト アカウントの有効期限が切れた場合にコントローラによって通知を送信することもできます。WCS はこのトラップを処理し、コントローラの設定からそのゲスト ユーザ アカウントを削除します。