FlexConnect の設定

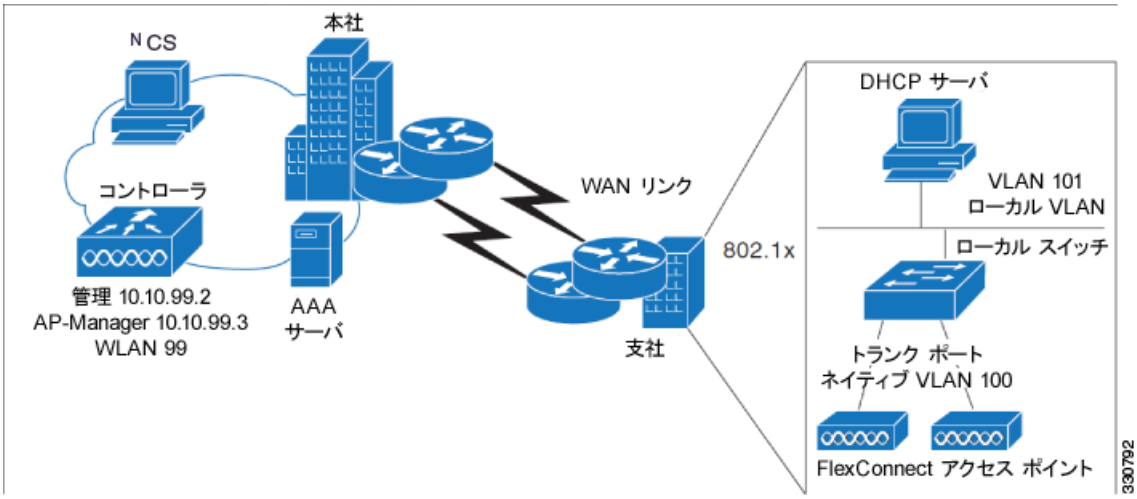
この章では、FlexConnect、およびこの機能をコントローラとアクセス ポイント上で設定する方法について説明します。ここで説明する内容は、次のとおりです。

FlexConnect について

FlexConnect は、ブランチ オフィスおよびリモート オフィスに導入されるソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリア ネットワーク）経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。ロケーションごとに導入できる FlexConnect のアクセス ポイント数は無制限です。FlexConnect アクセス ポイントは、クライアント データ トラフィックをローカルで切り替えて、コントローラへの接続が失われるとクライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

FlexConnect がサポートされているのは、1130AG、1240AG、1142 および 1252 アクセス ポイント、2000 および 4400 シリーズ コントローラ、Catalyst 3750G Integrated Wireless LAN Controller Switch、Cisco WiSM、Integrated Services Routers 用コントローラ ネットワーク モジュール、および Catalyst 3750G Integrated Wireless LAN Controller Switch 内のコントローラだけです。図 12-1 に一般的な FlexConnect の導入方法を示します。

図 12-1　FlexConnect の導入



ここでは、次の内容について説明します。

- 「FlexConnect 認証プロセス」（P.12-758）
- 「FlexConnect ガイドライン」（P.12-760）

FlexConnect 認証プロセス

FlexConnect アクセス ポイントは、ブート時にコントローラを検索します。コントローラが見つかると、そのコントローラに接続し、コントローラから最新のソフトウェアのイメージと設定情報をダウンロードし、無線を初期化します。スタンドアロン モードで使用するために、ダウンロードした設定を不揮発性メモリに保存します。

FlexConnect アクセス ポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセス ポイントが IP アドレスを DHCP サーバから割り当てられている場合、通常の CAPWAP 検出プロセス（レイヤ 3 ブロードキャスト、無線プロビジョニング（OTAP）、DNS、または DHCP オプション 43）によりコントローラを検出します。

（注）　OTAP は、購入後初のブート時には動作しません。

- アクセス ポイントが静的 IP アドレスを割り当てられている場合、DHCP オプション 43 を除く CAPWAP 検出プロセスのメソッドのいずれかを使用してコントローラを検出できます。アクセス ポイントがレイヤ 3 ブロードキャストでも OTAP でもコントローラを検出できない場合は、DNS 解決を使用することを推奨します。DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセス ポイントは、最低 1 つのコントローラを見つけることができます。
- アクセス ポイントで CAPWAP 検出メカニズムを使用できないリモート ネットワークからコントローラを検出させる場合には、プライミングを使用できます。この方法を使用すると、アクセス ポイントの接続先のコントローラを（アクセス ポイントのコマンドライン インターフェイスにより）指定できます。

FlexConnect アクセス ポイントがコントローラに到達できるとき（*接続済みモード*と呼ばれます）、コントローラはクライアント認証を支援します。FlexConnect アクセス ポイントがコントローラにアクセスできないとき、アクセス ポイントはスタンドアロン モードに入り、独自にクライアントを認証します。

（注）　アクセス ポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。LED パターンの情報については、アクセス ポイントのハードウェア インストール ガイドを参照してください。

クライアントが FlexConnect アクセス ポイントにアソシエートするとき、アクセス ポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアント データ パケットをローカルにスイッチする（ローカル スイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータ パケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：この状態では、コントローラがクライアント認証を処理し、すべてのクライアント データがコントローラにトンネル バックします。この状態は、接続済みモードの場合にだけ有効です。
- **中央認証、ローカル スイッチング**：この状態では、コントローラがクライアント認証を処理し、FlexConnect アクセス ポイントがデータ パケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードとともにコンフィギュレーション コマンドを送信し、FlexConnect アクセス ポイントに対して、ローカルにデータ パケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。
- **ローカル認証、ローカル スイッチング**：この状態では、FlexConnect アクセス ポイントがクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。この状態はスタンドアロン モードおよび接続済みモードの場合に有効です。

  ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定の基準を維持できない場合に役立ちます。ローカル スイッチングでは、認証機能はアクセス ポイント自体に存在します。そのため、ローカル認証によって、ブランチ オフィスの遅延要件が軽減されます。

（注）　ローカル認証は、ローカル スイッチング モードの FlexConnect アクセス ポイントの WLAN 上のみで有効にできます。

  ローカル認証は、次のシナリオではサポートされません。

  - FlexConnect ローカル認証を有効にした WLAN では、ゲスト認証は実行できません。
  - RRM 情報は、FlexConnect ローカル認証を有効にした WLAN のコントローラでは使用不可です。
  - ローカル RADIUS はサポートされません。
  - クライアントがいったん認証されると、ローミングは WLC の後でのみサポートされ、グループ内の他の FlexConnect は、クライアント情報で更新されます。
- **認証ダウン、スイッチング ダウン**：この状態になると、WLAN は既存クライアントのアソシエートを解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロン モードでのみ有効です。

FlexConnect アクセス ポイントがスタンドアロン モードに入ったときに、WLAN がオープン、共有、WPA-PSK、または WPA2-PSK 認証を行うように設定されている場合は、WLAN は「ローカル認証、ローカル スイッチング」状態に入り、引き続き新しいクライアントの認証を行います。その他の WLAN は、「認証ダウン、スイッチング ダウン」状態（WLAN が中央スイッチングに設定されている場合）または「認証ダウン、ローカル スイッチング」状態（WLAN がローカル スイッチングに設定されている場合）に入ります。

FlexConnect アクセス ポイントがスタンドアロン モードに入ると、中央スイッチング WLAN 上にあるすべてのクライアントのアソシエートが解除されます。802.1X または Web 認証 WLAN の場合、既存クライアントはアソシエートを解除されませんが、FlexConnect アクセス ポイントはアソシエートされたクライアントの数がゼロ（0）になると、ビーコンの送信を停止します。また、802.1X または Web 認証 WLAN にアソシエートしている新規クライアントへアソシエート解除のメッセージを送信します。802.1X 認証、NAC、および Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティは無効になり、アクセス ポイントはコントローラに侵入検知システム（IDS）レポートを送信しません。さらに、ほとんどの無線リソース管理（RRM）機能（ネイバー探索、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバー リストの使用、不正の封じ込めおよび検出）は無効化されます。ただし、FlexConnect アクセス ポイントではスタンドアロン モードで動的周波数選択がサポートされています。

（注）　コントローラに Network Access Control（NAC）が設定されている場合、クライアントはアクセス ポイントが接続済みモードのときだけアソシエートできます。NAC が有効化されているときは、正常に動作しない VLAN（または隔離 VLAN）を作成してください。この VLAN に割り当てられたクライアントのデータ トラフィックがコントローラを経由するようにするためです。これは、WLAN がローカル スイッチングを行うように設定されている場合でも必要です。クライアントが隔離 VLAN に割り当てられると、そのクライアントのデータ パケットはすべて中央でスイッチングされます。

FlexConnect アクセス ポイントは、スタンドアロン モードに入った後も、クライアントの接続を維持します。ただし、アクセス ポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect ガイドライン

FlexConnect を使用する際は、次のガイドラインを考慮します。

- FlexConnect アクセス ポイントを導入するときは、固定 IP アドレスと DHCP アドレスのいずれも使用できます。DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセス ポイントの IP アドレスを提供できる必要があります。
- FlexConnect は、最小 500 バイトの最大伝送単位（MTU）の WAN リンクをサポートします。
- アクセス ポイントとコントローラの間のラウンドトリップ遅延が 300 ミリ秒（ms）を超えてはなりません。また、CAPWAP コントロール パケットは他のすべてのトラフィックよりも優先される必要があります。これを実現できない場合は、アクセス ポイントを設定してローカル認証を実行できます。ローカル認証およびローカル スイッチングを使用する FlexConnect ローカル認証の詳細については、「FlexConnect 認証プロセス」（P.12-758）を参照してください。
- コントローラはユニキャスト パケットまたはマルチキャスト パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。FlexConnect モードでは、アクセス ポイントはマルチキャスト パケットをユニキャスト形式以外では受信しません。
- FlexConnect は CCKM 完全認証をサポートしますが、CCKM 高速ローミングをサポートしません。

- FlexConnect は 1 対 1 のネットワーク アドレス変換（NAT）設定をサポートします。また、真のマルチキャストを除くすべての機能に対してポート アドレス変換（PAT）もサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャスト オプションを使用して設定されている場合）。
- VPN、IPsec、L2TP、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプがアクセス ポイントにおいてローカルでアクセスできれば、ローカル スイッチングのトラフィックに対してサポートされます。

FlexConnect の設定

FlexConnect を設定するには、この項の手順を記載順に実行します。ここでは、次の内容について説明します。

- 「リモート サイトでのスイッチの設定」（P.12-761）
- 「FlexConnect に対するコントローラの設定」（P.12-762）
- 「FlexConnect のアクセス ポイントの設定」（P.12-764）
- 「クライアント デバイスの WLAN への接続」（P.12-765）

リモート サイトでのスイッチの設定

リモート サイトでスイッチを準備するには、次の手順を実行します。

ステップ 1　FlexConnect が有効になっているアクセス ポイントを、スイッチ上のトランクまたはアクセス ポートに接続します。

（注）　次に示す設定例では、FlexConnect アクセス ポイントはスイッチ上のトランク ポートに接続されます。

ステップ 2　次の設定例に従って、FlexConnect アクセス ポイントをサポートするようにスイッチを設定します。

この設定例では、FlexConnect アクセス ポイントは、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。このアクセス ポイントは、このネイティブ VLAN 上での IP 接続を必要とします。リモート サイトのローカル サーバとリソースは、VLAN 101 上にあります。DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。最初の DHCP プール（ネイティブ）は FlexConnect アクセス ポイントにより使用され、2 つ目の DHCP プール（ローカル スイッチング）は、クライアントがローカルでスイッチされる WLAN にアソシエートする場合、クライアントにより使用されます。設定例の太字のテキストは、これらの設定を示します。

（注）　この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに適合している必要があります。

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
```

```
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

FlexConnect に対するコントローラの設定

この項では、FlexConnect に対するコントローラの設定手順について説明します。FlexConnect のコントローラの設定には、中央スイッチング VLAN とローカル スイッチング VLAN を作成する操作が含まれます。この手順では、次の 3 つの WLAN を例として使用します。

WLAN	セキュリティ	スイッチング	インターフェイス マッピング（VLAN）
employee	WPA1+WPA2	中央	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2（PSK）	ローカル	101（ローカル スイッチング VLAN）
guest-central	Web 認証	中央	management（中央でスイッチされる VLAN）

中央スイッチングの WLAN を作成するには、次の手順を実行します。例では、これは最初の WLAN（employee）です。

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

ステップ 2　[IP Address] 列から目的のコントローラをクリックします。

ステップ 3　[WLANs] > [WLAN Configuration] を選択し、[WLAN Configuration] ページにアクセスします。

ステップ 4　[Select a command] ドロップダウン リストから [Add a WLAN] を選択し、[Go] をクリックします。

（注）　Cisco アクセス ポイントは、コントローラごとに最大 16 の WLAN をサポートします。ただし Cisco アクセス ポイントの中には、8 より大きい WLAN ID を持つ WLAN をサポートしないものがあります。この場合、WLAN を作成しようとすると、「Not all types of AP support WLAN ID greater than 8, do you wish to continue?」というメッセージが表示されます。[OK] をクリックすると、次に使用可能な WLAN ID を持つ WLAN が作成されます。ただし、8 より小さい WLAN ID を持つ WLAN を削除すると、削除した WLAN の WLAN ID が、次に作成される WLAN に適用されます。

ステップ 5　このコントローラにテンプレートを適用する場合には、ドロップダウン リストからテンプレート名を選択します。テンプレートの設定方法に応じて、フィールドが読み込まれます。新しい WLAN テンプレートを作成するには、[click here] リンク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します（「WLAN テンプレートの設定」（P.11-620）を参照）。

ステップ 6　この WLAN の設定パラメータを変更します。この employee WLAN の例では、[Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択する必要があります。

ステップ 7　[General Policies] の下にある [Status] チェックボックスをオンにして、この WLAN を必ず有効にします。

（注）　NAC が有効で、これで使用するために隔離 VLAN が作成されている場合には、[General Policies] の下にある [Interface] ドロップダウン リストから必ずこれを選択します。また、[Allow AAA Override] チェックボックスをオンにして、コントローラが確実に隔離 VLAN 割り当てを検証するようにします。

ステップ 8　[Save] をクリックして変更をコミットします。

ステップ 9　ローカルにスイッチされる WLAN を作成する手順は次のとおりです。例では、これは 2 番めの WLAN（employee-local）です。

a. ステップ のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「employee-local」です。

b. 元の [WLAN] ページで [WLAN ID] をクリックして、[WLANs edit] ページへ移動します。この WLAN の設定パラメータを変更します。この employee WLAN の例では、[Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択する必要があります。必ず [PSK authentication key management] を選択して、事前共有キーを入力します。

（注）　[Admin Status] チェックボックスをオンにして、この WLAN を必ず有効にします。また、[FlexConnect Local Switching] チェックボックスをオンにして、ローカル スイッチングを必ず有効にします。ローカル スイッチングを有効にすると、この WLAN をアドバタイズする FlexConnect アクセス ポイントはデータ パケットをローカルでスイッチできます（データ パケットをコントローラにトンネルしない）。

（注）　FlexConnect アクセス ポイントの場合、FlexConnect ローカル スイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。これは SSID ごと、FlexConnect アクセス ポイントごとに簡単に変更できます。FlexConnect 以外のアクセス ポイントでは、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは WLAN の各インターフェイス マッピングによって決定されます。

c. [Save] をクリックして変更をコミットします。

ステップ 10　ゲスト アクセスに使用される中央スイッチングの WLAN も作成する場合は、次の手順に従ってください。例では、これは 3 番めの WLAN（guest-central）です。中央サイトからの保護されていないゲスト トラフィックに対する企業データ ポリシーを施行できるように、ゲスト トラフィックをコントローラにトンネリングする必要のある場合があります。

a. ステップ のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「guest-central」です。

b. [WLANs Edit] ページで、この WLAN の設定パラメータを変更します。employee WLAN の例では、[Security] タブの [Layer 2 Security] および [Layer 3 Security] ドロップダウン リストから [None] を選択し、[Web Policy] チェックボックスをオンにして、[Authentication] が選択されていることを確認します。

（注）　外部 Web サーバを使用する場合、事前認証アクセス コントロール リスト（ACL）をサーバの WLAN 上に設定してから、この ACL を WLAN の事前認証 ACL として選択する必要があります。

c. [Status] チェックボックスをオンにして、これを必ず有効にします。

d. [Save] をクリックして変更をコミットします。

e. ゲスト ユーザがこれにアクセスしたとき最初に表示されるログイン ページのコンテンツと外観をカスタマイズする場合は、「Web 認証テンプレートの設定」（P.11-667）の手順に従ってください。

f. この WLAN にローカル ユーザを追加するには、[Configure] > [Controller Template Launch Pad] を選択します。

g. 左側のサイドバーのメニューから、[Security] > [Local Net Users] を選択します。

h. [Local Net Users] ページが表示されたら、[Select a command] ドロップダウン リストから [Add Template] を選択して、[Go] をクリックします。

i. [Import from File] チェックボックスをオフにします。

j. ローカル ユーザのユーザ名とパスワードを入力します。

k. [Profile] ドロップダウン リストから、適切な SSID を選択します。

l. ゲスト ユーザ アカウントの説明を入力します。

m. [Save] をクリックします。

ステップ 11　FlexConnect に対して 2 つまたは 3 つのアクセス ポイントを設定する場合には、「FlexConnect のアクセス ポイントの設定」（P.12-764）を参照してください。

FlexConnect のアクセス ポイントの設定

この項では、FlexConnect のアクセス ポイントを設定する方法を説明します。

FlexConnect のアクセス ポイントを設定するには、次の手順を実行します。

ステップ 1　アクセス ポイントが物理的にネットワークに追加されていることを確認します。

ステップ 2　[Configure] > [Access Points] の順に選択します。

ステップ 3　[AP Name] リストでアクセス ポイントをクリックして、FlexConnect を設定するアクセス ポイントを選択します。[Access Point Detail] ページが表示されます。

[Inventory Information] グループ ボックスに表示される最後のフィールドは、このアクセス ポイントが FlexConnect に対して設定可能かどうかを示します。FlexConnect をサポートしているのは、1130AG および 1240AG アクセス ポイントだけです。

ステップ 4　[AP Mode] フィールドに *FlexConnect* が表示されることを確認します。そのように表示されない場合、ステップ 5 に進みます。FlexConnect がサポートされていると表示されている場合には、ステップ 9 に進みます。

ステップ 5　[Configure] > [AP Configuration Templates] > [Lightweight AP] または [Autonomous AP] を選択します。

ステップ 6　[AP Name] リストでアクセス ポイントをクリックして、FlexConnect を設定するアクセス ポイントを選択します。[Lightweight AP Template Detail] ページが表示されます。

ステップ 7　[FlexConnect Mode supported] チェックボックスをオンにします。この設定を有効にすると、すべてのプロファイル マッピングが表示できます。

（注）　モードを FlexConnect に変更するときに、アクセス ポイントがまだ FlexConnect モードでない場合、他のすべての FlexConnect パラメータはそのアクセス ポイントに適用されません。

ステップ 8　[VLAN Support] チェックボックスをオンにし、[Native VLAN ID] テキスト ボックスにリモート ネットワーク上のネイティブ VLAN の番号（100 など）を入力します。

（注）　デフォルトで、VLAN は FlexConnect アクセス ポイント上では有効化されていません。FlexConnect を有効にすると、アクセス ポイントは WLAN にアソシエートされた VLAN ID を継承します。この設定はアクセス ポイントで保存され、join response が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの FlexConnect アクセス ポイントごとに、ネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。クライアントが RADIUS サーバから VLAN を割り当てられている場合、その VLAN はローカル スイッチングの WLAN にアソシエートされます。

ステップ 9　[Apply/Schedule] タブをクリックして変更を保存します。

ステップ 10　[Locally Switched VLANs] セクションに、ローカル スイッチングの WLAN およびその VLAN ID が表示されます。[Edit] リンクをクリックして、クライアント IP アドレスを取得する VLAN の番号を変更できます。それによって、VLAN ID の変更を保存できるページにリダイレクトされます。

ステップ 11　[Save] をクリックして変更を保存します。

ステップ 12　リモート サイトで、FlexConnect に対して設定が必要なその他すべてのアクセス ポイントについて、この手順を繰り返します。

クライアント デバイスの WLAN への接続

「FlexConnect に対するコントローラの設定」（P.12-762）で作成した WLAN に接続するプロファイルをクライアント デバイスに作成する手順は次のとおりです。

例では、クライアント上で 3 つのプロファイルを作成します。

1. 「employee」WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN から IP アドレスが取得されます。

2. 「employee-local」WLAN に接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、ローカル スイッチの VLAN 101 から IP アドレスが取得されます。
3. 「guest-central」WLAN に接続するには、オープン認証を使用するプロファイルを作成します。クライアントが認証されると、アクセス ポイントへのネットワーク ローカル上の VLAN 101 から IP アドレスが取得されます。クライアントが接続されると、ローカル ユーザは任意の HTTP アドレスを Web ブラウザに入力します。Web 認証プロセスを完了するため、コントローラに自動的に誘導されます。Web ログイン ページが表示されたら、ユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカル スイッチングか中央スイッチングかを確認するには、[Monitor] > [Devices] > [Clients] の順に選択します。

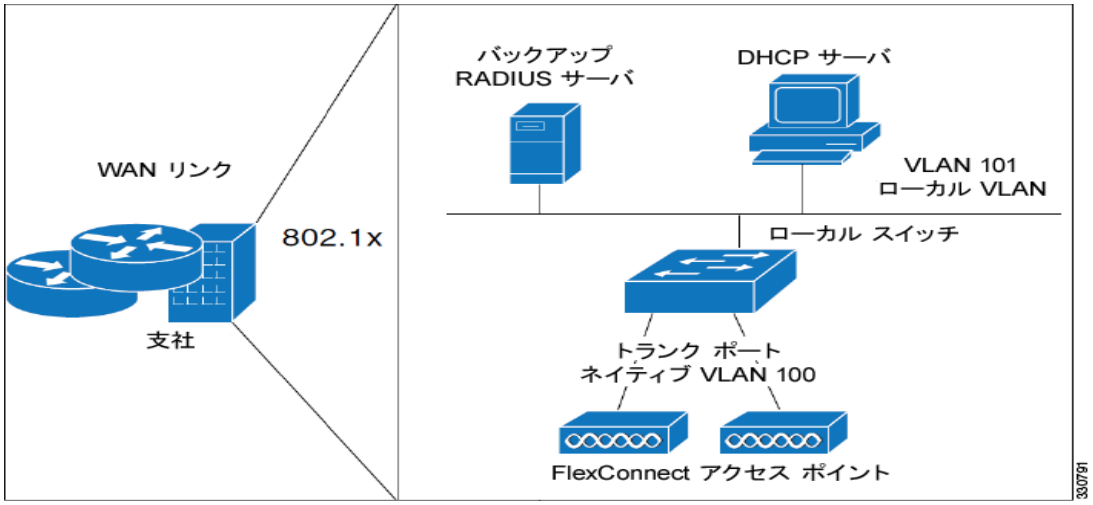
FlexConnect のアクセス ポイント グループ

FlexConnect を使用すると、ブランチ オフィスまたはリモート オフィスにあるアクセス ポイントを本社のオフィスからワイドエリア ネットワーク（WAN）リンクを使用して、各オフィスでコントローラを導入せずに、設定および制御できます。ロケーションごとに展開できる FlexConnect のアクセス ポイント数は無制限ですが、ブランチ オフィスは同じ設定を共有していることが多いため、フロアごとにアクセス ポイントを組織化してグループ化し、ビルディングごとに制限できます。

同じ設定でアクセス ポイント グループを作成することによって、個別にコントローラにアクセスするよりも CCKM 高速ローミングのような手順をより速く処理できます。たとえば、CCKM 高速ローミングを起動するには、FlexConnect アクセス ポイントがアソシエートできるすべてのクライアントの CCKM キャッシュを認識している必要があります。300 のアクセス ポイントと 1000 のクライアントに接続できるコントローラがある場合、1000 のクライアントすべてではなく FlexConnect グループの CCKM キャッシュを処理して送信する方が迅速で実用的です。特定の 1 つの FlexConnect グループでアクセス ポイントの少ないブランチ オフィスに焦点を絞ることができます。こうすることで、ブランチ オフィスのクライアントはこれらのいくつかのアクセス ポイント間にだけ接続し、ローミングできるようになります。確立されたグループがある場合、CCKM キャッシュやバックアップ RADIUS などの機能は、各アクセス ポイントで設定されるのではなく、FlexConnect グループ全体に対して設定されます。

グループ内のすべての FlexConnect アクセス ポイントは、同じ WLAN、バックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。この機能は、リモート オフィス内や建物のフロア上に複数の FlexConnect アクセス ポイントがあり、すべてを一度に設定する場合に役立ちます。たとえば、FlexConnect グループに対してバックアップ RADIUS サーバを 1 つ設定しておけば、個々のアクセス ポイント上で同じサーバを設定する必要はありません。図 12-2 は、ブランチ オフィスにバックアップ RADIUS サーバを持つ、一般的な FlexConnect グループの導入を示しています。

図 12-2　FlexConnect グループの導入



ここでは、次の内容について説明します。

- 「FlexConnect グループおよびバックアップ RADIUS サーバ」（P.12-767）
- 「FlexConnect グループおよび CCKM」（P.12-767）
- 「FlexConnect グループおよびローカル認証」（P.12-768）
- 「FlexConnect グループの設定」（P.12-768）
- 「FlexConnect グループの監査」（P.12-770）

FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect アクセス ポイントが完全な 802.1X 認証を実行して RADIUS サーバをバックアップできるようにコントローラを設定できます。プライマリ RADIUS サーバを設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。

FlexConnect グループおよび CCKM

CCKM 高速ローミングが FlexConnect アクセス ポイントで動作するためには、FlexConnect グループが必要です。CCKM 高速ローミングは、ワイヤレス クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスター キーの派生キーをキャッシュすることにより実現します。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。たとえば、300 台のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。少数のアクセス ポイントからなる FlexConnect グループを作成すれば（たとえば、同じリモート オフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがそれらのアクセス ポイントの 1 つにアソシエートするときだけとなります。

（注）　FlexConnect アクセス ポイントと FlexConnect 以外のアクセス ポイント間の CCKM 高速ローミングはサポートされていません。

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect アクセス ポイントが最大 20 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるようにコントローラを設定できます。コントローラは、各 FlexConnect アクセス ポイントがコントローラに接続したときに、ユーザ名とパスワードの静的リストをそのアクセス ポイントに送信します。グループ内の各アクセス ポイントは、そのアクセス ポイントにアソシエートされたクライアントのみを認証します。

この機能は、Autonomous アクセス ポイント ネットワークから Lightweight FlexConnect アクセス ポイント ネットワークに移行する顧客で、かつ、より大きなユーザ データベースを保持する必要もなく、Autonomous アクセス ポイントで使用できる RADIUS サーバの機能と置き換える別のハードウェア デバイスを追加することもない顧客に最適です。

（注）　この機能は、FlexConnect バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect アクセス ポイントは常に、まずプライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバで試行し（プライマリに到達できない場合）、最後に FlexConnect アクセス ポイント自身で試行します（プライマリとセカンダリの両方に到達できない場合）。

FlexConnect グループの設定

FlexConnect グループを設定するには、次の手順を実行します。に従ってください。複数のコントローラに FlexConnect テンプレートを適用するには、「FlexConnect AP グループ テンプレートの設定」（P.11-645）のテンプレートの手順を参照してください。

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

ステップ 2　目的の IP アドレスをクリックして特定の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、[FlexConnect] > [FlexConnect AP Groups] の順に選択します。確立された FlexConnect AP グループが表示されます。

ステップ 4　[Group Name] 列に FlexConnect アクセス ポイント グループに割り当てられたグループ名が表示されます。別のグループを追加する場合は、[Select a command] ドロップダウン リストから [Add FlexConnect AP Group] を選択します。

または

既存のテンプレートを変更するには、[Template Name] 列のテンプレートをクリックします。[FlexConnect AP Groups Template] ページの [General] タブが表示されます。

（注）　グループ名を削除するには、削除するグループ名をクリックして、[Select a command] ドロップダウン リストから [Delete FlexConnect AP Group] を選択します。

[Template Name] フィールドに FlexConnect アクセス ポイント グループに割り当てられたグループ名が表示されます。

ステップ 5　各グループのプライマリ RADIUS 認証サーバを選択します。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。

（注）　Prime Infrastructure の FlexConnect RADIUS サーバ設定を適用する前に、コントローラ上で RADIUS サーバ設定を設定する必要があります。

ステップ 6　各グループのセカンダリ RADIUS 認証サーバを選択します。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。

ステップ 7　グループにアクセス ポイントを追加するには、[FlexConnect AP] タブをクリックします。

ステップ 8　アクセス ポイントのイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループに存在できません。複数のグループが同じコントローラに適用されている場合は、[Ethernet MAC] チェックボックスをオンにして、グループの 1 つのアクセス ポイントの選択を解除します。この変更を保存するか、コントローラに適用する必要があります。

ステップ 9　FlexConnect グループのローカル認証を有効にするには、[FlexConnect Configuration] タブをクリックします。[FlexConnect Configuration] タブが表示されます。

（注）　[General] タブで、[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

ステップ 10　この FlexConnect グループのローカル認証を有効にするには、[FlexConnect Local Authentication] チェックボックスをオンにします。デフォルト値はオフです。

（注）　この機能を使用しようとすると、ライセンスの必要な機能であることを知らせる警告メッセージが表示されます。

ステップ 11　FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるようにするには、[LEAP] チェックボックスを選択します。それ以外の場合は、FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるようにするには、[EAP-FAST] チェックボックスを選択します。

ステップ 12　Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。

- 手動の PAC プロビジョニングを使用するには、[EAP-FAST Key] テキスト ボックスに、PAC の暗号化と復号化に使用するキーを入力します。キーは 32 桁の 16 進数文字である必要があります。
- PAC プロビジョニング中に PAC のないクライアントに自動的に PAC を送信できるようにするには、[Auto Key Generation] チェックボックスをオンにします。

ステップ 13　[EAP-FAST Authority ID] テキスト ボックスに EAP-FAST サーバの認証局 ID を入力します。識別子は 32 桁の 16 進数文字である必要があります。

ステップ 14　[EAP-FAST Authority Info] テキスト ボックスに EAP-FAST サーバの認証局 ID に関する情報をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。

ステップ 15　[EAP-FAST Pac Timeout] テキスト ボックスの編集ボックスに PAC が表示され続ける秒数を入力することにより、PAC タイムアウト値を指定します。有効範囲は 2 ～ 4095 秒です。

（注）　個々のアクセス ポイントが FlexConnect グループに属していることを確認するには、[Users configured in the group] リンクをクリックします。[FlexConnect AP Group] ページが開き、グループの名前と、そのグループに属しているアクセス ポイントが表示されます。

FlexConnect グループの監査

FlexConnect 設定が Prime Infrastructure またはコントローラ上で時間とともに変化した場合は、設定を監査できます。変化は、後続の画面に表示できます。Prime Infrastructure またはコントローラを更新して、設定の同期を選択できます。