802.11r BSS Fast Transition 導入ガイド

初版：2016 年 07 月 06 日

802.11r BSS Fast Transition

802.11r Fast Transition について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行（FT）と呼ばれるローミングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- Over-the-Air
- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

リリース 8.0 から、WPAv2 WLAN でもある 802.11r WLAN を作成できます。以前のリリースでは、802.11r の WLAN と通常のセキュリティ用にそれぞれ個別の WLAN を作成する必要がありました。802.11r WLAN が非 802.11r アソシエーションを受け入れることができるため、非 802.11r クライアントが 802.11r WLAN 対応 WLAN に接続できるようになりました。混合モードまたは 802.11r 接続をサポートしないクライアントは、非 802.11r WLAN に接続できます。FT PSK 以降を設定すると、PSK を混合モードで WLAN を結合できる PSK だけ結合できるクライアントを定義します。

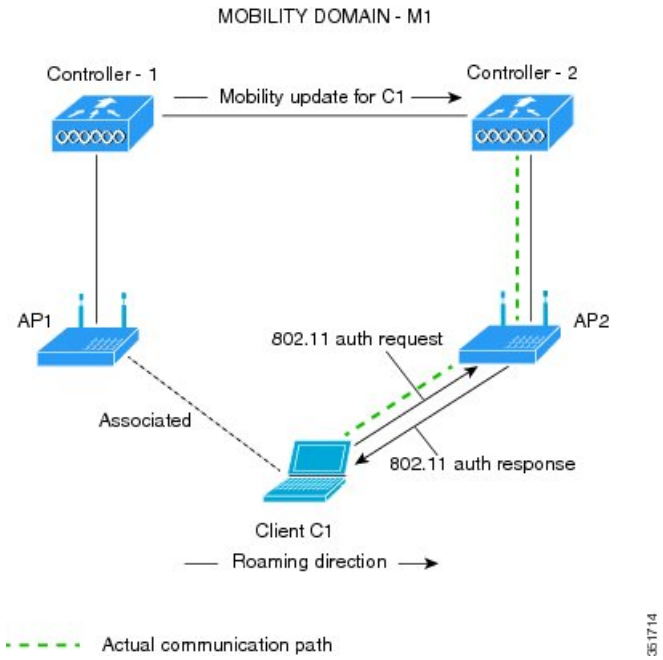
クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行されてから、コントローラによって送信されます。

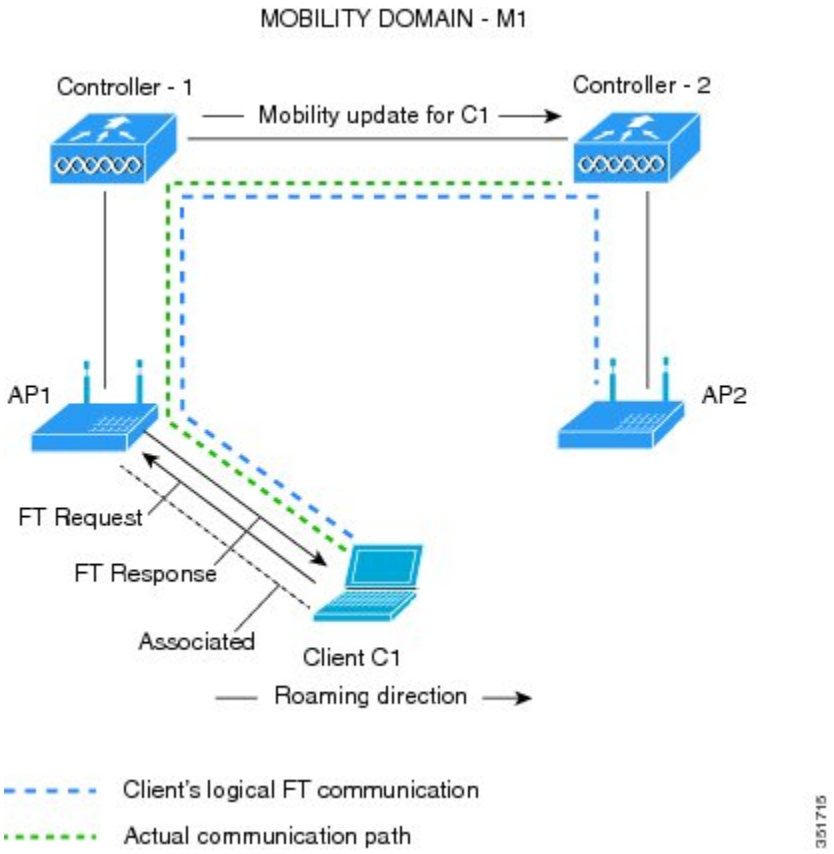
この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *1*：*Over the Air* クライアントのローミングの設定時にメッセージが交換されます



この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *2*：*Over the DS* クライアントのローミングの設定時にメッセージが交換されます



802.11r Fast Transition の制約事項

- この機能はメッシュ アクセス ポイントでサポートされません。
- 8.1 以前のリリースでは、この機能は FlexConnect モードのアクセス ポイントでサポートされていません。リリース 8.2 では、この制約がなくなります。
- FlexConnect モードのアクセス ポイントの場合：
  - 802.11r Fast Transition は、ローカルで集中的に切り替わる WLAN でサポートされています。
  - この機能は、ローカル認証が有効になっている WLAN ではサポートされません。
  - 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
  - 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。

- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。
- AP が同じ FlexConnect グループに存在する場合のみ、802.11r 高速ローミングは機能します。

- この機能は、Cisco 600 シリーズ OfficeExtend アクセス ポイントなどの Linux ベースの AP ではサポートされません。
- クライアントがスタンドアロン モードの Over-the-DS 事前認証を使用する場合、802.11r 高速ローミングはサポートされません。
- EAP LEAP 方式はサポートされません。WAN リンク遅延は、最大 2 秒間にアソシエーション時間を抑制します。
- スタンドアロン AP からクライアントへのサービスは、セッション タイマーが切れるまでサポートされます。
- TSpec は 802.11r 高速ローミングではサポートされません。したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。Cisco WLC は、Over-the-Air および Over-the-DS DS 方式の両方をローミングする間、802.11r Fast Transition の認証要求を処理します。
- この機能は、オープンな WPA2 設定の WLAN でサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシークライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、Cisco WLC では、異なる AP と最大 3 つの Fast Transition ハンドシェイクが可能です。
- 非 802.11r 対応デバイスは FT 対応 WLAN にアソシエートできなくなります。
- 802.11r FT + PMF はお勧めしません。

• 802.11r FT Over-the-Air ローミングは FlexConnect 導入にお勧めします。

802.11r の Fast Transition の設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ウィンドウを開きます。

ステップ 2 WLAN ID をクリックして、[WLANs > Edit] ウィンドウを開きます。

ステップ 3 [Security] > [Layer 2] タブを選択します。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。
Fast Transition の認証キー管理パラメータが表示されます。

ステップ 5 [Fast Transition] ドロップダウン リストから、WLAN の Fast Transition を選択します。

ステップ 6 [Over the DS] チェックボックスをオンまたはオフにして、分散システム経由の Fast Transition を有効または無効にします。
このオプションは、Fast Transition を有効にしたとき、または Fast Transition が適応型の場合のみ指定できます。

802.11r Fast Transition を使用するには、over-the-air および over-the-ds を無効にする必要があります。

ステップ 7 [Reassociation Timeout] フィールドに、AP へのクライアントの再関連付けの試行がタイムアウトになる秒数を入力します。有効範囲は 1 ～ 100 秒です。

（注） このオプションは、高速移行を有効にした場合だけ使用できます。

ステップ 8 [Authentication Key Management] で、[FT 802.1X] または [FT PSK] を選択します。キーを有効または無効にするには、対応するチェックボックスをオンまたはオフにします。[FT PSK] チェックボックスをオンにした場合は、[PSK Format] ドロップダウン リストから [ASCII] または [Hex] を選択して、キー値を入力します。

（注） Fast Transition 適応型が有効な場合、[802.1X] および [PSK AKM] のみ使用できます。

ステップ 9 [WPA gtk-randomize State] ドロップダウン リストで [Enable] または [Disable] を選択して、Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state を設定します。

ステップ 10 [Apply] をクリックして設定値を保存します。

802.11r Fast Transition の設定（CLI）

ステップ 1 802.11r Fast Transition パラメータを有効または無効にするには、config wlan security ft {adaptiveenable | disable} wlan-id コマンドを使用します。

ステップ 2 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、config wlan security ft over-the-ds {enable | disable} wlan-id コマンドを使用します。
クライアント デバイスは通常、機能が WLAN でアドバタイズされている場合 fast transition over-the-ds を優先します。クライアントに fast transition over-the-air を強制的に実行させるには、fast transition over-the-ds を無効にします。

ステップ 3 事前共有キー（PSK）を使用した Fast Transition の認証キー管理を有効または無効にするには、config wlan security wpa akm ft psk {enable | disable} wlan-id コマンドを使用します。
デフォルトで、PSK を使用した認証キー管理は無効です。

ステップ 4 PSK を使用した適応型の認証キー管理を有効または無効にするには、config wlan security wpa akm psk {enable | disable} wlan-id コマンドを使用します。

ステップ 5 802.1X を使用した Fast Transition の認証キー管理を有効または無効にするには、config wlan security wpa akm ft-802.1X {**enable** | disable} wlan-id コマンドを使用します。
デフォルトでは、802.1X を使用した認証キー管理は有効です。

ステップ 6 802.1x を使用した適応型の認証キー管理を有効または無効にするには、config wlan security wpa akm 802.1x {**enable** | **disable**} wlan-id コマンドを使用します。
（注） 適応型 Fast Transition が有効な場合、802.1X および PSK AKM のみ使用できます。

ステップ 7 802.11r Fast Transition の再アソシエーション タイムアウトを有効または無効にするには、config wlan security ft reassociation-timeout timeout-in-seconds wlan-id コマンドを使用します。
有効範囲は 1 ～ 100 秒です。再アソシエーション タイムアウトのデフォルト値は 20 秒です。

ステップ 8 WLAN の Fast Transition 設定を表示するには、show wlan wlan-id コマンドを使用します。

ステップ 9 クライアントの Fast Transition 設定を表示するには、show client detail client-mac コマンドを使用します。
（注） このコマンドは、接続済みまたは接続中のクライアント ステーション（STA）にのみ該当します。

ステップ 10 高速移行イベントのデバッグを有効または無効にするには、debug ft events {enable | disable} コマンドを使用します。

802.11r BSS Fast Transition のトラブルシューティング

症状	解決策
非 802.11r レガシー クライアントはすでに接続していません。	WLAN で FT が有効であるかどうかを確認します。その場合、非 FT WLAN が作成される必要があります。
WLAN を設定する場合、FT 設定オプションは表示されません。	WPA2 が使用されているかどうかを確認します（802.1x/PSK）。FT は WPA2 SSID およびオープン SSID だけでサポートされます。

症状	解決策
802.11r クライアントは、新しいコントローラにレイヤ 2 のローミングを実行するときに、再認証されると想定されます。	コントローラの GUI で、[WLANs] > [WLAN Name] > [Security] > [Layer 2] と移動して、再認証タイムアウトがデフォルトの 20 よりも小さくなっているかどうかを確認します。

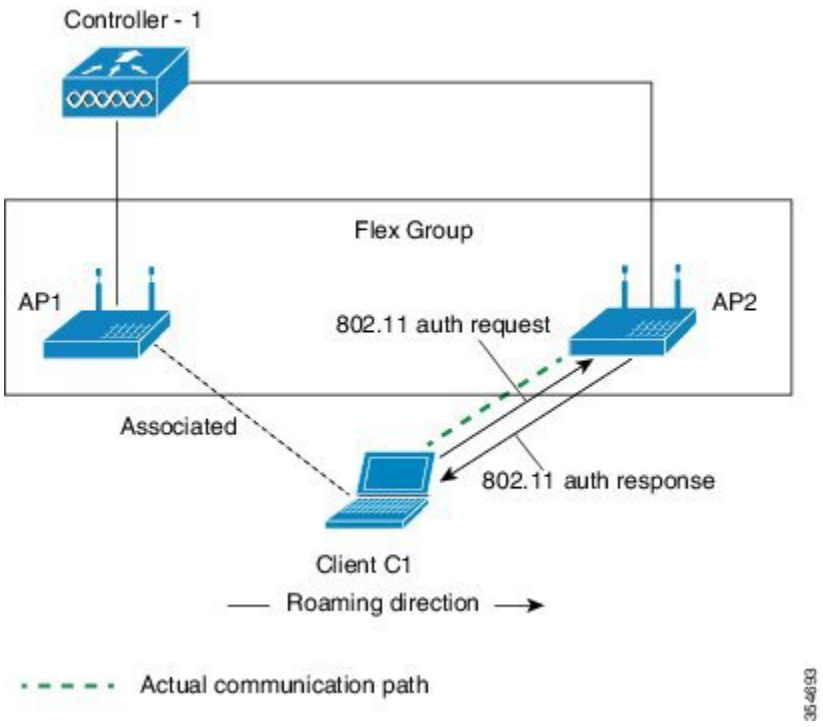
FlexConnect 導入での 802.11r BSS Fast Transition

FlexConnect の導入シナリオでは、同じ FlexConnect グループ内の AP 間で 802.11r BSS FT ローミングがサポートされます。シームレスなローミングを実現するために、802.11r キー キャッシュが同じ FlexConnect グループのすべての AP に配布されます。キー キャッシュは、クライアント デバイスが中央認証で最初の FT 関連付けを実行した後に、Cisco WLC から配布されます。

Flex 導入は、Over-the-Air ローミングと Over-the-DS ローミングの両方をサポートします。2 つのローミング シナリオは次の図に示されています。

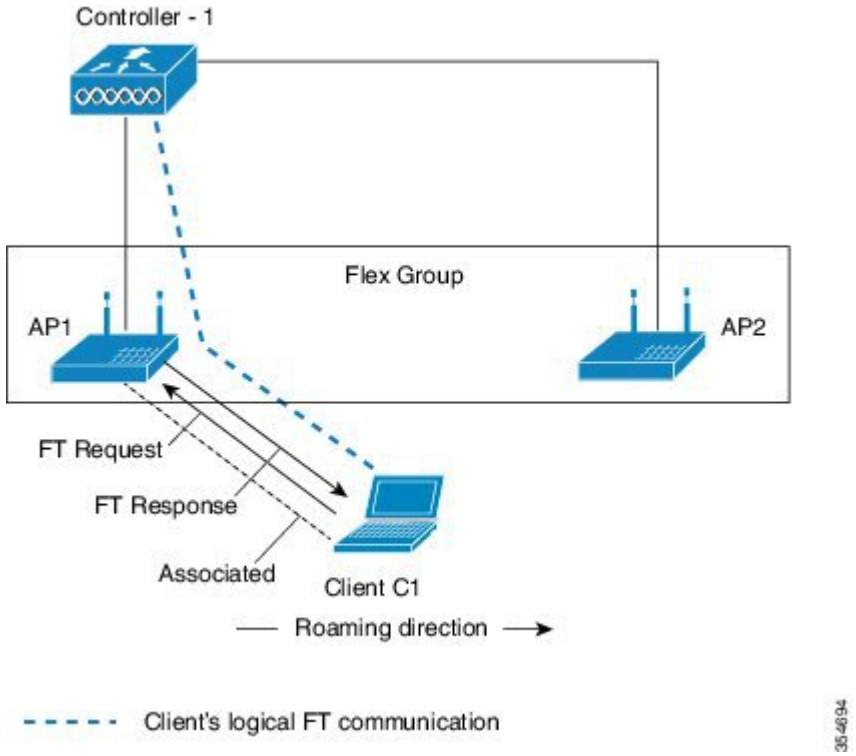
Over-the-Air ローミング

図 *3* : *Over-the-Air* ローミング シナリオ



Over-the-DS ローミング

図 *4* : ***Over-the-DS*** ローミング シナリオ



FlexConnect 導入向けの最適化

FlexConnect モード AP 用の 802.11r Fast Transition（FT）機能は、FT の認証要求プロセスと検証が Cisco AP 自体で発生し、Cisco AP 自体が FT 認証応答を送信するように最適化されています。キー生成システムに変更はありません。

（注） この新しい設計は、FlexConnect の中央認証トポロジにのみ適用されます。FlexConnect のローカル認証のシナリオでは、802.11r BSS Fast Transition はサポートされていません。

認証要求

1. Cisco AP は、FT 認証要求を Cisco WLC でも処理するために転送します。
2. Cisco WLC から FT 認証応答を受信すると、Cisco AP はそれが成功したかどうかを確認します。
   - 成功の場合、Cisco AP はパケットを消費します。
   - 失敗の場合、Cisco AP はクライアントに認証無効通知を送信します。
3. ANonce は、Cisco AP で生成され、FT 認証要求の ANonce フィールドをピギーバックして Cisco WLC に送信されます。

（注） Cisco WLC と Cisco AP でキー生成に使用する ANonce は同じものです。

認証要求と関連付け要求

1. FT 認証要求と関連付け要求は、Cisco WLC に同時に送信され、確認後、処理されます。
2. Cisco AP が、FT 認証応答と再関連付け応答を Cisco WLC から受信し、成功したかどうかを確認します。
   - 成功の場合、Cisco AP は成功応答をすでに送信しているため、成功応答を破棄します。
   - 失敗の場合、Cisco AP はクライアントに認証無効を送信します。

（注） キー生成は、Cisco AP と Cisco WLC の両方で実行されます。