



CHAPTER 8

IP 登録の終了

この章では、Cisco Mobile Wireless Home Agent が IP 登録を終了し、この機能を実行するよう Home Agent (HA) を設定する方法について説明します。

この章は、次の内容で構成されています。

- 「モバイル IPv4 登録の失効」 (P.8-1)
- 「I-bit のサポート」 (P.8-3)
- 「MIPv4 登録失効の設定」 (P.8-3)
- 「モバイル IPv4 リソース失効の制約事項」 (P.8-3)
- 「同時バインディング」 (P.8-4)
- 「Remote Authentication Dial-In User Service (RADIUS) 切断」 (P.8-4)
- 「RADIUS 切断クライアントの設定」 (P.8-4)
- 「RADIUS 切断の制約事項」 (P.8-5)
- 「バインディングの同期化および削除のサポート」 (P.8-5)
- 「Selective FA Revocation」 (P.8-7)

モバイル IPv4 登録の失効

基本的なモバイル IP リソースの失効は、モビリティ エージェント (モバイル IP サービスをモバイル ノードに提供する) が他のモビリティ エージェントに、管理上の理由または Mobile IP (MIP; モバイル IP) ハンドオフによって登録の終了を通知できる方式を定義する IS-835-C イニシアチブです。

この機能は、Cisco MobileIP Bind Update 機能と類似しています。モバイルが接続ポイント (Foreign Agent (FA; 外部エージェント)) を変更する、または管理上、セッションを終了する必要がある場合、HA は Registration Revocation メッセージを古い FA に送信します。古い FA はセッションを切断し、Registration Revocation acknowledgement (ACK) メッセージを HA に送信します。さらに、PDSN (Packet Data Serving Node) /FA が管理上、セッションを終了する必要がある場合、FA は Registration Revocation メッセージを HA に送信します。HA はモバイルのバインディングを削除し、Registration Revocation ACK を FA に送信します。

モバイル IPv4 の登録失効をサポートするよう設定された HA には、有効な登録失効拡張を含んだ PDSN から関連付けられた MIP Registration Request (RRQ; 登録要求) に対するすべての MIP RRP の失効サポート拡張が含まれます。HA が失効サポート拡張を受信し、以後の失効サポート拡張に回答した登録は、HA によって取り消し可能と見なされます。

次のコールフローでは、モバイル IP リソース失効（登録 フェーズ）を示します。

-
- ステップ 1** MS はコールを発信し、Point-to-Point Protocol (PPP; ポイントツーポイントプロトコル) セッションがアップします。
- ステップ 2** MIPv4 登録失効サポートをアドバタイズするよう PDSN/FA は設定されました。PDSN/FA は MIPv4 登録失効サポート ビット "X" セットのあるアドバタイズメントを送信します。
- ステップ 3** PDSN/FA は Mobile Node (MN; モバイル ノード) から MIP RRQ を受信します。これには、FA-Challenge Handshake Authentication Protocol (CHAP; チャレンジ ハンドシェイク 認証プロトコル) 時のアクセス要求で 2 に設定された Session Termination Capability (STC) アトリビュートが含まれます。RRQ を HA を転送すると、失効サポート拡張が Mobile-Home Authentication Extension (MHAE) の後に追加されます。失効サポート拡張の I-bit は 1 に設定され、必要な場合はいつでも MS がバインディングの失効に関する明示的な通知を受け取ったことを示します。
- ステップ 4** 失効拡張を含んだ MIP RRQ を受信すると、HA は失効サポート拡張を含み、I-bit を MIP RRQ で受信した値に設定する MIP RRP を戻します。HA-CHAP (MN-Authentication, Authorization and Accounting (AAA; 認証、許可、アカウントイング) 認証) の場合、STC アトリビュート (値 2) は、AAA に送信されたアクセス要求に含まれます。
- ステップ 5** PDSN は失効サポート拡張を含んだ MIP RRP を受信します。データ フローは取り消し可能と見なされます。
-

次のコールフローでは、モバイル IP リソース失効（HA が開始）を示します。

-
- ステップ 1** モバイルは、PDSN/FA (1) のあるモバイル IP データセッションを開始します。
- ステップ 2** PDSN/FA (1) は、登録失効サポート拡張をモバイル登録要求に追加し、これを HA に転送します。
- ステップ 3** 応答として、HA は登録失効サポート拡張を登録応答に追加し、これを PDSN/FA (1) に送信します。
- ステップ 4** PDSN/PDSN ハンドオフが発生し、モバイルは PDSN/FA (2) のあるモバイル IP データセッションを再開します。
- ステップ 5** PDSN/FA (2) は登録要求を HA に送信します。
- ステップ 6** HA は登録応答を PDSN/FA (2) に送信します。
- ステップ 7** HA はモバイル IP Resource Revocation メッセージを PDSN/FA (1) に送信します。
- ステップ 8** PDSN/FA (1) はモバイル IP リソース失効 ACK を HA に送信し、モバイルのモバイル IP データセッションを終了します。
-

次のコールフローでは、モバイル IP リソース失効（FA が失効を開始）を示します。

-
- ステップ 1** モバイルは、PDSN/FA のあるモバイル IP データセッションを開始します。
- ステップ 2** PDSN/FA は、登録失効サポート拡張をモバイル登録要求に追加し、これを HA に転送します。
- ステップ 3** 応答として、HA は登録失効サポート拡張を登録応答に追加し、これを PDSN/FA に送信します。
- ステップ 4** PDSN/FA では一部のイベントが発生し、PDSN/FA はセッションを終了するよう決定します。
-

- ステップ 5** PDSN/FA はモバイル IP Resource Revocation メッセージを HA に送信します。
- ステップ 6** HA はモバイル IP リソース失効 ACK を PDSN/FA に送信します。HA はバインディングをクリアし、PDSN/FA はセッションをクリアします。

I-bit のサポート

登録失効フェーズ中、Mobile Node (MN; モバイル ノード) に複数のモバイル IP フローがある場合に、I (Inform) ビットは、MN に対して失効したデータ サービスを通知します。登録フェーズ中、RRQ/RRP の失効サポート拡張のモビリティ エージェントによってこのビットが **1** に設定されている場合、エージェントが Revocation メッセージの "I" ビットの使用をサポートすることを示します。

現在の実装では、MobileIP RRQ が失効サポート拡張に設定された I ビットで受信された場合、HA も I-bit を **1** に設定します。I-bit は失効フェーズ中も使用できます。HA が失効を開始した (I ビットはネゴシエートされた) ときに、バインディングが管理上、解除された場合、HA は I ビットを Revocation メッセージで **1** に設定します。PDSN 間ハンドオフが HA によって検出された場合、I ビットを **0** に設定します。失効が PDSN によって開始され、Revocation メッセージで I-bit が **1** に設定されている場合、HA も Revocation ACK メッセージで I-bit を **1** に設定します。

MIPv4 登録失効の設定

HA で MIPv4 登録失効機能をイネーブルにするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	Router(config)# ip mobile home-agent revocation	HA で MIPv4 登録失効のサポートをイネーブルにします。
ステップ 2	Router(config)# ip mobile home-agent revocation timeout 5 retransmit 6	(任意) Revocation メッセージの再送信カウントおよびタイムアウト値を設定します。

次に、**ip mobile home-agent revocation** コマンドの例を示します。

```
Router(config)# ip mobile home-agent revoc timeout ?
<1-100> Wait time (default 3 secs)
Router(config)# ip mobile home-agent revoc retransmit ?
<0-100> Number of retries for a transaction (default 3)
```

モバイル IPv4 リソース失効の制約事項

次のリストでは、現在のリリースのモバイル IPv4 リソース失効機能の制約事項を特定します。

- HA-CHAP (MN-AAA 認証) 時に access-accept で受信した STC アトリビュートは無視され、HA の機能設定が優先されます。
- Revocation メッセージ、Revocation ACK メッセージ、失効サポート拡張 (Foreign-Home Authentication Extension (FHAE) または IPSec によって保護されない) は廃棄されませんが、処理されます。HA に FA-HA セキュリティ アソシエーションを設定する、または FA と HA の間に IPSec トンネルが存在することを推奨します。

- リリース失効とバインドアップデートを同時にイネーブルにはできません。いずれか 1 つを選択する必要があります。
- HA management information base (MIB; 管理情報ベース) は登録失効情報でアップデートされません。

同時バインディング

HA は次の理由で同時バインディングをサポートしません。

- 同じ Network Access Identifier (NAI; ネットワーク アクセス識別子) に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。したがって、この機能は同じ IP アドレスに対する複数のフローを維持するので、同時バインディングは必要ありません。

Remote Authentication Dial-In User Service (RADIUS) 切断

RADIUS 切断 (または Packet of Disconnect (POD; パケット オブ ディスコネクト)) は、RADIUS サーバが Radius Disconnect メッセージを HA に送信してリソースを解放できるメカニズムです。リソースは管理上の目的で解放され、主に HA のモバイル IP バインディングです。

Cisco Home Agent での RADIUS 切断のサポートは RFC 3576 に準拠します。HA はリソース管理機能を Access Request メッセージでホーム AAA サーバに送信します。このメッセージは、3GPP2 ベンダー固有の Session Termination Capability (STC) Vendor-Specific Attribute (VSA; ベンダー固有のアトリビュート) を含めることで、認証/許可手順用には送信されます。STC VSA で送信された値は設定から取得されます。**radius-server attribute 32 include-in-access-req format** コマンドの設定時、HA には、Access Request の Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を含んだ Network Access Server (NAS; ネットワーク アクセス サーバ) -Identifier アトリビュートがあります。

Disconnect Request が HA で受信されると、次のイベントが発生します。

-
- ステップ 1** ユーザ名に対応するユーザセッションを検出します (NAI)。
 - ステップ 2** Framed-IP-Address アトリビュートが Disconnect Request で受信された場合、アドレスに対応するバインディングを終了します。
 - ステップ 3** Framed-IP-Address が Disconnect Request で受信されない場合、ユーザのすべてのバインディングを終了します (NAI)。
-

RADIUS 切断クライアントの設定

クライアントと関連したキーに RADIUS 切断を設定するため、次の手順を実行します。

コマンド	目的
Router(config)# aaa server radius dynamic-author client a.b.c.d server-key hakey	HA 上で POD と Care-Of Address (CoA; 気付アドレス) の処理をイネーブルにします。
Router(config)# ip mobile radius disconnect	HA で RADIUS Disconnect メッセージを処理する機能をイネーブルにします。

コマンド	目的
Router (config) #radius-server attribute 32 include-in-access-req	任意の NAS-Identifier アトリビュートをホーム AAA に対するアクセス要求に含めるのに、このコマンドが必要です。
Router# debug aaa pod	AAA サブシステム レベルでの Radius Disconnect メッセージ処理のデバッグ情報を表示します。

RADIUS 切断の制約事項

次のリストには、RADIUS 切断機能の制約事項が含まれます。

- RADIUS 切断情報では MIB はアップデートされません。
- モバイル IP 条件デバッグはサポートされません。

バインディングの同期化および削除のサポート

現在の HA 冗長性の実装では、アクティブ スタンバイ モードのアクティブ HA（またはピアツーピアモードのピア）で削除されるバインディングは、Revocation メッセージまたは RADIUS Disconnect メッセージの受信により、スタンバイ HA またはピア HA に同期化されます。また、Revocation および Radius Disconnect の追加の拡張およびアトリビュートはスタンバイにリレーされます。

Registration Revocation および Radius Disconnect (**clear ip mobile binding** コマンドを使用) は、HA 冗長性でサポートされます。次のリストでは、このサポートの利点を示します。

HA 冗長性のアクティブ/スタンバイ モード

- トリガー（たとえば、Revocation メッセージまたは RADIUS Disconnect メッセージの受信）によって削除されるアクティブ HA 上のバインディングは、スタンバイ HA に同期化されます。
- 設定解除するコマンド（たとえば、**ip mobile host** など）によって削除されるバインディングは同期化されません。
- スタンバイ HA 上で削除されるバインディングは、アクティブ スタンバイ モードの場合にはアクティブに同期化されません。
- Revocation および Radius Disconnect の追加の拡張（失効サポート拡張）やアトリビュート（STC アトリビュート）はスタンバイ HA にリレーされます。

HA 冗長性のピアツーピア モード

- トリガー（たとえば、Revocation メッセージまたは RADIUS Disconnect メッセージの受信）によっていずれかのピアで削除されるバインディングは、他のピアに同期化されます。
- 設定解除するコマンド（たとえば、**ip mobile host** など）によって削除されるバインディングは同期化されません。
- Revocation および Radius Disconnect の追加の拡張（失効サポート拡張）やアトリビュート（STC アトリビュート）はピア HA にリレーされます。

バインディングの同期化

次のコールフローでは、モバイル IP フローを起動し、情報をスタンバイ HA に同期化するのに使用される、さまざまなネットワーク エンティティの間のシーケンスおよびメッセージ交換を示します。

1. MS はコールを発信し、PPP セッションがアップします。
2. PDSN は MN から MIP RRQ を受信し、FA-CHAP によって MN を認証します。適切な値 (2 または 3) を持った STC VSA は、AAA に送信されたアクセス要求メッセージに含まれます。認証が成功すると、PDSN は RRQ を HA に転送し、失効サポート拡張を MHAЕ の後に含めます。
3. 失効拡張を含んだ MIP RRQ を受信すると、HA では PDSN に送信された MIP RRP に失効サポート拡張が含まれます。MS を認証する HA-CHAP 時、適切な値 (2 または 3) を持った STC VSA は、AAA に送信されたアクセス要求メッセージに含まれます。HA でのバインディングは現在、取り消し可能であると見なされます。
4. PDSN は失効拡張を含んだ MIP RRP を受信します。MIP RRP に失効拡張が含まれているので、PDSN でのバインディングは取り消し可能です。
5. HA は冗長モードで設定されているので、Bind Update メッセージは追加情報 (失効サポート拡張および STC Normal Vendor Specific Extension (NVSE)) とともにスタンバイに送信されます。
6. スタンバイ HA は Bind Update メッセージで受信した情報を使用してバインディングを再生成し、スタンバイでバインディングを正常に作成したときのコード "accept" とともに Bind Update ACK メッセージを戻します。

バインディングの削除

このサポートの一部として 2 つの新しいメッセージ、"Bind Delete Request" と "Bind Delete ACK" が追加されました。これらのメッセージは、バインディングが削除されたときに冗長 HA の間で交換されます。次のコールフローでは、Revocation メッセージの受信によりバインディングがアクティブ HA で削除され、バインディングの削除がスタンバイ HA と同期するときを示します。

1. MS はコールを発信し、PPP セッションがアップします。モバイル IP フローは、登録失効機能がイネーブルとなりネゴシエートされたアクティブ HA でセットアップされます。同様にスタンバイ HA に同期化されます。
2. ユーザは administrative clear コマンドを発行し、PDSN は Revocation メッセージをアクティブ HA に送信し、ビジター エントリを削除し、関連付けられたリソースをクリアします。
3. MIP Revocation メッセージを受信すると、アクティブ HA は削除するバインディングを特定します。バインディングを特定すると、Bind Delete Request メッセージがスタンバイ HA に送信されます。
4. Bind Delete Request が送信されると、アクティブ HA は、着信した Revocation メッセージのバインディングに関連付けられたリソースを消去し、MIP Revocation ACK メッセージを PDSN に送信します。
5. Bind Delete Request メッセージを受信すると、スタンバイ HA は削除するバインディングを特定し、コード "accept" とともに Bind Delete ACK メッセージを戻します。
6. Bind Delete ACK メッセージが設定された時間内にアクティブ HA で受信されないと、Bind Delete Request メッセージは再送信されます。このプロセスは、最大再送信カウントの間繰り返されます。

バインディングの同期化中、拡張 (失効サポート拡張) と、Revocation および RADIUS Disconnect のアトリビュート (STC アトリビュート) がアクティブ HA からスタンバイ HA へ同期化されます。アクティブ HA がダウンし、スタンバイがアクティブになるシナリオでは、現在のアクティブ HA は RADIUS Disconnect メッセージの受信時にバインディングを削除できます。失効の場合、現在のアクティブ HA のバインディングは取り消し可能です。HA は現在、Revocation メッセージを送受信できます。

Selective FA Revocation

3GPP2 環境では、サブスライバが自分のサービス プロバイダーのネットワークと他のパートナーのサービス プロバイダーのネットワークの間でローミングすると、PDSN ゲートウェイは Resource Revocation メッセージを HA に送信してサブスライバを削除します。これによりタイミング問題が発生します。したがって、Selective FA Revocation はこれらの "remove subscriber" 要求を選択して無視します。失効は FA に基づいて実行されます。所定の HA は、"remove subscriber" メッセージを無視する FA のリストをスタティックに設定します。

次に、Selective FA Revocation の詳細なコール フローを示します。

1. デュアル 1x/DO ハンドセットは Redundancy Framework (RF; 冗長フレームワーク) に登録し、DO でデータ コールを確立します。音声コールとは異なり、RF ネットワークは Evolved Data Optimized (EVDO) ネットワークを認識していないので (標準により)、このデータ コールを Visitor Location Register (VLR; ビジター ロケーション レジスタ) に登録しません。
2. ハンドセットは休止します (Samsung で 35 秒、RIM で 30 秒、Sierra で 40 秒)。
3. ハンドセットは DO カバレレッジエリアから 1x カバレレッジエリアに移行します。この移行の一部として、ハンドセットは、MTX 経由でアクティブ データ セッションがあることを 1x RF に通知しますが、休止している (DRS ビットは 0 に設定されている) ので送信するデータはありません。新しいセッションが MTX Packet Control Function (PCF; パケット制御機能) 経由で PDSN に確立されます。
4. ステップ 3 のイベントに基づいて、1x PCF は、ハンドセットで述べたこのアクティブ データ セッションの VLR をクエリーします。ステップ 1 により、このようなセッションは検出できません。
5. ステップ 3 のイベントの一部として、PCF は現在、0 に設定された Mobility Event Indicator (MEI) で PDSN メッセージを (OpenRP インターフェイス経由で) 送信します。PDSN に対して、このイベントは、コールセットアップの一部としてまったく新しいセッション用であり、次のチェックを実行します。
 - MEI=0、および IMSI が既存のセッションに現在割り当てられていない新しい IMSI である場合、処理を進め、新しいセッションを確立します。
 - MEI=0、および IMSI が現在、セッションに割り当てられている場合、このセッションを古いものと見なし、セッションを切断します。
6. MEI=0、および IMSI が現在セッションに割り当てられているので (これは Hybrid PDSN であり、DO と 1X セッション両方を同時に処理するので)、PDSN は PPP TermReq をハンドセットに送信し、Resource Revocation を HA に送信します。
7. モバイル ノードは休止しており、TermReq を検出しません。MTX RF はしばらくメッセージをバッファリングします。
8. モバイル ノードはアクティブになりますが、送信するデータはありません。これは、まだ有効なモバイル IP セッションがあるかのように機能し、TermReq (バッファリングされた) メッセージおよび ACK メッセージを受信してからただちに RF セットアップ/RRQ を受信します。RRQ には、ハンドセットに割り当てられた IP アドレスや HA の IP アドレスなど、事前に割り当てられた値が含まれます。
9. PDSN はこれを新しいセッション (MEI=0、および IMSI は現在、セッションに割り当てられていません) と見なし、RRQ を HA に送信します。
10. 現在、HA は既存のバインディングがなく (ステップ 6 で失効)、RRQ にパラメータがある RRQ を検出し、これをスタティックに割り当てられた MN と見なします。
11. HA は Code-139 (管理上の禁止) を MN に戻します。

Selectable FA Revocation ならば、Hybrid PDSN/FA は上記の条件を通り、Revocation を HA に送信します。ただし、HA が Revocation を無視すると、RR 応答を PDSN に送信します。

この結果、MN と HA にはまだバインディング ステートがありますが、PDSN/FA には PPP セッション/ビジター テーブル エントリはありません。実際にモバイルはアクティブになり、Data Ready to Send があります。これには 1x RF チャネル **DRS=1** が含まれます。このシナリオでは、VLR はクエリーされず、PDSN への OpenRP メッセージでは **MEI** が 1 に設定されています。MEI 値に関係なく、PDSN は PPP を開始し、事前に割り当てられたホーム アドレスのある RRQ を送信します。この場合、HA は Re-registration を受信します。

Selective FA Revocation の設定

Selective FA Revocation を設定するには、次の手順を実行します。

コマンド	目的
Router(config)# ip mobile home-agent revocation ignore fa acl	HA をイネーブルにして、Revocation ACK を PDSN/FA に送信しますが、バインディングは削除しません。 <i>fa-acl</i> は ACK 番号 1-99 または名前です。

次に、**ip mobile home-agent revocation ignore** コマンドの例を示します。

standard access-list 番号または **standard access-list** 名を指定することで、FA からの失効を無視できます。

COA 5.1.1.4 からの要求を無視するよう **access-list** 名を設定

```
Router(config)#ip access-list standard ?
  <1-99>      Standard IP access-list number
  <1300-1999> Standard IP access-list number (expanded range)
  WORD       Access-list name
Router(config)#ip access-list standard fa_acl1
Router(config-std-nacl)#permit 5.1.1.4
```

COA 5.1.1.5 からの要求を無視するよう **access-list** 番号を設定

```
Router(config)#ip access-list standard ?
  <1-99>      Standard IP access-list number
  <1300-1999> Standard IP access-list number (expanded range)
  WORD       Access-list name
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit 5.1.1.5
```

FA 5.1.1.4 からの要求を選択して、無視するよう **access-list** 名を設定。これは、上記で作成した ACK と **ip mobile home-agent revocation ignore** コマンドを関連付けます。

```
Router((config)#ip mobile home-agent revocation ignore ?
  <1-99> fa Access-list number
  WORD   fa Access-list name
Router(config)#ip mobile home-agent revocation ignore fa_acl1
```

FA 5.1.1.5 からの要求を選択して、無視するよう `access-list` 番号を設定

```
Router(config)#ip mobile home-agent revocation ignore 1
```



(注) `ip mobile home-agent revocation ignore` は現在、1300 ~ 1999 (標準 IP `access-list` 番号 (拡張範囲)) の使用はサポートしていません。

Revocation メッセージでのオプションの NAI のサポート

3GPP2 標準仕様によると、Registration Revocation メッセージで NAI は必須アトリビュートであり、RFC3543 によると NAI はオプションのアトリビュートです。この機能は、NAI を Registration Revocation 要求メッセージに含めるようデフォルト動作を変更し、Revocation 要求メッセージから NAI を除外する CLI を提供します。Revocation Ack メッセージは Revocation 要求メッセージで受信したすべての拡張機能を保持します。



(注) HA Release 5.1 まで、Registration Revocation メッセージで FHAE 拡張機能だけがサポートされます。

冗長性の考慮事項

- 冗長性がサポートされています。Calling Station ID (CLID; 発信ステーション ID) は、バックアップ HA に同期し、スタンバイでのバインディングの場合にも一意の代替 MN ID として機能します。

Revocation メッセージでのオプションの NAI の設定

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	<code>Router(config)# ip mobile home-agent revocation exclude-nai</code>	(任意) IP Mobile Home Agent オプションの設定をイネーブルにして、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。

