CHAPTER 5

ユーザ認証および認可

この章では、ユーザ認証および認可について、さらに Cisco Mobile Wireless Home Agent でこの機能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。

ユーザ認証および認可

Home Agent（HA）は、PAP または CHAP を使用してユーザを認証するように設定できます。Foreign Agent（FA: 外部エージェント）チャレンジ手順がサポートされ（RFC 3012）、次の機能拡張が組み込まれています。

- モバイル IP エージェント アドバタイズ チャレンジの機能拡張
- MN-FA チャレンジの機能拡張
- MN-AAA 認証拡張機能

（注） MN-AAA 拡張機能がない場合は PAP を使用します。MN-AAA が存在する場合は、必ず CHAP を使用します。PAP ユーザのパスワードは、**ip mobile home-agent aaa user-password** コマンドで設定できます。

ホーム AAA サーバでユーザを認証するように設定されているときに、HA が Registration Request（RRQ; 登録要求）で MN-AAA 認証機能拡張を受信した場合は、その内容が使用されます。機能拡張がない場合は、デフォルトの設定可能なパスワードが使用されます。このデフォルトのパスワードは "vendor" など、ローカルで定義された文字列です。

HA は最初の登録の MN-FA チャレンジ機能拡張および MN-AAA 認証機能拡張（存在する場合）を受け付けて維持し、その後の登録更新で使用します。

HA が設定されたタイムアウトまでに AAA サーバから応答を受信しなかった場合は、設定可能な回数だけ、メッセージを再送できます。AAA サーバ グループと通信するように HA を設定できます。この場合、サーバはラウンドロビン方式で、設定された使用可能サーバから選択されます。

HA 上で認証および認可を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile host {lower [upper] | nai string {static-address {addr1 [addr2] [addr3] [addr4] [addr5] | local-pool name} | address {addr | pool {local name | dhcp-proxy-client [dhcp-server addr]} {interface name | virtual-network network_address mask} [skip-chap | aaa [load-sa [permanent]] [authorized-pool pool name] [skip-aaa-reauthentication] [care-of-access acl] [lifetime seconds]`	HA 上でモバイル ホストまたはモバイル ノード グループを設定します。 **aaa load-sa** オプションを設定した場合、HA は最初の登録でローカルに SA をキャッシュします。この場合、HA は再登録のための Remote Authentication Dial-In User Service（RADIUS）認証手順を開始しません。 **aaa load-sa skip-aaa-reauthentication** を設定した場合、HA は最初の登録でローカルに SA をキャッシュしますが、再登録のための HA-CHAP 手順は開始しません。 **aaa load-sa permanent** オプションは Mobile Wireless Home Agent ではサポートされないので、設定しないでください。

HA は RADIUS access accept パケットの 3GPP2 およびシスコ独自のセキュリティ機能拡張アトリビュートをサポートします。HA 上で、RADIUS サーバへのアクセス要求で 3GPP2 MN-HA SPI を送信し、RADIUS サーバから受け取った MN-HA 秘密鍵を処理することを設定できます。

Cisco IOS には、それぞれのレルムに基づいてサブスクライバを認可するメカニズムがあります。これには「サブスクライバの認可」という機能を使用します。詳細については、http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463 を参照してください。

（注） HA はユーザ プロファイルを受け付けますが、グループ プロファイルで返された情報に基づいて、モバイル サブスクライバを認可することはありません。

認証設定拡張機能

HA を使用して、特定のモバイル IP イベントについて AAA を使用した外部認証がいつ行われるかを設定できます。複数の FA をまたがるハンドオフは登録および登録解除イベントとして処理され、ハンドオフに対する特定の設定はありません。

再登録要求が前回の登録またはこのセッションに対する再登録に使用されたものとは別の SPI を使用して受信された場合は、このユーザの再登録時の認証に使用する設定オプション **enable** | **disable** は無視されます。

設定の適用または修正は、特定のバインディングに関する次回のイベントで行われます。

次の設定は、レルム単位（VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング））で行われる可能性のある再登録および登録解除イベント向けのものです。

ip mobile host nai *string* aaa **load-sa skip-aaa-reauth** [*reregistration* | *deregistration*]

デフォルト設定では、認証は 3 つのイベントすべてに対して発生します（**ip mobile host nai** *string* **aaa load-sa**）。

デフォルト設定が適切であることを前提とした例を次に示します。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** を実行すると、AAA 認証は登録に対してのみ発生します。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *deregistration* を実行すると、AAA 認証は登録および再登録に対して発生します。

ip mobile host nai *string* **aaa skip-chap** を実行すると、初回登録、再登録、および登録解除イベントに対して認証は発生しません。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** ***reregistration*** を実行すると、AAA 認証は登録および登録解除に対してのみ発生します。

load-sa キーワードを使用すると、HA はセッション全体にわたって mobile-home 認証に関するセキュリティ アトリビュートをダウンロードしてローカルで保存します。このパラメータを使用しなかった場合、HA は mobile-home 認証に関するセキュリティ アトリビュートをローカルで保存しないため、以降の再登録または登録解除時には AAA からこれらの情報を取得します。

Mobile-Home Authentication Extension（MHAE）を持たない 3GPP2 登録要求（RRQ）

現在、HA は RRQ での MN-HA オーセンティケータの拡張機能を必須機能として扱います。HA が MHAE 拡張機能を持たない RRQ を受信した場合、その RRQ は無視されます。

ただし MHAE 拡張機能は、標準/RFC に従うと必須ではないため、3GPP2 PMIP RRQ はこの機能を持たない場合があります。Cisco HA Release 5.1 では、MHAE 拡張機能を持たない 3GPP2 PMIP RRQ が FA-HA 認証に成功すれば、それを許可するよう HA を設定できます。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options mhae optional`	設定すると、HA は、MHAE を持たず、有効な Foreign-Home Authentication Extension（FHAE）を持った 3GPP2 RRQ を受信した場合、RRQ を処理します。

（注）　MHAE を持たず、有効な FHAE を持った CMIP RRQ を受信し、コマンドが設定されている場合、HA は RRQ を処理します。HA がこの RRQ を拒否しない理由は、HA が PMIP RRQ と CMIP RRQ を区別できないことです。この状況を回避するには、必ず FA が CMIP RRQ をチェックするようにして、FA が MHAE を持たない CMIP RRQ を HA に転送しないようにします。

3GPP2 のローカル認証

既存の HA 5.0 では、AAA からダウンロードした SA、またはローカルで設定されている HA のいずれかを使用してユーザを認証できます。これは、**ip mobile host nai** コンフィギュレーション コマンドで **aaa** キーワードを使用することでプロビジョニングできます。

HA 5.0 の機能はユーザ/nai ごとに設定できますが、アクセス タイプごとには設定できません。

HA Release 5.1 では、この機能をローカルの MN-HA SPI と Key を備えた NAI 認証と併用することで、ダウンロードした SA またはアクセス タイプに基づくローカル SA のいずれかを使用した柔軟なユーザ認証が可能になります。

この機能は、3gpp2 アクセス タイプにローカル SA を使用したユーザの認証、および Wimax アクセス タイプに AAA SA を使用した同一ユーザの認証に関する要件に対応しています。3gpp2 アクセス タイプ使用時は、アクセス要求は AAA に送信されません。

イネーブルな場合、RRQ が MN-AAA 拡張機能を備えている場合でも、アクセス要求は AAA に送信されません。

HA が 3GPP2 に対してローカル認証を実行するよう設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options`	サブモードをイネーブルにして、3GPP2 に対するローカル認証の設定を許可します。
ステップ 2	`Router(config)#access-type 3gpp2 suppress aaa access-request`	設定を許可して、AAA へのアクセス要求を抑制します。

この設定を **ip mobile host nai aaa** および **ip mobile secure host nai** と併用した場合、3gpp2 アクセスタイプにローカル SA を使用したユーザの認証、および Wimax アクセス タイプに AAA SA を使用した同一ユーザの認証に関する要件に対応します。

ローカル MN-HA SPI および Key を使用した NAI 認証

HA R5.0 は、MN-HA セキュリティ アソシエーション（SA）または AAA からダウンロードした MN-HA SA 向けのローカル設定をサポートしますが、これら両方を同時にはサポートしません。

HA Release 5.1 では、HA は MN-HA SA および AAA からダウンロードした SA のローカル設定の両方をサポートします。SA がローカルに設定されているかどうかにかかわらず、HA が AAA からのアクセス応答メッセージ内の SA を受信した場合は、AAA からダウンロードした SA だけが MN-HA 認証に使用されます。

制限事項および制約事項

- **ip mobile host** コマンドが完全な NAI 向けに設定されている場合、対応するレルムにローカルで設定されている SA（単数または複数）は適用されません。ローカル SA を適用する必要がある場合、SA を完全な NAI に対して個別に設定する必要があります。

  次の例を考えてみましょう。

  - **ip mobile host nai *@cisco.com* virtual-network** *ip1 mask1* **aaa**
  - **ip mobile host nai** *user1@cisco.com* virtual-network ip2 mask2 **aaa**
  - **ip mobile secure host nai** *@cisco.com* **spi** *100* **key ascii** *CISCO*

  ここで、*@cisco.com* に設定されている SA は *user1@cisco.com*. には適用されません。ローカル SA をこのユーザに適用する必要がある場合は、次に示すとおり SA を個別に設定する必要があります。

  ip mobile secure host nai *user1@cisco.com* **spi** *100* **key ascii** *YAHOO*

- この機能がサポートされるのは 3GPP2 ユーザだけで、Wimax ユーザではサポートされません。

再登録 / 登録解除に対する無認可

ローカル MN-HA SPI および Key 機能と NAI 認証を併用すると、ローカル設定された SA および AAA からダウンロードした SA が共にサポートされます。

ただし、次のコマンドを設定すると、再認証と再認可が回避されるのは、MN-HA 向けの SA が Access-Accept で受信された場合に限られます。

```
router (config)# ip mobile host nai realm virtual-network ip mask aaa load-sa
skip-aaa-reauth [rereg | dereg]
```

ローカル登録時に MN-HA 認証がローカル SA を使用している場合は、上記の設定を使用しても、再認証 / 再認可は省略されません。これは、**load-sa** がキャッシュするのは、AAA からダウンロードした SA だけであるためです。

load-sa が設定されていれば、ローカル設定されている SA を使用している場合でも、この機能は SA のキャッシングをサポートします。**load-sa** が設定されている場合、ローカル設定されている SA を使用しても、再認証は回避されます。さらに、**skip-aaa-reauth** が設定されている場合、ローカル設定されている SA を使用すると、AAA を使用した再認証は回避されます。

[**rereg** | **dereg**] オプションを指定した場合、再登録または登録解除のどちらか一方だけに対して、再認証と再認可の回避を選択できます。

MN-FA Challenge Extension（MFCE）による HA-CHAP の省略

この機能を使用すると、ホーム AAA サーバで HA-CHAP 手順を実行して、各登録要求のユーザに対応するセキュリティ アソシエーション（SA）をダウンロードするのではなく、HA に SA をダウンロードさせ、ディスクにローカルにキャッシュさせることができます。HA は、ユーザが初めて HA に登録したときに、HA-CHAP（MN-AAA 認証）を行い、SA をダウンロードして、ローカルにキャッシュします。その後、再登録要求があると、HA はローカル キャッシュの SA を使用してユーザを認証します。ユーザのバインディングが削除されると、SA キャッシュ エントリが削除されます。

この機能は、上記の **ip mobile host** コマンドを使用して、HA 上で設定します。

設定例

次に、仮想ネットワーク 10.99.1.0 に配置するモバイル ノード グループを設定し、AAA サーバからモバイル ノードの SA を取得してキャッシュする例を示します。その後の再登録には、キャッシュの SA が使用されます。

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

次に、cisco.com ドメインのモバイル ノードに IP アドレスを割り当てるために使用する、ローカルなダイナミック アドレス プールの設定例を示します。AAA サーバから受け取った SA は、手動で削除されるまで、永久にキャッシュされます。

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

認証および認可の RADIUS アトリビュート

HA および RADIUS サーバは、認証および認可サービスに関して、表 1 の RADIUS アトリビュートをサポートします。

表 1　Cisco IOS がサポートする認証および認可 AVP

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	フォーマット	説明	アクセス要求 アクセス受諾での可否	
User-Name	1	該当しない	64	ストリング	認証および認可のユーザ名	可	不可
User-Password	2	該当しない	>=18 && <=130	ストリング	PAP 使用時の認証パスワード HA で CLI を使用して設定されたパスワード	可	不可
CHAP-Password	3	該当しない	19	ストリング	CHAP パスワード	可	不可
NAS-IP-Address	4	該当しない	4	IP アドレス	RADIUS サーバとの通信に使用する HA インターフェイスの IP アドレス	可	不可
Service Type	6	該当しない	4	整数	ユーザが利用するサービスのタイプ サポートされる値： • PAP 用に送信されるアウトバウンド • CHAP 用に送信されるフレーム化 • 両方のケースで受信するフレーム化	可	可
Framed-Protocol	7	該当しない	4	整数	フレーミング プロトコル ユーザが使用。CHAP の場合の送信、PAP および CHAP の場合の受信 サポートされる値： • PPP	可	可
Framed Compression	13	該当しない	4	整数	圧縮方式 サポートされる値： • 0：なし	不可	可
Framed-Routing	10	該当しない	4	整数	ルーティング方式 サポートされる値： • 0：なし	不可	可
Vendor Specific	26	該当しない			ベンダー固有のアトリビュート	可	可
CHAP-Challenge（任意）	60	該当しない	>=7	ストリング	CHAP Challenge	可	不可

表 1　Cisco IOS がサポートする認証および認可 AVP （続き）

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	フォーマット	説明	アクセス要求 アクセス受諾での可否	
NAS-Port-Type	61	該当しない	4	整数	ポート タイプ サポート対象： • 0：非同期	可	不可
spi#*n*	26/1	Cisco	>=3	ストリング	*n* は、1 ユーザに複数の SA を許可する、**0** から始まる数値 ID MIP 登録時にモバイル ユーザを認証するための、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）を提供します。 コンフィギュレーション コマンド **ip mobile secure host** *addr* と同じ構文の情報です。基本的に、そのストリングの後ろに残りのコンフィギュレーション コマンドを一字一句指定します。	不可	可
static-ip-addresses	26/1	Cisco	>=3	ストリング	同じ NAI でマルチ フローのスタティック アドレスに対応する IP アドレス リスト	不可	可
static-ip-pool	26/1	Cisco	>=3	ストリング	同じ NAI でマルチ フローのスタティック アドレスに対応する IP アドレス プール名	不可	可
ip-addresses	26/1	Cisco	>=3	ストリング	ダイナミック アドレス割り当てに使用する IP アドレス リスト	不可	可
ip-pool	26/1	Cisco	>=3	ストリング	ダイナミック アドレス割り当てに使用する IP アドレス プール名	不可	可
dhcp-server	26/1	Cisco	>=3	ストリング	指定された DHCP サーバからアドレスを取得	不可	可
MN-HA SPI Key	26/57	3GPP2	6	整数	MN HA 共有鍵に対応する SPI	可	不可
MN-HA Shared Key	26/58	3GPP2	20	ストリング	MHAE を認証するためのセキュア キー	不可	可