CHAPTER 4

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。

この章の構成は、次のとおりです。

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。外部エージェント（FA）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 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加入者を認可するメカニズムがあります。これには「加入者の認可」という機能を使用します。詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463

（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、モバイル加入者を認可することはありません。

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 4-1 の RADIUS アトリビュートをサポートします。

表 4-1　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	可否	
						アクセス要求	アクセス受諾
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
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

表 4-1　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	可否	
						アクセス要求	アクセス受諾
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、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