



## モバイル IP の概要

モバイル IP は、Internet Engineering Task Force (IETF) RFC 3220 で定義されたオープン スタンダードです。モバイル IP を使用することで、IP ネットワーク間でローミングを行う間も同じ IP アドレスを維持し、接続を継続し、現行のアプリケーションを続行できます。モバイル IP は IP に基づいているため、インターネットに対する拡張性を持ちます。IP をサポートするメディアはすべてモバイル IP をサポートします。

ここではモバイル IP テクノロジーの概要について説明します。

### モバイル IP の概要

シスコ モバイル ネットワーク機能を使用すると、モバイル アクセス ルータおよびそのサブネットを移動したり、モバイル アクセス ルータを通してすべての IP 接続を IP ホストにトランスペアレントに接続し続けたりすることができます。現在、この機能はスタブルータのみをサポートするスタティック ネットワークに実装されています。

IP ネットワークでは、ルーティングは固定 IP アドレスに基づいて行われます。ネットワーク上のデバイスには、ネットワークで割り当てられた IP アドレスによる通常の IP ルーティングを使用して到達できます。デバイスがホーム ネットワークから離れた場所でローミングする場合、通常の IP ルーティングではアドレスに到達できません。

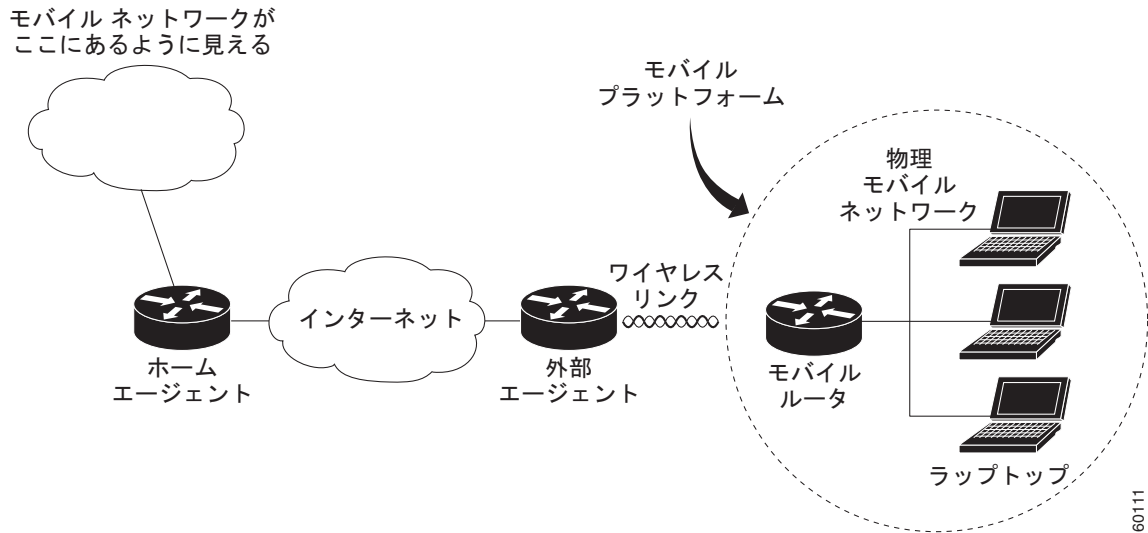
その結果、デバイスのアクティブなセッションが終了します。モバイル IP を使用すると、別のネットワークに移動している間も同じ IP アドレスが維持されるため、個々のローミング ユーザはセッションまたは接続を中断せずに通信を続けることができます。

モバイル IP のモビリティ機能は物理レイヤではなくネットワーク レイヤで実行されるため、モバイル デバイスは接続を維持しながら異なるタイプのワイヤレスおよびワイヤ回線ネットワークを移動できます。個々のユーザがネットワーク境界を越えてローミングする間も通信の中断を避けるべきアプリケーションとして、リモート ログイン、リモート印刷、ファイル転送があげられます。またソフトウェア ライセンスやアクセス権限などの特定のネットワーク サービスは、IP アドレスをベースにしています。これらの IP アドレスを変更すると、ネットワーク サービスが損なわれる可能性があります。

ホーム ネットワークに存在するユーザのように見えながらローミングが行えるデバイスをモバイル ノードと呼びます。モバイル ノードの例として、Personal Digital Assistant (PDA)、ラップトップ コンピュータ、データレディ携帯電話があげられます。これらはネットワークまたはサブネット間で接続ポイントを変更できるものです。このモバイル ノードはリンク間を移動でき、同じ IP アドレスを使用して通信を維持します。このソリューションはネットワーク レイヤで実行され、透過的にネットワークを移動するため、アプリケーションの変更は不要です。

シスコ モバイル ネットワーク機能は モバイル アクセス ルータ (MR)、ホーム エージェント (HA)、および外部エージェント (FA) の 3 つのコンポーネントで構成されます。図 3-1 に、この 3 つのコンポーネント (モバイル アクセス ルータ、ホーム エージェント、および外部エージェント) およびモバイル ネットワーク内のこれらの関係を示します。

図 3-1 シスコ モバイル ネットワークのコンポーネントと関連性



モバイル アクセス ルータはモバイル ノードと同じように機能しますが、モバイル アクセス ルータではネットワーク全体でのローミングが可能になるという重要な違いがあります。たとえば、モバイル アクセス ルータを搭載した航空機は、乗客がインターネットに接続している状態で世界中を飛行できます。このような通信は、モバイル ネットワーク上のホスト宛てのパケットを、モバイル アクセス ルータがアクセスするロケーションにトンネリングするルータをモバイル IP が認識することで実現します。そのあとモバイル アクセス ルータはパケットを宛先のデバイスに転送します。

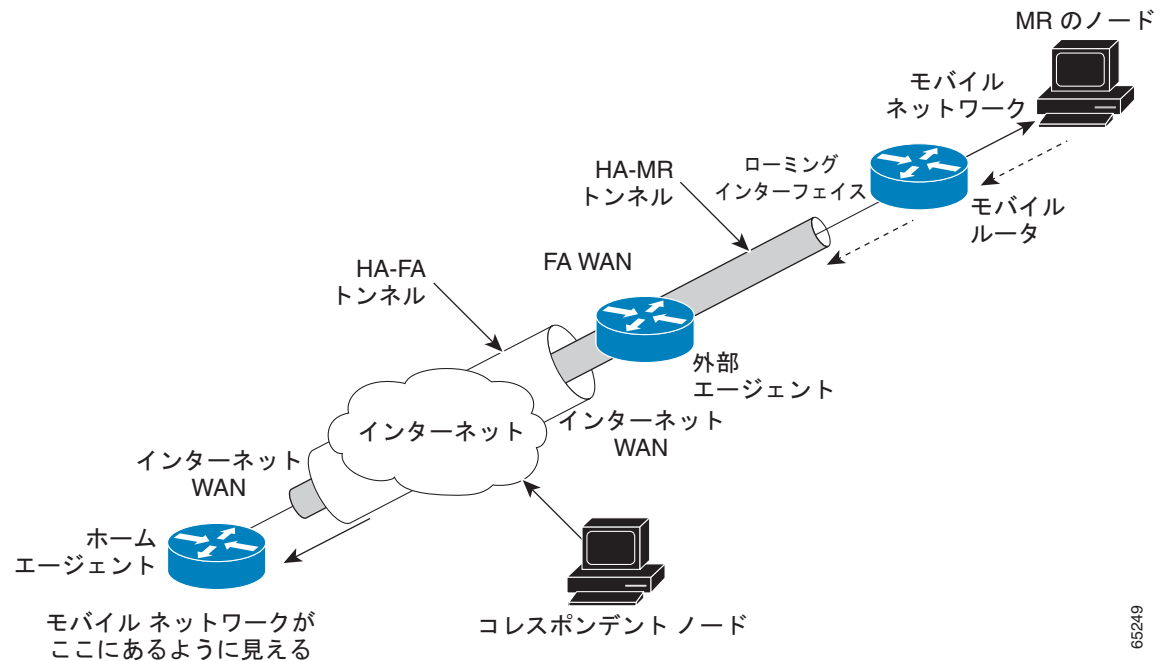
これらのデバイスが、モバイル IP クライアントのソフトウェアを使用せずにモバイル ノードになる場合があります。モバイル アクセス ルータにより、モバイル IP クライアントが不要になります。モバイル アクセス ルータは、ローカル IP ノードから IP ローミングを「隠す」ことで、ローカル ノードが直接ホーム ネットワークに接続しているように見せます。

ホーム エージェントはモバイル アクセス ルータのホーム ネットワーク上のルータです。モバイル ネットワークのアンカー ポイントを提供します。ホーム エージェントはモバイル アクセス ルータのホーム IP アドレスと、外部またはビジター接続ネットワーク上のモバイル アクセス ルータの現在位置である Care-of Address (CoA; 気付アドレス) とのアソシエーションを維持します。ホーム エージェントはモバイル アクセス ルータのローミング場所と、モバイル ネットワークの現在位置にトンネリングされているパケットの追跡を担当します。またホーム エージェントはモバイル ネットワークをルーティング テーブルに追加します。

外部エージェントはモバイル アクセス ルータがホーム エージェントに現在の CoA を通知するのを支援する外部ネットワーク上のルータです。外部エージェントは、モバイル アクセス ルータの接続ポイントとして機能し、パケットをホーム エージェントからモバイル アクセス ルータに送信します。外部エージェントは直接モバイル アクセス ルータと論理的に接続する固定ルータです。モバイル アクセス ルータと外部エージェントは、ワイヤレス リンクで直接接続する必要はありません。たとえば、モバイル アクセス ルータがローミングする場合、同じサブネット上にないインターフェイスで外部エージェントとモバイル アクセス ルータの接続が開始します。この機能によって、外部エージェント コンポーネントに機能が新たに付加されることはありません。

図 3-2 にモバイル IP コンポーネントを示します。

図 3-2 モバイル IP のコンポーネントと関連性



65249

## モバイル IP のプロセス

モバイル IP プロセスは 3 つのフェーズで構成されています。

- **エージェントの検出**：エージェント検出の実行中に、モバイル ノードが外部エージェントとホーム エージェントを検出します。
- **登録**：登録の実行中に、モバイル ノードは現在の位置を外部エージェントとホーム エージェントに登録します。
- **トンネリング**：CoA（外部ネットワークのモバイル ノードの現在の位置）への相互トンネルがホーム エージェントによって設定され、パケットをローミング中のモバイル ノードにルーティングします。

## エージェントの検出

エージェントの検出フェーズでは、ホーム エージェントと外部エージェントは ICMP Router Discovery Protocol (IRDP) を使用してネットワーク上で各サービスをアドバタイズします。モバイル ノードはこれらのアドバタイズを待ち受けて、ホーム ネットワークと外部ネットワークのどちらに接続されているのかを判断します。

IRDP アドバタイズによって、リバース トンネリングや Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) などの Type of Service (ToS; サービス タイプ)、およびモバイル ノードにアクセスする場合の許容登録期間とローミング期間を含むモバイル IP 拡張機能が搬送され、このモバイル IP 拡張機能によってエージェントが、ホーム エージェントと外部エージェントのどちらかまたはその両方であるかどうか指定されます。モバイル ノードはエージェントのアドバタイズを待機することなく、エージェント送信請求を送信できます。リンク上のすべてのエージェントは、この送信請求が発行されると速やかにエージェント アドバタイズを送信する必要があります。

モバイル ノードが外部ネットワークに接続されていると判断すると、モバイル ノードは CoA を取得します。次の 2 種類の CoA があります。

- 外部エージェントから取得する CoA
- Collocated Care-of Address (CCoA; 連結型気付アドレス)

外部エージェントの CoA は、外部エージェントがアクセスする外部ネットワーク上にインターフェイスを持つモバイル ノードの IP アドレスです。このタイプの CoA を取得するモバイル ノードは、他のモバイル ノードとアドレスを共有できます。CCoA は、モバイル ノードのインターフェイスに一時的に割り当てられた IP アドレスです。CCoA は、外部ネットワーク上のモバイル ノードの現在位置を表します。CCoA を使用できるのは、一度に 1 つのモバイル ノードだけです。

モバイル ノードが外部エージェントのアドバタイズを受信し、外部エージェントがホーム ネットワークの外部に移動したことを検出すると、モバイル ノードは登録を開始します。

## 登録

モバイル ノードには、ホーム エージェントの IP アドレスと（共有キーを含む）モビリティのセキュリティ アソシエーションが設定されます。これ以外に、モバイル ノードにはホーム IP アドレスまたは Network Access Identifier などの別のユーザ識別情報が設定されます。

モバイル ノードはこの情報を外部エージェントのアドバタイズから学習した情報とともに使用して、モバイル IP レジストレーション要求を形成します。モバイル ノードはレジストレーション要求を保留リストに追加し、ホーム エージェントを通じて、または、CCoA を使用して外部エージェントを通じて登録する必要がない場合は直接、外部エージェントにレジストレーション要求を送信します。レジストレーション要求が外部エージェントを通じて送信される場合、外部エージェントは要求された有効期間が制限を超えていないか、要求されたトンネル カプセル化が使用できるかどうか、またリバース トンネルがサポートされているかなど、レジストレーション要求の有効性を確認します。

レジストレーション要求が有効であれば、外部エージェントはアクセスしているモバイル ノードを保留リストに追加してから、ホーム エージェントに要求の応答をリレーします。レジストレーション要求が無効の場合、外部エージェントは適切なエラー コードを含めたレジストレーション応答をモバイル ノードに送信します。

ホーム エージェントは、モバイル ノードの認証を含むレジストレーション要求の有効性を確認します。レジストレーション要求が有効であれば、ホーム エージェントはモビリティ バインディング（モバイル ノードの CoA とのアソシエーション）、CoA へのトンネル、およびトンネルを通じてパケットをホーム アドレスに転送するためのルーティング エントリを作成します。

次にホーム エージェントは（モバイル ノードを通じてレジストレーション要求を受け取っている場合は）外部エージェントを通じて外部エージェントに、または直接モバイル ノードにレジストレーション応答を送信します。レジストレーション要求が無効の場合、ホーム エージェントは適切なエラー コードを含めたレジストレーション応答を送信して要求を拒絶します。

外部エージェントは、関連付けられているレジストレーション要求が保留リストに存在することの確認を含めて、レジストレーション応答の有効性を確認します。レジストレーション応答が有効な場合、外部エージェントは Visitor List（ビジター リスト）にモバイル ノードを追加して、ホーム エージェントへのトンネルを確立し、パケットをホーム アドレスに転送するためのルーティング エントリを作成します。次に外部エージェントは、レジストレーション応答をモバイル ノードにリレーします。

最後にモバイル ノードは、関連付けられた要求が保留リストにあること、およびホーム エージェントの認証が適切であることの確認を含めて、レジストレーション応答の有効性を確認します。レジストレーション応答が無効の場合、モバイル ノードはその応答を廃棄します。有効なレジストレーション応答に登録の許可が指定されている場合、モバイル ノードのローミングがモバイル エージェントによって確認されています。CCoA の場合、モバイル ノードはホーム エージェントにトンネルを追加します。そのあと、モバイル ノードはすべてのパケットを外部エージェントに送信します。

モバイル ノードは登録有効期間が終了する前に再登録を行います。ホーム エージェントおよび外部 エージェントは、再登録の間にそれぞれモビリティ バインディングとビジター エントリを更新します。登録が拒絶された場合、モバイル ノードは必要な調整を行い、再度登録を試みます。たとえば、登録が時間の不一致のために拒絶され、ホーム エージェントが同期のためにタイム スタンプを戻した場合、モバイル ノードはそのあとのレジストレーション要求でタイム スタンプを調整します。

登録に成功したモバイル IP は、ローミング中のモバイル ノードとの間でパケットを相互送信するためのルーティング メカニズムを設定します。

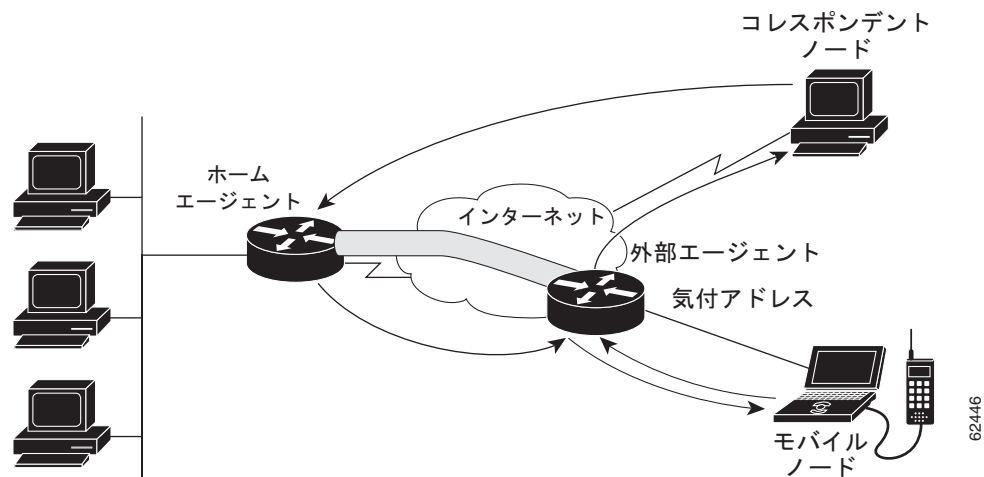
## トンネリング

モバイル ノードはホーム IP アドレスを使用してパケットを送信し、実際に常にホーム ネットワーク上に存在しているように見えます。モバイル ノードは外部ネットワーク上をローミングしている間も、その動きは **Correspondent Node (CN; コレスポンデント ノード)** には見えません。

モバイル ノード宛てのデータ パケットはホーム ネットワークにルーティングされ、ホーム ネットワークのホーム エージェントがそれを代行受信し、モバイル ノード宛ての **CoA** にトンネリングします。トンネリングには大きく 2 つの機能があります。トンネルのエンドポイントに向かうデータ パケットのカプセル化、およびエンドポイントに着信したパケットのカプセル化解除です。デフォルトのトンネルモードは、**IP Encapsulation within IP Encapsulation** です。任意で **GRE within IP** も使用できます。

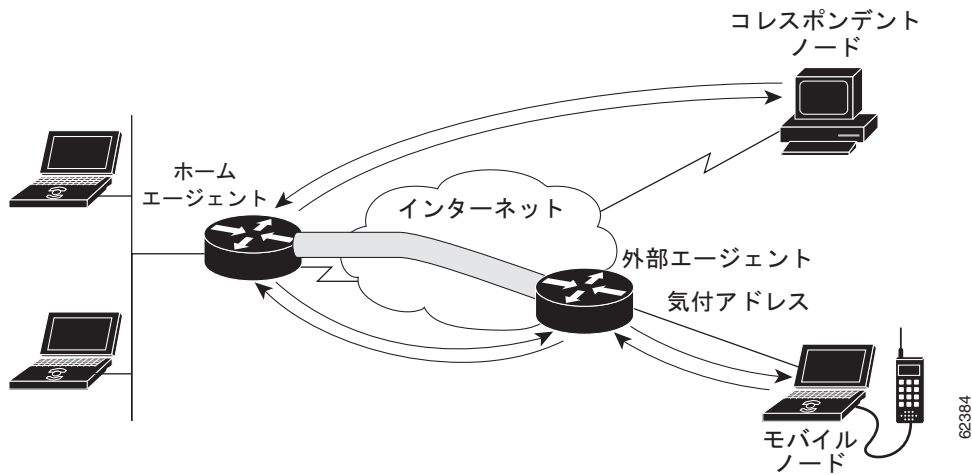
一般に、[図 3-3](#) に示されるように、モバイル ノードは外部エージェントにパケットを送信し、そこで最終的な宛先、CN にルーティングされます。

図 3-3 パケットの転送



ただし、このデータ パスはデータの実際の IP ネットワーク ソースではなく、モバイル ノードのホーム ネットワークを反映しているため、トポロジー上は正しくありません。パケットは外部ネットワーク内部の送信元としてホーム ネットワークを示しているため、ネットワークのルータ上にある入力側フィルタリングと呼ばれる **Access Control List (ACL; アクセス制御リスト)** によって、転送されずに廃棄されます。この問題はリバース トンネリングと呼ばれる機能によって解決されます。この場合外部エージェントがモバイル ノードからパケットを受け取ると、パケットを元のホーム エージェントにトンネリングします。[図 3-4](#)を参照してください。

図 3-4 リバース トンネル



トンネル MTU（最大伝送ユニット）検出は、ホーム エージェントなどのトンネル エンカプスレータがパス MTU 検出に参加して、CN とモバイル ノード間のルーティング パスでパケットが分割されるのを防ぐためのメカニズムです。モバイル ノード宛てのパケットの場合、ホーム エージェントは CoA へのトンネルの MTU を維持し、低減したパケット サイズを CN に通知します。これにより、トンネルのエンドポイントでの分割と再アセンブリを防ぎ、パケットが確実にモバイル ノードに到達するための効率的なルーティングが実現します。

## モバイル IP と DHCP の比較

PDA や次世代データレディ式の携帯電話およびサービスなどの新しいデバイスと商慣習により、ネットワーク接続を維持しながらユーザがローミングできることに関心が高まっています。このようなユーザ層に向けたデータ接続ソリューションの要件は、固定式のダイヤルアップ ユーザや固定ワイヤ LAN ユーザとは大きく異なります。ソリューションはデータ セッション中または会話中の移動という問題に対応する必要があります。

IP ルーティングは、IP アドレスのネットワーク プレフィクスに基づいて決定します。同じリンク上のすべてのノードは、共通のネットワーク プレフィクスを共有します。ノードが別のリンクに移動すると、ネットワーク プレフィクスは新しいリンクのネットワーク プレフィクスと一致しなくなります。その結果、新しいリンクへ移動すると、IP ルーティングでパケットのノードへのルーティングに失敗します。

企業環境では、Dynamic Host Configuration Protocol (DHCP) が一般に使用されます。DHCP を使用するサーバは、ノードに IP アドレスを動的に割り当て、ノードに設定パラメータを送信できます。DHCP サーバはノードの ID を検証し、事前に決められた期間、アドレス プールから IP アドレスをリースし、リースの期限が終了すると再割り当てのためにアドレスを再申請します。ノードは既存の通信セッションを終了し、ネットワークの新しい接続ポイントに移動し、ネットワークに再度接続します。そのあと DHCP から新しい IP アドレスを受け取ります。これによって IP アドレスが維持され、インターネットのアクセス コストが抑えられます。ただし、ユーザがモバイル ユーザで、連続的な通信とアクセス機能が必要になる場合、DHCP は十分なソリューションになりません。DHCP では、アプリケーションはサブネットとネットワークの境界を越えて接続を維持できません。ノードの IP アドレスのネットワーク プレフィクスは、インターネットにおけるパケットの適切なルーティングと連続的な接続に欠かすことができません。モバイル IP はこのプレフィクスを廃棄しません。