CHAPTER 21

# NAT の設定

この項では、ネットワーク アドレス変換について説明します。次の項目を取り上げます。

# NAT の概要

この項では、FWSM で NAT がどのように機能するかを説明します。次の項目を取り上げます。



## NAT の概要

アドレス変換は、パケット上にある実際のアドレスを、宛先ネットワークでルーティングできるマッピング済みアドレスに置き換えます。NAT は、実際のアドレスをマッピング済みアドレスに変換するプロセスと、トラフィックを返すために変換を元に戻すプロセスの 2 段階で構成されています。NAT はルーテッド モードと透過ファイアウォール モードの両方でサポートされています。

FWSM は、NAT のルールがトラフィックと一致した場合にアドレスを変換します。NAT のルールが一致しない場合、パケットの処理が続行されます。NAT の制御をイネーブルにする場合は例外です。NAT の制御では、上位のセキュリティ インターフェイス（内部）から下位のセキュリティ インターフェイス（外部）へ通過するパケットが NAT のルールと一致している必要があります。一致しない場合はパケットの処理が停止します（セキュリティ レベルの詳細については、P.5-3 の「等位セキュリティ レベル間の通信のイネーブル化」を参照してください。NAT 制御の詳細については、P.21-5 の「NAT 制御」を参照してください）。

（注）　このマニュアルでは、変換の種類に関係なくすべて NAT としています。NAT について説明する場合、*内部*と*外部*は相対的であり、2 つのインターフェイス間のセキュリティ関係を表しています。上位のセキュリティ レベルが内部で、下位のセキュリティ レベルが外部となっています。たとえば、インターフェイス 1 のセキュリティ レベルが 60 でインターフェイス 2 のセキュリティ レベルが 50 の場合、インターフェイス 1 が「内部」、インターフェイス 2 が「外部」となります。

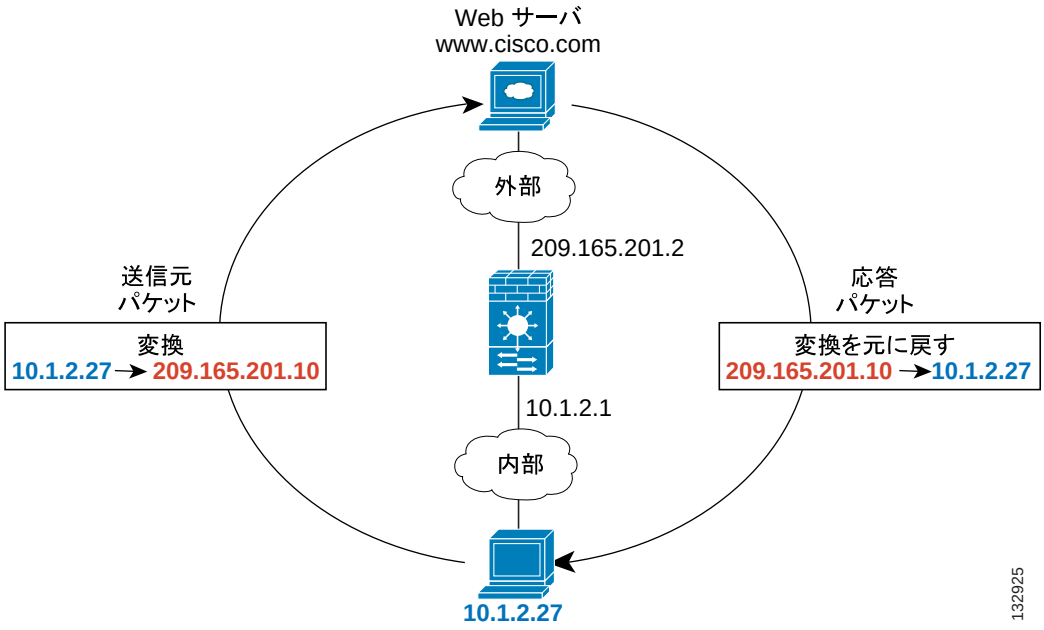
NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT は実際のアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- アドレスの重複などの IP ルーティングの問題点を解決できます。

## ルーテッド モードの NAT

図 21-1 は、内部にプライベート ネットワークを持つ一般的なルーテッド モードの NAT シナリオを示しています。10.1.1.27 の内部ホストから Web サーバへパケットが送信される場合、パケットの実際の送信元アドレス 10.1.1.27 がマッピング済みアドレス 209.165.201.10 に変換されます。Web サーバは応答をマッピング済みアドレス 209.165.201.10 に送信し、FWSM はパケットを受信します。次に、FWSM がマッピング済みアドレス 209.165.201.10 の変換を実際のアドレス 10.1.1.27 に戻してから、ホストへ送信します。

**図 21-1　NAT の例：ルーテッド モード**




## 透過モードの NAT

透過モードで NAT を使用すると、そのネットワークに対する NAT をアップストリーム ルータまたはダウンストリーム ルータで実行する必要がなくなります。たとえば、透過ファイアウォール FWSM を 2 つの VRF 間に配置すると、VRF とグローバル テーブルの間で BGP ネイバーの関係を確立するのに役立ちます。ただし、VRF ごとの NAT はサポートされていない場合があります。この場合、透過モードで NAT を使用する必要があります。

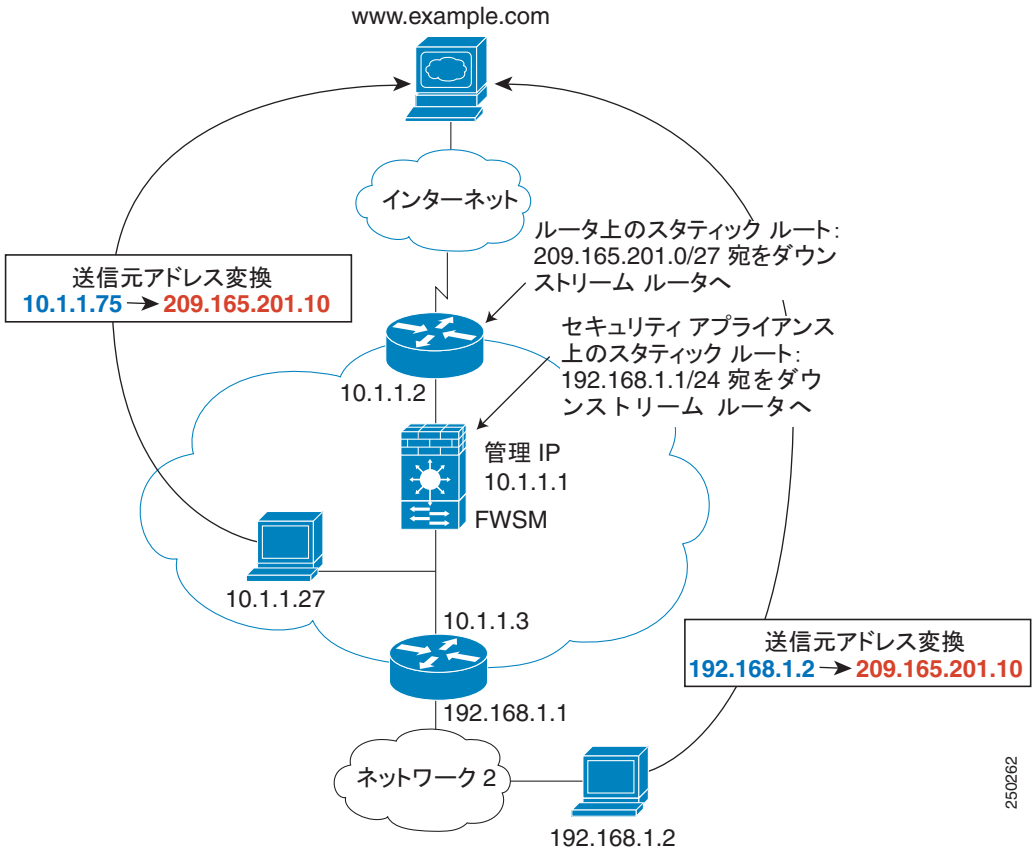
透過モードの NAT には、次のような要件および制限事項があります。

- マッピング済みアドレスが透過ファイアウォールと同じネットワークにない場合、（FWSM 経由で）ダウンストリーム ルータをポイントする、マッピング済みアドレスのスタティック ルートをアップストリーム ルータで追加する必要があります。
- 実際の宛先アドレスが直接 FWSM に接続されていない場合、ダウンストリーム ルータをポイントする実際の宛先アドレスのスタティック ルートも FWSM で追加する必要があります。NAT を使用しない場合、アップストリーム ルータからダウンストリーム ルータへのトラフィックで MAC アドレス テーブルを使用するため、FWSM のルートは不要です。ただし、NAT により FWSM が MAC アドレス ルックアップではなくルート ルックアップを使用するため、ダウンストリーム ルータへのスタティック ルートが必要になります。
- **alias** コマンドはサポートされていません。

- 透過ファイアウォールにはインターフェイスの IP アドレスがないため、インターフェイスの PAT を使用できません。
- ARP 検査はサポートされていません。さらに、何らかの理由でファイアウォール内外のどちらかのホストから相手のホストに ARP 要求が送信され、開始側のホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされた場合、実際のアドレスは ARP 要求で可視のままになっています。

図 21-2 に、内部インターフェイスと外部インターフェイスに同じネットワークがある場合の、一般的な透過モードの NAT シナリオを示します。このシナリオでは、透過ファイアウォールが NAT サービスを実行するので、アップストリーム ルータで NAT を実行する必要がありません。10.1.1.27 の内部ホストから Web サーバにパケットが送信された場合、そのパケットの実際の送信元アドレス 10.1.1.27 は、マッピング済みアドレス 209.165.201.10 に変換されます。サーバは応答をマッピング済みアドレス 209.165.201.10 に送信し、FWSM はパケットを受信します。これは、アップストリーム ルータで、FWSM を経由するスタティック ルート内にこのマッピング済みネットワークが指定されているからです。次に、FWSM が変換を元に戻し、マッピング済みアドレス 209.165.201.10 を実際のアドレス 10.1.1.27 に戻します。実際のアドレスは直接に接続されているので、FWSM がホストに直接に応答を送信します。192.168.1.2 のホストの場合、FWSM は自分のルート テーブルでルートをルックアップし、スタティック ルートに基づいてパケットを 10.1.1.3 のダウンストリーム ルータへ送信すること以外は、同じプロセスが実行されます。

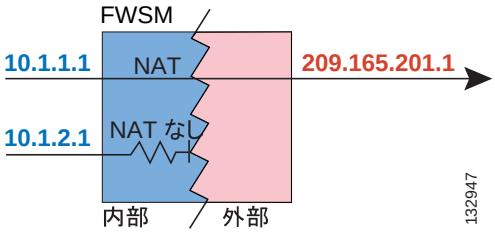
**図 21-2　NAT の例：透過モード**



## NAT 制御

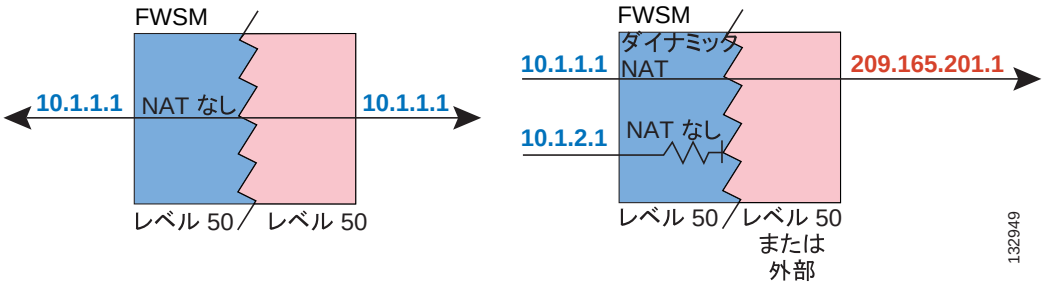
NAT 制御では、内部インターフェイスから外部インターフェイスへ通過するパケットが NAT のルールと一致している必要があります。内部ネットワークのホストから外部ネットワークのホストへアクセスする場合、内部ホストのアドレスを変換するよう NAT を設定する必要があります（図 21-3 を参照）。

**図 21-3　NAT 制御と発信トラフィック**



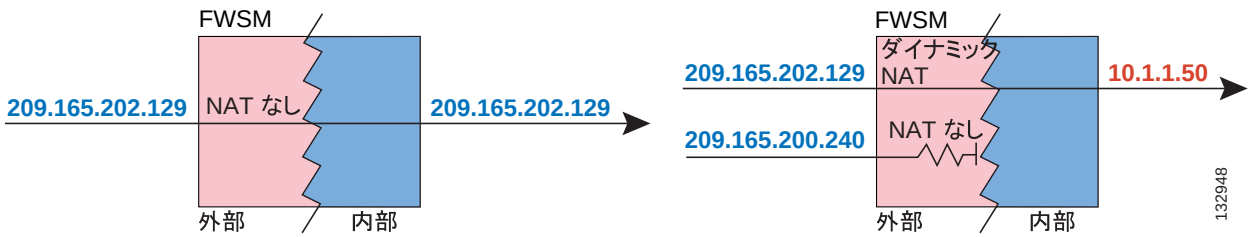

セキュリティ レベルが等位のインターフェイス間の通信では、NAT は必須ではありません。ただし、NAT 制御がイネーブルの状態でセキュリティが等位のインターフェイスにダイナミック NAT または PAT を設定すると、等位セキュリティのインターフェイスまたは外部インターフェイスからのトラフィックは、すべて NAT のルールと一致している必要があります（図 21-4 を参照）。

**図 21-4　NAT 制御と等位セキュリティ レベルのトラフィック**




同様に、NAT 制御がイネーブルの状態で外部ダイナミック NAT または PAT を設定すると、すべての外部トラフィックは、内部インターフェイスへのアクセス時に NAT のルールと一致している必要があります（図 21-5 を参照）。

**図 21-5　NAT 制御と着信トラフィック**



NAT 制御がイネーブルの状態でスタティック NAT を使用する場合は、このような制約事項はありません。

デフォルトでは NAT 制御がディセーブルになっているので、NAT を実行する事情が特にない限り、どのネットワークでも NAT を実行する必要はありません。ただし、旧バージョンのソフトウェアからアップグレードした場合は、NAT 制御をシステムでイネーブルにする場合があります。

NAT 制御でセキュリティを強化したいが、内部アドレスを変換したくない場合がいくつかあるときは、NAT 免除ルールまたはアイデンティティ NAT ルールをこれらの内部アドレスに適用できます（詳細については、P.21-37 の「NAT 免除の使用」を参照してください）。

NAT 制御の設定については、P.21-17 の「NAT 制御の設定」を参照してください。

（注）　マルチコンテキスト モードの場合、パケット分類子が NAT の設定に従ってパケットをコンテキストに割り当てる場合があります。NAT 制御がディセーブルなので NAT を実行していない場合、分類子がネットワーク構成の変更を必要とする場合があります。分類子と NAT の関係の詳細については、P.7-3 の「FWSM によるパケットの分類方法」を参照してください。

## NAT のタイプ

この項では、使用可能な NAT タイプについて説明します。アドレス変換は、ダイナミック NAT、Port Address Translation（PAT; ポート アドレス変換）、スタティック NAT、スタティック PAT、またはこれらのタイプの組み合せとして実装できます。また、たとえば NAT 制御をイネーブルにしたが NAT を実行したくない場合などは、NAT をバイパスするよう設定することもできます。この項では、次の項目を取り上げます。



### ダイナミック NAT

ダイナミック NAT では、実際のアドレス グループを、宛先ネットワークでルーティング可能なマッピング済みアドレスのプールに変換します。マッピング済みプールに含まれるアドレスの数は、実際のアドレス グループよりも少ない場合があります。変換するホストが宛先ネットワークにアクセスすると、FWSM がマッピング済みアドレスのプールからそれらに IP アドレスを割り当てます。変換が追加されるのは、実際のホストが接続を開始した場合のみです。変換は接続が確立されている間のみ有効です。また、変換のタイムアウト後にユーザが同じ IP アドレスを維持することはできません（Timeout を参照）。そのため、宛先ネットワークのユーザは、（アクセスリストでその接続が許可されている場合でも）ダイナミック NAT を使用するホストに対しては、信頼できる接続を開始できません。また、実際のホスト アドレスに直接接続しようとすると、FWSM によって拒否されます。ホストへの信頼できるアクセスについては、以降の「スタティック NAT」または「スタティック PAT」の項目を参照してください。

図 21-6 に、実際のアドレスに接続しようとするリモート ホストを示します。FWSM はマッピング済みアドレスへのリターン接続のみを許可しているため、接続は拒否されます。

**図 21-6　実際のアドレスに接続しようとするリモート ホスト**

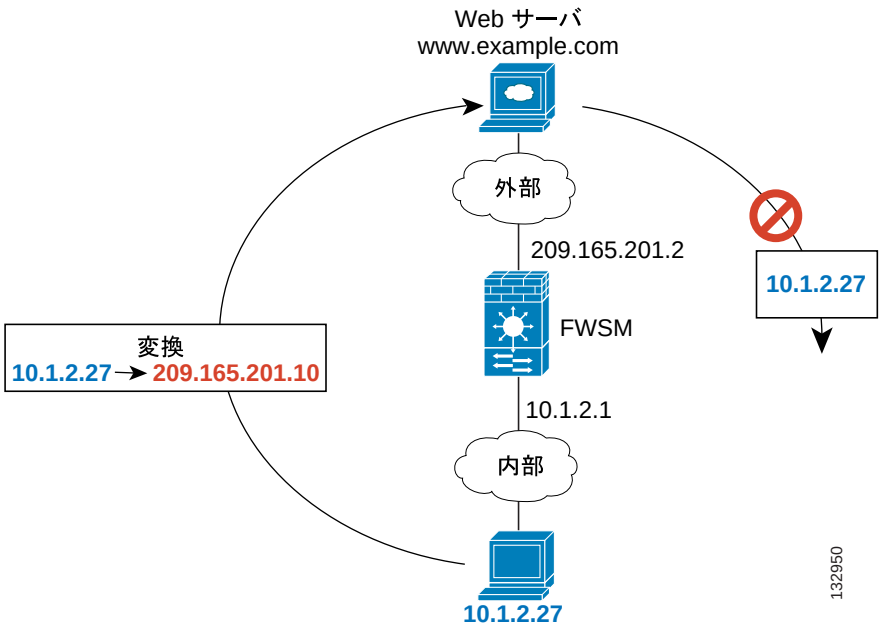
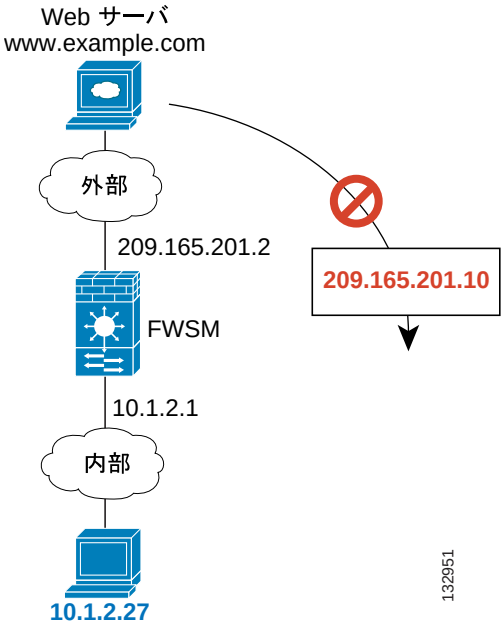



図 21-7 に、マッピング済みアドレスへの接続を開始しようとするリモート ホストを示します。現在、このアドレスは変換テーブルにないので、FWSM がパケットをドロップします。

**図 21-7　マッピング済みアドレスへの接続を開始しようとするリモート ホスト**




（注）　変換が確立されている間、アクセスリストで許可されていれば、リモート　ホストは変換対象ホストへの接続を試みることができます。アドレスを予測できないので、リモートホストが変換対象ホストに接続できる可能性は非常に低くなります。万一、接続が成功した場合でも、アクセスリストのセキュリティに頼ることができます。

ダイナミック NAT には、次の短所があります。

- マッピング済みプールのアドレスが実際のアドレスよりも少ない場合、トラフィック量が予想を超えた場合にアドレスが足りなくなる場合があります。

  このような現象が頻繁に発生した場合は PAT を使用します。PAT では、単一アドレスのポートを使用して 64,000 より多くの変換を実現できます。
- マッピング済みアドレスのプールではルーティング可能なアドレスを多数使用する必要があります。宛先ネットワークでインターネットなどの登録済みアドレスを使用する必要がある場合、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、プロトコルによっては PAT が使用できない場合があることです。たとえば、オーバーロード変換用のポート番号がない IP プロトコル（GRE version 0 など）では、PAT は機能しません。また PAT は、データ ストリームと制御パスが異なるポートに存在する、非オープン スタンダードの一部のアプリケーション（一部のマルチメディア アプリケーションなど）では機能しません。NAT と PAT のサポートの詳細については、P.21-2 の「NAT の概要」を参照してください。

## PAT

PAT は複数の実際のアドレスを単一のマッピング済み IP アドレスに変換します。特に FWSM は、実際のアドレスと送信元ポート（実際のソケット）を、マッピング済みアドレスと 1024 より多くの一意のポート（マッピング済みソケット）に変換します。送信元ポートが接続ごとに異なるため、接続ごとに個別の変換が必要です。たとえば、10.1.1.1:1025 の場合、10.1.1.1:1026 とは別の変換が必要です。

接続がタイムアウトになってから非アクティブ状態が 30 秒間続くと、ポート変換もタイムアウトになります。タイムアウト設定は変更できません。宛先ネットワークのユーザは、（アクセスリストで接続が許可されている場合でも）PAT を使用するホストへの信頼できる接続を開始できません。ホストの実際のポート番号またはマッピング済みポートの番号を予測できないだけでなく、変換対象ホストが開始側ホストでない限り、FWSM は変換をまったく作成しません。ホストへの信頼できるアクセスについては、以降の「スタティック NAT」または「スタティック PAT」の項目を参照してください。

PAT では単一のマッピング済みアドレスを使用できるため、ルーティング可能なアドレスを節約できます。FWSM インターフェイスの IP アドレスを PAT アドレスとして使用することも可能です。PAT は、制御パスとデータ ストリームが異なるポートにある一部のマルチメディア アプリケーションでは機能しません。NAT と PAT のサポートの詳細については、P.21-2 の「NAT の概要」を参照してください。

**（注）** 変換が確立されている間、アクセスリストで許可されていれば、リモート ホストは変換対象ホストへの接続を試みることができます。ポートのアドレス（実際のポートとマッピング済みポートの両方）を予測できないため、リモートホストが変換対象ホストに接続できる可能性は非常に低くなります。万一、接続が成功した場合でも、アクセスリストのセキュリティに頼ることができます。

## スタティック NAT

スタティック NAT では、実際のアドレスからマッピング済みアドレスへの固定変換を行います。ダイナミック NAT および PAT では、ホストは以降の各変換で異なるアドレスまたはポートを使用します。スタティック NAT では、以降の接続でもマッピング済みアドレスは同一で、永続的な変換ルールが存在します。そのため、スタティック NAT では、宛先ネットワークのホストは変換対象ホストへのトラフィックを開始できます（アクセスリストでその接続が許可されている場合）。

ダイナミック NAT とスタティック NAT のアドレス範囲の主な違いは、スタティック NAT では、リモート ホストが変換対象ホストへの接続を開始できます（アクセスリストでその接続が許可されている場合）が、ダイナミック NAT の場合はそれができないという点です。また、スタティック NAT ではマッピング済みアドレスの数と実際のアドレスの数を同じにする必要があります。

## スタティック PAT

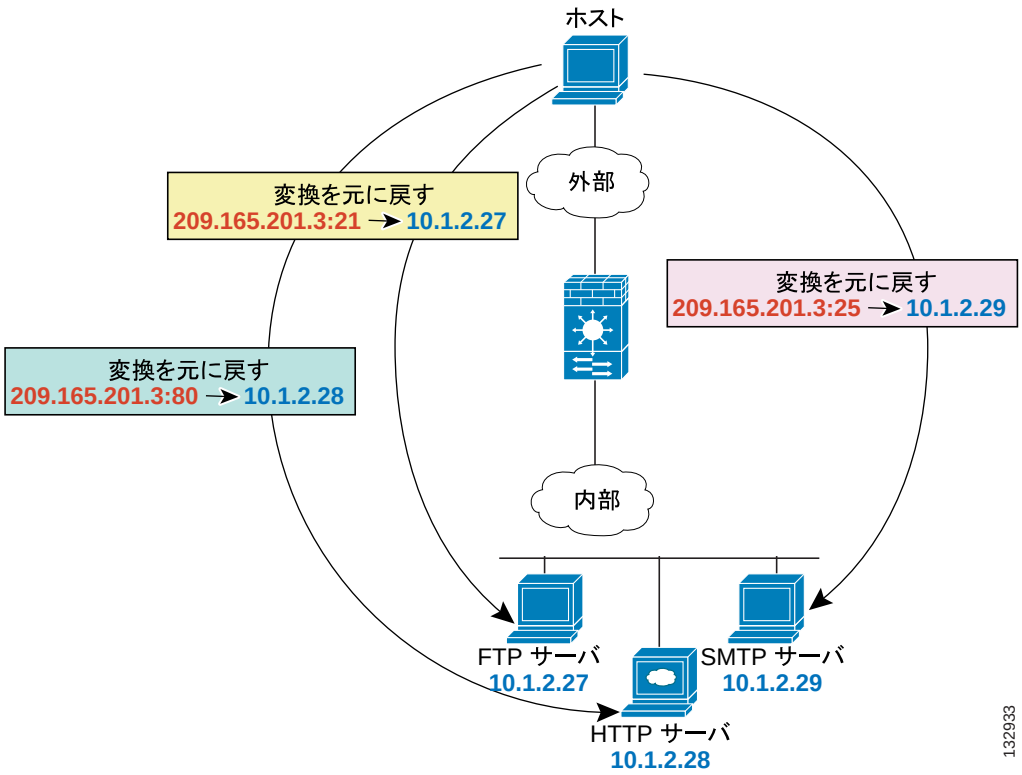
スタティック PAT は、実際のアドレスとマッピング済みアドレスに対してプロトコル（TCP または UDP）とポートを指定できること以外は、スタティック NAT と同じです。

この機能では、文ごとにポートが異なっていれば、多数の異なるスタティック文でマッピング済みアドレスを同じにすることができます（複数のスタティック *NAT* 文に対して同じマッピング済みアドレスを使用することはできません）。

セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、FWSM が自動的にセカンダリ ポートを変換します。

たとえば、FTP、HTTP、SMTP にアクセスするための単一アドレスをリモート ユーザに提供するが、実際のネットワーク上ではこれらが別のサーバである場合、使用するマッピング済みアドレスは同一だがポートは異なる各サーバに対してスタティック PAT 文を指定できます（図21-8 を参照）。

**図 21-8　スタティック PAT**



また、スタティック PAT を使用すると、ウェルノウン ポートと非標準ポートの変換が可能です。たとえば、内部 Web サーバでポート 8080 を使用している場合、外部ユーザにポート 80 への接続を許可してから、変換を元のポート 8080 に戻すことができます。同様に、セキュリティを強化したい場合、非標準のポート 6785 に接続するよう Web ユーザに通知してから、変換を元のポート 80 に戻すことができます。

## NAT 制御がイネーブルの場合の NAT のバイパス

NAT 制御をイネーブルにすると、内部ホストは外部ホストへのアクセス時に NAT のルールと一致している必要があります。一部のホストに NAT を実行したくない場合、それらのホストで NAT をバイパスできます（または、NAT 制御をディセーブルにすることもできます）。たとえば、NAT をサポートしないアプリケーションを使用する場合、NAT をバイパスします（NAT をサポートしない検査エンジンの詳細については、P.21-2 の「NAT の概要」を参照してください）。

次の 3 つのいずれかの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法も検査エンジンとの互換性があります。ただし、それぞれの方法は次のように機能が若干異なります。

- アイデンティティ NAT：（ダイナミック NAT とよく似ている）アイデンティティ NAT を設定する場合、特定インターフェイスのホストに対して変換を制限するのではなく、すべてのインターフェイスの接続でアイデンティティ NAT を使用する必要があります。そのため、インターフェイス A にアクセスする場合は実際のアドレスで通常の変換を実行し、インターフェイス B にアクセスする場合はアイデンティティ NAT を使用するということはできません。一方、通常のダイナミック NAT では、アドレスを変換する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実際のアドレスが、アクセスリストで使用可能なすべてのネットワークでルーティング可能かどうか確認してください。

  アイデンティティ NAT の場合、マッピング済みアドレスが実際のアドレスと同じでも、（インターフェイス アクセスリストで許可されていても）外部から内部には接続を開始できません。外部から内部への接続には、スタティック アイデンティティ NAT または NAT 免除を使用します。
- スタティック アイデンティティ NAT：スタティック アイデンティティ NAT では、実際のアドレスを見せてもよいインターフェイスを指定できるので、インターフェイス A にアクセスする場合はアイデンティティ NAT を使用し、インターフェイス B にアクセスする場合は通常の変換を使用するということができます。また、スタティック アイデンティティ NAT では、ポリシー NAT を使用することもできます。ポリシー NAT では、変換する実際のアドレスを決定する際に、実際のアドレスと宛先アドレスを識別します（ポリシー NAT の詳細については、P.21-11 の「ポリシー NAT」を参照してください）。たとえば、内部アドレスから外部インターフェイスにアクセスするときに、宛先がサーバ A の場合はスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスする場合は通常の変換を使用するということができます。
- NAT 免除：NAT 免除により、変換対象ホストとリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様、ホストの変換を特定のインターフェイスに制限するのではなく、すべてのインターフェイスの接続で NAT 免除を使用する必要があります。ただし、NAT 免除では、（ポリシー NAT と同様）変換する実際のアドレスを決定する際に実際のアドレスと宛先アドレスを指定できるので、NAT 免除を使用すると、より詳細な制御が可能になります。一方、ポリシー NAT とは異なり、NAT 免除ではアクセスリストでポートが考慮されません。

## ポリシー NAT

ポリシー NAT では、拡張アクセスリストで送信元アドレスと宛先アドレスを指定することにより、アドレス変換に使用する実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。たとえば、ポリシー NAT の場合、サーバ A にアクセスする場合は実際のアドレスをマッピング済みアドレス A に変換し、サーバ B にアクセスする場合は実際のアドレスをマッピング済みアドレス B に変換するということができます。

セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、ポリシー NAT 文にセカンダリ ポートを指定する必要があります。ポートを予測できない場合は、ポリシーでセカンダリ チャネルの IP アドレスだけを指定する必要があります。この指定により、FWSM はセカンダリ ポートを変換します。

（注）　NAT 免除以外のすべてのタイプの NAT で、ポリシー NAT がサポートされています。NAT 免除では、アクセスリストを使用して実際のアドレスを識別しますが、ポートを考慮しない点でポリシー NAT とは異なります。その他の違いについては、P.21-37 の「NAT 免除の使用」を参照してください。スタティック アイデンティティ NAT を使用しても、ポリシー NAT をサポートしているので NAT 免除と同じ結果が得られます。

図 21-9 に、2 つの異なるサーバにアクセスする 10.1.2.0/24 というネットワーク上のホストを示します。このホストが 209.165.201.11 のサーバにアクセスすると、実際のアドレスが 209.165.202.129 に変換されます。このホストが 209.165.200.225 のサーバにアクセスすると、実際のアドレスが 209.165.202 130 に変換されます。ホストがサーバと同じネットワーク上にあるように見えるので、ルーティングに役立ちます。

**図 21-9　宛先アドレスが異なるポリシー NAT**

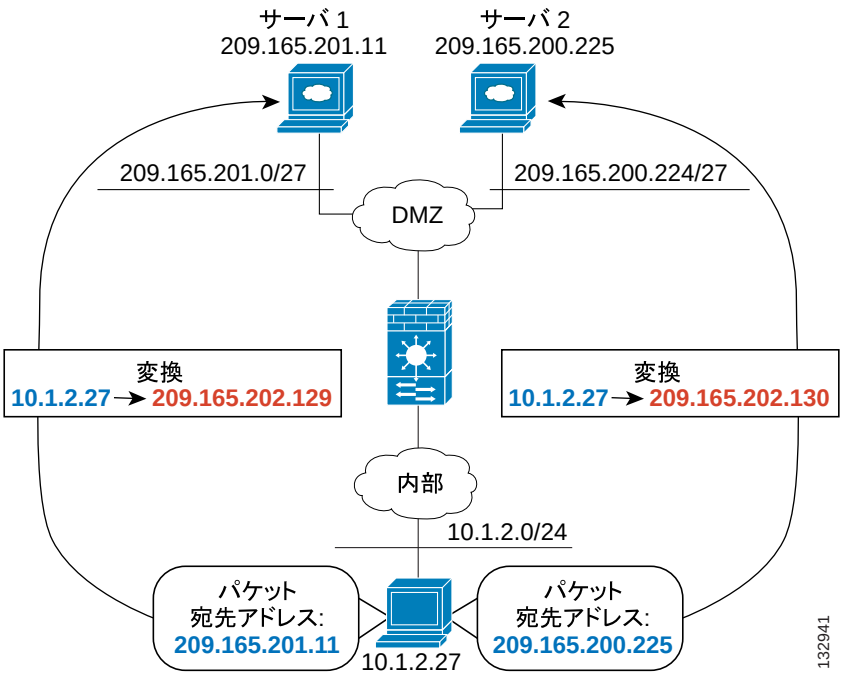
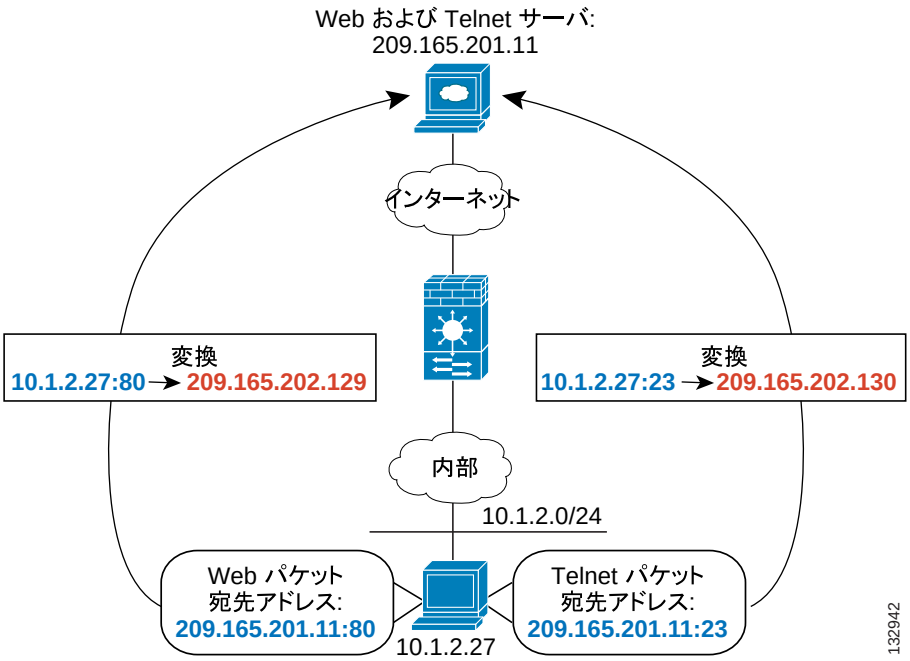


図 21-10 に、送信元と宛先のポートの使用例を示します。10.1.2.0/24 というネットワーク上にあるこのホストは、Web サービスと Telnet サービスの両方で同じホストにアクセスします。このホストが Web サービスのためにサーバにアクセスすると、実際のアドレスが 209.165.202.129 に変換されます。このホストが 同じサーバに Telnet サービスのためにアクセスすると、実際のアドレスが 209.165.202.130 に変換されます。

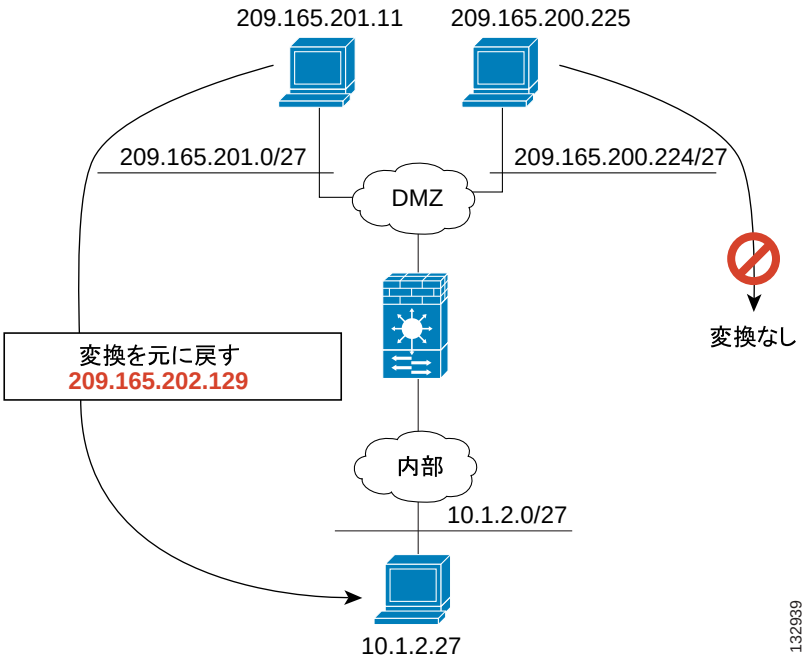
**図 21-10　宛先ポートが異なるポリシー NAT**




ポリシー スタティック NAT（および同様にアクセスリストを使用してトラフィックを識別する NAT 免除）の場合、変換対象ホストとリモート ホストの両方がトラフィックを発信できます。変換対象ネットワークから発信されるトラフィックの場合、NAT のアクセスリストで実際のアドレスと*宛先*アドレスを指定します。一方、リモート ネットワークから発信されるトラフィックの場合、実際のアドレスと、この変換によるホストへの接続が許可されているリモート ホストの*送信元*アドレスをアクセスリストで指定します。

図 21-11 に、変換対象ホストに接続するリモート ホストを示します。この変換対象ホストには、209.165.201.0/27 ネットワークとの送受信トラフィックだけについて、実際のアドレスを変換するポリシー スタティック NAT 変換が設定されています。209.165.200.224/27 ネットワークには、変換が設定されていないので、変換対象ホストはそのネットワークに接続できません。また、そのネットワークのホストも変換対象ホストに接続できません。

図 21-11　宛先アドレス変換を行うポリシー スタティック NAT




（注）　ポリシー NAT では SQL*Net がサポートされていませんが、通常の NAT ではサポートされています。他のプロトコルでの NAT のサポートについては、P.21-2 の「NAT の概要」を参照してください。

## NAT セッション（Xlate）の作成

NAT を使用しない場合でも、デフォルトで FWSM がすべての接続に対して NAT セッションを作成します。たとえば、NAT 制御をイネーブルにしない場合、NAT 免除またはアイデンティティ NAT を使用する場合、またはセキュリティが等位のインターフェイスを使用しており NAT を設定しない場合でも、変換対象でない接続ごとに NAT セッションが作成されます。NAT セッションには最大数があるので（P.A-5 の「管理対象のシステム リソース」を参照）、これらの種類の NAT セッションにより制限に達してしまう場合があります。

このような制限に達するのを回避するために、変換対象でないトラフィックに対する NAT セッションをディセーブルにできます（xlate バイパスと呼ばれます）。xlate バイパスをイネーブルにする方法については、P.21-17 の「xlate バイパスのイネーブル」を参照してください。NAT 制御をディセーブルにして変換対象でないトラフィックを存在させる場合、または NAT 制御をイネーブルにして NAT 免除を使用する場合、xlate バイパスを使用すると、FWSM はこれらの変換対象でないトラフィックに対する NAT セッションを作成しません。ただし、次の場合は NAT セッションが作成されます。

- アイデンティティ NAT を設定する（NAT 制御がイネーブルまたはディセーブルの状態）。アイデンティティ NAT は変換と見なされます。
- NAT 制御でセキュリティが等位のインターフェイスを使用する。等位セキュリティのインターフェイス間のトラフィックの場合、そのトラフィックに対して NAT を設定しなくても NAT セッションが作成されます。このような場合に NAT セッションを回避するには、まず NAT 制御をディセーブルにするか、または NAT 免除を使用します。その上で xlate バイパスを使用します。

## NAT およびセキュリティ レベルが等位のインターフェイス

セキュリティ レベルが等位のインターフェイス間では、NAT 制御をイネーブルにしている場合でも NAT は不要です。任意で NAT を設定することもできますが、必須ではありません。ただし、NAT 制御がイネーブルのときにダイナミック NAT を設定する場合、NAT は必須です。詳細については、P.21-5 の「NAT 制御」を参照してください。また、等位セキュリティのインターフェイスでダイナミック NAT または PAT の IP アドレス グループを指定する場合、そのアドレス グループが等位または下位のセキュリティ レベルのインターフェイスにアクセスする際に、（NAT 制御がイネーブルでない場合でも）そのアドレス グループに対して NAT を実行する必要があります。スタティック NAT として識別されるトラフィックは影響を受けません。

セキュリティが等位の通信をイネーブルにする方法については、P.5-3 の「等位セキュリティ レベル間の通信のイネーブル化」を参照してください。

（注）　FWSM は、等位セキュリティのインターフェイスで NAT を設定する場合の VoIP 検査エンジンをサポートしていません。これらの検査エンジンには Skinny、SIP、H.323 などが含まれます。サポートされる検査エンジンについては、P.21-2 の「NAT の概要」を参照してください。

## 実際のアドレスの照合に使用する NAT ルールの順序

FWSM は、次の順序で実際のアドレスと NAT コマンドを照合します。

1. NAT 免除：最初の一致が見つかるまで順番に照合します。アイデンティティ NAT は、このカテゴリではなく通常のスタティック NAT または通常の NAT のカテゴリに含まれます。NAT 免除文でアドレスが重複すると予想外の結果が発生する場合があるため、お勧めできません。
2. スタティック NAT とスタティック PAT（通常およびポリシー）：最適な一致が見つかるまで照合します。スタティック アイデンティティ NAT はこのカテゴリに含まれます。スタティック ルールでアドレスが重複する場合は警告が表示されますが、サポートされています。スタティック ルールの順序は関係なく、実際のアドレスと最も一致するスタティック ルールが使用されます。
3. ポリシー ダイナミック NAT：最初の一致が見つかるまで順番に照合されます。アドレスの重複は許可されています。
4. 通常のダイナミック NAT：最適な一致が見つかるまで照合されます。通常のアイデンティティ NAT はこのカテゴリに含まれます。NAT コマンドの順序は関係なく、実際のアドレスと最も一致する NAT 文が使用されます。たとえば、あるインターフェイス上のすべてのアドレス（0.0.0.0）を変換する汎用文を作成できます。ユーザ ネットワークのサブセット（10.1.1.1）を別のアドレスに変換する場合、10.1.1.1 のみを変換する文を作成できます。10.1.1.1 の接続が開始されると、10.1.1.1 を指定した文が実際のアドレスと最も一致するので、この文が使用されます。重複文を使用するとメモリの使用量が増えて FWSM のパフォーマンスが低下する場合があるため、お勧めできません。

## NAT 文の最大数

FWSM は、すべてのコンテキスト合計で、またはシングルモードで、次の数の **nat**、**global**、および **static** コマンドをサポートします。

- **nat** コマンド：2 K
- **global** コマンド：4 K
- **static** コマンド：2 K

また FWSM は、ポリシー NAT に使用するアクセスリストには、シングルモードで最大 3942 個、マルチモードで最大 7272 個の ACE をサポートします。

## マッピング済みアドレスのガイドライン

実際のアドレスをマッピング済みアドレスに変換する場合、次のマッピング済みアドレスを使用できます。

- マッピング済みインターフェイスと同じネットワーク上にあるアドレス

  （トラフィックが FWSM から発信されるときに通過する）マッピング済みインターフェイスと同じネットワーク上にあるアドレスを使用すると、FWSM はプロキシ ARP を使用してマッピング済みアドレスへの要求に応答するので、実際のアドレス宛のトラフィックを代行受信します。同じネットワーク上のアドレスを使用すると、FWSM が追加ネットワークのゲートウェイである必要がないので、ルーティングが簡略化されます。ただし、同じネットワーク上のアドレスを使用すると、変換に使用できるアドレス数が制限されます。

  PAT の場合、マッピング済みインターフェイスの IP アドレスも使用できます。

- 一意のネットワーク上にあるアドレス

  マッピング済みインターフェイス のネットワークで使用できる数よりも多くのアドレスが必要な場合、別のサブネットにあるアドレスを指定できます。FWSM は、プロキシ ARP を使用してマッピング済みアドレスの要求に応答するので、実際のアドレス宛のトラフィックを代行受信します。OSPF を使用してマッピング済みインターフェイスのルートをアドバタイズする場合、FWSM はマッピング済みアドレスをアドバタイズします。マッピング済みインターフェイスがパッシブの場合（ルートをアドバタイズしない場合）、またはスタティック ルーティングを使用する場合、マッピング済みアドレス宛のトラフィックを FWSM に送信するスタティック ルートをアップストリーム ルータで追加する必要があります。

## DNS と NAT

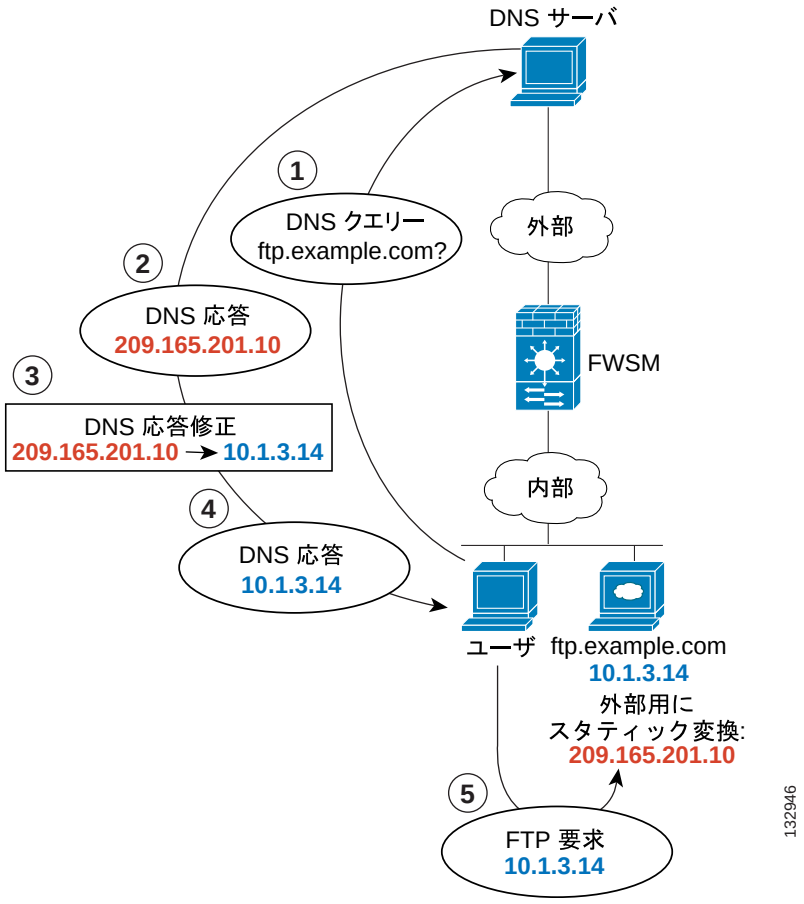
DNS 応答の修正を行うよう FWSM を設定する必要がある場合があります。修正では、NAT コンフィギュレーションと一致するアドレスに DNS 応答内のアドレスが置換されます。DNS の修正は、各変換の設定時に設定できます。

たとえば、DNS サーバに外部インターフェイスからアクセスできるとします。サーバ ftp.example.com は内部インターフェイスに接続されているとします。ftp.example.com の実際のアドレス（10.1.3.14）を、外部ネットワークから見えるマッピング済みアドレス（209.165.201.10）へスタティックに変換するように FWSM を設定できます（図 21-12 を参照）。この場合、このスタティック文で DNS 応答の修正をイネーブルにできます。DNS 応答の修正をイネーブルにすると、実際のアドレスを使用して ftp.example.com にアクセスする内部ユーザが、DNS サーバからマッピング済みアドレスではなく実際のアドレスを受信できるようになります。

内部ホストが ftp.example.com のアドレスに対して DNS 要求を送信すると、DNS サーバはマッピング済みアドレス（209.165.201.10）で応答します。FWSM は内部サーバのスタティック文を参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答の修正をイネーブルにしないと、内部ホストは ftp.example.com へ直接アクセスせずに、トラフィックを 209.165.201.10 へ送信しようとします。

（注）　DNS クエリーの応答内に記述されている実際の IP アドレスへのルートが存在している必要があります。存在しない場合、FWSM はその IP アドレスへの NAT を実行しません。必要なルートは、スタティック ルーティングまたは RIP や OSPF など他のルーティング プロトコルからラーニングできます。

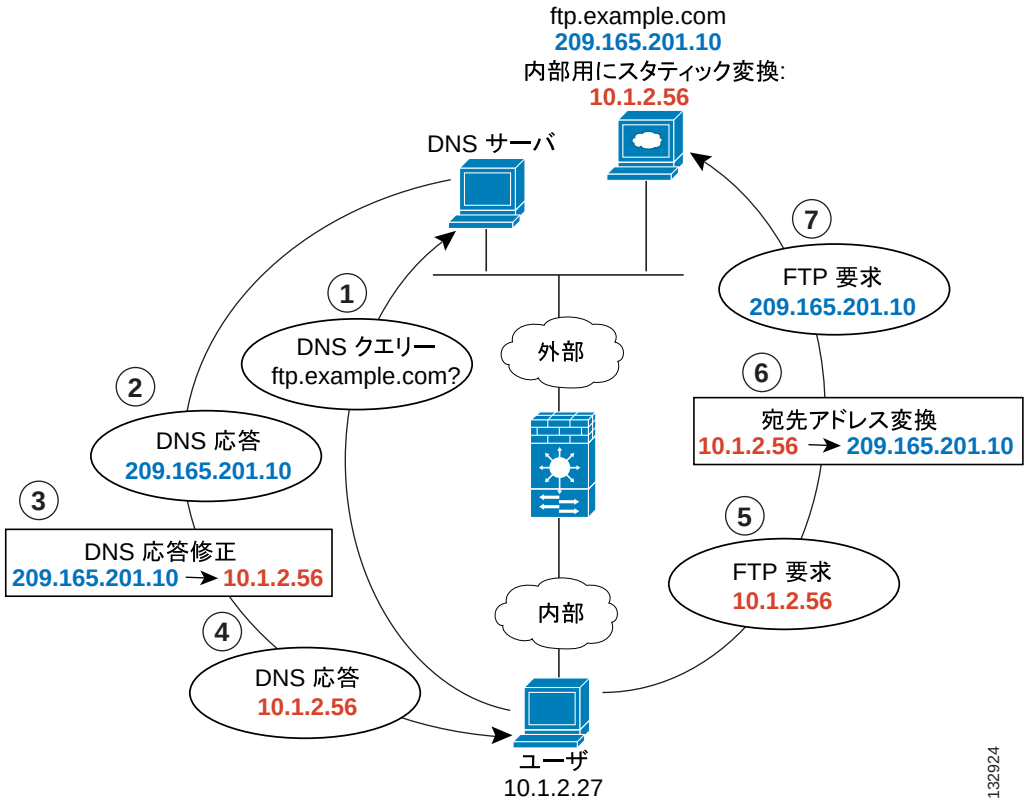
図 21-12　DNS 応答の変更




（注）　別のネットワーク（DMZ など）上のユーザが外部の DNS サーバに ftp.example.com の IP アドレスを要求した場合も、**static** コマンドで参照した内部インターフェイスにそのユーザが接続されていなくても、DNS 応答内の IP アドレスがそのユーザ用に変更されます。

図 21-13 に、外部の Web サーバと DNS サーバを示します。FWSM には外部サーバのスタティック変換があります。この場合、内部ユーザが DNS サーバから ftp.example.com のアドレスを要求すると、DNS サーバは実際のアドレス 209.165.201.10 で応答します。内部ユーザに ftp.example.com のマッピング済みアドレス（10.1.2.56）を使用させたい場合、そのスタティック変換用の DNS 応答の修正を設定する必要があります。

図 21-13　外部 NAT を使用した DNS 応答の修正




# NAT 制御の設定

NAT 制御では、内部インターフェイスから外部インターフェイスへ通過するパケットが NAT のルールと一致している必要があります。詳細については、P.21-5 の「NAT 制御」を参照してください。

NAT 制御をイネーブルにするには、Configuration > Firewall > NAT Rules ペインで **Enable traffic through the firewall without address translation** チェックボックスをオンにします。

# xlate バイパスのイネーブル

デフォルトでは、NAT を使用しない場合でも、FWSM がすべての接続に対して NAT セッションを作成します。詳細については、P.21-13 の「NAT セッション（Xlate）の作成」を参照してください。

xlate バイパスをイネーブルにするには、Configuration > Firewall > NAT Rules ペインで **Enable Xlate-bypass** チェックボックスをオンにします。

# ダイナミック NAT の使用

この項では、ダイナミック NAT、ダイナミック PAT、ダイナミック ポリシー NAT/PAT、およびアイデンティティ NAT の設定方法について説明します。

ポリシー NAT では、送信元アドレスと宛先アドレスを指定することにより、アドレス変換を行う実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。詳細については、P.21-11 の「ポリシー NAT」を参照してください。

ここでは、次の項目について説明します。



## ダイナミック NAT の実装

この項では、ダイナミック NAT の実装方法について説明します。次の項目を取り上げます。



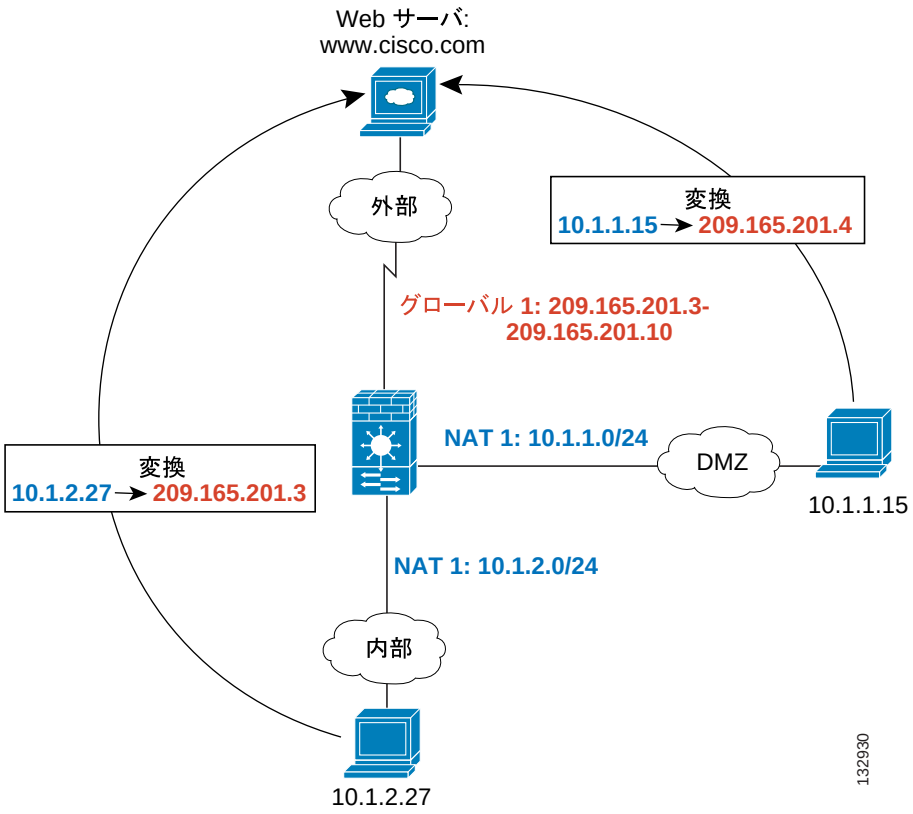
### プール ID による実際のアドレスとグローバル プールの組み合せ

ダイナミック NAT ルールでは、実際のアドレスを指定してから、それを複数のアドレスから成るグローバル プールと組み合せます（ただし、PAT の場合は 1 つのアドレスを組み合わせに指定し、アイデンティティ NAT の場合は実際のアドレスと同一のアドレスを組み合わせに指定します）。実際のアドレスのトラフィックが別のインターフェイスから出るときに、組み合せに指定されたグローバル プールのアドレスに実際のアドレスがマッピングされます。各グローバル プールには個別のプール ID が割り当てられます。

## 同一グローバル プールによる複数インターフェイス上の NAT ルール

同じグローバル アドレス プールを使用して、インターフェイスごとに NAT ルールを作成できます。たとえば、外部インターフェイスのグローバル プール 1 を使用して、内部インターフェイスと DMZ インターフェイスに NAT ルールを設定できます。内部インターフェイスと DMZ インターフェイスのトラフィックは、外部インターフェイスを出るときに、マッピング済みプールまたは PAT アドレスを共有します（図 21-14 を参照）。

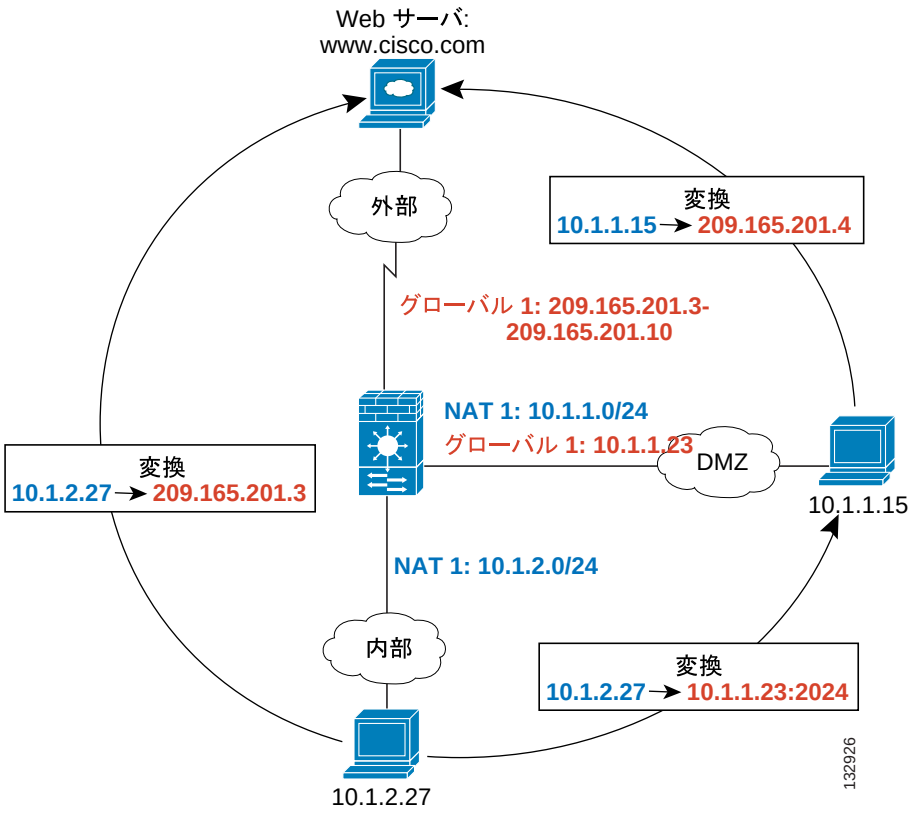
**図 21-14　同一グローバル プールを使用する複数インターフェイス上の NAT ルール**



## 同一プール ID による異なるインターフェイス上のグローバル プール

同じプール ID を使用するグローバル プールを各インターフェイスに作成できます。外部インターフェイスと DMZ インターフェイスに ID 1 のグローバル プールを作成すると、ID 1 に関連付けられた単一の NAT ルールにより、トラフィックが外部インターフェイスと DMZ インターフェイスへ向かう際に、変換されるトラフィックが識別されます。同様に、DMZ インターフェイスに対する ID 1 の NAT ルールを作成すると、ID 1 のすべてのグローバル プールが DMZ のトラフィックに使用されます（図 21-15 を参照）。

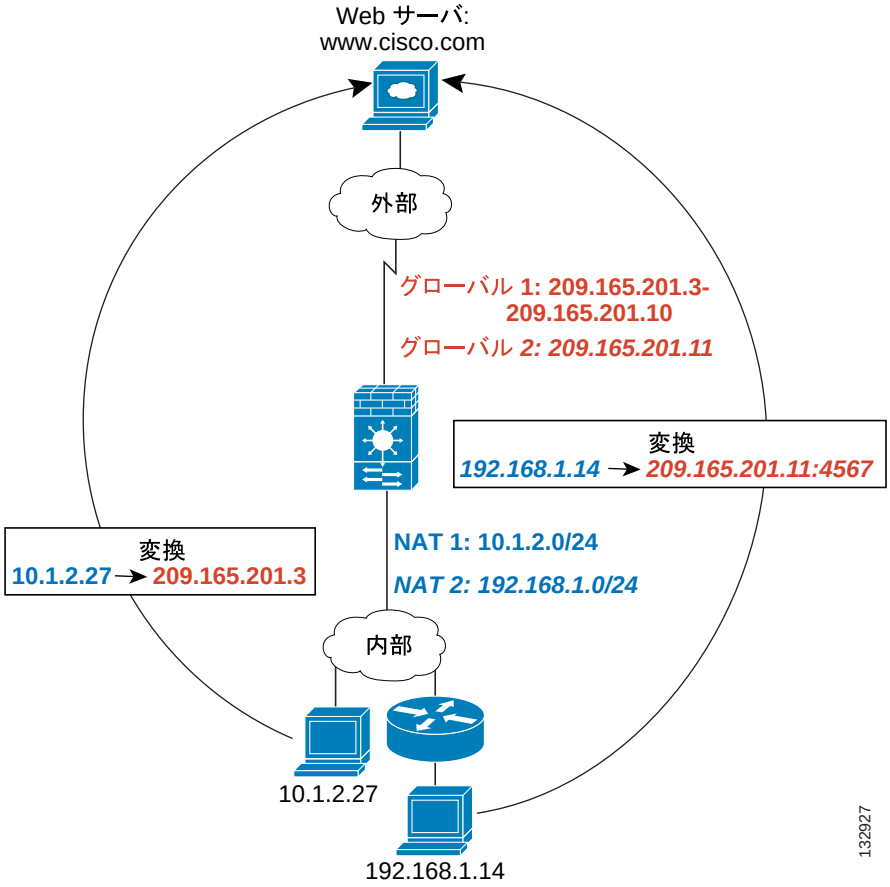
**図 21-15　複数のインターフェイスで同じ ID を使用する NAT ルールとグローバル プール**



## 同一インターフェイス上の異なるグローバル プールによる複数の NAT ルール

実際のアドレスの複数のグループを区別して、別々のマッピング済みアドレスを指定できます。たとえば、内部インターフェイスで、2 つの異なるプール ID で 2 つの NAT ルールを指定できます。外部インターフェイスでは、これら 2 つの ID に対してグローバル プールを 2 つ設定します。次に、内部ネットワーク A のトラフィックが外部インターフェイスを出る場合、IP アドレスはプール 1 のアドレスに変換されます。一方、内部ネットワーク B のトラフィックは、プール 2 のアドレスに変換されます（図 21-16 を参照）。ポリシー NAT を使用する場合、宛先アドレスおよびポートがアクセスリストごとに一意であれば、複数の NAT ルールに対して同じ実際のアドレスを指定できます。

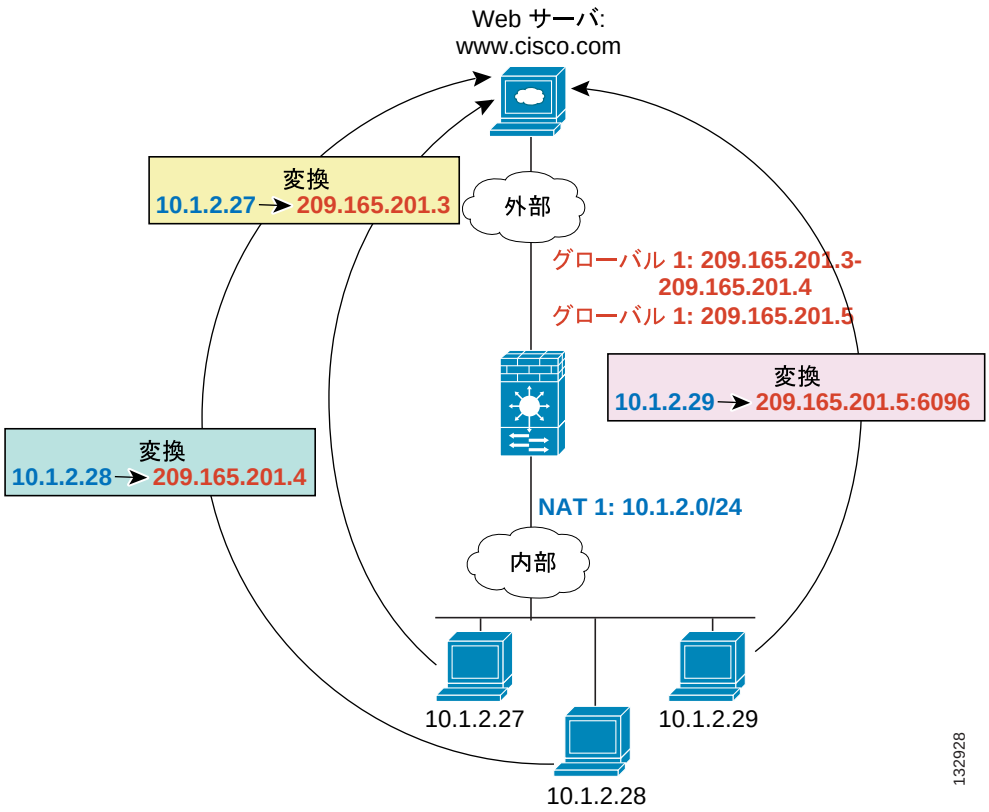
**図 21-16　異なる NAT ID**



## 同一グローバル プールの複数のアドレス

同一のグローバル プールで複数のアドレスを指定できます。FWSM は、設定されている順序でダイナミック NAT の範囲内のアドレスを使用してから、PAT の単一アドレスを順番に使用します。たとえば、特定のアプリケーションでダイナミック NAT を使用する必要があるが、ダイナミック NAT のアドレスが不足した場合に備えてバックアップ PAT ルールを用意したい場合、アドレス範囲と PAT アドレスの両方を追加できます。同様に、1 つの PAT マッピング済みアドレスでサポートされる約 64,000 の PAT セッションよりも多くのアドレスが必要な場合は、プールで 2 つの PAT アドレスを使用できます（図 21-17 を参照）。

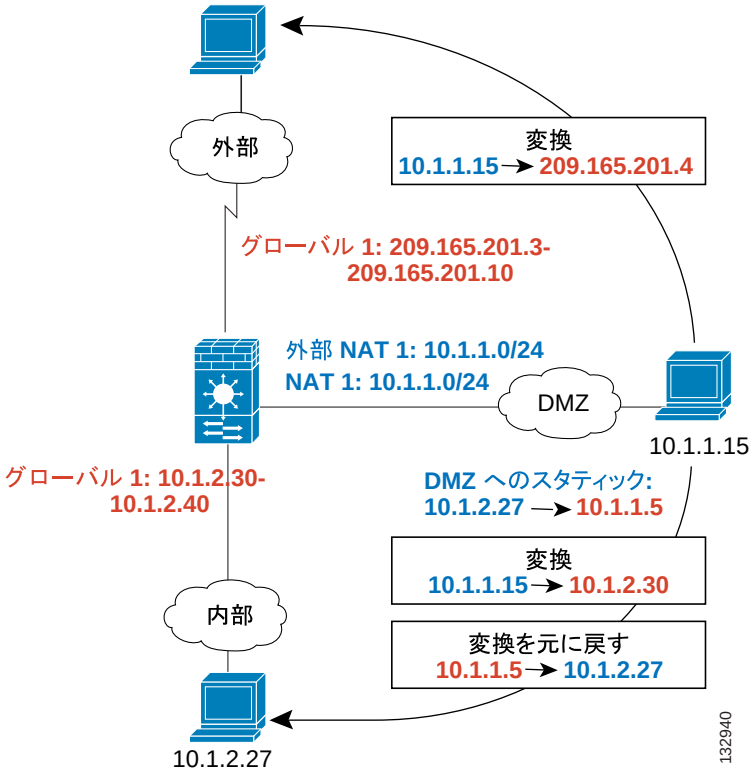
**図 21-17　NAT と PAT の併用**



## 外部 NAT

NAT ルールにより外部インターフェイスから内部インターフェイスにアドレスを変換する場合、そのルールは外部 NAT となるので、着信トラフィックを変換するように指定する必要があります。また、下位のセキュリティ インターフェイスにアクセスする際にも同じトラフィックを変換する場合（たとえば、内部インターフェイスと外部インターフェイスにアクセスする際に DMZ のトラフィックが変換される場合）、同じ NAT ID を使用する 2 番目の NAT ルールを作成できますが（図 21-18 を参照）、発信であることを指定する必要があります。外部 NAT（DMZ インターフェイスから内部インターフェイス）の場合、内部ホストはスタティック ルールを使用して外部アクセスを許可するため、送信元と宛先の両方のアドレスが変換されます。

**図 21-18　外部 NAT と内部 NAT の組み合せ**




## NAT ルールの実際のアドレスをすべての下位または等位のセキュリティ インターフェイス上で変換する必要性

IP アドレス グループに対して NAT ルールを作成する場合、下位または等位のセキュリティ レベルのインターフェイスにアクセスする際にそのアドレス グループに NAT を実行する必要があります。同じプール ID を持つグローバル プールを各インターフェイスに作成するか、またはスタティック ルールを使用する必要があります。上位のセキュリティ インターフェイスにアクセスする場合は、NAT は不要です。外部 NAT ルールを作成すると、すべての上位セキュリティ インターフェイスにアクセスする際に、そのアドレス グループに対する前述の NAT の条件が適用されます。スタティック ルールにより識別されるトラフィックは影響を受けません。

## グローバル プールの管理

ダイナミック NAT では、グローバル プールを使用して変換を行います。グローバル プールの仕組みについては、P.21-18 の「ダイナミック NAT の実装」を参照してください。

グローバル プールを管理するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > Objects > Global Pools ペインで **Add** をクリックして新しいプールを追加するか、またはプールを選択してから **Edit** をクリックします。

また、**Manage** ボタンをクリックすると、Add/Edit Dynamic NAT Rule ダイアログボックスからもグローバル プールを管理できます。

Add/Edit Global Address Pool ダイアログボックスが表示されます。

**ステップ 2**　新規プールの場合、Interface ドロップダウン リストからマッピング済み IP アドレスを使用するインターフェイスを選択します。

**ステップ 3**　新規プールの場合、Pool ID フィールドに 1 ～ 2147483647 の数値を入力します。使用中のプール ID を入力すると、コンフィギュレーションが拒否されます。

**ステップ 4**　IP Addresses to Add 領域で、**Range**、**Port Address Translation (PAT)**、または **PAT Address Translation (PAT) Using IP Address of the interface** をクリックします。

アドレスの範囲を指定すると、FWSM はダイナミック NAT を実行します。Netmask フィールドでサブネット マスクを指定すると、その値により、ホストに割り当てられる際にマッピング済みアドレスに割り当てられるサブネット マスクが決まります。マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

**ステップ 5**　Addresses Pool ウィンドウにアドレスを追加するには、**Add** をクリックします。

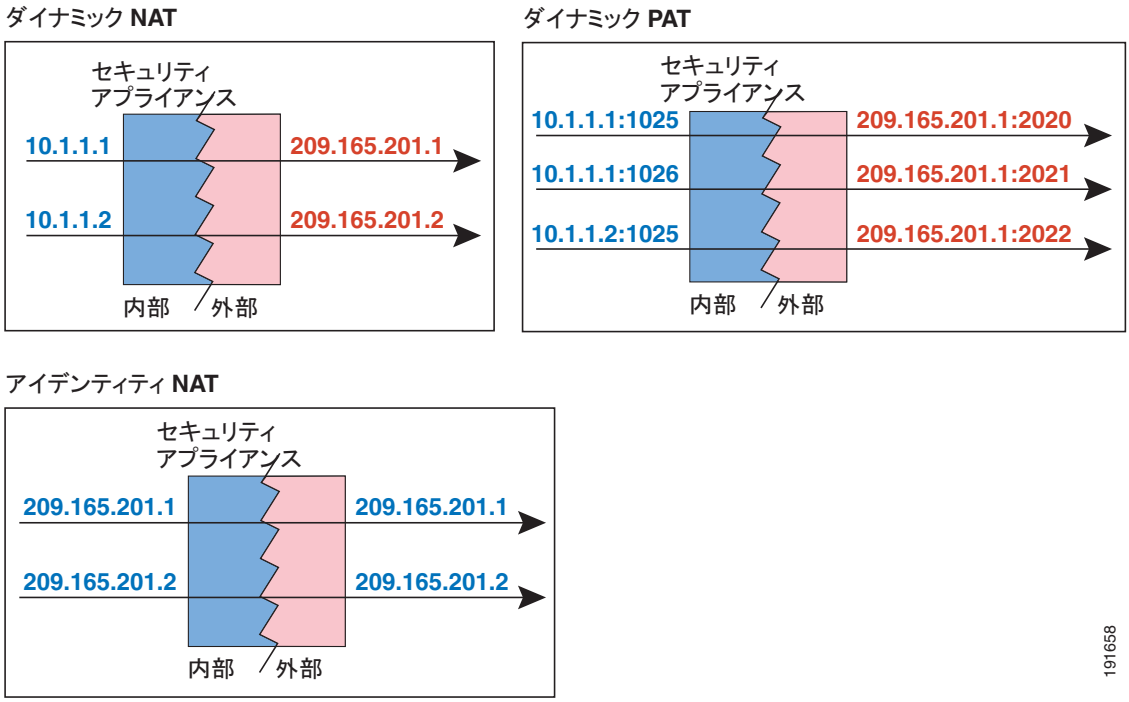
**ステップ 6**　（オプション）複数のアドレスをグローバル プールに追加できます。たとえば、ダイナミックな範囲を設定した後に PAT アドレスを追加する場合、PAT の値を入力してから再度 **Add** をクリックします。インターフェイスで同じプール ID のアドレスを複数使用する方法については、P.21-22 の「同一グローバル プールの複数のアドレス」を参照してください。

**ステップ 7**　**OK** をクリックします。

# ダイナミック NAT、PAT、またはアイデンティティ NAT の設定

図 21-19 に、一般的なダイナミック NAT、ダイナミック PAT、およびアイデンティティ NAT のシナリオを示します。接続を開始できるのは実際のホストのみです。

**図 21-19　ダイナミック NAT のシナリオ**




ダイナミック NAT、ダイナミック PAT、またはアイデンティティ NAT のルールを設定するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > NAT Rules ペインで **Add > Add Dynamic NAT Rule** を選択します。

Add Dynamic NAT Rule ダイアログボックスが表示されます。

**ステップ 2**　Original 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続されるインターフェイスを選択します。

**ステップ 3**　Source フィールドに実際のアドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

**ステップ 4**　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- 定義済みのグローバル プールを選択します。

プールにアドレスの範囲を含めると、FWSM はダイナミック NAT を実行します。プールに単一のアドレスを含めると、FWSM はダイナミック PAT を実行します。プールに範囲と単一アドレスの両方を含めると、範囲が順番に使用されてから PAT アドレスが順番に使用されます。詳細については、P.21-22 の「同一グローバル プールの複数のアドレス」を参照してください。

プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有している場合、それらはグループ化されます。複数のインターフェイスにかかるプール ID を選択すると、トラフィックは、プール内のインターフェイスにアクセスする際に指定どおりに変換されます。プール ID の詳細については、P.21-18 の「ダイナミック NAT の実装」を参照してください。

- 新しいグローバル プールを作成、または既存のプールを編集するには、**Manage** をクリックします。P.21-24 の「グローバル プールの管理」を参照してください。
- アイデンティティ NAT を選択するには、プール 0 を選択します。

**ステップ 5**　（オプション）DNS 応答内のアドレス変換をイネーブルにするには、**Connection Settings** 領域をクリックして開き、**Translate the DNS replies that match the translation rule** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。通常、他のインターフェイスからのアクセスを許可する必要があるホストではスタティック変換を使用するため、このオプションはスタティック ルールで使用する場合が多くなります。詳細については、P.21-15 の「DNS と NAT」を参照してください。

**ステップ 6**　（オプション）接続の設定をイネーブルにするには、**Connection Settings** 領域をクリックして開き、次のいずれかのオプション（複数可）を設定します。

**（注）**　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

- **Randomize sequence number**：このチェックボックスをオンにすると（デフォルト）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  - 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
  - FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。

— FWSM が接続のシーケンス番号をランダム化しないようにする必要がある WAAS デバイスを使用する場合。

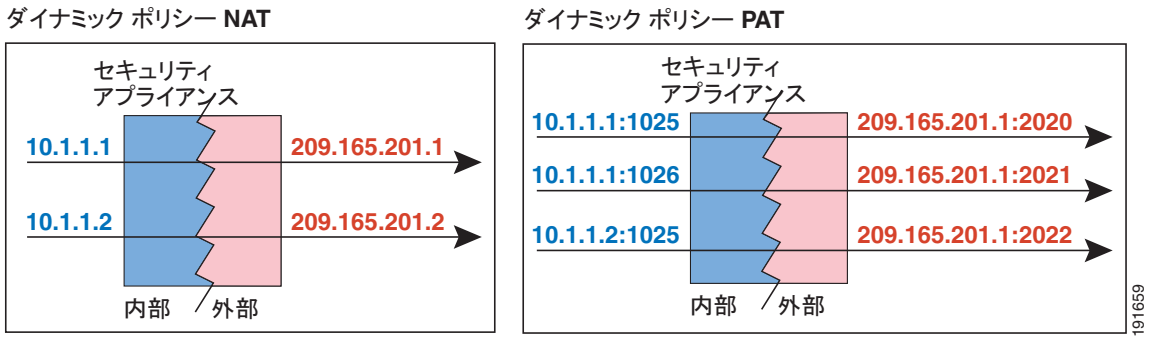
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、クライアントからセキュリティ レベルのより高いサーバへ送信される TCP SYN パケットが TCP 代行受信機能によって代行受信されます。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

**ステップ 7**　**OK** をクリックします。

## ダイナミック ポリシー NAT または PAT の設定

図 21-20 に、一般的なダイナミック ポリシー NAT と PAT のシナリオを示します。接続を開始できるのは実際のホストのみです。

**図 21-20　ダイナミック ポリシー NAT のシナリオ**




ダイナミック ポリシー NAT または PAT を設定するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > NAT Rules ペインで **Add > Advanced > Add Dynamic Policy NAT Rule** を選択します。

Add Dynamic Policy NAT Rule ダイアログボックスが表示されます。

**ステップ 2**　Original 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続されるインターフェイスを選択します。

**ステップ 3**　Source フィールドに実際のアドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の実際のアドレスはカンマで区切ります。

**ステップ 4**　Destination フィールドに宛先アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、このフィールドには任意の宛先アドレスを許可する **any** が表示されています。

**ステップ 5**　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- 定義済みのグローバル プールを選択します。

  プールにアドレスの範囲を含めると、FWSM はダイナミック NAT を実行します。プールに単一のアドレスを含めると、FWSM はダイナミック PAT を実行します。プールに範囲と単一アドレスの両方を含めると、範囲が順番に使用されてから PAT アドレスが順番に使用されます。詳細については、P.21-22 の「同一グローバル プールの複数のアドレス」を参照してください。

  プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有している場合、それらはグループ化されます。複数のインターフェイスにかかるプール ID を選択すると、トラフィックは、プール内のインターフェイスにアクセスする際に指定どおりに変換されます。プール ID の詳細については、P.21-18 の「ダイナミック NAT の実装」を参照してください。
- 新しいグローバル プールを作成、または既存のプールを編集するには、**Manage** をクリックします。P.21-24 の「グローバル プールの管理」を参照してください。
- アイデンティティ NAT を選択するには、プール 0 を選択します。

**ステップ 6**　（オプション）Description フィールドに説明を入力します。

**ステップ 7**　（オプション）DNS 応答内のアドレス変換をイネーブルにするには、**Connection Settings** 領域をクリックして開き、**Translate the DNS replies that match the translation rule** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。通常、他のインターフェイスからのアクセスを許可する必要があるホストではスタティック変換を使用するため、このオプションはスタティック ルールで使用する場合が多くなります。詳細については、P.21-15 の「DNS と NAT」を参照してください。

**ステップ 8**　（オプション）接続の設定をイネーブルにするには、**Connection Settings** 領域をクリックして開き、次のいずれかのオプション（複数可）を設定します。

**（注）**　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

- **Randomize sequence number**：このチェックボックスをオンにすると（デフォルト）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  - 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
  - FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
  - FWSM が接続のシーケンス番号をランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、クライアントからセキュリティ レベルのより高いサーバへ送信される TCP SYN パケットが TCP 代行受信機能によって代行受信されます。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

**ステップ 9**　**OK** をクリックします。

# スタティック NAT の使用

この項では、通常またはポリシー スタティック NAT、PAT、またはアイデンティティ NAT を使用するスタティック変換の設定方法について説明します。

スタティック NAT の詳細については、P.21-8 の「スタティック NAT」を参照してください。

ポリシー NAT では、送信元アドレスと宛先アドレスを指定することにより、アドレス変換に使用する実際のアドレスを識別します。また、送信元ポートと宛先ポートを指定することもできます。通常の NAT で考慮されるのは送信元アドレスのみで、宛先アドレスは考慮されません。詳細については、P.21-11 の「ポリシー NAT」を参照してください。

スタティック PAT では、実際の IP アドレスをマッピング済み IP アドレスに変換し、実際のポートをマッピング済みポートに変換します。実際のポートを同じポートに変換することもできます。この場合、指定した種類のトラフィックのみを変換するか、別のポートに変換することでさらに変換を実行することもできます。セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査が必要なアプリケーションの場合、FWSM が自動的にセカンダリ ポートを変換します。スタティック PAT の詳細については、P.21-9 の「スタティック PAT」を参照してください。

スタティック PAT を使用している場合を除き、同じ 2 つのインターフェイス間で複数のスタティック ルールに同一の実際のアドレスまたはマッピング済みアドレスを使用することはできません。同じマッピング済みインターフェイスのグローバル プールで定義されているマッピング済みアドレスをスタティック ルールに使用しないでください。

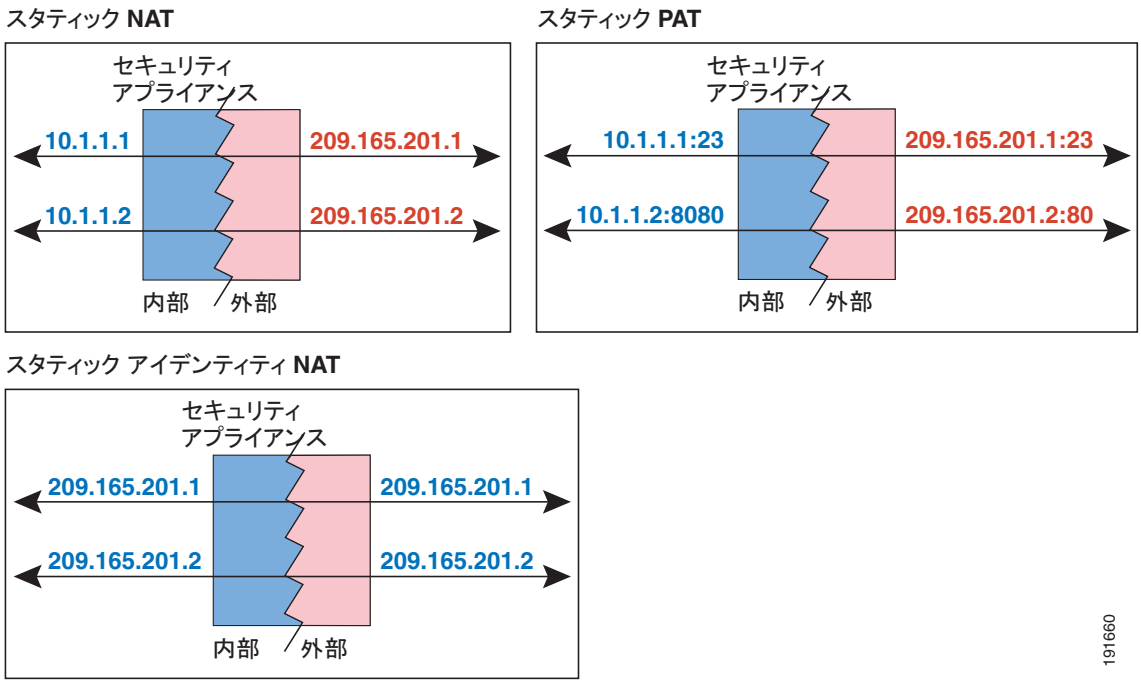
スタティック アイデンティティ NAT は、実際の IP アドレスを同じ IP アドレスに変換します。

ここでは、次の項目について説明します。

# スタティック NAT、PAT、またはアイデンティティ NAT の設定

図 21-21 に、一般的なスタティック NAT、スタティック PAT、およびスタティック アイデンティティ NAT のシナリオを示します。変換は常にアクティブなので、変換対象ホストとリモート ホストの両方が接続を開始できます。

**図 21-21　スタティック NAT のシナリオ**




スタティック NAT、スタティック PAT、またはアイデンティティ NAT を設定するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > NAT Rules ペインで **Add > Add Static NAT Rule** を選択します。

Add Static NAT Rule ダイアログボックスが表示されます。

**ステップ 2**　Original 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続されるインターフェイスを選択します。

**ステップ 3**　Source フィールドに実際のアドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

**ステップ 4**　Translated 領域の Interface ドロップダウン リストから、マッピング済みアドレスを使用するインターフェイスを選択します。

**ステップ 5**　次のいずれかをクリックしてマッピング済み IP アドレスを指定します。

- **Use IP Address**

  IP アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

  10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

- **Use Interface IP Address**

実際のアドレスとマッピング済みアドレスのサブネット マスクが同じでなければなりません。

**（注）**　アイデンティティ NAT の場合、Original フィールドと Translated フィールドに同じ IP アドレスを入力します。

**ステップ 6**　（オプション）スタティック PAT を使用する場合、**Enable Port Address Translation (PAT)** チェックボックスをオンにします。

**a.**　Protocol で **TCP** または **UDP** をクリックします。

**b.**　Original Port フィールドに実際のポート番号を入力します。

**c.**　Translated Port フィールドにマッピング済みポート番号を入力します。

**ステップ 7**　（オプション）DNS 応答内のアドレス変換をイネーブルにするには、**Connection Settings** 領域をクリックして開き、**Translate the DNS replies that match the translation rule** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。詳細については、P.21-15 の「DNS と NAT」を参照してください。

**ステップ 8**　（オプション）接続の設定をイネーブルにするには、**Connection Settings** 領域をクリックして開き、次のいずれかのオプション（複数可）を設定します。

**（注）**　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

- **Randomize sequence number**：このチェックボックスをオンにすると（デフォルト）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

- 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
- FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
- FWSM が接続のシーケンス番号をランダム化しないようにする必要がある WAAS デバイスを使用する場合。

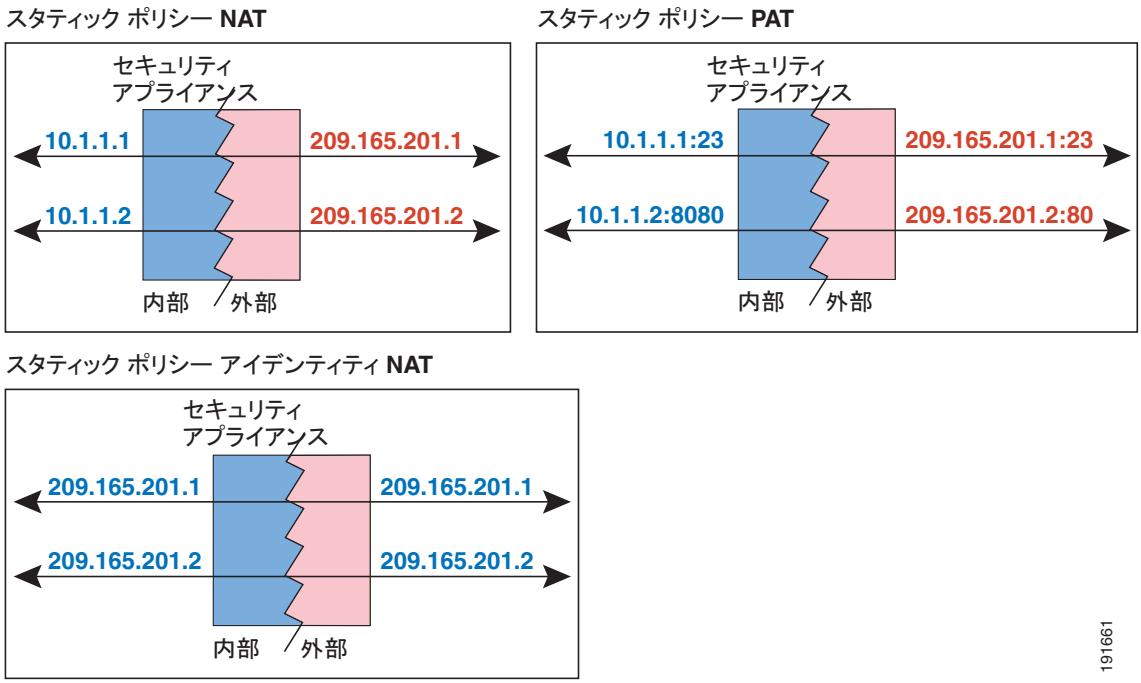
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、クライアントからセキュリティ レベルのより高いサーバへ送信される TCP SYN パケットが TCP 代行受信機能によって代行受信されます。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

**ステップ 9**　**OK** をクリックします。

# スタティック ポリシー NAT、PAT、またはアイデンティティ NAT の設定

図 21-22 に、一般的なスタティック ポリシー NAT、スタティック ポリシー PAT、およびスタティック ポリシー アイデンティティ NAT のシナリオを示します。変換は常にアクティブなので、変換対象ホストとリモート ホストの両方が接続を開始できます。

**図 21-22　スタティック ポリシー NAT のシナリオ**




スタティック ポリシー NAT、スタティック ポリシー PAT、またはアイデンティティ NAT を設定するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > NAT Rules ペインで **Add > Advanced > Add Static Policy NAT Rule** を選択します。

Add Static Policy NAT Rule ダイアログボックスが表示されます。

**ステップ 2**　Original 領域の Interface ドロップダウン リストから、変換する実際のアドレスを持つホストに接続されるインターフェイスを選択します。

**ステップ 3**　Source フィールドに実際のアドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

**ステップ 4**　Destination フィールドに宛先アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、このフィールドには任意の宛先アドレスを許可する **any** が表示されています。

**ステップ 5**　Translated 領域で、Interface ドロップダウン リストからマッピング済みアドレスを使用するインターフェイスを選択します。

**ステップ 6**　次のいずれかをクリックしてマッピング済み IP アドレスを指定します。

- **Use IP Address**

  IP アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

  10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。
- **Use Interface IP Address**

実際のアドレスとマッピング済みアドレスのサブネット マスクが同じでなければなりません。

**ステップ 7**　（オプション）スタティック PAT を使用する場合、**Enable Port Address Translation (PAT)** チェックボックスをオンにします。

**a.**　Protocol で **TCP** または **UDP** をクリックします。

**b.**　Original Port フィールドに実際のポート番号を入力します。

**c.**　Translated Port フィールドにマッピング済みポート番号を入力します。

**ステップ 8**　（オプション）Description フィールドに説明を入力します。

**ステップ 9**　（オプション）DNS 応答内のアドレス変換をイネーブルにするには、**Connection Settings** 領域をクリックして開き、**Translate the DNS replies that match the translation rule** チェックボックスをオンにします。

DNS サーバにエントリがあるホストの実際のアドレスを NAT ルールに指定するが、DNS サーバはクライアントとは別のインターフェイスにある場合、クライアントと DNS サーバではホストのアドレスとして別々のアドレスが必要となります。クライアントではマッピング済みアドレスが必要で、DNS サーバでは実際のアドレスが必要です。このオプションをイネーブルにすると、クライアントへの DNS 応答内のアドレスが修正されます。マッピング済みホストは、クライアントか DNS サーバのどちらかと同じインターフェイスになければなりません。詳細については、P.21-15 の「DNS と NAT」を参照してください。

**ステップ 10**　（オプション）接続の設定をイネーブルにするには、**Connection Settings** 領域をクリックして開き、次のいずれかのオプション（複数可）を設定します。

（注）　セキュリティ ポリシー ルールを使用してこれらの値の一部を設定することもできます（P.23-3 の「Connection Settings（透過モードのみ）」を参照）。両方で値の設定を行うと、FWSM は小さい値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

- **Randomize sequence number**：このチェックボックスをオンにすると（デフォルト）、FWSM は TCP パケットのシーケンス番号をランダム化します。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。FWSM は、発信方向と着信方向の両方を通過する TCP SYN の ISN をランダム化します。

  保護されたホストの ISN をランダム化すると、攻撃者が新しい接続の次の ISN を予測できなくなり、新しいセッションを乗っ取ることができなくなります。

  必要に応じて TCP 初期シーケンス番号のランダム化をディセーブルにできます。次の例を参考にしてください。

  - 別のインライン ファイアウォールでも初期シーケンス番号をランダム化している場合。このアクションがトラフィックに影響しない場合でも、両方のファイアウォールが共にこのアクションを実行する必要はありません。
  - FWSM を経由して eBGP マルチホップを使用し、eBGP ピアで MD5 を使用する場合。ランダム化により MD5 チェックサムが中断されます。
  - FWSM が接続のシーケンス番号をランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- **Maximum TCP Connections**：TCP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum UDP Connections**：UDP 接続の最大数を 0 ～ 65,535 で指定します。この値を 0 に設定すると、接続数は無制限になります。
- **Maximum Embryonic Connections**：初期接続のホストごとの最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。デフォルトは **0** で、最大初期接続数であることを示します。TCP 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、クライアントからセキュリティ レベルのより高いサーバへ送信される TCP SYN パケットが TCP 代行受信機能によって代行受信されます。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。

**ステップ 11**　**OK** をクリックします。

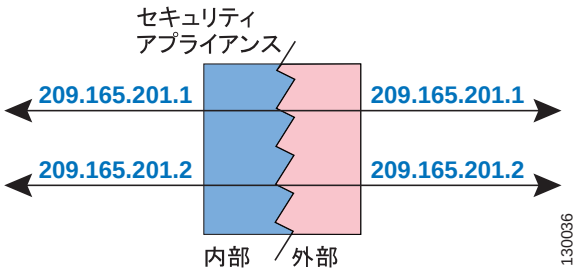
# NAT 免除の使用

NAT 免除を使用すると、アドレスが変換から免除され、実際のホストとリモート ホストの両方が接続を発信できます。NAT 免除では、（ポリシー NAT と同様）免除するトラフィックを決定する場合に、実際のアドレスと宛先アドレスを指定できるので、ダイナミック アイデンティティ NAT よりも NAT 免除を使用した場合の方が、より詳細な制御が可能になります。ただし、ポリシー NAT とは異なり、NAT 免除でポートは考慮されません。ポートを考慮するにはスタティック ポリシー アイデンティティ NAT を使用します。

NAT 免除の詳細については、P.21-10 の「NAT 制御がイネーブルの場合の NAT のバイパス」を参照してください。

図 21-23 に、一般的な NAT 免除のシナリオを示します。

**図 21-23　NAT 免除**




NAT 免除を設定するには、次の手順を実行します。

**ステップ 1**　Configuration > Firewall > NAT Rules ペインで **Add > Add NAT Exempt Rule** を選択します。

Add NAT Exempt Rule ダイアログボックスが表示されます。

**ステップ 2**　**Action: Exempt** をクリックします。

**ステップ 3**　Original 領域の Interface ドロップダウン リストから、免除する実際のアドレスを持つホストに接続されるインターフェイスを選択します。

**ステップ 4**　Source フィールドに実際のアドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

**（注）**　免除しないアドレスを後で指定することもできます。たとえば、10.1.1.0/24 のように免除するサブネットを指定できますが、10.1.1.50 を変換する場合、そのアドレスに対して免除を行わない別のルールを作成できます。

複数の実際のアドレスはカンマで区切ります。

**ステップ 5**　Destination フィールドに宛先アドレスを入力するか、または **...** ボタンをクリックして、ASDM で定義済みの IP アドレスを選択します。

10.1.1.0/24 のように、プレフィックス / 長さの表記を使用してアドレスとサブネット マスクを指定します。マスクなしで IP アドレスを入力すると、0 で終わる場合でもそのアドレスはホスト アドレスと見なされます。

複数の宛先アドレスはカンマで区切ります。

デフォルトでは、このフィールドには任意の宛先アドレスを許可する **any** が表示されています。

**ステップ 6**　NAT Exempt Direction 領域で、下位のセキュリティ インターフェイスに発信されるトラフィックを免除するか（デフォルト）、または、上位のセキュリティ インターフェイスに発信されるトラフィックを免除するかを、適切なオプション ボタンをクリックして選択します。

**ステップ 7**　（オプション）Description フィールドに説明を入力します。

**ステップ 8**　**OK** をクリックします。

**ステップ 9**　（オプション）NAT 免除のルールに含まれているアドレスの一部を免除しない場合、免除を除外する別のルールを作成できます。既存の NAT 免除ルールを右クリックして **Insert** チェックボックスをオンにします。

Add NAT Exempt Rule ダイアログボックスが表示されます。

a. **Action: Do not exempt** をクリックします。

b. 手順 3 から 8 まで実行すると、ルールが完成します。

No Exempt ルールを Exempt ルールの前に追加します。Exempt ルールと No Exempt ルールの順序は重要です。FWSM がパケットを免除するかどうかを決定する場合、FWSM は、リスト上のルールの順序で NAT exempt および No Exempt のルールに照合してパケットをテストします。一致が見つかると、その後のルールはチェックされません。