CHAPTER 12

NAT の設定

この章では、Network Address Translation（NAT; ネットワーク アドレス変換）について説明します。ルーテッド ファイアウォール モードでは、FWSM は各ネットワーク間で NAT を実行します。

（注） 透過ファイアウォール モードでは、接続制限を設定する場合を除き、FWSM は NAT をサポートしません。「透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定」（p.7-8）を参照してください。

この章で説明する内容は、次のとおりです。

- NAT の概要（p.12-2）
- NAT 制御の設定（p.12-16）
- ダイナミック NAT および PAT の使用方法（p.12-17）
- スタティック NAT の使用方法（p.12-27）
- スタティック PAT の使用方法（p.12-29）
- NAT のバイパス（p.12-32）
- NAT の例（p.12-36）

NAT の概要

ここでは、FWSM 上での NAT の機能について説明します。

- NAT の説明（p.12-2）
- NAT 制御（p.12-3）
- NAT のタイプ（p.12-5）
- ポリシー NAT（p.12-10）
- NAT および同一セキュリティ レベルのインターフェイス（p.12-13）
- 実アドレス照合用 NAT コマンドの順序（p.12-13）
- NAT ステートメントの最大数（p.12-13）
- マップ アドレスに関する注意事項（p.12-14）
- DNS および NAT（p.12-14）

NAT の説明

アドレス変換は、パケットの実アドレスを宛先ネットワーク上でルーティング可能なマップ アドレスに置き換えます。NAT は、実アドレスをマップ アドレスに変換する処理と、その後、変換を取り消してトラフィックを戻す処理の 2 つの手順で構成されています。

FWSM は NAT ルールと トラフィックが一致したときにアドレスを変換します。NAT ルールが一致しない場合は、パケット処理を続行します。ただし、NAT 制御をイネーブルにした場合は別です。NAT 制御では、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）へのトラフィックは NAT ルールと一致する必要があり、一致しない場合、パケット処理は中止されます（セキュリティ レベルの詳細については「セキュリティ レベルの概要」[p.6-2] 、NAT 制御の詳細については「NAT 制御」[p.12-3] を参照）。

（注）　このマニュアルでは、通常すべてのタイプの変換を NAT と呼びます。NAT について説明する場合、*内部*および*外部*という用語も関連し、任意の 2 つのインターフェイス間のセキュリティ関係を表します。セキュリティ レベルの高い方が内部で、低い方が外部です。たとえば、インターフェイス 1 が 60 で、インターフェイス 2 が 50 という設定の場合、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。

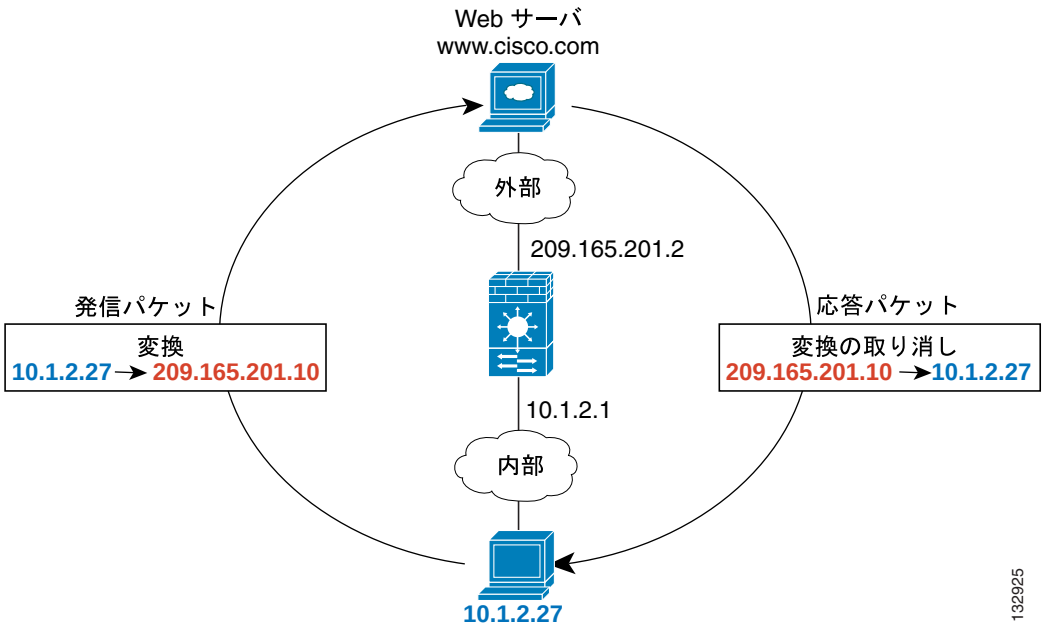
NAT の利点の一部を紹介します。

- 内部ネットワーク上でプライベート 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上でルーティングできません（詳細については、「プライベート ネットワーク」[p.D-2] を参照）。
- NAT は他のネットワークから実アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- アドレスの重複といった IP ルーティング関連の問題を解決できます。

（注）　NAT でサポートされないプロトコルについては、表 20-1（p.20-5）を参照してください。

図 12-1 に、内部にプライベート ネットワークのある、NAT の一般的な使用例を示します。10.1.1.27 にある内部ホストが Web サーバにパケットを送信すると、そのパケットの送信元実アドレス 10.1.1.27 がマップ アドレス 209.165.201.10 に変更されます。応答時、Web サーバはマップ アドレス 209.165.201.10 に応答を送り、FWSM がパケットを受信します。その後、FWSM はマップ アドレス 209.165.201.10 の変換を取り消して実アドレス 10.1.1.1.27 に戻してから、ホストにパケットを送信します。

図 12-1　NAT の例



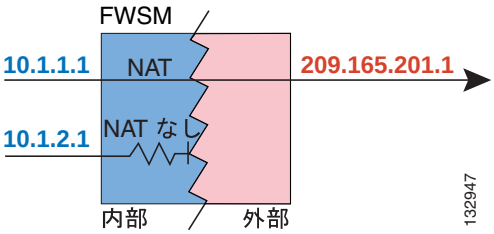
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.15
```

NAT 制御

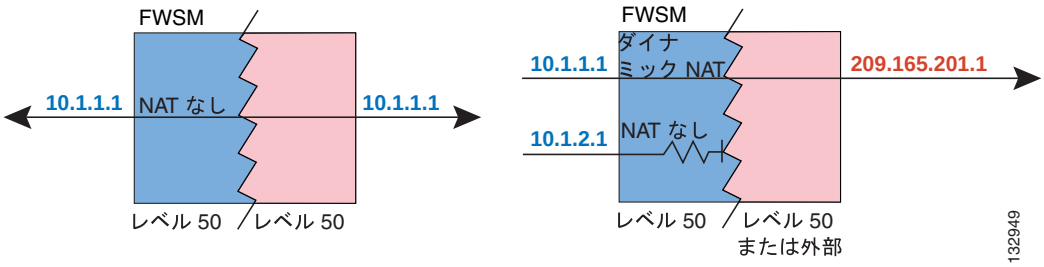
NAT 制御では、内部インターフェイスから外部インターフェイスへのパケットは NAT ルールと一致する必要があります。内部ネットワークのホストから外部ネットワークのホストにアクセスする場合は、内部ホスト アドレスを変換するように NAT を設定する必要があります（図 12-2 を参照）。

図 12-2　NAT 制御と発信トラフィック



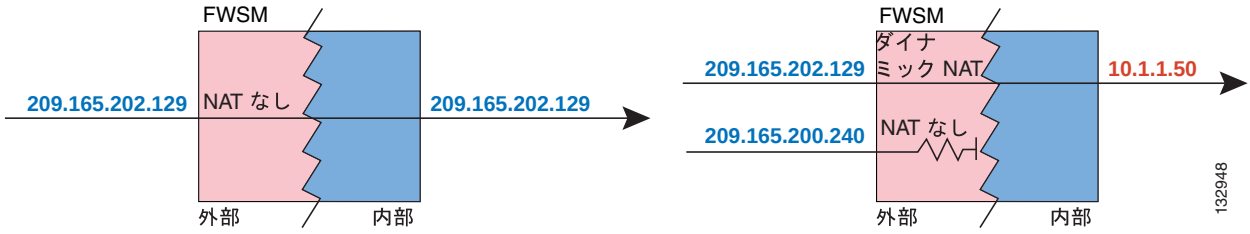
セキュリティ レベルが同一のインターフェイスは、通信に NAT を使用する必要がありません。ただし、NAT 制御をイネーブルにして同一セキュリティ インターフェイスでダイナミック NAT または PAT を設定する場合、そのインターフェイスから同一セキュリティ インターフェイスまたは外部インターフェイスへのすべてのトラフィックは、NAT ルールと一致する必要があります（図 12-3 を参照）。

図 12-3　NAT 制御と同一セキュリティ トラフィック



同様に、NAT 制御で外部ダイナミック NAT または PAT をイネーブルにする場合、内部インターフェイスにアクセスするすべての外部トラフィックは NAT ルールと一致する必要があります（図 12-4 を参照）。

図 12-4　NAT 制御と着信トラフィック



NAT 制御でスタティック NAT をイネーブルにした場合、これらの制約は発生しません。

デフォルトでは NAT 制御はディセーブルになっているため、ネットワーク上で NAT を使用するかどうかを任意に選択できます。ただし、新バージョンのソフトウェアにアップグレードした場合、NAT 制御がイネーブルになっていることがあります。

（注）　NAT を設定しない場合でも、FWSM はすべてのトラフィックに対して自動的に変換セッションを作成します。この場合、実アドレスから同じ実アドレスへの変換が行われます。変換セッションについては、**show xlate** コマンドを参照してください。

NAT 制御によってセキュリティ レベルを上げたいけれども、一部のケースで内部アドレスを変換したくない場合、このようなアドレスに NAT 除外またはアイデンティティ NAT ルールを適用できます。（詳細については、「NAT のバイパス」[p.12-32] を参照）。

NAT 制御を設定するには、「NAT 制御の設定」（p.12-16）を参照してください。

（注）　マルチコンテキスト モードにおいて、パケット分類機能は NAT コンフィギュレーションに依存してパケットをコンテキストに割り当てることがあります。NAT 制御がディセーブルであるために NAT を実行しない場合、分類機能により、ネットワーク コンフィギュレーションの変更が必要になることがあります。分類機能と NAT の関係の詳細については、「FWSM によるパケットの分類方法」（p.4-3）を参照してください。

NAT のタイプ

ここでは、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を組み合わせたものとして実行できます。NAT 制御をイネーブルにしても NAT を実行しない場合など、NAT をバイパスするルールを設定することもできます。ここでは次の内容について説明します。

- ダイナミック NAT（p.12-5）
- PAT（p.12-7）
- スタティック NAT（p.12-7）
- スタティック PAT（p.12-8）
- NAT 制御をイネーブルにした場合の NAT のバイパス（p.12-9）

ダイナミック NAT

ダイナミック NAT では、実アドレス グループを宛先ネットワーク上でルーティング可能なマップ アドレスのプールに変換します。マップ プールは、実グループより少ないアドレスで構成されます。変換対象のホストが宛先ネットワークにアクセスすると、FWSM はホストにマップ プール内の IP アドレスを割り当てます。変換は、実ホストが接続を開始するときにのみ追加されます。変換が有効なのは、接続されている間だけなので、どのユーザも変換のタイムアウト後に同じ IP アドレスを維持することはできません（『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **timeout xlate** コマンドを参照）。そのため、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストに対して（接続がアクセス リストによって許可された場合でも）、接続を確実に開始することはできず、FWSM は実ホスト アドレスに直接行われる接続試行をすべて拒否します。ホストへの確実なアクセスについては、次の 「スタティック NAT」または「スタティック PAT」を参照してください。

図 12-5 は、リモート ホストによる実アドレスへの接続試行を示しています。FWSM はマップ アドレスへの戻り接続しか許可しないため、接続は拒否されます。

図 12-5　リモート ホストによる実アドレスへの接続試行

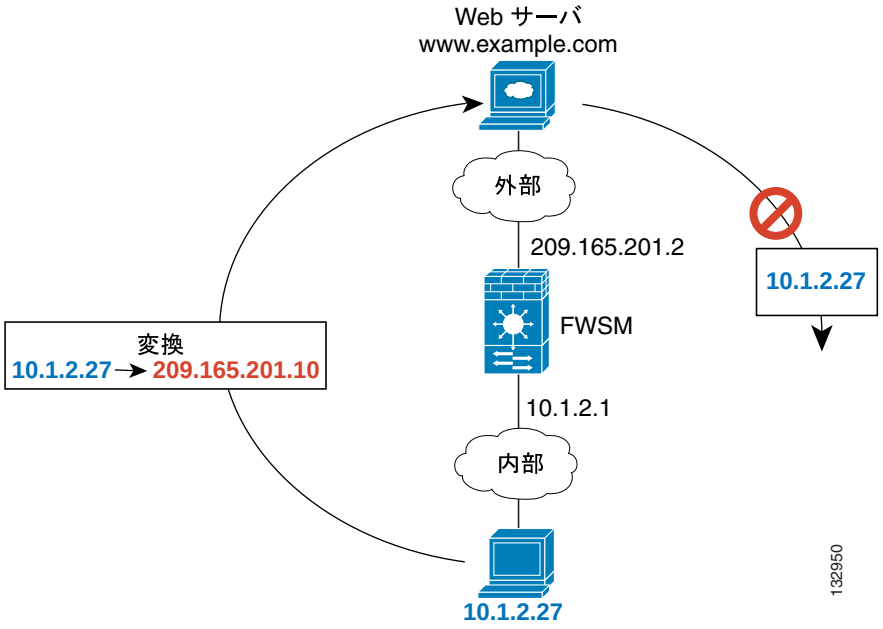
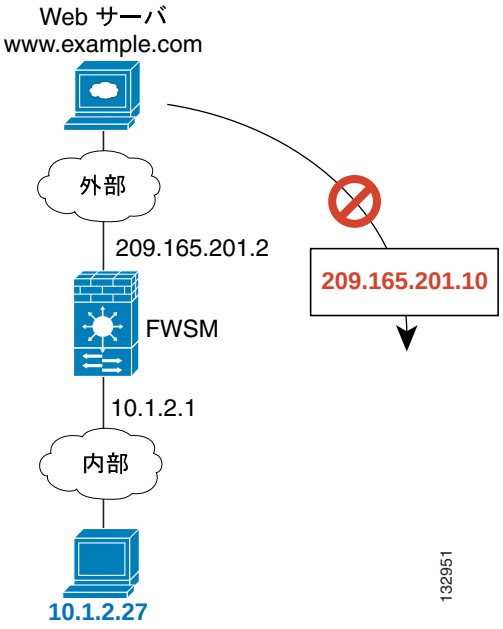


図 12-6 は、リモート ホストによるマップ アドレスへの接続試行を示しています。このアドレスは現在変換テーブルにないため、FWSM はパケットを廃棄します。

図 12-6　リモート ホストによるマップ アドレスへの接続試行



（注）　変換中であれば、リモート ホストはアクセス リストで許可されている場合は、変換対象ホストへの接続を開始できます。アドレスは予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続に成功した場合は、アクセス リストのセキュリティに頼ることになります。

ダイナミック NAT の短所は、次のとおりです。

- マップ プール内のアドレスが実グループより少ない場合、トラフィック量が予想を上回るとアドレスが不足する可能性があります。

  この現象が頻繁に発生する場合は、PAT を使用します。PAT は単一アドレスのポートを使用して 64,000 以上の変換を実行できます。

- ルーティング可能なアドレスをマップ プールで大量に使用する必要があります。インターネットなどの登録アドレスが宛先ネットワークに必要な場合は、使用可能なアドレスが不足することがあります。

ダイナミック NAT の利点は、一部のプロトコルで PAT を使用できないということです。たとえば、PAT は GRE バージョン 0 などオーバーロード ポートを持たない IP プロトコルでは動作しません。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マルチメディア アプリケーションでも動作しません。NAT および PAT のサポートの詳細については、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

PAT

PAT では、複数の実アドレスを 1 つのマップ IP アドレスに変換します。特に、FWSM は実アドレスと送信元ポート（実ソケット）を、マップ アドレスおよび 1024 より上の一意のポートに変換します（マップ ソケット）。送信元ポートは接続ごとに異なるため、接続ごとに別個の変換が必要となります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

接続が期限切れになったあと、ポート変換も 30 秒の休止状態後に期限切れになります。タイムアウトは設定できません。宛先ネットワークのユーザは、PAT を使用するホストに対して（ACL によって接続が許可されていた場合でも）、接続を確実に開始することはできません。ホストの実またはマップ ポート番号を予測できないだけでなく、FWSM は変換対象ホストが接続を開始する側でないかぎり、変換を作成しません。ホストへの確実なアクセスについては、次の「スタティック NAT」または「スタティック PAT」を参照してください。

PAT で使用するマップ アドレスは 1 つだけなので、ルーティング可能アドレスの節約になります。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できます。PAT は、データ ストリームが制御パスと異なる一部のマルチメディア アプリケーションでは動作しません。NAT および PAT のサポートの詳細については、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

（注）　変換中であれば、リモート ホストはアクセス リストで許可されている場合は、変換対象ホストへの接続を開始できます。ポート アドレスは（実およびマップの両方とも）予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続に成功した場合は、アクセス リストのセキュリティに頼ることになります。

スタティック NAT

スタティック NAT では、実アドレスからマップ アドレスへの固定変換を作成します。ダイナミック NAT および PAT の場合、各ホストは以後の各変換で異なるアドレス / ポートを使用します。スタティック NAT では、マップ アドレスは連続する各接続で同じあり、持続型の変換ルールが適用されるので、スタティック NAT の場合、（アクセス リストで許可されていれば）宛先ネットワークのホストから変換対象ホストへのトラフィックを開始できます。

ダイナミック NAT とスタティック NAT のアドレス範囲における主な相違は、スタティック NAT では、（アクセス リストで許可されていれば）リモート ホストから変換対象ホストへ接続を開始できるのに対して、ダイナミック NAT では開始できないことです。スタティック NAT ではさらに、実アドレスと同数のマップ アドレスが必要です。

スタティック PAT

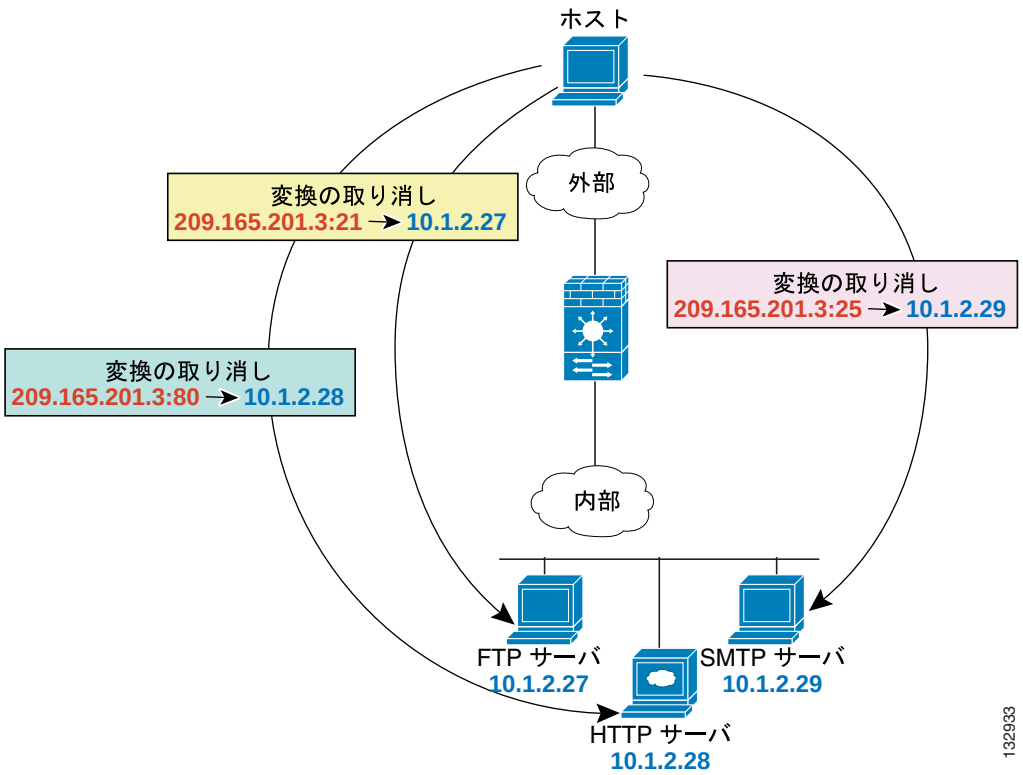
スタティック PAT は、実アドレスとマップ アドレスに対応するプロトコル（TCP または UDP）とポートを指定できることを除き、スタティック NAT と同じです。

この機能を使用すると、ステートメントごとにポートが異なるかぎり、多数のさまざまなスタティック ステートメントで同じマップ アドレスを指定できます（複数のスタティック *NAT* ステートメントに同じマップ アドレスを指定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を必要とするアプリケーションの場合、FWSM はセカンダリ ポートを自動的に変換します。

たとえば、FTP、HTTP、および SMTP にアクセスする複数のリモート ユーザに単一アドレスを提供し、実際にはそれぞれが実ネットワーク上の別々のサーバである場合、マップ IP アドレスは同じでもポートが異なる各サーバに対し、スタティック PAT ステートメントを指定できます（図 12-7 を参照）。

図 12-7　スタティック PAT



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) tcp 209.165.201.3 ftp 10.1.2.27 ftp netmask
255.255.255.255
hostname(config)# static (inside,outside) tcp 209.165.201.3 http 10.1.2.28 http
netmask 255.255.255.255
hostname(config)# static (inside,outside) tcp 209.165.201.3 smtp 10.1.2.29 smtp
netmask 255.255.255.255
```

スタティック PAT を使用して、well-known ポートを非標準ポートに、またはその逆に変換することもできます。たとえば、内部 Web サーバがポート 8080 を使用する場合、外部ユーザにポート 80 へのアクセスを許可したあと、元のポート 8080 に対する変換を取り消すことができます。同様に、セキュリティを強化したい場合に、Web ユーザに非標準ポート 6785 に接続するように通知したあと、ポート 8080 に対する変換を取り消すことができます。

NAT 制御をイネーブルにした場合の NAT のバイパス

NAT 制御をイネーブルにした場合、外部ホストにアクセスするときに、内部ホストは NAT ルールと一致する必要があります。一部のホストで NAT を実行したくない場合は、これらのホストに対して 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）。NAT をサポートしないアプリケーションを使用している場合などに、NAT をバイパスできます（NAT をサポートしないインスペクション エンジンについては、「アプリケーション インスペクション エンジンの概要」[p.20-2] を参照）。

3 とおりの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法でも、インスペクション エンジンとの互換性が確保されます。ただし、機能は少しずつ異なります。

- アイデンティティ NAT（**nat 0** コマンド）— アイデンティティ NAT を設定する場合（ダイナミック NAT と同様）、ホストの変換を特定のインターフェイスに限定しないでください。すべてのインターフェイスでの接続にアイデンティティ NAT を使用する必要があります。したがって、インターフェイス A にアクセスするときに、実アドレス上で標準変換を実行し、インターフェイス B にアクセスするときにアイデンティティ NAT を使用するといった選択はできません。これに対して、通常のダイナミック NAT を使用した場合は、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 を使用する実アドレスは、アクセス リストに基づく使用可能なすべてのネットワーク上でルーティング可能でなければなりません。

  アイデンティティ NAT を使用した場合、マップ アドレスが実アドレスと同じでも、（アクセス リストで許可されている場合を含めて）外部から内部への接続を開始することはできません。外部から内部に接続するには、スタティック アイデンティティ NAT を使用するか、または NAT 除外を適用します。
- スタティク アイデンティティ NAT（**static** コマンド）— スタティック アイデンティティ NAT を使用すると、実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 にアクセスするときにアイデンティティ NAT を使用し、インターフェイス B にアクセスするときに標準変換を使用することが可能です。スタティック アイデンティティ NAT では、ポリシー NAT も使用できます。この場合、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」（p.12-10）を参照）。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し、宛先がサーバ A の場合に、内部アドレスにスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスするときには標準変換を使用するといったことが可能です。
- NAT 除外（**nat 0 access-list** コマンド）— 変換対象ホストとリモート ホストの両方で接続を開始できます。アイデンティティ NAT と同様に、ホストの変換を特定インターフェイスに制限せずに、NAT 除外をすべてのインターフェイスでの接続に使用する必要があります。ただし、NAT 除外では、変換する実アドレスを決定するときに、（ポリシー NAT と同様）実アドレスと宛先アドレスを指定できるので、きめ細い制御が可能になります。一方、ポリシー NAT と異なり、NAT 除外ではアクセス リストのポートは考慮されません。

ポリシー NAT

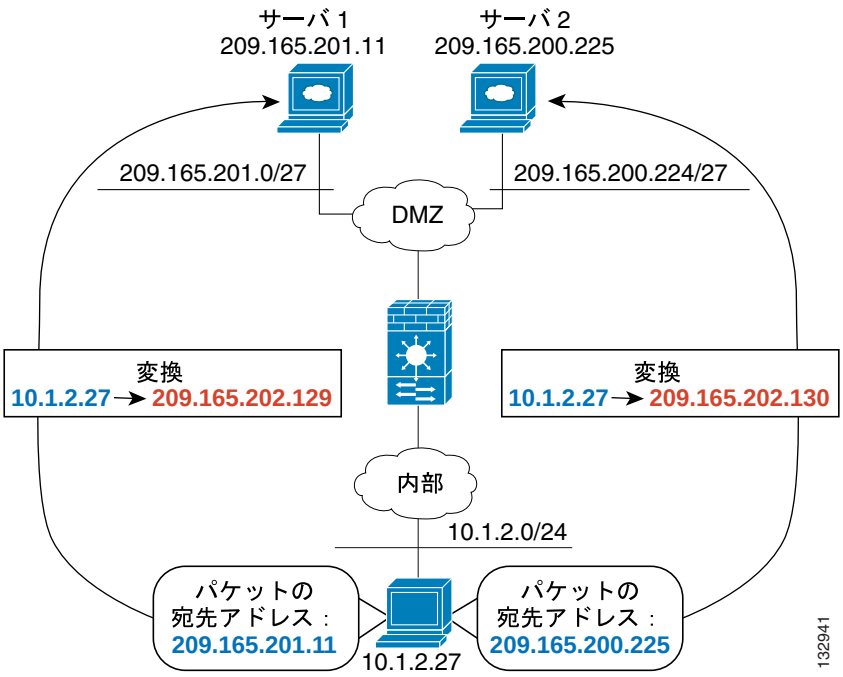
ポリシー NAT では、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象の実アドレスを特定します。任意で、送信元ポートと宛先ポートも指定できます。標準 NAT で考慮されるのは、実アドレスだけです。たとえば、サーバ A にアクセスするときには実アドレスをマップ アドレス A に変換しますが、アクセス サーバ B にアクセスするときには実アドレスをマップ アドレス B に変換します。

アプリケーション検査がセカンダリ チャネル（FTP、VoIP など）用に必要なアプリケーションに対してポリシー NAT でポートを指定するとき、FWSM はセカンダリ ポートを自動的に変換します。

（注）　NAT 除外を除くすべてのタイプの NAT がポリシー NAT をサポートします。NAT 除外では、アクセス リストを使用して実アドレスを識別しますが、ポートが考慮されない点がポリシー NAT とは異なります。その他の相違点については、「NAT のバイパス」（p.12-32）を参照してください。ポリシー NAT をサポートしないスタティック アイデンティティ NAT を使用すると、NAT 除外と同じ結果を得ることができます。

図 12-8 に、10.1.2.0/24 のネットワークに存在し、2 種類のサーバにアクセスするホストを示します。ホストが 209.165.201.11 のサーバにアクセスすると、実アドレスが 209.165.202.129 に変換されます。ホストが 209.165.200.255 のサーバにアクセスすると、実アドレスが 209.165.202.130 に変換され、ホストがサーバと同じネットワーク上にあるように見せかけることができるため、ルーティングが可能になります。

図 12-8　異なる宛先アドレスを使用するポリシー NAT

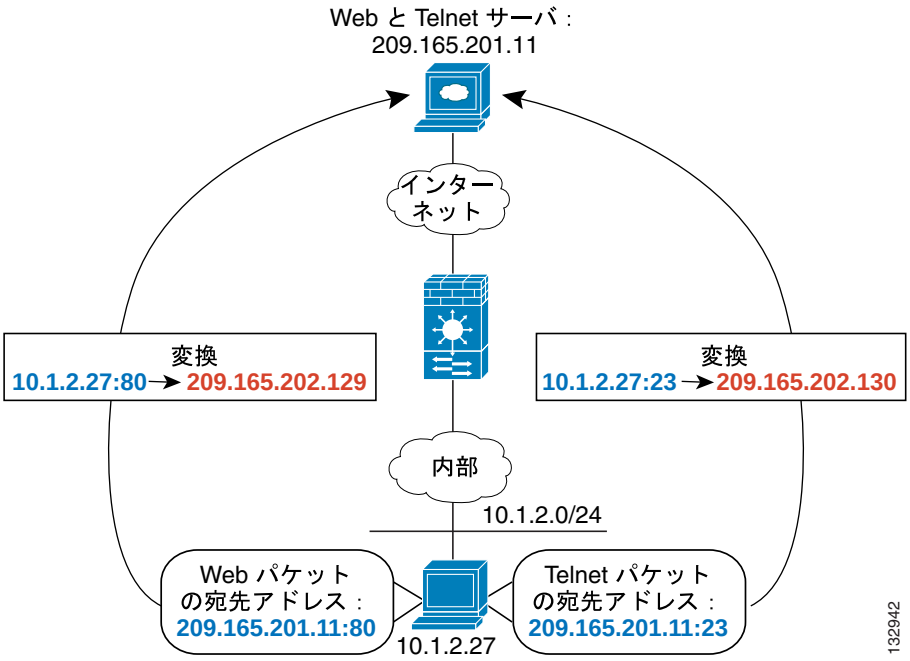


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2
hostname(config)# global (outside) 2 209.165.202.130
```

図 12-9 に、送信元ポートと宛先ポートの使用例を示します。10.1.2.0/24 のネットワーク上のホストは、単一ホストにアクセスして Web サービスと Telnet サービスの両方を利用します。ホストが Web サービスのためにサーバにアクセスした場合、実アドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスのために同じサーバにアクセスした場合は、実アドレスは 209.165.202.130 に変換されます。

図 12-9　異なる宛先ポートを使用するポリシー NAT



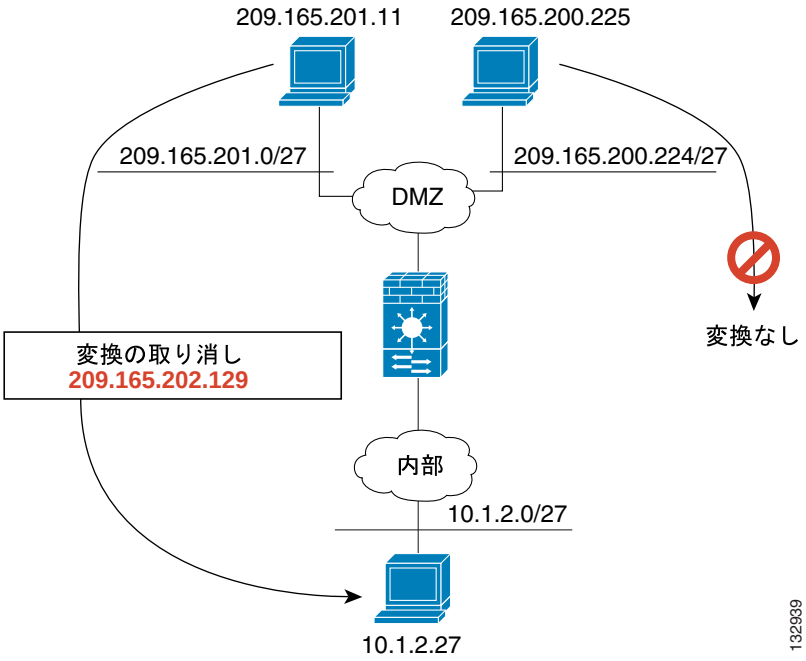
この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー スタティック NAT（および、同様にアクセス リストでトラフィックを識別する NAT 除外）の場合、変換対象ホストとリモート ホストの両方からトラフィックを発信できます。NAT アクセス リストは、変換対象ネットワークから発信されたトラフィックについては、実アドレスと*宛先*アドレスを指定しますが、リモート ネットワークから発信されたトラフィックについては、この変換を使用してホストに接続を許可されたリモート ホストの実アドレスと*送信元*アドレスを識別します。

図 12-10 は、変換対象ホストに接続するリモート ホストを示しています。変換対象ホストには、ネットワーク 209.165.201.0/27 との双方向のトラフィックだけに対し実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。ネットワーク 209.165.200.224/27 には変換が設定されていないので、変換対象ホストからこのネットワークに接続することはできません。また、このネットワーク上のホストから変換対象ホストに接続することもできません。

図 12-10　宛先アドレス変換を行うポリシー スタティック NAT



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.224 209.165.201.0
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
```

（注）　ポリシー NAT は SQL*Net をサポートしませんが、標準 NAT は SQL*Net をサポートします。他のプロトコルの NAT サポートについては、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

NAT および同一セキュリティ レベルのインターフェイス

同一セキュリティ レベルのインターフェイス間では、NAT 制御がイネーブルになっている場合であっても、NAT は必要ありません。必要に応じて任意で NAT を設定することは可能です。ただし、NAT 制御がイネーブルになっている場合にダイナミック NAT を設定するときは、NAT が必要です。詳細については、「NAT 制御」（p.12-3）を参照してください。また、同一セキュリティ レベルのインターフェイス上でダイナミック NAT または PAT に対して IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときには、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（NAT 制御がイネーブルでない場合でも）。スタティック NAT として識別されたトラフィックは影響を受けません。

同一セキュリティ レベルの通信をイネーブルにする方法については、「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）を参照してください。

（注）　同じセキュリティ レベルのインターフェイス上に NAT を設定した場合、FWSM は VoIP インスペクション エンジンをサポートしません。これらのインスペクション エンジンには、Skinny、SIP、および H.323 が含まれます。サポートされるインスペクション エンジンについては、「アプリケーション インスペクション エンジンの概要」（p.20-2）を参照してください。

実アドレス照合用 NAT コマンドの順序

FWSM は、次の順序で NAT コマンドに対して実アドレスを照合します。

1. NAT 除外（**nat 0 access-list**）— 最初の一致が見つかるまで順番どおり。アイデンティティ NAT はこのカテゴリではなく、標準スタティック NAT または標準 NAT のカテゴリに含まれます。予想外の結果が生じる可能性があるので、NAT 除外ステートメントには重複するアドレスを指定しないことを推奨します。
2. スタティック NAT およびスタティック PAT（標準およびポリシー）（**static**）— 最初の一致が見つかるまで順番どおり。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せん。**スタティック** ステートメント内でアドレスが重複する場合、警告が表示されますが、サポートは行われます。
3. ポリシー ダイナミック NAT（**nat access-list**）— 最初の一致が見つかるまで順番どおり。アドレスの重複は可能です。
4. 標準ダイナミック NAT（**nat**）— 最良の一致。標準アイデンティティ NAT はこのカテゴリに含まれます。NAT コマンドの順番は重要ではありません。実アドレスと最も一致した NAT ステートメントが使用されます。たとえば、インターフェイス上のすべてのアドレス（0.0.0.0）を変換する汎用ステートメントを作成できます。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は、10.1.1.1 だけを変換するステートメントを作成できます。10.1.1.1 が接続を開始する場合、実アドレスと最も一致するので、10.1.1.1 用のステートメントが使用されます。重複するステートメントの使用は推奨できません。メモリの消費量が増え、FWSM のパフォーマンスが低下する可能性があるからです。

NAT ステートメントの最大数

FWSM は、次に示す数の **nat** コマンド、**global** コマンド、および **static** コマンドをサポートします。この数はすべてのコンテキスト間で分割されるか、またはシングルモードで使用されます。

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

FWSM ではポリシー NAT 用として、シングルモードではアクセス リストに最大 3942 の ACE、マルチモードでは 7272 の ACE を指定できます。

マップ アドレスに関する注意事項

実アドレスをマップ アドレスに変換するときには、次のマップ アドレスを使用できます。

- マップ インターフェイスと同じネットワーク上のアドレス

  （FWSM から出ていくトラフィックが通過する）マップ インターフェイスと同じネットワーク上のアドレスを使用した場合、FWSM はプロキシ ARP を使用してマップ アドレスの要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。このソリューションにより、FWSM は他のネットワークに対するゲートウェイにはならないので、ルーティングが簡素化されます。ただし、この方式は、変換に使用できるアドレス数に制限があります。

  PAT の場合、マップ インターフェイスの IP アドレスも使用できます。

- 固有のネットワーク上のアドレス

  マップ インターフェイス ネットワーク上で使用できる数より多くのアドレスが必要な場合、別のサブネット上のアドレスを指定できます。FWSM は、プロキシ ARP を使用してマップ アドレス要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。OSPF を使用し、マップ インターフェイス上でルートをアドバタイズする場合、FWSM はマップ アドレスをアドバタイズします。マップ 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）、またはスタティック ルーティングを使用する場合は、マップ アドレス宛てのトラフィックを FWSM に送信するアップストリーム ルータ上でスタティック ルートを追加する必要があります。

DNS および NAT

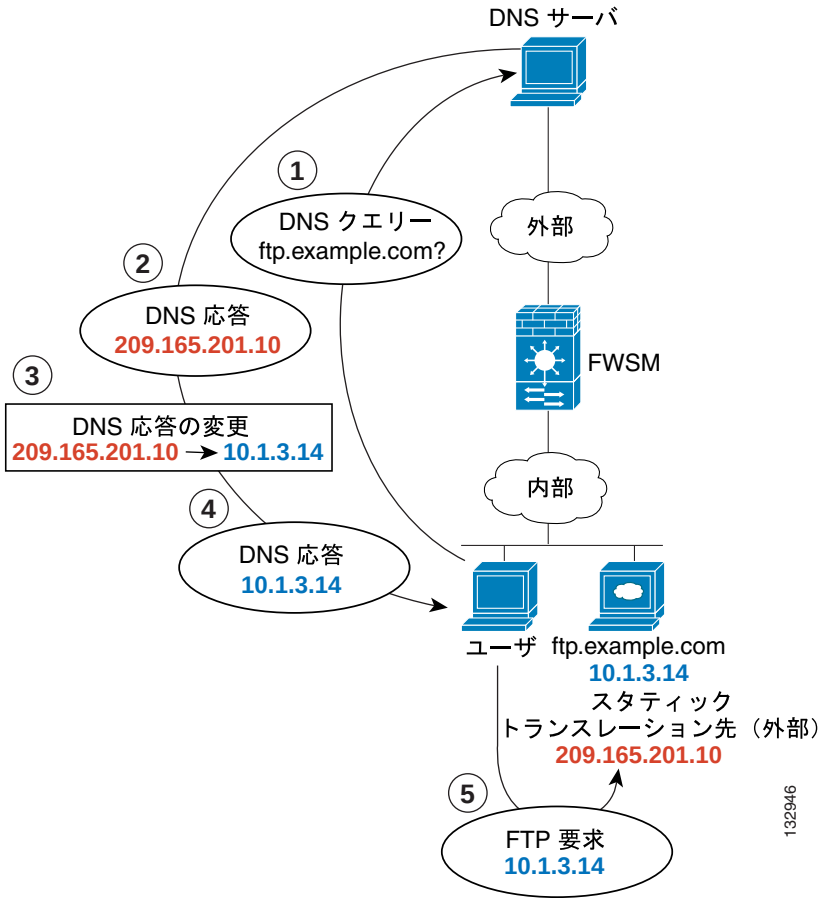
DNS 応答内のアドレスを NAT の設定と一致するアドレスに置き換えることで応答を変更するように、FWSM を設定しなければならない場合があります。DNS の変更は、各変換を設定するときに行うことができます。

たとえば、DNS サーバは外部インターフェイスからアクセスできます。サーバ ftp.example.com は内部インターフェイス上にあります。ftp.example.com の実アドレス（10.1.3.14）が外部ネットワークで表示されるマップ アドレス（209.165.201.10）にスタティックに変換されるように、FWSM を設定します（図 12-11 を参照）。この場合、このスタティック ステートメントで DNS 応答の変更をイネーブルに設定し、実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、マップ アドレスではなく、DNS サーバから実アドレスを受信するようにします。

内部ホストが ftp.example.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマップ 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 ステートメントを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答の変換をイネーブルにしなかった場合、内部ホストは ftp.example.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信しようとします。

（注）　DNS クエリー応答内の実 IP アドレスに対し、ルートを指定する必要があります。指定しないと、FWSM は 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 などのルーティング プロトコルによって突き止めることができます。

図 12-11　DNS 応答の変更

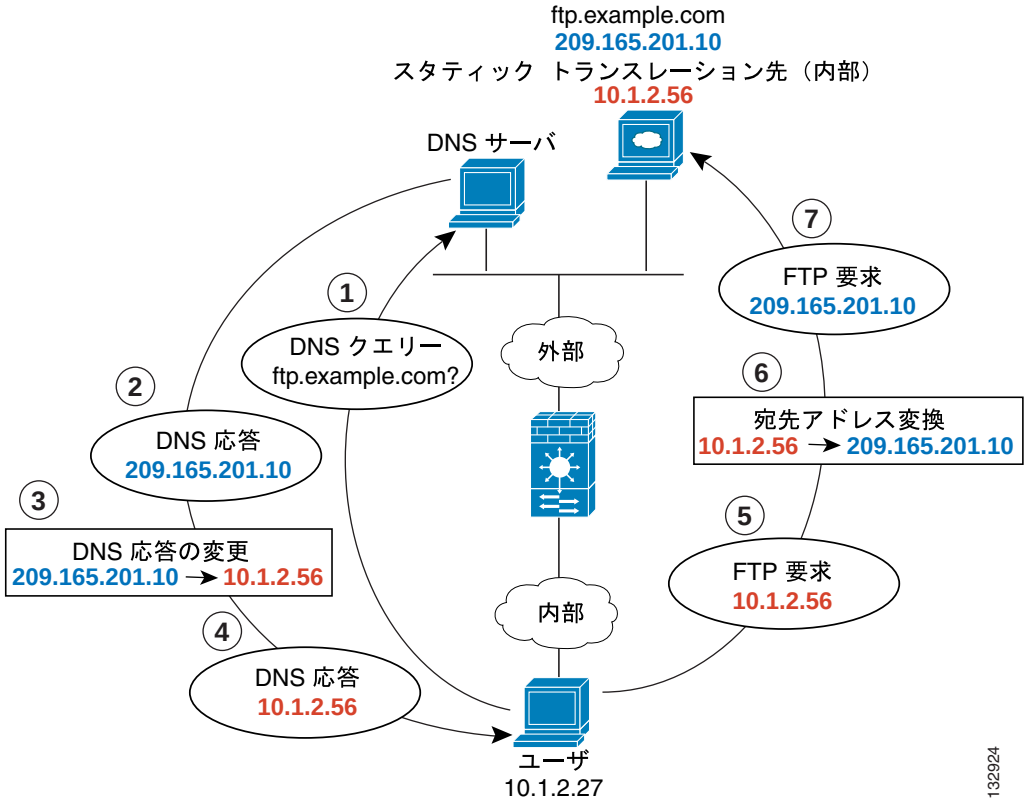


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (inside,outside) 209.165.201.10 10.1.3.14 netmask
255.255.255.255 dns
```

図 12-12 に、外部の Web サーバと DNS サーバを示します。FWSM には、外部サーバ用のスタティック トランスレーションが設定されています。この場合、内部ユーザが DNS サーバに ftp.example.com のアドレスを要求すると、DNS サーバは実アドレス 209.165.20.10 で応答します。内部ユーザには、ftp.example.com のマップ アドレス（10.1.2.56）を使用させるので、このスタティック トランスレーションに対して DNS 応答の変更を設定する必要があります。

図 12-12　DNS 応答の変更（外部 NAT を使用する場合）



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# static (outside,inside) 10.1.2.56 209.165.201.10 netmask
255.255.255.255 dns
```

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のパケットは NAT ルールと一致する必要があります。詳細については、「NAT 制御」（p.12-3）を参照してください。

NAT 制御をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# nat-control
```

NAT 制御をディセーブルにするには、このコマンドの **no** 形式を入力します。

ダイナミック NAT および PAT の使用方法

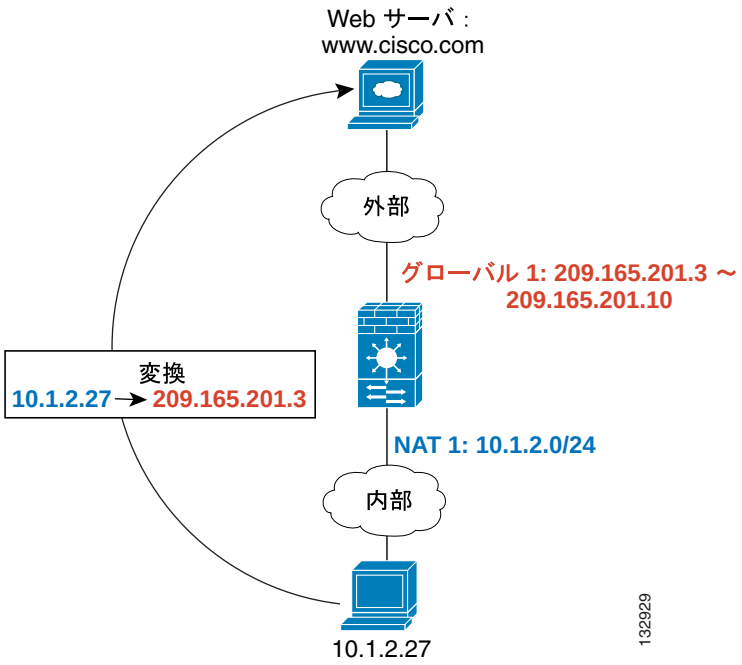
ここでは、ダイナミック NAT および PAT の設定方法について説明します。内容は次のとおりです。

- ダイナミック NAT および PAT の実装（p.12-17）
- ダイナミック NAT または PAT の設定（p.12-23）

ダイナミック NAT および PAT の実装

ダイナミック NAT および PAT の場合、最初に **nat** コマンドを設定して、変換するインターフェイス上の実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマップ アドレスを指定します（PAT の場合、このアドレスは 1 つです）。NAT ID、各コマンドに割り当てる番号を比較して、各 **nat** コマンドと **global** コマンドを照合します（図 12-13 を参照）。

図 12-13　NAT およびグローバル ID の照合

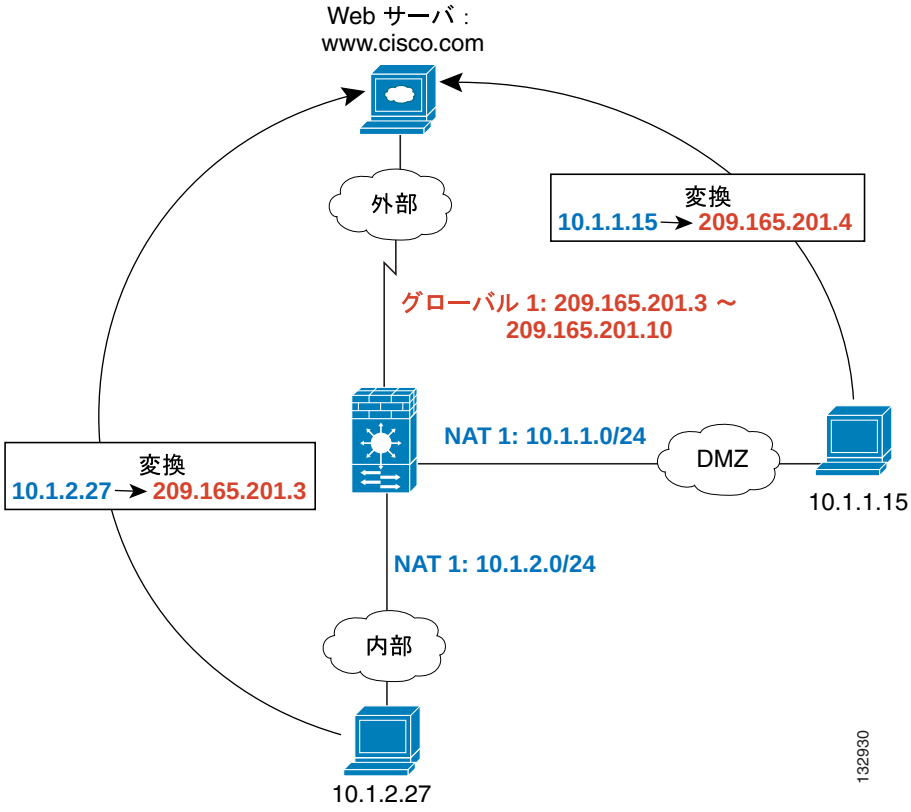


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

同じ NAT ID を使用して各インターフェイスに 1 つずつ **nat** コマンドを入力できます。その場合、トラフィックがインターフェイスから出ていくときに、すべてのインターフェイスで同じ **global** コマンドが使用されます。たとえば、内部インターフェイスと DMZ インターフェイスに NAT ID 1 を使用して、**nat** コマンドを設定します。さらに、同様に ID 1 を使用して、外部インターフェイスに **global** コマンドを設定します。内部インターフェイスと DMZ インターフェイスからのトラフィックは、外部インターフェイスを出るときに、マップ プールまたは PAT アドレスを共有します（図 12-14 を参照）。

図 12-14　複数のインターフェイスにおける NAT コマンド

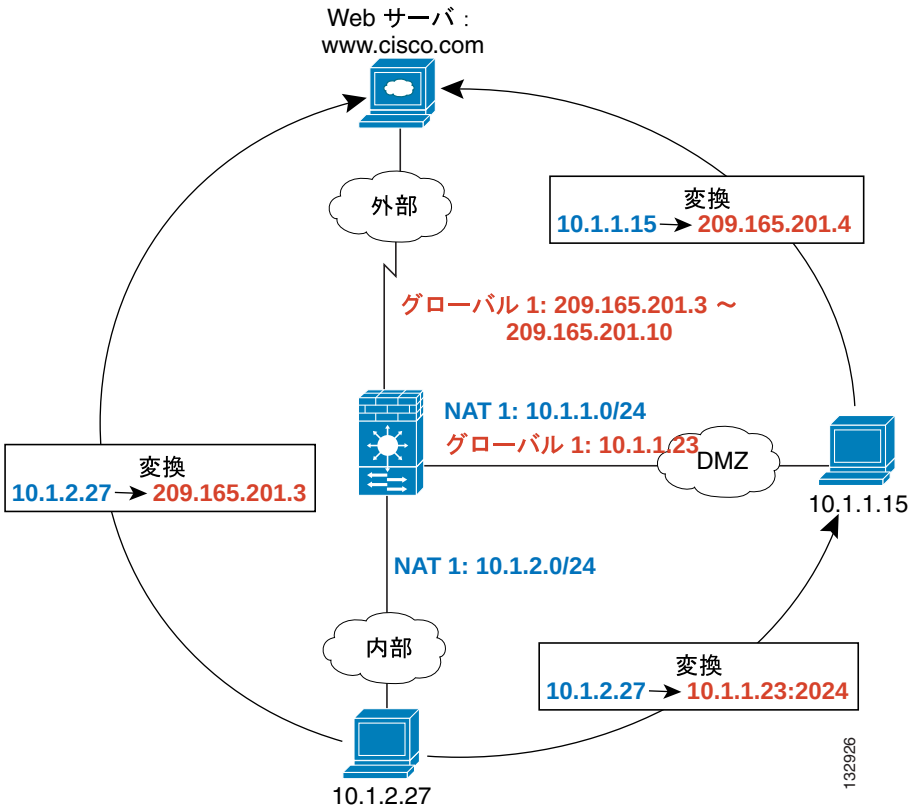


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
```

同じ NAT ID を使用して、各インターフェイスに **global** コマンドを 1 つずつ入力することもできます。ID 1 を使用して、外部インターフェイスと DMZ インターフェイスに **global** コマンドを入力した場合、内部 **nat** コマンドでは、外部インターフェイスと DMZ インターフェイスの両方に送る場合に、トラフィックを変換することを指定します。同様に、DMZ インターフェイスにも ID 1 を使用して **nat** コマンドを入力した場合、DMZ トラフィックにも外部インターフェイス上の **global** コマンドが使用されます（図 12-15 を参照）。

図 12-15　複数のインターフェイスにおけるグローバルおよび NAT コマンド

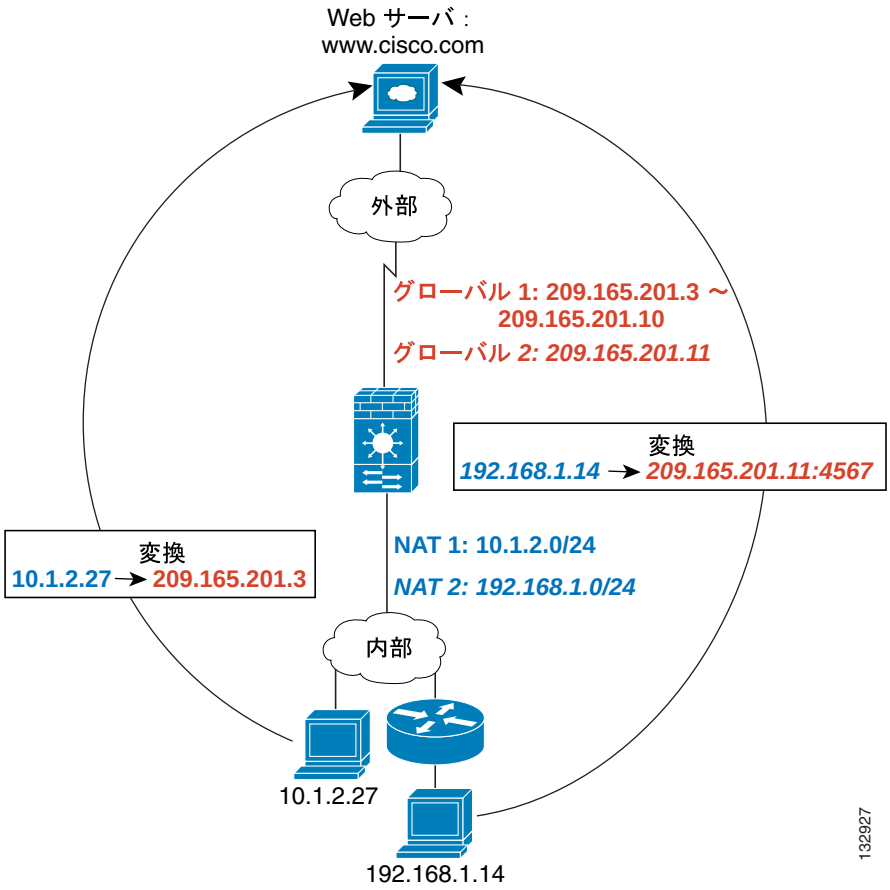


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
hostname(config)# global (dmz) 1 10.1.1.23
```

複数の異なる NAT ID を使用する場合は、さまざまな実アドレス セットにそれぞれ異なるマップ アドレスが割り当てられるように指定します。たとえば、内部インターフェイス上で、2 つの **nat** コマンドを 2 つの NAT ID に指定できます。外部インターフェイスでは、この 2 つの ID に対応する **global** コマンドを 2 つ設定できます。さらに、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から出るときに、IP アドレスはプール A のアドレスに変換されます。内部ネットワーク B のトラフィックはプール B のアドレスに変換されます（図 12-16 を参照）。ポリシー NAT を使用する場合、各アクセス リストで宛先アドレスとポートが一意であれば、複数の **nat** コマンドに同一の実アドレスを指定できます。

図 12-16　異なる NAT ID

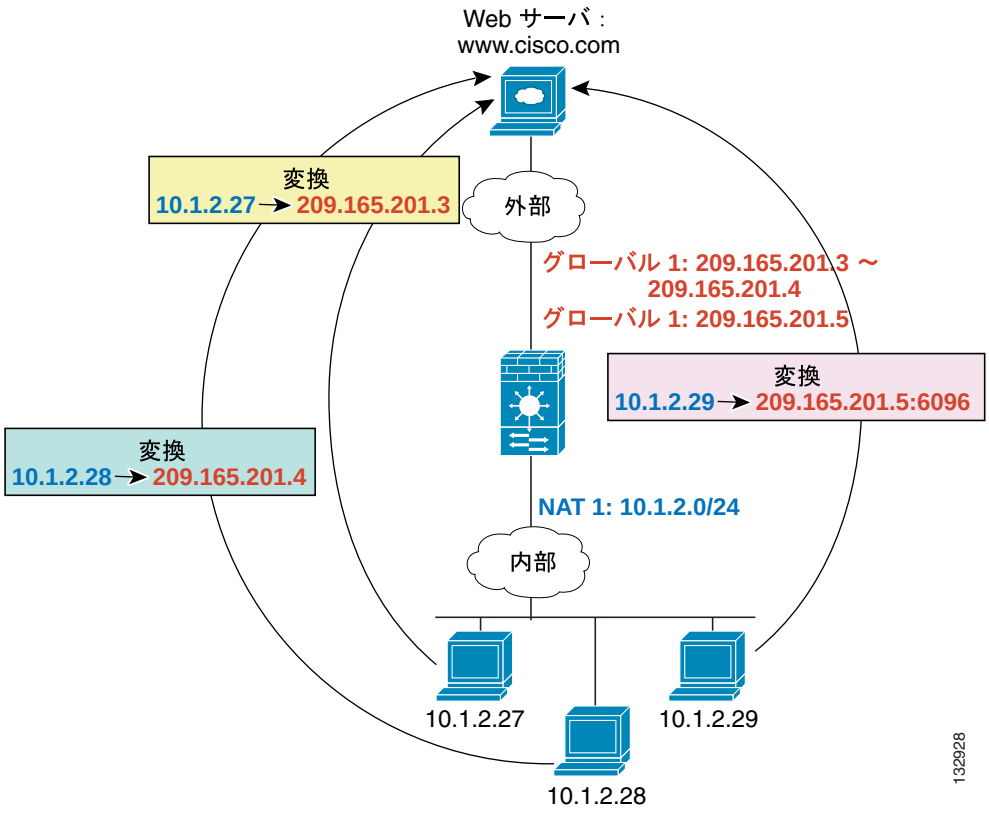


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# nat (inside) 2 192.168.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.10
hostname(config)# global (outside) 2 209.165.201.11
```

同じ NAT ID を使用して、1 つのインターフェイスに複数の **global** コマンドを入力できます。この場合、FWSM は最初に、ダイナミック NAT の **global** コマンドをコンフィギュレーションで指定された順番どおりに使用し、次に PAT の **global** コマンドを順番どおりに使用します。特定のアプリケーションにダイナミック NAT を使用する必要があり、なおかつダイナミック NAT アドレスをすべて使い果たした場合に備えてバックアップ用の PAT ステートメントも必要だという場合、ダイナミック NAT **global** コマンドと PAT **global** コマンドの両方を入力します。同様に、1 つの PAT マップ ステートメントでサポートされる約 64,000 より多くの PAT セッションが必要な場合、PAT ステートメントを 2 つ入力できます（図 12-17 を参照）。

図 12-17　NAT および PAT の併用

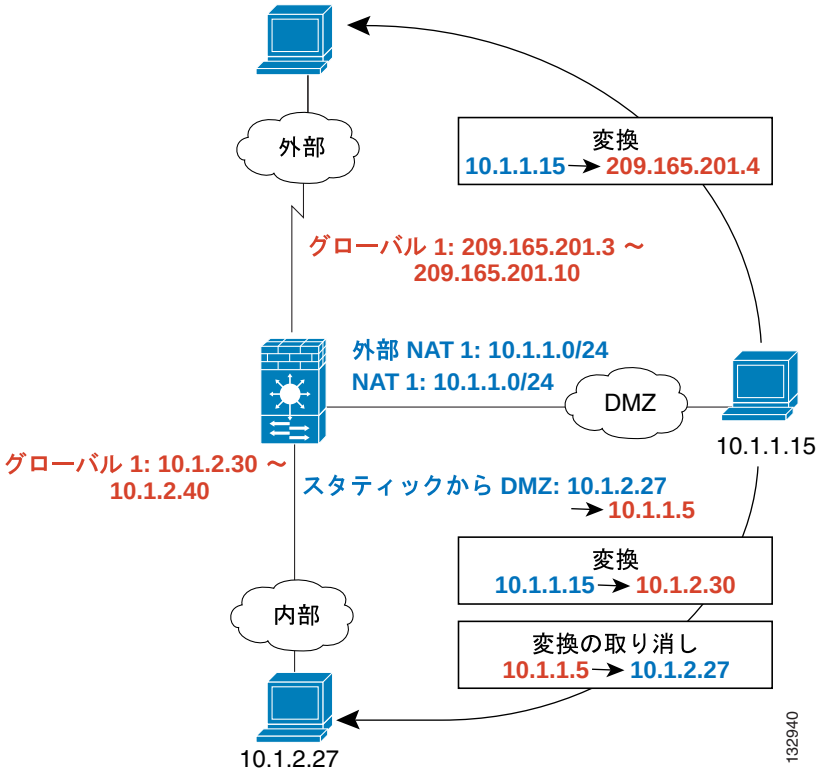


この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (inside) 1 10.1.2.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.4
hostname(config)# global (outside) 1 209.165.201.5
```

外部 NAT の場合、外部 NAT 用の **nat** コマンドを識別する必要があります（**outside** キーワード）。内部インターフェイスにアクセスしたときにも同じトラフィックを変換する場合は（DMZ 上のトラフィックを内部インターフェイスにアクセスするときにも、外部インターフェイスにアクセスするときにも変換するような状況）、**outside** オプションを使用せずに、別個の **nat** コマンドを設定する必要があります。この場合、両方のステートメントで同じアドレスを指定し、同じ NAT ID を使用できます（図 12-18 を参照）。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 **static** コマンドを使用して外部アクセスを許可するので、送信元アドレスと宛先アドレスの両方が変換されることに注意してください。

図 12-18　外部 NAT および内部 NAT の組み合わせ



この例に対応するコマンドは、次のとおりです。

```
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0 outside
hostname(config)# nat (dmz) 1 10.1.1.0 255.255.255.0
hostname(config)# static (inside,dmz) 10.1.2.27 10.1.1.5 netmask 255.255.255.255
hostname(config)# global (outside) 1 209.165.201.3-209.165.201.4
hostname(config)# global (inside) 1 10.1.2.30-1-10.1.2.40
```

nat コマンドで IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときに、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。各インターフェースで同じ NAT ID を持つ **global** コマンドを適用するか、**static** コマンドを使用します。アドレス グループが上位セキュリティ レベルのインターフェイスにアクセスする場合、NAT は必要ありません。外部から内部に NAT を実行するには、**outside** キーワードを使用して別個の **nat** コマンドを作成する必要があるためです。外部 NAT を適用する場合、アドレス グループがすべての上位セキュリティ レベルのインターフェイスにアクセスするときに、直前の NAT 要件がそのアドレス グループに対して有効になります。**static** コマンドによって識別されたトラフィックは影響を受けません。

ダイナミック NAT または PAT の設定

ここでは、ダイナミック NAT またはダイナミック PAT の設定方法について説明します。ダイナミック NAT およびダイナミック PAT の設定方法はほぼ同じですが、NAT ではマップ アドレス範囲を指定するのに対して、PAT では単一アドレスを指定します。

図 12-19 に、一般的なダイナミック NAT の使用例を示します。変換対象ホストのみが NAT セッションを作成することができ、応答トラフィックの返信が許可されます。マップ アドレスは **global** コマンドによって定義されたプールから動的に割り当てられます。

図 12-19　ダイナミック NAT

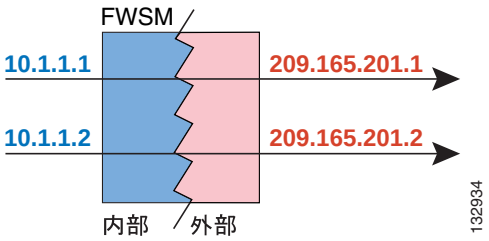
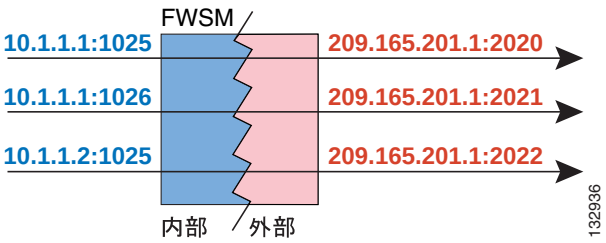


図 12-20 に、一般的なダイナミック PAT の使用例を示します。変換対象ホストのみが NAT セッションを作成することができ、応答トラフィックの返信が許可されます。**global** コマンドによって定義されたマップ アドレスは各変換で同一ですが、ポートは動的に割り当てられます。

図 12-20　ダイナミック PAT



ダイナミック NAT の詳細については、「ダイナミック NAT」（p.12-5）を参照してください。PAT の詳細については、「PAT」（p.12-7）を参照してください。

（注）　NAT の設定を変更し、既存の変換がタイムアウトする前に新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して、変換テーブルを消去します。ただし、変換テーブルを消去すると、その変換を使用するすべての接続が切断されます。

ダイナミック 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　次のコマンドを入力して、変換する実アドレスを指定します。

- ポリシー NAT：

```
hostname(config)# nat (real_interface) nat_id access-list acl_name [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

他の **nat** コマンドで重複するアドレスを指定できます。たとえば、あるコマンドで 10.1.1.0 を指定し、別のコマンドで 10.1.1.1 を指定できます。トラフィックは最初の一致が見つかるまで順番にポリシー NAT コマンドと照合されます。または標準 NAT の場合は、最良の一致を使用します。

このコマンドのオプションについて説明します。

- **access-list** *acl_name* — 拡張アクセス リストを使用して、実アドレスと宛先アドレスを指定します。**access-list** コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。**eq** 演算子を使用して、アクセス リストに実ポートと宛先ポートを任意に指定できます。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。
- *nat_id* — 1 ～ 65,535 の整数です。NAT ID は **global** コマンドの NAT ID と一致する必要があります。NAT ID の使用方法の詳細については、「ダイナミック NAT および PAT の実装」（p.12-17）を参照してください。**0** は NAT 除外用として予約されています（NAT 除外の詳細については、「NAT 除外の設定」[p.12-34] を参照）。
- **dns** — DNS サーバにエントリが作成されているホストのアドレスを **nat** コマンドに指定し、なおかつ DNS サーバがクライアントとは異なるインターフェイス上に配置されている場合、クライアントと DNS サーバに必要なホスト アドレスはそれぞれ異なります。一方はマップ アドレスが必要で、もう一方は実アドレスが必要です。このオプションを使用すると、クライアントに対する DNS 応答のアドレスが書き換えられます。変換対象のホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上に存在していなければなりません。通常、外部インターフェイスからアクセス許可が必要なホストにはスタティック変換を使用するので、このオプションは **static** コマンドと組み合わせて使用するのが一般的です（詳細については、「DNS および NAT」[p.12-14] を参照）。
- **outside** — このインターフェイスのセキュリティ レベルが **global** ステートメントの一致によって特定されたインターフェイスより低い場合、**outside** を入力し、NAT インスタンスを外部 NAT として指定する必要があります。
- **tcp** *tcp_max_conns* — サブネット全体における同時 TCP 接続の最大数（65,536 まで）を指定します。デフォルトは 0 で、これは最大接続数を意味します。
- *emb_limit* — ホストごとの初期接続の最大数（65,536 まで）です。デフォルトは 0 で、これは最大接続数を意味します。*emb_limit* を入力する前に、**tcp** *tcp_max_conns* を入力する必要があります。*tcp_max_conns* にはデフォルト値を使用し、*emb_limit* を変更する場合は、*tcp_max_conns* に **0** を入力します。

  初期接続とは、送信元と宛先間で所定のハンドシェークが完了していない接続要求のことです。初期接続数を制限すると、DoS 攻撃からシステムを保護できます。FWSM は初期接続制限を使用して、TCP 代行受信機能をトリガーします。TCP 代行受信では、SYN クッキー アルゴリズムを使用して、TCP SYN フラッディング攻撃を阻止します。SYN フラッディング攻撃では通常、スプーフィングされた IP アドレスから一連の SYN パケットが送信されます。継続的に送信される SYN パケットにより、サーバの SYN キューが常に満杯状態になり、接続要求を処理できなくなります。接続が、初期接続スレッシュホールドに達すると、FWSM はサーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成します。FWSM は、クライアントから ACK の返信を受信すると、そのクライアントを認証し、サーバへの接続を許可します。
- **udp** *udp_max_conns* — サブネット全体における同時 UDP 接続の最大数（65,536 まで）を設定します。デフォルトは 0 で、これは最大接続数を意味します。

— **norandomseq** — TCP Initial Sequence Number（ISN）ランダム化をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化し、その結果、データのスクランブルが発生する場合だけです。各 TCP 接続には、2 つの Initial Sequence Number（ISN）があります。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM はホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションを乗っ取る可能性を排除するために、ISN の少なくとも一方はランダムに作成する必要があります。

（注） Modular Policy Framework を使用して接続制限（初期接続制限は設定できません）を設定することもできます。詳細については、「接続制限とタイムアウトの設定」（p.19-2）を参照してください。NAT を使用する場合のみ、初期接続制限を設定できます。両方の方法を使用する同一トラフィックに対してこれらを設定した場合、FWSM は低い制限値を使用します。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なっている場合、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。

- 標準 NAT

```
hostname(config)# nat (real_interface) nat_id real_ip [mask [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]]
```

nat_id は 1 ～ 2,147,483,647 の整数です。NAT ID は **global** コマンドの NAT ID と一致する必要があります。NAT ID の使用方法の詳細については、「ダイナミック NAT および PAT の実装」（p.12-17）を参照してください。**0** はアイデンティティ NAT 用として予約されています。アイデンティティ NAT の詳細については、「アイデンティティ NAT の設定」（p.12-32）を参照してください。

その他のオプションについては、前述のポリシー NAT コマンドを参照してください。

ステップ 2　次のコマンドを入力して、特定のインターフェイスから送信される実アドレスに割り当てるマップ アドレス（複数可）を指定します。

```
hostname(config)# global (mapped_interface) nat_id {mapped_ip[-mapped_ip]}
```

この NAT ID は、**nat** コマンドの NAT ID と一致する必要があります。対応する **nat** コマンドで、このインターフェイスを出るときに変換するアドレスを指定します。

単一アドレス（PAT の場合）またはアドレス範囲（NAT の場合）を指定できます。範囲は必要に応じて、サブネット境界を超えて指定できます。次に、指定できる「スーパーネット」の例を示します。

```
192.168.1.1-192.168.2.254
```

たとえば、内部インターフェイスの 10.1.1.0/24 ネットワークを変換する場合、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT のアドレス プールとともに、NAT プールを使い果たしたときのために PAT アドレスを指定する場合は、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングを簡素化する場合など、セキュリティ レベルの低い DMZ ネットワークのアドレスを変換し、内部ネットワーク（10.1.1.0）と同じネットワーク上にあるように見せるには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実アドレスに 2 つの宛先アドレスを指定するには、次のコマンドを入力します（図 12-8（p.12-10）を参照）。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、1 つの実アドレス / 宛先アドレス ペアに複数の異なるポートを指定するには、次のコマンドを入力します（図 12-9（p.12-11）を参照）。

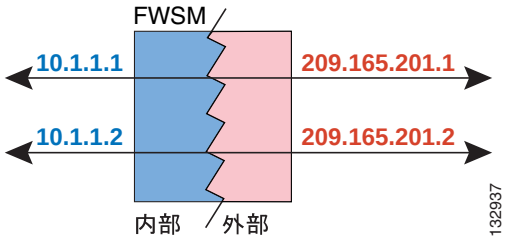
```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

スタティック NAT の使用方法

ここでは、スタティック トランスレーションの設定方法について説明します。

図 12-21 に、一般的なスタティック NAT の使用例を示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 12-21　スタティック NAT



同じ 2 つのインターフェイス間で複数の **static** コマンドに、同じ実アドレスまたはマップ アドレスを使用することはできません。同一マップ インターフェイスの **global** コマンドにも定義されたマップ アドレスを、**static** コマンドに使用しないでください。

スタティック NAT の詳細については、「スタティック NAT」（p.12-7）を参照してください。

（注）　**static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック NAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック NAT の場合、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) mapped_ip
access-list acl_name [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
[norandomseq]
```

access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストで使用した送信元サブネット マスクをマップ アドレスにも使用します。**eq** 演算子を使用して、アクセス リストに実ポートと宛先ポートを指定することもできます。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。詳細については、「ポリシー NAT」（p.12-10）を参照してください。

変換のためにネットワークを指定する場合（10.1.1.0 255.255.255.0 など）、FWSM はアドレス .0 および .255 を変換します。これらのアドレスへのアクセスを阻止する場合は、アクセスを拒否するようにアクセス リストを設定します。

その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック NAT を設定する場合、次のコマンドを入力します。

  ```
  hostname(config)# static (real_interface,mapped_interface) mapped_ip real_ip
  [netmask mask] [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
  [norandomseq]
  ```

  オプションについては、「ダイナミック NAT または PAT の設定」(p.12-23)を参照してください。

次のポリシー スタティック NAT の例では、1 つの実アドレスが宛先アドレスに応じて 2 つのマップ アドレスに変換されます（図 12-8 [p.12-10] を参照）。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドで、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）に対応付けます。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

次のコマンドで、外部アドレス（209.165.201.15）を内部アドレス（10.1.1.6）に対応付けます。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

次のコマンドで、サブネット全体をスタティックに対応付けます。

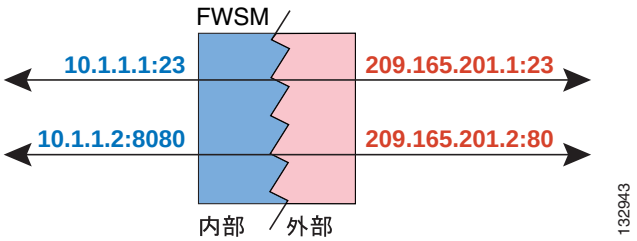
```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

スタティック PAT の使用方法

ここでは、スタティック ポート トランスレーションの設定方法について説明します。スタティック PAT を使用すると、実 IP アドレスをマップ IP アドレスに変換し、さらに実ポートをマップ ポートに変換できます。実ポートを同一ポートを変換する場合は、特定のトラフィック タイプのみを変換できます。または、別のポートに変換することによってさらに細かく制御することもできます。

図 12-22 に、一般的なスタティック PAT の使用例を示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスおよびポートは **static** コマンドによって静的に割り当てられます。

図 12-22　スタティック PAT



セカンダリ チャネル（FTP、VoIP など）でアプリケーション検査を必要とするアプリケーションの場合、FWSM はセカンダリ ポートを自動的に変換します。

同じ 2 つのインターフェイス間で複数の **static** ステートメントに、同じ実アドレスまたはマップ アドレスを使用することはできません。同一マップ インターフェイスの **global** コマンドにも定義されたマップ アドレスを、**static** コマンドに使用しないでください。

スタティック PAT の詳細については、「スタティック PAT」（p.12-8）を参照してください。

（注）　**static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック PAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック PAT の場合、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {tcp | udp} mapped_ip
mapped_port access-list acl_name [dns] [[tcp] tcp_max_conns [emb_limit]]
[udp udp_max_conns] [norandomseq]
```

  access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。アクセス リストのプロトコルとこのコマンドで設定するプロトコルは一致している必要があります。たとえば、**static** コマンドで **tcp** を指定する場合は、アクセス リストで **tcp** を指定する必要があります。ポートを指定するには、**eq** 演算子を使用します。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストで使用した送信元サブネット マスクをマップ アドレスにも使用します。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。

変換に対してネットワークを指定する場合（10.1.1.0 255.255.255.0 など）、FWSM はアドレス .0 および .255 を変換します。これらのアドレスへのアクセスを阻止する場合は、アクセスを拒否するようにアクセス リストを設定します。

その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック PAT を設定する場合は、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) {tcp | udp} mapped_ip
mapped_port real_ip real_port [netmask mask] [dns] [[tcp] tcp_max_conns
[emb_limit]] [udp udp_max_conns] [norandomseq]
```

オプションについては、「ダイナミック NAT または PAT の設定」(p.12-23)を参照してください。

たとえば、ネットワーク 10.1.3.0 上のホストから FWSM の外部インターフェイス（10.1.2.14）に Telnet トラフィックを送信する場合、次のコマンドを入力すると、10.1.1.15 の内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

ネットワーク 10.1.3.0 上のホストから FWSM の外部インターフェイス（10.1.2.14）に HTTP トラフィックを送信する場合、次のように入力すると、10.1.1.15 の内部ホストにトラフィックをリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

FWSM の外部インターフェイス（10.1.2.14）から 10.1.1.15 の内部ホストに Telnet トラフィックをリダイレクトする場合、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

ただし、この例で前述の実 Telnet サーバに接続を開始させる場合は、追加の変換が必要です。たとえば、他のすべてのトラフィック タイプを変換する場合は、次のコマンドを入力します。元の **static** コマンドがサーバへの Telnet を変換するのに対して、**nat** コマンドおよび **global** コマンドはサーバからの発信接続に PAT を実行します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

さらに、すべての内部トラフィックに別個の変換を実行し、内部ホストで Telnet サーバとは異なるマップ アドレスを使用する場合でも、Telnet サーバから開始されたトラフィックに、サーバへの Telnet トラフィックを可能にする **static** ステートメントと同じマップ アドレスを使用できます。その場合、Telnet サーバ用に、より排他的な **nat** ステートメントを作成する必要があります。**nat** ステートメントは最良の一致方式で読み取られるので、排他性の強い **nat** ステートメントは一般的な

ステートメントより先に照合されます。次に、Telnet **static** ステートメント、Telnet サーバから開始されたトラフィックに対応する排他性の強い **nat** ステートメント、および他の内部ホストに対応し、別のマップ アドレスを使用するステートメントの例を示します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

well-known ポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

NAT のバイパス

ここでは、NAT のバイパス方法について説明します。NAT 制御をイネーブルにするときに、NAT をバイパスできます。アイデンティティ NAT、スタティック アイデンティティ NAT、または NAT 除外を使用することによって、NAT をバイパスできます。各方式の詳細については、「NAT 制御をイネーブルにした場合の NAT のバイパス」（p.12-9）を参照してください。このセクションでは、次の内容について説明します。

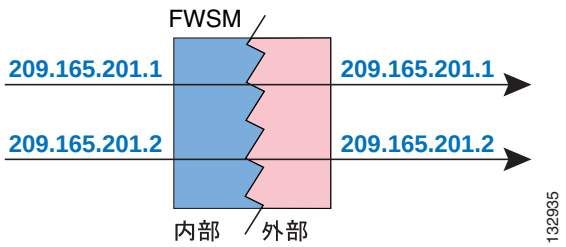
- アイデンティティ NAT の設定（p.12-32）
- スタティック アイデンティティ NAT の設定（p.12-33）
- NAT 除外の設定（p.12-34）

アイデンティティ NAT の設定

アイデンティティ NAT では、実 IP アドレスを同一 IP アドレスに変換します。「変換対象」ホストのみが NAT 変換を作成することができ、応答トラフィックの返信が許可されます。

図 12-23 に、一般的なアイデンティティ NAT の使用例を示します。

図 12-23　アイデンティティ NAT



（注）　NAT の設定を変更し、既存の変換がタイムアウトする前に新しい NAT 情報を使用する必要がある場合は、**clear xlate** コマンドを使用して、変換テーブルを消去します。ただし、変換テーブルを消去すると、その変換を使用するすべての接続が切断されます。

アイデンティティ NAT を設定するには、次のコマンドを入力します。

```
hostname(config)# nat (real_interface) 0 real_ip [mask [dns] [outside]
[[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]]
```

オプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

たとえば、内部のネットワーク 10.1.1.0/24 にアイデンティティ NAT を使用する場合、次のコマンドを入力します。

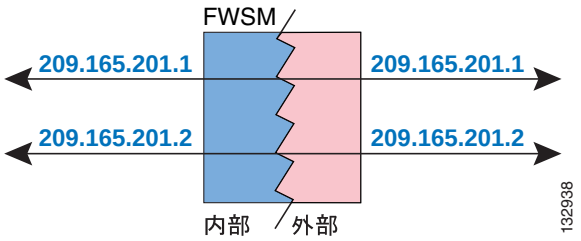
```
hostname(config)# nat (inside) 0 10.1.1.0 255.255.255.0
```

スタティック アイデンティティ NAT の設定

スタティック アイデンティティ NAT では、実 IP アドレスを同一 IP アドレスに変換します。変換は常にアクティブであるため、「変換対象」ホストとリモート ホストの両方で接続を生成できます。スタティック アイデンティティ NAT では、標準 NAT またはポリシー NAT を使用できます。ポリシー NAT の場合は、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」[p.12-10] を参照）。たとえば、内部アドレスが外部インターフェイスにアクセスし、宛先がサーバ A の場合に、内部アドレスにポリシー スタティック アイデンティティ NAT を使用します。ただし、外部サーバ B にアクセスするときには標準変換を使用します。

図 12-24 に、一般的なスタティック アイデンティティ NAT の使用例を示します。

図 12-24　スタティック アイデンティティ NAT



（注）　**static** コマンドを削除しても、その変換を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

変換テーブルから **clear xlate** コマンドでスタティック トランスレーションを消去することはできません。代わりに、**static** コマンドを削除する必要があります。**nat** および **global** コマンドで作成されたダイナミック変換のみ、**clear xlate** コマンドで削除できます。

スタティック アイデンティティ NAT を設定するには、次のいずれかのコマンドを入力します。

- ポリシー スタティック アイデンティティ NAT を設定する場合は、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) real_ip access-list
acl_id [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

  access-list コマンドを使用してアクセス リストを作成します（「拡張アクセス リストの追加」[p.10-7] を参照）。このアクセス リストには、**permit** ACE しか含めることができません。アクセス リストの送信元アドレスが、このコマンドの *real_ip* と一致する必要があります。ポリシー NAT では **inactive** または **time-range** キーワードは考慮されず、すべての ACE がポリシー NAT コンフィギュレーションに対してアクティブであるとみなされます。詳細については、「ポリシー NAT」（p.12-10）を参照してください。

  その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

- 標準スタティック アイデンティティ NAT を設定する場合、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) real_ip real_ip
[netmask mask] [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
[norandomseq]
```

  両方の *real_ip* 引数に、同じ IP アドレスを指定します。

  その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

次のコマンドでは、外部からアクセスされたときに、スタティック アイデンティティ NAT を内部 IP アドレス（10.1.1.3）に対して使用します。

```
hostname(config)# static (inside,outside) 10.1.1.3 10.1.1.3 netmask 255.255.255.255
```

次のコマンドでは、内部からアクセスされたときに、スタティック アイデンティティ NAT を外部アドレス（209.165.201.15）に対して使用します。

```
hostname(config)# static (outside,inside) 209.165.201.15 209.165.201.15 netmask
255.255.255.255
```

次のコマンドで、サブネット全体をスタティックに対応付けます。

```
hostname(config)# static (inside,dmz) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
```

次のスタティック アイデンティティ ポリシー NAT の例で、ある宛先アドレスにアクセスするときにアイデンティティ NAT を使用し、別の宛先アドレスにアクセスするときには変換を使用する、単一実アドレスを示します。

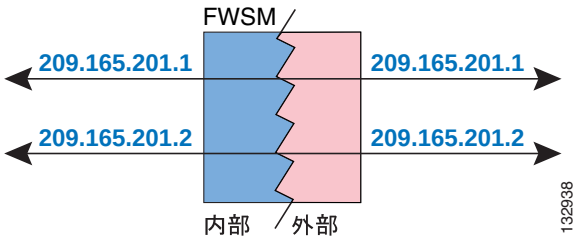
```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 10.1.2.27 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

NAT 除外の設定

NAT 除外ではアドレスを変換処理から除外して、実ホストとリモート ホストの両方で接続を開始できるようにします。NAT 除外では、（ポリシー NAT と同様）除外する実トラフィックを決定するときに実アドレスと宛先アドレスを指定できるので、アイデンティティ NAT を使用するよりも NAT 除外を使用する方がきめ細かい制御が行えます。ただし、NAT 除外はポリシー NAT とは異なり、アクセス リストに指定されたポートを考慮しません。アクセス リストのポートを考慮するには、スタティック アイデンティティ NAT を使用します。

図 12-25 に、一般的な NAT 除外の使用例を示します。

図 12-25　NAT 除外



（注）　NAT 除外の設定を削除しても、その NAT 除外を使用する既存の接続は影響を受けません。これらの接続を削除するには、**clear local-host** コマンドを入力します。

NAT 除外を設定するには、次のコマンドを入力します。

```
hostname(config)# nat (real_interface) 0 access-list acl_name [outside] [[tcp]
tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

access-list コマンドを使用してアクセス リストを作成します(「拡張アクセス リストの追加」[p.10-7]を参照)。このアクセス リストには、**permit** ACE と **deny** ACE の両方を含めることができます。アクセス リストで実ポートと宛先ポートを指定しないでください。NAT 除外では、ポートは考慮されません。NAT 除外では **inactive** または **time-range** キーワードも考慮されず、すべての ACE が NAT 除外コンフィギュレーションに対してアクティブであるとみなされます。

その他のオプションについては、「ダイナミック NAT または PAT の設定」（p.12-23）を参照してください。

デフォルトでは、このコマンドは内部から外部へのトラフィックを除外します。外部から内部へのトラフィックに対して NAT をバイパスする場合は、新たに **nat** コマンドを追加して **outside** を入力し、NAT インスタンスを外部 NAT として識別します。外部インターフェイスに対してダイナミック NAT を設定して、他のトラフィックを除外する場合は、外部 NAT 除外を使用できます。

任意の宛先アドレスにアクセスするときに、内部ネットワークを適用除外にする場合は、次のコマンドを入力します。

```
hostname(config)# access-list EXEMPT permit ip 10.1.2.0 255.255.255.0 any
hostname(config)# nat (inside) 0 access-list EXEMPT
```

DMZ ネットワークにダイナミック外部 NAT を使用し、他の DMZ ネットワークを除外するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
hostname(config)# access-list EXEMPT permit ip 10.1.3.0 255.255.255.0 any
hostname(config)# nat (dmz) 0 access-list EXEMPT
```

2 つの異なる宛先アドレスにアクセスするときに、内部ネットワークを適用除外にする場合は、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 0 access-list NET1
```

NAT の例

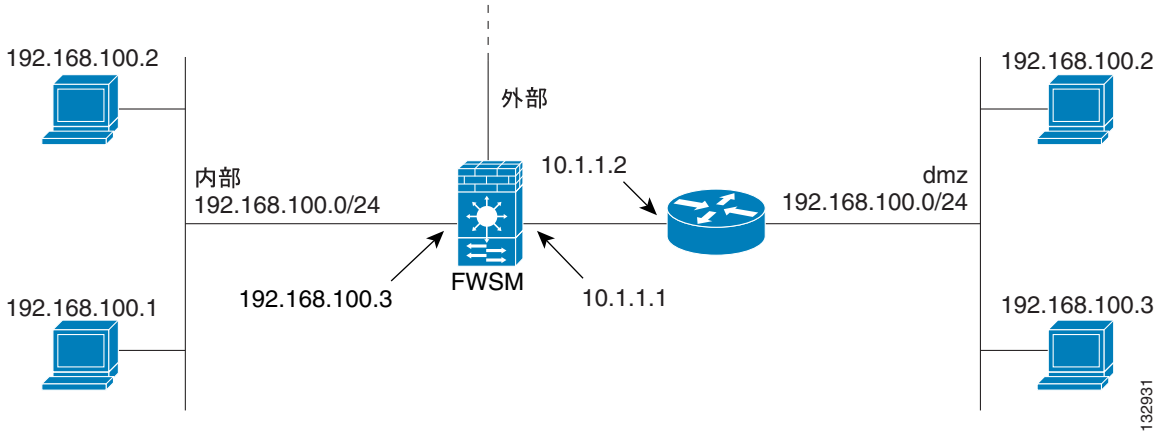
ここでは、一般的な NAT ソリューションの使用例を示します。内容は次のとおりです。

- 重複したネットワーク（p.12-36）
- ポートのリダイレクション（p.12-37）

重複したネットワーク

図 12-26 では、FWSM はアドレス範囲の重複する 2 つのプライベート ネットワークを接続します。

図 12-26　重複したネットワークで外部 NAT を使用する場合



2 つのネットワークで重複するアドレス スペース（192.168.100.0/24）が使用されていますが、各ネットワーク上のホストは（アクセス リストの許可に従って）相互に通信しなければなりません。NAT を使用しない場合、内部ネットワーク上のホストが重複した DMZ ネットワーク上のホストにアクセスしようとしても、パケットは FWSM を通過できません。パケットの宛先アドレスが内部ネットワーク上のアドレスであるとみなされるためです。さらに、内部ネットワーク上の別のホストがその宛先アドレスを使用している場合は、そのホストがパケットを受信します。

この問題を解決するには、NAT を使用して重複しないアドレスを提供します。双方向にアクセスできるようにするには、両方のネットワークにスタティック NAT を使用します。内部インターフェイスから DMZ 上のホストへのアクセスだけを許可する場合は、内部アドレスにダイナミック NAT を使用し、アクセス先の DMZ アドレスにスタティック NAT を使用します。この例は、スタティック NAT を示しています。

この 2 つのインターフェイスにスタティック NAT を設定するための手順は、次のとおりです。DMZ 上のネットワーク 10.1.1.0/24 は変換されません。

ステップ 1　内部から DMZ にアクセスするときに、内部の 192.168.100.0/24 を 10.1.2.0/24 に変換するため、次のコマンドを入力します。

```
hostname(config)# static (inside,dmz) 10.1.2.0 192.168.100.0 netmask 255.255.255.0
```

ステップ 2　DMZ から内部にアクセスするときに、DMZ のネットワーク 192.168.100.0/24 を 10.1.3.0/24 に変換するため、次のコマンドを入力します。

```
hostname(config)# static (dmz,inside) 10.1.3.0 192.168.100.0 netmask 255.255.255.0
```

ステップ 3　FWSM が DMZ ネットワークへのトラフィックを正しくルーティングできるように、次のスタティック ルートを設定します。

```
hostname(config)# route dmz 192.168.100.128 255.255.255.128 10.1.1.2 1
hostname(config)# route dmz 192.168.100.0 255.255.255.128 10.1.1.2 1
```

FWSM にはすでに、内部ネットワーク用に接続されたルートがあります。FWSM はこれらのスタティック ルートを使用して、ネットワーク 192.168.100.0/24 宛てのトラフィックを DMZ インターフェイスから 10.1.1.2 のゲートウェイ ルータに送信します（接続されたルートとまったく同じネットワークを指定してスタティック ルートを作成することはできないので、ネットワークを 2 つに分割する必要があります）。または、DMZ トラフィックにデフォルト ルートなど、より一般的なルートを使用することもできます。

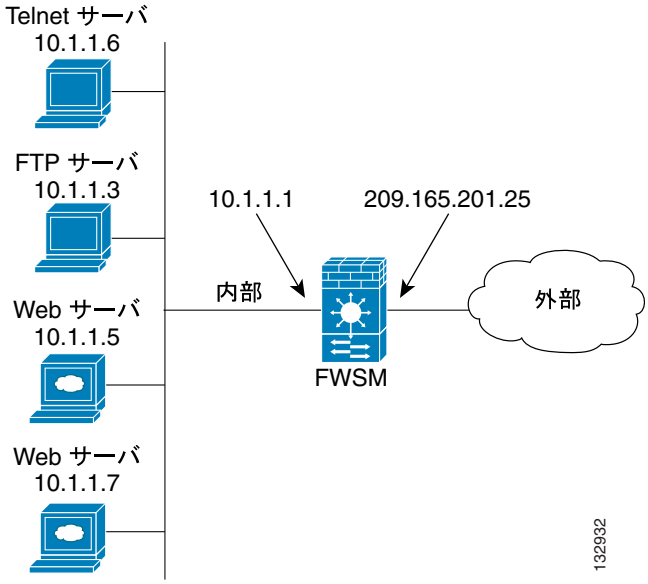
DMZ ネットワーク上のホスト 192.168.100.2 が内部ネットワーク上のホスト 192.168.100.2 への接続を開始しようとすると、次のイベントが発生します。

1. DMZ ホスト 192.168.100.2 が IP アドレス 10.1.2.2 にパケットを送信します。
2. FWSM がこのパケットを受信すると、送信元アドレスが 192.168.100.2 から 10.1.3.2 に変換されます。
3. その後、宛先アドレスが 10.1.2.2 から 192.168.100.2 に変換されたあとで、パケットが転送されます。

ポートのリダイレクション

図 12-27 に、ポートのリダイレクション機能が役立つ一般的なネットワーク例を示します。

図 12-27　スタティック PAT を使用するポートのリダイレクション



ここで説明する設定では、外部ネットワーク上のホストに対してポート リダイレクションが次のように実行されます。

- IP アドレス 209.165.201.5 に対する Telnet 要求は、10.1.1.6 にリダイレクトされます。
- IP アドレス 209.165.201.5 に対する FTP 要求は、10.1.1.3 にリダイレクトされます。
- FWSM の外部 IP アドレス 209.165.201.5 に対する HTTP 要求は、10.1.1.5 にリダイレクトされます。
- PAT アドレス 209.165.201.15 に対する HTTP ポート 8080 要求は、10.1.1.7 のポート 80 にリダイレクトされます。

この実装を行うための設定手順は、次のとおりです。

ステップ 1　内部ネットワークに PAT を設定するため、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
hostname(config)# global (outside) 1 209.165.201.15
```

ステップ 2　209.165.201.5 への Telnet 要求を 10.1.1.6 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.5 telnet 10.1.1.6 telnet
netmask 255.255.255.255
```

ステップ 3　IP アドレス 209.165.201.5 への FTP 要求を 10.1.1.3 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.5 ftp 10.1.1.3 ftp netmask
255.255.255.255
```

ステップ 4　FWSM の外部インターフェイス アドレスへの HTTP 要求を 10.1.1.5 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp interface www 10.1.1.5 www netmask
255.255.255.255
```

ステップ 5　PAT アドレス 209.165.201.15 へのポート 8080 の HTTP 要求を 10.1.1.7 のポート 80 にリダイレクトするため、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 209.165.201.15 8080 10.1.1.7 www netmask
255.255.255.255
```