CHAPTER 34

ネットワーク オブジェクト NAT の設定

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT* ルールと見なされます。ネットワーク オブジェクト NAT は、単一の IP アドレス、アドレス範囲、またはサブネットの NAT を設定するための迅速かつ容易な方法です。ネットワーク オブジェクトを設定したら、このオブジェクトのマッピング アドレスを識別できます。

この章では、ネットワーク オブジェクト NAT を設定する方法について説明します。この章は、次の項で構成されています。

（注） NAT の機能の詳細については、第 33 章「NAT に関する情報」を参照してください。

ネットワーク オブジェクト NAT に関する情報

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはありません。したがって、宛先 X に向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換されるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.33-15）を参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT の順序の詳細については、「NAT ルールの順序」（P.33-20）を参照してください。

ネットワーク オブジェクト NAT のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ネットワーク オブジェクト NAT の前提条件

コンフィギュレーションによっては、必要に応じてマッピング アドレスをインラインで設定したり、マッピング アドレスの別のネットワーク オブジェクトまたはネットワーク オブジェクト グループを作成したりできます（**object network** コマンドまたは **object-group network** コマンド）。ネットワーク オブジェクト グループは、非連続的な IP アドレス範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。ネットワーク オブジェクトまたはグループを作成するには、「ネットワーク オブジェクトとグループの設定」（P.18-2）を参照してください。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」の項も参照してください。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。**any** は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。「NAT と IPv6」（P.33-13）も参照してください。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。

- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

その他のガイドライン

- 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などのように、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待機せずに新しい NAT コンフィギュレーション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できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、**clear xlate** コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- 複数の NAT ルールで同じマッピングされたオブジェクトまたはグループを使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）では、IP アドレスではなく、**interface** キーワードを使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。
- NAT または PAT のアプリケーション インスペクションの制限については、第 46 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト設定」（P.46-4）を参照してください。

デフォルト設定

- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- アイデンティティ NAT のデフォルト動作ではプロキシ ARP がイネーブルになっており、他のスタティック NAT ルールと一致します。必要に応じて、プロキシ ARP をディセーブルにできます。詳細については、「NAT パケットのルーティング」（P.33-21）を参照してください。
- オプションのインターフェイスを指定した場合は、ASA は NAT コンフィギュレーションを使用して出力インターフェイスを決定しますが、代わりに常時ルート ルックアップを使用するように指定することもできます。詳細については、「NAT パケットのルーティング」（P.33-21）を参照してください。

ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を設定する方法について説明します。次の項目を取り上げます。

マッピング アドレスのネットワーク オブジェクトの追加

ダイナミック NAT の場合は、マッピングされたアドレスに対してオブジェクトまたはグループを使用する必要があります。他のタイプの NAT の場合は、インライン アドレスを使用することも、この項の説明に従ってオブジェクトまたはグループを作成することもできます。ネットワーク オブジェクトまたはグループの設定の詳細については、「ネットワーク オブジェクトとグループの設定」（P.18-2）を参照してください。

ガイドライン

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインライン アドレスを入れることができます。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- 拒否されるマッピング IP アドレスについては、「ガイドラインと制限事項」（P.34-2）を参照してください。
- ダイナミック NAT：
  - インライン アドレスは使用できません。ネットワーク オブジェクトまたはグループを設定する必要があります。
  - オブジェクトまたはグループにサブネットを入れることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。

  - マッピングされたネットワーク オブジェクトに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォール バックとして使用されます。
- ダイナミック PAT（隠蔽）：
  - オブジェクトを使用する代わりに、任意でインライン ホスト アドレスを設定するか、またはインターフェイス アドレスを指定できます。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを入れることはできません。オブジェクトは、1 つのホスト、または範囲（PAT プールの場合）を定義する必要があります。グループ（PAT プールの場合）には、複数のホストと範囲を入れることができます。
- スタティック NAT またはポート変換を使用するスタティック NAT：
  - オブジェクトを使用する代わりに、インライン アドレスを設定するか、またはインターフェイス アドレスを指定できます（ポート変換を使用するスタティック NAT の場合）。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにホスト、範囲、またはサブネットを入れることができます。
- アイデンティティ NAT
  - オブジェクトを使用する代わりに、インライン アドレスを設定できます。
  - オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。

手順の詳細

コマンド	目的

object network *obj_name*
{**host** *ip_address* | **range** *ip_address_1 ip_address_2* | **subnet** *subnet_address netmask*}
 	
例：
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
	ネットワーク オブジェクト（IPv4 または IPv6）を追加します。

コマンド	目的
object-group network *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*} **例：** hostname(config)# object network TEST hostname(config-network-object)# range 10.1.1.1 10.1.1.70 hostname(config)# object network TEST2 hostname(config-network-object)# range 10.1.2.1 10.1.2.70 hostname(config-network-object)# object-group network MAPPED_IPS hostname(config-network)# network-object object TEST hostname(config-network)# network-object object TEST2 hostname(config-network)# network-object host 10.1.2.79	ネットワーク オブジェクト グループ（IPv4 または IPv6）を追加します。

ダイナミック NAT の設定

この項では、ダイナミック NAT のネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.33-7）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	マッピングされたアドレスに対して、ネットワーク オブジェクトまたはネットワーク グループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.34-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** hostname(config)# object network my-host-obj1	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**] **例：** hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface	オブジェクト IP アドレスの**ダイナミック NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.34-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：次のものとしてマッピング IP アドレスを指定します。 – 既存のネットワーク オブジェクト（ステップ 1 を参照） – 既存のネットワーク オブジェクト グループ（ステップ 1 を参照） • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、インターフェイス PAT のフォール バックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（トランスペアレント モードでは、**interface** を指定できません）。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.33-23）を参照してください。

例

次の例では、外部アドレス 10.2.2.1 ～ 10.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。ネットワーク 10.76.11.0 内のホストは、まず nat-range1 プール（10.10.10.10 ～ 10.10.10.20）にマッピングされます。nat-range1 プール内のすべてのアドレスが割り当てられたら、pat-ip1 アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。万一、PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20
```

```
hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

次の例では、ダイナミック NAT とダイナミック PAT バックアップを使用して IPv6 ホストを IPv4 に変換するように設定します。内部ネットワーク 2001:DB8::/96 上のホストは最初に、IPv4_NAT_RANGE プール（209.165.201.30 ～ 209.165.201.1）にマッピングされます。IPv4_NAT_RANGE プール内のすべてのアドレスが割り当てられた後は、IPv4_PAT アドレス（209.165.201.31）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）のネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック PAT」（P.33-8）を参照してください。

ガイドライン

PAT プールの場合：

- 可能な場合は、実際の送信元ポート番号がマッピング ポートに使用されます。ただし、実際のポートが使用できない場合は、デフォルトでマッピング ポートは実際のポート番号と同じポートの範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。（8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます（1024 ～ 65535、または 1 ～ 65535）。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールに対する拡張 PAT の場合：

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションのリストについては、第 46 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト設定」（P.46-4）を参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート トランスレーション ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンド ロビン方式の場合：

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。**注**：この「スティッキ性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトまたはグループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.34-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** `hostname(config-network-object)# range 10.1.1.1 10.1.1.90`	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] | **interface** [**ipv6**]} [**interface** [**ipv6**]] [**dns**] **例：** hostname(config-network-object)# nat (any,outside) dynamic interface	オブジェクト IP アドレスの**ダイナミック PAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.34-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン ホスト アドレス。 – ホスト アドレスとして定義される既存のネットワーク オブジェクト（ステップ 1 を参照）。 – **pat-pool**：複数のアドレスを含む、既存のネットワーク オブジェクトまたはグループ。 – **interface**：（ルーテッド モードのみ）マッピング インターフェイスの IP アドレスは、マッピング アドレスとして使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。 • PAT プールについて、次のオプションの 1 つ以上を指定できます。 – ラウンド ロビン：**round-robin** キーワードは、PAT プールのラウンド ロビン アドレス割り当てをイネーブルにします。ラウンド ロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンド ロビン方式は、最初のアドレス、次に 2 つめのアドレスというように使用するために戻る前にプールの各 PAT アドレスからアドレス/ポートを割り当てます。 （続き）

コマンド	目的
	（続き） – 拡張 PAT：**extended** キーワードは、拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。 – フラット範囲：**flat** キーワードを指定すると、ポートを割り当てるときに 1024 ～ 65535 のポート範囲全体を使用できるようになります。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 • インターフェイス PAT のフォール バック：（任意）**interface** キーワードは、プライマリ PAT アドレスの後に入力されたときにインターフェイス PAT のフォール バックをイネーブルにします。プライマリ PAT アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。（トランスペアレント モードでは、**interface** を指定できません）。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.33-23）を参照してください。

例

次の例では、アドレス 10.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

次の例では、外部インターフェイス アドレスの背後に 192.168.2.0 ネットワークを隠蔽するダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
```

```
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

次の例では、ダイナミック PAT と PAT プールを使用して内部 IPv6 ネットワークを外部 IPv4 ネットワークに変換するように設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

スタティック NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。詳細については、「スタティック NAT」（P.33-3）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトまたはグループを作成します。	「マッピング アドレスのネットワーク オブジェクトの追加」（P.34-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	NAT を設定するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** `hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0`	新しいネットワーク オブジェクトを作成する場合は、変換する**実際の** IP アドレス（IPv4 または IPv6）を定義します。

	コマンド	目的
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] **例：** `hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS service tcp 80 8080`	オブジェクト IP アドレスの**スタティック NAT** を設定します。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング IP アドレスを次のものとして指定できます。 – インライン IP アドレス。マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。 – 既存のネットワーク オブジェクトまたはグループ（ステップ 1 を参照）。 – **interface**：（ポート変換を設定したスタティック NAT のみ、ルーテッド モード）このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**service** キーワードも必ず設定します 通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。「スタティック NAT」（P.33-3）を参照してください。 • ネットツーネット：（任意）NAT 46 の場合は、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。 • DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。「DNS および NAT」（P.33-23）を参照してください。**service** キーワードを指定した場合、このオプションは使用できません • ポート変換：（ポート変換を設定したスタティック NAT のみ）**tcp** または **udp** および実際のポートとマッピング ポートを指定します。ポート番号または予約済みポートの名前（**ftp** など）のいずれかを入力できます。 • No Proxy ARP：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.33-21）を参照してください。

例

次の例では、内部にある実際のホスト 10.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

次の例では、内部にある実際のホスト 10.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 2.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、10.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を設定したスタティック NAT を設定します。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

次の例では、内部 IPv4 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

次の例では、内部 IPv6 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

アイデンティティ NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。詳細については、「アイデンティティ NAT」（P.33-10）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意）マッピング アドレスのためのネットワーク オブジェクトを作成します。	オブジェクトには、変換するアドレスと同じものが含まれている必要があります。「マッピング アドレスのネットワーク オブジェクトの追加」（P.34-4）を参照してください。
ステップ 2	**object network** *obj_name* **例：** `hostname(config)# object network my-host-obj1`	アイデンティティ NAT を実行するネットワーク オブジェクトを設定するか、既存のネットワーク オブジェクトについてオブジェクト ネットワーク コンフィギュレーション モードを開始します。このネットワーク オブジェクトの名前は、マッピングされたネットワーク オブジェクトとは異なります（ステップ 1 を参照）。両方に同じ IP アドレスが含まれていても、このようになります。

	コマンド	目的
ステップ 3	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **例：** hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	新しいネットワーク オブジェクトを作成する場合は、実行するアイデンティティ NAT の変換先となる実際の IP アドレス（IPv4 または IPv6）を定義します。ステップ 1 でマッピング アドレスのネットワーク オブジェクトを設定した場合、これらのアドレスは一致する必要があります。
ステップ 4	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**] **例：** hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS	オブジェクト IP アドレスの**アイデンティティ NAT** を設定します。 **（注）** 特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。「その他のガイドライン」（P.34-3）を参照してください。 次のガイドラインを参照してください。 • インターフェイス：（トランスペアレント モードの場合に必須）実際のインターフェイスおよびマッピング インターフェイスを指定します。コマンドには、丸カッコを含める必要があります。ルーテッド モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定しない場合、すべてのインターフェイスが使用されます。インターフェイスの 1 つまたは両方に **any** キーワードを指定することもできます。 • マッピング IP アドレス：マッピング アドレスと実際のアドレスの両方に同じ IP アドレスを設定するようにしてください。次のいずれかを使用します。 – ネットワーク オブジェクト：実際のオブジェクトと同じ IP アドレスを含めます（ステップ 1 を参照）。 – インライン IP アドレス：マッピング ネットワークのネットマスクまたは範囲は、実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲で定義されている場合、マッピング アドレスとして 10.1.1.1 を指定するには、マッピングされた範囲に 10.1.1.1 ～ 10.1.1.6 が含まれます。 • No Proxy ARP：マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「マッピング アドレスとルーティング」（P.33-21）を参照してください。 • ルート ルックアップ：（ルーテッド モードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「出力インターフェイスの決定」（P.33-23）を参照してください。

例

次の例では、インラインのマッピング アドレスを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

次の例では、ネットワーク オブジェクトを使用して、ホスト アドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

Per-Session PAT ルールの設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。Per-Session PAT と Multi-Session PAT の違いの詳細については、「Per-Session PAT と Multi-Session PAT」（P.33-9）を参照してください。

デフォルト

デフォルトでは、次のルールがインストールされます。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

（注）　これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

手順の詳細

コマンド	目的
xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port* **例：** `hostname(config)# xlate per-session deny tcp any4 209.165.201.3 eq 1720`	許可または拒否ルールを作成します。このルールはデフォルト ルールの上に置かれますが、他の手動作成されたルールよりは下です。ルールは必ず、適用する順序で作成してください。 変換元と変換先の IP アドレスについては、次のように設定できます。 • **host** *ip_address* : IPv4 ホスト アドレスを指定します。 • *ip_address mask* : IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address*/*prefix-length* : IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any4** および **any6** : **any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。 *operator* では、変換元または変換先で使用されるポート番号の条件を指定します。使用できる演算子は、次のとおりです。 • lt : より小さい • gt : より大きい • eq : 等しい • neq : 等しくない • range : 値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`

例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

ネットワーク オブジェクト NAT のモニタリング

オブジェクト NAT をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show nat	各 NAT ルールのヒットを含む NAT の統計情報を表示します。
show nat pool	割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。

コマンド	目的

show running-config nat	NAT コンフィギュレーションを表示します。
	（注） NAT コンフィギュレーションは、**show running-config object** コマンドを使用して表示できません。**nat** コマンドで作成されていないオブジェクトまたはオブジェクト グループを参照することはできません。**show** コマンド出力での転送または循環参照を回避するために、**show running-config** コマンドは **object** コマンドを 2 回表示します。1 回目は、IP アドレスが定義される場所、2 回目は **nat** コマンドが定義される場所で表示されます。このコマンド出力によって、オブジェクト、オブジェクト グループ、NAT の順に定義されることが保証されます。例：
	`hostname# show running-config`
	`...`
	`object network obj1`
	`  range 192.168.49.1 192.150.49.100`
	`object network obj2`
	`  object 192.168.49.100`
	`object network network-1`
	`  subnet <network-1>`
	`object network network-2`
	`  subnet <network-2>`
	`object-group network pool`
	`  network-object object obj1`
	`  network-object object obj2`
	`...`
	`object network network-1`
	`  nat (inside,outside) dynamic pool`
	`object network network-2`
	`  nat (inside,outside) dynamic pool`

show xlate	現在の NAT セッション情報を表示します。

ネットワーク オブジェクト NAT の設定例

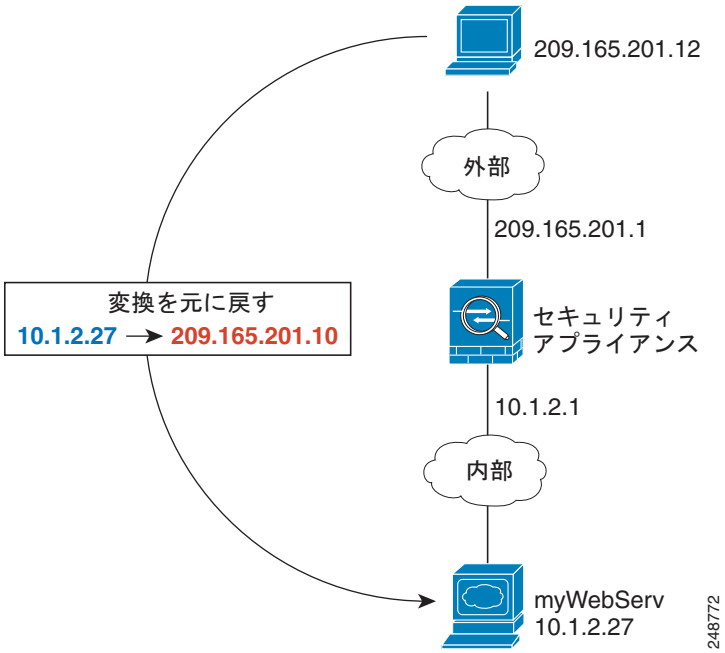
この項では、次の設定例を示します。

- 「内部 Web サーバへのアクセスの提供（スタティック NAT）」（P.34-19）
- 「内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）」（P.34-19）
- 「複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ」（P.34-21）
- 「FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）」（P.34-22）
- 「マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）」（P.34-23）
- 「マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）」（P.34-25）
- 「マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）」（P.34-26）

内部 Web サーバへのアクセスの提供（スタティック NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です （図 34-1 を参照）。

図 34-1　内部 Web サーバのスタティック NAT



ステップ 1　内部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
```

ステップ 2　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

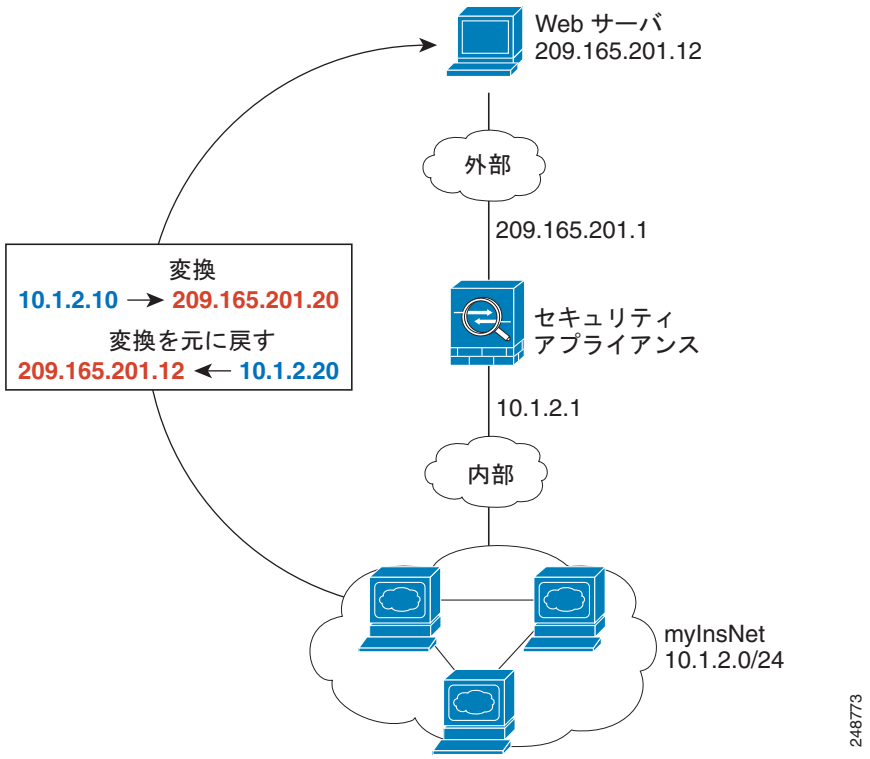
ステップ 3　オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます （図 34-2 を参照）。

図 34-2　内部のダイナミック NAT、外部 Web サーバのスタティック NAT



ステップ 1　内部アドレスに変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

ステップ 2　内部ネットワークのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 3　内部ネットワークのダイナミック NAT をイネーブルにします。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

ステップ 4　外部 Web サーバのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
```

ステップ 5　Web サーバのアドレスを定義します。

```
hostname(config-network-object)# host 209.165.201.12
```

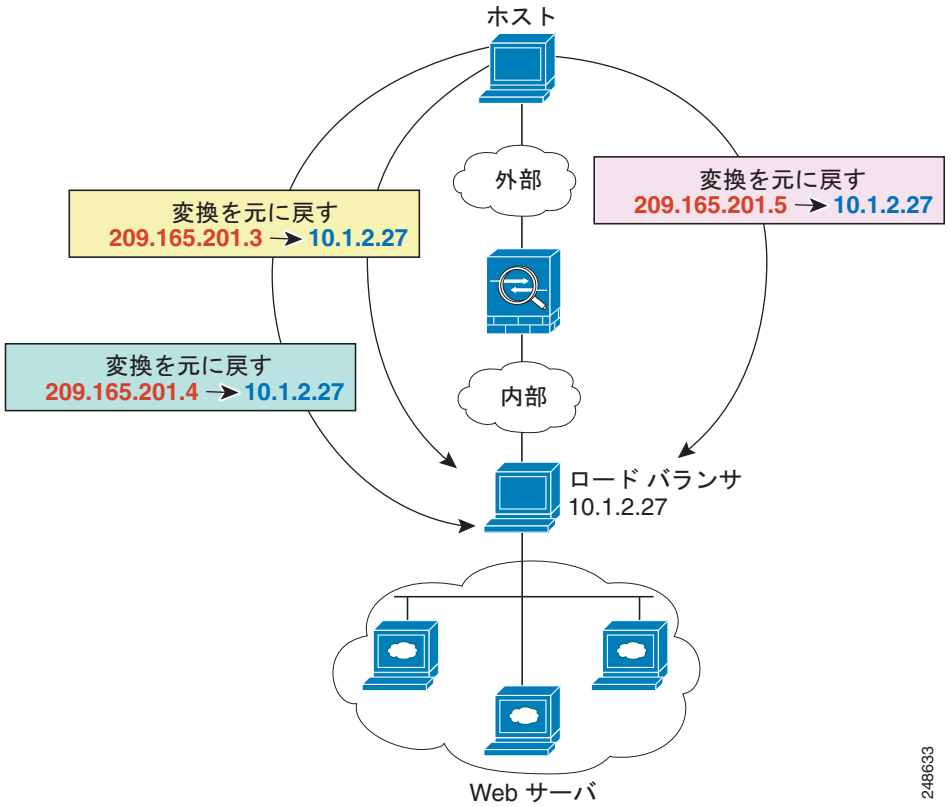
ステップ 6　Web サーバのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。（図 34-3 を参照）。

図 34-3　内部ロード バランサのスタティック NAT（1 対多）



ステップ 1　ロード バランサをマッピングするアドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

ステップ 2　ロード バランサのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myLBHost
```

ステップ 3　ロード バランサのアドレスを定義します。

```
hostname(config-network-object)# host 10.1.2.27
```

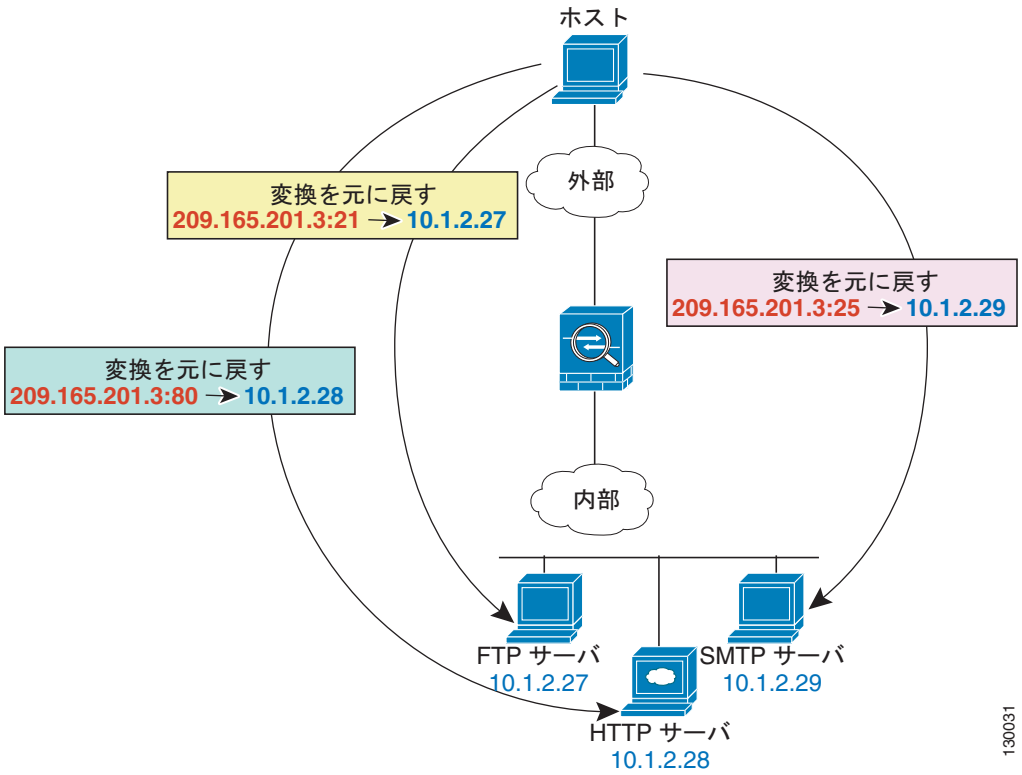
ステップ 4　ロード バランサのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。実際にはこれらのサーバは、実際のネットワーク上の異なるデバイスですが、各サーバに対して、異なるポートでも同じマッピング IP アドレスを使用するというポート変換を設定したスタティック NAT ルールを指定できます。（図 34-4 を参照）。

図 34-4　ポート変換を設定したスタティック NAT



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

ステップ 2　FTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を FTP サーバに設定します。

```
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

ステップ 3　HTTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network HTTP_SERVER
```

ステップ 4　HTTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を HTTP サーバに設定します。

```
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

ステップ 5　SMTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network SMTP_SERVER
```

ステップ 6　SMTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を SMTP サーバに設定します。

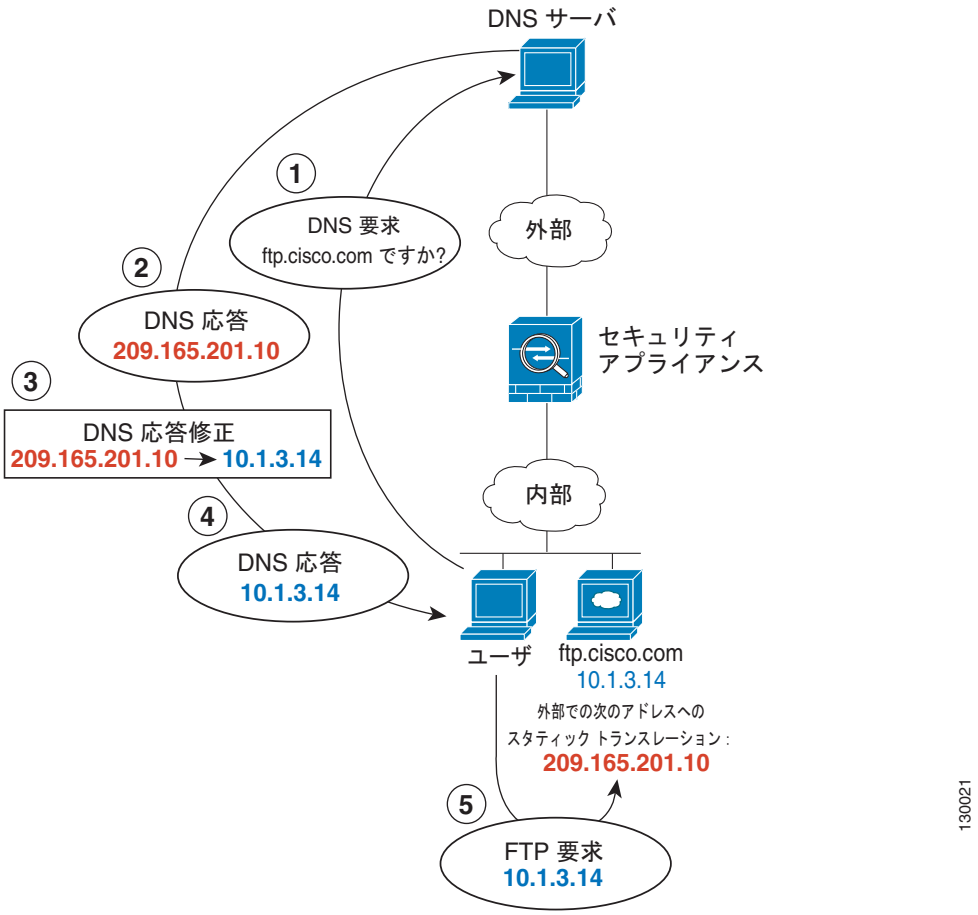
```
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）

たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します （図 34-5 を参照）。この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.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することを試みます。

図 34-5　　DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

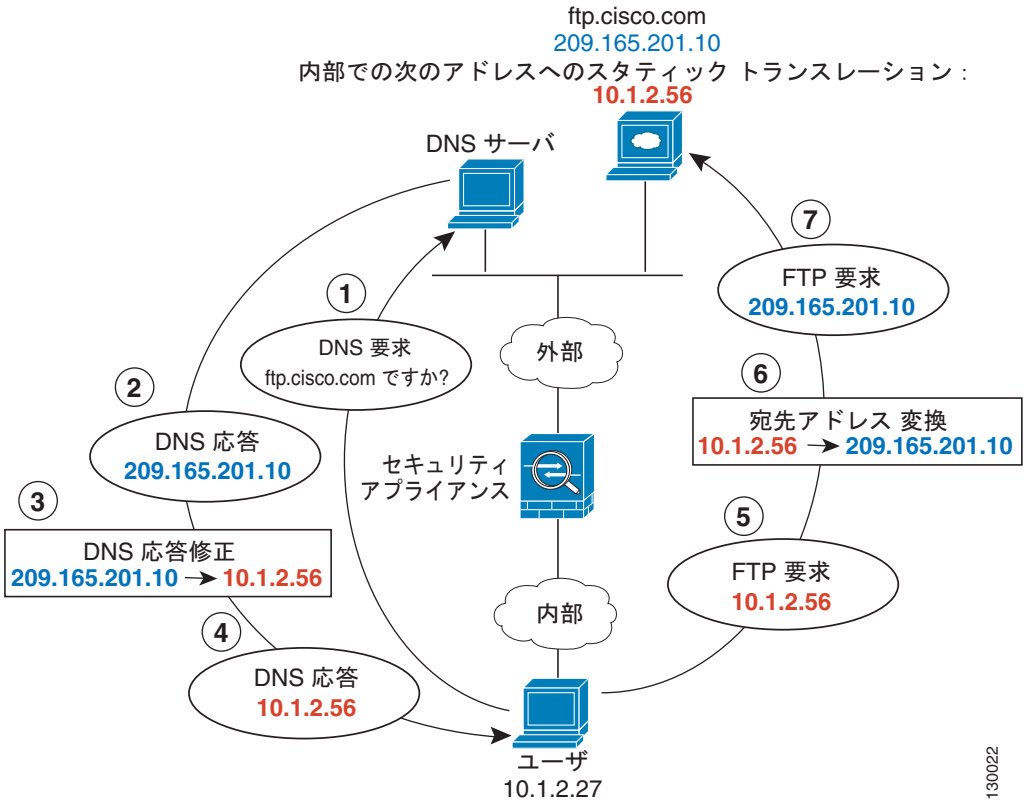
ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 10.1.3.14
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）

図 34-6 に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.201.10 を返します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

図 34-6　外部 NAT を使用する DNS 応答修正



ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

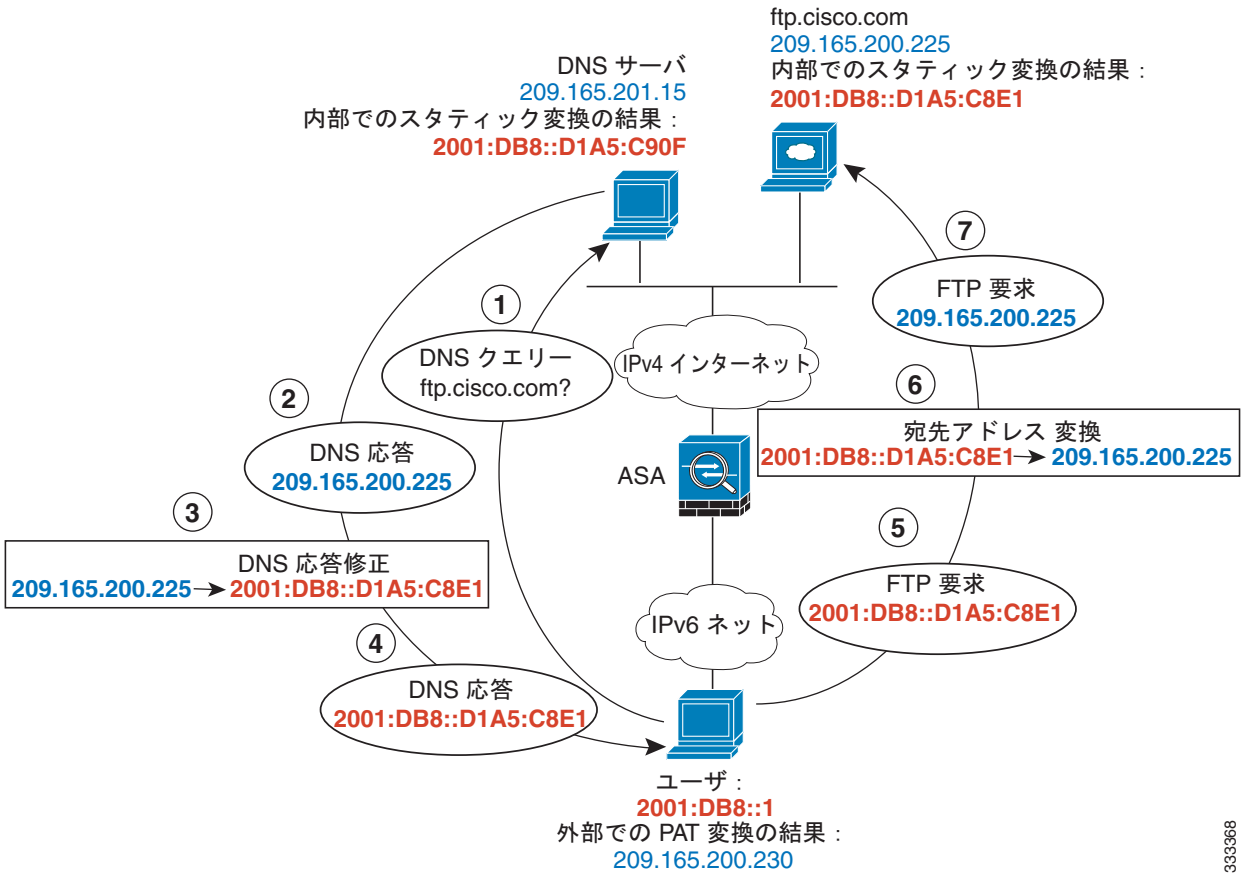
ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# host 209.165.201.10
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）

図 34-6 に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

図 34-7　外部 NAT を使用する DNS 応答修正



ステップ 1　FTP サーバのための、DNS 修正を設定したスタティック NAT を設定します。

a. FTP サーバ アドレスのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

b. FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT46 に対して net-to-net 方式を設定します。

```
hostname(config-network-object)# host 209.165.200.225
```

```
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

ステップ 2　DNS サーバの NAT を設定します。

a. DNS サーバ アドレスのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network DNS_SERVER
```

b. DNS サーバのアドレスを定義し、net-to-net 方式を使用してスタティック NAT を設定します。

```
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

ステップ 3　内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
```

ステップ 4　内部 IPv6 ネットワークのための PAT を設定します。

a. 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

```
hostname(config)# object network IPv6_INSIDE
```

b. IPv6 ネットワーク アドレスを定義し、PAT プールを使用するダイナミック NAT を設定します。

```
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

ネットワーク オブジェクト NAT の機能履歴

表 34-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 34-1　ネットワーク オブジェクト NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 **nat**（オブジェクト ネットワーク コンフィギュレーション モード）、**show nat**、**show xlate**、**show nat pool** コマンドが導入または変更されました。
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2) 以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。 **nat static** [**no-proxy-arp**] [**route-lookup**] コマンドが変更されました。
PAT プールおよびラウンド ロビン アドレス割り当て	8.4(2)/8.5(1)	1 つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。プールの次のアドレスを使用する前に、最初に PAT アドレスのすべてのポートを使用するのではなく、PAT アドレスのラウンド ロビン割り当てを必要に応じてイネーブルにすることもできます。これらの機能は、1 つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。 **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。

表 34-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 変更されたコマンドはありません。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの PAT ポートのフラットな範囲	8.4(3)	使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートには、小さい PAT プールのみがあります。 下位ポート範囲を使用するトラフィックが数多くある場合は、PAT プールを使用するときに、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。 **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*
PAT プールの拡張 PAT	8.4(3)	各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。 **nat dynamic** [**pat-pool** *mapped_object* [**extended**]] コマンドが変更されました。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 34-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用することが必要になる場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻すことが必要になることがあります。たとえば、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合です。 この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。 **（注）** ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。 • Cisco IPsec および AnyConnect クライアントのみがサポートされます。 • NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。 • ロードバランシングはサポートされません（ルーティングの問題のため）。 • ローミング（パブリック IP 変更）はサポートされません。 **nat-assigned-to-public-ip** *interface* コマンド（トンネル グループ一般属性コンフィギュレーション モード）が導入されました。

表 34-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
IPv6 用の NAT のサポート	9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。 **nat**（オブジェクト ネットワーク コンフィギュレーション モード）、**show nat**、**show nat pool**、**show xlate** の各コマンドが変更されました。
Per-session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。 Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。 Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。 デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。 **xlate per-session**、**show nat pool** の各コマンドが導入されました。