CHAPTER 13

Twice NAT の設定

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。この章では、Twice NAT の設定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 11 章「NAT に関する情報」を参照してください。

Twice NAT に関する情報

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、たとえば送信元アドレスが宛先 X に向かう場合は A に変換され、宛先 Y に向かう場合は B に変換されるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート アドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、このコマンドで、変換する*送信元*ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバ アドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換を設定したスタティック NAT のサービス オブジェクトを使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

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.11-13）を参照してください。

Twice NAT ルールは、NAT ルール テーブルのセクション 1 に追加されます。指定した場合には、セクション 3 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.11-18）を参照してください。

Twice NAT の前提条件

- 実際のアドレスとマッピング アドレスの両方について、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 グループを設定します（**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 アドレスの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、「オブジェクトとグループの設定」（P.8-1）を参照してください。
- ポート変換を設定したスタティック NAT の場合、TCP または UDP サービス オブジェクトを設定します（**object service** コマンド）。サービス オブジェクトを作成するには、「サービス オブジェクトの設定」（P.8-4）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

- 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 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。
- 複数のルールで同じオブジェクトを使用できます。
- 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 の場合は、IP アドレスの代わりに **interface** キーワードを使用します。
  - （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。
- インターフェイス PAT には IP アドレスがないため、内部セキュリティ プロファイル インターフェイスで設定できません。

デフォルト設定

- デフォルトでは、NAT テーブルのセクション 1 の最後にルールが追加されます。
- 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。
- 任意のインターフェイスを指定すると、ASA 1000V 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。アイデンティティ NAT では、デフォルトの動作は NAT コンフィギュレーションを使用するようになっていますが、オプションで常にルート ルックアップを代わりに使用することもできます。

Twice NAT の設定

この項では、Twice NAT を設定する方法について説明します。この項は、次の内容で構成されています。

- 「ダイナミック NAT の設定」（P.13-3）
- 「ダイナミック PAT（隠蔽）の設定」（P.13-8）
- 「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」（P.13-16）
- 「アイデンティティ NAT の設定」（P.13-21）

ダイナミック NAT の設定

この項では、ダイナミック NAT の Twice 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.11-9）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	ネットワーク オブジェクト： **object network** *obj_name* {**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} ネットワーク オブジェクト グループ： **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 MyInsNet hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	**実際の送信元**アドレスを設定します。 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 グループのいずれかを設定できます。詳細については、「オブジェクトの設定」（P.8-3）を参照してください。 すべてのトラフィックを変換する場合、この手順をスキップして、オブジェクトまたはグループを作成するのではなく、**any** キーワードを指定できます。
ステップ 2	ネットワーク オブジェクト： **object network** *obj_name* **range** *ip_address_1 ip_address_2* ネットワーク オブジェクト グループ： **object-group network** *grp_name* {**network-object** {**object** *net_obj_name* | **host** *ip_address*} | **group-object** *grp_obj_name*} **例：** hostname(config)# object network NAT_POOL hostname(config-network-object)# range 209.165.201.10 209.165.201.20	**マッピングされた送信元**アドレスを設定します。 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 グループのいずれかを設定できます。 ダイナミック NAT では、通常、大きいアドレスのグループが小さいグループにマッピングされます。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。 **（注）**　マッピングされたオブジェクトまたはグループは、サブネットを含むことはできません。 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.13-2）を参照してください。

	コマンド	目的

ステップ 3	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1`
	`hostname(config-network-object)# host 209.165.201.8`
		実際の宛先アドレスを設定します。
		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 グループのいずれかを設定できます。
		Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクトと Twice NAT の主な違い」（P.11-13）を参照してください。

ステップ 4	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1_mapped`
	`hostname(config-network-object)# host 10.1.1.67`
		マッピングされた宛先アドレスを設定します。
		宛先変換は、常にスタティックです。アイデンティティ NAT では、この手順をスキップして、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。
		宛先アドレスを変換する場合、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 グループを設定できます。スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.11-4）を参照してください。
		ポート変換を設定したスタティック インターフェイス NAT の場合、この手順をスキップして、マッピング アドレスのネットワーク オブジェクト / グループの代わりに **interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。

コマンド	目的
ステップ 5　（任意） **object service** *obj_name* 　**service** {**tcp** | **udp**} **destination** 　*operator port* **例：** hostname(config)# object service REAL_SVC hostname(config-service-object)# service tcp destination eq 80 hostname(config)# object service MAPPED_SVC hostname(config-service-object)# service tcp destination eq 8080	次のポートのサービス オブジェクトを設定します。 • 実際の宛先ポート • マッピングされた宛先ポート ダイナミック NAT では、ポート変換はサポートされません。しかし、*宛先*変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal」（**neq**）演算子は、サポートされていません。

	コマンド	目的
ステップ 6	**nat** [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface**]} [**destination static** {*mapped_obj* | **interface**} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC`	**ダイナミック NAT** を設定します。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：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。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。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます（「NAT ルールの順序」（P.11-18）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します（ステップ 1 を参照）。実際のインターフェイスからマッピングされたインターフェイスへのすべてのトラフィックを変換する場合、**any** キーワードを使用します。 – マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 2 を参照）。必要に応じて、次のフォールバック方式を設定できます。 インターフェイス PAT のフォール バック：**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。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。

コマンド	目的
	（続き） • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します（ステップ 4 を参照）。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。 – 実際のアドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 3 を参照）。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。 • 宛先ポート：（任意）マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、**service** キーワードを指定します（ステップ 5 を参照）。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。 • DNS：（オプション、送信元にのみ適用されるルール）**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）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.11-23）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

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 Twice 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.11-11）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。したがって、1024 未

満のポートに使用できるのは、小さな PAT プール 1 つだけです。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、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。

- 2 つの別個のルールで同じ PAT プール オブジェクトを使用する場合は、各ルールに対して同じオプションを指定してください。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 プールの拡張 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 19 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.19-3）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、PAT プールのアドレスを、ポート変換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、ポート変換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、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。**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 1000V 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	ネットワーク オブジェクト： **object network** *obj_name* {**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} ネットワーク オブジェクト グループ： **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 MyInsNet hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0	**実際の送信元**アドレスを設定します。 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 グループのいずれかを設定できます。詳細については、「オブジェクトの設定」（P.8-3）を参照してください。 すべてのトラフィックを変換する場合、この手順をスキップして、オブジェクトまたはグループを作成するのではなく、**any** キーワードを指定できます。
ステップ 2	ネットワーク オブジェクト： **object network** *obj_name* {**host** *ip_address* | **range** *ip_address_1 ip_address_2*} ネットワーク オブジェクト グループ： **object-group network** *grp_name* {**network-object** {**object** *net_obj_name* | **host** *ip_address*} | **group-object** *grp_obj_name*} **例：** hostname(config)# object network PAT_POOL1 hostname(config-network-object)# range 10.5.1.80 10.7.1.80 hostname(config)# object network PAT_POOL2 hostname(config-network-object)# range 10.9.1.1 10.10.1.1 hostname(config)# object network PAT_IP hostname(config-network-object)# host 10.5.1.79 hostname(config-network-object)# object-group network PAT_POOLS hostname(config-network)# network-object object PAT_POOL1 hostname(config-network)# network-object object PAT_POOL2 hostname(config-network)# network-object object PAT_IP	（変換先である）**マッピング** アドレスを指定します。1 つのアドレス、または PAT プールに対して複数のアドレスを設定できます。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 グループを設定できます。ネットワーク オブジェクト グループは、オブジェクトまたはインライン アドレス、あるいはその両方を含むことができます。**nat** コマンドのインライン値として 1 つの IP アドレスを入力する場合や、**interface** キーワードを指定してインターフェイス アドレスを使用する場合は、この手順をスキップすることもできます。 PAT プールとして使用するマッピング アドレスの場合、オブジェクト内または範囲を含むグループ内のすべてのアドレスが PAT アドレスとして使用されます。 **（注）**　オブジェクトまたはグループは、サブネットを含むことはできません。 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.13-2）を参照してください。 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、「オブジェクトの設定」（P.8-3）を参照してください。

	コマンド	目的

ステップ 3	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1`
	`hostname(config-network-object)# host 209.165.201.8`
		実際の宛先アドレスを設定します。
		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 グループのいずれかを設定できます。
		Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクトと Twice NAT の主な違い」（P.11-13）を参照してください。

ステップ 4	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1_mapped`
	`hostname(config-network-object)# host 10.1.1.67`
		マッピングされた宛先アドレスを設定します。
		宛先変換は、常にスタティックです。アイデンティティ NAT では、この手順をスキップして、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。
		宛先アドレスを変換する場合、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 グループを設定できます。スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.11-4）を参照してください。
		ポート変換を設定したスタティック インターフェイス NAT の場合、この手順をスキップして、マッピング アドレスのネットワーク オブジェクト / グループの代わりに **interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。

コマンド	目的
ステップ 5　（任意） **object service** *obj_name* 　**service** {**tcp** | **udp**} **destination** 　*operator port* **例：** hostname(config)# object service REAL_SVC hostname(config-service-object)# service tcp destination eq 80 hostname(config)# object service MAPPED_SVC hostname(config-service-object)# service tcp destination eq 8080	次のポートのサービス オブジェクトを設定します。 • **実際の宛先ポート** • **マッピングされた宛先ポート** ダイナミック PAT では、追加のポート変換はサポートされません。しかし、*宛先*変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal」（**neq**）演算子は、サポートされていません。

	コマンド	目的
ステップ 6	**nat** [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface**] | [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**interface**] | **interface**} [**destination static** {*mapped_obj* | **interface**} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,outside) source dynamic MyInsNet interface destination static Server1 Server1 description Interface PAT for inside addresses when going to server 1`	**ダイナミック PAT（隠蔽）**を設定します。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：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。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。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます（「NAT ルールの順序」（P.11-18）を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します（ステップ 1 を参照）。実際のインターフェイスからマッピングされたインターフェイスへのすべてのトラフィックを変換する場合、**any** キーワードを使用します。 – マッピング：次のいずれかを設定します。 - ネットワーク オブジェクト：ホスト アドレスを含むネットワーク オブジェクトを指定します（ステップ 2 を参照）。 - **pat-pool**：**pat-pool** キーワードおよびネットワーク オブジェクトまたは複数のアドレスを含むグループを指定します（ステップ 2 を参照）。 - **interface**：インターフェイス PAT だけを使用するように **interface** キーワード単独で指定します。PAT プールまたはネットワーク オブジェクトと一緒に指定した場合、**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。PAT 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。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。 （続き）

コマンド	目的
	（続き） 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。 -- 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。 -- フラットな範囲：**flat** キーワードは、ポートを割り当てる場合、1024 ～ 65535 ポート範囲全体の使用をイネーブルにします。変換のマッピング ポート番号を選択するときに、ASA 1000V 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。 （続き）

コマンド	目的
	（続き） • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します（ステップ 4 を参照）。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。 – 実際のアドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 3 を参照）。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。 • 宛先ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します（ステップ 5 を参照）。アイデンティティ ポート変換では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用します。 • DNS：（オプション、送信元にのみ適用されるルール）**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）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.11-23）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

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、Twice 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。スタティック NAT の詳細については、「スタティック NAT」（P.11-4）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	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	
	ネットワーク オブジェクト グループ：
	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 MyInsNet`
	`hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`
		実際の送信元アドレスを設定します。
		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 グループのいずれかを設定できます。詳細については、「オブジェクトの設定」（P.8-3）を参照してください。

ステップ 2	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	
	ネットワーク オブジェクト グループ：
	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 MyInsNet_mapped`
	`hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0`
		マッピングされた送信元アドレスを設定します。
		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 グループのいずれかを設定できます。スタティック NAT のマッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.11-4）を参照してください。
		ポート変換を設定したスタティック インターフェイス NAT の場合、この手順をスキップして、マッピング アドレスのネットワーク オブジェクト/グループの代わりに **interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。
		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.13-2）を参照してください。

	コマンド	目的

ステップ 3	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1`
	`hostname(config-network-object)# host 209.165.201.8`
		実際の宛先アドレスを設定します。
		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 グループのいずれかを設定できます。
		Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクトと Twice NAT の主な違い」（P.11-13）を参照してください。

ステップ 4	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1_mapped`
	`hostname(config-network-object)# host 10.1.1.67`
		マッピングされた宛先アドレスを設定します。
		宛先変換は、常にスタティックです。アイデンティティ NAT では、この手順をスキップして、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。
		宛先アドレスを変換する場合、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 グループを設定できます。スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.11-4）を参照してください。
		ポート変換を設定したスタティック インターフェイス NAT の場合、この手順をスキップして、マッピング アドレスのネットワーク オブジェクト / グループの代わりに **interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。

コマンド	目的
ステップ 5　（任意） **object service** *obj_name* 　**service** {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*] **例：** hostname(config)# object service REAL_SRC_SVC hostname(config-service-object)# service tcp source eq 80 hostname(config)# object service MAPPED_SRC_SVC hostname(config-service-object)# service tcp source eq 8080	次のポートのサービス オブジェクトを設定します。 • 送信元*または*宛先の実際のポート • 送信元*または*宛先のマッピングされたポート サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービス オブジェクトに送信元ポート*または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal」（**neq**）演算子は、サポートされていません。 たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

	コマンド	目的
ステップ 6	**nat** [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface**] [**destination static** {*mapped_obj* | **interface**} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**dns**] [**no-proxy-arp**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC`	**スタティック NAT** を設定します。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：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。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。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます。セクションの詳細については、「NAT ルールの順序」（P.11-18）を参照してください。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 送信元アドレス： – 実際のアドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 1 を参照）。 – マッピング アドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 2 を参照）。ポート変換を設定したスタティック インターフェイス NAT に限り、**interface** キーワードを指定できます。**interface** を指定する場合、**service** キーワードも設定します（この場合、サービス オブジェクトは送信元ポートだけを含む必要があります）。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。 • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します（ステップ 4 を参照）。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。 – 実際のアドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 3 を参照）。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

コマンド	目的
	（続き） • ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します（ステップ 5 を参照）。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。 • DNS：（オプション、送信元にのみ適用されるルール）**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）。**宛先**アドレスを設定する場合、**dns** キーワードは設定できません。詳細については、「DNS および NAT」（P.11-23）を参照してください。 • 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.11-20）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例

次に、ポート変換を使用するスタティック インターフェイス NAT の使用例を示します。外部にあるホストが、宛先ポート 65000 ～ 65004 を指定して外部インターフェイス IP アドレスに接続することにより、内部にある FTP サーバにアクセスします。トラフィックは、192.168.10.100:6500 ～ :65004 の内部 FTP サーバに変換されません。コマンドで指定した送信元アドレスとポートを変換するため、サービス オブジェクトには送信元ポートの範囲（宛先ポートではなく）を指定することに注意してください。宛先ポートは「any」です。スタティック NAT は双方向であるため、「送信元」および「宛先」を使用して一次的にコマンドのキーワードを扱うものであり、パケット内の実際の送信元および実際の宛

先のアドレスとポートは、パケットを送信するホストによって異なります。この例では、外部から内部への接続が発生しているため、FTP サーバの「送信元」アドレスとポートは、実際には発信元パケット内では宛先アドレスとポートになります。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

アイデンティティ NAT の設定

この項では、Twice 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。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」（P.11-12）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	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	
	ネットワーク オブジェクト グループ：
	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 MyInsNet`
	`hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`
		実際の送信元アドレスを設定します。
		
		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 グループのいずれかを設定できます。詳細については、「オブジェクトの設定」（P.8-3）を参照してください。
		
		これらは、アイデンティティ NAT を実行するアドレスです。すべてのアドレスに対してアイデンティティ NAT を実行する場合は、この手順を省略して、代わりに **any any** キーワードを使用できます。

	コマンド	目的

ステップ 2	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1`
	`hostname(config-network-object)# host 209.165.201.8`
		実際の宛先アドレスを設定します。
		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 グループのいずれかを設定できます。
		Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、「ネットワーク オブジェクトと Twice NAT の主な違い」（P.11-13）を参照してください。

ステップ 3	（任意）
	ネットワーク オブジェクト：
	object network *obj_name*
	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
	ネットワーク オブジェクト グループ：
	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 Server1_mapped`
	`hostname(config-network-object)# host 10.1.1.67`
		マッピングされた宛先アドレスを設定します。
		宛先変換は、常にスタティックです。アイデンティティ NAT では、この手順をスキップして、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。
		宛先アドレスを変換する場合、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 グループを設定できます。スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、「スタティック NAT」（P.11-4）を参照してください。
		ポート変換を設定したスタティック インターフェイス NAT の場合、この手順をスキップして、マッピング アドレスのネットワーク オブジェクト/グループの代わりに **interface** キーワードを指定できます。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。

	コマンド	目的

ステップ 4	（任意）
	object service *obj_name*
	service {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]
	
	例：
	`hostname(config)# object service REAL_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 80`
	
	`hostname(config)# object service MAPPED_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 8080`
		次のポートのサービス オブジェクトを設定します。
		• **送信元*または*宛先の実際のポート**
		• **送信元*または*宛先のマッピングされたポート**
		サービス オブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービス オブジェクトに送信元ポート*または*宛先ポートの*いずれか*を指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの*両方*を指定する必要がありますが、固定の送信元ポートはめったに使用されません。NAT では、TCP または UDP だけがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。「not equal」（**neq**）演算子は、サポートされていません。
		たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

	コマンド	目的
ステップ 5	**nat** [**(***real_ifc*,*mapped_ifc***)**] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface**} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*] **例：** `hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet destination static Server1 Server1`	アイデンティティ **NAT** を設定します。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：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。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。いずれかまたは両方のインターフェイスに **any** キーワードを指定することもできます。 • セクションおよび行：（任意）デフォルトでは、NAT ルールは、NAT テーブルのセクション 1 の末尾に追加されます。セクションの詳細については、「NAT ルールの順序」（P.11-18）を参照してください。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。 • 宛先アドレス：実際のアドレスとマッピング アドレスの両方にネットワーク オブジェクト、グループ、または **any** キーワードを指定します（ステップ 1 を参照）。 • 宛先アドレス（任意）： – マッピング アドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します（ステップ 3 を参照）。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービス オブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、*mapped_ifc* の外部インターフェイスを設定する必要があります。内部セキュリティ プロファイル インターフェイスではインターフェイス PAT はサポートされません。詳細については、「ポート変換を設定したスタティック インターフェイス NAT」（P.11-6）を参照してください。 – 実際のアドレス：異なるネットワーク オブジェクトまたはグループを指定します（ステップ 2 を参照）。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。

コマンド	目的
	（続き） • ポート：（任意）実際のサービス オブジェクトおよびマッピングされたサービス オブジェクトとともに、**service** キーワードを指定します（ステップ 4 を参照）。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービス オブジェクトの順序は、**service** *real_obj mapped_obj* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービス オブジェクトの順序は、**service** *mapped_obj real_obj* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。 • 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.11-20）を参照してください。 • ルート ルックアップ：（オプション、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.11-22）を参照してください。 • 非アクティブ：（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。 • 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

Twice NAT のモニタリング

Twice 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。
`show xlate`	現在の NAT セッション情報を表示します。

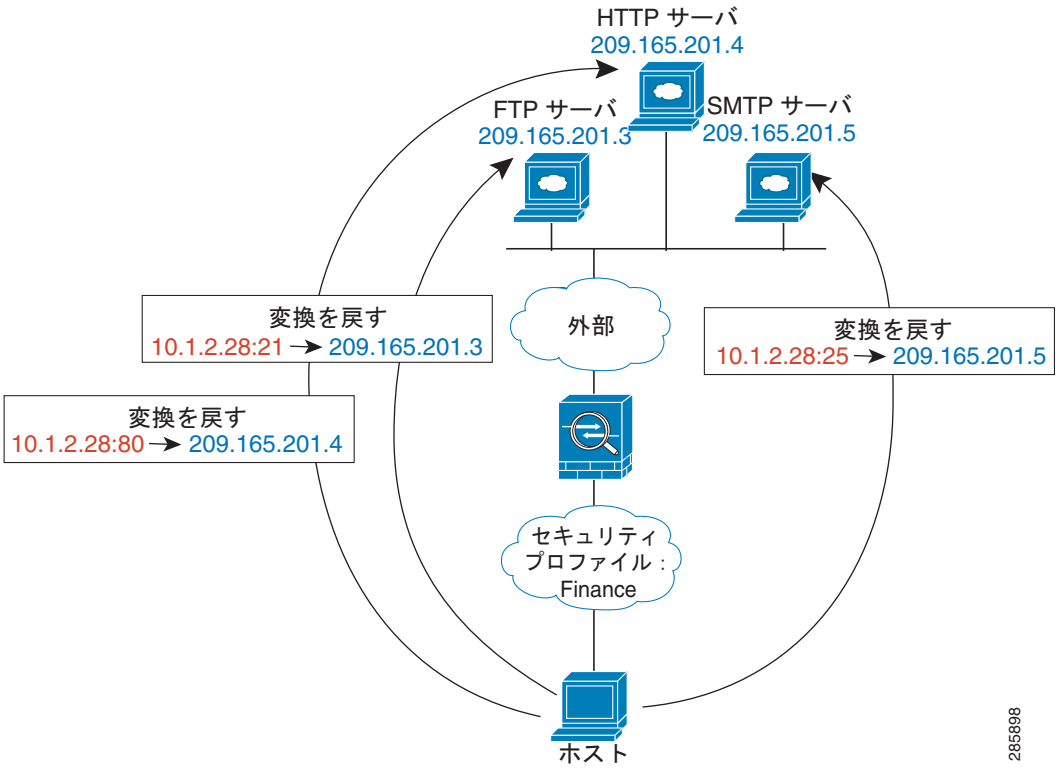
Twice NAT の設定例

この項では、次の設定例を示します。

宛先に応じて異なる変換（ダイナミック PAT）

図 13-1 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129: *ポート*に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130: *ポート*に変換されます。

図 13-1　異なる宛先アドレスを使用する Twice NAT



ステップ 1　内部ネットワークのネットワーク オブジェクトを追加します。

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

ステップ 2　外部ネットワーク 1 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network outsideNetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

ステップ 3　PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
```

```
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4　最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (Mktg,outside) source dynamic myInsideNetwork PATaddress1
destination static outsideNetwork1 outsideNetwork1
```

宛先アドレスは変換しないため、実際の宛先アドレスとマッピング宛先アドレスの両方に同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。

デフォルトでは、NAT ルールは NAT テーブルのセクション 1 の末尾に追加されます。NAT ルールのセクションおよび行番号の指定の詳細については、「ダイナミック PAT（隠蔽）の設定」（P.13-8）を参照してください。

ステップ 5　外部ネットワーク 2 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network outsideNetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

ステップ 6　PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

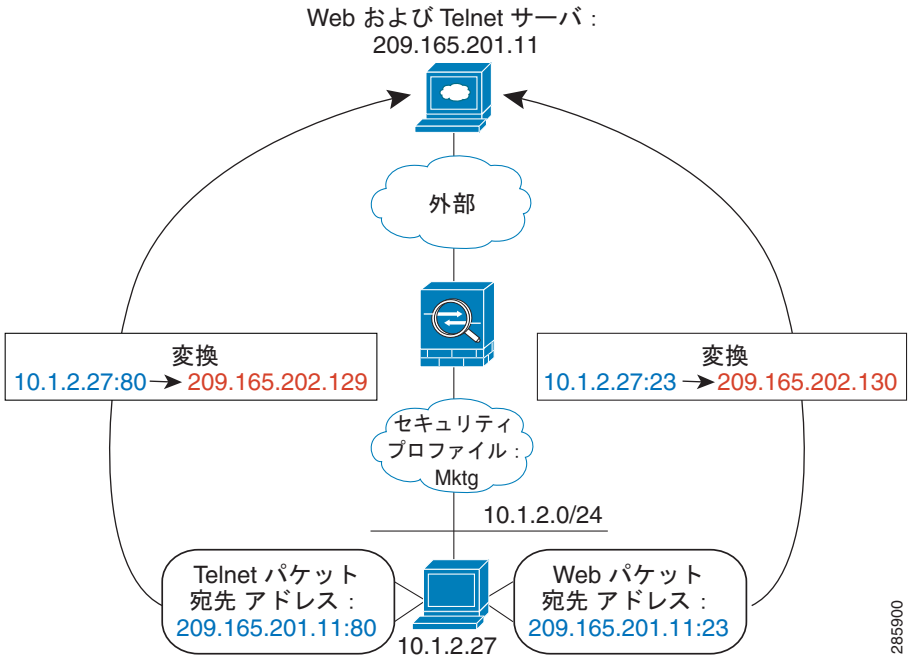
ステップ 7　2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (Mktg,outside) source dynamic myInsideNetwork PATaddress2
destination static outsideNetwork2 outsideNetwork2
```

宛先アドレスおよびポートに応じて異なる変換（ダイナミック PAT）

図 13-2 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129: *ポート*に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130: *ポート*に変換されます。

図 13-2　異なる宛先ポートを使用する Twice NAT



ステップ 1　内部ネットワークのネットワーク オブジェクトを追加します。

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

ステップ 2　Telnet/Web サーバのネットワーク オブジェクトを追加します。

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

ステップ 3　Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4　Telnet のサービス オブジェクトを追加します。

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

ステップ 5　最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (Mktg,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

宛先アドレスまたはポートを変換しないため、実際の宛先アドレスとマッピング宛先アドレスに同じアドレスを指定し、実際のサービスとマッピング サービスに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。

デフォルトでは、NAT ルールは NAT テーブルのセクション 1 の末尾に追加されます。NAT ルールのセクションおよび行番号の指定の詳細については、「ダイナミック PAT（隠蔽）の設定」（P.13-8）を参照してください。

ステップ 6　HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7　HTTP のサービス オブジェクトを追加します。

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

ステップ 8　2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (Mktg,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

Twice NAT の機能履歴

表 13-1 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 13-1　Twice 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
Twice NAT	8.3(1)	Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。 **nat**、**show nat**、**show xlate**、**show nat pool** コマンドが変更または導入されました。
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 よりも前の設定では、8.4(2) 以降への NAT 免除ルール（**nat 0 access-list コマンド**）の移行には、プロキシ ARP をディセーブルにし、ルート ルックアップを使用するために、**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りました。8.3(2) および 8.4(1) に移行するために使用した **unidirectional** キーワードは、それ以降の移行に使用されません。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。**unidirectional** キーワードは削除されました。 **nat source static** [**no-proxy-arp**] [**route-lookup**] コマンドが変更されました。

表 13-1　Twice 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
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 source dynamic** [**pat-pool** *mapped_object* [**round-robin**]] コマンドが変更されました。
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。 any コマンドを変更できませんでした。 *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 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 source 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。*

表 13-1　Twice 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
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 source 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。*
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、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などに、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 アドレスに戻す場合があります。 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 1000V 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。 次のコマンドが導入されました。 **nat-assigned-to-public-ip** *interface*（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）。