



n

- [nac-authentication-server-group \(廃止\)](#) (3 ページ)
- [nac-policy \(廃止\)](#) (5 ページ)
- [nac-settings \(廃止\)](#) (7 ページ)
- [name \(ダイナミック フィルタ ブラックリストまたはホワイトリスト\)](#) (9 ページ)
- [name \(グローバル\)](#) (13 ページ)
- [nameif](#) (16 ページ)
- [names](#) (18 ページ)
- [name-separator \(pop3s、imap4s、smtps\) \(廃止\)](#) (20 ページ)
- [name-server](#) (22 ページ)
- [nat \(グローバル\)](#) (25 ページ)
- [nat \(オブジェクト\)](#) (41 ページ)
- [nat \(VPN ロード バランシング\)](#) (53 ページ)
- [nat-assigned-to-public-ip](#) (55 ページ)
- [nat-rewrite](#) (58 ページ)
- [nbns-server](#) (60 ページ)
- [neighbor \(ルータ EIGRP\)](#) (62 ページ)
- [neighbor \(ルータ OSPF\)](#) (64 ページ)
- [neighbor activate](#) (66 ページ)
- [neighbor advertise-map](#) (68 ページ)
- [neighbor advertisement-interval](#) (71 ページ)
- [neighbor default-originate](#) (73 ページ)
- [neighbor description](#) (75 ページ)
- [neighbor disable-connected-check](#) (77 ページ)
- [neighbor distribute-list](#) (79 ページ)
- [neighbor ebgp-multihop](#) (81 ページ)
- [neighbor fall-over bfd \(ルータ BGP\)](#) (83 ページ)
- [neighbor filter-list](#) (85 ページ)
- [neighbor ha-mode graceful-restart](#) (87 ページ)
- [neighbor local-as](#) (89 ページ)
- [neighbor maximum-prefix](#) (93 ページ)

- neighbor next-hop-self (95 ページ)
- neighbor password (97 ページ)
- neighbor prefix-list (100 ページ)
- neighbor remote-as (102 ページ)
- neighbor remove-private-as (105 ページ)
- neighbor route-map (108 ページ)
- neighbor send-community (110 ページ)
- neighbor shutdown (112 ページ)
- neighbor timers (114 ページ)
- neighbor transport (116 ページ)
- neighbor ttl-security (119 ページ)
- neighbor update-source (122 ページ)
- neighbor version (124 ページ)
- neighbor weight (126 ページ)
- nem (128 ページ)
- netmod (130 ページ)
- network (アドレス ファミリ) (132 ページ)
- network (ルータ EIGRP) (134 ページ)
- network (ルータ RIP) (136 ページ)
- network-acl (138 ページ)
- network area (140 ページ)
- network-object (142 ページ)
- network-service-member (144 ページ)
- nis address (146 ページ)
- nis domain-name (149 ページ)
- nisp address (152 ページ)
- nisp domain-name (155 ページ)
- nop (158 ページ)
- nsf cisco (160 ページ)
- nsf cisco helper (162 ページ)
- nsf ietf (164 ページ)
- nsf ietf helper (166 ページ)
- nt-auth-domain-controller (168 ページ)
- ntp authenticate (170 ページ)
- ntp authentication-key (172 ページ)
- ntp server (174 ページ)
- ntp trusted-key (176 ページ)
- num-packets (178 ページ)
- nve (180 ページ)
- nve-only (183 ページ)

nac-authentication-server-group (廃止)

ネットワーク アドミッション コントロールのポスチャ検証に使用される認証サーバーグループを識別するには、トンネルグループ一般属性コンフィギュレーション モードで **nac-authentication-server-group** コマンドを使用します。デフォルトのリモートアクセスグループから認証サーバーグループを継承するには、継承元となる代替のグループポリシーにアクセスし、このコマンドの **no** 形式を使用します。

nac-authentication-server-group *server-group*
no nac-authentication-server-group

構文の説明

server-group **aaa-server host** コマンドを使用して ASA に設定されたポスチャ検証サーバーグループの名前。この名前は、そのコマンドに指定された **server-tag** 変数に一致する必要があります。

コマンドデフォルト

このコマンドには引数またはキーワードはありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネルグループ一般属性コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース 変更内容

7.2(1) このコマンドが追加されました。

8.0(1) このコマンドは廃止されました。nac ポリシー nac フレームワーク コンフィギュレーション モードの **authentication-server-group** コマンドに置き換えられました。

使用上のガイドライン

NAC をサポートするように、少なくとも 1 つのアクセス コントロール サーバーを設定します。ACS グループの名前を指定するには、**aaa-server** コマンドを使用します。次に、その同じ名前をサーバーグループに使用して、**nac-authentication-server-group** コマンドを使用します。

例

次に、NAC ポスチャ検証に使用される認証サーバーグループとして `acs-group1` を識別する例を示します。

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

次に、デフォルトのリモートアクセスグループから認証サーバーグループを継承する例を示します。

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバーまたはグループのレコードを作成し、ホスト固有のAAAサーバー属性を設定します。
debug eap	EAP イベントのロギングをイネーブルにして、NAC メッセージをデバッグします。
debug eou	NAC メッセージングをデバッグするための EAP over UDP (EAPoUDP) イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループポリシーに対するネットワーク アドミッション コントロールをイネーブルにします。

nac-policy (廃止)



(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

シスコ ネットワーク アドミッション コントロール (NAC) ポリシーを作成し、または NAC ポリシーにアクセスし、ポリシーのタイプを指定するには、グローバルコンフィギュレーション モードで **nac-policy** コマンドを使用します。NAC ポリシーを構成から削除するには、このコマンドの **no** 形式を使用します。

nac-policy *nac-policy-name* **nac-framework**
no **nac-policy** *nac-policy-name* **nac-framework**

構文の説明

nac-policy-name NAC ポリシーの名前。最大 64 文字で NAC ポリシーの名前を指定します。
show running-config nac-policy コマンドは、セキュリティアプライアンスにすでに存在する各 NAC ポリシーの名前および構成を表示します。

nac-framework NAC フレームワークを使用して、リモートホストのネットワーク アクセスポリシーを提供することを指定します。ASA の NAC フレームワーク サービスを提供するには、シスコ アクセス コントロール サーバーがネットワークに存在している必要があります。

このタイプを指定した場合、プロンプトは現在のモードが設定 **nac** ポリシー **nac** フレームワーク コンフィギュレーション モードであることを示します。このモードでは、NAC フレームワーク ポリシーを設定できます。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース 変更内容

8.0(2) このコマンドが追加されました。

9.1(2) このコマンドは廃止されました。

使用上のガイドライン

グループポリシーに割り当てられる NAC アプライアンスごとにこのコマンドを一度使用します。次に、**nac-settings** コマンドを使用して、該当する各グループポリシーに NAC ポリシーを割り当てます。IPSec または Cisco AnyConnect VPN トンネルのセットアップ時に、ASA は使用中のグループポリシーに関連付けられた NAC ポリシーを適用します。

NAC ポリシーが 1 つ以上のグループポリシーにすでに割り当てられている場合、**no nac-policy name** コマンドを使用してその NAC ポリシーを削除できません。

例

次のコマンドでは、NAC フレームワーク ポリシーを **nac-framework1** という名前で作成し、そのポリシーにアクセスしています。

```
ciscoasa
(config)
# nac-policy nac-framework1 nac-framework
ciscoasa
(config-nac-policy-nac-framework)
```

次のコマンドでは、**nac-framework1** という名前の NAC フレームワーク ポリシーを削除しています。

```
ciscoasa
(config)
# no nac-policy nac-framework1
ciscoasa
(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
show running-config nac-policy	ASA 上の各 NAC ポリシーの構成を表示します。
show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
nac-settings	NAC ポリシーをグループポリシーに割り当てます。
clear configure nac-policy	グループポリシーに割り当てられているものを除き、すべての NAC ポリシーを実行コンフィギュレーションから削除します。

nac-settings (廃止)



(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC ポリシーをグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで **nac-settings** コマンドを実行します。

```
nac-settings { value nac-policy-name | none }
no nac-settings { value nac-policy-name | none }
```

構文の説明

nac-policy-name グループ ポリシーに割り当てられる NAC ポリシー。名前を付ける NAC ポリシーは、ASA の構成に存在している必要があります。**show running-config nac-policy** コマンドは、各 NAC ポリシーの名前および構成を表示します。

none グループ ポリシーから **nac-policy-name** を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから **nac-settings** 値を継承しません。

value 名前を付ける NAC ポリシーをグループ ポリシーに割り当てます。

コマンドデフォルト

このコマンドには引数またはキーワードはありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース 変更内容

8.0(2) このコマンドが追加されました。

9.1(2) このコマンドは廃止されました。

使用上のガイドライン **nac-policy** コマンドを使用してNACポリシーの名前とタイプを指定してから、このコマンドを使用して名前とタイプをグループポリシーに割り当てます。

show running-config nac-policy コマンドは、各NACポリシーの名前および構成を表示します。

NACポリシーをグループポリシーに割り当てると、ASAはそのグループポリシーのNACを自動的に有効にします。

例

次のコマンドでは、グループポリシーから *nac-policy-name* を削除しています。グループポリシーは、デフォルトのグループポリシーから *nac-settings* 値を継承します。

```
ciscoasa(config-group-policy)
# no nac-settings
ciscoasa(config-group-policy)
```

次のコマンドでは、グループポリシーから *nac-policy-name* を削除し、このグループポリシーに関してNACポリシーの使用をディセーブルにしています。グループポリシーは、デフォルトグループポリシーから *nac-settings* 値を継承しません。

```
ciscoasa(config-group-policy)
# nac-settings none
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
show running-config nac-policy	ASA 上の各 NAC ポリシーの構成を表示します。
show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPsecセッション、WebVPNセッション、およびNACセッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

name (ダイナミック フィルタ ブラックリストまたはホワイトリスト)

ドメイン名をボットネット トラフィック フィルタ ブラックリストまたはホワイトリストに追加するには、ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーションモードで **name** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。スタティック データベースを使用すると、ホワイトリストまたはブラックリストに追加するドメイン名または IP アドレスでダイナミック データベースを増強できます。

name *domain_name*
no name *domain_name*

構文の説明

domain_name ブラックリストに名前を追加します。このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリを追加できます。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック フィルタ ブラックリスト またはホワイト リスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
 ス

8.2(1) このコマンドが追加されました。

使用上のガイドライン

ダイナミック フィルタ ホワイトリストまたはブラックリスト コンフィギュレーションモードを開始した後、**address** コマンドおよび **name** コマンドを使用して、適切な名前としてホワイトリストに、または不適切な名前としてブラックリストにタグ付けするドメイン名または IP アドレス (ホストまたはサブネット) を手動で入力できます。

このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリストエントリと、最大 1000 個のホワイトリストエントリを追加できます。

スタティックデータベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を DNS ホストキャッシュに追加します (このアクションはバックグラウンドプロセスで、ASA の設定の続行に影響しません)。

ASA にドメイン名サーバーが設定されていない、あるいはドメイン名サーバーが利用できない場合は、代わりにボットネットトラフィック フィルタ スヌーピング (**inspect dns dynamic-filter-snooping** コマンド参照) を使用した DNS パケットインスペクションを有効にできます。DNS スヌーピングを使用している場合、感染したホストがスタティックデータベース内の名前に対して DNS 要求を送信すると、ASA は DNS パケットの中からそのドメイン名と関連 IP アドレスを見つけ出し、その名前と IP アドレスを DNS 逆ルックアップキャッシュに追加します。DNS 逆ルックアップキャッシュについては、**inspect dns dynamic-filter-snooping** コマンドを参照してください。

DNS ホスト キャッシュのエントリには、DNS サーバーから提供される存続可能時間 (TTL) 値があります。許容される最大 TTL 値は 1 日 (24 時間) です。DNS サーバーによって提供された TTL がこれより大きい場合は、TTL が 1 日以下に切り詰められます。

DNS ホストキャッシュの場合、エントリがタイムアウトすると、ASA がエントリの更新を定期的に要求します。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-l1ist)# name bad1.example.com
ciscoasa(config-l1ist)# name bad2.example.com
ciscoasa(config-l1ist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-l1ist)# dynamic-filter whitelist
ciscoasa(config-l1ist)# name good.example.com
ciscoasa(config-l1ist)# name great.example.com
ciscoasa(config-l1ist)# name awesome.example.com
ciscoasa(config-l1ist)# address 10.1.1.2
255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネットトラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネットトラフィックフィルタのDNSスヌーピングデータをクリアします。
clear dynamic-filter reports	ボットネットトラフィックフィルタのレポートデータをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。

コマンド	説明
show dynamic-filter dns-snoop	ボットネットトラフィックフィルタのDNSスヌーピングの概要を表示します。 detail キーワードを指定した場合は、実際のIP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネットサイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネットトラフィックフィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。
show running-config dynamic-filter	ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。

name (グローバル)

IP アドレスに名前を関連付けるには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。テキスト名の使用は無効にするが、構成からは削除しない場合は、このコマンドの **no** 形式を使用します。

```
name ip_address [ name [ description text ] ]
no name ip_address [ name [ description text ] ]
```

構文の説明

description (任意) IP アドレス名の説明を指定します。

ip_address 名前を付けるホストの IP アドレスを指定します。

name IP アドレスに割り当てられる名前を指定します。使用できる文字は、a～z、A～Z、0～9、ダッシュ、およびアンダースコアです。**name** は、63 文字以下である必要があります。また、**name** は数値で開始できません。

text 説明のテキストを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

7.0(4) このコマンドは、任意の説明を含めることができるように拡張されました。

8.3(1) **nat** コマンドまたは **access-list** コマンドでは名前付き IP アドレスを使用できなくなりました。代わりに **object network** 名を使用する必要があります。オブジェクトグループの **network-object** コマンドでは、**object network** 名を指定できますが、**name** コマンドで指定した名前付き IP アドレスも引き続き使用できます。

使用上のガイドライン

名前と IP アドレスとの関連付けを有効にするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に、まず **names** コマンドを使用する必要があります。name コマンドは、names コマンドの使用直後、かつ **write memory** コマンドの前に使用します。

name コマンドを使用すると、テキスト名でホストを識別し、テキスト文字列を IP アドレスにマッピングします。**no name** コマンドを使用すると、テキスト名の使用を無効化できますが、構成からテキスト名は削除されません。構成から名前前のリストをクリアするには、**clear configure name** コマンドを使用します。

name 値の表示を無効にするには、**no names** コマンドを使用します。

name コマンドと names コマンドは両方ともコンフィギュレーションに保存されます。

name コマンドは、ネットワーク マスクへの名前前の割り当てをサポートしません。たとえば、次のコマンドは拒否されます。

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```



(注) マスクを必要とするいずれのコマンドも、受け入れ可能なネットワークマスクとして名前前を処理できません。

例

次に、**names** コマンドを使用して、**name** コマンドの使用を有効にする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前前を使用できます。**no names** コマンドは、**name** コマンド値の表示を無効にします。後で **names** コマンドを使用すると、**name** コマンド値が再度表示されるようになります。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前前のリストをクリアします。

コマンド	説明
names	名前と IP アドレスの関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスの名前を指定するには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。インターフェイス名はインターフェイスタイプおよび ID (gigabitethernet0/1 など) ではなく ASA のすべてのコンフィギュレーション コマンドで使用されるため、トラフィックがインターフェイスを通過するためにはインターフェイス名が必要です。

nameif name
no nameif

構文の説明

name 最大 48 文字で名前を設定します。名前は大文字と小文字が区別されません。「Metrics_History」または「MH」という名前を使用しないでください。これらの名前を使用すると、ASDM はインターフェイスをダウン状態として表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、**nameif** コマンドを入力する前に、**vlan** コマンドで VLAN を割り当てる必要があります。

名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

例

次に、2つのインターフェイスにそれぞれ「inside」と「outside」という名前を設定する例を示します。

```

ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

名前と IP アドレスの関連付けを有効にするには、グローバル コンフィギュレーション モードで **names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。**name** 値の表示を無効にするには、**no names** コマンドを使用します。

names

no names

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

7.0(1) このコマンドが追加されました。

使用上のガイドライン

名前と IP アドレスとの関連付けを有効にするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に、まず **names** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドの使用直後、かつ **write memory** コマンドの前に使用します。

name 値の表示を無効にするには、**no names** コマンドを使用します。

name コマンドと **names** コマンドは両方ともコンフィギュレーションに保存されます。

例

次に、**names** コマンドを使用して、**name** コマンドの使用を有効にする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示を無効にします。後で **names** コマンドを使用すると、**name** コマンド値が再度表示されるようになります。

```
ciscoasa(config)# names
```

```

ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224

```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前の一覧をクリアします。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられた名前の一覧を表示します。
show running-config names	IP アドレスと名前の変換を表示します。

name-separator (pop3s、imap4s、smtps) (廃止)



(注) このコマンドをサポートする最後のリリースは、Version 9.5(1)でした。

電子メール、VPNユーザー名、パスワード間のデリミタとなる文字を指定するには、適用可能な電子メールプロキシモードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** 形式を使用します。

name-separator [*symbol*]

no name-separator

構文の説明

シンボ (任意) 電子メール、VPN ユーザー名、パスワードを区切る文字。使用できるのは、「@」(アットマーク)、「|」(パイプ)、「:」(コロン)、「#」(番号記号)、「,」(カンマ)、および「;」(セミコロン)です。

コマンド デフォルト

デフォルトは「:」(コロン)です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
pop3s	• 対応	• —	• 対応	• —	—
Imap4s	対応	—	対応	—	—
Smtps	対応	—	対応	—	—

コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

9.5(2) このコマンドは廃止されました。

使用上のガイドライン

名前の区切り文字には、サーバーの区切り文字とは異なる文字を使用する必要があります。

例

次に、番号記号 (#) を POP3S の名前区切り文字として設定する例を示します。

```
ciscoasa
```

```
(config)#  
pop3s  
ciscoasa(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバー名を区切ります。

name-server

ASA がホスト名を IP アドレスに解決できるように 1 つ以上の DNS サーバーを識別するには、DNS サーバー グループ コンフィギュレーションモードで **name-server** コマンドを使用します。1 つ以上のサーバーを削除するには、このコマンドの **no** 形式を使用します。



- (注) ASA では、機能に応じて DNS サーバーの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用を有効にした場合だけです。

```
name-server ip_address [ ip_address2 ] [ ... ] [ ip_address6 ] [ interface_name ]
no name-server ip_address [ ip_address2 ] [ ... ] [ ip_address6 ] [ interface_name ]
```

構文の説明

interface_name (オプション) ASA がサーバーとの通信に使用するインターフェイス名を指定します。インターフェイスを指定しなかった場合、ASA はデータルーティングテーブルを確認し、一致するものが見つからなければ、管理専用ルーティングテーブルを確認します。

ip_address DNS サーバーの IP アドレスを指定します。最大 6 つのアドレスを個別のコマンドとして指定するか、便宜上最大 6 つのアドレスをスペースで区切って 1 つのコマンドで指定できます。1 つのコマンドに複数のサーバーを入力した場合、ASA は各サーバーを個別のコマンドとして構成に保存します。ASA では、応答を受信するまで各 DNS サーバを順に試します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DNS サーバーグループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(1)	<code>interface_name</code> 引数が追加されました。

使用上のガイドライン

DNS ルックアップを有効にするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバーは使用されません。

ASA のデフォルトでは、発信要求に **dns server-group DefaultDNS** サーバーグループが使用されます。**dns-group** コマンドを使用してデフォルトのサーバーグループを変更できます。他のサーバーグループを特定のドメインに関連付けることができます。DNSサーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の `eng.cisco.com` サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、`eng.cisco.com` を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。PN トンネルグループ用に他の DNS サーバーグループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバーにアクセスするために DNS サーバーを使用する必要があります。たとえば、ボットネットトラフィックフィルタ機能では、ダイナミックデータベースサーバーにアクセスして、スタティックデータベースのエントリを解決するために DNS サーバーが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機能のアドレスの解決に DNS が必要です。他の機能 (**ping** コマンドや **traceroute** コマンドなど) では、**ping** や **traceroute** を実行する名前を入力できるため、ASA は DNS サーバーと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび **certificate** コマンドでもサポートされます。また、アクセスルールに完全修飾ドメイン名 (FQDN) ネットワークオブジェクトを使用するために、DNS サーバーを設定する必要もあります。

name-server のインターフェイスを指定しない場合、ASA はデータのルーティングテーブルをチェックします。ここで一致が見つからない場合は、管理専用のルーティングテーブルをチェックします。データインターフェイスを経由するデフォルトルートがある場合は、すべての DNS トラフィックがそのルートに一致するため、管理専用ルーティングテーブルが確認されることはありません。このシナリオでは、管理インターフェイスを経由してサーバーにアクセスする必要がある場合は常にインターフェイスを指定します。

例

次に、3つの DNS サーバーをグループ「DefaultDNS」に追加する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA では、次に示すように、別々のコマンドとして構成が保存されます。

```
name-server 10.1.1.1
```

```
name-server 10.2.3.4
name-server 192.168.5.5
```

さらに2つのサーバーを追加するには、それらを1つのコマンドとして入力します。

```
ciscoasa(config)# dns server-group
DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

複数のサーバーを削除するには、次のようにそれらのサーバーを複数のコマンドまたは1つのコマンドとして入力します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# no
name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
retries	ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数を指定します。
timeout	次の DNS サーバーを試行するまでに待機する時間を指定します。
show running-config dns server-group	既存の DNS サーバーグループコンフィギュレーションのうちの1つまたはすべてを表示します。

nat (グローバル)

IPv4、IPv6、または IPv4 と IPv6 の間 (NAT64) で Twice NAT を設定するには、グローバル コンフィギュレーションモードで **nat** コマンドを使用します。Twice NAT コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

スタティック NAT の場合：

```
nat [ ( real_ifc , mapped_ifc ) ] [ line | { after-auto [ line ] } ] source static { real_obj | any } {
mapped_obj | interface [ ipv6 ] | any } [ destination static { mapped_obj | interface [ ipv6 ] } {
real_obj | any } ] [ service { real_src_mapped_dest_svc_obj | any } mapped_src_real_dest_svc_obj
] [ net-to-net ] [ dns ] [ unidirectional | [ no-proxy-arp ] [ route-lookup ] ] [ inactive ] [ description
desc
```

```
no nat [ ( real_ifc , mapped_ifc ) ] [ line | { after-auto [ line ] } ] source static { real_obj | any } {
mapped_obj | interface [ ipv6 ] | any } [ destination static { mapped_obj | interface [ ipv6 ] } {
real_obj | any } ] [ service { real_src_mapped_dest_svc_obj | any } mapped_src_real_dest_svc_obj
] [ net-to-net ] [ dns ] [ unidirectional | [ no-proxy-arp ] [ route-lookup ] ] [ inactive ] [ description
desc
```

ダイナミック NAT の場合：

```
nat [ ( real_ifc , mapped_ifc ) ] [ line | { after-auto [ line ] } ] source dynamic { real_obj | any } {
mapped_obj | interface [ ipv6 ] | pat-pool mapped_obj [ round-robin ] [ extended ] [ flat [
include-reserve ] ] [ block-allocation ] [ interface [ ipv6 ] ] | interface [ ipv6 ] } [ destination
static { mapped_obj | interface [ ipv6 ] } { real_obj | any } ] [ service { mapped_dest_svc_obj
real_dest_svc_obj } ] [ dns ] [ unidirectional ] [ inactive ] [ description desc
```

```
no nat [ ( real_ifc , mapped_ifc ) ] [ line | { after-auto [ line ] } ] source dynamic { real_obj | any
} { mapped_obj | interface [ ipv6 ] | pat-pool mapped_obj [ round-robin ] [ extended ] [ flat [
include-reserve ] ] [ block-allocation ] [ interface [ ipv6 ] ] | interface [ ipv6 ] } [ destination
static { mapped_obj | interface [ ipv6 ] } { real_obj | any } ] [ service { mapped_dest_svc_obj
real_dest_svc_obj } ] [ dns ] [ unidirectional ] [ inactive ] [ description desc
```

または

```
no nat { line after-auto line }
```

構文の説明

(real_ifc,mapped_ifc)

(任意) 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。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は、すべてのインターフェイスが使用されます。また、インターフェイスのいずれかまたは両方に **any** キーワードを指定できます。ブリッジグループのメンバーインターフェイス (トランスペアレントモードまたはルーテッドモード) の場合、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。

Twice NAT は送信元アドレスと宛先アドレスの両方を変換するため、これらのインターフェイスを送信元インターフェイスと宛先インターフェイスとして考えると理解しやすくなります。

after-auto

NAT テーブルのセクション 3 の最後の、ネットワーク オブジェクト NAT ルールの後にルールを挿入します。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。 *line* 引数を使用して、セクション 3 の任意の場所にルールを挿入できます。

any

(任意) ワイルドカードの値を指定します。**any** の主な用途は次のとおりです。

- インターフェイス：インターフェイスのいずれかまたは両方に **any** を使用できます (**any,outside**) など)。インターフェイスを指定しない場合は、**any** がデフォルトです。ただし、**any** はブリッジグループのメンバーインターフェイスに適用されません。また、**any** はトランスペアレントモードで使用できません。
- スタティック NAT 送信元の実際の IP アドレスおよびマッピング IP アドレス：**source static any any** を指定して、すべてのアドレスに対してアイデンティティ NAT を有効にできます。
- ダイナミック NAT またはダイナミック PAT 送信元の実際のアドレス：**source dynamic any mapped_obj** を指定して、送信元インターフェイス上のすべてのアドレスを変換できます。

スタティック NAT の場合、実際の送信元ポートやマッピング宛先ポートに対しても、送信元または宛先の実際のアドレスに対しても、**any** を使用できますが (マッピングアドレスとしての **any** は除く)、使用すると、予期せぬ動作が発生する可能性があります。

- (注) 「any」トラフィックの定義 (IPv4 と IPv6) は、ルールによって異なります。ASA がパケットに対して NAT を実行するためには、そのパケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件により、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバーへのルールを設定しており、このサーバーが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングインターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

block-allocation	ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては round-robin と互換性がありますが、 extended または flat [include-reserve] オプションは使用できません。また、インターフェイス PAT のフォールバックを使用することもできません。
description desc	(任意) 最大 200 文字で説明を入力します。
destination	(任意) 宛先アドレスの変換を設定します。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、CLI 設定ガイドを参照してください。
dns	(任意) DNS 応答を変換します。DNS インспекションが有効になっていることを確認してください (inspect dns) (デフォルトでは有効)。 destination 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。このオプションを PAT ルールとともに使用することはできません。詳細については、CLI コンフィギュレーションガイドを参照してください。
dynamic	送信元アドレスのダイナミック NAT またはダイナミック PAT を設定します。宛先変換は、常にスタティックです。
extended	(オプション) PAT プールの拡張 PAT をイネーブルにします。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、 service ごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 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。

flat [include-reserve] include-reserve	<p>(任意、9.15 より前) 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 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、デフォルトでは、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) からマッピングポートが選択されます。下位の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。</p> <p>(9.15 以降) 9.15 以降、falt は PAT プールのデフォルト設定不可能な動作です。include-reserve キーワードは flat キーワードから独立しているため、予約済みポートの 1 ~ 1023 を PAT プールに含めることを引き続き選択できます。</p>
inactive	<p>(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。</p>
interface [ipv6]	<p>(任意) インターフェイス IP アドレスをマッピングアドレスとして使用します。ipv6 を指定した場合、インターフェイスの IPv6 アドレスが使用されます。</p> <p>ダイナミック NAT の送信元マッピングアドレスに対して、マッピングされたオブジェクトまたはグループに続けて interface キーワードを指定した場合、マッピングインターフェイスの IP アドレスは、他のすべてのマッピングアドレスがすでに割り当てられている場合にのみ使用されます。</p> <p>ダイナミック PAT の場合は、送信元マッピングアドレスに対して interface のみ指定できます。</p> <p>ポート変換を使用するスタティック NAT (送信元または宛先) の場合は、service キーワードも設定します。</p> <p>このオプションでは、<i>mapped_ifc</i> に特定のインターフェイスを設定する必要があります。</p> <p>このオプションは、トランスペアレントモードでは使用できません。ルーテッドモードでは、宛先インターフェイスがブリッジグループのメンバーの場合、このオプションを使用することはできません。</p>

<i>line</i>	<p>(任意) NAT テーブルのセクション 1 の任意の場所にルールを挿入します。デフォルトでは、セクション 1 の最後に NAT ルールが追加されます (詳細については、設定ガイドを参照してください)。その代わりに、セクション 3 に (ネットワークオブジェクト NAT ルールの後) ルールを追加する場合は、after-auto line オプションを使用します。</p>
<i>mapped_dest_svc_obj</i>	<p>(任意) ダイナミック NAT およびダイナミック PAT の場合は、マッピング宛先ポートを指定します (宛先の変換は常に固定です)。詳細については、service キーワードを参照してください。</p>
<i>mapped_object</i>	<p>マッピングされたネットワークオブジェクトまたはオブジェクトグループ (object network または object-group network) を指定します。</p> <p>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。</p> <p>(注) マッピングされたオブジェクトやグループにサブネットを含めることはできませんが、必要に応じて、このマッピングされた IP アドレスを異なるダイナミック NAT ルール間で共有できます。IPv4 アドレスと IPv6 アドレスの両方で 1 つのオブジェクトグループを使用することはできません。そのオブジェクトグループには、1 種類のアドレスのみを含める必要があります。</p> <p>ダイナミック PAT の場合は、単一のアドレスにマッピングするアドレスのグループを設定します。実際のアドレスを選択した単一のマッピングアドレスに変換するか、またはマッピングインターフェイスアドレスに変換できます。インターフェイスアドレスを使用する場合は、マッピングアドレスにネットワークオブジェクトを設定せずに、interface キーワードを使用します。</p> <p>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、CLI 設定ガイドを参照してください。</p>
<i>mapped_src_real_dest_svc_obj</i>	<p>(オプション) スタティック NAT の場合は、マッピング送信元ポート、実際の宛先ポート、またはその両方を指定します。詳細については、service キーワードを参照してください。</p>
net-to-net	<p>(任意) スタティック 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 番目に変換されます (以降も同様)。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。</p>

no-proxy-arp	(オプション) スタティック NAT の場合に、マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。
pat-pool mapped_obj	(オプション) アドレスの PAT プールをイネーブルにします。オブジェクトのすべてのアドレスが PAT アドレスとして使用されるようになります。ダイナミック NAT の場合、PAT プールをフォールバック方式として設定できます。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。
real_dest_svc_obj	(任意) ダイナミック NAT およびダイナミック PAT の場合は、実際の宛先ポートを指定します (宛先の変換は常に固定です)。詳細については、 service キーワードを参照してください。
real_ifc	(任意) パケットが発信される可能性のあるインターフェイスの名前を指定します。送信元オプション。送信元オプションの場合、 origin_ifc は実際のインターフェイスです。宛先オプションの場合、 real_ifc はマッピング インターフェイスです。
real_object	マッピングされた実際のネットワークオブジェクトまたはオブジェクトグループ (object network または object-group network) を指定します。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。
real_src_mapped_dest_svc_obj	(任意) スタティック NAT の場合は、実際の送信元ポート、マッピング宛先ポート、またはその両方を指定します。詳細については、 service キーワードを参照してください。
round-robin	(オプション) 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。デフォルトでは、次の PAT アドレスが使用される前に PAT アドレスのすべてのポートが割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
route-lookup	(オプション) ルーテッドモードのアイデンティティ NAT で、NAT コマンドで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します。NAT コマンドでインターフェイスを指定しない場合、デフォルトでルートルックアップが使用されます。

service	<p>(任意) ポート変換を指定します。</p> <ul style="list-style-type: none">• ダイナミック NAT およびダイナミック PAT : ダイナミック NAT およびダイナミック PAT では、(追加的な) 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 (object service) 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、両方含めた場合、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。• ポート変換を使用するスタティック NAT : 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 サーバーなど) 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。
<p>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。この場合、コマンドのサービスオブジェクトの順番は、service real_port mapped_port 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。この場合、サービスオブジェクトの順番は、service mapped_port real_port 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。「送信元」および「宛先」の用語については、「使用上のガイドライン」を参照してください。</p> <p>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。「not equal (等しくない) 」 (neq) 演算子はサポートされていません。</p> <p>NAT では、TCP または UDP のみ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なるようにします (両方とも TCP または両方とも UDP) 。</p>	
source	送信元アドレスの変換を設定します。
static	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 を設定します。

unidirectional

(任意) スタティック NAT の場合は、変換を送信元から宛先への単方向にします。宛先アドレスは、送信元アドレスへのトラフィックを開始できません。テストを目的とする場合は、このオプションが便利です。

コマンド デフォルト

- 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。
- *real_ifc* および *mapped_ifc* のデフォルト値は **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。
- (8.3(1)、8.3(2)、8.4(1)) アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。(8.4(2)以降) アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、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 を無効にできます。
- オプションのインターフェイスを指定する場合、ASA によって NAT 構成が使用されて、出力インターフェイスが決定されます。(8.3(1)～8.4(1)) 唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルートルックアップが使用されます。(8.4(2)以降) アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルートルックアップを常に使用するオプションがあります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴**リリース 変更内容**

- | | |
|--------|---|
| 8.3(1) | このコマンドが追加されました。 |
| 8.3(2) | 8.3 よりも前の NAT 免除コンフィギュレーションの移行時にスタティック アイデンティティ NAT ルールを生成する unidirectional キーワードが追加されました。 |

リリース 変更内容

- 8.4(2)/8.5(1) **no-proxy-arp**、**route-lookup**、**pat-pool**、および **round-robin** キーワードが追加されました。
- アイデンティティ NAT のデフォルトの動作が、プロキシ ARP をイネーブルにし、他のスタティック NAT ルールと照合するように変更されました。
- 8.3 よりも前の設定の場合、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 を無効にするキーワード **no-proxy-arp** およびルートルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードする場合、既存の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りました。**unidirectional** キーワードが削除されました。
-
- 8.4(3) **extended**、**flat**、および **include-reserve** キーワードが追加されました。
- ラウンドロビン割り当てで PAT プールを使用するとき、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。
- この機能は、8.5(1) では使用できません。
-
- 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。**interface ipv6** オプションと **net-to-net** オプションが追加されました。
-
- 9.5(1) **block-allocation** キーワードが追加されました。
-
- 9.15(1) **flat** キーワードが削除され、**include-reserve** キーワードは **flat** のサブパラメータではなくなりました。すべての PAT プールで 1024 ～ 65535 のフラットなポート範囲が使用されるようになり、オプションで予約済みポート (1 ～ 1023) を含めることができるようになりました。
-
- 9.17(1) 変換された (マッピングされた) 宛先として FQDN ネットワークオブジェクトを指定できます。
-

使用上のガイドライン 使用上のガイドライン

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 サーバーとして指定する場合には、Telnet サーバー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 サーバーアドレスを **source** 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、ポート変換が設定されたスタティック 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、CLI 設定ガイド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 順序の詳細については、CLI 設定ガイドを参照してください。

マッピングアドレスのガイドライン

マッピング IP アドレス プールに、次のアドレスを含めることはできません。

- 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した場合は、すべてのインターフェイス IP アドレスが無効になります。インターフェイス PAT（ルーテッドモードのみ）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。
- (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。

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、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** 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。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。

- ポート変換を使用するスタティック NAT の場合は、TCP または UDP のサービスオブジェクト (**object service** コマンド) を設定します。

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。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

PAT プールのガイドライン

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- (9.15 より前) 使用可能な場合、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多数ある場合は、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)。
- (9.15 以降) ポートは、1024 ~ 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

クラスタで動作する場合、アドレスごとに512個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも512です。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは1024 ~ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号 (1 ~ 1023) を必要とするときは、機能しない可能性があります。たとえば、ポート22 (SSH) を要求するアプリケーションは、1024 ~ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。
- ダイナミック NAT によってマッピングされた IP アドレスにオブジェクトグループを使用し、そのグループにホストアドレスを含める場合、PAT プールをイネーブルにすると、ホストアドレスの使用が PAT フォールバックからダイナミック NAT へと変更されます。
- (8.4(3) 以降、8.5(1) または 8.6(1) を除く) 2つの個別のルールで同じ 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ます。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 のガイドライン

- 多くのアプリケーション インспек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спекションのリストについては、設定ガイド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、ポート変換ルールを設定した別のスタティック 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のガイドライン

- (8.4(3)以降、8.5(1)または8.6(1)を除く) 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。
Note : この「粘着性」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最初の IP アドレスが使用されない場合があります。
- (8.4(2)、8.5(1)、および 8.6(1)) 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、ラウンドロビン割り当てのため、接続ごとに別の PAT アドレスが使用される可能性があります。この場合、ホストについて情報を交換する 2 つの Web サイト (e-コマースサイトと支払サイトなど) にアクセスするときに問題が発生する可能性があります。これらのサイトが、1 つのホストとして扱うべきものを 2 つの異なる IP アドレスと見なした場合、トランザクションは失敗することがあります。

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます (ルーテッドモードのみ)。次のベスト プラクティスを推奨します。インターフェイスが同じブリッジグループのメンバーの場合は NAT64/46 を実行できないことに注意してください。

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (Twice NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (Twice NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスは IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アド

レスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。

- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

一 例

次の例では、2つの異なるサーバーにアクセスする、10.1.2.0/24 ネットワーク上のホストがあります。ホストがサーバー 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:port に変換されます。ホストがサーバー 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:port に変換されます。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

次に、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ーにアクセスすると、実際のアドレスは 209.165.202.129:port 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ーにアクセスすると、実際のアドレスは 209.165.202.130:port に変換されます。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# service
tcp
destination eq telnet
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# service
```

```

tcp
destination eq http
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATAddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj

```

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 サーバーにアクセスします。トラフィックは、192.168.10.100:6500 ~ :65004 の内部 FTP サーバーに変換されません。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 サーバーの「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。

```

ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-object)# service tcp source range 65000 65004
ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-object)# host 192.168.10.100
ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE

```

次に、IPv4 209.165.201.1/27 ネットワークのサーバーおよび 203.0.113.0/24 ネットワークのサーバーにアクセスする場合の IPv6 内部ネットワーク 2001:DB8:AAAA::/96 のダイナミック NAT を設定する例を示します。

```

ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254
ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158
ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2

```

次に、外部 IPv6 Telnet サーバー 2001:DB8::23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、2001:DB8:AAAA::/96 ネットワーク上のサーバーへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```

ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200
ciscoasa(config)# object network TELNET_SVR

```

```

ciscoasa(config-network-object)# host 2001:DB8::23
ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23
ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS

```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーション (Twice NAT とネットワーク オブジェクト NAT の両方) を削除します。
show nat	NAT ポリシーの統計情報を表示します。
show nat pool	NAT プールに関する情報を表示します。
show running-config nat	NAT コンフィギュレーションを表示します。
show xlate	NAT セッション (xlate) 情報を表示します。
xlate block-allocation	PAT ポートブロック割り当ての特性を設定します。

nat (オブジェクト)

ネットワークオブジェクト用の NAT を設定するには、ネットワーク オブジェクト コンフィギュレーションモードで **nat** コマンドを使用します。NAT 構成を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック NAT およびダイナミック PAT の場合：

```
nat [ ( real_ifc , mapped_ifc ) ] dynamic { mapped_inline_host_ip [ interface [ ipv6 ] ] | [ mapped_obj ] [ pat-pool mapped_obj [ round-robin ] [ extended ] [ flat [ include-reserve ] ] [ block-allocation ] ] [ interface [ ipv6 ] ] } [ dns ]
```

```
no nat [ ( real_ifc , mapped_ifc ) ] dynamic { mapped_inline_host_ip [ interface [ ipv6 ] ] | [ mapped_obj ] [ pat-pool mapped_obj [ round-robin ] [ extended ] [ flat [ include-reserve ] ] [ block-allocation ] ] [ interface [ ipv6 ] ] } [ dns ]
```

スタティック NAT およびポート変換を使用するスタティック NAT の場合：

```
nat [ ( real_ifc , mapped_ifc ) ] static { mapped_inline_host_ip | mapped_obj | interface [ ipv6 ] } [ net-to-net ] [ dns | service { tcp | udp | sctp } real_port mapped_port ] [ no-proxy-arp ] [ route-lookup ]
```

```
no nat [ ( real_ifc , mapped_ifc ) ] static { mapped_inline_host_ip | mapped_obj | interface [ ipv6 ] } [ net-to-net ] [ dns | service { tcp | udp | sctp } real_port mapped_port ] [ no-proxy-arp ] [ route-lookup ]
```

構文の説明

(real_ifc,mapped_ifc) (任意) スタティック NAT の場合は、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は、すべてのインターフェイスが使用されます。また、インターフェイスのいずれかまたは両方に **any** キーワードを指定できます。コマンドには、丸カッコを含める必要があります。ブリッジグループのメンバーインターフェイス (トランスペアレントモードまたはルーテッドモード) の場合、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。

block-allocation

ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024～65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、**extended** または **flat [include-reserve]** オプションは使用できません。また、インターフェイス PAT のフォールバックを使用することもできません。

dns	(任意) DNS 応答を変換します。DNS インスペクションが有効になっていることを確認してください (inspect dns) (デフォルトでは有効)。(スタティック NAT の場合) service キーワードを指定する場合、このオプションは使用できません。このオプションを PAT ルールとともに使用することはできません。詳細については、CLI 設定ガイドを参照してください。
dynamic	ダイナミック NAT またはダイナミック PAT を設定します。
extended	(オプション) PAT プールの拡張 PAT をイネーブルにします。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、 <i>service</i> ごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 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。
flat [include-reserve] include-reserve	(任意、9.15 より前) 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します。変換のマッピングポート番号を選択するとき、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、デフォルトでは、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) からマッピングポートが選択されます。下位の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。 (9.15 以降) 9.15 以降、 flat は PAT プールのデフォルト設定不可能な動作です。 include-reserve キーワードは flat キーワードから独立しているため、予約済みポートの 1 ~ 1023 を PAT プールに含めることを引き続き選択できます。

interface [ipv6] (任意) ダイナミック NAT では、マッピング IP アドレス、オブジェクト、またはグループの後に続けて **interface** キーワードを指定した場合、マッピングインターフェイスの IP アドレスは、他のすべてのマッピングアドレスがすでに割り当てられている場合のみ使用されます。

ダイナミック PAT では、マッピング IP アドレス、オブジェクト、またはグループの代わりに **interface** キーワードを指定した場合、マッピング IP アドレスのインターフェイス IP アドレスを使用します。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。

ipv6 を指定した場合、インターフェイスの IPv6 アドレスが使用されます。

ポート変換を使用するスタティック NAT では、**service** キーワードを設定する場合にも **interface** キーワードを指定できます。

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。

透過モードでは **interface** を指定できません。ルーテッドモードでは、宛先インターフェイスがブリッジグループのメンバーの場合、このオプションを使用することはできません。

mapped_inline_host_ip **dynamic** を指定する場合は、ホスト IP アドレスを使用してダイナミック PAT を設定します。**static** を指定する場合、マッピングネットワークのネットマスクや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、ホストアドレスとして処理されます。範囲またはサブネットの場合、マッピングアドレスには、実際の範囲またはサブネット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。推奨されない多対 1 のマッピングが必要な場合は、インラインアドレスの代わりにホストネットワーク オブジェクトを使用します。

<i>mapped_obj</i>	<p>1つ以上のマッピング IP アドレスをネットワークオブジェクト (object network) またはオブジェクトグループ (object-group network) として指定します。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。</p> <p>ダイナミック NAT の場合は、オブジェクトまたはグループにサブネットを含めることはできません。必要に応じて、このマッピングされたオブジェクトを異なるダイナミック NAT ルール間で共有できます。拒否されるマッピング IP アドレスについては、「マッピングアドレスのガイドライン」を参照してください。</p> <p>スタティック NAT の場合、通常は、1対1のマッピングに対応するように、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。詳細については、CLI 設定ガイドを参照してください。</p>
<i>mapped_port</i>	(オプション) マッピング TCP/UDP/SCTP ポートを指定します。リテラル名または 0 ~ 65535 の範囲の数字でポートを指定できます。
net-to-net	(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番目に変換されます (以降も同様)。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。
no-proxy-arp	(オプション) スタティック NAT の場合に、マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。
pat-pool mapped_obj	(オプション) アドレスの PAT プールをイネーブルにします。オブジェクトのすべてのアドレスが PAT アドレスとして使用されるようになります。ダイナミック NAT の場合、PAT プールをフォールバック方式として設定できます。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。
<i>real_port</i>	(オプション) スタティック NAT の場合は、実際の TCP/UDP/SCTP ポートを指定します。リテラル名または 0 ~ 65535 の範囲の数字でポートを指定できます。
round-robin	(オプション) 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。デフォルトでは、次の PAT アドレスが使用される前に PAT アドレスのすべてのポートが割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。

route-lookup	(オプション) ルーテッドモードのアイデンティティ NAT で、NAT コマンドで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します。NAT コマンドでインターフェイスを指定しない場合、デフォルトでルートルックアップが使用されます。
service {tcp udp sctp}	(オプション) ポート変換を使用するスタティック NAT の場合は、ポート変換用のプロトコル (TCP、UDP、SCTP) を指定します。
static	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 を設定します。

コマンド デフォルト

- *real_ifc* および *mapped_ifc* のデフォルト値は **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。
- (8.3(1)、8.3(2)、8.4(1)) アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。(8.4(2)以降) アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、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 を無効にできます。
- オプションのインターフェイスを指定する場合、ASA によって NAT 構成が使用されて、出力インターフェイスが決定されます。(8.3(1)～8.4(1)) 唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルートルックアップが使用されます。(8.4(2)以降) アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルートルックアップを常に使用するオプションがあります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクト ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

8.3(1) このコマンドが追加されました。

リリース	変更内容
8.4(2)/8.5(1)	<p>no-proxy-arp、route-lookup、pat-pool、および round-robin キーワードが追加されました。</p> <p>アイデンティティ NAT のデフォルトの動作が、プロキシ ARP をイネーブルにし、他のスタティック NAT ルールと照合するように変更されました。</p> <p>8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードする場合、既存の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りました。</p>
8.4(3)	<p>extended、flat、および include-reserve キーワードが追加されました。</p> <p>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。</p> <p>この機能は、8.5(1) では使用できません。</p>
9.0(1)	<p>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。interface ipv6 オプションと net-to-net オプションが追加されました。</p>
9.5(1)	<p>block-allocation キーワードが追加されました。</p>
9.5(2)	<p>service sctp キーワードが追加されました。</p>
9.15(1)	<p>flat キーワードが削除され、include-reserve キーワードは flat のサブパラメータではなくなりました。すべての PAT プールで 1024 ～ 65535 のフラットなポート範囲が使用されるようになり、オプションで予約済みポート (1 ～ 1023) を含めることができるようになりました。</p>

使用上のガイドライン

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アドレスと宛先アドレスは、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、CLI 設定ガイド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 順序の詳細については、CLI 設定ガイドを参照してください。

構成に応じて、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に対応する別のネットワークオブジェクトやネットワーク オブジェクト グループを作成したりできます (**object network** または **object-group network** コマンドを使用)。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作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。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。

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。

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。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複数のオブジェクトを作成する必要があります。

マッピングアドレスのガイドライン

マッピング IP アドレス プールに、次のアドレスを含めることはできません。

- 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した場合は、すべてのインターフェイス IP アドレスが無効になります。インターフェイス PAT (ルーテッドモードのみ) 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。
- (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。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

PAT プールのガイドライン

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- (9.15 より前) 使用可能な場合、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多数ある場合は、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)。

- (9.15以降) ポートは、1024～65535の範囲の使用可能なポートにマッピングされます。必要に応じ、1024番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

クラスタで動作する場合、アドレスごとに512個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも512です。

- PATプールに対してブロック割り当てを有効にする場合、ポートブロックは1024～65535の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1～1023）を必要とするときは、機能しない可能性があります。たとえば、ポート22（SSH）を要求するアプリケーションは、1024～65535の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。

ダイナミック NAT によってマッピングされた IP アドレスにオブジェクトグループを使用し、そのグループにホストアドレスを含める場合、PAT プールをイネーブルにすると、ホストアドレスの使用が PAT フォールバックからダイナミック NAT へと変更されます。

- (8.4(3)以降、8.5(1)または8.6(1)を除く) 2つの個別のルールで同じ 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ます。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 のガイドライン

- 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、設定ガイド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、ポート変換ルールを設定した別のスタティック 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のガイドライン

- (8.4(3)以降、8.5(1)または8.6(1)を除く) 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。
Note : この「粘着性」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最初の IP アドレスが使用されない場合があります。

- (8.4(2)、8.5(1)、および 8.6(1)) 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、ラウンドロビン割り当てのため、接続ごとに別の PAT アドレスが使用される可能性があります。この場合、ホストについて情報を交換する 2 つの Web サイト (e-コマースサイトと支払サイトなど) にアクセスするときに問題が発生する可能性があります。これらのサイトが、1 つのホストとして扱うべきものを 2 つの異なる IP アドレスと見なした場合、トランザクションは失敗することがあります。
- 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

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます (ルーテッドモードのみ)。次のベストプラクティスを推奨します。インターフェイスが同じブリッジグループのメンバーの場合は NAT64/46 を実行できないことに注意してください。

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (Twice NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (Twice NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスは IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

例

ダイナミック NAT の例

次の例では、外部アドレス 2.2.2.1 ~ 2.2.2.10 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。

```
ciscoasa(config)# object network my-range-obj
```

```
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(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。PAT 変換もすべて使用されることはほとんどありませんが、このような場合には、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。

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20
ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21
ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(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。

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30
ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31
ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

ダイナミック PAT の例

次の例では、アドレス 2.2.2.2 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。

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

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。

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

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

スタティック NAT の例

次の例では、内部にある実際のホスト 1.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 2.2.2.2 へのスタティック NAT を設定します。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

次の例では、内部にある実際のホスト 1.1.1.1 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。

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、1.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を使用するスタティック NAT を設定します。

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(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。

```
ciscoasa(config)# object network inside_v4_v6
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(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。

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

アイデンティティ NAT の例

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。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(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。

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

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーション (Twice NAT とネットワーク オブジェクト NAT の両方) を削除します。
show nat	NAT ポリシーの統計情報を表示します。
show nat pool	NAT プールに関する情報を表示します。
show running-config nat	NAT コンフィギュレーションを表示します。
show xlate	xlate 情報を表示します。
xlate block-allocation	PAT ポートブロック割り当ての特性を設定します。

nat (VPN ロード バランシング)

NAT で変換されるこのデバイスの IP アドレスの変換先 IP アドレスを設定するには、VPN ロード バランシング コンフィギュレーション モードで **nat** コマンドを使用します。この NAT 変換を無効にするには、このコマンドの **no** 形式を使用します。

```
nat ip-address
no nat [ ip-address ]
```

構文の説明

ip-address この NAT でこのデバイスの IP アドレスの変換先となる IP アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース 変更内容

7.0(1) このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始する必要があります。

このコマンドの **no nat** 形式で任意の *ip-address* 値を指定する場合、IP アドレスは実行コンフィギュレーションの既存の NAT IP アドレスに一致する必要があります。

例

次に、**nat** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。この例では、NAT で変換するアドレスを 192.168.10.10 に設定しています。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
```

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシングモードを開始します。

nat-assigned-to-public-ip

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 アドレスに自動的に戻すには、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で **nat-assigned-to-public-ip** コマンドを使用します。NAT ルールを無効にするには、このコマンドの **no** 形式を使用します。

nat-assigned-to-public-ip interface
no nat-assigned-to-public-ip interface

構文の説明

interface NATを適用するインターフェイスを指定します。

コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネルグループ一般属性コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

8.4(3) このコマンドが追加されました。

使用上のガイドライン

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、内部サーバー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。

データフロー

次に、この機能を有効にした場合に ASA を通過するパケットフローの手順を示します。

1. VPN ピアから ASA にパケットが送信されます。

外部用の送信元/宛先は、ピアのパブリック IP アドレスまたは ASA の IP アドレスで構成されます。暗号化された内部用の送信元/宛先は、VPN で割り当てられた IP アドレス/内部サーバーのアドレスで構成されます。

2. ASA でパケットが復号されます（外部用の送信元/宛先が削除されます）。
3. ASA で内部サーバーのルートルックアップが実行され、内部インターフェイスにパケットが送信されます。
4. 自動的に作成される VPN NAT ポリシーに基づいて、VPN で割り当てられた送信元 IP アドレスがピアのパブリック IP アドレスに変換されます。
5. 変換されたパケットが ASA からサーバーに送信されます。
6. パケットに対するサーバーからの応答がピアのパブリック IP アドレスに送信されます。
7. 応答を受け取ると、ASA により、宛先 IP アドレスが VPN で割り当てられた IP アドレスに戻されます。
8. 変換が解除されたパケットが ASA から暗号化が行われた外部インターフェイスに転送され、ASA の IP アドレスまたはピアのパブリック IP アドレスで構成される外部用の送信元/宛先が追加されます。
9. ASA からピアにパケットが返送されます。
10. ピアでデータが復号化されて処理されます。

制限事項

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 セキュアクライアント 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。
- リバースルート インジェクション（**set reverse-route** コマンドを参照）を有効にすると、VPN で割り当てられた IP アドレスだけがアドバタイズされます。
- 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。

例

次に、「vpnclient」トンネルグループに対してパブリック IP への NAT をイネーブルにする例を示します。

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

次に、IP 10.1.226.174 が割り当てられたピア 209.165.201.10 の自動 NAT ルールを表示する **show nat detail** コマンドの出力例を示します。

```
ciscoasa# show nat detail
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

関連コマンド

コマンド	説明
show nat	現在の xlate を表示します。
tunnel-group general-attributes	トンネル グループの一般属性を設定します。
debug menu webvpn 99	AnyConnect SSL セッションで、VPN NAT インターフェイスがセッションに保存されます。
debug menu ike 2 peer_ip	Cisco IPsec クライアントセッションで、VPN NAT インターフェイスが SA に保存されます。
debug nat 3	NAT のデバッグ メッセージを表示します。

nat-rewrite

DNS 応答の A レコードに組み込まれている IP アドレスの NAT リライトを有効にするには、パラメータ コンフィギュレーションモードで **nat-rewrite** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-rewrite
no nat-rewrite

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

NAT リライトは、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していない場合でも、**inspect dns** コマンドを設定していれば有効にできます。無効にするには、ポリシーマップコンフィギュレーションで **no nat-rewrite** コマンドを明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ コンフィギュ レーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

7.2(1) このコマンドが追加されました。

使用上のガイドライン

この機能は、DNS 応答の A タイプのリソース レコード (RR) の NAT 変換を実行します。

例

次に、DNS インスペクション ポリシー マップで NAT リライトをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# nat-rewrite
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

nbns-server

NBNS サーバーを設定するには、トンネルグループ `webvpn` 属性コンフィギュレーション モードで `nbns-server` コマンドを使用します。構成から NBNS サーバーを削除するには、このコマンドの `no` 形式を使用します。

ASA は、NetBIOS 名を IP アドレスにマップするために NBNS サーバーをクエリします。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

```
nbns-server { ipaddr | hostname } [ master ] [ timeout timeout ] [ retry retries ]
no nbns-server
```

構文の説明

<code>hostname</code>	NBNS サーバーのホスト名を指定します。
<code>ipaddr</code>	NBNS サーバーの IP アドレスを指定します。
<code>master</code>	これは WINS サーバーではなく、マスター ブラウザであることを示します。
<code>retry</code>	再試行値が後に続くことを示します。
<code>retries</code>	NBNS サーバーへのクエリを再試行する回数を指定します。ASA は、エラーメッセージを送信するまでに、ここに指定する回数、サーバーのリストを繰り返し使用します。デフォルト値は 2 で、指定できる範囲は 1 ~ 10 です。
<code>timeout</code>	タイムアウト値が後に続くことを示します。
<code>timeout</code>	NBNS サーバーが 1 つだけ存在する場合は同じサーバーに、複数存在する場合は別のサーバーに、ASA がクエリを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ~ 30 秒です。

コマンド デフォルト

NBNS サーバーは、デフォルトでは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネルグループ <code>webvpn</code> 属性コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

7.1(1) `webvpn` モードからトンネル グループ `webvpn` コンフィギュレーション モードに移行しました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを `webvpn` コンフィギュレーション モードで入力すると、トンネルグループ `webvpn` 属性コンフィギュレーションモードの同等のコマンドに変換されます。

サーバー エントリは最大 3 つです。冗長性のために、設定する最初のサーバーはプライマリサーバーで、その他のサーバーはバックアップです。

`no` オプションを使用して、構成から一致するエントリを削除します。

例

次に、NBNS サーバーでトンネル グループ「test」を設定する例を示します。NBNS サーバーはマスターブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバーを設定する例も示します。

```
ciscoasa
(config)#
  tunnel-group test type webvpn
ciscoasa
(config)#
  tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
<code>clear configure group-policy</code>	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
<code>show running-config group-policy</code>	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
<code>tunnel-group webvpn-attributes</code>	指定したトンネル グループの WebVPN 属性を指定します。

neighbor (ルータ EIGRP)

ルーティング情報を交換する EIGRP ネイバルルータを定義するには、ルータ EIGRP コンフィギュレーションモードで **neighbor** コマンドを使用します。ネイバーエントリを削除するには、このコマンドの **no** 形式を使用します。

neighbor ip_address interface name
no neighbor ip_address interface name

構文の説明

interface name **nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。

ip_address ルーティング情報を交換するネイバルルータの IPv4 アドレス。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ EIGRP コンフィギュレーション	—	•	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

8.0(2) このコマンドが追加されました。

使用上のガイドライン

複数のネイバー ステートメントを使用して、特定の EIGRP ネイバーでピアリングセッションを確立できます。EIGRP がルーティング更新を交換するインターフェイスは、ネイバー ステートメントで指定する必要があります。2つの EIGRP ネイバーがルーティング更新を交換するインターフェイスは、同じネットワークにある IP アドレスで設定する必要があります。



(注) インターフェイスに対して **passive-interface** コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング アップ デートメッセージと **hello** メッセージが抑制されます。EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

EIGRP hello メッセージは、**neighbor** コマンドを使用して定義されたネイバーにユニキャストメッセージとして送信されます。

例

次に、ネイバーを 192.168.1.1 および 192.168.2.2 として EIGRP ピアリングセッションを設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバーメッセージに関するデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

neighbor (ルータ OSPF)

ポイントツーポイントの非ブロードキャストネットワークにスタティックネイバーを定義するには、ルータ OSPF コンフィギュレーションモードで **neighbor** コマンドを使用します。コンフィギュレーションからスタティックに定義されたネイバーを削除するには、このコマンドの **no** 形式を使用します。

neighbor *ip_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

構文の説明

interface *name* (任意) **nameif** コマンドで指定されたインターフェイス名を指定します。ネイバーにはこのインターフェイス経由で到達できます。

ip_address ネイバー ルータの IP アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

9.0(1) マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

neighbor コマンドは、VPN トンネル経由で OSPF ルートをアドバタイズするために使用されます。既知の非ブロードキャスト ネットワーク ネイバーごとにネイバー エントリを 1 つ含める必要があります。ネイバー アドレスは、インターフェイスのプライマリ アドレスに存在する必要があります。

ネイバーがシステムに直接接続されたいずれかのインターフェイスと同じネットワークにない場合は、**interface** オプションを指定する必要があります。また、ネイバーに到達するには、スタティック ルートを作成する必要があります。

例

次に、アドレス 192.168.1.1 でネイバー ルータを定義する例を示します。

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバルルータ コンフィギュレーションのコマンドを表示します。

neighbor activate

ボーダー ゲートウェイ プロトコル (BGP) ネイバーとの情報交換をイネーブルにするには、アドレスファミリ コンフィギュレーションモードで **neighbor activate** コマンドを使用します。BGP ネイバーとのアドレス交換を無効にするには、このコマンドの **no** 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **activate**
no neighbor { *ip_address* | *ipv6-address* } **activate**

構文の説明

ip_address BGP ルータの IP アドレス。

ipv6-address BGP ルータの IPv6 アドレス。

コマンド デフォルト

BGP ネイバーとのアドレス交換は、IPv4 アドレス ファミリについてデフォルトでイネーブルになります。それ以外のアドレスファミリについてアドレス交換をイネーブルにすることはできません。



(注) IPv4 アドレス ファミリのアドレス交換は、**neighbor remote-as** コマンドで定義された各 BGP ルーティングセッションに対してデフォルトで有効になります。ただし、**neighbor remote-as** コマンドの設定前に **no bgp default ipv4-activate** コマンドを設定した場合や、**no neighbor activate** コマンドを使用して特定のネイバーとのアドレス交換を無効にした場合は除きます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.2(1) このコマンドが追加されました。

9.3(2) *ipv6-address* 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン このコマンドを使用すると、アドレス情報を IP プレフィックスの形式でアドバタイズできます。BGP では、このアドレスプレフィックス情報をネットワーク層到達可能性情報（NLRI）と呼びます。

例

次に、BGP ネイバー 172.16.1.1 について、IPv4 アドレス ファミリ ユニキャストのアドレス交換をイネーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

次に、group2 という名前の BGP ピア グループのすべてのネイバーと BGP ネイバー 7000::2 について、IPv6 アドレス ファミリのアドレス交換をイネーブルにする例を示します。

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルに エントリを追加します。

neighbor advertise-map

設定されたルートマップに一致する BGP テーブル内のルートをアドバタイズするには、ルータ コンフィギュレーションモードで `neighbor advertise-map` コマンドを使用します。ルートアドバタイズメントをディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } advertise-map map-name { exist-map map-name | non-exist-map map-name } [ check-all-paths ]
```

```
no neighbor { ip_address | ipv6-address } advertise-map map-name { exist-map map-name | non-exist-map map-name } [ check-all-paths ]
```

構文の説明

<code>ipv4_address</code>	条件付きアドバタイズメントを受け取るルータの IPv4 アドレスを指定します。
<code>ipv6_address</code>	条件付きアドバタイズメントを受け取るルータの IPv6 アドレスを指定します。
<code>advertise-map map-name</code>	存在マップまたは非存在マップの条件を満たす場合にアドバタイズするルートマップの名前を指定します。
<code>exist-map map-name</code>	アドバタイズマップのルートをアドバタイズするかどうかを決定するために BGP テーブル内のルートと比較する存在マップの名前を指定します。
<code>non-exist-map map-name</code>	アドバタイズマップのルートをアドバタイズするかどうかを決定するために BGP テーブル内のルートと比較する非存在マップの名前を指定します。
<code>check-all-paths</code>	(オプション) BGP テーブル内のプレフィックスを使用した存在マップによるすべてのパスのチェックをイネーブルにします。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

`neighbor advertise-map` コマンドは、選択されたルートを条件付きでアドバタイズするために使用します。条件付きでアドバタイズされるルート（プレフィックス）は、アドバタイズマップと存在マップまたは非存在マップの2つのルートマップで定義されます。

存在マップまたは不在マップと関連付けられているルートマップは、BGP スピーカーが追跡するプレフィックスを指定します。

アドバタイズマップと関連付けられているルートマップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィックスを指定します。

存在マップが設定されている場合、プレフィックスがアドバタイズマップと存在マップの両方に存在するときに条件が満たされます。

非存在マップが設定されている場合、プレフィックスがアドバタイズマップには存在するが、不在マップには存在しないときに条件が満たされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティングテーブルに存在する必要があります。

例

次のルート コンフィギュレーションの例では、すべてのパスをチェックするように BGP を設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

次のアドレスファミリ コンフィギュレーションの例では、非存在マップを使用して、10.1.1.1 ネイバーに条件付きでプレフィックスをアドバタイズするように BGP を設定しています。プレフィックスが MAP3 にあり、MAP4 がない場合に条件を満たし、プレフィックスがアドバタイズされます。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

次のピア グループ コンフィギュレーションの例では、BGP ネイバーのすべてのパスをプレフィックスと照合してチェックするように BGP を設定しています。

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor routel send-community both
ciscoasa(config-router-af)# neighbor routel advertise-map MAP1 exist-map MAP2
check-all-paths
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードを開始します。

neighbor advertisement-interval

BGP ルーティング アップデートを送信する最小ルートアドバタイズメントインターバル (MRAI) を設定するには、アドレス ファミリ コンフィギュレーション モードで `neighbor advertisement-interval` コマンドを使用します。デフォルト値に戻すには、このコマンドの `no` 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*
no neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

seconds BGP ルーティングアップデートの最小送信間隔。
 有効な値は、0 ~ 600 です。

コマンドデフォルト

VRF 以外の eBGP セッション : 30 秒

VRF の eBGP セッション : 0 秒

iBGP セッション : 0 秒

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

MRAI が 0 秒の場合は、BGP ルーティング テーブルが変更された時点ですぐに BGP ルーティング アップデートが送信されます。

例

次に、BGP ルーティング アップデートの最小送信間隔を 10 秒に設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

次に、BGPv6 ルーティング アップデートの最小送信間隔を 100 秒に設定する例を示します。

```
asa(config-router-af)# neighbor 2001::1 advertisement-interval 100
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルに エントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor default-originate

BGP スピーカー（ローカルルータ）にネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、そのルートがデフォルトルートとして使用されるようにするには、アドレスファミリ コンフィギュレーション モードで `neighbor default-originate` コマンドを使用します。デフォルト ルートを送信しないようにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } default-originate [ route-map route-map name ]
no neighbor { ip_address | ipv6-address } default-originate [ route-map route-map name ]
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>route-map route-map name</code>	(オプション) ルートマップの名前。ルートマップでは、条件に応じてルート 0.0.0.0 を挿入できます。

コマンド デフォルト

ネイバーにデフォルト ルートは送信されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	<code>ipv6-address</code> 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、ローカルルータの 0.0.0.0 が不要になります。 `match ip address` 句を含むルート マップとともに使用することで、IP アクセス リストと完全に一致するルートがある場合にデフォルトルート 0.0.0.0 が挿入されるようにすることができます。ルート マップには他の `match` 句も含めることができます。

neighbor default-originate コマンドでは、標準アクセスリストまたは拡張アクセスリストを使用できます。

例

次に、ネイバー 72.16.2.3 にルート 0.0.0.0 を無条件で挿入するようにローカルルータを設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
In the following example, the local router injects route 0.0.0.0 to the neighbor 2001::1:
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルに エントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor description

説明をネイバーに関連付けるには、アドレス ファミリ コンフィギュレーション モードで `neighbor description` コマンドを使用します。説明を削除するには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } description text
no neighbor { ip_address | ipv6-address } description text
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

`text` ネイバーを説明するテキスト（最大 80 文字）。

コマンド デフォルト

ネイバーの説明はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

例

次に、ネイバーに「peer with example.com」という説明を設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

次に、IPv6 ネイバーに「peer with example.com」という説明を設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 description peer with example.com
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルに エントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor disable-connected-check

ループバック インターフェイスを使用するシングル ホップ ピアとの eBGP ピアリング セッションを確立するために接続の検証をディセーブルにするには、アドレス ファミリ コンフィギュレーション モードで `neighbor disable-connected-check` コマンドを使用します。eBGP ピアリングセッションについての接続の検証をイネーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } disable-connected-check
no neighbor { ip_address | ipv6-address } disable-connected-check
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

コマンド デフォルト

デフォルトでは、シングル ホップ eBGP ピアリングセッション (TTL=254) について、BGP ルーティングプロセスで接続が検証され、eBGP ピアが同じネットワークセグメントに直接接続されているかどうか確認されます。ピアが同じネットワークセグメントに直接接続されていない場合、ピアリングセッションは確立されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

`neighbor disable-connected-check` コマンドは、シングルホップで到達可能だが、ループバック インターフェイス上に設定されている、あるいは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にする場合に使用します。

このコマンドが必要になるのは、`neighbor ebgp-multihop` コマンドで TTL 値を 1 に設定している場合だけです。シングルホップ eBGP ピアのアドレスに到達できる必要があります。`neighbor update-source` コマンドを使用して、BGP ルーティングプロセスでピアリングセッションにループバック インターフェイスを使用できるように設定する必要があります。

例

次に、2つの BGP ピア間でシングルホップ eBGP ピアリングセッションを設定する例を示します。この2つのピアは各ルータ上のローカルループバック インターフェイスを経由して同じネットワーク セグメント上で到達可能になっています。

BGP ピア 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
BGP Peer 2
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
BGPv6 Peer
ciscoasa(config-router)# neighbor 2001::1 disable-connected-check
```

関連コマンド

コマンド	説明
<code>neighbor remote-as</code>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
<code>neighbor ebgp-multihop</code>	直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れるか、または開始します。

neighbor distribute-list

アクセスリストで指定された BGP ネイバー情報を配布するには、アドレスファミリ コンフィギュレーションモードで `neighbor distribute-list` コマンドを使用します。エントリを削除するには、このコマンドの `no` 形式を使用します。

```
neighbor ip_address distribute-list { access-list-name } { in | out }
no neighbor ip_address distribute-list { access-list-name } { in | out }
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>access-list-name</code>	標準アクセス リスト名。
<code>in</code>	指定したネイバーからの着信アドバタイズメントにアクセス リストを適用します。
<code>out</code>	指定したネイバーへの発信アドバタイズメントにアクセス リストを適用します。

コマンドデフォルト

BGP ネイバーは指定されません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

9.2(1) このコマンドが追加されました。

使用上のガイドライン

配布リストは、アドバタイズメントをフィルタリングする方法の1つです。アドバタイズメントをフィルタリングする方法には、ほかにも次のような方法があります。

- `ip as-path access-list` コマンドおよび `neighbor filter-list` コマンドで自律システムパスフィルタを設定できます。

- **access-list (IP 標準)** コマンドでアドバタイズメントのフィルタリングに使用する標準アクセスリストを設定できます。
- **route-map (IP)** コマンドでアドバタイズメントをフィルタリングできます。ルートマップは、自律システム フィルタ、プレフィックス フィルタ、アクセス リスト、配布リストで設定できます。

標準アクセスリストはルーティングアップデートのフィルタリングに使用できます。ただし、クラスレス ドメイン間ルーティング (CIDR) を使用している場合、標準アクセスリストによるルートフィルタリングでは、ネットワーク アドレスやマスクの高度なフィルタリングに必要な細かい設定は行えません。

例

次に、標準アクセスリスト **distribute-list-acl** の BGP ネイバー情報をネイバー 172.16.4.1 の着信アドバタイズメントに適用する例を示します。

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
network	BGP でアドバタイズするネットワークを指定します。
access-list permit	転送するパケットを指定します。
access-list deny	拒否するパケットを指定します。

neighbor ebgp-multihop

直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れて試行するには、アドレスファミリ コンフィギュレーション モードで `neighbor ebgp-multihop` コマンドを使用します。デフォルトに戻るには、`no` 形式のコマンドを使用します。

neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop** [*ttl*]
no neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop**

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

ttl (オプション) 存続可能時間。
 有効な値の範囲は 1 ~ 255 ホップです。

コマンド デフォルト

直接接続されたネイバーだけが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

この機能は、シスコ テクニカル サポート 担当者 の 指示 の もと で のみ 使用 して ください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート (0.0.0.0) だけの場合はマルチホップは確立されません。

例

次に、直接接続されていないネットワークに存在するネイバー 10.108.1.1 との間の接続を許可する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

次に、直接接続されていないネットワークに存在するネイバー2001::1 との間の接続を許可する例を示します。

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af) neighbor 12001::1 ebgp-multihop
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor fall-over bfd (ルータ BGP)

BGP の BFD サポートを設定して、BFD からの転送パス検出障害メッセージを受信するように BGP を登録するには、ネイバーの設定時に **fall-over** オプションを使用します。

neighbor ip_address | ipv6_address fall-over bfd

構文の説明

ip_address/ipv6_address ネイバー ルータの IP/IPv6 アドレス (A.B.C.D/ X:X:X:X形式)。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ BFD コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.6(2) このコマンドが追加されました。

使用上のガイドライン

マルチホップ用に BGP の BFD サポートを設定する場合は、送信元/宛先ペアに関して BFD マップがすでに作成されていることを確認します。

例

次に、172.16.10.2 ネイバーと 1001::2 ネイバーの BFD サポートを設定する例を示します。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.10.2 fall-over bfd
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 1001::2 fall-over bfd
```

関連コマンド

コマンド	説明
authentication	シングルホップセッションとマルチホップセッションの BFD テンプレートに認証を設定します。

コマンド	説明
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップテンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーションモードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

neighbor filter-list

BGP フィルタを設定するには、アドレスファミリ コンフィギュレーション モードで `neighbor filter-list` コマンドを使用します。この機能をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } filter-list access-list-name { in | out }
no neighbor { ip_address | ipv6-address } filter-list access-list-name { in | out }
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>access-list-name</code>	自律システム パス アクセス リストの名前。このアクセスリストは <code>as-path access-list</code> コマンドで定義します。
<code>in</code>	着信ルートにアクセス リストを適用します。
<code>out</code>	発信ルートにアクセス リストを適用します。

コマンド デフォルト

BGP フィルタは使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	<code>ipv6-address</code> 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドでは、着信と発信の両方 BGP ルートに対するフィルタを作成します。



- (注) 特定の方向（着信または発信）のネイバーに対して `neighbor distribute-list` コマンドと `neighbor prefix-list` コマンドの両方を適用しないでください。これら2つのコマンド（`neighbor distribute-list` コマンドと `neighbor prefix-list` コマンド）は相互に排他的であり、着信または発信の各方向に対して1つしか適用できません。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、隣接する自律システム 123 を経由するすべてのパスについて、IP アドレス 172.16.1.1 のネイバーでアドバタイズメントを送信しないように設定しています。

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_
ciscoasa(config)# as-path access-list as-path-acl deny ^123$
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

次のアドレス ファミリ コンフィギュレーション モードの例では、隣接する自律システムを経由するすべてのパスについて、IP アドレス 2001::1 の BGPv6 ネイバーでアドバタイズメントを送信しないように設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 filter-list as-path-acl out
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
<code>neighbor activate</code>	BGP ネイバーとの情報交換をイネーブルにします。
<code>neighbor remote-as</code>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
<code>network</code>	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor ha-mode graceful-restart

ボーダーゲートウェイプロトコル (BGP) ネイバーの BGP グレースフルリスタート機能をイネーブルまたはディセーブルにするには、アドレスファミリ コンフィギュレーション モードで `neighbor ha-mode graceful-restart` コマンドを使用します。コンフィギュレーションからネイバーの BGP グレースフルリスタート機能を削除するには、このコマンドの `no` 形式を使用します。

neighbor *ip_address* ha-mode graceful-restart [disable]
no neighbor *ip_address* ha-mode graceful-restart

構文の説明

ip_address ネイバーの IP アドレス。

`disable` (オプション) ネイバーの BGP グレースフルリスタート機能をディセーブルにします。

コマンド デフォルト

BGP グレースフルリスタート機能はディセーブルになっています。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

`neighbor ha-mode graceful-restart` コマンドは、個々の BGP ネイバーについて、グレースフルリスタート機能をイネーブルまたはディセーブルにする場合に使用します。グレースフルリスタート機能が BGP ピアでイネーブルになっている場合は、`disable` キーワードを使用してディセーブルにできます。

グレースフルリスタート機能は、セッションの確立時に OPEN メッセージのノンストップフォワーディング (NSF) 対応ピアと NSF 認識ピアの間でネゴシエートされます。BGP セッションの確立後にグレースフルリスタート機能をイネーブルにした場合は、セッションをソフトリセットまたはハードリセットして再起動する必要があります。

グレースフル リスタート機能は、NSF 対応 ASA および NSF 認識 ASA でサポートされます。NSF 対応 ASA では、ステートフル スイッチオーバー（SSO）処理（グレースフル リスタート）を実行し、その処理が完了するまでルーティングテーブル情報を保持することによってピアの再起動を支援できます。NSF 認識ルータは NSF 対応 ルータと同様に機能しますが、SSO 処理を実行することはできません。



- (注) BGP グレースフル リスタート機能をすべての BGP ネイバーに対してグローバルにイネーブルにするには、`bgp graceful-restart` コマンドを使用します。個別のネイバーで BGP グレースフル リスタート機能が設定されている場合は、グレースフル リスタートを設定するためのそれぞれの方法のプライオリティは同じであり、最後の設定インスタンスがネイバーに適用されます。

BGP ネイバーの BGP グレースフル リスタートの設定を確認するには、`show bgp neighbors` コマンドを使用します。

例

次に、BGP ネイバー 172.21.1.2 に対して BGP グレースフル リスタート機能をイネーブルにする例を示します。

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

関連コマンド

コマンド	説明
bgp graceful-restart	BGP グレースフル リスタート機能をすべての BGP ネイバーに対してグローバルにイネーブルまたはディセーブルにします。
<code>show bgp neighbors</code>	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。

neighbor local-as

外部ボーダー ゲートウェイ プロトコル (eBGP) ネイバーから受信したルートの AS_PATH 属性をカスタマイズするには、アドレス ファミリ コンフィギュレーション モードで `neighbor local-as` コマンドを使用します。AS_PATH 属性のカスタマイズを無効にするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } local-as [ autonomous-system-number [ no-prepend [ replace-as [ dual-as ] ] ] ]
```

```
no neighbor { ip_address | ipv6-address } local-as
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>autonomous-system-number</code>	(オプション) AS_PATH 属性の先頭に追加する自律システムの番号。この引数の値の範囲は、1 ~ 65535 の有効な自律システム番号です。 (注) この引数では、ローカル BGP ルーティングプロセスまたはリモート ピアのネットワークからの自律システム番号は指定できません。 自律システム番号の形式の詳細については、 <code>router bgp</code> コマンドの説明を参照してください。
<code>no-prepend</code>	(オプション) eBGP ネイバーから受信したルートにローカル自律システム番号を追加しません。
<code>replace-as</code>	(オプション) 実際の自律システム番号を eBGP アップデートのローカル自律システム番号で置き換えます。ローカル BGP ルーティングプロセスからの自律システム番号は、追加されません。
<code>dual-as</code>	(任意) ローカル BGP ルーティングプロセスからの実際の自律システム番号または <code>autonomous-system-number</code> 引数 (<code>local-as</code>) で設定した自律システム番号を使用してピアリングセッションを確立するように eBGP ネイバーを設定します。

コマンド デフォルト

ローカル BGP ルーティング プロセスからの自律システム番号は、デフォルトで、すべての外部ルートに追加されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	・対応	—	・対応	・対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

`neighbor local-as` コマンドを使用して、eBGP ネイバーから受信するルートの自律システム番号を追加および削除して、`AS_PATH` 属性がカスタマイズされます。このコマンドの設定により、自律システム番号を移行するために、外部ピアに対して別の自律システムのメンバとしてルータを表示できます。この機能を使用すると、既存のピアリング関係を維持したまま、ネットワーク オペレータが通常のサービス時間内に顧客を新しいコンフィギュレーションに移行できるため、BGP ネットワークの自律システム番号を変更するプロセスが簡単になります。



注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは自律システムの移行のためだけに設定し、移行が完了した後は設定を解除する必要があります。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によってルーティング ループが作成される可能性があります。

このコマンドは、正しい eBGP ピアリングセッションにのみ使用できます。2つのピアがコンフェデレーションの別々のサブ自律システムにある場合は機能しません。

円滑に移行するには、4 バイト自律システム番号を使用して指定されている自律システム内にあるすべての BGP スピーカーで、4 バイト自律システム番号をサポートするようアップグレードすることを推奨します。

例

Local-AS の例

次に、`local-as` 機能を使用して、ルータ 1 とルータ 2 のピアリングを自律システム 300 を介して確立する例を示します。

Router 1 (Local router)

```

ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300
Router 2 (Remote router)
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300

```

no-prepend キーワードの設定例

次に、ネイバー 192.168.1.1 から受信したルートに自律システム 500 を追加しないように BGP を設定する例を示します。

```

ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend

```

replace-as キーワードの設定例

次の例では、プライベート自律システム 64512 を 172.20.1.1 ネイバーに対するアウトバウンドルーティングアップデートから取り除き、これを自律システム 600 に置き換えます。

```

ciscoasa(config)# router bgp 64512

ciscoasa(config-router)# address-family ipv4

ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as

ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as

```

dual-as キーワードの設定例

次に、2つのプロバイダー ネットワークと1つの顧客ネットワークの設定例を示します。ルータ1は自律システム100に属し、ルータ2は自律システム200に属しています。自律システム200は自律システム100にマージされます。この移行は自律システム300（顧客ネットワーク）のルータ3へのサービスを中断せずに行う必要があります。ルータ1でneighbor local-as コマンドを設定して、この移行の実行中にルータ3で自律システム200とのピアリングを維持するようにします。移行の完了後、通常のメンテナンス時間中またはその他のスケジュール済みのダウンタイム中にルータ3の設定を自律システム100を持つピアに対してアップデートできます。

Router 1 Configuration (Local Provider Network)

```

ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# no synchronization

```

```
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

Router 2 Configuration (Remote Provider Network)

```
ciscoasa(config)# router bgp 200

ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

Router 3 Configuration (Remote Customer Network)

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

2つの自律システムをマージした後、移行を完了するために、ルータ3でピアリングセッションを更新します。

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

BGPv6 の設定

```
ciscoasa(config-router-af)# neighbor 2001::1 local-as 500 no-prepend
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーション モードに入ります。
bgp router-id	ローカル ボーダー ゲートウェイ プロトコル (eBGP) ルーティング プロセスの固定ルータ ID を設定します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。
同期	BGP と内部ゲートウェイプロトコル (IGP) システムの間の同期をイネーブルにします。

neighbor maximum-prefix

ネイバーから受信できるプレフィックスの数を制御するには、アドレスファミリーコンフィギュレーションモードで `neighbor maximum-prefix` コマンドを使用します。この機能をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } maximum-prefix maximum [ threshold ] [ restart
restart-interval ] [ warning-only ]
no neighbor { ip_address | ipv6-address } maximum-prefix maximum
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>maximum</code>	このネイバーから許可されるプレフィックスの最大数。
<code>threshold</code>	(任意) <code>maximum</code> の値の何パーセントになったらルータが警告メッセージを生成するかを示す整数。指定できる範囲は 1 ~ 100 です。デフォルト値は 75 (%) です。
<code>restart</code>	(オプション) 最大プレフィックス数の制限を超えたためにディセーブルになったピアリングセッションを BGP を実行するルータで自動的に再確立するように設定します。再起動タイマーは <code>restart-interval</code> 引数で設定します。
<code>restart-interval</code>	(オプション) ピアリングセッションを再確立する時間間隔 (分)。範囲は 1 ~ 65535 分です。
<code>warning-only</code>	(任意) <code>maximum</code> の値を超えた場合、ピアリングを終了せずに、ルータがログメッセージを生成できるようにします。

コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。プレフィックス数に制限はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリーコンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、BGP ルータがピアから受信できるプレフィックスの最大数を設定できます。これは、ピアから受信されるプレフィックスの制御メカニズムを提供します（配布リスト、フィルタリスト、ルートマップに加えて）。

受信プレフィックスの数が設定されている最大数を超えると、ルータはピアリングを終了します（デフォルト）。しかし、`warning-only` キーワードが設定されている場合、代わりにログメッセージが送信されるだけで、送信元とのピアリングは続行されます。終了されたピアは、`clear bgp` コマンドが発行されるまでダウンしたままになります。

例

次に、ネイバー 192.168.6.6 から受信できるプレフィックスの最大数を 1000 に設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

次に、ネイバー 2001::1 から受信できるプレフィックスの最大数を 1000 に設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

関連コマンド

コマンド	説明
<code>address-family ipv4</code>	アドレスファミリ コンフィギュレーション モードに入ります。
<code>neighbor activate</code>	BGP ネイバーとの情報交換をイネーブルにします。
<code>network</code>	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor next-hop-self

ルータを BGP スピーキングネイバーのネクストホップとして設定するには、アドレスファミリ コンフィギュレーションモードで `neighbor next-hop-self` コマンドを使用します。この機能をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } next-hop-self
no neighbor { ip_address | ipv6-address } next-hop-self
```

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

`warning-only` (任意) `maximum` の値を超えた場合、ピアリングを終了せずに、ルータがログメッセージを生成できるようにします。

コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレスファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドは、BGP ネイバーから同じ IP サブネット上の他の一部のネイバーに直接アクセスできない非メッシュ型のネットワーク（フレームリレーや X.25 など）で便利です。

例

次に、10.108.1.1 向けのすべてのアップデートに対し、このルータをネクストホップとしてアドバタイズするように設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

次に、2001::1 向けのすべてのアップデートに対し、このルータをネクストホップとしてアドバタイズするように設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 next-hop-selfs
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor password

2つのBGPピアの間のTCP接続でMessage Digest 5 (MD5) 認証を有効にするには、アドレスファミリーコンフィギュレーションモードでneighbor password コマンドを使用します。この機能をディisableにするには、このコマンドのno形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **password** [0-7] *string*
no neighbor { *ip_address* | *ipv6-address* } **password**

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

string 最大 25 文字のパスワード。大文字と小文字が区別されます。

最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

0 ~ 7 (オプション) 暗号化タイプ。0 ~ 6 を指定した場合は暗号化されません。暗号化する場合は 7 を使用します。

コマンドデフォルト

2つのBGPピアの間のTCP接続でMD5認証は使用されません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリーコンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) *ipv6-address* 引数が追加され、IPv6 アドレスファミリーがサポートされるようになりました。

使用上のガイドライン 2つのBGPピアの間でMD5認証を設定できます。ピア間のTCP接続で送信された各セグメントが検証されます。MD5認証は、両方のBGPピアで同じパスワードを使用して設定する必要があります。そうしないと、接続を行うことはできません。MD5認証を設定すると、ASAソフトウェアにより、TCP接続で送信される各セグメントのMD5ダイジェストが生成され、チェックされるようになります。

MD5認証を設定する場合、`service password-encryption` コマンドが有効になっているかどうかに関係なく、最大25文字のパスワード（大文字と小文字を区別する）を指定できます。パスワードの長さが25文字を超える場合は、エラーメッセージが表示され、パスワードが受け入れられません。この文字列には、スペースも含め、あらゆる英数字を使用できます。ただし、数字-スペース-任意の文字の形式でパスワードを設定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。さらに、英数字とともに次の記号を任意に組み合わせて使用できます。

```
`~!@#$%^&*()-_+=+|\}]{["`";/;><.,?
```



注意 認証文字列が正しく設定されていないと、BGPピアリングセッションは確立されません。認証文字列を注意して入力するとともに、認証の設定後にピアリングセッションが確立されたかどうかを確認することを推奨します。

ネイバーに対してパスワードを設定しているルータと設定していないルータとの間でBGPセッションを確立しようとする時、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179
```

同様に、2台のルータに異なるパスワードが設定されている場合、次のようなメッセージが画面に表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
```

BGPセッション確立後のMD5パスワードの設定

2つのBGPピアの間でMD5認証に使用されるパスワードやキーを設定または変更した場合、パスワードの設定後にローカルルータの既存のセッションは切断されません。ローカルルータでは、BGPホールドダウンタイマーの期限が切れるまで、新しいパスワードを使用してピアリングセッションを維持しようとします。デフォルトの期間は180秒です。ホールドダウンタイマーの期限が切れるまでの間にローカルルータでパスワードを入力または変更しないと、セッションはタイムアウトします。



(注) ホールドダウンタイマーに対して新しいタイマー値を設定した場合、その値はセッションがリセットされてからでないと有効になりません。したがって、ホールドダウンタイマーの設定を変更しても、BGPセッションのリセットの回避には役立ちません。

例

次に、10.108.1.1 ネイバーとのピアリングセッションに対してMD5認証を設定する例を示します。ホールドダウンタイマーの期限が切れるまでの間に、リモートピアで同じパスワードを設定する必要があります。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

次に、`service password-encryption` コマンドが無効になっている状態で 25 文字を超えるパスワードを設定する例を示します。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
ciscoasa(config-router-af)# neighbor 209.165.200.225 password 1234567891234567891234567890
```

```
% BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
no service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

次に、`service password-encryption` コマンドが有効になっている状態で 25 文字を超えるパスワードを設定した場合のエラーメッセージの例を示します。

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 1234567891234567891234567890

% BGP: Password length must be less than or equal to 25.
Router(config-router)# do show run | i password service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

関連コマンド

コマンド	説明
<code>address-family ipv4</code>	アドレスファミリー コンフィギュレーション モードに入ります。
<code>neighbor activate</code>	BGP ネイバーとの情報交換をイネーブルにします。
<code>bgp router-id</code>	ローカル ボーダー ゲートウェイ プロトコル (eBGP) ルーティング プロセスの固定ルータ ID を設定します。
<code>neighbor remote-as</code>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルに エントリを追加します。

neighbor prefix-list

プレフィックスリストで指定されたボーダー ゲートウェイ プロトコル (BGP) ネイバー情報を配布しないようにするには、アドレス ファミリ コンフィギュレーション モードで `neighbor prefix-list` コマンドを使用します。フィルタリストを削除するには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } prefix-list prefix-list-name { in | out }
no neighbor { ip_address | ipv6-address } prefix-list prefix-list-name { in | out }
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>prefix-list-name</code>	プレフィックス リストの名前。
<code>in</code>	指定したネイバーからの着信アドバタイズメントにフィルタ リストを適用します。
<code>out</code>	指定したネイバーへの発信アドバタイズメントにフィルタ リストを適用します。

コマンド デフォルト

外部アドレスおよびアドバタイズされたアドレスのすべてのプレフィックスが BGP ネイバーに配布されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレス ファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	<code>ipv6-address</code> 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

プレフィックスリストは、BGP アドバタイズメントをフィルタリングする 3 つの方法のうちの 1 つです。また、`ip as-path access-list` グローバル コンフィギュレーション コマンドで定義した AS パスフィルタを、`neighbor filter-list` コマンドで使用して BGP アドバタイズメントをフィルタリングできます。さらに、BGP アドバタイズメントをフィルタリングする 3 つ目の方法として、`neighbor distribute-list` コマンドでアクセスリストまたはプレフィックスリストを使用する方法があります。



- (注) 特定の方向（着信または発信）のネイバーに対して `neighbor distribute-list` コマンドと `neighbor prefix-list` コマンドの両方を適用しないでください。これら 2 つのコマンド（`neighbor distribute-list` コマンドと `neighbor prefix-list` コマンド）は相互に排他的であり、着信または発信の各方向に対して 1 つしか適用できません。

例

次のアドレスファミリ コンフィギュレーション モードの例では、`abc` という名前のプレフィックスリストをネイバー 10.23.4.1 からの着信アドバタイズメントに適用しています。

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

次のアドレスファミリ ルータ コンフィギュレーション モードの例では、`CustomerA` という名前のプレフィックスリストをネイバー 10.23.4.3 への発信アドバタイズメントに適用しています。

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
The following address family router configuration mode example applies the prefix list
named CustomerA to outgoing advertisements to neighbor 2001::1:
ciscoasa(config-router-af)#neighbor 2001::1 prefix-list CustomerA out
```

関連コマンド

コマンド	説明
<code>address-family ipv4</code>	アドレスファミリ コンフィギュレーション モードに入ります。
<code>neighbor activate</code>	BGP ネイバーとの情報交換をイネーブルにします。
<code>network</code>	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor remote-as

BGP またはマルチプロトコル BGP ネイバーテーブルにエントリを追加するには、アドレスファミリー コンフィギュレーション モードで **neighbor remote-as** コマンドを使用します。テーブルからエントリを削除するには、このコマンドの **no** 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*
no neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*

構文の説明

<i>ip_address</i>	ネイバー ルータの IP アドレス。
<i>ipv6-address</i>	ネイバー ルータの IPv6 アドレス。
<i>autonomous-system-number</i>	<p>ネイバーが属する自律システムの 1 ～ 65535 の範囲内の番号。</p> <p>自律システム番号の形式の詳細については、router bgp コマンドの説明を参照してください。</p> <p>alternate-as キーワードと一緒に使用した場合は、5 つまでの自律システム番号を入力できます。</p>

コマンド デフォルト

BGP ネイバー ピアもマルチプロトコル BGP ネイバー ピアありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリー コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.2(1) このコマンドが追加されました。

9.3(2) *ipv6-address* 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

router bgp グローバル コンフィギュレーション コマンドで指定されている自律システム番号に一致する自律システム番号を持つネイバーを指定することにより、ローカル自律システムの内部にネイバーが指定されます。それ以外の場合は、ネイバーは外部にあると認識されます。

デフォルトでは、ルータ コンフィギュレーション モードで `neighbor remote-as` コマンドを使用して定義したネイバーが、ユニキャスト アドレス プレフィックスのみを交換します。

`alternate-as` キーワードを使用すると、ダイナミックな BGP ネイバーを識別できる代替自律システムを最大 5 つまで指定できます。BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。`bgp listen` コマンドでサブネットの範囲が設定されて BGP ピアグループに関連付けられた後、そのサブネットの範囲の IP アドレスに対する TCP セッションを開始すると、新しい BGP ネイバーがそのグループのメンバーとして動的に作成されます。この新しい BGP ネイバーは、グループの設定やテンプレートをすべて継承します。

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として `asplain` (たとえば、65538) を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を `asplain` 形式および `asdot` 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを `asdot` 形式に変更するには、`bgp asnotation dot` コマンドに続けて、`clear bgp *` コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

例

次に、アドレス 10.108.1.2 にあるルータが、自律システム番号 65200 にある内部 BGP (iBGP) ネイバーになるよう指定する例を示します。

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

次に、BGP ルータを自律システム 65400 に割り当て、自律システムの送信元として 2 つのネットワークのリストが表示される例を示します。3 つのリモート ルータ (とその自律システム) のアドレスのリストが表示されます。設定中のルータでは、ネットワーク 10.108.0.0 とネットワーク 192.168.7.0 の情報が、隣接ルータと共有されます。1 つ目の `router` は、この設定が入力されたルータ (eBGP ネイバー) とは異なる自律システムにあるリモートルータです。2 つ目の `neighbor remote-as` コマンドにより、アドレス 10.108.234.2 の (自律システムの番号が同じの) 内部 BGP ネイバーが表示されます。最後の `neighbor remote-as` コマンドにより、この設定が入力されたルータとは異なるネットワークにあるネイバー (これも eBGP ネイバー) が指定されます。

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

次に、ユニキャスト ルータだけでやり取りするため、自律システム番号 65001 にあるネイバー 10.108.1.1 を設定する例を示します。

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31.1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーションモードに入ります。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。
neighbor remove private-as	プライベート自律システム番号を eBGP アウトバウンドルーティング アップデートから削除します。

neighbor remove-private-as

eBGP アウトバウンドルーティングアップデートからプライベート自律システム番号を削除するには、アドレスファミリ コンフィギュレーション モードで `neighbor remove-private-as` コマンドを使用します。この機能をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } remove-private-as [ all [ replace-as ] ]
no neighbor { ip_address | ipv6-address } remove-private-as [ all [ replace-as ] ]
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

`all` (オプション) 発信更新の AS パスからプライベート AS 番号をすべて削除します。

`replace-as` (任意) `all` キーワードを指定している限り、`replace-as` キーワードを指定すると、AS パスのすべてのプライベート AS 番号がルータのローカルの AS 番号に置き換わります。

コマンド デフォルト

AS パスからプライベート AS 番号は削除されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドは、外部 BGP (eBGP) ネイバーでのみ使用できます。プライベート AS の値の範囲は 64512 ~ 65535 です。外部ネイバーにアップデートを渡すときに AS パスにプライベート AS 番号が含まれていると、それらのプライベート AS 番号が削除されます。

- **neighbor remove-private-as** コマンドでは、AS パスにパブリックとプライベートの両方の ASN が含まれている場合でも、AS パスからプライベート AS 番号が削除されます。
- **neighbor remove-private-as** コマンドでは、AS パスにプライベート AS 番号のみが含まれている場合でも、AS パスからプライベート AS 番号が削除されます。このコマンドは eBGP ピアのみ適用され、その場合、eBGP ピアではローカルルータの AS 番号が AS パスに付加されるため、長さ 0 の AS パスにはなることはありません。**neighbor remove-private-as** コマンドでは、AS パスでコンフェデレーションセグメントの前にプライベート ASN が出現する場合でも、プライベート AS 番号が削除されます。
- AS パスからプライベート AS 番号を削除すると、送信されるプレフィックスのパス長が減少します。AS パス長は BGP 最良パス選択の重要な要素であるため、パス長を保持するために必要な場合があります。**replace-as** キーワードは、削除されたすべての AS 番号をローカルルータの AS 番号で置き換えることでパス長が維持されるようにします。
- この機能は、アドレスファミリ単位でネイバーに適用できます。そのため、この機能をあるアドレスファミリのネイバーには適用して、別のアドレスファミリでは適用しないようにすることで、機能が設定されているアドレスファミリのみのアウトバウンド側のアップデートメッセージに影響を与えることができます。

例

次に、172.16.2.33 に送信されるアップデートからプライベート AS 番号を削除するように設定する例を示します。これにより、10.108.1.1 でアドバタイズされた AS 100 を経由するパスの AS パス (自律システム 2051 で認識されるパス) が「100」だけになります。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer

ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as
```

```
Router-in-AS100# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non-peer-group peers:
    172.16.2.33
    65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
```

```
172.16.2.32 from 172.16.2.32  
Origin IGP, metric 0, localpref 100, valid, external, best
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor description	ネイバーに説明を関連付けます。
neighbor remote-as	ルーティングテーブルにBGPまたはマルチプロトコルBGPのルーティング エントリを追加します。

neighbor route-map

着信ルートまたは発信ルートにルートマップを適用するには、アドレスファミリー コンフィギュレーションモードで `neighbor route-map` コマンドを使用します。ルート マップを削除するには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } route-map map-name { in | out }
no neighbor { ip_address | ipv6-address } route-map map-name { in | out }
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

`map-name` ルート マップの名前。

`in` 着信ルートにルートマップを適用します。

`out` 発信ルートにルートマップを適用します。

コマンド デフォルト

ピアにルート マップは適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリー コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドをアドレスファミリー コンフィギュレーションモードで指定した場合、そのアドレスファミリーだけにルートマップが適用されます。ルータ コンフィギュレーションモードで指定した場合は、IPv4 ユニキャストルートだけにルートマップが適用されます。

発信ルートマップを指定した場合、ルートマップの少なくとも1のセクションに一致するルートだけがアドバタイズされます。これは適切な動作です。

例

次に、172.16.70.24 からの BGP 着信ルートに `internal-map` という名前のルート マップを適用する例を示します。

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

次に、2001::1 からの BGP 着信ルートに `internal-map` という名前のルート マップを適用する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 route-map internal-map in
```

関連コマンド

コマンド	説明
<code>address-family ipv4</code>	アドレスファミリ コンフィギュレーション モードに入ります。
<code>match as-path</code>	アクセス リストで指定されている BGP 自律システム パスを照合します。
ルート マップ	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
<code>match as-path</code>	アクセス リストで指定されている BGP 自律システム パスを照合します。
<code>set local-preference</code>	自律システム パスのプリファレンス値を指定します。

neighbor send-community

コミュニティ属性を BGP ネイバーに送信するように指定するには、アドレス ファミリ コンフィギュレーション モードで `neighbor send-community` コマンドを使用します。エントリを削除するには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } send-community
no neighbor { ip_address | ipv6-address } send-community
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

コマンド デフォルト

いずれのネイバーにもコミュニティ属性は送信されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

例

次に示すアドレス ファミリ コンフィギュレーション モードの例では、ルータが自律システム 109 に属しており、IP アドレス 172.16.70.23 のネイバーにコミュニティ属性を送信するように設定します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

次の例では、IP アドレス 2001::1 のネイバーにコミュニティ属性を送信するようにルータを設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 send-community
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。

neighbor shutdown

ネイバーを無効にするには、アドレスファミリ コンフィギュレーション モードで `neighbor shutdown` コマンドを使用します。ネイバーを再び有効にするには、このコマンドの `no` 形式を使用します。

neighbor ip_address shutdown
no neighbor ip_address shutdown

構文の説明

ip_address ネイバールータのIPアドレス。

コマンド デフォルト

いずれの BGP ネイバーの状態も変更されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
 ス

9.2(1) このコマンドが追加されました。

使用上のガイドライン

`neighbor shutdown` コマンドを使用すると、指定したネイバーに対するアクティブなセッションが終了し、関連するルーティング情報がすべて削除されます。

BGP ネイバーの要約を表示するには、`show bgp summary` コマンドを使用します。アイドル状態のネイバーと Admin エントリは `neighbor shutdown` コマンドによって無効化されています。

「State/PfxRcd」には、BGP セッションの現在の状態、またはルータがネイバーから受信したプレフィックスの数が表示されます。最大数 (`neighbor maximum-prefix` コマンドで設定) に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルになります。

例

次に、ネイバー 172.16.70.23 に対するアクティブなセッションをディセーブルにする例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
show bgp summary	BGP ネイバー ステータスの要約を表示します。

neighbor timers

特定のBGPピアのタイマーを設定するには、アドレスファミリ コンフィギュレーションモードでneighbor timers コマンドを使用します。特定のBGPピアのタイマーをクリアするには、このコマンドのno形式を使用します。

neighbor { ip_address | ipv6-address } **timers** keepalive holdtime [min-holdtime]

no neighbor { ip_address | ipv6-address } **timers**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
Keepalive (キープアラ イブ)	ASA ソフトウェアからピアにキープアライブメッセージを送信する 間隔 (秒数)。デフォルトは 60 秒で、範囲は 0 ~ 65535 秒です。
holdtime	キープアライブメッセージを受信できない状態が継続して、ピアが デッドであるとソフトウェアが宣言するまでの時間 (秒単位)。デ フォルト値は 180 秒です。範囲は 0 ~ 65535 です。
min-holdtime	(オプション) BGP ネイバーからの最小許容ホールドタイムを指定 する間隔 (秒単位)。最小許容ホールドタイムは、holdtime 引数で指 定された間隔以下にする必要があります。指定できる範囲は 0 ~ 65535 です。

コマンド デフォルト

キープアライブ時間 : 60 秒
ホールド時間 : 180 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモー ド	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペア レント	シングル	マルチ	
				コンテキスト	システム
アドレスファ ミリ コンフィ ギュレーショ ンモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

リリース 変更内容

- 9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。
-

使用上のガイドライン

- 特定のネイバーに対して設定したタイマーは、`timers bgp` コマンドを使用してすべての BGP ネイバーに対して設定したタイマーよりも優先されます。
- `holdtime` 引数の値を 20 秒未満に設定すると、「A hold time of less than 20 seconds increases the chances of peer flapping」という警告が表示されます。
- 指定したホールド時間よりも最小許容ホールド時間の方が長い場合、「Minimum acceptable hold time should be less than or equal to the configured hold time」という通知が表示されます。



- (注) BGP ルータに最小許容ホールドタイムが設定されている場合、リモート BGP ピアセッションは、リモート ピアが最小許容ホールドタイム間隔以上のホールドタイムをアドバタイズする場合にのみ確立されます。最小許容ホールドタイム間隔が、設定されたホールドタイムを超過する場合、次回のリモートセッション確立の試行は失敗し、ローカルルータは「unacceptable hold time」という示す通知を送信します。
-

例

次に、BGP ピア 192.168.47.0 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 210 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

次に、BGP ピア 192.168.1.2 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 130 秒、最小ホールド時間を 100 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

次に、BGP ピア 2001::1 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 210 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 timers 70 210
```

関連コマンド

コマンド	説明
<code>address-family ipv4</code>	アドレスファミリ コンフィギュレーションモードに入ります。
<code>neighbor activate</code>	BGP ネイバーとの情報交換をイネーブにします。

neighbor transport

ボーダー ゲートウェイ プロトコル (BGP) セッションの TCP 転送セッションオプションを有効にするには、ルータ コンフィギュレーションモードまたはアドレス ファミリ コンフィギュレーションモードで `neighbor transport` コマンドを使用します。BGP セッションの TCP 転送セッションオプションを無効にするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } transport { connection-mode { active | passive } |
path-mtu-discovery [ disable ] }
no neighbor { ip_address | ipv6-address } transport { connection-mode { active | passive } |
path-mtu-discovery [ disable ] }
```

構文の説明

<code>ip_address</code>	ネイバー ルータの IP アドレス。
<code>ipv6-address</code>	ネイバー ルータの IPv6 アドレス。
<code>connection-mode</code>	接続のタイプ (アクティブまたはパッシブ) を指定します。
<code>active</code>	アクティブ接続を指定します。
<code>passive</code>	パッシブ接続を指定します。
<code>path-mtu-discovery</code>	TCP 転送パスの最大伝送ユニット (MTU) ディスカバリをイネーブルにします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
<code>disable</code>	TCP パス MTU ディスカバリをディセーブルにします。

コマンド デフォルト

このコマンドを設定しない場合、TCP パス MTU ディスカバリはデフォルトでイネーブルになりますが、それ以外の TCP 転送セッション オプションはイネーブルになりません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

リリース **変更内容**

- 9.3(2) **ipv6-address** 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。
-

使用上のガイドライン

このコマンドは、各種の転送オプションを指定するために使用されます。BGPセッションに対して、アクティブまたはパッシブのいずれかの転送接続を指定できます。より大規模な MTU のリンクを BGP セッションで利用するには、TCP 転送パスの MTU ディスカバリをイネーブルにします。TCP パスの MTU ディスカバリが有効になっているか確認するには、`show bgp neighbors` コマンドを使用します。`disable` キーワードを使用してディスカバリを無効にした場合、無効にしたディスカバリのテンプレートを継承するすべてのピアでディスカバリが無効になります。

例

次に、1つの内部 BGP (iBGP) ネイバーについて、TCP 転送接続をアクティブに設定する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

次に、1つの外部 BGP (eBGP) ネイバーについて、TCP 転送接続をパッシブに設定する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

次に、1つの BGP ネイバーについて、TCP パスの MTU ディスカバリをディセーブルにする方法の例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

次に、1つの BGPv6 ネイバーについて、TCP 転送接続をアクティブに設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 transport connection-mode active
```

次に、1つの BGPv6 ネイバーについて、TCP パスの MTU ディスカバリをイネーブルにする方法の例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 transport path-mtu-discovery
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	BGP またはマルチプロトコル BGP のルーティング テーブルにエントリを追加します。
show bgp neighbor	BGP ネイバーに関する情報を表示します。

neighbor ttl-security

ボーダー ゲートウェイ プロトコル (BGP) ピアリングセッションを保護し、2つの外部 BGP (eBGP) ピアを区切るホップの最大数を設定するには、アドレスファミリ コンフィギュレーションモードで `neighbor ttl-security` コマンドを使用します。この機能をディセーブルにするには、このコマンドの `no` 形式を使用します。

```
neighbor { ip_address | ipv6-address } ttl-security hops hop-count
no neighbor { ip_address | ipv6-address } ttl-security hops hop-count
```

構文の説明

`ip_address` ネイバー ルータの IP アドレス。

`ipv6-address` ネイバー ルータの IPv6 アドレス。

`hop-count` eBGP ピアを区切るホップの数。TTL 値は、設定された `hop-count` 引数に基づいてルータにより計算されます。

有効な値は 1 ~ 254 の数値です。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

`neighbor ttl-security` コマンドは、CPU 利用率に基づく攻撃から BGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケットヘッダーの送信元と宛先の IP アドレスを偽造した大量の IP パケットでネットワークをあふれ

させてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。

この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。

この機能は、参加している各ルータで設定する必要があります。この機能では、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモートルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケットヘッダーの TTL 値がピアリングセッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能は BGP ピアリングセッションには影響しません。この機能がイネーブルの場合でも、キープアライブパケットを受信しなければピアリングセッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージプロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。

この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するように hop-count の値を正確に設定する必要があります。また、この機能をマルチホップピアリングセッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。

このコマンドの設定には、次の制限が適用されます。

- この機能は、内部 BGP（iBGP）ピアではサポートされません。
- neighbor ttl-security コマンドは、すでに neighbor ebgp-multihop コマンドが設定されているピアには設定できません。これらのコマンドのコンフィギュレーションは相互に排他的であり、マルチホップ eBGP ピアリングセッションをイネーブルにする場合はどちらか一方のみを設定する必要があります。同じピアリングセッションに対して両方のコマンドを設定しようとすると、コンソールにエラーメッセージが表示されます。
- 大きい直径のマルチホップピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影響を受けたピアリングセッションをシャットダウンして、この攻撃に対処する必要がある場合があります。
- この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワークセグメント上のピアも含まれます。

例

次に、直接接続されたネイバーのホップ カウントを 2 に設定する例を示します。hop-count 引数が 2 に設定されるため、BGP は、ヘッダーの TTL カウントが 253 以上の IP パケットだけを受け入れます。IP パケットヘッダーの TTL 値がそれ以外の値であるパケットは、サイレントに廃棄されます。

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

次に、直接接続された BGPv6 ネイバーのホップ カウントを 2 に設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 ttl-security hops 2
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor ebgp-multihop	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor update-source

インターフェイスを BGP スピーキングネイバーの送信元として設定するには、アドレスファミリ コンフィギュレーションモードで **neighbor update-source** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

neighbor { *ipv_address* | *ipv6-address* } **update-source** { *interface name* }

構文の説明

ipv_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

interface name ASA が BGP ルーティングの送信元として使用する、*nameif* コマンドで指定されたインターフェイスの名前を指定します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.18(2) このコマンドが追加されます。

使用上のガイドライン

このコマンドは、ループバック インターフェイス上で BGP プロトコルを実行し、ループバック インターフェイスが再配布とプレフィックス アドバタイズメントに参加できるようにする場合に役立ちます。

例

次に、BGP ネイバー 10.108.1.1 の送信元としてループバック インターフェイス loop1 を更新する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 109
ciscoasa(config-router-af)# neighbor 10.108.1.1 update-source loop1
```

次に、BGP ネイバー 2001::1 の送信元としてループバック インターフェイス loop1 を更新する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 2001::1 remote-as 109
ciscoasa(config-router-af)# neighbor 2001::1 update-source loop1
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	ルーティング テーブルに BGP またはマルチプロトコル BGP のルーティング エントリを追加します。

neighbor version

特定のバージョンの BGP だけを受け入れるように ASA ソフトウェアを設定するには、アドレスファミリ コンフィギュレーションモードで **neighbor version** コマンドを使用します。デフォルトのバージョンレベルのネイバーを使用するには、このコマンドの **no** 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **version number**
no neighbor { *ip_address* | *ipv6-address* } **version number**

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

number BGP バージョン番号。バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

コマンド デフォルト

BGP バージョン 4。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) *ipv6-address* 引数が追加され、IPv6 アドレスファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを入力すると、バージョンの動的なネゴシエーションがディセーブルになります。

例

次に、BGP プロトコルをバージョン 4 だけに制限する例を示します。

```
ciscoasa(config)# router bgp 109  
ciscoasa(config-router)# address-family ipv4  
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4  
ciscoasa(config-router-af)# neighbor 2001::1 version 4
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリー コンフィギュレーションモードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor weight

ネイバー接続に重みを割り当てるには、アドレス ファミリ コンフィギュレーション モードで `neighbor weight` コマンドを使用します。重みの割り当てを削除するには、このコマンドの `no` 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **weight number**
no neighbor { *ip_address* | *ipv6-address* } **weight number**

構文の説明

ip_address ネイバー ルータの IP アドレス。

ipv6-address ネイバー ルータの IPv6 アドレス。

number 割り当てる重み。
有効な値は、0 ~ 65535 です。

コマンド デフォルト

別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

9.2(1) このコマンドが追加されました。

9.3(2) `ipv6-address` 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このネイバーから学習したすべてのルートに、まず重みが割り当てられます。特定のネットワークへのルートが複数ある場合、重みが最大のルートが優先ルートとして選ばれます。

`set weight route-map` コマンドで割り当てた重みは、`neighbor weight` コマンドで割り当てた重みより優先されます。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、172.16.12.1 から学習したすべてのルートの重みを 50 に設定しています。

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

次のアドレス ファミリ コンフィギュレーション モードの例では、2001::1 から学習したすべてのルートの重みを設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 weight 50
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

nem

ハードウェアクライアントのネットワーク拡張モードを有効にするには、グループポリシーコンフィギュレーションモードで **nem enable** コマンドを使用します。NEM を無効にするには、**nem disable** コマンドを使用します。実行コンフィギュレーションから NEM 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループポリシーの値を継承できます。

nem { enable|disable }

no nem

構文の説明

disable ネットワーク拡張モードをディセーブルにします。

enable ネットワーク拡張モードをイネーブルにします。

コマンドデフォルト

ネットワーク拡張モードはディセーブルになっています。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループポリシーコンフィギュレーション	• 対応	—	• 対応	—	—

使用上のガイドライン

ネットワーク拡張モードを使用すると、ハードウェアクライアントは、VPN トンネルを介したリモートプライベートネットワークへの単一のルーティング可能なネットワークを提供できます。IPsecは、ハードウェアクライアントの背後にあるプライベートネットワークからASAの背後にあるネットワークへのトラフィックをすべてカプセル化します。PATは適用されません。したがって、ASAの背後にあるデバイスは、ハードウェアクライアントの背後にある、トンネルを介したプライベートネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェアクライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

例

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
ciscoasa
(config)#
  group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
```

netmod

ネットワークモジュールを無効にするには、グローバル コンフィギュレーション モードで **netmod** コマンドを使用します。ネットワークモジュールを有効にするには、このコマンドの **no** 形式を使用します。



(注) このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

netmod 2 disable
no netmod 2 disable

構文の説明

2 スロット 2 のモジュールを指定します。

disable ネットワークモジュールを無効にしました。

コマンド デフォルト

最初の起動時にインストールされていたモジュールは、有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース 変更内容

9.17(1) このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、このコマンドを使用します。

新しいモジュールを追加したり、モジュールを完全に削除したりする場合は、リロードが必要です。リロードすることなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。ネットワークモジュールを別のタイプに交換する場合は、リロードが必要

要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

例

次に、ネットワークモジュールを無効にする例を示します。

```
ciscoasa(config)# netmod 2 disable
```

次に、ネットワークモジュールを有効にする例を示します。

```
ciscoasa(config)# no netmod 2 disable
```

network (アドレスファミリー)

ボーダー ゲートウェイ プロトコル (BGP) ルーティングプロセスでアドバタイズするネットワークを指定するには、アドレスファミリー コンフィギュレーション モードで **network** コマンドを使用します。ルーティング テーブルからエントリを削除するには、このコマンドの **no** 形式を使用します。

```
network { ipv4_address [ mask network_mask ] | IPv6_prefix | prefix_length | prefix_delegation_name
[ subnet_prefix | prefix_length ] } [ route-map route_map_name ]
no network { ipv4_address [ mask network_mask ] | IPv6_prefix | prefix_length |
prefix_delegation_name [ subnet_prefix | prefix_length ] } [ route-map route_map_name ]
```

構文の説明

<i>ipv4_address</i>	BGP またはマルチプロトコル BGP でアドバタイズする IPv4 ネットワーク。
<i>ipv6_prefix/prefix_length</i>	BGP またはマルチプロトコル BGP でアドバタイズする IPv6 ネットワーク。
mask <i>network_mask</i>	(オプション) ネットワークまたはサブネットワークのマスクとそのアドレス。
<i>prefix_delegation_name</i>	DHCPv6 プレフィックス委任クライアント (ipv6 dhcp client pd) を有効にすると、プレフィックスをアドバタイズできます。
<i>subnet_prefix/prefix_length</i>	(オプション) プレフィックスをサブネットするには、 <i>subnet_prefix/prefix_length</i> プレフィックス長を指定します。
route-map <i>route_map_name</i>	(オプション) 設定されているルートマップの ID。ルートマップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。このキーワードを指定し、ルートマップ タグを 1 つも指定しないと、いずれのネットワークもアドバタイズされません。

コマンド デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリー コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

9.2(1) このコマンドが追加されました。

9.6(2) `prefix_delegation_name [subnet_prefix/prefix_length]` 引数が追加されました。

使用上のガイドライン

BGP およびマルチプロトコル BGP のネットワークは、接続されたルート、ダイナミック ルーティング、およびスタティック ルートの情報源から学習できます。

使用できる `network` コマンドの最大数は、設定されている NVRAM や RAM など、ルータのリソースで決まります。

例

次に、ネットワーク 10.108.0.0 を BGP アップデートに含めるように設定する例を示します。

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

関連コマンド

コマンド	説明
<code>show bgp interfaces</code>	BGP ルーティングテーブル内のエントリを表示します。

network (ルータ EIGRP)

EIGRP ルーティングプロセスのネットワークのリストを指定するには、ルータ コンフィギュレーションモードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

```
network ip_addr [ mask ]
no network ip_addr [ mask ]
```

構文の説明

ip_addr 直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、EIGRP ルーティング プロセスに参加します。

mask (任意) IP アドレスのネットワーク マスク。

コマンド デフォルト

ネットワークは指定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

8.0(2) このコマンドが追加されました。

使用上のガイドライン

network コマンドは、指定されたネットワークに IP アドレスが少なくとも 1 つ存在するすべてのインターフェイスで EIGRP を開始します。また、指定されたネットワークから接続済みのサブネットを EIGRP トポロジテーブルに挿入します。

次に、ASA は一致したインターフェイス経由でネイバーを確立します。ASA に設定できる **network** コマンドの数に制限はありません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして EIGRP を定義する例を示します。

```
ciscoasa(config)# router eigrp 100
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0  
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp interfaces	EIGRP に設定されているインターフェイスに関する情報を表示します。
show eigrp topology	EIGRP トポロジ テーブルを表示します。

network (ルータ RIP)

RIPルーティングプロセスのネットワークのリストを指定するには、ルータコンフィギュレーションモードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

```
network { ip_addr | ipv6-address } | < prefix-length >
no network { ip_addr | ipv6-address } | < prefix-length > [ route-map route-map-name ]
```

構文の説明

<i>ip_addr</i>	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、RIP ルーティングプロセスに参加します。
<i>ipv6-address</i>	使用する IPv6 アドレス。IPv6 アドレスは、X:X:X:X の形式で入力する必要があります。
<i>prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 有効な値は、0 ~ 128 です。
<i>route-map-name</i>	属性を変更するルートマップ。

コマンドデフォルト

ネットワークは指定されていません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション、アドレスファミリーコンフィギュレーションモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

7.2(1) このコマンドが追加されました。

リリース 変更内容

- 9.0(1) マルチ コンテキスト モードのサポートが追加されました。
-
- 9.3(2) ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。
-

使用上のガイドライン

指定されたネットワーク番号は、サブネット情報に含めないでください。ルータで使用できる network コマンドの数に制限はありません。指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング更新が送受信されます。また、インターフェイスのネットワークが指定されていない場合は、どのRIPルーティング更新でもインターフェイスがアドバタイズされません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティングプロトコルとして RIP を定義する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
In the following example the attributes of the test-route-map route map connected to the
2001::1 network will be modified.
ciscoasa(config-router)# network 2001:0:0:0::1 route-map test-route-map
```

関連コマンド

コマンド	説明
router rip	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバルルータ コンフィギュレーションのコマンドを表示します。

network-acl

access-list コマンドを使用して以前に設定したファイアウォールの ACL 名を指定するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **network-acl** コマンドを使用します。既存のネットワーク ACL を削除するには、このコマンドの **no** 形式を使用します。すべてのネットワーク ACL を削除するには、このコマンドを引数なしで使用します。

network-acl name

no network-acl [name]

構文の説明

name ネットワーク ACL の名前を指定します。名前の最大文字数は 240 文字です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック アクセス ポリ シー レコード コンフィギュ レーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

8.0(2) このコマンドが追加されました。

使用上のガイドライン

複数のファイアウォール ACL を DAP レコードに割り当てるには、このコマンドを複数回使用します。

ASA は、指定された各 ACL を検証して、アクセスリストエントリの許可ルールのみまたは拒否ルールのみが含まれていることを確認します。指定されたいずれかの ACL に許可ルールと拒否ルールが混在している場合、ASA はコマンドを拒否します。

次に、Finance Restrictions というネットワーク ACL を Finance という DAP レコードに適用する例を示します。

```
ciscoasa
(config)#
```

```
dynamic-access-policy-record Finance
```

```

ciscoasa
(config-dynamic-access-policy-record)#
network-acl Finance Restrictions
ciscoasa
(config-dynamic-access-policy-record)#

```

関連コマンド

コマンド	説明
access-policy	ファイアウォールアクセス ポリシーを設定します。
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record <i>[name]</i>	すべてのDAP レコードまたは指定したDAP レコードの実行コンフィギュレーションを表示します。

network area

OSPFが動作するインターフェイスを定義し、そのインターフェイスのエリアIDを定義するには、ルータ コンフィギュレーションモードで **network area** コマンドを使用します。アドレス/ネットマスクのペアで定義されたインターフェイスのOSPFルーティングを無効にするには、このコマンドの **no** 形式を使用します。

network addr mask area area_id
no network addr mask area area_id

構文の説明

addr [IP Address]。

area area_id OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進表記で指定できます。10 進表記で指定する場合、有効な値の範囲は、0 ~ 4294967295 です。

mask ネットワーク マスク。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリー 変更内容
 ス

7.0(1) このコマンドが追加されました。

使用上のガイドライン

インターフェイスでOSPFを動作させるには、インターフェイスのアドレスを **network area** コマンドの対象にする必要があります。**network area** コマンドがインターフェイスのIPアドレスを対象にしていない場合、そのインターフェイスを経由するOSPFは有効になりません。

ASA で使用できる **network area** コマンドの数に制限はありません。

例

次に、192.168.1.1 インターフェイスでOSPFをイネーブルにし、エリア2に割り当てる例を示します。

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバルルータ コンフィギュレーションのコマンドを表示します。

network-object

ホストオブジェクト、ネットワークオブジェクト、またはサブネットオブジェクトをネットワークオブジェクトグループに追加するには、オブジェクトグループネットワークコンフィギュレーションモードで **network-object** コマンドを使用します。ネットワークオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object { **host** *address* | *IPv4_address mask* | *IPv6_address* | *IPv6_prefix* | **object name** }
no network-object { **host** *ip_address* | *ip_address mask* | **object name** }

構文の説明

host <i>ip_address</i>	ホストの IPv4 アドレスまたは IPv6 アドレスを指定します。
<i>IPv4_address mask</i>	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。
<i>IPv6_address/IPv6_prefix</i>	IPv6 ネットワークアドレスおよびプレフィックス長を指定します。
object name	ネットワークオブジェクト (object network コマンドで作成) を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクトグループ ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容

- 8.3(1) ネットワークオブジェクト (**object network** コマンド) をサポートするために、**object** 引数が追加されました。
- 9.0(1) 以前は、ネットワークオブジェクトグループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりません。現在は、ネットワークオブジェクトグループで IPv4 と IPv6 の両方のアドレスの混合がサポートされるようになりました。ただし、NAT で混合グループを使用することはできません。

使用上のガイドライン **network-object** コマンドは、ホストオブジェクト、ネットワークオブジェクト、またはサブネットオブジェクトを定義するために、**object-group** コマンドとともに使用されます。

例

次に、**network-object** コマンドを使用して、新しいホストオブジェクトをネットワーク オブジェクト グループに作成する例を示します。

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての object-group コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object network	ネットワーク オブジェクトを追加します。
object-group network	ネットワーク オブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

network-service-member

ネットワーク サービス グループにネットワーク サービス オブジェクトを追加するには、オブジェクト グループ コンフィギュレーション モードで **network-service-member** コマンドを使用します。オブジェクトをグループから削除するには、コマンドの **no** 形式を使用します。

network-service-member *object_name*
no network-service-member *object_name*

構文の説明

object_name ネットワーク サービス オブジェクトの名前。名前にスペースが含まれている場合は、その名前を二重引用符で囲みます。

コマンド デフォルト

デフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ネットワーク サービス オブジェクトグループ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.17(1) このコマンドが追加されました。

例

次に、3つの既存のネットワーク サービス オブジェクトをネットワーク サービス オブジェクト グループに追加する例を示します。

```
object-group network-service SaaS_Applications
  description This group includes relevant 'Software as a Service' applications
  network-service-member "outlook 365"
  network-service-member webex
  network-service-member box
```

関連コマンド

コマンド	説明
clear object-group	オブジェクトグループのヒットカウントをクリアします。
object-group network-service	ネットワーク サービス オブジェクト グループを定義します。
show object-group network-service	ネットワークサービスオブジェクトとそれぞれのヒットカウントを表示します。

nis address

DHCPv6 サーバーの設定時にネットワーク インフォメーションサービス (NIS) アドレスをステートレスアドレス自動設定 (SLAAC) クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nis address** コマンドを使用します。NIS サーバーを削除するには、このコマンドの **no** 形式を使用します。

```
nis address nis_ipv6_address
no nis address nis_ipv6_address
```

構文の説明

nis_ipv6_address NIS の IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

9.6(2) このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求 (IR) パケットを ASA に送信したときに、NIS アドレスを含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2つの IPv6 DHCP プールを作成して、2つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```

ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nis domain-name

DHCPv6 サーバーの設定時にネットワーク インフォメーションサービス (NIS) ドメイン名をステートレスアドレス自動設定 (SLAAC) クライアントに提供するには、IPv6 DHCP プール コンフィギュレーションモードで **nis domain-name** コマンドを使用します。NIS ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

nis domain-name *nis_domain_name*
no nis domain-name *nis_domain_name*

構文の説明

nis_domain_name NIS ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コン フィギュ レー ション	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

9.6(2) このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求 (IR) パケットを ASA に送信したときに、NIS ドメイン名を含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```

ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
    
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nisp address

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス プラス (NIS+) サーバーの IP アドレスをステートレスアドレス自動設定 (SLAAC) クライアントに提供するには、IPv6 DHCP プールコンフィギュレーションモードで **nisp address** コマンドを使用します。NIS+ サーバーを削除するには、このコマンドの **no** 形式を使用します。

nisp address nisp_ipv6_address
no nisp address nisp_ipv6_address

構文の説明

nisp_ipv6_address NIS+サーバーの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
 ス

9.6(2) このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求 (IR) パケットを ASA に送信したときに、NIS+サーバーを含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2つの IPv6 DHCP プールを作成して、2つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```

ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nisp domain-name

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス プラス (NIS+) ドメイン名をステートレスアドレス自動設定 (SLAAC) クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nisp domain-name** コマンドを使用します。NIS+ ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

nisp domain-name *nisp_domain_name*
no nisp domain-name *nisp_domain_name*

構文の説明

nisp_domain_name NIS+ ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コン フィギュ レー ション	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

9.6(2) このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求 (IR) パケットを ASA に送信したときに、NIS+ ドメイン名を含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```

ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag

```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nop

IP オプションインスペクションが設定されたパケットヘッダーで No Operation IP オプションが発生したときに実行するアクションを定義するには、パラメータコンフィギュレーションモードで **nop** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

```
nop action { allow | clear }
no nop action { allow | clear }
```

構文の説明

allow No Operation IP オプションを含むパケットを許可します。

clear No Operation オプションをパケットヘッダーから削除してから、パケットを許可します。

コマンドデフォルト

デフォルトでは、IP オプションインスペクションは、No Operation IP オプションを含むパケットをドロップします。

IP オプションインスペクションポリシーマップで **default** コマンドを使用すると、デフォルト値を変更できます。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

8.2(2) このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプションインスペクションポリシーマップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍

数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合は、オプションが 32 ビット境界に合うように、No Operation (NOP) または IP オプション 1 が「内部パディング」として使用されます。

例

次に、IP オプションインスペクションのアクションをポリシーマップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシーマップのクラスマップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクションクラスマップを作成します。
policy-map	レイヤ 3/4 のポリシーマップを作成します。
show running-config policy-map	現在のポリシーマップコンフィギュレーションをすべて表示します。

nsf cisco

Open Shortest Path First (OSPF) を実行している ASA で Cisco ノンストップ フォワーディング (NSF) 動作をイネーブルにするには、ルータ コンフィギュレーション モードで `nsf cisco` コマンドを使用します。デフォルトに戻るには、`no` 形式のコマンドを使用します。

nsf cisco [enforce global]

no nsf cisco [enforce global]

構文の説明

enforce global (オプション) NSF の再起動時にいずれかのインターフェイスで NSF 認識でないネイバー ネットワーキング デバイスが検出された場合に、すべてのインターフェイスで再起動をキャンセルします。

コマンド デフォルト

Cisco NSF グレースフル リスタートはデフォルトではディセーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、OSPF ルータで Cisco NSF がイネーブルになります。ルータで NSF がイネーブルになっている場合、ルータは NSF 対応であり、リスタートモードで動作します。

ルータが NSF グレースフル リスタートを実行するネイバーとしか連携しないと想定される場合、隣接するルータで NSF をサポートするシスコ ソフトウェア リリースが実行されている必要がありますが、ルータで NSF が設定されている必要はありません。NSF をサポートするシスコ ソフトウェア リリースを実行している場合、ルータは NSF 認識です。

デフォルトでは、隣接する NSF 認識ルータは、グレースフル リスタート時に NSF ヘルパーモードで動作します。

NSF グレースフル リスタートの実行時にネットワーク インターフェイスで NSF 認識でないネイバーが検出された場合、そのインターフェイスでのみ再起動が中止され、他のインターフェイスではグレースフル リスタートが続行されます。再起動時に NSF 認識でないネイバーが検

出された場合に OSPF プロセス全体で再起動をキャンセルするには、`enforce global` キーワードを指定してこのコマンドを設定します。



- (注) ネイバーとの隣接関係のリセットが任意のインターフェイスで検出された場合、または、OSPF インターフェイスがダウンした場合も、プロセス全体で NSF の再起動がキャンセルされます。

例

次に、`enforce global` オプションを指定して Cisco NSF グレースフルリスタートをイネーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# cisco nsf enforce global
```

関連コマンド

コマンド	説明
<code>nsf cisco helper</code>	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
<code>nsf ietf</code>	IETF NSF をイネーブルにします。

nsf cisco helper

Open Shortest Path First (OSPF) を実行している ASA で Cisco ノンストップ フォワーディング (NSF) ヘルパー モードをイネーブルにするには、ルータ コンフィギュレーション モードで `nsf cisco helper` コマンドを使用します。Cisco NSF ヘルパー モードはデフォルトでイネーブルになり、ルータ コンフィギュレーション モードで `no nsf cisco helper` を発行することでディセーブルにできます。

nsf cisco helper
no nsf cisco helper

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Cisco NSF ヘルパー モードはデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
 ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

ASA で NSF をイネーブルにしている場合、この ASA は NSF 対応であると考えられ、グレースフル リスタート モードで動作します。OSPF ルータ プロセスは、ルート プロセッサ (RP) スイッチオーバーのため、ノンストップ フォワーディング の復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディング の復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディング の復帰を ASA で支援しないようにするには、`no nsf cisco helper` コマンドを入力します。

例

次に、NSF ヘルパー モードをディセーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa  
(config-router)# no nsf cisco helper
```

関連コマンド

コマンド	説明
<code>nsf cisco</code>	ASA で Cisco NSF をイネーブルにします。
<code>nsf ietf</code>	IETF NSF をイネーブルにします。

nsf ietf

OSPF を実行している ASA で Internet Engineering Task Force (IETF) NSF 動作をイネーブルにするには、ルータ コンフィギュレーション モードで `nsf ietf` コマンドを使用します。デフォルトに戻るには、`no` 形式のコマンドを使用します。

nsf ietf [*restart-interval seconds*]
no nsf ietf

構文の説明

restart-interval seconds (オプション) グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ~ 1800 です。デフォルトは 120 です。

(注) 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

コマンド デフォルト

IETF NSF グレースフル リスタート モードはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
 ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、ASA で IETF NSF がイネーブルになります。ASA で NSF がイネーブルになっている場合、ASA は NSF 対応であり、リスタート モードで動作します。

ASA が NSF グレースフル リスタートを実行するネイバーとしか連携しないと想定される場合、隣接する ASA で NSF がサポートされている必要がありますが、ルータで NSF が設定されている必要はありません。NSF をサポートするアプリケーションを実行している場合、ASA は NSF 認識です。

例

次に、NSF ヘルパー モードをディセーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa  
(config-router)# nsf ietf restart-interval 240
```

関連コマンド

コマンド	説明
nsf cisco	ASA で Cisco NSF をイネーブルにします。
nsf cisco helper	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
nsf ietf helper	ASA で IETF NSF ヘルパー モードをイネーブルにします。

nsf ietf helper

IETF NSF ヘルパー モードはデフォルトでイネーブルになります。IETF NSF ヘルパー モードを明示的にイネーブルにするには、ルータ コンフィギュレーション モードで `nsf ietf helper` コマンドを使用します。ディセーブルにするには、このコマンドの `no` 形式を使用します。

必要に応じて、`nsf ietf helper strict-lsa-checking` コマンドを使用してリンクステート アドバタイズメント (LSA) の厳密なチェックを有効にできます。

nsf ietf helper [strict-lsa-checking]

no nsf ietf helper

構文の説明

strict-lsa-checking (オプション) ヘルパー モードの厳密なリンクステート アドバタイズメント (LSA) をイネーブルにします。

コマンド デフォルト

IETF NSF ヘルパー モードはデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.3(1) このコマンドが追加されました。

使用上のガイドライン

ASA が NSF をイネーブルにしている場合、ASA は NSF 対応であると考えられ、グレースフルリスタート モードで動作します。OSPF プロセスは、ルート プロセッサ (RP) スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフルリスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、`no nsf ietf helper` コマンドを入力します。

NSF 認識 ASA および NSF 対応 ASA の両方で厳密な LSA チェックをイネーブルにするには、`nsf ietf helper strict-lsa-checking` コマンドを入力します。ただし、IETF グレースフルリスタート プロセス時に ASA がヘルパー ASA になるまでは厳密な LSA チェックは有効になりません。

厳密な LSA チェックをイネーブルにすると、ヘルパー ASA は、LSA の変更があるために再起動 ASA にフラッシュされる場合、または、グレースフルリスタートプロセスが開始されたときに再起動 ASA の再送リスト内の LSA に変更があると検出された場合、再起動 ASA のプロセスの支援を終了します。

例

次に、厳密な LSA チェックを指定して IETF NSF ヘルパーをイネーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# nsf ietf helper strict-lsa-checking
```

関連コマンド

コマンド	説明
nsf cisco	ASA で Cisco NSF をイネーブルにします。
nsf cisco helper	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
nsf ietf	ASA で IETF NSF をイネーブルにします。

nt-auth-domain-controller

このサーバーの NT プライマリ ドメイン コントローラの名前を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **nt-auth-domain-controller** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

nt-auth-domain-controller *string*
no nt-auth-domain-controller

構文の説明

string このサーバーのプライマリ ドメインコントローラの名前を最大 16 文字で指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コン フィギュレー ション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
 ス

7.0(1) このコマンドが追加されました。

使用上のガイドライン

このコマンドは、NT 認証 AAA サーバに対してのみ有効です。ホスト コンフィギュレーションモードを開始するには、まず **aaa-server host** コマンドを使用する必要があります。*string* 変数の名前は、そのサーバー自体の NT エントリに一致する必要があります。

例

次に、このサーバーの NT プライマリ ドメイン コントローラの名前を「primary1」に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol nt
ciscoasa
(config-aaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa
(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	ホスト固有の AAA サーバー パラメータを設定できるように、aaa サーバー ホスト コンフィギュレーション モードを開始します。
clear configure aaa-server	すべての AAA コマンドステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

ntp authenticate

NTPサーバーによる認証を有効にするには、グローバルコンフィギュレーションモードで **ntp authenticate** コマンドを使用します。NTP認証を無効にするには、このコマンドの **no** 形式を使用します。

ntp authenticate
no ntp authenticate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

使用上のガイドライン

認証を有効にしている、NTPサーバーがパケットで正しい信頼できるキーを使用している場合 (**ntp trusted-key** コマンドを参照)、ASA はその NTP サーバーとのみ通信します。サーバーキーも指定する必要があります (**ntp server key** コマンドを参照)。サーバーキーを指定しないと、ASA は、**ntp authenticate** コマンドが設定されている場合でも、認証なしでサーバーと通信します。また、ASA は認証キーを使用して NTP サーバーと同期します (**ntp authentication-key** コマンドを参照)。

例

次に、2つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
```

```
ciscoasa(config)# ntp authentication-key 2 md5  
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバーを指定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバーで認証するキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

```
ntp authentication-key key_id { md5 | sha1 | sha256 | sha512 | cmac } key
no ntp authentication-key key_id [ { md5 | sha1 | sha256 | sha512 | cmac } [ 0|8 ] key ]
```

構文の説明

0 (任意) <key_value> がプレーンテキストであることを示します。0 または 8 が示されない場合、形式はプレーンテキストです。

8 (任意) <key_value> が暗号化されたテキストであることを示します。0 または 8 が示されない場合、形式はプレーンテキストです。

key キー値を最大 32 文字のストリングとして設定します。

key_id キー ID 1 ~ 4294967295 を識別します。この ID は、**ntp trusted-key** コマンドを使用して信頼できるキーとして指定する必要があります。

md5 認証アルゴリズムとして MD5 を指定します。

sha1 認証アルゴリズムとして SHA-1 を指定します。

sha256 認証アルゴリズムとして SHA-256 を指定します。

sha512 認証アルゴリズムとして SHA-512 を指定します。

cmac 認証アルゴリズムとして AES-CMAC を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

リリース 変更内容

9.13(1) **sha1**、**sha256**、**sha512**、および**cmac** キーワードが追加されました。

使用上のガイドライン NTP 認証を使用するには、**ntp authenticate** コマンドと **ntp server key** コマンドも設定する必要があります。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバーを指定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

NTP サーバーを指定して、ASA 上の時間を設定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

```
ntp server ip_address [ key key_id ][ source interface_name ][ prefer ]
no ntp server ip_address [ key key_id ][ source interface_name ][ prefer ]
```

構文の説明

<i>ip_address</i>	NTP サーバーの IPv4 または IPv6 IP アドレスを設定します。
key key_id	ntp authenticate コマンドを使用して認証を有効にした場合は、このサーバーの信頼できるキー ID を設定します。 ntp trusted-key コマンドも参照してください。
source interface_name	ルーティング テーブルにデフォルトのインターフェイスを使用しない場合に、NTP パケットの発信インターフェイスを識別します。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。
prefer	精度に差がないサーバーが複数ある場合は、この NTP サーバーを優先サーバーとして設定します。NTP では、どのサーバーの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバーに同期します。サーバーの精度に差がない場合は、 prefer キーワードで使用するサーバーを指定します。ただし、優先サーバーよりも精度が大幅に高いサーバーがある場合、ASA は精度の高いそのサーバーを使用します。たとえば、ASA は優先サーバーであるストラタム 3 のサーバーよりもストラタム 2 のサーバーを使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリー 変更内容
ス

7.0(1) このコマンドは、送信元インターフェイスを任意とするように変更されました。

リリース 変更内容

9.12(1) IPv6 のサポートが追加されました。

9.14(1) NTPv4 のサポートが追加されました。

使用上のガイドライン

NTP を使用して階層的なサーバシステムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバーを設定できます。ASA は、データ信頼度の尺度となる一番下のストラタムのサーバーを選択します。マルチ コンテキスト モードでは、システム コンフィギュレーションにのみ NTP サーバーを設定します。

手動で設定した時刻はすべて、NTP サーバーから取得された時刻によって上書きされます。

ASA は NTPv4 をサポートします。

例

次に、2つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

NTP サーバーによる認証を必要とする信頼できるキーに認証キー ID を指定するには、グローバルコンフィギュレーションモードで **ntp trusted-key** コマンドを使用します。信頼できるキーを削除するには、このコマンドの **no** 形式を使用します。複数のサーバーで使用できるように複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*
no ntp trusted-key *key_id*

構文の説明

key_id キー ID 1 ~ 4294967295 を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース 変更内容
 ス

7.0(1) このコマンドが追加されました。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドと **ntp server key** コマンドも設定する必要があります。サーバーと同期するには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次に、2つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバーを指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

num-packets

SLA 動作中に送信される要求パケットの数を指定するには、SLA モニター プロトコル コンフィギュレーションモードで **num-packets** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

num-packets *number*
no num-packets *number*

構文の説明

number SLA 動作中に送信されるパケットの数。有効な値は、1 ~ 100 です。

(注) このコマンドで **number** 引数として指定したすべてのパケットが失われた場合は、追跡したルートで障害が発生しています。

コマンド デフォルト

エコー タイプの場合に送信されるデフォルトのパケット数は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
SLA モニター プロトコル コンフィギュ レーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリー 変更内容
ス

7.2(1) このコマンドが追加されました。

使用上のガイドライン

パケット損失のために到達可能性情報が不正確になるのを防ぐには、送信されるデフォルトのパケット数を増やします。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロードサイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。5 つのパケットがすべて失われるまでは、追跡したルートは削除されません。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
```

```
ciscoasa(config-sla-monitor-echo)# request-data-size 48  
ciscoasa(config-sla-monitor-echo)# timeout 4000  
ciscoasa(config-sla-monitor-echo)# threshold 2500  
ciscoasa(config-sla-monitor-echo)# frequency 10  
ciscoasa(config)# sla monitor schedule 123 life forever start-time now  
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

nve

VXLAN カプセル化のためのネットワーク仮想化エンドポイント (NVE) インスタンスを作成するには、グローバル コンフィギュレーション モードで **nve** コマンドを使用します。NVE インスタンスを削除するには、このコマンドの **no** 形式を使用します。

nve 1
no nve 1

構文の説明

1NVE インスタンスを指定します (常に1)。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

9.4(1) このコマンドが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに1つの VTEP 送信元インターフェイスを設定できます。この VTEP 送信元インターフェイスを指定する NVE インスタンスを1つ設定できます。すべての VNI インターフェイスはこの NVE インスタンスに関連付けられている必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャストグループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャストグループアドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレステーブル）を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。

コマンド	説明
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

nve-only

VXLAN 送信元インターフェイスが NVE のみであることを指定するには、インターフェイス コンフィギュレーション モードで **nve-only** コマンドを使用します。NVE のみという制限を削除するには、このコマンドの **no** 形式を使用します。

nve-only
 [**cluster**]
no nve-only

構文の説明

構文の説明

cluster ASA 仮想 クラスタリングを構成する場合、クラスタ制御リンクの **nve-only cluster** を指定する必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
 ス

9.4(1) このコマンドが追加されました。

9.17(1) ASA 仮想 クラスタリングをサポートするために、**cluster** キーワードが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント (NVE) として定義されます。VXLAN VTEP が現時点でサポートされている NVE です。

トランスペアレントモードでは、VTEP インターフェイスに関して **nve-only** を設定する必要があり、VTEP インターフェイスの IP アドレスを設定できます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されるルーテッドモードではオプションです。

ASA 仮想 クラスタリングの場合、クラスタ制御リンクに VXLAN インターフェイスを使用する必要があります。この場合、**nve-only cluster** を指定します。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、そのインターフェイスが NVE のみであることを指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャストグループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモートセグメントドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレステーブル）を表示します。

コマンド	説明
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元 インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理 インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元 インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元 インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元 インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。