CHAPTER 21

nac コマンド～ override-account-disable コマンド

nac

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またはディセーブルにするには、グループ ポリシー コンフィギュレーション モードで **nac** コマンドを使用します。デフォルトのグループ ポリシーから NAC 設定を継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

nac {enable | disable}

no nac [enable | disable]

シンタックスの説明

enable	NAC をイネーブルにします。リモート アクセスにはポスチャ確認が必要です。リモート コンピュータが確認チェックをパスすると、ACS サーバはセキュリティ アプライアンスのアクセス ポリシーをダウンロードして施行します。
disable	NAC をディセーブルにします。

デフォルト

デフォルト設定はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　アクセス コントロール サーバがネットワーク上に存在する必要があります。

例

次の例では、グループ ポリシー用に NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)
```

次の例では、グループ ポリシー用に NAC をディセーブルにします。

```
hostname(config-group-policy)# nac disable
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから NAC 設定を継承します。

```
hostname(config-group-policy)# no nac
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバまたは AAA サーバ グループのレコードを作成し、ホスト固有の AAA サーバ アトリビュートを設定します。
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージ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-authentication-server-group	認証サーバのグループがネットワーク アドミッション コントロールのポスチャ確認に使用されることを示します。

nac-authentication-server-group

ネットワーク アドミッション コントロールのポスチャ確認に使用される認証サーバのグループを特定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **nac-authentication-server-group** を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を継承するには、継承元となる別のグループ ポリシーにアクセスして、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

シンタックスの説明

server-group	**aaa-server host** コマンドを使用してセキュリティ アプライアンスで設定された、ポスチャ確認サーバ グループの名前です。この名前は、aaa-server host コマンドで指定した server-tag 変数と一致している必要があります。

デフォルト

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

NAC をサポートするために、アクセス コントロール サーバを少なくとも 1 つ設定します。**aaa-server** コマンドを使用して ACS グループに名前を付けます。
次に、**nac-authentication-server-group** コマンドを使用します。サーバ グループには同じ名前を使用します。

例

次の例では、acs-group1 を NAC のポスチャ確認に使用する認証サーバ グループとして指定します。

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

次の例では、デフォルトのリモート アクセス グループから認証グループを継承します。

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

関連コマンド

コマンド	説明
aaa-server	AAA サーバまたは AAA サーバ グループのレコードを作成し、ホスト固有の AAA サーバ アトリビュートを設定します。
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージ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 ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-default-acl

ポスチャ認証に失敗するネットワーク アドミッション コントロール セッションのデフォルト ACL として使用する ACL を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-default-acl** コマンドを使用します。

nac-default-acl value *acl-name*

nac-default-acl none

デフォルトのグループ ポリシーから ACL を継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

no nac-default-acl

シンタックスの説明

acl-name	セキュリティ アプライアンスで設定されているとおりに、**aaa-server host** コマンドを使用してポスチャ確認サーバ グループに名前を付けます。この名前は、aaa-server host コマンドで指定した server-tag 変数と一致している必要があります。
none	デフォルトのグループ ポリシーからの ACL の継承をディセーブルにします。ポスチャ確認に失敗する NAC セッションに ACL を適用しません。

デフォルト

デフォルトは **none** です。

NAC はデフォルトでディセーブルになっているので、セキュリティ アプライアンスを経由する VPN トラフィックは、NAC がイネーブルになるまで NAC のデフォルト ACL の影響を受けません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ポスチャ確認の失敗時に適用される ACL として acl-1 を指定します。

```
hostname(config-group-policy)# nac-default-acl value acl-1
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから ACL を継承します。

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーからの ACL の継承をディセーブルにします。ポスチャ確認に失敗する NAC セッションに ACL は適用されません。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージ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 ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-reval-period

ネットワーク アドミッション コントロール セッションでのポスチャ確認の成功後から次のポスチャ確認までの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-reval-period** コマンドを使用します。デフォルトのグループ ポリシーから再確認のタイマーを継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

nac-reval-period *seconds*

no nac-reval-period [*seconds*]

シンタックスの説明

seconds	正常に完了した各ポスチャ確認の間隔を示す秒数。範囲は 300 ～ 86400 です。

デフォルト

デフォルト値は 36000 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、ポスチャ確認が成功すると再確認のタイマーを開始します。このタイマーが切れると、無条件のポスチャ確認が開始されます。セキュリティ アプライアンスは再確認中、ポスチャ確認を維持します。デフォルトのグループ ポリシーは、アクセス コントロール サーバがポスチャ確認または再確認中に無効な場合に有効になります。

例

次の例では、再確認タイマーを 86400 秒に変更します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから再確認タイマーの値を継承します。

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージ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 ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-sq-period

ネットワーク アドミッション コントロール セッションでのポスチャ確認が成功してからホスト ポスチャの変更に関する次のクエリーまでの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-sq-period** コマンドを使用します。デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承元となる別のグループ 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-sq-period *seconds*

no nac-sq-period [*seconds*]

シンタックスの説明

seconds	正常に完了した各ポスチャ確認の間隔を示す秒数。範囲は 300 ～ 1800 です。

デフォルト

デフォルト値は 300 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスはポスチャ確認とステータス クエリーの応答が正常に実行された後、ステータス クエリー タイマーを開始します。このタイマーが切れると、*ステータス クエリー*と呼ばれる、ホスト ポスチャの変更に関するクエリーが開始されます。

例

次の例では、ステータス クエリー タイマーの値を 1800 秒に変更します。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承します。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージ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 ポリシーでネットワーク アドミッション コントロールをイネーブルにします。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。

name

名前を IP アドレスに関連付けるには、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。コンフィギュレーションから名前を削除することなく、テキスト名の使用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。

name *ip_address name* [description *text*]]

no name *ip_address* **[***name* [description *text*]**]**

シンタックスの説明

description	（オプション）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。a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアの文字を使用します。*name* は、63 文字以下にする必要があります。また、*name* の先頭は数字にはできません。
text	この説明のテキストを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.0(4)	オプションとして description を使用できるように機能が拡張されました。

使用上のガイドライン

IP アドレスとの名前の関連付けをイネーブルにするには、***names*** コマンドを使用します。IP アドレスに関連付けることができるのは、1 つの名前だけです。

まず **names** コマンドを使用してから、**name** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドの直後、かつ **write memory** コマンドの前に使用してください。

name コマンドを使用すると、ホストをテキスト名で識別し、テキスト文字列を IP アドレスにマッピングできます。**no name** コマンドを使用すると、テキスト名を使用できないようにできますが、コンフィギュレーションから名前は削除しません。名前のリストをコンフィギュレーションから消去するには、***clear configure name*** コマンドを使用します。

name 値の表示をディセーブルにするには、**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 コマンドでは、ネットワーク マスクに名前を割り当てることはサポートされていません。たとえば、次のコマンドは拒否されます。

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

（注）　マスクを必要とするどのコマンドも、受け入れたネットワーク　マスクとして名前を処理できません。

例

次の例は、**names** コマンドによって、**name** コマンドの使用をイネーブルにする方法を示しています。**name** コマンドは、192.168.42.3 への参照の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用できるようにします。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際に、**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ディセーブルにします。その後で **names** コマンドを再度使用すると、**name** コマンド値の表示が元に戻ります。

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(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

hostname(config)# no names
hostname(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

hostname(config)# names
hostname(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	名前のリストをコンフィギュレーションから消去します。
names	IP アドレスとの名前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

インターフェイスに名前を付けるには、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。セキュリティ アプライアンスのすべてのコンフィギュレーション コマンドで、インターフェイス タイプと ID（gigabitethernet0/1 など）ではなくインターフェイス名が使用されるので、トラフィックがインターフェイスを通過できるようにするにはインターフェイス名が必要です。

nameif *name*

no nameif

シンタックスの説明

name	最大 48 文字の名前を設定します。名前は大文字と小文字の区別がありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、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 モードの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、**vlan** コマンドを使用して VLAN を割り当ててから、**nameif** コマンドを入力する必要があります。

新しい値でこのコマンドを再入力することによって、名前を変更できます。**no** 形式のコマンドは入力しないでください。このコマンドを入力すると、該当する名前に適用されるコマンドがすべて削除されます。

例

次の例では、2 つのインターフェイスの名前を「inside」と「outside」に設定します。

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

関連コマンド

コマンド	説明
clear xlate	既存の接続に関するすべての変換をリセットして、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 モードに入ります。
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

name コマンドで設定可能な、IP アドレスから名前への変換をイネーブルにするには、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。アドレスから名前への変換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。

names

no names

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

name コマンドで設定した IP アドレスとの名前の関連付けをイネーブルにするには、**names** コマンドを使用します。**name** または **names** コマンドを入力する順番は、重要ではありません。

例

次の例は、名前と IP アドレスとの関連付けをイネーブルにする方法を示してします。

```
hostname(config)# names
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
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ている名前のリストを表示します。
show running-config names	IP アドレスから名前への変換を表示します。

name-separator

電子メール、VPN ユーザ名、およびパスワード間のデリミタとして文字を指定するには、該当する電子メール 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

シンタックスの説明

symbol	（オプション）電子メール、VPN ユーザ名、およびパスワード間を区切る文字。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。

デフォルト

デフォルトは、「:」（コロン）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前セパレータには、サーバ セパレータと異なるものを指定する必要があります。

例

次の例は、POP3S の名前セパレータとしてハッシュ（#）を設定する方法を示しています。

```
hostname(config)# pop3s
hostname(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名を区切ります。

nat

別のインターフェイスのマッピング アドレスに変換される、1 つのインターフェイスのアドレスを指定するには、グローバル コンフィギュレーション モードで **nat** コマンドを使用します。このコマンドは、ダイナミック NAT または PAT を設定します。ダイナミック NAT または PAT では、アドレスをマッピング アドレスのいずれかのプールに変換します。**nat** コマンドを削除するには、このコマンドの **no** 形式を使用します。

標準ダイナミック NAT の場合：

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

ポリシー ダイナミック NAT と NAT 免除の場合：

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

シンタックスの説明

access-list *access_list_name*	拡張アクセス リスト（別名、ポリシー NAT）を使用して、ローカル アドレスと宛先アドレスを指定します。**access-list** コマンドを使用してアクセス リストを作成します。***eq*** 演算子を使用して、アクセス リストにローカル ポートと宛先ポートをオプションで指定できます。NAT ID が **0** の場合、アクセス リストは NAT から免除されたアドレスを指定します。NAT 免除はポリシー NAT とは異なります。たとえば、ポート アドレスを指定できません。 **（注）** アクセス リストのヒット カウント（**show access-list** コマンドを参照）は、NAT 免除アクセス リストの場合は増分されません。
dns	（オプション）このコマンドに一致する DNS 応答で、A レコード（アドレス レコード）を書き直します。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。 DNS サーバにエントリがあるホストのアドレスが NAT 文に含まれ、クライアントとは異なるインターフェイスに DNS サーバがある場合、クライアントと DNS サーバに必要なホスト アドレスはそれぞれ異なります。一方にはグローバル アドレスが必要で、もう一方にはローカル アドレスが必要です。変換対象のホストは、クライアントまたは DNS サーバのどちらかと同じインターフェイス上になければなりません。通常、他のインターフェイスからのアクセスを許可する必要があるホストがスタティック トランスレーションを使用するので、このオプションは **static** コマンドと併せて使用するのが一般的です。

emb_limit	（オプション）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実際のアドレスを指定します。**0.0.0.0**（または短縮形の **0**）を使用すると、すべてのアドレスを指定できます。
mask	（オプション）実際のアドレスのサブネット マスクを指定します。マスクを入力しない場合、IP アドレス クラスのデフォルト マスクが使用されます。
nat_id	NAT ID の整数を指定します。標準 NAT の場合、この整数は 1 ～ 2147483647 です。ポリシー NAT（nat id access-list）の場合、この整数は 1 ～ 65535 です。 アイデンティティ NAT（**nat 0**）と NAT 免除（**nat 0 access-list**）は、**0** の NAT ID を使用します。 **global** コマンドはこの ID を参照して、グローバル プールを *real_ip* に関連付けます。
norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは、外部 NAT には適用されません。ファイアウォールがランダム化するのは、セキュリティの高いインターフェイスに対してホストまたはサーバが生成する ISN のみです。外部 NAT に対して **norandomseq** を設定しても、その **norandomseq** キーワードは無視されます。
outside	（オプション）このインターフェイスのセキュリティ レベルが、**global** 文の一致で特定するインターフェイスより低い場合、**outside** を入力する必要があります。この機能は、外部 NAT または双方向 NAT と呼ばれます。
tcp *tcp_max_conns*	サブネット全体に関して、同時 TCP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。
udp *udp_max_conns*	（オプション）サブネット全体に関して、同時 UDP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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	透過	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	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、1 つの **global** コマンドと一致します。

セキュリティ アプライアンスは、NAT 規則がトラフィックに一致する場合に、アドレスを変換します。NAT 規則が一致しない場合、パケットの処理が続行します。例外は、**nat-control** コマンドを使用して NAT コントロールをイネーブルにする場合です。NAT コントロールでは、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）に移動するパケットが NAT 規則に一致する必要があります。一致していないと、パケットの処理が停止します。NAT コントロールをイネーブルにした場合でも、NAT は同一セキュリティ レベルのインターフェイスでは必要ありません。必要に応じて、オプションで NAT を設定できます。

ダイナミック NAT は、宛先ネットワークでルーティング可能なマッピング アドレスのプールに実際のアドレスのグループを変換します。マッピング プールは、実際のグループより少ないアドレスで構成されます。変換するホストが宛先ネットワークにアクセスするときに、セキュリティ アプライアンスがマッピング プールの IP アドレスをホストに割り当てます。実際のホストが接続を開始する場合にのみ、変換が追加されます。変換が有効なのは接続されている間だけなので、所定のユーザが変換のタイムアウト後も同じ IP アドレスを維持することはありません（**timeout xlate** コマンドを参照）。そのため、アクセス リストによって接続が許可されている場合でも、ダイナミック NAT（または PAT）を使用するホストに、宛先ネットワーク上のユーザから確実に接続を開始できません。また、実ホスト アドレスに直接接続しようとすると、セキュリティ アプライアンスが拒否します。ホストへの信頼できるアクセスについては、**static** コマンドを参照してください。

ダイナミック NAT には、次の短所があります。

- マッピング プール内のアドレスが実際のグループより少ない場合、トラフィック量が予想を超えるとアドレスが不足する可能性があります。

  PAT は単一アドレスのポートを使用して 64,000 を超える変換を実行できるので、この現象が頻繁に発生する場合は、PAT を使用してください。
- マッピング　プールで大量のルーティング可能なアドレスを使用しなければなりません。インターネットなどの登録アドレスが宛先ネットワークに必要な場合は、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、GRE バージョン 0 のように、オーバーロードするポートを持たない IP プロトコルでは、PAT は動作しません。一部のマルチメディア アプリケーションのように、あるポートでデータ ストリームを流して別のポートで制御パスを提供するオープンスタンダードではない一部のアプリケーションでも、PAT は動作しません。

PAT では、複数の実アドレスを 1 つのマッピング IP アドレスに変換します。具体的には、セキュリティ アプライアンスが実アドレスと送信元ポート（実ソケット）をマッピング アドレスと一意なポート（マッピング ソケット）に変換します。送信元ポートが TCP/UDP の場合、送信元アドレスは PAT を使用して同じ範囲のアドレスに変換されます。範囲には、1 ～ 511、512 ～ 1023、および 1024 ～ 65535 が含まれます。送信元ポートはそれぞれの接続で異なるので、各接続には別個の変換が必要になります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

接続の期限が切れると、ポートの変換も 30 秒の非アクティビティの後、期限切れになります。タイムアウトは、設定できません。

PAT で使用できるマッピング アドレスは 1 つなので、ルーティング可能なアドレスの節約になります。セキュリティ アプライアンスのインターフェイス IP アドレスを PAT アドレスとして使用することもできます。PAT は、データ ストリームが制御パスと異なる一部のマルチメディア アプリケーションでは動作しません。

（注） 変換中であれば、リモート ホストは、アクセス リストで許可されているかぎり変換対象のホストへの接続を開始できます。アドレスは（実際のアドレスとマッピング アドレスの両方とも）予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続が成功した場合は、アクセス リストのセキュリティに頼ることができます。

NAT コントロールをイネーブルにする場合、内部ホストは、外部ホストにアクセスするときに NAT 規則に一致する必要があります。一部のホストで NAT を実行しない場合は、それらのホストで NAT をバイパスできます（または、NAT コントロールをディセーブルにできます）。たとえば、NAT をサポートしていないアプリケーションを使用する場合に、NAT をバイパスすることになる可能性があります。**static** コマンドを使用して NAT をバイパスするか、次のいずれかのオプションを使用できます。

- アイデンティティ NAT（**nat 0** コマンド）：アイデンティティ NAT（ダイナミック NAT と類似）を設定する場合、特定のインターフェイスのホストの変換を制限しません。すべてのインターフェイスを通過する接続に、アイデンティティ NAT を使用する必要があります。そのため、インターフェイス A にアクセスするときに、実際のアドレスで標準変換を実行し、インターフェイス B にアクセスするときに、アイデンティティ NAT を使用するといった選択はできません。これに対して、標準ダイナミック NAT を使用した場合は、アドレスを変換する特定のインターフェイスを指定できます。アクセス リストに基づいて使用可能なすべてのネットワーク上で、アイデンティティ NAT を使用する実際のアドレスがルーティング可能でなければなりません。

  アイデンティティ NAT の場合、マッピング アドレスが実際のアドレスと同じでも、（アクセス リストで許可されている場合を含めて）外部から内部へ接続を開始することはできません。この機能では、スタティック アイデンティティ NAT または NAT 免除を使用してください。
- NAT 免除（**nat 0 access-list** コマンド）：NAT 免除を使用すると、変換対象のホストとリモート ホストの両方で接続を開始できます。アイデンティティ NAT と同様、特定のインターフェイスのホストに対する変換を制限しないでください。すべてのインターフェイスを通過する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実際のアドレスを決定するときに（ポリシー NAT と同様）、実際のアドレスと宛先アドレスを指定できるので、NAT 免除を使用すると詳細な制御が可能になります。一方、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートは考慮されません。

ポリシー NAT では、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象の実アドレスを指定できます。オプションで、送信元ポートと宛先ポートも指定できます。標準 NAT で考慮されるのは、実際のアドレスだけです。たとえば、実際のアドレスがサーバ A にアクセスするときはマッピング アドレス A に変換できますが、サーバ B にアクセスするときにはマッピング アドレス B に変換できます。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

（注）　NAT 免除を除くすべてのタイプの NAT がポリシー NAT をサポートしています。NAT 免除では、アクセス リストを使用して実際のアドレスを指定しますが、ポートが考慮されない点がポリシー NAT と異なります。ポリシー NAT をサポートしていない**スタティック** アイデンティティ NAT を使用すると、NAT 免除と同じ結果を得られます。

別の方法として、モジュラ ポリシー フレームワークを使用して接続制限（ただし初期接続制限はでない）を設定できます。詳細については、**set connection** コマンドを参照してください。NAT を使用する場合、初期接続制限のみが設定できます。同じトラフィックに対して両方の方法を使用してこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

NAT コンフィギュレーションを変更し、既存の変換のタイムアウトを待機せずに新しい NAT 情報が使用される場合、**clear xlate** コマンドを使用して、変換テーブルを消去できます。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

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

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

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

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

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

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

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

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

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

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

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
clear configure nat	NAT コンフィギュレーションを削除します。
global	グローバル アドレス プールに対してエントリを作成します。
interface	インターフェイスを作成および設定します。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

nat（VPN ロード バランシング）

この装置の IP アドレスが NAT で変換される先の IP アドレスを設定するには、VPN ロードバランシング モードで **nat** コマンドを使用します。この NAT 変換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 *ip-address*

no nat [*ip-adddress*]

シンタックスの説明

ip-address	この NAT で、この装置の IP アドレスを変換する先の IP アドレス。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

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 モードに入る必要があります。

このコマンドの **no nat** 形式では、オプションの *ip-address* 値を指定する場合、IP アドレスが実行コンフィギュレーションの既存の NAT IP アドレスと一致する必要があります。

例

次は、VPN ロードバランシング コマンド シーケンスの例です。NAT 変換のアドレスを 192.168.10.10 に設定する **nat** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(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 モードに入ります。

nat-control

NAT コントロールを適用するには、グローバル コンフィギュレーション モードで **nat-control** コマンドを使用します。NAT コントロールでは、内部ホストが外部にアクセスする場合、内部ホストには NAT が必要になります。NAT コントロール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-control

no nat-control

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

NAT コントロールは、デフォルトではディセーブルです（**no nat-control** コマンド）。ただし、ソフトウェアを以前のバージョンからアップグレードしたときに、以前のバージョンでデフォルトがイネーブルであった場合は、NAT コントロールがイネーブルになることがあります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

NAT コントロールでは、内部インターフェイスから外部インターフェイスに移動するパケットは、1 つの NAT 規則に一致している必要があります。外部ネットワークのホストにアクセスする内部ネットワークのホストではすべて、内部ホスト アドレスを変換するように NAT を設定してください。

同じセキュリティ レベルのインターフェイスでは、通信用に NAT を使用する必要はありません。ただし、NAT コントロールがイネーブルになっている状態で同じセキュリティ インターフェイスのダイナミック NAT または PAT を設定する場合、内部インターフェイスから同じセキュリティのインターフェイスあるいは外部インターフェイスへのトラフィックはすべて、NAT 規則に一致している必要があります。

同様に、NAT コントロールと共に外部のダイナミック NAT または PAT をイネーブルにする場合、内部インターフェイスへのアクセス時には、すべての外部トラフィックが 1 つの NAT 規則に一致している必要があります。

NAT コントロールを使用するスタティック NAT では、このような制限は発生しません。

デフォルトでは、NAT コントロールはディセーブルになっているため、NAT の実行を選択しないかぎり、ネットワーク上で NAT を実行する必要はありません。

NAT コントロールのセキュリティを強化する必要があるが、内部アドレスが変換されることを望まない場合は、これらのアドレスに NAT 免除（**nat 0 access-list**）またはアイデンティティ NAT（**nat 0** または **static**）規則が適用できます。

（注）　マルチ コンテキスト モードでは、パケット分類子はパケットをコンテキストに割り当てるために、NAT 設定に依存する場合があります。NAT コントロールがディセーブルであるという理由で NAT を実行しない場合、分類子によってはネットワーク コンフィギュレーションの変更が必要になることがあります。

例

次の例では、NAT コントロールをイネーブルにします。

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

関連コマンド

コマンド	説明
nat	1 つのインターフェイス上のアドレスを他の 1 つのインターフェイス上のマッピング アドレスに変換することを定義します。
show running-config nat-control	NAT コンフィギュレーションの要件を表示します。
static	実アドレスをマッピング アドレスに変換します。

nat-rewrite

DNS 応答の A レコードに埋め込まれた IP アドレスに対して NAT リライトをイネーブルにするには、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合はイネーブルにできます。このコマンドをディセーブルにするには、**no nat-rewrite** をポリシー マップ コンフィギュレーションで明示的に指定する必要があります。**inspect dns** を設定していない場合、NAT リライトは実行されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この機能は、DNS 応答で 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

次の例では、DNS 検査ポリシー マップで NAT リライトをイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

nbns-server（トンネル グループ webvpn アトリビュート モード）

NBNS サーバを設定するには、トンネル グループ webvpn 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。NBNS サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは NBNS サーバに照会して、NetBIOS 名を IP アドレスにマッピングします。リモート システム上のファイルにアクセスしたり、ファイルを共有したりするため、WebVPN には NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [***master***] [***timeout*** *timeout*] [***retry*** *retries*]

no nbns-server

シンタックスの説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバの照会をリトライする回数を指定します。セキュリティ アプライアンスは、ユーザが指定した回数、サーバのリストを循環した後で、エラー メッセージを送信します。デフォルト値は 2 です。有効な範囲は、1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	セキュリティ アプライアンスがクエリーを再送信する前の待機時間を指定します。NBNS サーバが 1 つのみの場合は同じサーバに、複数ある場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒です。有効な範囲は、1 ～ 30 秒です。

デフォルト

デフォルトでは、NBNS サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
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 モードに変更されました。

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 アトリビュート モードの同等のコマンドに変換されます。

最大 3 つのサーバ エントリを設定できます。設定する最初のサーバはプライマリ サーバで、残りの 2 つのサーバは冗長構成用のバックアップになります。

一致するエントリをコンフィギュレーションから削除するには、**no** オプションを使用します。

例

次の例は、10.10.10.19 の IP アドレス、10 秒のタイムアウト値、および 8 回のリトライでマスター ブラウザである NBNS サーバを設定して使用して、トンネル グループ「テスト」を設定する方法を示しています。また、10.10.10.24 の IP アドレス、15 秒のタイムアウト値、および 8 回のリトライで NBNS WINS サーバを設定する方法を示しています。

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

関連コマンド

コマンド	説明
clear configure group-policy	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。
show running-config group-policy	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。
tunnel-group webvpn-attributes	名前付きのトンネル グループの WebVPN アトリビュートを指定します。

nbns-server（webvpn モード）

NBNS サーバを設定するには、トンネル グループ webvpn 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。NBNS サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは NBNS サーバに照会して、NetBIOS 名を IP アドレスにマッピングします。リモート システム上のファイルにアクセスしたり、ファイルを共有したりするため、WebVPN には NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname*} [***master***] [***timeout*** *timeout*] [***retry*** *retries*]

no nbns-server

シンタックスの説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバの照会をリトライする回数を指定します。セキュリティ アプライアンスは、ユーザが指定した回数、サーバのリストを循環した後で、エラー メッセージを送信します。デフォルト値は 2 です。有効な範囲は、1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	セキュリティ アプライアンスがクエリーを再送信する前の待機時間を指定します。NBNS サーバが 1 つのみの場合は同じサーバに、複数ある場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒です。有効な範囲は、1 ～ 30 秒です。

デフォルト

デフォルトでは、NBNS サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
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 モードに変更されました。

使用上のガイドライン

このコマンドは、webvpn コンフィギュレーション モードでは廃止されました。トンネル グループ webvpn アトリビュート コンフィギュレーション モードの nbns-server コマンドで置き換えられています。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 アトリビュート モードの同等のコマンドに変換されます。

最大 3 つのサーバ エントリを設定できます。設定する最初のサーバはプライマリ サーバで、残りの 2 つのサーバは冗長構成用のバックアップになります。

一致するエントリをコンフィギュレーションから削除するには、**no** オプションを使用します。

例

次の例は、10.10.10.19 の IP アドレス、10 秒のタイムアウト値、および 8 回のリトライでマスターブラウザである NBNS サーバを設定する方法を示しています。また、10.10.10.24 の IP アドレス、15 秒のタイムアウト値、および 8 回のリトライで NBNS WINS サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

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 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。スタティックに定義されたネイバーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。**neighbor** コマンドは、VPN トンネルを介して OSPF ルートをアドバタイジングする場合に使用します。

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

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

シンタックスの説明

interface *name*	（オプション）**nameif** コマンドで指定されるインターフェイス名。これを介して、ネイバーに到達できるようになります。
ip_address	隣接ルータの IP アドレス。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

既知の各非ブロードキャスト ネットワーク ネイバーに、ネイバー エントリが 1 つ含まれている必要があります。インターフェイスのプライマリ アドレスに、ネイバー アドレスが存在する必要があります。

システムに直接接続されているインターフェイスと同じネットワーク上にネイバーがない場合、***interface*** オプションが指定されている必要があります。さらに、ネイバーに到達するには、スタティック ルートが作成されている必要があります。

例

次の例では、192.168.1.1 のアドレスの隣接ルータを定義します。

```
hostname(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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

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イネーブルにするには、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 をディセーブルにするには、**nem disable** コマンドを使用します。NEM アトリビュートを実行コンフィギュレーションから削除するには、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、値を別のグループ ポリシーから継承できます。

nem {**enable** | **disable**}

no nem

シンタックスの説明

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。

デフォルト

ネットワーク拡張モードはディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

使用上のガイドライン

ネットワーク拡張モードにより、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 ネットワークに対して、ルーティング可能なネットワークを 1 つ提示できます。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 ネットワークからセキュリティ アプライアンス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、セキュリティ アプライアンスの背後にある装置は、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。ハードウェア クライアントがトンネルを開始する必要がありますが、トンネルがアップの状態になった後は、どちらの側から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
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループ ポリシーの NEM を設定する方法を示しています。

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

network

RIP ルーティング プロセスのネットワーク 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*

no network *ip_addr*

シンタックスの説明

ip_addr	直接接続されたネットワークの IP アドレスを指定します。指定されたネットワークに接続されたインターフェイスは、RIP ルーティング プロセスに参加します。

デフォルト

指定されているネットワークはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

指定のネットワーク番号にサブネット情報を含めないようにしてください。ルータで使用できるネットワーク コマンドの数には制限がありません。RIP ルーティング アップデートは、指定されたネットワークのインターフェイスを経由してのみ送受信されます。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、そのインターフェイスは RIP アップデートでアドバタイズされません。

例

次の例では、ネットワーク 10.0.0.0 および 192.168.7.0 に接続された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 を定義します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# network 192.168.7.0
```

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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

network area

OSPF が動作するインターフェイスを定義し、これら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したインターフェイスの OSPF ルーティング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。

network *addr mask* ***area*** *area_id*

no network *addr mask* ***area*** *area_id*

シンタックスの説明

addr	IP アドレスを指定します。
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 進数形式のいずれかで指定できます。10 進数形式で指定した場合、有効値の範囲は 0 ～ 4294967295 です。
mask	ネットワーク マスク。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

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、**network area** コマンドでインターフェイスのアドレスが指定されている必要があります。**network area** コマンドでカバーされていないインターフェイスの IP アドレスがあれば、そのインターフェイス上では OSPF がイネーブルになりません。

セキュリティ アプライアンスで使用できる **network area** コンドの数には制限がありません。

例

次の例では、192.168.1.1 のインターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てます。

```
hostname(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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

network-object

ネットワーク オブジェクト グループにネットワーク オブジェクトを追加するには、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 *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

シンタックスの説明

host_addr	ホスト IP アドレス（**name** コマンドを使用してホスト名がまだ定義されていない場合）。
host_name	ホスト名（**name** コマンドを使用してホスト名が定義されている場合）。
net_addr	ネットワーク アドレス。*netmask* と共に使用してサブネット オブジェクトを定義します。
netmask	ネットマスク。*net_addr* と共に使用してサブネット オブジェクトを定義します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ネットワーク コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ネットワーク コンフィギュレーション モードでホストまたはサブネット オブジェクトを定義するには、**object-group** コマンドと共に **network-object** コマンドを使用します。

例

次の例は、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用して、新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
hostname(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-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

nt-auth-domain-controller

このサーバの NT プライマリ ドメイン コントローラ名を指定するには、AAA サーバ ホスト 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

シンタックスの説明

string	このサーバの、最大 16 文字のプライマリ ドメイン コントローラ名を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT 認証の AAA サーバでのみ有効です。最初に **aaa-server host** コマンドを使用して、ホスト コンフィギュレーション モードに入る必要があります。*string* 変数の名前は、サーバ自体の NT エントリに一致する必要があります。

例

次の例では、このサーバの NT プライマリ ドメイン コントローラ名を「primary1」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文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、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

ntp authenticate

NTP サーバを使用する認証をイネーブルにするには、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。

ntp authenticate

no ntp authenticate

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

認証をイネーブルにすると、セキュリティ アプライアンスは、NTP サーバが正しい信頼できるキーをパケットで使用している場合に限り、NTP サーバと通信します（**ntp trusted-key** コマンドを参照）。セキュリティ アプライアンスは、認証キーを NTP サーバと同期をとるためにも使用します（**ntp authentication-key** コマンドを参照）。

例

次の例では、NTP パケットで認証キー 42 を使用しているシステムのみと同期するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
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 サーバを使用して認証を行うための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*** *key*

no ntp authentication-key *key_id* [***md5*** *key*]

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を指定します。**ntp trusted-key** コマンドを使用して、この ID を信頼できるキーとして指定する必要があります。
md5	MD5 として認証アルゴリズムを指定します。MD5 はサポートされている唯一のアルゴリズムです。
key	キーの値を、最大 32 文字の文字列として設定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(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 サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
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

セキュリティ アプライアンスの時刻を設定するために NTP サーバを指定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。Auto Update Server を削除するには、このコマンドの **no** 形式を使用します。複数のサーバを指定できます。セキュリティ アプライアンスは、最も正確なサーバを使用します。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 サーバを設定します。

ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

no ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

シンタックスの説明

ip_address	NTP サーバの 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イネーブルにする場合、このサーバの信頼できるキー 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 テーブルでデフォルトのインターフェイスを使用しない場合は、NTP パケットの発信インターフェイスを指定します。システムはマルチ コンテキスト モードのインターフェイスを包含しないので、管理コンテキストで定義されたインターフェイス名を指定します。
prefer	複数のサーバの正確性がほとんど変わらない場合、この NTP サーバを優先サーバとして設定します。NTP はアルゴリズムを使用して、最も正確なサーバを判別し、そのサーバと同期を取ります。複数のサーバの正確性がほとんど変わらない場合、***prefer*** キーワードが使用するサーバを指定します。しかし、特定のサーバの正確性が優先サーバより際立っている場合、セキュリティ アプライアンスはより正確なサーバを使用します。たとえば、セキュリティ アプライアンスは、優先された層 3 のサーバではなく、層 2 のサーバを使用します。

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

次の表は、このコマンドを入力できるモードを示しています。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、送信元インターフェイスをオプションで使用するように修正されました。

例

次の例では、2 つの NTP サーバを指定し、キー ID 1 と 2 の認証をイネーブルにします。

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(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 サーバと同期するための暗号化認証キーを設定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
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

信頼できるキー（NTP サーバを使用する認証に必要）として認証キー 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。複数のサーバで使用する、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*

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を設定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。サーバと同期を取るには、**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

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(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 サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
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 オペレーション中に送信される要求パケット数を指定するには、SLA モニタ 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*

シンタックスの説明

number	SLA オペレーション中に送信されるパケットの数を指定します。有効な値は 1 ～ 100 です。

デフォルト

送信されるエコー タイプのパケットのデフォルト数は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケット損失による正確でない到達情報を防止するために送信されるパケットのデフォルト数を増やします。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(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 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

object-group

コンフィギュレーションの最適化に使用できるオブジェクト グループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。コンフィギュレーションからオブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

no object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

シンタックスの説明

icmp-type	echo や echo-reply など、ICMP タイプのグループを定義します。メインの **object-group icmp-type** コマンドを入力した後、**icmp-object** コマンドと **group-object** コマンドを使用して ICMP オブジェクトを ICMP タイプ グループに追加します。
network	ホストまたはサブネット IP アドレスのグループを定義します。メインの **object-group network** コマンドを入力した後、**network-object** コマンドと **group-object** コマンドを使用してネットワーク オブジェクトをネットワーク グループに追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。
protocol	TCP や UDP などのプロトコル グループを定義します。メインの **object-group protocol** コマンドを入力した後、**protocol-object** コマンドと **group-object** コマンドを使用してプロトコル オブジェクトをプロトコル グループに追加します。
service	「eq smtp」や「range 2000 2010」などの TCP/UDP ポート仕様のグループを定義します。メインの **object-group service** コマンドを入力した後、**port-object** コマンドと **group-object** コマンドを使用してポート オブジェクトをサービス グループに追加します。
tcp	サービス グループが TCP に使用されることを指定します。
tcp-udp	サービス グループが TCP および UDP に使用できることを指定します。
udp	サービス グループが UDP に使用されることを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　ホスト、プロトコル、サービスなどのオブジェクトはグループ化できます。グループ化をすると、グループ名を使用して 1 つのコマンドを発行してグループ内のすべての項目に適用できます。

object-group コマンドでグループを定義してから、任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはグループ内のすべての項目に適用されます。この機能によってコンフィギュレーション サイズをかなり削減できます。

オブジェクト グループを定義したら、次のように、該当するすべてのセキュリティ アプライアンス コマンドで **object-group** キーワードの後にグループ名を使用する必要があります。

```
hostname# show running-config object-group group_name
```

group_name はグループの名前です。

次の例は、オブジェクト グループを定義した後で使用する方法を示しています。

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

また、**access list** コマンドの引数をグループ化できます。

個々の引数	代替用のオブジェクト グループ
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドは階層構造にグループ化できます。したがって、あるオブジェクト グループを別のオブジェクト グループのメンバーにできます。

オブジェクト グループを使用するには、次のことを実行する必要があります。

- **object-group** キーワードは、すべてのコマンドでオブジェクト グループ名の前に使用する。

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group
  locals object-group eng_svc
  ```

  ここで、*remotes* および *locals* はオブジェクト グループ名です。
- オブジェクト グループを空にしない。
- 別のコマンドで現在使用されている場合は、オブジェクト グループを削除したり、空にしたりすることはできない。

メインの **object-group** コマンドが入力されると、コマンド モードは対応するモードに変わります。オブジェクト グループは新規のモードで定義されます。アクティブ モードがコマンド プロンプト形式で示されます。たとえば、コンフィギュレーション端末モードのプロンプトは次のように表示されます。

```
hostname(config)#
```

ここで、*hostname* はセキュリティ アプライアンスの名前です。

しかし、**object-group** コマンドを入力すると、プロンプトは次のように表示されます。

```
hostname(config-type)#
```

hostname はセキュリティ アプライアンスの名前、*type* は*オブジェクト グループのタイプ*です。

object-group モードを抜け、**object-group** メイン コマンドを終了するには、**exit** や **quit** コマンド、または **access-list** コマンドなどの有効な任意のコンフィギュレーション モードのコマンドを使用します。

show running-config object-group コマンドは、定義されているすべてのオブジェクト グループを表示します。このとき、**show running-config object-group** *grp_id* コマンドを入力した場合は *grp_id* ごとに、**show running-config object-group** *grp_type* コマンドを入力した場合はグループ タイプごとに表示されます。引数を指定せずに **show running-config object-group** コマンドを入力すると、定義されているすべてのオブジェクト グループが表示されます。

それまでに定義した **object-group** コマンドのグループを削除するには、**clear configure object-group** コマンドを使用します。引数を指定せずに **clear configure object-group** コマンドを使用すると、コマンドで使用中でない定義済のオブジェクト グループすべてが削除できます。*grp_type* 引数は、コマンドで使用中でない定義済のオブジェクト グループすべてのうち、そのグループ タイプだけを削除します。

object-group モードでは、**show running-config** および **clear configure** コマンドを含む他のすべてのセキュリティ アプライアンス コマンドを使用できます。

object-group モード内のコマンドは、**show running-config object-group** コマンド、**write** コマンド、または **config** コンドで表示または保存した場合は、字下げして表示されます。

object-group モード内のコマンドには、メイン コマンドと同じコマンド特権レベルがあります。

access-list コマンドで複数のオブジェクト グループを使用している場合、このコマンドで使用されるすべてのオブジェクト グループの要素は相互に連結されます。最初に 1 番目のグループ要素が 2 番目のグループ要素に連結され、1 番目と 2 番目のグループ要素が 3 番目のグループ要素に連結されるというようになります。

説明テキストの開始位置は、**description** キーワードに続く空白（ブランクまたはタブ）直後の文字です。

例

次の例は、**object-group icmp-type** モードを使用して新しい icmp-type オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成し、既存のオブジェクト グループにマッピングする方法を示しています。

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

次の例は、**object-group protocol** モードを使用して新しいプロトコル オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

次の例は、**object-group service** モードを使用して新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

次の例は、テキスト説明をオブジェクト グループに追加およびオブジェクト グループから削除する方法を示しています。

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal
network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

次の例は、**group-object** モードを使用して、すでに定義済みのオブジェクトで構成される新しいオブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit

hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを使用しない場合は、*host_grp_1* と *host_grp_2* にすでに定義済みの IP アドレスをすべて含むように *all_hosts* グループを定義する必要があります。**group-object** コマンドを指定する場合は、重複してホストを定義する必要がなくなります。

次の例は、オブジェクト グループを使用してアクセス リストのコンフィギュレーションを簡略化する方法を示しています。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 172.23.56.10
hostname(config-network)# network-object host 172.23.56.20
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object host 172.23.56.195

hostname(config)# object-group service eng_svc ftp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

このグループ化により、グループ化を使用しないと 24 行になるアクセス リストを 1 行で設定できます。その代わり、グループ化を使用するとアクセス リストのコンフィギュレーションは次のようになります。

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

（注）　**show running-config object-group** コマンドおよび **write** コマンドを使用すると、オブジェクト グループ名で設定されているようにアクセス リストを表示できます。**show access-list** コマンドは、オブジェクトをグループ化せずに、アクセス リスト エントリを個々のエントリに展開して表示します。

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。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

ocsp disable-nonce

デフォルトでは、OCSP 要求にナンス拡張子が含まれます。これは、要求を暗号でバインドしてリプレイ アタックを防ぐためのものです。ただし、一部の OCSP サーバは、この照合ナンス拡張子が含まれない、事前に生成された応答を使用します。これらのサーバで OCSP を使用するには、ナンス拡張子をディセーブルにする必要があります。

ナンス拡張子をディセーブルにするには、暗号 CA トラストポイント モードで **ocsp disable-nonce** コマンドを使用します。ナンス拡張子をもう一度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。

ocsp disable-nonce

no ocsp disable-nonce

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトでは、OCSP 要求にナンス拡張子が含まれます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、OCSP 要求には OCSP ナンス拡張子が含まれず、セキュリティ アプライアンスはチェックを行いません。

例

次の例では、newtrust というトラストポイントのナンス拡張子をディセーブルにする方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp disable-nonce
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするための OCSP サーバを指定します。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

ocsp url

クライアント証明書の AIA 拡張子に指定されているサーバではなくトラストポイントに関連付けられているすべての証明書をチェックするよう、セキュリティ アプライアンスを使用して OCSP サーバを設定するには、暗号 CA トラストポイント モードで **ocsp url** コマンドを使用します。サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*

no ocsp url

シンタックスの説明

このコマンドには、キーワードも引数もありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは HTTP URL のみサポートし、各トランスポイントに URL を 1 つだけ指定できます。

セキュリティ アプライアンスでは OCSP サーバ URL を定義する方法が 3 つあり、定義する方法に従って次の順序で OCSP サーバの使用を試みます。

- **match certificate** コマンドを使用して設定する OCSP サーバ
- **ocsp url** コマンドを使用して設定する OCSP サーバ
- クライアント証明書の AIA フィールドの OCSP サーバ

match certificate コマンド、または **ocsp url** コマンドを使用して OCSP URL を設定しない場合、セキュリティ アプライアンスはクライアント証明書の AIA 拡張子で OCSP サーバを使用します。証明書に AIA 拡張が含まれていない場合、失効ステータスのチェックは失敗します。

例

次の例では、URL http://10.1.124.22 で OCSP サーバを設定する方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp url http://10.1.124.22
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

ospf authentication

OSPF 認証の使用をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf authentication** コマンドを使用します。デフォルトの認証スタンスに戻すには、このコマンドの **no** 形式を使用します。

ospf authentication [***message-digest*** | ***null***]

no ospf ***authentication***

シンタックスの説明

message-digest	（オプション）OSPF メッセージ ダイジェスト認証を使用するように指定します。
null	（オプション）OSPF 認証を使用しないように指定します。

デフォルト

デフォルトでは、OSPF 認証はイネーブルではありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。***message-digest*** キーワードを使用する場合、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージ ダイジェスト キーを設定します。

下位互換性を維持するため、エリアの認証タイプが継続してサポートされます。認証タイプがインターフェイスに指定されていない場合、エリアの認証タイプが使用されます（エリアのデフォルトは null 認証です）。

オプションを指定せずにこのコマンドを使用する場合、簡易パスワード認証がイネーブルにされます。

例

次の例は、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする方法を示しています。

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

関連コマンド

コマンド	説明
ospf *authentication-key*	隣接ルーティング デバイスで使用するためのパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

隣接ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

ospf *authentication-key* *password*

no ospf authentication-key

シンタックスの説明<

password	隣接ルーティング デバイスで使用するための OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字の間にブランク スペースを含めることができます。パスワードの最初または最後のスペースは無視されます。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドによって作成されたパスワードは、ルーティング プロトコル パケットが発信されるときに、OSPF ヘッダーに直接挿入されるキーとして使用されます。インターフェイス単位で、別個のパスワードを各ネットワークに割り当てることができます。同一ネットワーク上のすべての隣接ルータが、OSPF 情報を交換できる同じパスワードを持つ必要があります。

例

次の例は、OSPF 認証のパスワードを指定する方法を示しています。

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイスを介した 1 パケットの送信コストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイス コストをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ospf cost *interface_cost*

no ospf cost

シンタックスの説明

interface_cost	インターフェイスを介した 1 パケットの送信コスト（リンク状態メトリック）。これは 0 ～ 65535 の符号なし整数値です。0 は、インターフェイスに直接接続されているネットワークを表し、インターフェイスの帯域幅が高くなるほど、そのインターフェイスを通してパケットを送信する関連コストは低くなります。つまり、大きいコスト値は低い帯域幅のインターフェイスを表し、小さいコスト値は高い帯域幅のインターフェイスを表します。 セキュリティ アプライアンス上にある OSPF インターフェイスのデフォルト コストは 10 です。このデフォルトは Cisco IOS ソフトウェアのデフォルト コスト、ファースト イーサネットおよびギガビット イーサネットの場合の 1、10BaseT の場合の 10 とは異なります。ECMP をネットワークで使用している場合は、このことを考慮に入れておくことが重要です。

デフォルト

デフォルトの *interface_cost* は 10 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでの 1 パケットの送信コストを明示的に指定できます。*interface_cost* パラメータは、0 ～ 65535 の符号なし整数値です。

no ospf cost コマンドを使用すると、パス コストをデフォルト値にリセットできます。

例

次の例は、選択したインターフェイスで 1 パケットの送信コストを指定する方法を示しています。

```
hostname(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定したインターフェイスのコンフィギュレーションを表示します。

ospf database-filter

同期およびフラッディング中に OSPF インターフェイスへのすべての発信 LSA をフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter ***all out***

no ospf database-filter ***all out***

シンタックスの説明

all out	OSPF インターフェイスへのすべての発信 LSA をフィルタリングします。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA のフォワーディングを復元します。

例

次の例は、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする方法を示しています。

```
hostname(config-if)# ospf database-filter all out
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-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。

ospf dead-interval *seconds*

no ospf dead-interval

シンタックスの説明

seconds	hello パケットを 1 つも受信しない時間。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（範囲は 1 ～ 65,535）。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドで設定した間隔の 4 倍です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（hello パケットを 1 つも受信しない時間）を設定できます。*seconds* 引数はデッド間隔を指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。*seconds* のフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（1 ～ 65,535）。

no ospf dead-interval コマンドを使用すると、デフォルトの間隔値に戻ります。

例

次の例では、OSPF デッド間隔を 1 分に設定します。

```
hostname(config-if)# ospf dead-interval 60
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイスで hello パケットを送信する間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf hello-interval

インターフェイスで hello パケットを送信する間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 間隔を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。

ospf hello-interval *seconds*

no ospf hello-interval

シンタックスの説明

seconds	インターフェイスで hello パケットを送信する間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

hello-interval *seconds* のデフォルト値は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔が短いほど、トポロジの変更が早急に検出されますが、より多くのルーティング トラフィックが結果として生じます。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、OSPF の hello 間隔を 5 秒に設定します。

```
hostname(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf message-digest-key

OSPF の MD5 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf message-digest-key** コマンドを使用します。MD5 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。

ospf message-digest-key *key-id* ***md5*** *key*

no ospf message-digest-key

シンタックスの説明

key-id	MD5 認証をイネーブルにし、数値による認証キー ID 番号を指定します。有効値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字によるパスワード。キー文字の間にスペースを含めることができます。キーの最初または最後のスペースは無視されます。MD5 認証は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。このコマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、1 ～ 255 の認証キー用数値 ID で、*key* は、最大 16 バイトの英数字によるパスワードです。MD5 は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

例

次の例は、OSPF 認証の MD5 キーを指定する方法を示しています。

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

関連コマンド

コマンド	説明
area authentication	OSPF エリア認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf mtu-ignore

データベース パケット受信時の OSPF の Maximum Transmission Unit（MTU; 最大伝送ユニット）ミスマッチ検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore

no ospf mtu-ignore

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、**ospf mtu-ignore** はイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF は、ネイバーが共通のインターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが Database Descriptor（DBD）パケットを交換するときに実行されます。DBD パケット受信時の MTU が着信インターフェイスに設定された IP MTU より高い場合、OSPF の隣接関係が確立されません。**ospf mtu-ignore** コマンドは、DBD パケット受信時の OSPF MTU ミスマッチ検出をディセーブルにします。これは、デフォルトでイネーブルになっています。

例

次の例は、**ospf mtu-ignore** コマンドをディセーブルにする方法を示しています。

```
hostname(config-if)# ospf mtu-ignore
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf network point-to-point non-broadcast

OSPF インターフェイスをポイントツーポイントの非ブロードキャスト ネットワークとして設定するには、インターフェイス コンフィギュレーション モードで **ospf network** ***point-to-point non-broadcast*** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。**ospf network** ***point-to-point non-broadcast*** コマンドを使用すると、VPN トンネルを介して OSPF ルートを送信できます。

ospf network ***point-to-point non-broadcast***

no ospf network ***point-to-point non-broadcast***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをポイントツーポイントとして指定する場合、OSPF ネイバーを手動で設定する必要があります。ダイナミック検出はできません。OSPF ネイバーを手動で設定するには、ルータ 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。

インターフェイスをポイントツーポイントとして設定すると、次の制約事項が適用されます。

- 2 つ以上のネイバーをインターフェイスに定義できない。
- 暗号エンドポイントに向かうスタティック ルートを定義する必要がある。
- ネイバーを明示的に設定しないと、インターフェイスが隣接関係を形成できない。
- トンネルを介した OSPF がインターフェイスで実行されている場合、同じインターフェイス上で上流のルータによる標準 OSPF を実行できない。
- VPN トンネルを介して OSPF アップデートを受け渡すように OSPF ネイバーを指定する前に、インターフェイスに暗号マップをバインドする必要がある。OSPF ネイバーを指定した後、暗号マップをインターフェイスにバインドする場合、**clear local-host all** コマンドを使用して、OSPF 接続を消去し、OSPF の隣接関係が VPN トンネルを介して確立されるようにします。

例

次の例は、選択したインターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして設定する方法を示しています。

```
hostname(config-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定された OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータの優先順位を変更するには、インターフェイス コンフィギュレーション モードで **ospf priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

ospf priority *number*

no ospf priority [*number*]

シンタックスの説明

number	ルータの優先順位を指定します。有効値は 0 ～ 255 です。

デフォルト

number のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ネットワークに接続されている 2 つのルータの両方が代表ルータになることを試行する場合、ルータの優先順位が高いルータが優先されます。両方のルータが同等である場合は、ルータ ID が高いルータが優先されます。ルータの優先順位が 0（ゼロ）に設定されているルータは、代表ルータまたはバックアップの代表ルータになる資格がありません。ルータの優先順位は、マルチアクセス ネットワーク（ポイントツーポイントではないネットワーク）へのインターフェイスにのみ設定されます。

例

次の例は、選択したインターフェイスで OSPF の優先順位を変更する方法を示しています。

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接ルータの LSA 再送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-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。

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

シンタックスの説明

seconds	インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

retransmit-interval *seconds* のデフォルト値は 5 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ルータは、LSA をネイバーに送信する場合に、確認応答メッセージを受信するまで LSA を保持します。確認応答を受信しない場合、ルータは LSA を再送信します。

このパラメータの設定を慎重に行う必要があります。そうしない場合、不要な再送信が生じます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次の例は、LSA の再送間隔を変更する方法を示しています。

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** 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。

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

シンタックスの説明

seconds	インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定します。デフォルト値は 1 秒で、範囲は 1 ～ 65,535 秒です。

デフォルト

seconds のデフォルト値は 1 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	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	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

アップデート パケットの LSA には、*seconds* 引数で指定された値ずつ加算された経過時間を格納してから送信する必要があります。値を割り当てるときは、インターフェイスの送信と伝搬遅延を考慮に入れる必要があります。

リンクを通じて送信される前に遅延が追加されていない場合、LSA がリンクを通じて伝播する時間が考慮されません。非常に低速のリンクでは、この設定は重要です。

例

次の例では、選択したインターフェイスの送信遅延を 3 秒に設定します。

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

outstanding

非認証の電子メール プロキシ セッションの数を制限するには、該当する電子メール プロキシ モードで **outstanding** コマンドを使用します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。これにより、非認証セッションは数が制限されずに許可されます。電子メール ポートに対する DoS 攻撃を制限するには、このコマンドを使用します。

電子メール プロキシ接続には、次の 3 つの状態があります。

1. 新しい電子メール接続は、「非認証」状態になります。
2. その接続でユーザ名が提示されると、「認証中」状態になります。
3. セキュリティ アプライアンスがその接続を認証すると、「認証済み」状態になります。

非認証状態の接続の数が、設定された限度を超えると、セキュリティ アプライアンスは、最も古い非認証接続を強制終了して、オーバーロードを防ぎます。認証済みの接続は、強制終了されません。

outstanding {*number*}

no outstanding

シンタックスの説明

number	許可される非認証セッション数。範囲は、1 ～ 1,000 です。

デフォルト

デフォルトは 20 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、POP3S 電子メール プロキシの非認証セッション数の限度を 12 に設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

override-account-disable

AAA サーバからのアカウント ディセーブル表示を無効にするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **override-account-disable** コマンドを使用します。表示の無効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。

override-account-disable

no override-account-disable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは「account-disabled」という表示を返すサーバ、たとえば NT LDAP を使用する RADIUS や、Kerberos に対して有効です。

このアトリビュートは、IPSec RA トンネル グループおよび WebVPN トンネル グループに設定できます。

例

次の例では、WebVPN トンネル グループ「testgroup」に対して AAA サーバからの「account-disabled」表示を無効にするようにします。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

次の例では、IPSec リモート アクセス トンネル グループ「Agroup」に対して AAA サーバからの「account-disabled」表示を無効にするようにします。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	特定のトンネル グループのトンネル グループ データベースまたはコンフィギュレーションを消去します。
tunnel-group general-attributes	トンネル グループ一般アトリビュート値を設定します。