CHAPTER 21

name ～ ospf transmit-delay コマンド

name

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。コンフィギュレーションからテキスト名を削除しないまま、使用でき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。

name *ip_address name*

no name *ip_address* [*name*]

シンタックスの説明

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る名前を指定します。使用する文字は a ～ z、A ～ Z、0 ～ 9、ダッシュ、および下線です。*name* の長さは 63 文字以下にする必要があります。また、*name* の先頭を数字にすることはできません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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

IP アドレスと名前の関連付けを可能にするには、***name*** コマンドを使用します。1 つの IP アドレスに関連付けることができる名前は 1 つだけです。

最初に **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** コマンドを使用してから **write memory** コマンドを使用するまでの間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たり、テキスト文字列を IP アドレスに関連付けたりできます。**no name** コマンドを使用すると、テキスト名の使用を禁止できますが、コンフィギュレーションからテキスト名は削除されません。設定から名前のリストを削除するには、***clear configure name*** コマンドを使用します。

name 値を表示できないようにするには、**no names** コマンドを使用します。

name および **names** コマンドは、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。

```
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、名前をネットワーク　マスクとして受け入れて処理することはできません。

例

次に、**names** コマンドを使用して、**name** コマンドを使用できるようにする例を示します。**name** コマンドにより、192.168.42.3 は **sa_inside** に、209.165.201.3 は **sa_outside** に置き換えられます。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場合は、これらの名前を **ip address** コマンドで使用できます。**no names** コマンドは、**name** コマンドの値を表示できないようにします。このコマンドのあとに **names** コマンドを使用すると、**name** コマンドの値を再び表示できるようになります。

```
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	コンフィギュレーションから名前のリストを消去します。
names	名前と IP アドレスの関連付けを可能にします。
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

インターフェイス名を指定するには、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。FWSM では、インターフェイス タイプ および ID（gigabitethernet1 など）の代わりに、インターフェイス名があらゆるコンフィギュレーション コマンドで使用されます。したがって、トラフィックにインターフェイスを通過させるには、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。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(1)	このコマンドが追加されました。
3.1(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 コマンドに変更されました。

使用上のガイドライン

新しい値を指定してこのコマンドを再入力すると、名前を変更できます。この場合、**no** 形式は使用しないでください。その名前を参照するすべてのコマンドが削除されてしまいます。

例

次に、2 つのインターフェイスに [inside] および [outside] という名前を設定する例を示します。

```
hostname(config)# interface gigabitethernet1
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
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	既存接続の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。

names

name コマンドで設定できる、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、引数またはキーワードはありません。

デフォルト　このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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　**names** コマンドは、***name*** コマンドで設定した IP アドレスに名前を関連付けられるようにする場合に使用します。**name** コマンドまたは **names** コマンドの入力順序は無関係です。

例　次に、IP アドレスに名前を関連付けられるようにする例を示します。

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

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リストを消去します。
name	IP アドレスに名前を関連付けます。
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。

nat

別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、特定のインターフェイス上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。このコマンドを使用すると、ダイナミック NAT（ネットワーク アドレス変換）または PAT（ポート アドレス変換）が設定され、マッピング アドレス プールの 1 つにアドレスが変換されます。**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 および 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 アドレスおよび宛先アドレスを指定します。アクセス リストは、**access-list** コマンドを使用して作成します。アクセス リストには、許可のアクセス制御エントリだけを指定する必要があります。***eq*** 演算子を使用して、任意でアクセス リストにローカル ポートおよび宛先ポートを指定できます。NAT ID が **0** の場合は、アクセス リストで NAT から除外するアドレスを指定します。NAT 適用除外は、ポリシー NAT と同じではありません。たとえば、ポート アドレスは指定できません。
dns	(任意) このコマンドと一致する DNS 応答の A レコードすなわちアドレス レコードを書き換えます。マッピング インターフェイスから実際のインターフェイスに DNS 応答が送信される場合、A レコードはマッピング先の値から実際の値に書き替えられます。逆に、実際のインターフェイスからマッピング先のインターフェイスに DNS 応答が送信される場合、A レコードは実際の値からマッピング先の値に書き替えられます。 NAT ステートメントに DNS サーバにエントリのあるホストのアドレスが指定されていて、なおかつ DNS サーバがクライアントとは異なるインターフェイス上に配置されている場合、クライアントと DNS サーバにはそのホストに対して異なる複数のアドレスが必要です。1 つはグローバル アドレスで、もう 1 つはローカル アドレスです。変換後のホストは、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のあるホストでは、スタティック変換を使用するので、このオプションは **static** コマンドと組み合わせて使用する可能性が高くなります。

emb_limit	（任意）ホストあたりの最大初期接続数を指定します。デフォルト値は 0 で、初期接続数は無制限です。 初期接続数を制限すると、DoS 攻撃から保護することができます。FWSM は初期制限を使用して、TCP 代行受信をトリガーします。これにより、TCP SYN パケットがインターフェイスでフラッディングすることによって発生する DoS 攻撃から内部システムが保護されます。初期接続は、送信元と宛先間で必要なハンドシェイクを終了しなかった接続要求です。
real_ifc	実際の IP アドレス ネットワークに接続されたインターフェイスの名前を指定します。
real_ip	変換する実際のアドレスを指定します。**0.0.0.0**（または省略形の **0**）を使用すると、すべてのアドレスを指定できます。
mask	（任意）実アドレスのサブネット マスクを指定します。マスクを入力しなかった場合は、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 に対応する整数を指定します。**global** コマンドでこの ID を参照して、グローバル プールと *real_ip* が対応付られます。 標準 NAT の場合、この整数は 1 ～ 2147483647 です。ポリシー NAT（nat id access-list）の場合は 1 ～ 65535 です。 アイデンティティ NAT（**nat 0**）および NAT 除外（**nat 0 access-list**）では、**0** の NAT ID を使用します。
norandomseq	（任意）TCP Initial Sequence Number（ISN）ランダム化の保護機能をディセーブルにします。別のインライン ファイアウォールで ISN のランダム化をイネーブルにしている場合は、ランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、ISN ランダム化を、両方のファイアウォールでイネーブルのままにしても、トラフィックに影響はありません。 各 TCP 接続には ISN が 2 つあります。1 つはクライアントによって生成され、もう 1 つはサーバによって生成されます。セキュリティ アプライアンスは、発信方向に渡される TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続では、SYN の ISN が両方向でランダム化されます。 保護されたホストで ISN をランダム化することにより、新規接続の次の ISN を予測して新規セッションをハイジャックする攻撃を阻止できます。 **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、セキュリティがより高いインターフェイス上のホスト/サーバで生成される ISN のみです。外部 NAT に norandomseq を設定しても、**norandomseq** キーワードは無視されます。
outside	（任意）このインターフェイスのセキュリティ レベルが対応する **global** ステートメントで特定され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。この機能を外部 NAT または双方向 NAT といいます。
tcp *tcp_max_conns*	（任意）サブネット全体で同時に可能な TCP 接続の最大数を指定します。デフォルト値は 0 で、接続数は無制限です（**timeout conn** コマンドで指定されたアイドル タイムアウトが経過すると、アイドル接続は終了します）。
udp *udp_max_conns*	（任意）サブネット全体における同時 UDP 接続の最大数を指定します。デフォルト値は 0 で、接続数は無制限です（**timeout conn** コマンドで指定されたアイドル タイムアウトが経過すると、アイドル接続は終了します）。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は、使用可能な最大値を示す 0（無制限）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。

	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	トランスペアレント	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
1.1(1)	このコマンドが追加されました。
2.2(1)	ローカル ホストの UDP 最大接続数をサポートするように、このコマンドが変更されました。
2.3(1)	外部 NAT の接続を設定できるように、このコマンドが変更されました。

使用上のガイドライン

ダイナミック NAT および PAT では、事前に **nat** コマンドを設定して、変換するインターフェイス上の実アドレスを特定します。さらに、別のインターフェイスを終了するときに、別個の **global** コマンドを設定して、マッピング アドレス（PAT の場合は 1 つのアドレス）を指定します。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 を比較することによって、**global** コマンドを照合します。

FWSM がアドレスを変換するのは、NAT ルールがトラフィックと一致した場合です。NAT ルールが一致しなかった場合は、パケットの処理が続けられます。例外は、**nat-control** コマンドで NAT 制御をイネーブルにした場合です。NAT 制御では、セキュリティ レベルの高いインターフェイス（内部）から低いインターフェイス（外部）へ移動するパケットが、NAT ルールと一致する必要があります。一致しない場合、そのパケットの処理は中止されます。NAT 制御をイネーブルにした場合でも、セキュリティ レベルが同じインターフェイス間では NAT は不要です。必要に応じて任意で NAT を設定できます。

ダイナミック NAT では、実アドレスのグループが宛先ネットワーク上でルーティング可能な、マッピング アドレスのプールに変換されます。マッピング プールは、実グループより少ないアドレスで構成できます。変換対象のホストが宛先ネットワークにアクセスする場合、FWSM は対応付けたプール内の IP アドレスをホストに割り当てます。変換が追加されるのは、実ホストが接続を開始するときだけです。変換が有効なのは、接続の間だけであり、個々のユーザが変換のタイムアウト（**timeout xlate** コマンドの項を参照）後も同じ IP アドレスを維持することはありません。したがって、宛先ネットワーク上のユーザは、ダイナミック NAT（または PAT、アクセス リストによって接続が許可される場合を含む）を使用するホストに対して、接続を確実に開始できるわけではありません。また、実ホスト アドレスへの直接接続は、FWSM によって拒否されます。確実なホスト アクセスについては、**static** コマンドの項を参照してください。

ダイナミック NAT の短所は、次のとおりです。

- マッピング　プールのアドレス数が実グループより少ない状況で、トラフィック量が予想を上回った場合、アドレスが不足する可能性があります。

  この状況が頻繁に発生する場合は、PAT を使用してください。PAT では、単一アドレスのポートを使用して 64,000 を超える変換が可能です。
- マッピング　プールで大量のルーティング可能アドレスを使用する必要があります。インターネットなど、宛先ネットワークが登録アドレスを要求する場合、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、一部のプロトコルで 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、ポートのオーバーロードが認められない IP プロトコルでは PAT を使用できません。PAT はまた、一部のアプリケーションでも使用できません。データ ストリームがあるポート上にあり、制御パスが別のポートにあって、オープンな標準ではない、一部のマルチメディア アプリケーションなどがこれに該当します。

PAT 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。具体的に言うと、FWSM は実アドレスおよび送信元ポート（実ソケット）をマッピング アドレスおよび 1024 以上の一意のポート（マッピング ソケット）に変換します。接続ごとに別々の変換が必要です。接続ごとに送信元ポートが異なるからです。たとえば、10.1.1.1:1025 には 10.1.1.1:1026 とは別個の変換が必要です。

接続のタイムアウト後、非アクティブ状態が 30 秒間続くと、ポート変換もタイムアウトします。このタイムアウトは設定できません。

PAT ではマッピング アドレスを 1 つだけ使用するので、ルーティング可能なアドレスを節約できます。FWSM インターフェイスの IP アドレスを PAT アドレスとして使用することもできます。PAT はデータ ストリームと制御パスが異なる、一部のマルチメディア アプリケーションでは使用できません。

（注） 変換が有効な間、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、変換されたホストへの接続を開始できます。アドレス（実アドレスとマッピング アドレスの両方）が予測不能なので、ホストに接続される可能性はほとんどありません。また、万一接続された場合は、アクセス リストのセキュリティを信頼できます。

NAT 制御がイネーブルの場合、内部ホストは外部ホストにアクセスするときに、NAT ルールと一致する必要があります。一部のホストに NAT を実行しないでおく場合は、それらのホストに対して NAT をバイパスできます。または、NAT 制御をディセーブルにできます。NAT のバイパスが必要になるのは、NAT をサポートしないアプリケーションを使用する場合などです。**static** コマンドを使用して NAT をバイパスするか、または次のオプションのいずれか 1 つを使用します。

- 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 に類似）を設定した場合、変換は特定のインターフェイス上のホストに限定されません。すべてのインターフェイスを経由する接続に対してアイデンティティ NAT を使用する必要があります。したがって、インターフェイス A にアクセスするときには、実アドレスの標準変換を実行し、インターフェイス B にアクセスするときにはアイデンティティ NAT を使用するという選択はできません。一方、標準ダイナミック NAT の場合は、アドレス変換を実行する特定のインターフェイスを指定できます。アイデンティティ NAT の使用対象となる実アドレスが、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 では、マッピング アドレスが実アドレスと同じ場合を含めて、（インターフェイスのアクセス リストで許可されていても）外部から内部へは接続を開始できません。この場合は、スタティック アイデンティティ NAT または NAT 除外を使用します。

- NAT 除外（**nat 0 access-list** コマンド）— NAT 除外を使用すると、変換されたホストとリモート ホストの両方から接続を開始できます。アイデンティティ NAT と同様に、特定のインターフェイス上のホストに変換が限定されないので、すべてのインターフェイスを経由する接続に対して NAT 除外を使用する必要があります。ただし、NAT 除外では（ポリシー NAT と同様）、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定できるので、NAT 除外を使用するときめ細かい制御が可能です。一方、NAT 除外はポリシー NAT と異なり、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、アドレス変換の対象となる実アドレスを特定できます。さらに任意で、送信元ポートと宛先ポートを指定できます。標準 NAT で考慮されるのは、実アドレスだけです。たとえば、実アドレスからサーバ A にアクセスするときには、実アドレスをマッピング アドレス A に変換できますが、実アドレスからサーバ B にアクセスするときには、実アドレスをマッピング アドレス B に変換できます。

セカンダリ チャネルに関してアプリケーション検査が必要なアプリケーション（FTP、VoIP など）に、ポリシー NAT でポートを指定した場合、FWSM はセカンダリ ポートを自動的に変換します。

（注） ポリシー NAT は、NAT 除外を除き、あらゆるタイプの NAT でサポートされます。NAT 除外では、アクセス リストを使用して実アドレスを特定しますが、ポートが考慮されない点がポリシー NAT と異なります。**スタティック** アイデンティティ NAT を使用して、NAT 除外と同じ結果を得ることもできます。この場合も、ポリシー NAT がサポートされます。

Modular Policy Framework を使用して、接続制限を設定することもできます（ただし、初期接続制限は設定できません）。詳細については、**set connection** コマンドを参照してください。初期接続限度を設定できるのは、NAT を使用する場合だけです。両方の方式を使用する同一トラフィックに、これらの限度を設定した場合、FWSM は低い方の限度を使用します。どちらかの方式で TCP シーケンスのランダム化がディセーブルになっている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

NAT の設定を変更し、既存の変換がタイムアウトしないうちに新しい NAT 情報が使用されるようにする場合は、**clear xlate** コマンドを使用して、変換テーブルを消去できます。ただし、変換テーブルを消去すると、現在のすべての接続が切断されます。

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 プールを指定し、さらに NAT プールを使い果たした場合に使用する PAT 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)# 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
```

セキュリティ レベルの低い dmz ネットワーク アドレスを変換して、たとえば、内部ネットワーク（10.1.1.0）と同じネットワーク上にあるように見せかけ、ルーティングを簡素化するには、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、1 つの実アドレスに 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、異なるポートを使用する実アドレスと宛先アドレスのペアを 1 つ指定するには、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	同時に作成できる拒否フローの最大数を指定します。
clear configure nat	NAT の設定を削除します。
global	グローバル アドレス プールからエントリを作成します。
interface	インターフェイスを作成して設定します。
show running-config nat	ネットワークに対応付られているグローバル IP アドレス プールを表示します。

nat-control

NAT 制御を適用するには、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 制御では、外部にアクセスする内部ホストに NAT が必要です。NAT 制御をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-control

no nat-control

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

NAT 制御はデフォルトでディセーブルです（**no nat-control** コマンド）。ただし、旧バージョンのソフトウェアからアップグレードした場合、NAT 制御がシステム上でイネーブルになる場合があります。一部の旧バージョンでは、イネーブルがデフォルトだったからです。

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。

	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	トランスペアレント	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
3.1(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

NAT 制御では、内部インターフェイスから外部インターフェイスに流れるパケットが NAT ルールと一致していなければなりません。したがって、内部ネットワーク上のホストから外部ネットワーク上のホストにアクセスできるようにするには、内部ホスト アドレスが変換されるように NAT を設定する必要があります。

セキュリティ レベルが同じインターフェイスの場合、NAT を使用して通信する必要はありません。

NAT 制御はデフォルトでディセーブルなので、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。

（注） NAT を設定した場合でも、FWSM はすべてのトラフィックに対して、引き続き自動的に変換セッションを作成します。この場合、実アドレスから同じ実アドレスへの変換になります。変換セッションの表示については、**show xlate** コマンドの項を参照してください。

NAT 制御のセキュリティを強化し、なおかつ状況によっては内部アドレスを変換しないでおく場合は、該当するアドレスに NAT 除外（**nat 0 access-list**）またはアイデンティティ NAT（**nat 0** または **static**）のルールを適用できます。

（注）　マルチコンテキスト　モードでは、コンテキストにパケットを割り当てるためのパケット分類子が NAT の設定によって左右されることがあります。NAT 制御がディセーブルなので NAT を実行しないという場合は、分類子がネットワーク設定の変更を要求する可能性があります。

例

次に、NAT 制御をイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
nat	別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、あるインターフェイス上のアドレスを定義します。
show running-config nat-control	NAT 設定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。

neighbor

ポイントツーポイント、非ブロードキャスト ネットワーク上のスタティック 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。コンフィギュレーションから静的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** コマンドは、VPN トンネル上の OSPF ルートをアドバタイズ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*	（任意）**name if** コマンドで指定された、ネイバーに到達できるインターフェイスの名前
ip_address	近接ルータの IP アドレス

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
3.1(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

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 1 つずつ、ネイバー エントリを指定する必要があります。ネイバー アドレスは、インターフェイスのプライマリ アドレス上になければなりません。

ネイバーがシステムの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ない場合は、***interface*** オプションを指定する必要があります。さらに、ネイバーに到達するスタティック 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 の近接ルータを定義する例を示します。

```
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に指定されているコマンドを表示します。

nem

ハードウェア クライアントに対して、Network Extension Mode（NEM; ネットワーク エクステンション 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。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 ポリシーから値を継承できます。

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

no nem

シンタックスの説明

disable	NEM をディセーブルにします。
enable	NEM をイネーブルにします。

デフォルト

NEM はディセーブルです。

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。

	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	トランスペアレント	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

NEM によって、ハードウェア クライアントは VPN トンネルを介して、リモート プライベート ネットワークに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 FWSM の背後にあるネットワークへの、すべてのトラフィックをカプセル化します。PAT は適用されません。したがって、FWSM の背後にあるデバイスは、トンネル経由で、ハードウェア クライアントの背後のプライベート ネットワークにあるデバイスに直接アクセスできます。逆も可能です。ただし、いずれもトンネルを経由する場合に限定されます。トンネルはハードウェア クライアントが開始しなければなりませんが、トンネルの確立後はどちら側からで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
3.1(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 ポリシーに対して NEM を設定する例を示します。

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

network area

OSPF が動作するインターフェイスを定義し、それらのインターフェイスにエリア 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。アドレスおよびネット マスクのペアで定義されたインターフェイスに対して、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
area *area_id*	OSPF アドレス範囲に関連付けるエリアを指定します。*area_id* は、IP アドレス形式または 10 進数形式のどちらでも指定できます。10 進数形式で指定する場合、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

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
3.1(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

インターフェイス上で OSPF を動作させるには、インターフェイスのアドレスが **network area** コマンドに含まれていなければなりません。**network area** コマンドにインターフェイスの IP アドレスが含まれていない場合、そのインターフェイス上で OSPF はイネーブルになりません。

FWSM 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、インターフェイス 192.168.1.1 上で OSPF をイネーブルにして、そのインターフェイスにエリア 2 を割り当てる例を示します。

```
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に指定されている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、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** コマンドでホスト名がまだ定義されていない場合）
host_name	ホスト名（**name** コマンドで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（サブネット オブジェクトを定義する場合に *netmask* と組み合わせて使用）
netmask	ネットマスク（サブネット オブジェクトを定義する場合に *net_addr* と組み合わせて使用）

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
3.1(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

network-object コマンドは **object-group** コマンドと組み合わせて、ネットワーク コンフィギュレーション モードで使用し、ホストまたはサブネット オブジェクトを定義します。

例

次に、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例を示します。

```
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	コンフィギュレーションからすべての **object-group** コマンドを削除します。
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	設定を最適化するオブジェクト 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 *hostname*

no nt-auth-domain-controller

シンタックスの説明

hostname	このサーバのプライマリ ドメイン コントローラ名を最大 16 文字で指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
3.1(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

このコマンドが有効なのは、NT 認証サーバに限定されます。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 モードを開始しておく必要があります。*string* 変数の名前は、サーバ自体の NT エントリと一致させる必要があります。

例

次に、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] に設定する例を示します。

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

関連コマンド

コマンド	説明
aaa-server	AAA サーバ ホスト コンフィギュレーション モードを開始し、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	コンフィギュレーションからすべての AAA コマンド ステートメントを削除します。
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について、AAA サーバの統計情報を表示します。

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 および IPv6 アドレスをサポートします。

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、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** コマンドを入力してから、**icmp-object** および **group-object** コマンドを使用して、ICMP タイプ グループに ICMP オブジェクトを追加します。
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** コマンドを入力してから、**network-object** および **group-object** コマンドを使用して、ネットワーク グループにネットワーク オブジェクトを追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、「_」、「-」、および「.」を任意に組み合わせることができます。
protocol	TCP、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** コマンドを入力してから、**protocol-object** および **group-object** コマンドを使用して、プロトコル グループにプロトコル オブジェクトを追加します。
service	[eq smtp]、[range 2000 2010] などの TCP/UDP ポート仕様グループを定義します。メインの **object-group service** コマンドを入力してから、**port-object** および **group-object** コマンドを使用して、サービス グループにポート オブジェクトを追加します。
tcp	サービス グループを TCP に使用するように指定します。
tcp-udp	サービス グループを TCP および UDP に使用できるように指定します。
udp	サービス グループを UDP に使用するように指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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　ホスト、プロトコル、またはサービスなどのオブジェクトをグループ化すると、グループ名を使用してコマンドを 1 つ発行し、グループ内のすべての項目に適用できます。

object-group コマンドを使用してグループを定義してから、任意の FWSM コマンドを使用すると、コマンドはグループ内のすべての項目に適用されます。この機能を使用すると、コンフィギュレーション サイズを大幅に削減できます。

オブジェクト グループを定義してから、次のように、適用可能なすべての FWSM コマンド内のグループ名の前で **object-group** キーワード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。

次に、定義されたオブジェクト グループを使用する例を示します。

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

さらに、**access list** コマンドの引数をグループにまとめることができます。

各引数	代用されるオブジェクト グループ
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドは階層的にグループ化できます。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することができます。

オブジェクト グループを使用するには、次の作業を行う必要があります。

- 次のように、すべてのコマンド内のオブジェクト グループ名の前で **object-group** キーワードを使用します。

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

  remotes および *locals* は、サンプルのオブジェクト グループ名です。
- オブジェクト グループを空にしないでください。
- コマンドで現在使用中のオブジェクト グループを削除したり、空にしたりすることはできません。

メインの **object-group** コマンドを入力すると、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 グループは新しいモードで定義されます。アクティブなモードはコマンド プロンプトの形式で示されます。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なります。

```
hostname(config)#
```

hostname は FWSM の名前です。

ただし、**object-group** コマンドを入力すると、次のようなプロンプトが表示されます。

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

hostname は FWSM の名前、*type* は *object-group* のタイプです。

object-group モードを終了して、**object-group** メイン コマンドを終了するには、**exit**、**quit**、または任意の有効な config-mode コマンド（**access-list** など）を使用します。

show running-config object-group コマンドは、すべての定義済みオブジェクト グループを表示します。**show running-config object-group** *grp_id* コマンドを入力した場合は *grp_id* 別に、**show running-config object-group** *grp_type* コマンドを入力した場合はグループ タイプ別に表示されます。引数を指定しないで **show running-config object-group** コマンドを入力した場合は、すべての定義済みオブジェクト 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。引数を指定しないで **clear configure object-group** コマンドを使用すると、コマンドで使用されていないすべての定義済みオブジェクト グループを削除できます。*grp_type* 引数を指定すると、コマンドで使用されていないすべての定義済みオブジェクト グループが、該当するグループ タイプに限って削除されます。

object-group モードでは、**show running-config** コマンド、**clear configure** コマンドをはじめ、その他のすべての FWSM 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**、**write**、または **config** コマンドで表示または保存したときに、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 特権レベルが与えられます。

access-list コマンドで複数のオブジェクト グループを使用すると、コマンドで使用されるすべてのオブジェクト グループの要素が結合されます。まず、最初のグループの要素と 2 番めのグループの要素が結合され、次に最初と 2 番めのグループの要素が 3 番めのグループの要素と結合されます（以下同様の処理）。

記述テキストの開始位置は、**description** キーワードに続くスペース（ブランクまたはタブ）の右側の文字です。

例

次に、**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例を示します。

```
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
```

次に、**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例を示します。

```
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
```

次に、**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例を示します。

```
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
```

次に、**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例を示します。

```
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
```

次に、**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例を示します。

```
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
```

次に、オブジェクト グループにテキスト記述を追加および削除する例を示します。

```
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
```

次に、**group-object** モードを使用して、定義済み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例を示します。

```
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* および *host_grp_2* で定義されたすべての IP アドレスを含むように *all_hosts* を定義する必要があります。**group-object** コマンドを使用すると、重複してホストを定義する必要がなくなります。

次に、オブジェクト グループを使用して、アクセス リストの設定を簡素にする例を示します。

```
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
```

このグループ化を使用すると、アクセス リストを 24 行（グループ化を使用しない場合に必要な行数）でなく、1 行で設定できます。グループ化を使用した場合のアクセス リストの設定は、次のとおりです。

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

（注）　**show running-config object-group** および **write** コマンドを使用すると、オブジェクト グループ名を使用して設定されたアクセス リストを表示できます。**show access-list** コマンドは、オブジェクトのグループ化を使用しないで、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	コンフィギュレーションから **object group** コマンドをすべて削除します。
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。

ospf authentication

OSPF 認証を使用できるようにするには、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	（任意）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	（任意）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 認証を使用できません。

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。

	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	トランスペアレント	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
1.1(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

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、インターフェイスに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は、**ospf message-digest-key** コマンドで、インターフェイスにメッセージ ダイジェスト鍵を設定します。

下位互換性を維持するために、エリアの認証タイプも引き続きサポートされます。インターフェイスに認証タイプを指定しなかった場合は、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ヌル認証）。

オプションを指定しないでコマンドを使用した場合は、単純なパスワード認証がイネーブルになります。

例

次に、選択したインターフェイス上で、OSPF に対して単純なパスワード認証をイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
ospf ***authentication-key***	近接ルーティング デバイスで使用する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て、MD5 鍵を指定します。

ospf authentication-key

近接ルーティング デバイスで使用す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	近接ルーティング デバイスで使用する 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 つの文字の間にブランク スペースを含めることができます。パスワードの先頭または末尾のスペースは無視されます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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

このコマンドで作成したパスワードは、ルーティング プロトコル パケットの発信時に、OSPF ヘッダーに直接組み込む鍵として使用されます。インターフェイス単位で、各ネットワークにそれぞれ異なるパスワードを割り当てることができます。OSPF 情報を交換できるようにするには、同じネットワーク上のすべての近接ルータに、同じパスワードを設定する必要があります。

例

次に、OSPF 認証用のパスワードを指定する例を示します。

```
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 認証を使用できるようにします。

ospf cost

インターフェイスを介したパケット送信の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使用してパケットを送信するコスト（リンクステート 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たネットワークを表し、インターフェイスの帯域が大きいほど、そのインターフェイス経由でパケットを送信する関連コストが小さくなります。言い換えると、大きいコスト値は帯域の小さいインターフェイスを表し、小さいコスト値は広帯域インターフェイスを表します。 FWSM における OSPF インターフェイスのデフォルト コストは 10 です。この値は Cisco IOS ソフトウェアのデフォルトとは異なります。Cisco IOS ソフトウェアのデフォルト コストは、ファスト イーサネットおよびギガビット イーサネットで 1、10BaseT で 10 です。ネットワークで ECMP を使用する場合は、この相違を考慮することが重要です。

デフォルト

デフォルトの *interface_cost* は 10 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
1.1(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

ospf cost コマンドを使用すると、インターフェイス上でパケットを送信するときの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

次に、選択したインターフェイス上で、パケットの送信コストを指定する例を示します。

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

関連コマンド

コマンド	説明
show running-config interface	指定されたインターフェイスの設定を表示します。

ospf database-filter all out

同期およびフラッディング時に、OSPF インターフェイスへのすべての発信 LSA を除外するには、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 all out** コマンドを使用します。LSA を元に戻すには、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

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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

ospf database-filter all out 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** コマンドを使用すると、インターフェイスへの LSA 転送が元に戻ります。

例

次に、**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例を示します。

```
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 パケットを受信しない時間の長さ。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定された間隔（1 ～ 65535）の 4 倍です。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドで設定された間隔の 4 倍になります。

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。

	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	トランスペアレント	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
1.1(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

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 パケットを受信しない時間の長さ）を設定できます。*seconds* 引数でデッド間隔を指定し、ネットワーク上のすべてのノードで同じ設定にする必要があります。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定された間隔（1 ～ 65535）の 4 倍です。

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

次に、OSPF のデッド間隔を 1 分に設定する例を示します。

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

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイス上で hello パケットが送信され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

インターフェイス上で hello パケットが送信され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送信される hello パケットの間隔を指定します。有効値は 1 ～ 65535 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
1.1(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

この値は hello パケットでアドバタイズされます。hello 間隔が小さいほど、トポロジ変更が迅速に検出されますが、発生するルーティング トラフィックが増えます。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 サーバで一致させる必要があります。

例

次に、OSPF hello 間隔を 5 秒に設定する例を示します。

```
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 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 鍵を削除するには、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て、認証鍵の ID 番号を数値で指定します。有効値は 1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字パスワード。鍵の文字の間にスペースを含めることができます。鍵の先頭または末尾のスペースは無視されます。MD5 認証は通信の整合性を検証し、送信元を認証し、タイミングが適切であるかをチェックします。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
1.1(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

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、MD5 鍵が削除されます。*key_id* 引数は、認証鍵を表す 1 ～ 255 の識別番号です。*key* 引数は、最大 16 バイトの英数字パスワードです。MD5 は通信の整合性を検証し、送信元を認証し、タイミングが適切であるかをチェックします。

例

次に、OSPF 認証用の MD5 鍵を指定する例を示します。

```
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 認証を使用できるようにします。

ospf mtu-ignore

データベース パケット受信時の OSPF Maximum Transmission Unit（MTU; 最大伝送ユニット）不一致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 不一致検出を元に戻すには、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、引数またはキーワードはありません。

デフォルト

mtu-ignore はデフォルトでイネーブルです。

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。

	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	トランスペアレント	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
1.1(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

OSPF は、ネイバーが共通のインターフェイス上で同じ MTU を使用しているかどうかを調べます。この検査は、ネイバーが Database Descriptor（DBD）パケットを交換するときに行われます。DBD パケットで受信した MTU が着信インターフェイス上で設定されている IP MTU より大きい場合、OSPF の隣接関係は確立されません。**ospf mtu-ignore** コマンドを使用すると、DBD パケット受信時の OSPF MTU 不一致検出がディセーブルになります。この機能はデフォルトでイネーブルです。

例

次に、**ospf mtu-ignore** コマンドをディセーブルにする例を示します。

```
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

ポイントツーポイント、非ブロードキャスト ネットワークとして OSPF インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **ospf network** ***point-to-point non-broadcast*** コマンドを使用します。コンフィギュレーションからこの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。**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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

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。

	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	トランスペアレント	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
3.1(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

ポイントツーポイントとしてインターフェイスを指定した場合、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 ディスカバリは実行できません。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。

ポイントツーポイントとしてインターフェイスを設定した場合は、次の制限事項が適用されます。

- インターフェイスに定義できるネイバーは 1 つだけです。
- 暗号エンドポイントを示すスタティック ルートを定義する必要があります。
- ネイバーを明示的に設定しないかぎり、インターフェイスは隣接関係を形成できません。
- インターフェイス上でトンネル経由の OSPF が動作している場合、同じインターフェイス上で上流のルータによる標準 OSPF を動作させることはできません。
- OSPF の更新情報が VPN トンネルを介して確実に受け渡されるように、OSPF ネイバーを指定する前に、暗号マップとインターフェイスを結合する必要があります。OSPF ネイバーを指定したあとで、暗号マップをインターフェイスに結合する場合は、**clear local-host all** コマンドを使用して、OSPF 接続を削除し、VPN トンネルを介して OSPF 隣接関係を確立できるようにします。

例

次に、インターフェイスを選択し、ポイントツーポイント、非ブロードキャスト インターフェイスとして設定する例を示します。

```
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	手動設定の 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 プライオリティを変更するには、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。デフォルトのプライオリティに戻すには、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	ルータのプライオリティを指定します。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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
1.1(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

ネットワークに接続された 2 つのルータがどちらも指定ルータになろうとした場合、ルータ プライオリティの高いルータに優先権が与えられます。プライオリティが同じ場合は、ルータ ID の大きいルータに優先権が与えられます。ルータ プライオリティがゼロに設定されているルータは、指定ルータまたはバックアップの指定ルータになる資格がありません。ルータ プライオリティは、（ポイントツーポイント ネットワークではなく）マルチアクセス ネットワークに接続するインターフェイスに限定して設定します。

例

次に、インターフェイスを選択し、OSPF プライオリティを変更する例を示します。

```
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所属する隣接の 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 再送信間隔を指定します。有効値は 1 ～ 65535 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
1.1(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

ネイバーに LSA を送信したルータは、確認メッセージを受信するまで、その LSA を保管します。確認応答を受信しなかった場合、ルータは LSA を再送信します。

このパラメータの設定は慎重に行う必要があります。そうしない場合、無用な再送信が行われます。シリアル回線または仮想リンクには、値を大きくしてください。

例

次に、LSA の再送信間隔を変更する例を示します。

```
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でリンクステート更新パケットを伝送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でリンクステート更新パケットを伝送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、有効値は 1 ～ 65535 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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
1.1(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

更新パケットの LSA には、伝送前に *seconds* 引数で指定された値によって増分されたエージが設定されていなければなりません。インターフェイスの伝送および伝播遅延を考慮して、値を割り当てる必要があります。

リンクでの伝送前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。この設定値は、低速リンクほど重要性が増します。

例

次に、インターフェイスを選択し、伝播遅延を 3 秒に設定する例を示します。

```
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。