O

- object-group （2 ページ）
- object-group-search （9 ページ）
- object network （12 ページ）
- object network-service （14 ページ）
- object service （17 ページ）
- ocsp disable-nonce （19 ページ）
- ocsp interface （21 ページ）
- ocsp url （23 ページ）
- onscreen-keyboard（廃止） （25 ページ）
- ospf authentication （27 ページ）
- ospf authentication-key （29 ページ）
- ospf cost （31 ページ）
- ospf database-filter （33 ページ）
- ospf dead-interval （35 ページ）
- ospf hello-interval （37 ページ）
- ospf message-digest-key （39 ページ）
- ospf mtu-ignore （41 ページ）
- ospf network point-to-point non-broadcast （42 ページ）
- ospf priority （44 ページ）
- ospf retransmit-interval （46 ページ）
- ospf transmit-delay （48 ページ）
- otp expiration （50 ページ）
- output console （52 ページ）
- output file （54 ページ）
- output none （56 ページ）
- outstanding（廃止） （58 ページ）
- override-account-disable（廃止） （60 ページ）
- override-svc-download （62 ページ）

object-group

構成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。構成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。

object-group { **protocol | network | icmp-type | security | user | network-service** } *grp_name*
object-group service *grp_name* [**tcp | udp | tcp-udp**]

構文の説明

grp_name	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「_」、「-」、「.」の組み合わせが使用可能です。
icmp-type	（推奨されません。代わりに **service** を使用してください）。echo や echo-reply など ICMP タイプのグループを定義します。**object-group icmp-type** コマンドを入力後、**icmp-object** コマンドと **group-object** コマンドを使用して ICMP オブジェクトを追加します。
network	ホストまたはサブネットの IP アドレスのグループを定義します。**object-group network** コマンドを入力後、**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追加します。IPv4 アドレスと IPv6 アドレスが混在したグループを作成できます。 （注） 混合オブジェクト グループを NAT に使用することはできません。
network-service	オプションのサービス仕様でサブネットまたはドメイン名のグループを定義します。このコマンドを入力したら、**network-service-member** コマンドを使用してネットワーク サービス オブジェクトを追加するか、**domain** コマンドと **subnet** コマンドを使用してメンバーを直接追加します。
protocol	（推奨されません。代わりに **service** を使用してください）。TCP や UDP などプロトコルのグループを定義します。**object-group protocol** コマンドを入力後、**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追加します。
security	Cisco TrustSec で使用するセキュリティ グループ オブジェクトを定義します。**object-group protocol** コマンドを入力後、**security-group** コマンドと **group-object** コマンドを使用してセキュリティ グループ オブジェクトを追加します。

service **[tcp | udp | tcp-udp**	プロトコル、ICMP タイプ、および TCP/UDP/SCTP ポートに基づいてサービスを定義します。 サービスの混合グループまたは SCTP ポートを定義する場合は、オブジェクトグループのプロトコルタイプを指定しないでください。**object-group service** コマンドを入力後、**service-object** コマンドと **group-object** コマンドを使用してサービスグループにサービスオブジェクトを追加します。オブジェクトに TCP ポートまたは UDP ポート（あるいはその両方）のリストしか含めない場合も、この方法を使用することを推奨します。 object-group service コマンドで **tcp**、**udp**、および **tcp-udp** キーワードを直接使用することは推奨されません。これらのキーワードを使用する代わりに、**service-object** コマンドで TCP ポートと UDP ポートを設定します。これらのキーワードを含めない場合は、**port-object** コマンドと **group-object** コマンドを使用してポートグループを追加します。
user	アイデンティティ ファイアウォールでアクセスを制御するために使用できるユーザーおよびユーザー グループを定義します。**object-group protocol** コマンドを入力後、**user**、**user-group**、および **group-object** コマンドを使用してユーザーおよびユーザー グループ オブジェクトを追加します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	アイデンティティ ファイアウォールをサポートするために **user** キーワードのサポートが追加されました。
9.0(1)	IPv4 アドレスと IPv6 アドレスが混在したネットワーク オブジェクト グループを作成できるようになりました。 Cisco TrustSec をサポートするために **security** キーワードのサポートが追加されました。

リリース	変更内容
9.14	**icmp-type** キーワードは推奨しません。代わりに、**service** キーワードを使用してオブジェクトに **service icmp** を指定します。
9.17(1)	**network-service** キーワードが追加されました。

使用上のガイドライン

ホストやサービスなどのオブジェクトをグループ化し、そのオブジェクトグループを ACL（**access-list**）やNAT（**nat**）などの機能で使用できます。次に、ACL でネットワーク オブジェクト グループを使用する例を示します。

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group
NWgroup1
```

コマンドを階層的にグループ化できます。つまり、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。

例

次に、**object-group network** コマンドを使用して、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。

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

次に、**object-group network** コマンドを使用して、既存のオブジェクトグループを含むネットワーク オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers

ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224

ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

次に、**group-object** モードを使用して、事前に定義した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し、それらのオブジェクトを ACL で使用する例を示します。

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
```

```
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(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* にすでに定義されているすべての IP アドレスが含まれるように、*all_hosts* グループを定義する必要があります。**group-object** コマンドを使用すると、重複するホストの定義が削除されます。

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# group-object SSH
ciscoasa(config-service-object-group)# group-object EIGRP
ciscoasa(config-service-object-group)# group-object HTTPS
```

次の例では、指定したプロトコル、ポート、および ICMP の組み合わせを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service mixed
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

次に、**service-object** サブコマンドを使用する例を示します。このサブコマンドは、TCP サービスおよび UDP サービスをグループ化する場合に便利です。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
ciscoasa(config-network-object-group)# network-object host kqk.suu.pyl.gnl
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group
locals object-group remote
```

次に、**object-group user** コマンドを使用して、ユーザー グループ オブジェクトを作成する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

（推奨されません。代わりにサービス オブジェクトを使用してください）次に、**object-group icmp-type** モードを使用して ICMP オブジェクトグループを作成する例を示します。

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

（推奨されません。代わりにサービス オブジェクトを使用してください）次に、**object-group protocol** モードを使用してプロトコル オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit
ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit
```

（推奨されません。**tcp** キーワードを使用する代わりに **service-object** コマンドでポートを定義します）。次に、**object-group service** モードを使用して TCP ポートオブジェクトグループを作成する例を示します。

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

次に、オブジェクト グループを使用して、アクセス リスト コンフィギュレーションを簡素化する例を示します。グループ化を使用しないとアクセス リストの設定には24行必要ですが、このグループ化により、1 行で設定できます。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host
209.165.200.225
ciscoasa(config-network-object-group)# network-object host
209.165.200.230
ciscoasa(config-network-object-group)# network-object host
209.165.200.235
ciscoasa(config-network-object-group)# network-object host
209.165.200.240
ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100
ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```

（注） **show running-config access-list** コマンドは、オブジェクトグループ名を指定して設定されたアクセスリストを表示します。**show access-list** コマンドは、その情報に加え、グループを使用するアクセスリストエントリを、オブジェクトはグループ化せずに個々のエントリに展開して表示します。

次に、事前に定義されたネットワーク サービス オブジェクトを使用して、一連の SaaS アプリケーションを設定する例を示します。

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

関連コマンド

コマンド	説明
clear 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。
security-group	セキュリティ グループ オブジェクト グループにセキュリティ グループを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

コマンド	説明
user	ユーザー グループ オブジェクトにユーザー名を追加します。
user-group	ユーザー グループ オブジェクトにユーザー グループ名を追加します。

object-group-search

ACL の最適化を有効にするには、グローバル コンフィギュレーション モードで **object-group-search** コマンドを使用します。ACL の最適化を無効にするには、このコマンドの **no** 形式を使用します。

object-group-search { **access-control | threshold** }
no object-group-search { **access-control | threshold** }

構文の説明

access-control	アクセス コントロール ルールのオブジェクト グループ検索を有効にします。
threshold	オブジェクト グループ検索処理の最大しきい値を有効にします。詳細については、「Usage Notes」を参照してください。

コマンド デフォルト

（9.18 より前）オブジェクトグループ検索はデフォルトで無効になっています。そのしきい値もデフォルトで無効になっています。

9.18以降、オブジェクトグループ検索は、新規展開のアクセス制御に対してデフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.12(1)	**threshold** キーワードが追加されました。このキーワードは、9.8、9.9、および 9.10 の暫定リリースでも追加されました。
9.18(1)	新規展開のアクセス制御のデフォルトが有効に変更されました。以前に有効にしていなかった場合は、アップグレード時に有効にする必要があります。

使用上のガイドライン

object-group-search コマンドは、着信方向のすべての ACL を最適化します。

オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下し、CPU使用率は増加しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索をイネーブルにした場合、ASP テーブルのネットワークまたはサー

ビス オブジェクトを使用する ACL は拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。これは **show access-list** 出力に表示されます。

オブジェクト グループ検索は、しきい値の影響を受けます。接続ごとに、送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。このチェックは、パフォーマンスの低下を防止します。一致件数が膨大になることを防ぐためにルールを設定します。しきい値に到達しないように、重複オブジェクトの作成を回避します。

リリース 9.12(1) 以降と暫定リリース 9.8(x) では、このしきい値はデフォルトで無効になっています。しきい値オプションが設定されているかどうか、および設定されている場合の現在の設定を確認するには、**show running-config all object-group-search** コマンドを使用します。

オブジェクト グループ検索を有効にした場合に、多数の機能が有効になっていると、アクティブな接続の数が増えて、アクセス グループのために大量の ACL が必要になり、処理中に接続が切断されたり、新しい接続を確立する際のパフォーマンスが低下したりすることがあります。パフォーマンスの低下は、トランザクションコミットを有効にしている場合でも発生する可能性があります（**asp rule-engine transactional-commit access-group**）。

（注） オブジェクト グループの検索は、ネットワーク オブジェクトとサービス オブジェクトのみで動作します。セキュリティ グループまたはユーザー オブジェクトでは動作しません。ACL にセキュリティ グループが含まれている場合は、この機能を有効にしないでください。ACL が非アクティブになったり、その他の予期しない動作となる可能性があります。

例

次に、**object-group-search** コマンドを使用して、ACL の最適化を有効にする例を示します。

```
ciscoasa(config)# object-group-search access-control
```

次に、**object-group-search** が有効になっていない場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
  access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
  access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
```

```
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

次に、**object-group-search** が有効になっている場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
 BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

関連コマンド

コマンド	説明
clear config object-group search	オブジェクト グループ検索コンフィギュレーションをクリアします。
show object-group	オブジェクト グループがネットワーク オブジェクト グループ タイプの場合にヒット カウントを表示します。
show running-config object-group	現在のオブジェクト グループを表示します。
show running-config object-group-search	実行コンフィギュレーション内のオブジェクト グループ検索コンフィギュレーションを表示します。

object network

名前付きネットワークオブジェクトを設定するには、グローバル コンフィギュレーション モードで **object network** 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を削除するには、このコマンドの **no** 形式を使用します。

object network *name* [**rename** *new_obj_name*]
no object network *name*

構文の説明

name	ネットワーク オブジェクトの名前を指定します。名前は 1 ～ 64 文字で、文字、数字、およびアンダースコア、ハイフン、カンマ、スラッシュ、ピリオドの特殊文字を使用できます。オブジェクトおよびオブジェクト グループは、同じ名前スペースを共有します。
rename *new_obj_name*	（オプション）オブジェクトの名前を新しいオブジェクト名に変更します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
8.4(2)	完全修飾ドメイン名（FQDN）がサポートされるようになりました。**fqdn** コマンドを参照してください。

使用上のガイドライン

ネットワーク オブジェクトには、ホスト、ネットワーク、IP アドレス（IPv4 または IPv6）の範囲、または FQDN を含めることができます。このコマンドを入力した後、**host**、**fqdn**、**subnet**、または **range** コマンドを使用してオブジェクトにアドレスを 1 つ追加します。

また、**nat** コマンドを使用して、このネットワークオブジェクトに対して NAT ルールを有効にできます。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。複数の NAT ルールを設定する場合は、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などのように、同じ IP アドレスを指定する複数のオブジェクトを作成する必要があります。

既存のネットワーク オブジェクトを異なるIPアドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object-group network	ネットワーク オブジェクト グループを作成します。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。
subnet	サブネット ネットワーク オブジェクトを指定します。

object network-service

名前付きネットワーク サービス オブジェクトを設定するには、グローバル コンフィギュレーション モードで **object network-service** 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を削除するには、このコマンドの **no** 形式を使用します。

object network-service *name* [**dynamic**]
no object network-service *name*

構文の説明

dynamic	（任意）**dynamic** キーワードは、オブジェクトが実行コンフィギュレーションに保存されず、**show object** 出力にのみ表示されることを意味します。**dynamic** キーワードは、主に外部デバイスマネージャーが使用するためのものです。
name	名前は最大128文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.17(2)	このコマンドが追加されました。

使用上のガイドライン

ネットワーク サービス オブジェクトでは、単一のアプリケーションを定義します。また、サブネット仕様やより一般的には DNS ドメイン名のいずれかによってアプリケーションの場所を定義します。必要に応じて、プロトコルとポートを含めて、アプリケーションの範囲を絞り込めます。

ネットワーク サービス オブジェクトは、ネットワーク サービス グループ オブジェクトでのみ使用できます。アクセス制御リストエントリ（ACE）でネットワーク サービス オブジェクトを直接使用することはできません。

次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの**no**形式を使用します。これらのコマンドは、複数回入力できます。

- **domain** *domain_name* [*service*]：最大 253 文字の DNS 名。この名前は、完全修飾名（www.example.com など）または部分的な名前（example.com など）にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー（www.example.com、www1.example.com、long.server.name.example.com など）に一致します。完全一致がある場合は、最も長い名前で接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みの IP アドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。
  - **eq** は、指定したポート番号と等しいポートを意味します。
  - **lt** は、指定したポート番号より小さい任意のポートを意味します。
  - **gt** は、指定したポート番号より大きい任意のポートを意味します。
  - **range** は、指定した 2 つのポートの間の任意のポートを意味します。
- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

例

次、ネットワーク サービス オブジェクトの例を示します。

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

関連コマンド

コマンド	説明
app-id	オブジェクトのアプリケーション ID を指定します。
clear object	ネットワーク サービス オブジェクトとヒットカウントをクリアします。
description	オブジェクトに説明を追加します。
domain	オブジェクトのドメイン名を指定します。
object-group network-service	ネットワークサービス オブジェクト グループを作成します。
show object	ネットワーク サービス オブジェクトを表示します。
subnet	オブジェクトのサブネットを指定します。

object service

サービスオブジェクトを、そのオブジェクトを使用しているすべての構成に自動的に反映させるように設定するには、グローバル コンフィギュレーション モードで **object service** コマンドを使用します。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。

object service *name*［ **rename** *new_obj_name* ］
no object service *object name*［ **rename** *new_obj_name* ］

構文の説明

name	サービス オブジェクトの名前を指定します。名前には、1～64 文字で、文字、数字、およびアンダースコア、ハイフン、カンマ、ピリオドの特殊文字を使用できます。オブジェクト名は文字で始める必要があります。
rename *new_obj_name*	（オプション）オブジェクトの名前を新しいオブジェクト名に変更します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

サービス オブジェクトには、プロトコル、ICMP、ICMPv6、または TCP /UDP/SCTP のポートまたはポート範囲を含めることができます。このコマンドを入力した後、**service** コマンドを使用してオブジェクトにサービス仕様を 1 つ追加します。

既存のサービス オブジェクトを別のプロトコルおよび1つ以上の別のポートを使用して設定する場合、新しいコンフィギュレーションにより、既存のプロトコルおよび1つ以上のポートが新しい設定に置き換わります。

例

次に、サービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
service	サービスオブジェクトのプロトコルとポートを設定します。

ocsp disable-nonce

ナンス拡張をディセーブルにするには、クリプトCAトラストポイントコンフィギュレーション モードで ocsp disable-nonce コマンドを使用します。ナンス拡張を再び有効にするには、このコマンドの **no** 形式を使用します。

ocsp disable-nonce
no ocsp disable-nonce

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、OCSP 要求にナンス拡張が含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するとき、OCSP 要求には OCSP ナンス拡張が含まれないため、ASA でチェックされません。デフォルトでは、OCSP 要求にナンス拡張が含まれています。ナンス拡張は、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。ただし、OCSP サーバーによっては、この一致するナンス拡張が含まれていない事前生成の応答が使用される場合があります。このようなサーバーでOCSPを使用するには、ナンス拡張をディセーブルにする必要があります。

例

次に、newtrust というトラストポイントのナンス拡張をディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。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 上書きルールを設定します。
ocsp interface*nameif*	OCSP 失効チェックで使用できるインターフェイスを指定します。
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に使用する OCSP サーバーを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

ocsp interface

ASA が OCSP に到達するように送信元インターフェイスを設定するには、crypto ca trustpool コンフィギュレーションモードで **interface** *nameif* コマンドを使用します。 構成からインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

ocsp interface *nameif*
no ocsp interface *nameif*

構文の説明

interface *nameif*	ASA が OCSP サーバーに到達するために使用するインターフェイスを指定します。

コマンド デフォルト

このコマンドのデフォルトはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(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

デフォルトでは、OCSP は管理インターフェイスエントリを含まないグローバル ルーティング テーブルを使用します。OCSP が管理インターフェイスの背後にある場合、OCSP 失効チェックは失敗します。このコマンドを使用すると、必要に応じて管理インターフェイスを含むインターフェイスを使用するように OCSP 失効チェックを設定できます。

例

次に、OCSP の送信元インターフェイスを設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
```

```
  url             OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt  url
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url  ?

crypto-ca-trustpoint mode commands/options:
  LINE < 500 char  URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url http://lal-bagh:8888
```

関連コマンド

コマンド	説明
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に使用する OCSP サーバーを指定します。
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	失効チェックに使用する方法と各方法を試す順序を指定します。

ocsp url

クライアント証明書の AIA 拡張で指定されたサーバーではなく、ASA の OCSP サーバーを、トラストポイントに関連付けられたすべての証明書のチェックに使用するように設定するには、暗号 CA トラストポイント コンフィギュレーション モードで **ocsp url** コマンドを使用します。このサーバーを構成から削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*
no ocsp url

構文の説明

URL OCSP サーバーの HTTP URL を指定します。

（注） ASA は、IPv4 と IPv6 両方の OCSP URL をサポートします。IPv6 アドレスは角カッコで囲みます（例：*http://[0:0:0:0:0.18:0a01:7c16/]*）。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.20(1)	IPv6 OCSP URL のサポートが追加されました。

使用上のガイドライン

ASA は HTTP URL のみをサポートします。トラストポイントごとに URL を 1 つだけ指定できます。

ASA では 3 つの方法で OCSP サーバーの URL を定義できます。また、定義方法に従って次の順序で OCSP サーバーの使用が試行されます。

- **match certificate** コマンドを使用して設定した OCSP サーバー。
- **ocsp url** コマンドを使用して設定した OCSP サーバー。

- クライアント証明書の AIA フィールドに指定された OCSP サーバー。

match certificate コマンドまたは **ocsp url** コマンドで OCSP URL を設定しない場合、ASA はクライアント証明書の AIA 拡張に指定された OCSP サーバーを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

次に、URL http://10.1.124.22 で OCSP サーバーを設定する例を示します。

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

次に、IPv6 URL を使用して OCSP を設定する方法の例を示します。

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp url  http://[0:0:0:0:0:ffff:0a01:7c16]
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。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 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp interface*nameif*	OCSP 失効チェックで使用できるインターフェイスを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

onscreen-keyboard（廃止）

ログイン/パスワード要件とともにオンスクリーンキーボードをログインペインまたはすべてのペインに挿入するには、webvpn モードで **onscreen-keyboard** コマンドを使用します。以前に設定したオンスクリーンキーボ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。

onscreen-keyboard { **logon** | **all** }
no onscreen-keyboard [**logon** | **all**]

構文の説明

logon	ログイン ペインのオンスクリーン キーボードを挿入します。
all	ログイン/パスワードの要件とともに、ログイン ペインおよび他のすべてのペインのオンスクリーン キーボードを挿入します。

コマンド デフォルト

オンスクリーン キーボードはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.17(1)	Web VPNのサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

オンスクリーン キーボードを使用すると、キーストロークなしでユーザー クレデンシャルを入力できます。

例

次に、ログイン ページのオンスクリーン キーボードをイネーブルにする例を示します。

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
```

```
 onscreen-keyboard logon
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn モードを開始し、クライアントレス SSLVPN 接続の属性を設定できるようにします。

ospf authentication

OSPF 認証の使用を有効にするには、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。デフォルトの認証状態に戻すには、このコマンドの **no** 形式を使用します。

ospf authentication { **key-chain key-chain-name** | **message-digest** | **null** }
no ospf authentication

構文の説明

key-chain *key-chain-name*	（任意）認証に使用するキー チェーンを指定します。key-name 引数には最大 63 文字の英数字を指定できます。
message-digest	（任意）OSPF メッセージ ダイジェスト認証を使用することを指定します。
null	（任意）OSPF 認証を使用しないことを指定します。

コマンド デフォルト

デフォルトでは、OSPF 認証はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.12(1)	OSPF 認証のローテーション キーをサポートするためにキー チェーン機能が追加されました。

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は、**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。

下位互換性を確保するため、エリアの認証タイプは引き続きサポートされます。インターフェイスの認証タイプを指定しないと、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です）。

このコマンドをオプションなしで使用すると、簡易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で OSPF の簡易パスワード認証をイネーブルにする例を示します。

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

次に、選択したインターフェイスで OSPF のキー チェーン パスワード認証を有効にする例を示します。

```
ciscoasa(config)# interface gigabitEthernet 0/0
ciscoasa(config-if)# ospf authentication key-chain CHAIN-INT-OSPFKEYS
```

関連コマンド

コマンド	説明
ospf **authentication-key**	ネイバー ルーティング デバイスで使用され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、MD5 キーを指定します。

ospf authentication-key

ネイバー 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 [**0** | **8** } *password*
no ospf authentication-key

構文の説明

0	暗号化されていないパスワードが後に続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
password	ネイバー ルーティング デバイスで使用される 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 文字間にブランク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ブランクは無視されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドが作成するパスワードは、ルーティング プロトコル パケットの送信時に、OSPF ヘッダーに直接挿入されるキーとして使用されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

例

次に、OSPF 認証のパスワードを指定する例を示します。

```
ciscoasa(config-if)# ospf authentication-key 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

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

インターフェイス経由でパケットを送信する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

構文の説明

interface_cost インターフェイス経由で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、符号なし整数値 0 ～ 65535 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、インターフェイス帯域幅が大きくなるほど、そのインターフェイス経由のパケット送信に伴うコストは低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。

ASA での OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファスト イーサネットおよびギガビット イーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでパケットを送信するコストを明示的に指定できます。*interface_cost* パラメータは、符号なし整数値 0 ～ 65535 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でパケットを送信するコストを指定する例を示します。

```
ciscoasa(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設定を表示します。

ospf database-filter

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発信 LSA をすべて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

構文の説明

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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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 の転送を復元します。

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。

```
ciscoasa(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* **minimal** | **hello-multiplier** *multiplier* }
no ospf dead-interval

構文の説明

seconds	hello パケットが確認されない時間の長さ。*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。
minimal	デッドインターバルを 1 秒に設定します。このキーワードを使用するには、キーワード hello-multiplier と引数 multiplier も設定する必要があります。
hello-multiplier multiplier	1 秒間に送信する hello パケットの個数を表す 3 ～ 20 の範囲の整数値。

コマンド 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 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.2(1)	fast hello パケットのサポートが追加されました。

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（no hello パケットが確認されない時間の長さ）を設定できます。*seconds* 引数にはデッド

間隔を指定し、その値はネットワーク上のすべてのノードで同じである必要があります。*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。

デッドインターバルは、OSPF helloパケットでアドバタイズされます。この値は、特定のネットワーク上の全ネットワーキング デバイスに対して同じにする必要があります。

小さいデッドインターバル（秒）を指定すると、ネイバーのダウンがより早く検出され、収束効率が高まりますが、ルーティングが不安定になる可能性があります。

fast hello パケットに対する OSPF のサポート

キーワード minimal とキーワード hello-multiplier を引数 multiplier とともに指定することで、OSPF fast hello パケットがイネーブルになります。キーワード minimal は、デッド インターバルを 1 秒に設定し、hello-multiplier の値は、その 1 秒間に送信される hello パケットの数を設定します。これにより、1 秒未満の「fast（高速な）」hello パケットの送信が可能になります。

インターフェイスで fast helloパケットが設定されている場合、このインターフェイスから送出される helloパケットでアドバタイズされる Helloインターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

デッド インターバルと fast hello 間隔を確認するには、show ospf interface コマンドを使用します。

例

次の例では、minimal キーワードおよび hello-multiplier キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

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の helloパケットの送信間隔を指定します。
show ospf interface	OSPF に関連する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送信される hello パケット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 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

構文の説明

seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。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 サーバーで同じにする必要があります。

例

次に、OSPF hello 間隔を 5 秒に設定する例を示します。

```
ciscoasa(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 に関連するインターフェイス情報を表示します。

ospf message-digest-key

OSPF MD5 認証を有効にするには、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** [**0** | **8**] *key*
no ospf message-digest-key

構文の説明

key-id	MD5 認証をイネーブルにし、認証キー ID 番号を数値で指定します。有効な値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字のパスワード。キーの文字間にスペースを含めることができます。キー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、発信元を認証し、適時性をチェックします。
0	暗号化されていないパスワードが後に続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

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。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、認証キーの 1 ～ 255 の数値識別子です。*key* は、最大 16 バイトの英数字のパスワードです。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。

例

次に、OSPF 認証の MD5 キーを指定する例を示します。

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

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

受信データベースパケットでOSPF最大伝送ユニット（MTU）ミスマッチ検出を無効にするには、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

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは **ospf mtu-ignore** は有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF は、ネイバーが共通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、ネイバーがデータベース記述子（DBD）パケットを交換するときに実行されます。DBDパケットの受信MTUが、着信インターフェイスに設定されているIPMTUよりも高い場合、OSPF 隣接関係は確立されません。**ospf mtu-ignore** コマンドは、受信 DBD パケットでOSPFMTUミスマッチ検出を無効にします。デフォルトでは有効になっています。

例

次に、**ospf mtu-ignore** コマンドを無効にする例を示します。

```
ciscoasa(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ノンブロードキャスト 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。構成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
no ospf network point-to-point non-broadcast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ospf network point-to-point non-broadcast コマンドを使用して、VPNトンネルを介して OSPF ルートを送信できます。

インターフェイスをポイントツーポイントとして指定したときは、OSPF ネイバーを手動で設定する必要があります。ダイナミック探索は機能しません。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したときには、次の制約事項が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- クリプト ポイントを指すスタティック 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限り、インターフェイスは隣接を形成できません。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、その同じインターフェイスでは上流のルータがある通常の OSPF を実行できません。
- OSPF 更新が VPN トンネルを通過できるように、OSPF ネイバーを指定する前に、クリプトマップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドする場合は、 **clear local-host all** コマンドを使用して OSPF 接続をクリアし、OSPF 隣接関係を VPN トンネル経由で確立できるようにします。

例

次に、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例を示します。

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

関連コマンド

コマンド	説明
neighbor	手動で設定した 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*]

構文の説明

number ルータのプライオリティを指定します。有効な値は、0 ～ 255 です。

コマンド 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。

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

使用上のガイドライン

ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。ルータのプライオリティは、マルチアクセス ネットワークへのインターフェイス専用に設定されます（つまり、ポイントツーポイント ネットワークへのインターフェイスには設定されません）。

マルチコンテキストモードでは、共有インターフェイスに 0 を指定して、デバイスが指定ルータにならないようにします。OSPFv2 インスタンスは、共有インターフェイス間で相互に隣接関係を形成できません。

例

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

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

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連する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*]

構文の説明

seconds インターフェイスに属する隣接ルータのLSA再送信間の時間を指定します。有効な値は、1 ～ 65535 秒です。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答メッセージを受信しないと、ルータは LSA を再送信します。

このパラメータの設定値は控えめにする必要があります。そうしないと、不要な再送信が発生します。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

次に、LSA の再送信間隔を変更する例を示します。

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

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連する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送信するために必要な推定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*]

構文の説明

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送信するために必要とされる時間を設定します。デフォルト値は 1 秒で、有効な値の範囲は 1 ～ 65535 秒です。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

更新パケット内の LSA には、送信前に、*seconds* 引数で指定した値によって増加された経過時間が格納されます。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。

リンクでの送信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。この設定は、非常に低速のリンクでより重要な意味を持ちます。

例

次に、選択したインターフェイスの送信遅延を 3 秒に設定する例を示します。

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

関連コマンド

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

otp expiration

ローカル認証局（CA）登録ページ用に発行されたワンタイムパスワード（OTP）の有効期間を時間単位で指定するには、CA サーバー コンフィギュレーション モードで **otp expiration** コマンドを使用します。期間をデフォルトの時間数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。

otp expiration *timeout*
no otp expiration

構文の説明

timeout 登録ページ用の OTP が期限切れになる前に、ユーザーがローカル CA から証明書を登録する必要がある期間を時間単位で指定します。有効な値の範囲は、1 ～ 720 時間（30 日）です。

コマンド デフォルト

デフォルトでは、証明書登録用の OTP の有効期限は 72 時間（3 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

OTP の有効期限には、ユーザが CA サーバの登録ページにログインする必要がある時間数を指定します。ユーザーがログインし、証明書を登録すると、**enrollment retrieval** コマンドで指定された期間が開始されます。

（注） 登録インターフェイス ページで証明書を登録するためのユーザー OTP は、そのユーザーの発行済みの証明書とキーペアが含まれている PKCS12 ファイルをアンロックするためのパスワードとしても使用されます。

例

次に、登録ページ用の OTP が 24 時間適用されることを指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# otp expiration 24
ciscoasa
(config-ca-server)
#
```

次に、OTP 期間をデフォルトの 72 時間にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# no otp expiration
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンドセットを使用することで、ローカル CA を設定および管理できます。
enrollment-retrieval	登録されたユーザーが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server	認証局コンフィギュレーションを表示します。

output console

action コマンドの出力をコンソールに送るには、イベントマネージャアプレットコンフィギュレーション モードで **output console** コマンドを使用します。コンソールを出力先から削除するには、このコマンドの **no** 形式を使用します。

output console
no output console

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**action** コマンドの出力をコンソールに送信する場合に使用します。

例

次に、**action** コマンドの出力をコンソールに送信する例を示します。

```
ciscoasa(config-applet)# output console
```

関連コマンド

コマンド	説明
output file append	**action** コマンドの出力は単一のファイルに書き込まれますが、ファイルには毎回出力が追加されます。
output file new	**action** コマンドの出力は、呼び出された各アプレットの新しいファイルに送信されます。

コマンド	説明
output file overwrite	**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。
output file rotate	ローテーションで使用する一連のファイルを作成します。
output none	**action** コマンドの出力を破棄します。

output file

指定したファイルに **action** コマンドの出力をリダイレクトするには、イベント マネージャ アプレット コンフィギュレーション モードで **output file** コマンドを使用します。指定したアクションを削除するには、このコマンドの **no** 形式を使用します。

output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]
no output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

構文の説明

append *filename*	指定したファイル名に出力を追加していきます。これは、ASAに対してローカルのファイル名です。
new	eem-*applet*-*timestamp* .log という名前の新しい出力先ファイルを作成します。*applet* はイベント マネージャ アプレットの名前、*timestamp* は YYYYMMDD-hhmmss の形式のタイムスタンプです。
overwrite *filename*	指定したファイルに出力を書き込み、イベント マネージャ アプレットを起動するたびに出力を上書きします。
rotate *n*	eem-*applet* -*x* .log という名前の出力ファイルを作成します。*applet* はイベント マネージャ アプレットの名前、*x* はファイルの番号です。新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数（*n* -1）で示されます。*n* 引数には、ローテーションの値を指定します。有効な値の範囲は 2 ～ 100 です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

output file コマンドは、指定したファイルに **action** コマンドの出力をリダイレクトする場合に使用します。

例

次に、単一のファイルに出力を追加する例を示します。

```
ciscoasa(config-applet)# output file append examplefile1
```

次に、**action** コマンドの出力を新しいファイルに送信する例を示します。

```
ciscoasa(config-applet)# output file new
```

次に、単一のファイルに出力を上書きする例を示します。

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

次に、ローテーションで使用する一連のファイルを作成する例を示します。

```
ciscoasa(config-applet)# output file rotate 50
```

関連コマンド

コマンド	説明
output console	**action** コマンドの出力をコンソールに送信します。
output none	**action** コマンドの出力を破棄します。

output none

action コマンドの出力を破棄するには、イベントマネージャアプレットコンフィギュレーション モードで **output none** コマンドを使用します。**action** コマンドの出力を保持するには、このコマンドの **no** 形式を使用します。

output none
no output none

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、**action** コマンドの出力はすべて破棄されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**action** コマンドの出力を破棄する場合に使用します。

例

次に、**action** コマンドの出力を破棄する例を示します。

```
ciscoasa(config-applet)# output none
```

関連コマンド

コマンド	説明
output console	**action** コマンドの出力をコンソールに送信します。
output file append	**action** コマンドの出力は単一のファイルに書き込まれますが、ファイルには毎回出力が追加されます。

コマンド	説明
output file new	**action** コマンドの出力は、呼び出された各アプレットの新しいファイルに送信されます。
output file overwrite	**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。
output file rotate	ローテーションで使用する一連のファイルを作成します。

outstanding（廃止）

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

認証されていない電子メールプロキシセッションの数を制限するには、適用可能な電子メールプロキシ コンフィギュレーション モードで **outstanding** コマンドを使用します。構成から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。

outstanding { *number* }
no outstanding

構文の説明

number	認証されていないセッションを許可する数。範囲は 1 ～ 1000 です。

コマンド デフォルト

デフォルトは 20 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

認証されていないセッションを許可する数に制限がないコンフィギュレーションから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。これは、電子メール ポートに対する DoS 攻撃も制限します。

電子メール プロキシ接続には、3 つの状態があります。

- **1.** 新規に電子メール接続が確立されると、「認証されていない」状態になります。

- **2.** この接続でユーザー名が提示されると、「認証中」状態になります。
- **3.** ASA が接続を認証すると、「認証済み」状態になります。

認証されていない状態の接続の数が設定済みの制限値を超えた場合、ASAは最も古い認証されていない接続を終了して、過負荷を回避します。認証済みの接続は終了しません。

例

次に、POP3S 電子メール プロキシの認証されていないセッションの制限を 12 に設定する例を示します。

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

override-account-disable（廃止）

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

AAA サーバーからの account-disabled インジケータを上書きするには、トンネルグループ一般属性コンフィギュレーション モードで **override-account-disable** コマンドを使用します。上書きを無効にするには、このコマンドの **no** 形式を使用します。

override-account-disable
no override-account-disable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、NT LDAP がある RADIUS や Kerberos など、「account-disabled」インジケータを返すサーバーに有効です。

IPsec RA および WebVPN トンネル グループにこの属性を設定できます。

例

次に、「testgroup」という WebVPN トンネル グループについて AAA サーバーからの「account-disabled」インジケータの上書きを許可する例を示します。

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

次に、「QAgroup」という IPsec リモート アクセス トンネル グループについて AAA サーバーからの「account-disabled」インジケータの上書きを許可する例を示します。

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(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クリアします。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

override-svc-download

AnyConnect クライアントまたは SSL VPN クライアントをダウンロードするためのグループポリシーまたはユーザー名属性構成を上書きするように接続プロファイルを設定するには、トンネルグループ webvpn 属性コンフィギュレーション モードで **override-svc-download** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、**no** 形式を使用します。

override-svc-download enable
no override-svc-download enable

コマンド デフォルト

デフォルトではディセーブルになっています。ASA は、クライアントをダウンロードするためのグループポリシーまたはユーザー名属性構成を上書きしません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

セキュリティアプライアンスは、**vpn-tunnel-protocol** コマンドによってグループポリシーまたはユーザー名属性でクライアントレスや SSL VPN が有効になっているかどうかに基づいて、リモートユーザーに対してクライアントレス接続、AnyConnect クライアント接続、または SSL VPN クライアント接続を許可します。**svc ask** コマンドは、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザーに要求して、クライアントのユーザーエクスペリエンスをさらに変更します。

ただし、特定のトンネル グループのもとでログインしているクライアントレス ユーザーが、ダウンロードの要求が期限切れになってクライアントレス SSL VPN ホームページが表示されるまで待たなくてもよいようにすることを推奨します。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザーに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザーには、**vpn-tunnel-protocol** コマンドまたは **svc ask** コマンドの設定に関係なく、クライアントレス SSL VPN ホームページがただちに表示されるようになります。

例

次に、ユーザーが接続プロファイル >*engineering* のトンネルグループ webvpn 属性コンフィギュレーション モードを開始し、この接続プロファイルでクライアントのダウンロード要求に関するグループポリシーおよびユーザー名属性の設定を上書きする例を示します。

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開するクライアント パッケージ ファイルを指定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。