shox ～ sn

shun

攻撃元ホストからの接続をブロックするには、特権 EXEC モードで shun コマンドを使用します。shun を無効にするには、このコマンドの **no** 形式を使用します。

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]
no shun *source_ip* [**vlan** *vlan_id*]

構文の説明

dest_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。
dest_ip	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。
protocol	（任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。
source_ip	攻撃元ホストのアドレスを指定します。送信元IPアドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shunがそのまま維持されます。
source_port	（任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。
vlan_id	（任意）送信元ホストが配置されている VLAN ID を指定します。

コマンド デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）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。

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
特権 EXEC	• 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。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続をブロックできます。送信元 IP アドレスからの今後のすべての接続は、手動または Cisco IPS センサーによってブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。shun コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

shun コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

shun コマンドは攻撃をダイナミックにブロックするために使用されるため、ASA コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。新しいインターフェイスを追加するか、または同じインターフェイスを（同じ名前を使用して）置き換える場合、IPS センサーでそのインターフェイスをモニターするには、そのインターフェイスを IPS センサーに追加する必要があります。

例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、ASA 接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、shun コマンドを適用します。

```
ciscoasa# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドにより、現在の接続はASA接続テーブルから削除され、10.1.1.27からの今後のすべてのパケットは ASA を通過できなくなります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。
show conn	すべてのアクティブな接続を表示します。
show shun	回避についての情報を表示します。

shutdown（ca サーバー）

ローカル認証局（CA）サーバーをディセーブルにし、ユーザーが登録インターフェイスにアクセスできないようにするには、CA サーバー コンフィギュレーション モードで **shutdown** コマンドを使用します。CA サーバーをイネーブルにし、コンフィギュレーションをロックして変更できないようにし、登録インターフェイスにアクセスできるようにするには、このコマンドの **no** 形式を使用します。

［ **no** ］**shutdown**

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

最初は、CA サーバーはデフォルトでシャットダウンされます。

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
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

CA サーバーモードのこのコマンドは、インターフェイスモードの **shutdown** コマンドと類似しています。セットアップ時に、ローカル CA サーバーはデフォルトでシャットダウンされるため、**no shutdown** コマンドを使用してイネーブルにする必要があります。**no shutdown** コマンドを初めて使用するときは、CA サーバーをイネーブルにし、CA サーバー証明書とキーペアを生成します。

（注） **no shutdown** コマンドを発行することによって、CA コンフィギュレーションをロックして CA 証明書を生成した後は、CA コンフィギュレーションを変更できません。

no shutdown コマンドで CA サーバーをイネーブルにして現在のコンフィギュレーションをロックするには、生成される CA 証明書とキーペアが含まれる PKCS12 ファイルを符号化してアー

カイブするために、7文字のパスワードが必要です。このファイルは、以前に指定した**database path** コマンドで識別されるストレージに格納されます。

例

次に、ローカル CA サーバーをディセーブルにし、登録インターフェイスにアクセスできないようにする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# shutdown
ciscoasa
(config-ca-server)
#
```

次に、ローカル CA サーバーをイネーブルにし、登録インターフェイスにアクセスできるようにする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no shutdown
ciscoasa
(config-ca-server)
#
ciscoasa
(config-ca-server)
# no shutdown
% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: caserver
Re-enter password: caserver
Keypair generation process begin. Please wait...
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 CLI 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。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

shutdown（インターフェイス）

インターフェイス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 **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown
no shutdown

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

すべての物理インターフェイスは、デフォルトではシャットダウンされます。セキュリティ コンテキスト内の割り当て済みのインターフェイスは、コンフィギュレーション内でシャットダウンされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

（注） このコマンドでは、ソフトウェアインターフェイスのみがディセーブルになります。物理リンクはアップのまま維持され、対応するインターフェイスが **shutdown** コマンドを使用して設定された場合でも、直接接続されたデバイスはアップであると認識されます。

例

次に、メイン インターフェイスをイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

次に、サブインターフェイスをイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、サブインターフェイスをシャットダウンする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

sip address

DHCPv6 サーバーを設定するときに、Session Initiation Protocol（SIP）サーバー IP アドレスをステートレスアドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sip address** コマンドを使用します。SIP サーバーを削除するには、このコマンドの **no** 形式を使用します。

sip address *sip_ipv6_address*
no sip address *sip_ipv6_address*

構文の説明

sip_ipv6_address	SIP サーバーの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

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

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

この機能は、クラスタリングではサポートされていません。

例

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

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sip domain-name eng.example.com
sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
sip domain-name it.example.com
sip server 2001:DB8:2::8
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

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

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

sip domain-name

DHCPv6 サーバーを設定するときに、Session Initiation Protocol（SIP）ドメイン名をステートレスアドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sip domain-name** コマンドを使用します。SIP ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

sip domain-name *sip_domain_name*
no sip domain-name *sip_domain_name*

構文の説明

sip_domain_name	SIP ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

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

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

この機能は、クラスタリングではサポートされていません。

例

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

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sip domain-name eng.example.com
sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
sip domain-name it.example.com
sip server 2001:DB8:2::8
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

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

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

site-id

サイト間クラスタリングの場合は、クラスタ グループ コンフィギュレーション モードで**site-id** コマンドを使用します。サイト ID を削除するには、このコマンドの **no** 形式を使用します。

site-id*number*
no site-id *number*

構文の説明

number	1 ～ 8 の範囲でサイト ID を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。
9.5(2)	LISP フロー モビリティとともに使用するために、トランスペアレント モードでこのコマンドを入力できるようになりました。
9.7(1)	FXOS では、FXOS 論理デバイス設定でサイト ID を設定する必要があります。ASA では変更できません。

使用上のガイドライン

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスで動作します。ASA クラスタから送信されたパケットはサイト固有の MAC アドレスを使用しますが、クラスタによって受信されるパケットはグローバル MAC アドレスを使用します。この機能により、スイッチが 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスを学習してしまうのを防いでいます。MAC フラッピングが発生しないよう、サイト MAC アドレスのみを学習します。サイト固有の MAC アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされています。

また、サイト ID は LISP インスペクションを使用するフロー モビリティを有効にするためにも使用されます。

マスターユニットに MAC アドレスを設定するには、**mac-address site-id** コマンドを使用し、その後、**site-id** コマンドを使用して、各ユニット（マスターとスレーブ）をクラスタブートストラップ設定の一部としてサイトに割り当てます。

例

次に、port-channel 2 のサイト固有の MAC アドレスを設定して、マスター ユニットをサイト 1 に割り当てる例を示します。

```
ciscoasa(config)# interface port-channel 2
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。

コマンド	説明
mac-address site-id	各サイトのサイト固有の MAC アドレスを設定します。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

site-periodic-garp interval

クラスタリングのための gratuitous ARP (GARP) 間隔をカスタマイズするには、クラスタ グループ コンフィギュレーション モードで **site-periodic-garp interval** コマンドを使用します。GARP 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。

site-periodic-garp interval *seconds*
no site-periodic-garp interval

構文の説明

seconds	GARP 生成の間隔を 1 ～ 1000000 秒間の秒単位で設定します。デフォルトは 290 秒です。

コマンド デフォルト

デフォルトの間隔は 290 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
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.12(1)	コマンドが追加されました。

使用上のガイドライン

ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保ちます。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。

クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。

例

次に、GARP 間隔を 500 秒に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ モードを開始します。

site-redundancy

サイトの障害からクラスタのフローを保護するには、クラスタ グループ コンフィギュレーション モードで **site-redundancy** コマンドを使用します。サイトの冗長性を無効にするには、このコマンドの **no** 形式を使用します。

site-redundancy
no site-redundancy

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

サイトの冗長性は、デフォルトで無効です。

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
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

使用上のガイドライン

サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。

ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。

例

次に、間隔を 300 ミリ秒に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-redundancy
```

関連コマンド

コマンド	説明
director-localization	ディレクタ ローカリゼーションを有効にします。これによりパフォーマンスが向上し、データ センターのサイト間クラスタリングでラウンドトリップ時間の遅延が減少します。

sla monitor

SLA 動作を作成するには、グローバル コンフィギュレーション モードで **sla monitor** コマンドを使用します。SLA 動作を削除するには、このコマンドの **no** 形式を使用します。

sla monitor *sla_id*
no sla monitor *sla_id*

構文の説明

sla_id	設定する SLA の ID を指定します。SLA が存在しない場合は、作成されます。有効な値は 1 ～ 2147483647 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
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	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

sla monitor コマンドによって、SLA 動作が作成され、SLA モニター コンフィギュレーション モードが開始されます。このコマンドを入力すると、コマンドプロンプトは ciscoasa (config-sla-monitor)# に変わり、SLA モニター コンフィギュレーション モードになったことが示されます。SLA動作がすでに存在し、それに対してタイプがすでに定義されている場合、プロンプトは ciscoasa (config-sla-monitor-echo)# と表示されます。最大 2000 個の SLA 動作を作成できます。任意の時点でデバッグできるのは 32 個の SLA 動作のみです。

no sla monitor コマンドによって、指定した SLA 動作およびその動作を設定するために使用されたコマンドが削除されます。

SLA動作を設定した後、**sla monitor schedule** コマンドで動作をスケジューリングする必要があります。スケジューリング後は、SLA動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択したSLA動作を完全に削除する必要があります。SLA動作を削除すると、

関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

動作の現在の設定を表示するには、**show sla monitor configuration** コマンドを使用します。SLA 動作の動作統計情報を表示するには、**show sla monitor operation-state command** コマンドを使用します。コンフィギュレーション内の SLA コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor schedule	SLA 動作をスケジューリングします。
timeout	SLA 動作が応答を待機する時間を設定します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

sla monitor schedule

SLA 動作をスケジューリングするには、グローバル コンフィギュレーション モードで **sla monitor schedule** コマンドを使用します。SLA 動作のスケジュールを削除し、動作を保留状態にするには、このコマンドの **no** 形式を使用します。

sla monitor schedule *sla-id* [**life** { **forever** | *seconds* }] [**start-time** { *hh:mm* [*:ss*] [*month day* | *day month*] **| pending | now | after** *hh:mm:ss* }] [**ageout** *seconds*] [**recurring**]
no sla monitor schedule *sla-id*

構文の説明

after *hh* : *mm* : *ss*	コマンドの入力後、何時間、何分、何秒で動作が開始されるかを示します。
ageout *seconds*	（任意）情報をアクティブに収集していない場合、動作をメモリに常駐させておく時間を秒数で指定します。エージング アウト後、SLA 動作は実行コンフィギュレーションから削除されます。
day	動作を開始する日。有効な値は、1 ～ 31 です。日を指定しない場合、現在の日が使用されます。日を指定する場合は、月も指定する必要があります。
hh : *mm* [: *ss*]	絶対開始時刻を 24 時間表記で指定します。秒は任意です。 *month* および *day* を指定しない場合は、指定した時刻が次に来たときとなります。
life forever	（任意）無期限に実行されるように動作をスケジューリングします。
life *seconds*	（任意）動作によって情報がアクティブに収集される秒数を設定します。
month	（オプション）動作を開始する月の名前。月を指定しない場合は、現在の月が使用されます。月を指定する場合は、日も指定する必要があります。 月の英語名を完全に入力するか、または、最初の 3 文字のみを入力します。
now	コマンドを入力するとすぐに動作が開始されることを示します。
pending	情報が収集されないことを示します。これは、デフォルトの状態です。
recurring	（任意）動作が毎日、指定した時刻に自動的に開始され、指定した時間継続されることを示します。
sla-id	スケジューリングする SLA 動作の ID。
start-time	SLA 動作が開始される時刻を設定します。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- SLA 動作は、スケジューリングされた時間になるまで **pending** 状態です。つまり、動作はイネーブルですが、データはアクティブに収集されていません。
- デフォルトの **ageout** 時間は、0 秒（エージングアウトしない）です。
- デフォルトの **life** は、3600 秒（1 時間）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
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	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

SLA 動作がアクティブ状態の場合、ただちに情報の収集が開始されます。次のタイム ラインは、動作のエージング アウト プロセスを示しています。

```
W----------------------X----------------------Y----------------------Z
```

- W は、SLA 動作が **sla monitor** コマンドで設定された時刻です。
- X は、SLA 動作の開始時刻です。これは、動作が「アクティブ」になったときです。
- Y は、 **sla monitor schedule** コマンドで設定された有効期間の終了です（ **life** の秒数は 0 までカウント減少されました）。
- Z は、動作のエージング アウトです。

エージアウト プロセスは、使用されている場合は、W でカウント ダウンを開始し、X と Y の間は中断され、設定されたサイズにリセットされると、再び Y でカウント ダウンを開始します。SLA 動作がエージ アウトすると、SLA 動作の設定は実行コンフィギュレーションから削除されます。動作は、実行される前にエージングアウトする可能性があります（つまり、Z が X の前に発生する可能性があります）。このような状況が発生しないようにするには、動作のコンフィギュレーション時刻と開始時刻（X と W）の差を、エージング アウトの秒数よりも小さくする必要があります。

recurring キーワードは、単一の SLA 動作のスケジューリングに対してのみサポートされています。1 つの **sla monitor schedule** コマンドを使用して複数の SLA 動作をスケジューリングすることはできません。定期的な SLA 動作の **life** 値は、1 日未満にする必要があります。定期

的な動作の **ageout** 値を「なし」（値 0 で指定）にするか、**life** 値と **ageout** 値の合計を 1 日よりも大きくする必要があります。recurring オプションを指定しないと、動作は既存の通常のスケジューリング モードで開始されます。

スケジューリング後は、SLA 動作のコンフィギュレーションを変更できません。スケジューリングした SLA 動作のコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA 動作を完全に削除する必要があります。SLA 動作を削除すると、関連づけられた **sla monitor schedule** コマンドも削除されます。その後、SLA 動作のコンフィギュレーションを再入力できます。

例

次に、4 月 5 日午後 3 時にデータの収集をアクティブに開始するようにスケジューリングされた SLA 動作 25 の例を示します。この動作は、非アクティブになって 12 時間後にエージング アウトします。この SLA 動作がエージング アウトすると、SLA 動作のすべてのコンフィギュレーション情報は実行コンフィギュレーションから削除されます。

```
ciscoasa(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

次に、5 分間の遅延の後にデータの収集を開始するようにスケジューリングされた SLA 動作 1 の例を示します。デフォルトの有効期間である 1 時間が適用されます。

```
ciscoasa(config)# sla monitor schedule 1 start after 00:05:00
```

次に、ただちにデータの収集を開始するようにスケジューリングされた SLA 動作 3 の例を示します。この例は、無期限に実行されるようにスケジューリングされています。

```
ciscoasa(config)# sla monitor schedule 3 life forever start-time now
```

次に、毎日午前 1 時 30 分にデータの収集を自動的に開始するようにスケジューリングされた SLA 動作 15 の例を示します。

```
ciscoasa(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

関連コマンド

コマンド	説明
show sla monitor configuration	SLA コンフィギュレーション設定を表示します。
sla monitor	SLA モニタリング動作を定義します。

smart-tunnel auto-signon enable（廃止）

クライアントレス（ブラウザベース）SSL VPNセッションでスマートトンネル自動サインオンをイネーブルにするには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-signon enable** コマンドを使用します。

グループポリシーまたはユーザー名から **smart-tunnel auto-signon enable** コマンドを削除し、デフォルトのグループポリシーから継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel auto-signon enable *list* [**domain** ドメイン] [**port** *port*] [**realm** *realm string*]

構文の説明

domain ドメイン	（任意）。認証中にユーザー名に追加されるドメインの名前。ドメインを入力する場合、**use-domain** キーワードをリストエントリに入力します。
list	ASA の webvpn コンフィギュレーションにすでに存在するスマートトンネル自動サインオンリストの名前。 SSL VPN コンフィギュレーション内のスマートトンネル自動サインオンリストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。
port	自動サインオンを実行するポートを指定します。
レルム	認証のレルムを設定します。

コマンド デフォルト

このコマンドに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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 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(4)	このコマンドが追加されました。
8.4(1)	オプションの *realm* 引数と *port* 引数が追加されました。
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

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバーと通信します。

smart-tunnel auto-signon *list* コマンドを使用して、最初にサーバーのリストを作成する必要があります。グループ ポリシーまたはユーザー名に割り当てることができるリストは 1 つだけです。

レルムの文字列は Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。対応するレルムがわからない場合、管理者はログインを一度実行し、プロンプト ダイアログから文字列を取得する必要があります。

管理者は、対応するホストに任意でポート番号を指定できるようになりました。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。

例

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにします。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR
ciscoasa(config-group-webvpn)
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをイネーブルにし、認証中に CISCO という名前のドメインをユーザー名に追加します。

```
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

次のコマンドでは、HR という名前のスマート トンネル自動サインオン リストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル自動サインオン リスト コマンドを継承します。

```
ciscoasa(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon *list*	スマート トンネル接続でクレデンシャルの送信を自動化する対象のサーバーのリストを作成します。
show running-config webvpn smart-tunnel	ASA のスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザーのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel *list*	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel auto-signon list（廃止）

スマートトンネル接続でクレデンシャルの送信を自動化する対象のサーバーのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel auto-signon list** コマンドを使用します。リストに追加する各サーバーに対してこのコマンドを使用します。

リストからエントリを削除するには、このコマンドの **no** 形式を使用します。リストと、ASA コンフィギュレーションに表示されている IP アドレスまたはホスト名を指定します。

no smart-tunnel auto-signon *list* [**use-domain**] { **ip** *ip-address* [*netmask*] | **host** *hostname-mask* }

スマートトンネル自動サインオンリストのエントリを表示するには、特権EXECモードで**show running-config webvpn smart-tunnel** コマンドを入力します。

サーバーのリスト全体を ASA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストのみを指定します。

no smart-tunnel auto-signon *list*

構文の説明

host	ホスト名またはワイルドカード マスクによって識別されるサーバー。
hostname-mask	自動認証する対象のホスト名またはワイルドカード マスク。
ip	IP アドレスおよびネット マスクによって識別されるサーバー。
ip-address [*netmask*]	自動認証する対象のホストのサブネットワーク。
list	リモート サーバーのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。文字列は最大 64 文字まで使用できます。コンフィギュレーション内にリストが存在しない場合は、ASA によって作成されます。存在する場合、リストにエントリを追加します。
use-domain	（任意）認証で必要な場合、Windows ドメインをユーザー名に追加します。このキーワードを入力する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーまたはユーザー名に割り当てるときにドメイン名を指定してください。

コマンド デフォルト

このコマンドに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
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(4)	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

スマート トンネル自動サインオン機能は、Microsoft WININET ライブラリを使用した HTTP および HTTPS 通信を行うアプリケーションだけをサポートしています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバーと通信します。

スマートトンネル自動サインオンリストの入力に続き、グループポリシー webvpn モードまたはユーザー名 webvpn モードで **smart-tunnel auto-signon enable** *list* コマンドを使用してリストを割り当てます。

例

次のコマンドでは、サブネット内のすべてのホストを追加し、認証で必要な場合に Windows ドメインをユーザー名に追加します。

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

次のコマンドは、リストからエントリを削除します。

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

前述のコマンドでは、削除されるエントリがリストの唯一のエントリである場合、HR という名前のリストも削除されます。唯一のエントリではない場合は、次のコマンドによってリスト全体が ASA コンフィギュレーションから削除されます。

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR
```

次のコマンドでは、ドメイン内のすべてのホストを intranet という名前のスマート トンネル自動サインオン リストに追加します。

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

次のコマンドは、リストからエントリを削除します。

```
ciscoasa(config-webvpn)# no smart-tunnel
 auto-signon intranet host *.exampledomain.com
```

関連コマンド

コマンド	説明
smart-tunnel auto-signon enable	コマンドモードで指定されたグループポリシーまたはユーザー名に対して、スマート トンネル自動サインオンをイネーブルにします。
smart-tunnel auto-signon enable *list*	グループ ポリシーまたはユーザー名にスマート トンネル自動サインオン リストを割り当てます。
show running-config webvpn smart-tunnel	スマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザーのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザーのログイン時にスマートトンネルアクセスをイネーブルにします。ただし、ユーザーはクライアントレス SSL VPN ポータルページの [**Application Access**] > [**Start Smart Tunnels**] ボタンを使用して、スマートトンネルアクセスを手動で開始する必要がある。

smart-tunnel auto-start（廃止）

クライアントレス（ブラウザベース）SSL VPNセッションでユーザーがログインしたときにスマートトンネルアクセスを自動的に開始するには、グループポリシーwebvpnコンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、**smart-tunnel auto-start** コマンドを使用します。

smart-tunnel auto-start *list*

グループポリシーまたはユーザー名から **smart-tunnel** コマンドを削除し、デフォルトグループポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list *list* は、ASA webvpn コンフィギュレーションにすでに存在するスマートトンネルリストの名前です。

SSL VPN コンフィギュレーション内にすでに存在するスマートトンネルリストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

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
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—
ユーザー名 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。

リリース	変更内容
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

このコマンドでは、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

ユーザーのログイン時にスマート トンネル アクセスを開始するこのオプションは Windows だけに適用されます。

例

次のコマンドでは、apps1 という名前のアプリケーションのリストについて、スマート トンネル アクセスを開始します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1
ciscoasa(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル コマンドを継承します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel enable	ユーザーのログイン時にスマートトンネルアクセスをイネーブルにします。ただし、ユーザーはクライアントレス SSL VPN ポータルページの [**Application Access**] > [**Start Smart Tunnels**] ボタンを使用して、スマートトンネルアクセスを手動で開始する必要がある。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel disable（廃止）

クライアントレス（ブラウザベース）SSL VPNセッションでスマートトンネルアクセスを禁止するには、グループポリシーwebvpnコンフィギュレーションモードまたはユーザー名webvpnコンフィギュレーション モードで、**smart-tunnel disable** コマンドを使用します。

smart-tunnel disable

グループポリシーまたはユーザー名から **smart-tunnel** コマンドを削除して、デフォルトのグループポリシーから [**no**] **smart-tunnel** コマンドを継承するには、このコマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

デフォルトではスマートトンネルはイネーブルではないため、**smart-tunnel disable** コマンドは（デフォルトの）グループポリシーまたはユーザー名コンフィギュレーションに、対象のポリ

シーまたはユーザー名に適用しない **smart-tunnel auto-start** または **smart-tunnel enable** コマンドが含まれている場合にのみ必要です。

例

次のコマンドでは、スマート トンネル アクセスを禁止します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel disable
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
smart-tunnel auto-start	ユーザーのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel enable	ユーザーのログイン時にスマートトンネルアクセスをイネーブルにします。ただし、ユーザーはクライアントレス SSL VPN ポータルページの [**Application Access**] > [**Start Smart Tunnels**] ボタンを使用して、スマートトンネルアクセスを手動で開始する必要がある。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel enable（廃止）

クライアントレス（ブラウザベース）SSL VPN セッションでスマートトンネルアクセスをイネーブルにするには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで、**smart-tunnel enable** コマンドを使用します。

smart-tunnel enable *list*

グループポリシーまたはユーザー名から **smart-tunnel** コマンドを削除し、デフォルトグループポリシーの [**no**] **smart-tunnel** コマンドを継承するには、コマンドの **no** 形式を使用します。

no smart-tunnel

構文の説明

list *list* は、ASA webvpn コンフィギュレーションにすでに存在するスマートトンネルリストの名前です。

SSL VPN コンフィギュレーション内のスマートトンネルリストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを入力します。

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
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—
ユーザー名 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

smart-tunnel enable コマンドによって、スマートトンネルアクセスに適格なアプリケーションのリストがグループポリシーまたはユーザー名に割り当てられます。ユーザーは、クライアントレス SSL VPN ポータルページの [アプリケーションアクセス（**Application Access**）] > [スマートトンネルの開始（**Start Smart Tunnels**）] ボタンを使用して、手動でスマートトンネルアクセスを開始する必要があります。または、**smart-tunnel auto-start** コマンドを使用して、ユーザーがログインしたときに自動的にスマートトンネルアクセスを開始できます。

いずれのコマンドでも、**smart-tunnel list** コマンドを使用して、最初にアプリケーションのリストを作成する必要があります。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストをイネーブルにします。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel enable apps1
ciscoasa(config-group-webvpn)
```

次のコマンドでは、apps1 という名前のリストをグループ ポリシーから削除し、デフォルトのグループ ポリシーからスマート トンネル リストを継承します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN コンフィギュレーションを、すべてのスマート トンネル リスト エントリを含めて表示します。
smart-tunnel auto-start	ユーザーのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。
smart-tunnel list	プライベート サイトへの接続にクライアントレス SSL VPN セッションを使用できるアプリケーションのリストにエントリを追加します。

smart-tunnel list（廃止）

プライベートサイトに接続する場合にクライアントレス（ブラウザベース）SSL VPNセッションを使用できるアプリケーションのリストに入力するには、webvpn コンフィギュレーションモードで **smart-tunnel list** コマンドを使用します。アプリケーションをリストから削除するには、このコマンドの **no** 形式を使用して、エントリを指定します。アプリケーションのリスト全体を ASA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用して、リストだけを指定します。

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]
no smart-tunnel list *list*

構文の説明

application	スマート トンネル アクセスが付与されるアプリケーションの名前。文字列は最大 64 文字まで使用できます。
hash	（任意。Windowsにのみ該当）この値を取得するには、アプリケーションのチェックサム（つまり、実行ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイルチェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。FCIV のインストール後、スペースを含まないパス（c:/fciv.exe など）に、ハッシュするアプリケーションの一時コピーを置き、コマンドラインで **fciv.exe -sha1** *application* と入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。 SHA-1 ハッシュは、常に 16 進数 40 文字です。
list	アプリケーションまたはプログラムのリストの名前。スペースを含む場合、名前の前後に引用符を使用します。コンフィギュレーション内にリストが存在しない場合は、CLI によって作成されます。存在する場合、リストにエントリを追加します。
path	Mac OS の場合は、アプリケーションのフルパス。Windows の場合は、アプリケーションのファイル名。または、ファイル名を含むアプリケーションのフルパスまたは部分パス。ストリングには最大 128 文字を使用できます。
platform *OS*	（OS が Microsoft Windows の場合は任意）**windows or mac** を入力して、アプリケーションのホストを指定します。

コマンド デフォルト

Windows がデフォルトのプラットフォームです。

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
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。
8.0(4)	**platform** *OS* 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

複数のスマートトンネルリストを ASA で設定できますが、複数のスマートトンネルリストを特定のグループポリシーまたはユーザー名に割り当てることはできません。スマートトンネルリストに入力するには、アプリケーションごとに **smart-tunnel list** コマンドを 1 回入力します。同じ *list* ストリングを入力しますが、OS で一意の *application* および *path* を指定します。リストでサポートする各 *OS* について、コマンドを 1 回入力します。

OS がエントリで指定されたものと一致しない場合、セッションでリスト エントリは無視されます。アプリケーションのパスが存在しない場合も、エントリは無視されます。

SSL VPN コンフィギュレーション内のスマートトンネルリストのエントリを表示するには、特権 EXEC モードで **show running-config webvpn smart-tunnel** コマンドを入力します。

path はコンピュータ上のものと一致する必要がありますが、完全である必要はありません。たとえば、実行ファイルとその拡張子だけで *path* を構成できます。

スマート トンネルには次の要件があります。

- スマートトンネル接続を開始するリモートホストでは、32 ビットバージョンの Microsoft Windows Vista、Windows XP、または Windows 2000、あるいは Mac OS 10.4 または 10.5 が実行されている必要があります。
- スマート トンネルまたはポート フォワーディングを使用する Microsoft Windows Vista のユーザーは、ASA の URL を [Trusted Site] ゾーンに追加する必要があります。信頼済みサイト ゾーンにアクセスするには、Internet Explorer を起動して、[Tools] > [Internet Options] > [Security] タブを選択する必要があります。Vista ユーザーは、[Protected Mode] をディセーブルにしてスマート トンネル アクセスを容易にすることもできます。ただし、攻撃に対するコンピュータの脆弱性が増すため、この方法は推奨しません。
- ブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- Mac OS のスマート トンネル サポートには、Safari 3.1.1 以降が必要です。

Microsoft Windows では、Winsock 2、TCP ベースのアプリケーションのみがスマート トンネル アクセスに適格です。

Mac OS では、SSL ライブラリにダイナミックにリンクされた、TCP を使用するアプリケーションをスマート トンネルで使用できます。次のタイプのアプリケーションは、スマート トンネルで使用できません。

- dlopen または dlsym を使用して libsocket コールを特定するアプリケーション
- libsocket コールを特定するためにスタティックにリンクされたアプリケーション
- 2 レベルのネーム スペースを使用する Mac OS アプリケーション。
- Mac OS のコンソールベースのアプリケーション（Telnet、SSH、cURL など）。
- Mac OS の PowerPC タイプのアプリケーション。Mac OS アプリケーションのタイプを判別するには、そのアイコンを右クリックして [Get Info] を選択します。

Mac OS では、ポータル ページから起動されたアプリケーションだけがスマート トンネル セッションを確立できます。この要件には、Firefox に対するスマート トンネルのサポートも含まれます。スマート トンネルを最初に使用する際に、Firefox を使用して Firefox の別のインスタンスを起動するには、csco_st という名前のユーザー プロファイルが必要です。このユーザー プロファイルが存在しない場合、セッションでは、作成するようにユーザーに要求します。

次の制限事項がスマート トンネルに適用されます。

- リモート コンピュータが ASA にアクセスするためにプロキシ サーバーを必要とする場合、接続の終端側の URL が、プロキシ サービスから除外される URL のリストに存在する必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。
- スマート トンネル自動サインオン機能では、Microsoft Windows OS 上の Microsoft WININET ライブラリを使用して HTTP または HTTPS 通信を行うアプリケーションのみがサポートされます。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバーと通信します。
- グループ ポリシーまたはローカル ユーザー ポリシーでは、スマート トンネル アクセスに適格なアプリケーションのリスト 1 つと、スマート トンネル自動サインオン サーバーのリスト 1 つだけがサポートされます。
- ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザーはフェールオーバー後に再接続する必要があります。

（注） スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*path* 値が最新でないことを示している場合があります。たとえば、アプリケーションおよび次のアップグレードを作成する会社が買収されると、アプリケーションのデフォルトのパスは通常は変更されます。

ハッシュを入力すると、*path* で指定したストリングと一致する不適格なファイルがクライアントレス SSL VPN によって認定されないことが、ある程度保証されます。チェックサムはアプ

リケーションの各バージョンまたはパッチによって異なるため、入力する *hash* が一致するのは、リモートホスト上の1つのバージョンまたはパッチのみです。アプリケーションの複数のバージョンに対して *hash* を指定するには、各バージョンに対して **smart-tunnel list** コマンドを1回入力します。このとき、各コマンドでは、同じ *list* ストリングを入力しますが、一意の *application* ストリングと一意の *hash* 値を指定します。

（注） *hash* 値を入力し、スマート トンネル アクセスでアプリケーションの今後のバージョンまたはパッチをサポートする場合は、今後もスマート トンネル リストを維持する必要があります。スマート トンネル アクセスで突然問題が発生した場合、アプリケーションのアップグレードにより、*hash* 値を含むアプリケーション リストが最新でないことを示している場合があります。この問題は *hash* を入力しないことによって回避できます。

スマートトンネルリストのコンフィギュレーションに続き、**smart-tunnel auto-start** コマンドまたは**smart-tunnel enable** コマンドを使用して、グループポリシーまたはユーザー名にリストを割り当てます。

例

次のコマンドでは、apps1 という名前のスマート トンネル リストに Microsoft Windows アプリケーションの接続を追加します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

次のコマンドでは、Windows アプリケーション msimn.exe を追加し、リモート ホスト上のアプリケーションのハッシュが、スマートトンネルアクセスを許可するために入力された最後のストリングと一致することを要求します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

次のコマンドでは、Mac OS ブラウザ Safari にスマート トンネル サポートを提供します。

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform
mac
```

関連コマンド

コマンド	説明
show running-config webvpn smart-tunnel	ASA のスマート トンネル コンフィギュレーションを表示します。
smart-tunnel auto-start	ユーザーのログイン時にスマート トンネル アクセスを自動的に開始します。
smart-tunnel disable	スマート トンネル アクセスを使用禁止にします。

コマンド	説明
smart-tunnel enable	ユーザーのログイン時にスマートトンネルアクセスをイネーブルにします。ただし、ユーザーはクライアントレス SSL VPN ポータルページの [**Application Access**] > [**Start Smart Tunnels**] ボタンを使用して、スマートトンネルアクセスを手動で開始する必要がある。

smart-tunnel network（廃止）

スマートトンネルポリシーの設定に使用するホストのリストを作成するには、webvpn コンフィギュレーション モードで **smart-tunnel network** コマンドを使用します。スマートトンネルポリシー用ホストのリストを不許可にするには、このコマンドの **no** 形式を使用します。

smart-tunnel network
no smart-tunnel network

構文の説明

host *host mask*	ホスト名（*.cisco.com など）。
ip *ip address*	ネットワークの IP アドレス。
netmask	ネットワークのネットマスク。
network name	トンネル ポリシーに適用するネットワーク名。

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
webvpn 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
8.3(1)	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

スマートトンネルがオンになっている場合、ネットワーク（ホストのセット）を設定する **smart-tunnel network** コマンド、および指定されたスマート トンネル ネットワークを使用してポリシーをユーザーに強制適用する **smart-tunnel tunnel-policy** コマンドによって、トンネル外のトラフィックを許可できます。

例

次に、**smart-tunnel network** コマンドの使用例を示します。

```
ciscoasa(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

関連コマンド

コマンド	説明
smart-tunnel tunnel-policy	指定されたスマート トンネル ネットワークを使用してポリシーをユーザーに強制適用します。

smart-tunnel tunnel-policy（廃止）

スマート トンネル トンネル ポリシーを特定のグループポリシーまたはユーザーポリシーに適用するには、コンフィギュレーション webvpn モードで **smart-tunnel tunnel-policy** コマンドを使用します。特定のグループからスマート トンネル トンネル ポリシーの適用をはずすには、このコマンドの [no] 形式を使用します。

smart-tunnel tunnel-policy
no smart-tunnel tunnel-policy

構文の説明

excludespecified	ネットワーク名で指定されたネットワークの外のネットワークだけをトンネリングします。
network name	トンネリングするネットワークをリストします。
tunnelall	すべてをトンネリング（暗号化）します。
tunnelspecified	ネットワーク名で指定されたネットワークだけをトンネリングします。

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
webvpn 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
8.3.1	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

スマートトンネルがオンになっている場合、ネットワーク（ホストのセット）を設定する **smart-tunnel network** コマンド、および指定されたスマート トンネル ネットワークを使用してポリシーをユーザーに強制適用する **smart-tunnel tunnel-policy** コマンドによって、トンネル外のトラフィックを許可できます。

例

次に、**smart-tunnel tunnel-policy** コマンドの使用例を示します。

```
ciscoasa(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

関連コマンド

コマンド	説明
smart-tunnel network	スマートトンネルポリシー設定のためホストのリストを作成します。

smtp from-address

ローカルCAサーバーが生成するすべての電子メール（ワンタイムパスワードの配布など）の送信者フィールドで使用する電子メールアドレスを指定するには、CAサーバー コンフィギュレーション モードで **smtp from-address** コマンドを使用します。電子メールアドレスをデフォルト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。

smtp from-address *e-mail_address*
no smtp from-address

構文の説明

e-mail_address	CA サーバーが生成するすべての電子メールの送信者フィールドに表示する電子メール アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

例

次に、ローカル CA サーバーからの、すべての電子メールの送信者フィールドに ca-admin@asa1-ca.example.com が含まれるように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp from-address ca-admin@asa1-ca.example.com
ciscoasa
(config-ca-server)
#
```

次に、ローカルCAサーバーからの、すべての電子メールの送信者フィールドをデフォルトのアドレス admin@asa1-ca.example.com にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp from-address admin@asa1-ca.example.com
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 CLI 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。
smtp subject	ローカル CA サーバーが生成するすべての電子メールの件名フィールドに表示するテキストをカスタマイズします。

smtp subject

ローカル認証局（CA）サーバーが生成するすべての電子メール（ワンタイムパスワードの配布など）の件名フィールドに表示するテキストをカスタマイズするには、CA サーバー コンフィギュレーションモードで**smtp subject**コマンドを使用します。テキストをデフォルト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。

smtp subject *subject-line*
no smtp subject

構文の説明

subject-line	CAサーバーから送信するすべての電子メールの件名フィールドに表示するテキストを指定します。最大文字数は 127 です。

コマンド デフォルト

デフォルトでは、件名フィールドのテキストは「Certificate Enrollment Invitation」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。

例

次に、CA サーバーからの、すべての電子メールの件名フィールドにテキスト *Action: Enroll for a certificate* を表示するように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp subject Action: Enroll for a certificate
ciscoasa
(config-ca-server)
#
```

次に、CAサーバーからの、すべての電子メールの件名フィールドのテキストをデフォルトのテキスト「Certificate Enrollment Invitation」にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no smtp subject
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 CLI 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。
smtp from-address	ローカル CA サーバーが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。

smtps（廃止）

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

SMTPS コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンドモードで入力された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。SMTPS は、SSL 接続での電子メールの送信を可能にする TCP/IP プロトコルです。

smtps
no smtps

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル 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。
9.5(2)	このコマンドは廃止されました。

例

次に、SMTPS コンフィギュレーション モードを開始する例を示します。

```
ciscoasa
(config)#
 smtps
ciscoasa(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバーを設定するには、グローバル コンフィギュレーション モードで **smtp-server** コマンドを使用します。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。

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*] *backup-smpt-server-ip-address*]
no smtp-server

構文の説明

primary-smpt-server-ip-address	プライマリ SMTP サーバーを指定します。IP アドレスまたはホスト名（**name** コマンドを使用して設定）を使用します。
backup-smpt-server-ip-address	（オプション）プライマリ SMTP サーバーが利用できない場合にイベント メッセージをリレーするバックアップ SMTP サーバーを指定します。IP アドレスまたはホスト名（**name** コマンドを使用して設定）を使用します。
primary_interface	（オプション）プライマリ smtp サーバーに到達するために使用できるプライマリ インターフェイス名を指定します。
backup_interface	（オプション）バックアップ smtp サーバーに到達するために使用できるバックアップ インターフェイス名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル 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。
9.5(2)	このコマンドは廃止されました。

リリース	変更内容
9.13(1)	ロギングのための適切な smtp サーバーに接続するために、プライマリおよびバックアップのインターフェイス名を任意で指定できます。

使用上のガイドライン

ASA には、内部 SMTP クライアントが含まれており、特定のイベントが発生したことを外部エンティティに通知するためにイベントシステムで使用できます。これらのイベント通知を受信し、指定された電子メールアドレスに転送するようにSMTPサーバーを設定できます。ASA に対して電子メールイベントをイネーブルにしている場合にのみ、SMTPファシリティはアクティブです。また、このコマンドにより、ロギングに使用するルーティング テーブル（管理ルーティング テーブルまたはデータ ルーティング テーブル）をインターフェイス アソシエーションで識別できるようにします。インターフェイスが指定されていない場合、ASA は管理ルーティング テーブル ルックアップを参照し、適切なルート エントリが存在しない場合は、データ ルーティング テーブルを参照します。

例

次に、SMTP サーバーを IP アドレス 10.1.1.24 を使用して設定し、バックアップ SMTP サーバーを IP アドレス 10.1.1.34 を使用して設定する例を示します。

```
ciscoasa
(config)#
 smtp-server 10.1.1.24 10.1.1.34
ciscoasa
(config)#
 smtp-server 10.1.1.24
ciscoasa
(config)#
 smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa
(config)#
 smtp-server management 10.1.1.24
```

snmp cpu threshold rising

高 CPU しきい値およびしきい値モニタリング期間のしきい値を設定するには、グローバル コンフィギュレーション モードで **snmp cpu threshold rising** コマンドを使用します。しきい値およびしきい値モニタリング期間を設定しない場合は、このコマンドの **no** 形式を使用します。

snmp cpu threshold rising *threshold_value monitoring_period*
no snmp cpu threshold rising *threshold_value monitoring_period*

構文の説明

monitoring_period	モニタリング期間を分単位で定義します。
threshold_value	しきい値レベルを CPU 使用率として定義します。

コマンド デフォルト

snmp cpu threshold rising コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70% の CPU 使用率を超えて設定されます。クリティカルしきい値レベルのデフォルトは 95% の CPU 使用率を超えて設定されます。I デフォルトのモニタリング期間は 1 分に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。ASA サービスモジュールには適用されません。

使用上のガイドライン

CPU のクリティカルしきい値レベルは設定できません。この値は 95 % に固定されています。有効なしきい値の範囲は 10 ～ 94% の CPU 使用率です。モニタリング期間の有効値は 1～60 分です。

例

次に、SNMP CPU しきい値レベルを 75% の CPU 使用率および 30 分のモニタリング期間に設定する例を示します。

```
ciscoasa(config)# snmp cpu threshold 75% 30
```

関連コマンド

コマンド	説明
snmp-server enable traps	SNMP-related トラップをイネーブルにします。
snmp link threshold	SNMP インターフェイスのしきい値を定義します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp interface threshold

SNMP物理インターフェイスのしきい値およびシステムメモリ使用率のしきい値を設定するには、グローバル コンフィギュレーション モードで **snmp interface threshold** コマンドを使用します。SNMP物理インターフェイスのしきい値およびシステムメモリ使用率のしきい値をクリアするには、このコマンドの **no** 形式を使用します。

snmp interface threshold *threshold_value*
no snmp interface threshold *threshold_value*

構文の説明

threshold_value	しきい値をCPU使用率として定義します。

コマンド デフォルト

snmp interface threshold コマンドを設定しない場合、デフォルトのしきい値はCPU使用率およびシステムメモリ使用率の70%です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

有効なしきい値の範囲は物理インターフェイスの30 ～ 99%です。**snmp interface threshold** コマンドを使用できるのは、管理コンテキストのみです。

例

次に、SNMPインターフェイスのしきい値をすべての物理インターフェイスの75%に設定する例を示します。

```
ciscoasa(config)# snmp interface threshold 75%
```

関連コマンド

コマンド	説明
snmp-server enable traps	SNMP-related トラップをイネーブルにします。

コマンド	説明
snmp cpu threshold rising	SNMP CPU しきい値を定義します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-map

SNMPインスペクションのパラメータを定義するための特定のマップを指定するには、グローバルコンフィギュレーションモードでsnmp-mapコマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map*map_name*
no snmp-map *map_name*

構文の説明

map_name	SNMPマップ名です。

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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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

snmp-map コマンドを使用して、SNMP インスペクションのパラメータを定義するために使用する特定のマップを指定します。このコマンドを入力すると、SNMPマップコンフィギュレーションモードが開始され、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップの定義後、inspect snmp コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、inspect コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
```

```
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

snmp-server community

SNMP コミュニティストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。SNMP コミュニティストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community［ **0 | 8** ］*community-string*
no snmp-server community［ **0 | 8** ］*community-string*

構文の説明

0	（任意）暗号化されていない（クリアテキストの）コミュニティストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community-string	SNMP コミュニティ ストリングを設定します。暗号化されたパスワード、または非暗号化（クリア テキスト）フォーマットのパスワードです。このコミュニティ ストリングは最大 32 文字です。 （注） コミュニティストリングでは特殊文字（!、@、#、$、%、^、&、*、\）を使用しないでください。一般に、オペレーティングシステムで使用される関数用に予約されている特殊文字を使用すると、予期しない結果が生じる可能性があります。たとえば、バックスラッシュ（\）はエスケープ文字と解釈されるため、コミュニティストリングでは使用できません。

コマンド デフォルト

デフォルトのコミュニティ ストリングは「public」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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	*text* 引数が *community-string* 引数に変更されました。

リリース	変更内容
8.3(1)	暗号化パスワ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

SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理されるネットワーク ノード間の共有秘密です。管理ステーションとデバイス間のバージョン 1 およびバージョン 2c の通信に対してのみ使用されます。ASA では、キーを使用して着信 SNMP 要求が有効かどうかを判別します。

コミュニティストリングでは特殊文字（!、@、#、$、%、^、&、*、\）を使用しないでください。一般に、オペレーティングシステムで使用される関数用に予約されている特殊文字を使用すると、予期しない結果が生じる可能性があります。たとえば、バックスラッシュ（\）はエスケープ文字と解釈されるため、コミュニティストリングでは使用できません。

たとえば、あるサイトにコミュニティストリングを指定し、さらに同じストリングを使用してルータ、ASA、管理ステーションを設定できます。ASAはこのストリングを使用し、無効なコミュニティストリングを持つ要求には応答しません。

暗号化されたコミュニティストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSMなど）に表示されます。クリアテキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常にASAによって生成されます。通常は、クリア テキストの形式で入力します。

（注） ASAソフトウェアをバージョン8.3(1)から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

例

次に、コミュニティ ストリングを「onceuponatime」に設定する例を示します。

```
ciscoasa(config)# snmp-server community onceuponatime
```

次の例では、暗号化されたコミュニティ ストリングを設定しています。

```
ciscoasa(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

次の例では、非暗号化コミュニティ ストリングを設定しています。

```
ciscoasa(config)# snmp-server community 0 cisco
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP カウンタをクリアします。

コマンド	説明
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server contact

SNMP サーバーのコンタクト名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。SNMP のコンタクト名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*
no snmp-server contact [*text*]

構文の説明

text	コンタクト担当者または ASA システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

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 コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP サーバーのコンタクトを EmployeeA に設定する例を示します。

```
ciscoasa(config)# snmp-server contact EmployeeA
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。

コマンド	説明
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server enable

ASA で SNMP サーバーを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP サーバーを無効にするには、このコマンドの **no** 形式を使用します。

snmp-server enable
no snmp-server enable

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

SNMP サーバーはイネーブルに設定されています。

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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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

SNMPトラップまたはその他のコンフィギュレーションを設定および再設定しなくても、SNMPを簡単にイネーブルおよびディセーブルにすることができます。

例

次の例では、SNMP をイネーブルにし、SNMP ホストとトラップを設定してから、syslog メッセージとしてトラップを送信しています。

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server enable oid

ASA が SNMP ウォーク操作を通じて空きメモリと使用メモリの統計をクエリできるようにするには、グローバル コンフィギュレーション モードで **snmp-server enable oid mempool** コマンドを使用します。メモリ統計情報のクエリ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。

snmp-server enable oid mempool
no snmp-server enable oid mempool

構文の説明

mempool SNMP ウォーク操作を実行するときに、空きメモリと使用済みメモリの統計をクエリします。

mempool クエリの排他 MIB オブジェクトには、次のものが含まれます。

- ciscoMemoryPoolUsed
- ciscoMemoryPoolFree
- cempMemPoolHCUsed
- cempMemPoolHCFree

コマンド デフォルト

デフォルトでは、MIB オブジェクトの SNMP ウォーク操作を可能にするために、**snmp-server enable oid mempool** は有効になっています。

このコマンドの **no** 形式を使用して、これらの MIB オブジェクトをディセーブルにすることができます。 **clear configure snmp-server** コマンドを使用すると、メモリのクエリ用の SNMP MIB オブジェクトがデフォルトの有効状態に戻ります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
9.10(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

SNMP ウォークの操作を実行すると、ASA は MEMPOOL_DMA プールと MEMPOOL_GLOBAL_SHARED プールからメモリ情報を照会します。ASA がメモリ情報を照会すると、CPU は他のプロセスに開放される前に SNMP プロセスによって長時間にわたり保持されることがあります。これにより、SNMP 関連の CPU ホグ状態になり、パケットがドロップされることがあります。

この問題を軽減するには、 **no snmp-server enable oid mempool** コマンドを使用して、グローバル共有プールに関連する OID をポーリングしないようにします。無効にすると、**mempool** OID は 0 バイトを返します。ただし、このコマンドに関係なく、そのプールに対する GET 要求を使用して明示的にクエリすることができます。

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server enable traps

ASA の NMS へのトラップ送信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 **snmp-server enable traps** コマンドを使用します。トラップ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。

snmp-server enable traps [**all | syslog | snmp** [*trap*] [….] [**cluster-state | failover-state | peer-flap**] [*trap*]] **| config | entity** [*trap*] [….] **| ipsec** [*trap*] [….] **| ikve2** [*trap*] [….] **| remote-access** [*trap*] **| connection-limit-reached | cpu threshold rising | link-threshold | memory-threshold | nat** [*trap*]

no snmp-server enable traps [**all | syslog | snmp** [*trap*] [….] [**cluster-state | failover-state | peer-flap**] [*trap*]] **| config | entity** [*trap*] [….] **| ipsec** [*trap*] [….] [*trap*] [….] **| remote-access** [*trap*] **| connection-limit-reached | cpu threshold rising | link-threshold | memory-threshold | nat** [*trap*]

構文の説明

all	すべてのトラップをイネーブルにします。
config	設定トラップをイネーブルにします。
connection-limit-reached	接続制限に達したトラップをイネーブルにします。
cpu threshold rising	CPU しきい値上限トラップをイネーブルにします。
cluster-state	クラスタ関連のトラップを有効にします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** トラップは次のとおりです。 • **accelerator-temperature** • **chassis-fan-failure** • **chassis-temperature** • **config-change** • **cpu-temperature** • **fan-failure** • **fru-insert** • **fru-remove** • **l1-bypass-status** • **power-supply** • **power-supply-failure** • **power-supply-presence** • **power-supply-temperature**

failover-state	フェールオーバー関連のトラップを有効にします。
ipsec [*trap*]	IPsec トラップをイネーブルにします。**ipsec** トラップは次のとおりです。 • **start** • **stop**
ikev2 [*trap*][ ]	IKEv2 IPsec トラップをイネーブルにします。**ikev2** トラップは次のとおりです。 • **start** • **stop**
link-threshold	リンクしきい値に達したトラップをイネーブルにします。
memory-threshold	メモリしきい値に達したトラップをイネーブルにします。
nat [*trap*]	NAT に関連するトラップをイネーブルにします。**nat** トラップは次のとおりです。 • **packet-discard**
peer-flap	BGP または OSPF ピアの MAC アドレスフラッピング関連のトラップを有効にします。
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。**remote-access** トラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップを有効にします。デフォルトでは、すべての SNMP トラップはイネーブルになっています。**snmp** トラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart** • warmstart
syslog	syslog メッセージ トラップをイネーブルにします。

コマンド デフォルト

デフォルトの設定では、次の **snmp** トラップがイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**）。このコマンドを入力し、トラップタイプを指定しない場合、デフォルトは **syslog** です（デフォルトの **snmp** トラップは **syslog** トラップ

とともに引き続きイネーブルのままです）。デフォルトでは他のトラップはすべてディセーブルです。

これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。 **clear configure snmp-server** コマンドを使用すると、SNMP トラップのデフォルトのイネーブル状態に戻ります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	**snmp warmstart**、**nat packet-discard**、**link-threshold**、**memory-threshold**、**entity power-supply**、**entity fan-failure**、**entity cpu-temperature**、**cpu threshold rising**、および **connection-limit-reached** トラップが追加されました。これらのトラップは、ASASM には適用されません。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために、**entity power-supply-failure**、**entity chassis-fan-failure**、**entity power-supply-presence**、**entity chassis-temperature**、および **entity power-supply-temperature** トラップが追加されました。
9.0(1)	IKEv2 および IPsec 用にマルチ コンテキスト モードのサポートが追加されました。
9.3(2)	**config** および **entity accelerator-temperature** トラップのサポートが追加されました。

使用上のガイドライン

個別のトラップまたはトラップのセットをイネーブルにするには、機能タイプごとにこのコマンドを入力します。すべてのトラップをイネーブルにするには、**all** キーワードを入力します。

NMS にトラップを送信するには、**logging history** コマンドを入力し、**logging enable** コマンドを使用してロギングをイネーブルにします。

管理コンテキストのみで生成されるトラップは、次のとおりです。

- **connection-limit-reached**
- **entity**

- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してのみ管理コンテキストを介して生成されるトラップは、次のとおりです。

- **interface-threshold**

その他すべてのトラップは、管理およびユーザー コンテキストで使用できます。

config トラップを指定すると、ciscoConfigManEvent 通知と ccmCLIRunningConfigChanged 通知がイネーブルになります。これらの通知は、コンフィギュレーション モードを終了した後に生成されます。

一部のトラップは、特定のハードウェア モデルに適用できません。トラップキーワードの代わりに ? を使用すると、デバイスで使用可能なトラップを確認できます。次に例を示します。

- **accelerator-temperature** しきい値トラップは、ASA 5506-X および ASA 5508-X にのみ適用されます。
- **chassis-fan-failure** トラップは、ASA 5506-X には適用されません。
- **fan-failure**、**fru-insert**、**fru-remove**、**power-supply**、**power-supply-presence**、および **power-supply-temperature** トラップは ASA 5506-X および ASA 5508-X には適用されません。
- Firepower 1000 シリーズ（1010 を除く）は、次のエンティティトラップのみをサポートします。**chassis-temperature**、**config-change**、および **cpu-temperature**。1010 は、次のトラップのみをサポートします。**config-change**、**fru-insert**、**fru-remove**。

マルチ コンテキスト モードのガイドライン

- マルチコンテキストモードでは、**fan-failure** トラップ、**power-supply-failure** トラップ、および **cpu-temperature** トラップは、ユーザーコンテキストではなく、管理コンテキストのみから生成されます。これらのトラップは、ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X にのみ適用され、ASA 5505 には適用されません。
- **snmp-server enable traps remote-access session-threshold-exceeded** コマンドはマルチコンテキストモードではサポートされません。

CPU使用率が、設定されたモニタリング期間の設定されたしきい値を超える場合、**cpu threshold rising** トラップが生成されます。

使用されたシステムメモリが 80% に達すると、**memory-threshold** トラップが生成されます。

（注） SNMP は電圧センサーをモニターしません。

例

次の例では、SNMP をイネーブルにし、SNMP ホストとトラップを設定してから、syslog メッセージとしてトラップを送信しています。

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server group

新しい SNMP グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP 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。

snmp-server group *group-name* { **v3** { **auth | noauth | priv** } }
no snmp-server group *group-name* { **v3** { **auth | noauth | priv** } }

構文の説明

auth	暗号化を使用しないパケット認証を指定します。
group-name	グループの名前を指定します。
noauth	パケット認証を指定しません。
priv	暗号化されたパケット認証を指定します。
v3	グループが SNMP バージョン 3 セキュリティ モデルを使用することを指定します。このセキュリティ モデルは、サポートされているものの中で最もセキュアです。このバージョンでは、認証特性を明示的に設定できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.3(1)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザーを設定した後、SNMP ホストを設定する必要があります。バージョン 3 およびセキュリティ レベルも指定する必要があります。コミュニティ ストリングが内部的に設定されている場合、「public」という名前の 2 つのグループが自動的に作成されます。1 つはバー

ジョン 1 セキュリティ モデル用、もう 1 つはバージョン 2c セキュリティ モデル用です。コミュニティ ストリングを削除すると、設定された両方のグループが自動的に削除されます。

（注） 特定のグループに属すように設定されるユーザーは、グループと同じセキュリティ モデルを持つ必要があります。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

（注） ASA ソフトウェアをバージョン 8.3(1) から下のバージョンにダウングレードし、暗号化されたパスワードを設定した場合、まず **no key config-key password encryption** コマンドを使用して暗号化されたパスワードをクリアテキストに戻してから結果を保存する必要があります。

例

次の例に、ASA が SNMP バージョン 3 セキュリティモデルを使用して SNMP 要求を受信する方法について示します。これには、グループ、ユーザー、ホストの作成が含まれます。

```
ciscoasa(config)#
snmp-server group
 vpn-group
 v3 priv
ciscoasa(config)# snmp-server
 user
 admin vpn-group
v3
 auth sha
 letmein
 priv
 3des
cisco123
ciscoasa(config)# snmp-server host
mgmt 10.0.0.1
version 3
admin
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server user	新しい SNMP ユーザーを作成します。

snmp-server host

ASA で SNMP を使用可能な NMS 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 **snmp-server host** コマンドを使用します。NMS 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。

snmp-server host { *interface* { *hostname* | *ip_address* } } [**trap | poll**] [**community** *0* | *8* *community-string*] [**version** { **1 | 2c | 3** *username* }] [**udp-port** *port*]

no snmp-server host { *interface* { *hostname* | *ip_address* } } [**trap | poll**] [**community** *0* | *8* *community-string*] [**version** { **1 | 2c | 3** *username* }] [**udp-port** *port*]

構文の説明

0	（任意）暗号化されていない（クリア テキストの）コミュニティ ストリングが続くことを指定します。
8	暗号化されたコミュニティ ストリングが続くことを指定します。
community	NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、または NMS からの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。暗号化フォーマットと非暗号化フォーマット（クリア テキスト）を使用できます。
hostname	SNMP 通知ホストを指定します。通常は NMS または SNMP マネージャです。
interface	NMS が ASA との通信に使用するインターフェイス名を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の送信元の NMS の IP アドレスを指定します。
trap | **poll**	（オプション）ホストでトラップの参照（ポーリング）または送信を許可するかどうかを指定します。何も指定されていない場合のデフォルトは **trap** です。同じホストに対して、トラップとポーリングの両方を有効にすることはできません。
udp-port *port*	（オプション）SNMP トラップがデフォルト以外のポートで NMS ホストに送信されるように指定し、NMS ホストの UDP ポート番号を設定します。
username	ホストに送信されるトラップ PDU に埋め込むユーザー名を指定します。SNMP バージョン 3 でのみ有効です。
version {**1** | **2c** | **3**}	（任意）トラップと要求（ポーリング）に使用される SNMP のバージョンを指定します。デフォルトは 1 です。

コマンド デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

SNMP トラップはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	• SNMP バージョン 3 がサポートされています。 • *username* 引数が追加されました。 • *text* 引数が *community-string* 引数に変更されました。 • *interface_name* 引数が *interface* 引数に変更されました。
8.3(1)	暗号化パスワードのサポートが追加されました。
9.7(1)	直接接続された SNMP 管理ステーションがある場合、ASA および SNMP サーバーの /31 サブネットを使用してポイントツーポイント接続を作成できます。
9.8(4)	SNMP のバージョンがトラップとポーリングの両方に適用されるようになりました。
9.9(2)	IPv6 のサポートが追加されました。

使用上のガイドライン

現在使用中のポートで **snmp-server host** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature.
SNMP requests to the device will fail until the snmp-server listen-port
command is configured to use a different port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

[**trap**|**poll**]のどちらも指定されていない場合、**trap**はです。このコマンドでは、同じホストに対して trap と polling の両方を有効にできないことに注意してください。

バージョン 3 セキュリティ モデルを使用するには、まず SNMP グループを設定してから、SNMP ユーザーを設定し、SNMP ホストを設定する必要があります。ユーザー名はデバイス上で設定済みである必要があります。デバイスがフェールオーバー ペアのスタンバイ ユニットとして設定される場合、SNMP エンジン ID とユーザー コンフィギュレーションはアクティブ ユニットから複製されます。このアクションによって、SNMP バージョン 3 クエリーの観点から、トランスペアレントなスイッチオーバーが可能になります。スイッチオーバーイベントに対応するために NMS でのコンフィギュレーション変更は必要ありません。

暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。

暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、ホストを内部インターフェイスに接続されている 192.0.2.5 に設定する例を示します。

```
ciscoasa(config)# snmp-server host inside 192.0.2.5
ciscoasa(config)# snmp-server host inside 192.0.2.5
 version 3 username user1 password cisco123 mschap md5aes128 udp-port 190
```

次に、ASA が SNMP バージョン 3 セキュリティモデルを使用して SNMP 要求を受信する例を示します。これには、グループ、ユーザー、ホストの作成が含まれます。

```
ciscoasa(config)# snmp-server group vpn-group v3 priv
ciscoasa(config)# snmp-server user admin vpn-group v3
auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3
username user1
```

次に、暗号化されたコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 8
LvAu+JdFG+GjPmZYlKvAhXpb28E= username user1 password cisco123 mschap
```

次に、暗号化されていないコミュニティ ストリングを使用するようにホストを設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 0
cisco username user1 password cisco123 mschap
```

次に、SNMP 通知バージョン 2c を使用して、ホストを IPv6 アドレス 12:ab:56:ce::11 に設定する例を示します。

```
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11
community public version 2c
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP コンフィギュレーション カウンタをクリアします。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを設定します。
snmp-server user	新しい SNMP ユーザーを設定します。

snmp-server host-group

ユーザーリストの1人のユーザーまたはユーザーグループをネットワークオブジェクトに関連付けるには、グローバル コンフィギュレーション モードで **snmp-server host-group** コマンドを使用します。関連付けを削除するには、このコマンドの **no** 形式を使用します。

snmp-server host-group *interface-network-object-name* [**trap | poll**] [**community** *community-string*] [**version** { **1 | 2c | 3** { *username* **| userlist** *list_name* } }] [**udp-port** *port*]

no snmp-server host-group *interface-network-object-name* [**trap | poll**] [**community** *community-string*] [**version** { **1 | 2c | 3** { *username* **| userlist** *list_name* } }] [**udp-port** *port*]

構文の説明

community	NMSからの要求に対して、またはNMSに送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。SNMP バージョン 1 または 2c でのみ有効です。
community-string	通知とともに、またはNMSからの要求内で送信される、パスワードに似たコミュニティ ストリングを指定します。このコミュニティ ストリングは最大 32 文字です。
interface-network-object-name	1 人のユーザーまたはユーザー グループを関連付けるインターフェイスのネットワーク オブジェクトの名前を指定します。
trap | **poll**	（オプション）ホストでトラップの参照（ポーリング）または送信を許可するかどうかを指定します。何も指定されていない場合のデフォルトは**poll**です。同じホストグループに対して、トラップとポーリングの両方を有効にすることはできません。
udp-port *port*	（オプション）SNMPトラップがデフォルト以外のポートでNMSホストに送信されるように指定し、NMS ホストの UDP ポート番号を設定します。
user-list *list_name*	ユーザー リストの名前を指定します。
username	ユーザーの名前を指定します。
version {**1** | **2c** | **3**}	（オプション）トラップの送信に使用するために、SNMP 通知バージョンをバージョン 1、2c、または 3 に設定します。

コマンド デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

SNMP ポーリングはデフォルトでイネーブルとなっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.17(1)	IPv6オブジェクトのサポートが追加されました。

使用上のガイドライン

最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト名または IP アドレスの範囲を使用してホストを定義できます。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザーを関連付けることができます。

[**trap** | **poll**] を指定していない場合のデフォルトは **poll** です。このコマンドでは、同じホストグループに対して trap と polling の両方を有効にできないことに注意してください。一部のホストがポーリング用に設定され、その他のホストがトラップ用に設定されている混合モニタリング環境では、**snmp-server host** コマンドを使用することを推奨します。**snmp-server host** コマンドでは、同じホスト ループに対して trap と polling の両方を有効にできないことに注意してください。デフォルトは **trap** です。

トラップの送信に SNMP 通知バージョン 1 または 2c を使用する場合、1 人のユーザーとネットワーク オブジェクトを関連付けることができます。トラップの送信に SNMP 通知バージョン 3 を使用する場合、1 人のユーザーまたはユーザー グループをネットワーク オブジェクトに関連付けることができます。ユーザーグループを作成するには、**snmp-server user-list** コマンドを使用します。ユーザーは、グループ設定に属する場合があります。

SNMP バージョン 3 を使用する場合、ユーザー名と SNMP ホストを関連付ける必要があります。

IPv4 と IPv6 をサポートします。

例

次に、SNMP 通知バージョン 1 を使用して 1 人のユーザーとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
```

次に、SNMP 通知バージョン 2c を使用して 1 人のユーザーとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

次に、SNMP 通知バージョン 3 を使用して 1 人のユーザーとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
```

次に、SNMP 通知バージョン 3 を使用してユーザー リストとネットワーク オブジェクトを関連付ける例を示します。

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

関連コマンド

コマンド	説明
clear configure snmp-server host-group	すべての SNMP ホスト グループ設定をクリアします。
show running-config snmp-server host-group	実行コンフィギュレーションから SNMP サーバー ホスト グループ設定をフィルタリングします。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server listen-port

SNMP 要求のリスニングポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルトのポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*
no snmp-server listen-port *lport*

構文の説明

lport	着信要求が受け入れられるポート。

コマンド デフォルト

デフォルト ポートは 161 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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応（管理コンテキストのみ）	—

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

マルチコンテキストモードでは、管理コンテキストでのみこのコマンドを使用できます。ポートはすべてのコンテキストに適用されます。コンテキストごとに異なるポートを使用することはできません。

現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature.
SNMP requests to the device will fail until the snmp-server listen-port
command is configured to use a different port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

例

次に、リスニング ポートを 192 に設定する例を示します。

```
ciscoasa(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。
snmp-server location	SNMP サーバーのロケーション文字列を設定します。

snmp-server location

SNMPのASAの場所を設定するには、グローバルコンフィギュレーションモードで**snmp-server location**コマンドを使用します。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。

snmp-server location *text*
no snmp-server location [*text*]

構文の説明

location *text*	セキュリティ アプライアンスの場所を指定します。**location** *text* は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

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 コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP の ASA の場所を Building 42、Sector 54 として設定する例を示します。

```
ciscoasa(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMPコミュニティストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップを有効にします。

コマンド	説明
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user

新しい SNMP ユーザーを設定するには、グローバル コンフィギュレーション モードで **snmp-server user** コマンドを使用します。指定した SNMP ユーザーを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** { **sha | sha224 | sha256 | sha384** } *auth_password* [**priv** { **3des | aes** { **128 | 192 | 256** } } *priv_password*]]
no snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** { **sha | sha224 | sha256 | sha384** } *auth_password* [**priv** { **3des | aes** { **128 | 192 | 256** } } *priv_password*]]

構文の説明

128	（任意）暗号化について 128 ビット AES アルゴリズムの使用を指定します。
192	（任意）暗号化について 192 ビット AES アルゴリズムの使用を指定します。
256	（任意）暗号化について 256 ビット AES アルゴリズムの使用を指定します。
3des	（任意）暗号化について 168 ビット 3DES アルゴリズムの使用を指定します。
aes	（任意）暗号化について AES アルゴリズムの使用を指定します。
auth	（任意）使用する認証レベルを指定します。
auth_password	（任意）エージェントがホストからパケットを受信できるようにするストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーン テキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
engineID	（オプション）ユーザーの認証と暗号化の情報をローカライズするために使用される ASA のエンジン ID を指定します。engineID 引数には、有効な ASA エンジン ID を指定する必要があります。
encrypted	（任意）パスワードが暗号化された形式で表示されるかどうかを指定します。暗号化されたパスワードは、16 進数の形式である必要があります。
group_name	ユーザーが属すグループの名前を指定します。
priv	暗号化されたパケット認証を指定します。

priv_password	（任意）プライバシー ユーザー パスワードを示すストリングを指定します。最小の長さは 1 文字、最低 8 文字で英文字と数字を含むものを推奨します。最大長は、64 文字です。プレーン テキストのパスワードか、ローカライズされた MD5 ダイジェストを指定できます。ローカライズされた MD5 または SHA ダイジェストを持っている場合は、プレーンテキストのパスワードではなく、その文字列を指定できます。ダイジェストは、aa:bb:cc:dd という形式であることが必要です（aa、bb、cc は 16 進数の値）。ダイジェストは正確に 16 個のオクテットであることが必要です。
sha	（任意）HMAC-SHA-96 認証レベルを指定します。
sha224	（任意）HMAC-SHA-224 認証レベルを指定します。
sha256	（任意）HMAC SHA-256 認証レベルを指定します。
sha384	（任意）HMAC SHA-384 認証レベルを指定します。
username	エージェントに接続するホストのユーザー名を指定します。
v3	SNMP バージョン 3 セキュリティ モデルを使用することを指定します。**encrypted, priv,** キーワードまたは **auth** キーワードの使用を許可します。

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 コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.14(1)	HMAC AES-256 認証レベルが追加されました。
9.16(1)	HMAC AES-224 認証レベルと AES-384 認証レベルが追加されました。 HMAC-MD5-96 認証レベルのサポートが削除されました。 56 ビット DES 暗号化アルゴリズムのサポートが削除されました。

使用上のガイドライン

SNMP ユーザーは、SNMP グループの一部である必要があります。バージョン 3 セキュリティ モデルを使用するには、まずSNMP グループを設定してから、SNMP ユーザーを設定した後、SNMP ホストを設定する必要があります。

（注） パスワードを忘れた場合は、回復できないため、ユーザーを再設定する必要があります。

snmp-server user のコンフィギュレーションがコンソールに表示されるか、ファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証およびプライバシー ダイジェストが常にプレーン テキストのパスワードの代わりに表示されます。この使用法は、RFC 3414、11.2 項によって要求されています。

（注） 3DES または AES アルゴリズムを使用してユーザーを設定するには、3DES または AES 機能のライセンスが必要です。

ASA の起動やアップグレードでは、単一の数字のパスワードや、数字で始まりその後にスペースが続くパスワードをサポートしなくなりました。たとえば、0 pass や 1 は不正なパスワードです。

クラスタリング環境では、クラスタ化されたそれぞれの ASA について手動で SNMPv3 ユーザーを更新する必要があります。これを行うには、マスターユニットに対する **snmp-server user** *username group-name* **v3** コマンドを入力し、ローカライズされていない形式で *priv-password* オプションおよび *auth-password* オプションを指定します。

クラスタリングの複製または設定時に、SNMPv3 ユーザー コマンドが複製されないことを通知するエラー メッセージが表示されます。この場合、SNMPv3 ユーザーおよびグループのコマンドをスレーブの ASA に対して個別に設定します。また、複製の実行時に既存の SNMPv3 ユーザーおよびグループのコマンドがクリアされない場合にもメッセージが表示されます。この場合は、クラスタのすべてのスレーブに対して SNMPv3 ユーザーおよびグループのコマンドを入力します。次に例を示します。

マスター ユニットに対するコマンドで入力したキーがすでにローカライズされている場合：

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

クラスタ複製時のスレーブユニットの場合（**snmp-server user** コマンドが設定にある場合にのみ表示されます）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

例

次に、ASA で SNMP バージョン 3 セキュリティモデルを使用して SNMP 要求を受信する例を示します。

```
ciscoasa(config)#
            snmp-server group

engineering


            v3
            auth
ciscoasa(config)# snmp-server
            user

engineering


            v3
            auth sha

mypassword
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバー コンフィギュレーションをクリアします。
snmp-server enable	ASA で SNMP をイネーブルにします。
snmp-server group	新しい SNMP グループを作成します。
snmp-server host	SNMP ホスト アドレスを設定します。

snmp-server user-list

指定されたユーザーグループを使用して SNMP ユーザーリストを設定するには、グローバル コンフィギュレーション モードで **snmp-server user-list** コマンドを使用します。指定した SNMP ユーザーリストを削除するには、このコマンドの **no** 形式を使用します。

snmp-server user-list *list_name* **username** *user_name*
no snmp-server user-list *list_name* **username** *user_name*

構文の説明

list_name	ユーザー リスト名（最長 33 文字）を指定します。
username *user_name*	ユーザー リストに設定できるユーザーを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

snmp-server user *username* コマンドを使用して、ユーザーリストのユーザーを設定します。ユーザー リストには複数のユーザーを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

例

次に、engineering という名前のユーザー リストのユーザー グループを作成する例を示します。

```
ciscoasa(config)#
snmp-server user-list
 engineering username
 user1
ciscoasa(config)# snmp-server
 user-list
 engineering username
```

```
 user2
ciscoasa(config)# snmp-server
 user-list
 engineering username
 user3
```

関連コマンド

コマンド	説明
show running-config snmp-server user-list	実行コンフィギュレーションからSNMPユーザー リストの設定をフィルタリングします。
clear snmp-server user-list	SNMP ユーザー リストの設定をクリアします。

sntp address

DHCPv6 サーバーを設定するときに、Simple Network Time Protocol（SNTP）サーバー IP アドレスをステートレスアドレス自動設定（SLAAC）クライアントに提供するには、ipv6 dhcp プール コンフィギュレーション モードで **sntp address** コマンドを使用します。SNTP サーバーを削除するには、このコマンドの **no** 形式を使用します。

sntp address *sntp_ipv6_address*
no sntp address *sntp_ipv6_address*

構文の説明

sntp_ipv6_address	SNTP サーバーの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

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

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

この機能は、クラスタリングではサポートされていません。

例

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

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sntp address 2001:DB8:1::5
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
sntp address 2001:DB8:1::5
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

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

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

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。