CHAPTER 15

shun コマンド～ sntp address コマンド

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。

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。

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。

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

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）

ローカル認証局（CA）サーバをディセーブルにし、ユーザ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 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。

デフォルト

最初は、CA サーバ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。

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

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 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 サーバをイネーブルにし、CA サーバ証明書とキー 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 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。

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。

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

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 コマンドに移されました。

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 サーバを設定するときに、Session Initiation Protocol（SIP）サーバ 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ipv6 dhcp pool configuration	• **Yes**	—	• **Yes**	—	—

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 サーバを含め、**ipv6 dhcp プール**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 サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**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 サーバを有効にします。
network	サーバ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。

コマンド	説明
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 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。

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

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 プール**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 サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**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 サーバを有効にします。
network	サーバ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。

コマンド	説明
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。
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。

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

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（クラスタ グループ）	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。
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（クラスタ グループ）	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。

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。

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。

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

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 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 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。

動作の現在のコンフィギュレーション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** 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。

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	• Yes	—	• Yes	—	—

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

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** *domain*] [port *port*] [realm *realm string*]

構文の説明

domain *domain*	（任意）。認証中にユーザ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。
realm	認証のレルムを設定します。

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。

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

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。

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s

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

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。
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。
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名に割り当てるときにドメイン名を指定してください。

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。

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

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。

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s

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 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、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access]> [Start Smart Tunnels] ボタンを使用して、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。

smart-tunnel auto-start

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。

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。

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

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

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s

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 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、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access]> [Start Smart Tunnels] ボタンを使用して、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。
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

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。

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。

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

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

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s

コマンド	説明
smart-tunnel auto-start	ユーザ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 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、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access]> [Start Smart Tunnels] ボタンを使用して、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。
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

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。

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。

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

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

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名に割り当てられます。ユーザは、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、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s

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

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** または **mac** を入力して、アプリケーションのホストを指定します。

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。

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

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。

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 プロファイルが必要です。このユーザ 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 サーバと通信します。
- グループ ポリシーまたはローカル ユーザ 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** 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 enable	ユーザ 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、ユーザがクライアントレス SSL VPN ポータル ページの [Application Access]> [Start Smart Tunnels] ボタンを使用して、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。

smart-tunnel network

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。

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。

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

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

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に強制適用します。

smart-tunnel tunnel-policy

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 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。

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。

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

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

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** コマンドの使用方法の例を示します。

```
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 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。

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。

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

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 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 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。

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。

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

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 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。

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。

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

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（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。

SMTP サーバを設定するには、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_server*} [*backup_server*]

no smtp-server

構文の説明

backup_server	プライマリ SMTP サーバ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_server	プライマリ SMTP サーバを指定します。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。

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。

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

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

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。

例

次に、SMTP サーバを 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
```

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。

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。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。

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

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 Services Module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。

コマンド	説明
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 サーバのロケーション文字列を設定します。

snmp link 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 link 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 link threshold *threshold_value*

no snmp link 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。

デフォルト

snmp link 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。

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

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 link threshold** コマンドは、管理コンテキストでのみ使用できます。

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 link 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。
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。

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。

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。

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

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。

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。

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

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。
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。

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。
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 サーバのロケーション文字列を設定します。

snmp-server contact

SNMP サーバ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。

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。

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

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。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバ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** コマンドを使用します。SNMP サーバ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

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。

デフォルト

SNMP サーバ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。

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

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*] [...]| **config** | **entity** [*trap*] [...]| **ipsec** [*trap*] [...]| **ikev2** [*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*] [...]| **config** | **entity** [*trap*] [...]| **ipsec** [*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。
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**
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**
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。

デフォルト

デフォルトのコンフィギュレーションでは、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。

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

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)	次のトラップが追加されました。**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**。これらのトラップは ASASMには適用されません。

リリース	変更内容
8.6(1)	ASA5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために次のトラップが追加されました。**entity power-supply-failure**、**entity chassis-fan-failure**、**entity power-supply-presence**、**entity chassis-temperature**、および **entity power-supply-temperature**。
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)	次のトラップのサポートが追加されました。**config** および **entity accelerator-temperature**。

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 コンテキストで使用できます。

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。

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。

次のトラップは ASA 5506-X および ASA 5508-X には適用されません。**fan-failure**、**fru-insert**、**fru-remove**、**power-supply**、**power-supply-failure**、**power-supply-presence**、および **power-supply-temperature**。

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 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、ASA5512-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。

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。

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

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、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。IPv4 アドレスのみをサポートしています。
poll	(任意)ホストはブラウズ(ポーリング)は可能だが、トラップは送信されないことを指定します。
port	NMS ホストの UDP ポート番号を設定します。
trap	(任意)トラップの送信のみが可能であり、このホストはブラウズ(ポーリング)できないことを指定します。
udp-port	(任意)SNMP トラップはデフォルト以外のポートで NMS ホストに送信される必要があることを指定します。
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**}	(オプション)SNMP トラップ バージョンを指定します。ASAでは、SNMP 要求(ポーリング)に基づくフィルタリングはサポートされません。

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	• Yes	• Yes	• Yes	• Yes	—

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。

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。

警告 **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。

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 ユーザを設定し、SNMP ホストを設定する必要があります。ユーザ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 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。

（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、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、ホストの作成が含まれます。

```
ciscoasa(config)# snmp-server group v3 vpn-group 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 password
cisco123 mschap priv admin
```

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
```

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 ユーザを設定します。

snmp-server host-group

ユーザ リストの 1 人のユーザまたはユーザ 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。アソシエーションを削除するには、このコマンドの **no** 形式を使用します。

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

no snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *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 人のユーザまたはユーザ 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。
poll	(任意)ホストはブラウズ(ポーリング)は可能だが、トラップは送信されないことを指定します。
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 リストの名前を指定します。
username	ユーザ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。

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。

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

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

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 1 または 2c を使用する場合、1 人のユーザとネットワーク 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 人のユーザまたはユーザ 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 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、ユーザ名と SNMP ホストを関連付ける必要があります。

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 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 ホスト グループ設定をフィルタリングします。

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[1]。

1. **snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。

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。

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

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

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。

警告 **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。

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。

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

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。
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 {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [**engineID** *engineID*] [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **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。
des	(任意)暗号化について 56 ビット DES アルゴリズムの使用を指定します。
engineID	(オプション)ユーザ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	ユーザが属すグループの名前を指定します。
md5	(任意)HMAC-MD5-96 認証レベルを指定します。
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 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。
username	エージェントに接続するホストのユーザ名を指定します。
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**、または **auth** キーワードの使用を許可します。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表に、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	• Yes	• Yes	• Yes	• Yes	—

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。

使用上のガイドライン　SNMP ユーザは、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 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 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 グループを使用して SNMP ユーザ 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 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 リスト名（最長 33 文字）を指定します。
username *user_name*	ユーザ リストに設定できるユーザを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 リストのユーザを設定します。ユーザ リストには複数のユーザ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 リストのユーザ 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 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 リストの設定をクリアします。

sntp address

DHCPv6 サーバを設定するときに、Simple Network Time Protocol（SNTP）サーバ 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。

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

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 サーバを含め、**ipv6 dhcp プール**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 サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**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 サーバを有効にします。
network	サーバ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。

コマンド	説明
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。