CHAPTER 2

aaa accounting コマンド～ accounting-server-group コマンド

aaa accounting command

CLI で **show** コマンド以外のコマンドを入力したときに TACACS+ アカウンティング サーバにアカウンティング メッセージを送信するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを入力します。コマンド アカウンティングのサポート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。

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

構文の説明

tacacs+-server-tag	**aaa-server protocol** コマンドで指定するように、アカウンティング レコードの送信先の TACACS+ サーバまたはサーバのグループを指定します。
privilege *level*	**privilege** コマンドを使用してコマンドの特権レベルをカスタマイズする場合、最小特権レベルを指定することによって、セキュリティ アプライアンスで処理の対象とするコマンドを制限できます。最小特権レベルよりも下のコマンドは、セキュリティ アプライアンスで処理の対象となりません。 **（注）** 廃止されたコマンドを入力して **privilege** キーワードをイネーブルにした場合、廃止されたコマンドのアカウンティング情報はセキュリティ アプライアンスによって送信されません。廃止されたコマンドを処理の対象とするには、**privilege** キーワードをディセーブルにします。CLI では数多くの廃止されたコマンドがまだ受け入れられています。これらのコマンドは、現在受け入れられるコマンドに CLI で変換される場合もあります。廃止されたコマンドは、CLI のヘルプまたはこのマニュアルには記載されていません。

デフォルト

デフォルトの特権レベルは 0 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

aaa accounting command コマンドを設定すると、管理者が入力する **show** コマンド以外の各コマンドが記録され、アカウンティング サーバに送信されます。

例

次に、サポート対象のコマンドについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のグループからサーバに送信されることを指定する例を示します。

```
hostname(config)# aaa accounting command adminserver
```

関連コマンド

コマンド	説明
aaa accounting	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting console

管理者アクセスの AAA アカウンティングのサポート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 **aaa accounting console** コマンドを使用します。管理者アクセスの AAA アカウンティングのサポート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。

aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

no aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

構文の説明

enable	特権 EXEC モードの開始と終了を示すアカウンティング レコードの生成をイネーブルにします。
serial	シリアル コンソール インターフェイスを介して確立される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
server-tag	**aaa-server protocol** コマンドで定義された、アカウンティング レコードの送信先のサーバ グループを指定します。有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。
ssh	SSH で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
telnet	Telnet で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

aaa-server コマンドで指定済みのサーバ グループの名前を指定する必要があります。

例

次に、イネーブル アクセスについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のサーバに送信されることを指定する例を示します。

```
hostname(config)# aaa accounting enable console adminserver
```

関連コマンド

コマンド	説明
aaa accounting match	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
aaa accounting command	管理者 / ユーザが入力する各コマンド（または、指定した特権レベル以上のコマンド）が記録され、アカウンティング サーバに送信されることを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting include, exclude

セキュリティ アプライアンスを介した TCP または UDP 接続のアカウンティング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 **aaa accounting include** コマンドを使用します。アカウンティングからアドレスを除外するには、**aaa accounting exclude** コマンドを使用します。アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスをアカウンティングから除外します。
include	アカウンティングが必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server host** コマンドで定義した AAA サーバ グループを指定します。
service	アカウンティングが必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port* • **udp**/*port*

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

アクセス リストで指定されているトラフィックのアカウンティングをイネーブルにするには、**aaa accounting match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa accounting include** および **exclude** コマンドを使用することはできません。その場合は、**aaa accounting match** コマンドを使用する必要があります。

例

次に、すべての TCP 接続でアカウンティングをイネーブルにする例を示します。

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

関連コマンド

コマンド	説明
aaa accounting match	アクセス リストで指定されているトラフィックのアカウンティングをイネーブルにします。
aaa accounting command	管理者アクセスのアカウンティングをイネーブルにします。
aaa-server host	AAA サーバを設定します。
clear configure aaa	AAA コンフィギュレーションをクリアします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting match

セキュリティ アプライアンス を介した TCP および UDP 接続のアカウンティング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 **aaa accounting match** コマンドを使用します。トラフィックのアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

構文の説明

acl_name	**access-list** 名との照合によるアカウンティングが必要なトラフィックを指定します。アクセス リスト内の permit エントリはアカウンティングの対象となり、deny エントリはアカウンティングから免除されます。このコマンドは、TCP トラフィックおよび UDP トラフィックについてのみサポートされます。このコマンドを入力し、他のプロトコルを許可するアクセス リストをこのコマンドが参照している場合、警告メッセージが表示されます。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、セキュリティ アプライアンスを通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

AAA サーバ プロトコル コンフィギュレーション モードで **accounting-mode** コマンドを使用して同時アカウンティングをイネーブルにしない限り、アカウンティング情報はサーバ グループ内のアクティブなサーバにのみ送信されます。

aaa accounting match コマンドは、**aaa accounting include** および **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

例

次に、特定のアクセス リスト acl2 と一致するトラフィックのアカウンティングをイネーブルにする例を示します。

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

関連コマンド

コマンド	説明
aaa accounting include、exclude	コマンドで IP アドレスを直接指定することによって、アカウンティングをイネーブルにします。
access-list extended	アクセス リストを作成します。
clear configure aaa	AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication console

シリアル、SSH、HTTPS（ASDM）、または Telnet 接続でセキュリティ アプライアンス CLI にアクセスするユーザを認証するか、**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証するには、グローバル コンフィギュレーション モードで **aaa authentication console** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

構文の説明

enable	**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証します。
http	HTTPS でセキュリティ アプライアンスにアクセスする ASDM ユーザを認証します。RADIUS サーバまたは TACACS+ サーバを使用する場合、設定する必要があるのは HTTPS 認証のみです。デフォルトでは、このコマンドを設定しなくても、ASDM によってローカル データベースが認証に使用されます。

LOCAL	認証にローカル データベースを使用します。**LOCAL** の文字は大文字と小文字が区別されます。ローカル データベースが空の場合、次の警告メッセージが表示されます。
	`Warning:local database is empty! Use 'username' command to define local users.`
	コンフィギュレーション内にまだ **LOCAL** があるときにローカル データベースが空になった場合、次の警告メッセージが表示されます。
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。HTTPS 管理認証では AAA サーバ グループ用に SDI プロトコルがサポートされません。 *server-tag* に加えて **LOCAL** キーワードを使用すると、AAA サーバを使用できない場合にフォールバック方式としてローカル データベースを使用するようにセキュリティ アプライアンスを設定できます。**LOCAL** の文字は大文字と小文字が区別されます。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、セキュリティ アプライアンスのプロンプトでは、いずれの方式が使用されているかが示されないためです。
serial	シリアル コンソール ポートを使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
ssh	SSH を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。
telnet	Telnet を使用してセキュリティ アプライアンスにアクセスするユーザを認証します。

デフォルト

デフォルトでは、ローカル データベースへのフォールバックはディセーブルになっています。

aaa authentication telnet console コマンドが定義されていない場合は、セキュリティ アプライアンスのログイン パスワード（**password** コマンドで設定）で、セキュリティ アプライアンス CLI にアクセスできます。

aaa authentication http console コマンドが定義されていない場合は、ユーザ名およびセキュリティ アプライアンスのイネーブル パスワード（**enable password** コマンドで設定）なしで、セキュリティ アプライアンスに（ASDM 経由で）アクセスできます。**aaa** コマンドが定義されているが、HTTPS 認証によってタイムアウトが要求される場合（AAA サーバがダウンしているか使用できないことを意味する）は、デフォルトの管理者ユーザ名とイネーブル パスワードを使用してセキュリティ アプライアンスにアクセスできます。デフォルトでは、イネーブル パスワードは設定されていません。

aaa authentication ssh console コマンドが定義されていない場合、ユーザ名 **pix** とセキュリティ アプライアンスのイネーブル パスワード（**enable password** コマンドで設定）を使用してセキュリティ アプライアンス CLI にアクセスできます。デフォルトでは、イネーブル パスワードは空白です。この動作は、AAA を設定しないでセキュリティ アプライアンスにログインする場合とは異なります。その場合は、ログイン パスワード（**password** コマンドで設定）を使用します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスで Telnet ユーザまたは SSH ユーザを認証する前に、**telnet** コマンドまたは **ssh** コマンドを使用してセキュリティ アプライアンスへのアクセスを設定する必要があります。これらのコマンドでは、セキュリティ アプライアンスとの通信を許可する IP アドレスを指定します。

セキュリティ アプライアンスへのログイン

セキュリティ アプライアンスに接続した後、ログインしてユーザ EXEC モードにアクセスします。

- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。SSH の場合、ユーザ名に「pix」と入力し、ログイン パスワードを入力します。
- このコマンドを使用して Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。

特権 EXEC モードへのアクセス

特権 EXEC モードを開始するには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースのみを使用している場合）。

- enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- enable 認証を設定している場合、セキュリティ アプライアンスによってユーザ名とパスワードの入力が求められます。

ローカル データベースを使用する認証の場合、**login** コマンドを使用できます。このコマンドでは、ユーザ名は維持されますが、認証をオンにするコンフィギュレーションは必要ありません。

ASDM へのアクセス

デフォルトでは、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワードを使用して ASDM にログインできます。ただし、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされます。

このコマンドを使用して HTTPS 認証を設定し、ローカル データベースを指定できますが、その機能はデフォルトで常にイネーブルです。AAA サーバを認証に使用する場合、設定する必要があるのは HTTPS 認証のみです。HTTPS 認証では AAA サーバ グループ用の SDI プロトコルがサポートされません。HTTPS 認証のユーザ名プロンプトの最大長は 30 文字です。パスワードの最大長は 16 文字です。

システム実行スペースでの AAA コマンドのサポートなし

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。

許可されるログイン試行の回数

次の表に示すように、**aaa authentication console** コマンドで選択するオプションによって、セキュリティ アプライアンス CLI への認証されたアクセスに対するプロンプトのアクションは異なります。

オプション	許可されるログイン試行の回数
enable	3 回失敗するとアクセスが拒否される。
serial	成功するまで何回も試行できる。
ssh	3 回失敗するとアクセスが拒否される。
telnet	成功するまで何回も試行できる。
http	成功するまで何回も試行できる。

ユーザ CLI および ASDM アクセスの制限

aaa authorization exec authentication-server コマンドを使用して管理認可を設定し、ローカル ユーザ、RADIUS、TACACS+、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を、CLI、ASDM、または **enable** コマンドへのアクセスを制限できます。

（注） シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** を設定している場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- RADIUS または LDAP（マッピングされた）ユーザ：次の値のいずれかについて、Service-Type 属性を設定します （LDAP 属性をマッピングするには、**ldap attribute-map** コマンドを参照してください）。
  - Service-Type 6（管理）：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）：**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - Service-Type 5（発信）：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPSec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。
- TACACS+ ユーザ：「service=shell」で認可が要求され、サーバは PASS または FAIL で応答します。
  - PASS、特権レベル 1：**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - PASS、特権レベル 2 以上：**aaa authentication** {**telnet | ssh**} **console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL：管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。
- ローカル ユーザ：**service-type** コマンドを設定します。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で、**aaa authentication console** コマンドを使用する例を示します。

```
hostname(config)# aaa authentication telnet console radius
```

次に、サーバ グループ「AuthIn」をイネーブル認証用に指定する例を示します。

```
hostname(config)# aaa authentication enable console AuthIn
```

次に、**aaa authentication console** コマンドを使用して、グループ「svrgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックさせる例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザ認証に使用する AAA サーバを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。

ldap map-attributes	LDAP 属性を、セキュリティ アプライアンスで認識できる RADIUS 属性にマッピングします。
service-type	ローカル ユーザの CLI アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication include, exclude

セキュリティ アプライアンスを経由する接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication include** コマンドを使用します。認証からアドレスを除外するには、**aaa authentication exclude** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを認証から除外します。
include	認証が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認証が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[**-***port*] • **udp**/*port*[**-***port*] • **icmp**/*type* • *protocol*[/*port*[**-***port*]] プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。詳細については、「使用上のガイドライン」を参照してください。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

アクセス リストで指定されているトラフィックの認証をイネーブルにするには、**aaa authentication match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authentication include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authentication match** コマンドを使用する必要があります。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については **timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」ストリングをキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- ポート 443 は HTTPS 用

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、セキュリティ アプライアンスにより元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（注）　**aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信して、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL でセキュリティ アプライアンスの直接認証を受けることができます。

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを表示します。

例

次に、外部インターフェイスで TCP トラフィックを認証に含める例を示します。内部 IP アドレス 192.168.0.0 およびネットマスク 255.255.0.0、すべてのホストの外部 IP アドレスを指定し、tacacs+ という名前のサーバ グループを使用します。2 番めのコマンドラインでは、外部インターフェイスで Telnet トラフィックを除外します。内部アドレス 192.168.38.0、すべてのホストの外部 IP アドレスを指定します。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

次に、*interface-name* パラメータの使用方法を示す例を示します。セキュリティ アプライアンスには、内部ネットワーク 192.168.1.0、外部ネットワーク 209.165.201.0（サブネット マスク 255.255.255.224）、および境界ネットワーク 209.165.202.128（サブネット マスク 255.255.255.224）があります。

次の例では、内部ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、内部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから内部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、境界ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

関連コマンド

コマンド	説明
aaa authentication console	管理アクセスの認証をイネーブルにします。
aaa authentication match	通過トラフィックのユーザ認証をイネーブルにします。
aaa authentication secure-http-client	HTTP 要求がセキュリティ アプライアンスを通過するのを許可する前に、セキュリティ アプライアンスに対してセキュアなユーザ認証方式を提供します。
aaa-server	グループ関連のサーバ属性を設定します。
aaa-server host	ホスト関連の属性を設定します。

aaa authentication listener

HTTP(S) リスニング ポートでネットワーク ユーザを認証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 **aaa authentication listener** コマンドを使用します。リスニング ポートをイネーブルにすると、セキュリティ アプライアンスでは直接接続に対して、およびオプションで通過トラフィックに対して認証ページを提供します。リスナー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。

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

構文の説明

http[s]	リッスンするプロトコル（HTTP または HTTPS）を指定します。このコマンドは、プロトコルごとに別々に入力します。
interface_name	リスナーをイネーブルにするインターフェイスを指定します。
port *portnum*	セキュリティ アプライアンスで直接トラフィックまたはリダイレクトされたトラフィックをリッスンするポート番号を指定します。デフォルトは 80（HTTP）および 443（HTTPS）です。任意のポート番号を使用して同じ機能を保持できますが、直接認証ユーザがそのポート番号を認識している必要があります。これは、リダイレクトされたトラフィックは正しいポート番号に自動的に送信されますが、直接認証するユーザは、ポート番号を手動で指定する必要があるためです。
redirect	セキュリティ アプライアンスによって提供される認証 Web ページに通過トラフィックをリダイレクトします。このキーワードを指定しないと、セキュリティ アプライアンス インターフェイスへのトラフィックだけが認証 Web ページにアクセスできます。

デフォルト

デフォルトでは、リスナー サービスはディセーブルであり、HTTP 接続では基本 HTTP 認証が使用されます。リスナーをイネーブルにした場合、デフォルトのポートは 80（HTTP）および 443（HTTPS）です。

7.2(1) からアップグレードする場合、リスナーはポート 1080（HTTP）および 1443（HTTPS）でイネーブルになります。**redirect** オプションもイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

aaa authentication listener コマンドを使用しないと、**aaa authentication match** または **aaa authentication include** コマンドの設定後に HTTP(S) ユーザがセキュリティ アプライアンスで認証する必要があるときに、セキュリティ アプライアンスでは基本 HTTP 認証が使用されます。HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードを指定して設定すると、セキュリティ アプライアンスにより、すべての HTTP(S) 認証要求はセキュリティ アプライアンスによって提供される Web ページにリダイレクトされます。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

aaa authentication listener コマンドを **redirect** オプションを*指定しない*で入力した場合、セキュリティ アプライアンスでの直接認証のみがイネーブルとなり、通過トラフィックでは基本 HTTP 認証が使用されます。**redirect** オプションによって、直接認証と通過トラフィック認証の両方がイネーブルになります。直接認証は、認証チャレンジをサポートしないトラフィック タイプを認証するときに役立ちます。他のサービスを使用する前に、各ユーザをセキュリティ アプライアンスで直接認証できます。

（注） **redirect** オプションをイネーブルにした場合、インターフェイスの IP アドレスを変換する同じインターフェイス、およびリスナー用に使用される同じポートに対して、スタティック PAT も設定することはできません。NAT は成功しますが、認証は失敗します。たとえば、次のコンフィギュレーションはサポートされません。

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside redirect
```

次のコンフィギュレーションはサポートされます。リスナーによって、ポートはデフォルトの 80 ではなく 1080 が使用されます。

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside port 1080 redirect
```

例

次に、HTTP および HTTPS 接続をデフォルトのポートにリダイレクトするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

次に、セキュリティ アプライアンスへの直接認証要求を許可する例を示します。通過トラフィックによって基本 HTTP 認証が使用されます。

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

次に、HTTP および HTTPS 接続をデフォルト以外のポートにリダイレクトするようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

関連コマンド

コマンド	説明
aaa authentication match	通過トラフィックのユーザ認証を設定します。
aaa authentication secure-http-client	SSL をイネーブルにし、HTTP クライアントとセキュリティ アプライアンスの間のユーザ名とパスワードのセキュアな交換をイネーブルにします。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。
virtual http	基本 HTTP 認証による HTTP 認証のカスケードをサポートします。

aaa authentication match

セキュリティ アプライアンス を通じた接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication match** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

構文の説明

acl_name	拡張アクセス リストの名前を指定します。
interface_name	ユーザを認証するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authentication match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については **timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」ストリングをキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- HTTPS の場合はポート 443（**aaa authentication listener** コマンドが必要）

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。

HTTP の場合、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、セキュリティ アプライアンスはカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、セキュリティ アプライアンスにより元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（注） **aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。セキュリティ アプライアンスは、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信して、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL でセキュリティ アプライアンスの直接認証を受けることができます。

http://*interface_ip*[:*port*]**/netaccess/connstatus.html**
https://*interface_ip*[:*port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを表示します。

例

次に、**aaa authentication match** コマンドを使用する例を示します。

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

このコンテキストでは、次のコマンドは

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

次のコマンドと同じです。

```
hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa コマンド ステートメントのリストでは、**access-list** コマンド ステートメント間の順序に依存します。たとえば、次のコマンドを入力します。

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

その後で、次のコマンドを入力します。

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

セキュリティ アプライアンスは、まず **mylist** 内の **access-list** コマンド ステートメント グループに一致があるか確かめ、次に **yourlist** 内の **access-list** コマンド ステートメント グループに一致があるかを確かめます。

関連コマンド

コマンド	説明
aaa authorization	ユーザ認可サービスをイネーブルにします。
access-list extended	アクセス リストを作成します。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication secure-http-client

SSL をイネーブルにし、HTTP クライアントとセキュリティ アプライアンスの間のユーザ名とパスワードのセキュアな交換をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication secure-http-client** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**aaa authentication secure-http-client** コマンドによって、ユーザの HTTP ベース Web 要求がセキュリティ アプライアンスを通過するのを許可する前に、セキュリティ アプライアンスに対するセキュアなユーザ認証方式が提供されます。

aaa authentication secure-http-client

no aaa authentication secure-http-client

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authentication secure-http-client コマンドによって、（SSL を介して）HTTP クライアント認証が保護されます。このコマンドは、HTTP カットスルー プロキシ認証用に使用されます。

aaa authentication secure-http-client コマンドには、次の制限があります。

- 実行時に、最大で 16 個の HTTPS 認証プロセスが許可されます。16 個の HTTPS 認証プロセスすべてが実行されている場合、認証を必要とする 17 番めの新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されると（**uauth timeout** が 0 に設定される）、HTTPS 認証は機能しない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この状況を回避するには、**timeout uauth 0:0:1** コマンドで **uauth timeout** を 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。
- HTTPS 認証は SSL ポート 443 で行われるため、HTTP クライアントから HTTP サーバ ポート 443 へのトラフィックをブロックするように、**access-list** コマンド ステートメントを設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、

SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、最初の行でスタティック PAT が Web トラフィックに対して設定されるため、HTTPS 認証コンフィギュレーションをサポートするために 2 番めの行を追加する必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

例

次に、HTTP トラフィックがセキュアに認証されるように設定する例を示します。

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

「...」は、*authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag* の値を表します。

次に、HTTPS トラフィックがセキュアに認証されるように設定するコマンドを示します。

```
hostname (config)# aaa authentication include https...
```

「...」は、*authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* の値を表します。

（注） **aaa authentication secure-https-client** コマンドは、HTTPS トラフィックには必要ありません。

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブルにします。
virtual telnet	セキュリティ アプライアンス仮想サーバにアクセスします。

aaa authorization command

aaa authorization command コマンドでは、CLI でのコマンド実行が認可の対象かどうかを指定します。コマンド認可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 **aaa authorization command** コマンドを使用します。コマンド認可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。

aaa authorization command {LOCAL | *tacacs+ server_tag* **[LOCAL]}**

no aaa authorization command {**LOCAL |** *tacacs+ server_tag* **[LOCAL]}**

構文の説明

LOCAL	**privilege** コマンドによって設定されるローカル コマンド特権レベルをイネーブルにします。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、セキュリティ アプライアンスはそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。 TACACS+ サーバ グループ タグの後に **LOCAL** を指定した場合、TACACS+ サーバ グループが使用できないときにフォールバックとしてのみ、ローカル ユーザ データベースがコマンド認可に使用されます。
tacacs+ server_tag	TACACS+ 認可サーバの定義済みのサーバ グループ タグを指定します。**aaa-server** コマンドで定義した AAA サーバ グループ タグです。

デフォルト

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	TACACS+ サーバ グループが一時的に使用できないときの LOCAL 認可へのフォールバックのサポートが追加されました。
8.0(2)	RADIUS サーバまたは LDAP サーバで定義される特権レベルのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセ

スできます。コマンドへのアクセスを制御する場合には、セキュリティ アプライアンス にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：セキュリティ アプライアンスでコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、セキュリティ アプライアンスはそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザが存在しなくても、また CLI 認証や enable 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、セキュリティ アプライアンスによってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、セキュリティ アプライアンスによってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド認可をオンにしない限り使用されません （詳細については、**enable** コマンドを参照してください）。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバでチェックされます。

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。これにより、異なるセキュリティ コンテキストに対して異なるコマンド認可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの認可が前のコンテキスト セッションでのユーザの認可と異なる場合に、混乱が生じる可能性があります。

  これは、発行される各コマンドを特定の管理者に正確に関連付けることができる場合に限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドの使用が許可されているすべての管理者は enable_15 ユーザ名を他のコンテキストで使用できるため、enable_15 ユーザ名でログインしたユーザをコマンド アカウンティング レコードで簡単に特定できるとは限りません。コンテキストごとに異なるアカウンティング サーバを使用する場合は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

コマンド許可を設定する場合は、次の点を考慮します。

- **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
- コンテキストごとに別々にコマンドを認可する場合は、**changeto** コマンドの使用許可を持つ管理者に対しても拒否されるコマンドが enable_15 ユーザ名でも拒否されることを、各コンテキストで確認してください。

セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

（注） システム実行スペースでは **aaa** コマンドはサポートされません。したがって、システム実行スペースではコマンド認可は使用できません。

ローカル コマンド認可の前提条件

- **aaa authentication enable console** コマンドを使用して、ローカル、RADIUS、または LDAP 認証の enable 認証を設定します。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を維持するために必要です。

  または、コンフィギュレーションが不要な **login** コマンド（認証を伴う **enable** コマンドと同じ）を使用できます。enable 認証ほどセキュアではないため、このオプションは推奨しません。

  CLI 認証（**aaa authentication** {**ssh** | **telnet** | **serial**} **console**）を使用することもできますが、必須ではありません。

- RADIUS が認証に使用されている場合、**aaa authorization exec authentication-server** コマンドを使用して、RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにすることができますが、必須ではありません。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可もイネーブルにします。このコマンドを使用すると、ローカル コマンド許可に影響するかも知れません。**authentication-server** キーワードを使用すると、ユーザの認証に使用されたサーバから特権レベルを取得するデフォルトの動作を維持します（LDAP（マッピング済み）、LOCAL および RADIUS サーバに適用されます）。ただし、このオプションは、TACACS+ サーバからのユーザ特権レベルの取得をイネーブルにします。
- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：**username** コマンドを使用して、ローカル データベース内のユーザを特権レベル 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。
- コマンド特権レベルの設定については、**privilege** コマンドを参照してください。

TACACS+ コマンド認可

TACACS+ コマンド認可をイネーブルにし、ユーザが CLI でコマンドを入力する場合、セキュリティ アプライアンスによってコマンドとユーザ名が TACACS+ サーバに送信され、コマンドが認可されているかどうかが判別されます。

TACACS+ サーバによるコマンド認可を設定するときは、意図したとおりに機能することが確認できるまで、コンフィギュレーションを保存しないでください。間違いによりロック アウトされた場合、通常はセキュリティ アプライアンスを再起動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムとセキュリティ アプライアンスへの完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合、ローカル ユーザおよびコマンド特権レベルを設定する必要があります。

TACACS+ サーバの設定については、『*Cisco ASA 5500 Series Command Line Configuration Guide*』を参照してください。

TACACS+ コマンド認可の前提条件

- **aaa authentication** {**ssh** | **telnet** | **serial**} **console** コマンドを使用して、CLI 認証を設定します。
- **aaa authentication enable console** コマンドを使用して、**enable** 認証を設定します。

例

次に、tplus1 という名前の TACACS+ サーバ グループを使用してコマンド認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization command tplus1
```

次に、tplus1 サーバ グループ内のすべてのサーバが使用できない場合に、ローカル ユーザ データベースへのフォールバックをサポートする管理認可を設定する例を示します。

```
hostname(config)# aaa authorization command tplus1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	CLI、ASDM、および enable 認証をイネーブルにします。
aaa authorization exec authentication-server	RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにします。
aaa-server host	ホスト関連の属性を設定します。
aaa-server	グループ関連のサーバ属性を設定します。
enable	特権 EXEC モードを開始します。
ldap map-attributes	LDAP 属性を、セキュリティ アプライアンスで使用できる RADIUS 属性にマッピングします。
login	ローカル データベースを認証に使用して特権 EXEC モードを開始します。
service-type	ローカル データベース ユーザの CLI、ASDM、およびイネーブル アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization exec authentication-server

管理認可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 **aaa authorization exec authentication-server** コマンドまたは **aaa authorization exec** コマンドを使用します。管理許可をディセーブルにするには、**aaa authorization exec authentication-server** コマンドの **no** 形式または、**no aaa authorization exec** コマンドを使用します。

aaa authorization exec [authentication-server]

no aaa authorization exec [authentication-server]

構文の説明

authentication-server	ユーザの認証に使用されたサーバから認可属性が取得されることを指定します。

デフォルト

デフォルトでは、このコマンドはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

aaa authorization exec authentication-server コマンドを使用すると、ユーザの service-type クレデンシャルはコンソール アクセスの許可の前に検査されます。

no aaa authorization exec authentication-server コマンドを使用するときは、以下に注意してください：

- コンソール アクセスの許可の前に、ユーザの service-type クレデンシャルはチェックされません。
- コマンド認可が設定されている場合、RADIUS、LDAP、および TACACS+ ユーザについて AAA サーバで特権レベル属性が見つかると、特権レベル属性が引き続き適用されます。

ユーザが CLI、ASDM、または **enable** コマンドにアクセスするときにユーザを認証するように **aaa authentication console** コマンドを設定すると、ユーザ コンフィギュレーションに応じて **aaa authorization exec authentication-server** コマンドで管理アクセスを制限できます。

（注） シリアル アクセスは管理認証に含まれないため、**aaa authentication serial console** を設定している場合は、認証したユーザはすべてコンソール ポートにアクセスできます。

ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- LDAP マッピング済みユーザ：LDAP 属性をマッピングするには、**ldap attribute-map** コマンドを参照してください。
- RADIUS ユーザ：次の値のいずれかにマッピングする IETF RADIUS numeric **service-type** 属性を使用します。
  - Service-Type 5（発信）は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。
  - Service-Type 6（管理）は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）は、**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。

（注） 認識される service-type は、ログイン（1）、フレーム化（2）、管理（6）、および NAS プロンプト（7）のみです。その他の service-type を使用すると、アクセスは拒否されます。

- TACACS+ ユーザ：「service=shell」エントリで許可を要求し、サーバは次のように PASS または FAIL で応答します。
  - PASS、特権レベル 1 は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - PASS、特権レベル 2 以上は、**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。
- ローカル ユーザ：**service-type** コマンドを設定します。これは、**username** コマンドのユーザ名コンフィギュレーション モードです。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で、**aaa authentication console** コマンドを使用する例を示します。

```
hostname(config)# aaa authentication telnet console radius
```

次に、サーバ グループ「AuthIn」をイネーブル認証用に指定する例を示します。

```
hostname(config)# aaa authentication enable console AuthIn
```

次に、**aaa authentication console** コマンドを使用して、グループ「svrgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックさせる例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	コンソール認証をイネーブルにします。
ldap attribute-map	LDAP 属性をマッピングします。
service-type	ローカル ユーザの制限 CLI アクセス。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization include, exclude

セキュリティ アプライアンス を介した接続の許可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 **aaa authorization include** コマンドを使用します。許可からアドレスを除外するには、**aaa authorization exclude** コマンドを使用します。許可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。

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを許可から除外します。
include	認可が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認可を要求するインターフェイスの名前を指定します。
outside_ip	（任意）セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	（任意）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認可が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[**-***port*] • **udp**/*port*[**-***port*] • **icmp**/*type* • *protocol*[/*port*[**-***port*]] **（注）** ポート範囲を指定すると、予期できない結果が許可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを許可する場合もありますが、範囲が受け入れられると、このような許可は行われません。

デフォルト

IP アドレス **0** は「すべてのホスト」を意味します。ローカル IP アドレスを **0** に設定すると、許可されるホストを許可サーバによって決定できます。

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**exclude** パラメータによって、特定のホストに対して除外するポートをユーザが指定できるようになりました。

使用上のガイドライン

アクセス リストで指定されているトラフィックの認可をイネーブルにするには、**aaa authorization match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authorization include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authorization match** コマンドを使用する必要があります。

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

IP アドレスごとに 1 つの **aaa authorization include** コマンドが許可されます。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

（注） ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、TACACS+ プロトコルを使用する例を示します。

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication ssh console tplus1
```

この例では、最初のコマンド ステートメントで tplus1 という名前のサーバ グループを作成し、このグループで使用する TACACS+ プロトコルを指定しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 3 つのコマンド ステートメントで指定しているのは、外部インターフェイス経由で外部ホストへの接続を開始するすべてのユーザを tplus1 サーバ グループを使用して認証すること、正常に認証されたユーザに対してはすべてのサービスの使用を認可すること、およびすべての発信接続情報をアカウンティング データベースに記録することです。最後のコマンド ステー

トメントでは、セキュリティ アプライアンスのコンソールへの SSH アクセスには、tplus1 サーバ グループからの認証が必要であることを指定しています。

次に、外部インターフェイスからの DNS ルックアップに対する認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

次に、内部ホストから内部インターフェイスに到着する ICMP echo-reply パケットの認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

これは、ユーザが Telnet、HTTP、または FTP を使用して認証されていない場合は外部ホストを ping できないことを意味します。

次に、内部ホストから内部インターフェイスに到着する ICMP エコー（ping）についてのみ認可をイネーブルにする例を示します。

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

関連コマンド

コマンド	説明
aaa authorization command	コマンドの実行が認可の対象かどうかを指定します。または、指定したサーバ グループ内のすべてのサーバがディセーブルである場合に、ローカル ユーザ データベースへのフォールバックをサポートするように管理認可を設定します。
aaa authorization match	特定の access-list コマンド名に対して LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization match

セキュリティ アプライアンス を通じた接続の許可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 **aaa authorization match** マンドを使用します。認可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。

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

構文の説明

acl_name	拡張アクセス リストの名前を指定します。**access-list extended** コマンドを参照してください。**許可** ACE は、一致したトラフィックを認可するようにマークします。一方、**拒否**エントリは、一致したトラフィックを認可から除外します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグを指定します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa authorization match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。**aaa authorization match** コマンドによる RADIUS 認可では、FWSM への VPN 管理接続の認可のみがサポートされます。

認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

（注） ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、**aaa** コマンドで tplus1 サーバ グループを使用する例を示します。

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization match myacl inside tplus1
```

この例では、最初のコマンド ステートメントで tplus1 サーバ グループを TACACS+ グループとして定義しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 2 つのコマンド ステートメントでは、内部インターフェイスを通過する、任意の外部ホストへの接続が tplus1 サーバ グループを使用して認証され、これらのすべての接続がアカウンティング データベースに記録されることを指定しています。最後のコマンド ステートメントでは、myacl 内の ACE に一致する接続が tplus1 サーバ グループ内の AAA サーバによって認可されることを指定しています。

関連コマンド

コマンド	説明
aaa authorization	ユーザ認可をイネーブルまたはディセーブルにします。
clear configure aaa	すべての aaa コンフィギュレーション パラメータをデフォルト値にリセットします。
clear uauth	1 人のユーザまたはすべてのユーザについて、AAA 認可キャッシュと AAA 認証キャッシュを削除します。これにより、次に接続を作成するときにユーザは再認証する必要があります。
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および認可のために認可サーバに提供されたユーザ名、ユーザ名がバインドされている IP アドレス、およびユーザは認証されただけかキャッシュされたサービスを持っているかを表示します。

aaa local authentication attempts max-fail

セキュリティ アプライアンス で特定のユーザ アカウントに対して許可されるローカル ログイン試行の連続失敗回数を制限するには（特権レベル 15 のユーザを除きます。この機能はレベル 15 のユーザには影響しません）、グローバル コンフィギュレーション モードで **aaa local authentication attempts max-fail** コマンドを使用します。このコマンドは、ローカル ユーザ データベースによる認証だけに影響します。この機能をディセーブルにし、ローカル ログイン試行の連続失敗回数を無制限に許可するには、このコマンドの **no** 形式を使用します。

aaa local authentication attempts max-fail *number*

構文の説明

number	ユーザがロック アウトされるまでに間違ったパスワードを入力できる最大回数。この数の範囲は、1 ～ 16 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを省略すると、ユーザが間違ったパスワードを入力できる回数に制限は設けられません。

間違ったパスワードを入力した試行回数が設定回数に達すると、ユーザはロック アウトされ、管理者がユーザ名をアンロックするまで、ユーザは正常にログインできません。ユーザ名のロックまたはアンロックにより、システム ログ メッセージが生成されます。

特権レベル 15 のユーザはこのコマンドの影響を受けず、ロック アウトされることはありません。

ユーザが正常に認証されるか、セキュリティ アプライアンスがリブートされると、失敗試行回数は 0 にリセットされ、ロックアウト ステータスは No にリセットされます。

例

次に、**aaa local authentication attempts max-limits** コマンドを使用して、許可される失敗試行の最大回数を 2 に設定する例を示します。

```
hostname(config)# aaa local authentication attempts max-limits 2
hostname(config)#
```

関連コマンド

コマンド	説明
clear aaa local user lockout	指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更しないで、ユーザ認証失敗試行回数をリセットします。
show aaa local user	現在ロックされているユーザ名のリストを表示します。

aaa mac-exempt

認証および認可から免除する MAC アドレスの定義済みリストの使用を指定するには、グローバル コンフィギュレーション モードで **aaa mac-exempt** コマンドを使用します。追加できる **aaa mac-exempt** コマンドは 1 つだけです。MAC アドレスのリストの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

構文の説明

id	**mac-list** コマンドで設定した MAC リスト番号を指定します。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

aaa mac-exempt コマンドを使用する前に、**mac-list** コマンドを使用して MAC リスト番号を設定します。MAC リスト内の permit エントリによって MAC アドレスは認証および認可から免除され、deny エントリによって MAC アドレスの認証および認可が要求されます（認証および認可がイネーブルの場合）。追加できる **aaa mac-exempt** コマンドのインスタンスは 1 つだけであるため、免除するすべての MAC アドレスを MAC リストに含めてください。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次に、00a0.c95d.02b2 を除く MAC アドレスのグループの認証をバイパスする例を示します。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
```

```
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。
mac-list	認証および認可から MAC アドレスを免除するために使用する MAC アドレスのリストを指定します。

aaa proxy-limit

ユーザごとに許可される同時プロキシ接続の最大数を設定することで、uauth セッションの制限を手動で設定するには、グローバル コンフィギュレーション モードで **aaa proxy-limit** コマンドを使用します。プロキシをディセーブルにするには、**disable** パラメータを使用します。デフォルトのプロキシ制限値（16）に戻すには、このコマンドの **no** 形式を使用します。

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

構文の説明

disable	プロキシは許可されません。
proxy_limit	ユーザごとに許可される同時プロキシ接続数（1 ～ 128）を指定します。

デフォルト

デフォルトのプロキシ制限値は 16 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

送信元アドレスがプロキシ サーバである場合は、この IP アドレスを認証から除外するか、許容される未処理 AAA 要求の数を増やすことを検討してください。

例

次に、ユーザごとに許可される未処理認証要求の最大数を設定する例を示します。

```
hostname(config)# aaa proxy-limit 6
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、あるいは ASDM ユーザ認証をイネーブルまたはディセーブルにするか、表示します。
aaa authorization	LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。

aaa-server host	AAA サーバを指定します。
clear configure aaa	設定済みの AAA アカウンティング値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa-server

AAA サーバ グループを作成し、すべてのグループ ホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server** コマンドを使用します。指定した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。

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

構文の説明

server-tag	サーバ グループ名を指定します。**aaa-server host** コマンドで指定した名前と同じにします。他の AAA コマンドで、この AAA サーバ グループ名を参照します。
protocol *server-protocol*	グループ内のサーバによってサポートされる AAA プロトコルを指定します。 • **http-form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	http-form プロトコルが追加されました。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループ プロトコルを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。

シングル モードで最大 15 個のサーバ グループ、マルチ モードでコンテキストごとに 4 個のサーバ グループを保持できます。各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

例

次に、**aaa-server** コマンドを使用して、TACACS+ サーバ グループ コンフィギュレーションの詳細を変更する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
```

関連コマンド

コマンド	説明
accounting-mode	アカウンティング メッセージが単一のサーバに送信されるか（シングル モード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定します。
reactivation-mode	障害の発生したサーバを再度アクティブにする方式を指定します。
max-failed-attempts	サーバ グループ内の所定のサーバが非アクティブ化されるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server active/fail

障害とマークされた AAA サーバを再度アクティブにするには、特権 EXEC モードで **aaa-server active** コマンドを使用します。アクティブなサーバを障害状態にするには、特権 EXEC モードで **aaa-server fail** コマンドを使用します。

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

構文の説明

active	サーバをアクティブ状態に設定します。
fail	サーバを障害状態に設定します。
host	ホストの IP アドレス名または IP アドレスを指定します。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server_ip	AAA サーバの IP アドレスを指定します。
server_tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用しないと、グループ内の障害が発生したサーバは、グループ内のすべてのサーバに障害が発生するまで障害状態のままになります。グループ内のすべてのサーバに障害が発生した後に、サーバはすべて再度アクティブにされます。

例

次に、サーバ 192.168.125.60 の状態を表示し、手動で再度アクティブにする例を示します。

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
hostname# aaa-server active host 192.168.125.60
```

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server host

AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト コンフィギュレーション モードが開始されます。このモードから、ホスト固有の AAA サーバ接続データを指定および管理できます。ホスト コンフィギュレ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。

aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

構文の説明

(*interface-name***)**	（任意）認証サーバが配置されているネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。インターフェイスを指定しない場合、デフォルトは **inside** です（使用可能な場合）。
key	（任意）127 文字までの大文字と小文字が区別される英数字のキーワードを指定します。RADIUS サーバまたは TACACS+ サーバ上のキーと同じ値です。127 文字を超えて入力された文字があれば無視されます。このキーは、セキュリティ アプライアンスとサーバの間でデータを暗号化するために使用されます。このキーは、セキュリティ アプライアンスとサーバ システムの両方で同じである必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。ホスト モードで **key** コマンドを使用して、キーを追加または変更できます。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server-ip	AAA サーバの IP アドレスを指定します。
server-tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。
timeout *seconds*	（任意）要求のタイムアウト間隔。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。ホスト モードで **timeout** コマンドを使用して、タイムアウト間隔を変更できます。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

デフォルトのインターフェイスは、inside 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	DNS 名のサポートが追加されました。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。

シングル モードで最大 15 個のサーバ グループ、マルチ モードでコンテキストごとに 4 個のサーバ グループを保持できます。各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

aaa-server host コマンドを入力した後、ホスト固有のパラメータを設定できます。

例

次に、「watchdogs」という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、そのサーバの Kerberos レルムを定義する例を示します。

（注）　Kerberos 領域名では数字と大文字だけを使用します。セキュリティ アプライアンスは領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

次に、「svrgrp1」という名前の SDI AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、タイムアウト間隔を 6 秒に、リトライ間隔を 7 秒に、SDI バージョンをバージョン 5 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

absolute

時間範囲が有効である場合に絶対時間を定義するには、時間範囲コンフィギュレーション モードで **absolute** コマンドを使用します。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。

absolute [**end** *time date*] [**start** *time date*]

no absolute

構文の説明

date	日付を day month year 形式で指定します（たとえば、1 January 2006）。年の有効な範囲は、1993 ～ 2035 です。
time	時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。

デフォルト

開始時刻および日付を指定しない場合、permit ステートメントまたは deny ステートメントはただちに有効になり、常にオンです。同様に、最大終了時刻は 23:59 31 December 2035 です。終了時刻および日付を指定しない場合、関連付けられている permit ステートメントまたは deny ステートメントは無期限に有効です。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

例

次に、ACL を 2006 年 1 月 1 日の午前 8 時にアクティブにする例を示します。例を示します。

```
hostname(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

関連コマンド

コマンド	説明
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

accept-subordinates

デバイスにインストールされていない下位 CA 証明書がフェーズ 1 の IKE 交換で提供されたときに、その証明書を受け入れるようにセキュリティ アプライアンスを設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **accept-subordinates** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

accept-subordinates

no accept-subordinates

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

デフォルト設定はオンです（下位証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェーズ 1 の処理中に、IKE ピアによって下位証明書とアイデンティティ証明書の両方が渡される場合があります。下位証明書はセキュリティ アプライアンスにインストールされない場合があります。このコマンドを使用すると、管理者はデバイス上にトラストポイントとして設定されていない下位 CA 証明書をサポートできます。確立されたすべてのトラストポイントのすべての下位 CA 証明書が受け入れ可能である必要はありません。つまり、このコマンドを使用すると、デバイスで、証明書チェーン全体をローカルにインストールすることなく、その証明書チェーンを認証できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、セキュリティ アプライアンスでトラストポイント central の下位証明書を受け入れることができるようにする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

access-group

アクセス リストをインターフェイスにバインドするには、グローバル コンフィギュレーション モードで **access-group** コマンドを使用します。アクセス リストをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

access-group *access-list* {**in | out**} **interface** *interface_name* [**per-user-override** | **control-plane**]

no access-group *access-list* {**in | out**} **interface** *interface_name*

構文の説明

access-list	アクセス リストの *ID*。
control-plane	（任意）ルールが to-the-box トラフィック用かどうかを指定します。
in	指定したインターフェイスで着信パケットをフィルタリングします。
interface *interface-name*	ネットワーク インターフェイスの名前。
out	指定したインターフェイスで発信パケットをフィルタリングします。
per-user-override	（任意）ダウンロード可能なユーザ アクセス リストが、インターフェイスに適用されているアクセス リストを上書きできるようにします。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

access-group コマンドは、アクセス リストをインターフェイスにバインドします。アクセス リストは、インターフェイスへの着信トラフィックに適用されます。**access-list** コマンド ステートメントで **permit** オプションを入力すると、セキュリティ アプライアンスによってパケットの処理は続行されます。**access-list** コマンド ステートメントで **deny** オプションを入力すると、セキュリティ アプライアンスによってパケットは廃棄され、次の syslog メッセージが生成されます。

```
%hostname-4-106019: IP packet from source_addr to destination_addr, protocol
protocol received from interface interface_name deny by access-group id
```

per-user-override オプションを指定すると、ダウンロードしたアクセス リストで、インターフェイスに適用されているアクセス リストを上書きできます。オプションの *per-user-override* 引数がないと、セキュリティ アプライアンスによって既存のフィルタリング動作が保持されます。*per-user-override* があると、セキュリティ アプライアンスにより、ユーザに関連付けられているユーザごとのアクセス

リスト（ダウンロードされた場合）の **permit** または **deny** ステータスで、**access-group** コマンドに関連付けられているアクセス リストの permit または deny ステータスを上書きできるようになります。さらに、次のルールが適用されます。

- パケットが到着した時点で、そのパケットに関連付けられているユーザごとのアクセス リストがない場合、インターフェイス アクセス リストが適用されます。
- ユーザごとのアクセス リストは、**timeout** コマンドの **uauth** オプションで指定されたタイムアウト値によって管理されますが、このタイムアウト値は、ユーザごとの AAA セッション タイムアウト値によって上書きできます。
- 既存のアクセス リスト ログ動作は同じです。たとえば、ユーザごとのアクセス リストのためにユーザ トラフィックが拒否された場合、syslog メッセージ 109025 が記録されます。ユーザ トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとのアクセス リストのログ オプションは、影響を及ぼしません。

access-list コマンドは常に **access-group** コマンドとともに使用します。

access-group コマンドは、アクセス リストをインターフェイスにバインドします。**in** キーワードによって、アクセス リストは指定したインターフェイス上のトラフィックに適用されます。**out** キーワードによって、アクセス リストは発信トラフィックに適用されます。

（注） 1 つ以上の **access-group** コマンドによって参照されるアクセス リストから、すべての機能エントリ（permit ステートメントおよび deny ステートメント）を削除すると、**access-group** コマンドはコンフィギュレーションから自動的に削除されます。**access-group** コマンドは、空のアクセス リストまたはコメントだけを含むアクセス リストを参照できません。

no access-group コマンドは、アクセス リストをインターフェイス *interface_name* からアンバインドします。

show running config access-group コマンドは、インターフェイスにバインドされている現在のアクセス リストを表示します。

clear configure access-group コマンドは、インターフェイスからすべてのアクセス リストを削除します。

（注） to-the-box 管理トラフィック用のアクセス コントロール ルール（**http**、**ssh**、**telnet** などのコマンドで定義）は、**control-plane** オプションで適用されるアクセス リストよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box アクセス リストで明示的に拒否されている場合でも着信が許可されます。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# static (inside,outside) 209.165.201.3 10.1.1.3
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

static コマンドでは、10.1.1.3 にある Web サーバにグローバル アドレス 209.165.201.3 を指定しています。**access-list** コマンドでは、任意のホストからポート 80 を使用してグローバル アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。
show running-config access-group	コンテキスト グループのメンバーを表示します。

access-list alert-interval

拒否フローの最大数メッセージの時間間隔を指定するには、グローバル コンフィギュレーション モードで **access-list alert-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list alert-interval *secs*

no access-list alert-interval

構文の説明

secs	拒否フローの最大数メッセージの生成の時間間隔。有効な値は、1 ～ 3600 秒です。デフォルト値は 300 秒です。

デフォルト

デフォルトは 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

access-list alert-interval コマンドでは、システム ログ メッセージ 106001 を生成する時間間隔を設定します。システム ログ メッセージ 106001 によって、セキュリティ アプライアンスが拒否フローの最大数に達したことが警告されます。拒否フローの最大数に達したときに、前回のシステム ログ メッセージ 106001 が生成されてから *secs* 秒以上経過していた場合は、さらに 106001 メッセージが生成されます。

拒否フローの最大数メッセージの生成については、**access-list deny-flow-max** コマンドを参照してください。

例

次に、拒否フローの最大数メッセージの時間間隔を指定する例を示します。

```
hostname(config)# access-list alert-interval 30
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。

access-list deny-flow-max

作成できる同時拒否フローの最大数を指定するには、グローバル コンフィギュレーション モードで **access-list deny-flow-max** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list deny-flow-max

no access-list deny-flow-max

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

デフォルトは、4096 個の同時拒否フローです。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスが ACL 拒否フローの最大数 *n* に達すると、システム ログ メッセージ 106101 が生成されます。

例

次に、作成できる同時拒否フローの最大数を指定する例を示します。

```
hostname(config)# access-list deny-flow-max 256
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list ethertype

EtherType に基づいてトラフィックを制御するアクセス 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 **access-list ethertype** コマンドを使用します。アクセス 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。

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

構文の説明

any	すべての対象へのアクセスを指定します。
bpdu	ブリッジ プロトコル データ ユニットへのアクセスを指定します。デフォルトでは、BPDU は拒否されます。
deny	条件に一致する場合、アクセスを拒否します。
hex_number	EtherType を示す 0x600 以上の 16 ビットの 16 進数値を指定します。
id	アクセス リストの名前または番号をリストします。
ipx	IPX へのアクセスを指定します。
mpls-multicast	MPLS マルチキャストへのアクセスを指定します。
mpls-unicast	MPLS ユニキャストへのアクセスを指定します。
permit	条件が一致した場合にアクセスを許可します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

log オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトの重大度レベルは 6（情報）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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、16 ビットの 16 進数値で示された任意の EtherType を制御できます。EtherType ACL によってイーサネット V2 フレームがサポートされます。802.3 形式のフレームは、タイプ フィールドではなく長さフィールドを使用するため、ACL によって処理されません。ブリッジ プロトコル データ ユニットは唯一の例外であり、ACL によって処理されます。ブリッジ プロトコル データ ユニットは SNAP 方式でカプセル化されており、セキュリティ アプライアンスは特に BPDU を処理するように設計されています。

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる場合は、両方のインターフェイスに ACL を適用する必要があります。

MPLS を許可する場合は、セキュリティ アプライアンスに接続されている両方の MPLS ルータが LDP セッションまたは TDP セッション用のルータ ID としてセキュリティ アプライアンス インターフェイス上の IP アドレスを使用するように設定することにより、LDP TCP 接続と TDP TCP 接続がセキュリティ アプライアンス経由で確立されるようにします （LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）の ACL を 1 つだけ適用できます。同じ ACL を複数のインターフェイスに適用することもできます。

（注） EtherType アクセス リストが **deny all** コマンドで設定されている場合、すべてのイーサネット フレームが廃棄されます。その場合でも、オートネゴシエーションなどの物理プロトコル トラフィックだけは許可されます。

例

次に、EtherType アクセス リストを追加する例を示します。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リストのカウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list extended

アクセス コントロール エントリを追加するには、グローバル コンフィギュレーション モードで **access-list extended** コマンドを使用します。アクセス リストは、同じアクセス リスト ID を持つ 1 つ以上の ACE で構成されます。アクセス リストは、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リスト全体を削除するには、**clear configure access-list** コマンドを使用します。

access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**}
{*protocol* | **object-group** *protocol_obj_grp_id*}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

no access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**} {**tcp** | **udp**}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port*] | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

構文の説明

default	（任意）ロギングをデフォルトの方式に設定します。拒否されたパケットごとにシステム ログ メッセージ 106023 を生成します。
deny	条件に合致している場合、パケットを拒否します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによってパケットはセキュリティ アプライアンスを通過できなくなります。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってトラフィックがインスペクションから免除されます。一部の機能では deny ACE の使用は許可されません（NAT など）。詳細については、アクセス リストを使用する各機能のコマンド マニュアルを参照してください。
dest_ip	パケットの送信先のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
disable	（任意）この ACE のロギングをディセーブルにします。
extended	（任意）ACE を追加します。
icmp_type	（任意）プロトコルが ICMP の場合、ICMP タイプを指定します。
id	アクセス リスト ID を最大 241 文字のストリングまたは整数として指定します。ID は、大文字と小文字が区別されます。 **ヒント** コンフィギュレーションでアクセス リスト ID を見やすくするには、すべて大文字にします。

inactive	（任意）ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。
interface *ifc_name*	インターフェイス アドレスを送信元アドレスまたは宛先アドレスとして指定します。 **（注）** トラフィックの宛先がデバイス インターフェイスである場合、アクセス リストに実際の IP アドレスを指定する代わりに interface キーワードを指定する必要があります。
interval *secs*	（任意）システム ログ メッセージ 106100 を生成するログ間隔を指定します。有効な値は、1 ～ 600 秒です。デフォルトは 300 です。
level	（任意）システム ログ メッセージ 106100 の重大度レベル（0 ～ 7）を設定します。デフォルトのレベルは 6（情報）です。
line *line-num*	（任意）ACE を挿入する行番号を指定します。行番号を指定しなかった場合は、アクセス リストの末尾に ACE が追加されます。行番号はコンフィギュレーションに保存されません。ACE の挿入場所を指定するだけです。
log	（任意）**ACE** がネットワーク アクセス（**access-group** コマンドで適用されたアクセス リスト）のパケットと一致したときのロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル（6）とデフォルト間隔（300 秒）でシステム ログ メッセージ 106100 が有効になります。**log** キーワードを入力しないと、デフォルトのシステム ログ メッセージ 106023 が生成されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。セキュリティ アプライアンスでは、ネットワーク マスク（たとえば、クラス C マスクの場合は 255.255.255.0）を使用します。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。
object-group *icmp_type_obj_grp_id*	（任意）プロトコルが ICMP の場合、ICMP タイプのオブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group icmp-type** コマンドを参照してください。
object-group *network_obj_grp_id*	ネットワーク オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group network** コマンドを参照してください。
object-group *protocol_obj_grp_id*	プロトコル オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group protocol** コマンドを参照してください。
object-group *service_obj_grp_id*	（任意）プロトコルを TCP または UDP に設定する場合、サービス オブジェクト グループの ID を指定します。オブジェクト グループを追加するには、**object-group service** コマンドを参照してください。

operator	（任意）送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい • **neq**：等しくない • **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200`
permit	条件に合致している場合、パケットを許可します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによってパケットはセキュリティ アプライアンスを通過できます。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってインスペクションがパケットに適用されます。
port	（任意）プロトコルを TCP または UDP に設定する場合、TCP ポートまたは UDP ポートの番号（整数）か名前を指定します。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。
protocol	IP プロトコルの名前または番号を指定します。たとえば、UDP は 17、TCP は 6、EGP は 47 です。
src_ip	パケットの送信元のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
time-range *time_range_name*	（任意）ACE に時間範囲を適用することによって、週および 1 日の中の特定の時刻に各 ACE がアクティブになるようにスケジューリングします。時間範囲の定義については、**time-range** コマンドを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- ACE ロギングは、拒否されたパケットについてシステム ログ メッセージ 106023 を生成します。拒否されたパケットをログに記録するには、**deny ACE** が存在している必要があります。
- **log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6（情報）で、デフォルトの間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

特定のアクセス リスト名に対して入力した各 ACE は、ACE で行番号を指定しない限り、そのアクセス リストの最後に追加されます。

ACE の順序は重要です。セキュリティ アプライアンスがパケットを転送するかドロップするかを決定するとき、セキュリティ アプライアンスでは、エントリがリストされている順に、各 ACE に対してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合、残りのステートメントはチェックされません。

アクセス リストの最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除き、セキュリティ アプライアンス経由でのネットワークへのアクセスをすべてのユーザに許可する場合は、特定のアドレスを拒否し、それ以外はすべて許可する必要があります。

NAT を使用する場合、アクセス リストに対して設定する IP アドレスは、アクセス リストが付加されるインターフェイスによって異なります。インターフェイスに接続されるネットワーク上で有効なアドレスを使用する必要があります。このガイドラインは、着信アクセス グループと発信アクセス グループの両方に適用されます。使用されるアドレスは、方向ではなく、インターフェイスのみによって決まります。

TCP 接続と UDP 接続では、リターン トラフィックを許可するアクセス リストは必要ありません。これは、FWSM によって、確立された双方向接続のすべてのリターン トラフィックが許可されるためです。ただし、ICMP などのコネクションレス型のプロトコルでは、セキュリティ アプライアンスによって単方向のセッションが確立されます。そのため、両方向の ICMP を許可するアクセス リストが必要となるか（アクセス リストを送信元インターフェイスおよび宛先インターフェイスに適用）、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ICMP はコネクションレス型プロトコルであるため、両方向の ICMP を許可するアクセス リストが必要となるか（アクセス リストを送信元インターフェイスおよび宛先インターフェイスに適用）、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンでは、ICMP セッションはステートフル接続として処理されます。ping を制御するには、**echo-reply (0)**（セキュリティ アプライアンスからホストへ）または **echo (8)**（ホストからセキュリティ アプライアンスへ）を指定します。ICMP タイプのリストについては、表 1 を参照してください。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用できます。インターフェイスへのアクセス リストの適用の詳細については、**access-group** コマンドを参照してください。

（注）　アクセス リスト コンフィギュレーションを変更する場合、既存の接続がタイムアウトするのを待たずに新しいアクセス リスト情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

表 1 に、使用できる ICMP タイプの値を示します。

表 2-1　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

例

次のアクセス リストは、（アクセス リストを適用するインターフェイス上の）すべてのホストがセキュリティ アプライアンスを通過するのを許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のサンプル アクセス リストでは、192.168.1.0/24 上のホストが 209.165.201.0/27 ネットワークにアクセスすることが禁止されます。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

一部のホストのみにアクセスを制限する場合は、制限された **permit ACE** を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次のアクセス リストでは、すべてのホスト（アクセス リスト適用先のインターフェイス上にあるすべてのホスト）がアドレス 209.165.201.29 の Web サイトにアクセスすることが禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

オブジェクト グループを使用する次のアクセス リストでは、内部ネットワーク上のいくつかのホストがいくつかの Web サーバへのアクセスを禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

ネットワーク オブジェクトの 1 つのグループ（A）からネットワーク オブジェクトの別のグループ（B）へのトラフィックを許可するアクセス リストを一時的にディセーブルにするには、次のコマンドを使用します。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベースのアクセス リストを実装するには、**time-range** コマンドを使用して、1 日および週の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲をアクセス リストにバインドします。次に、「Sales」という名前のアクセス リストを「New_York_Minute」という名前の時間範囲にバインドする例を示します。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

時間範囲の定義方法の詳細については、**time-range** コマンドを参照してください。

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	ACE を番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list remark

access-list extended コマンドの前または後に追加するコメントのテキストを指定するには、グローバル コンフィギュレーション モードで **access-list remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** [*text*]

構文の説明

id	アクセス リストの名前。
line *line-num*	（任意）コメントまたは Access Control Element（ACE）を挿入する行番号。
remark text	**access-list extended** コマンドの前または後に追加するコメントのテキスト。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

コメント テキストには、スペース以外の文字を少なくとも 1 つ含める必要があります。空のコメントは許可されません。コメント テキストは、スペースや句読点を含め、最大 100 文字です。

コメントのみを含む ACL では **access-group** コマンドは使用できません。

例

次に、**access-list** コマンドの前または後に追加するコメントのテキストを指定する例を示します。

```
hostname(config)# access-list 77 remark checklist
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list rename

アクセス リストの名前を変更するには、グローバル コンフィギュレーション モードで **access-list rename** コマンドを使用します。

access-list *id* **rename** *new_acl_id*

構文の説明

id	既存のアクセス リストの名前。
rename *new_acl_id*	新しいアクセス リスト ID を最大 241 文字のストリングまたは整数として指定します。ID は、大文字と小文字が区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

アクセス リストを同じ名前に変更すると、コマンドは適応型セキュリティ アプライアンスによって通知なしで無視されます。

例

次に、アクセス リストの名前を TEST から OUTSIDE に変更する例を示します。

```
hostname(config)# access-list TEST rename OUTSIDE
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list standard

OSPF 再配布のルート マップで使用できる、OSPF ルートの宛先 IP アドレスを指定するアクセス リストを追加するには、グローバル コンフィギュレーション モードで **access-list standard** コマンドを使用します。アクセス 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。

access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

構文の説明

any	すべての対象へのアクセスを指定します。
deny	条件に一致する場合、アクセスを拒否します。
host *ip_address*	ホスト IP アドレスへのアクセスを指定します（任意）。
id	アクセス リストの名前または番号。
ip_address ip_mask	特定の IP アドレス（任意）およびサブネット マスクへのアクセスを指定します。
line *line-num*	（任意）ACE を挿入する行番号。
permit	条件が一致した場合にアクセスを許可します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-group コマンドとともに **deny** キーワード使用すると、パケットはセキュリティ アプライアンスを通過できません。デフォルトでは、特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。

送信元アドレス、ローカル アドレス、または宛先アドレスを指定するには、次のガイドラインを使用します。

- 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。
- アドレスおよびマスク 0.0.0.0 0.0.0.0 の省略形としてキーワード **any** を使用します。
- マスク 255.255.255.255 の省略形として **host** *ip_address* オプションを使用します。

例

次に、適応型セキュリティ アプライアンス経由の IP トラフィックを拒否する例を示します。

```
hostname(config)# access-list 77 standard deny
```

次に、条件に合致している場合に、適応型セキュリティ アプライアンス経由の IP トラフィックを許可する例を示します。

```
hostname(config)# access-list 77 standard permit
```

次の例は、宛先アドレスを指定する方法を示しています。

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
clear access-group	アクセス リスト カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list webtype

クライアントレス SSL VPN のフィルタリングをサポートするコンフィギュレーションにアクセス リストを追加するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。アクセス 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。

access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

構文の説明

any	すべての IP アドレスを指定します。
any	（任意）すべての URL を指定します。
deny	条件に一致する場合、アクセスを拒否します。
host *ip_address*	ホスト IP アドレスを指定します。
id	アクセス リストの名前または番号。
interval *secs*	（任意）システム ログ メッセージ 106100 を生成する時間間隔を指定します。有効な値は、1 ～ 600 秒です。
ip_address ip_mask	特定の IP アドレスおよびサブネット マスクを指定します。
log [[**disable** | **default**] | *level*]	（任意）ACE に対してシステム ログ メッセージ 106100 が生成されることを指定します。詳細については、**log** コマンドを参照してください。
oper	*ip_address* ポートを比較します。使用できるオペランドは、lt（less than：未満）、gt（greater than：より大きい）、eq（equal：一致）、neq（not equal：不一致）、range（inclusive range：包含範囲）です。
permit	条件が一致した場合にアクセスを許可します。
port	TCP ポートまたは UDP ポートの 10 進数または名前を指定します。
time_range *name*	（任意）time-range オプションをこのアクセス リスト要素に付加するためのキーワードを指定します。
url	フィルタリングに URL を使用することを指定します。
url_string	（任意）フィルタリングする URL を指定します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。
- **log** オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトのレベルは 6（情報）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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　**access-list webtype** コマンドは、クライアントレス SSL VPN フィルタリングを設定するために使用されます。URL には、完全な URL またはファイルを除いた部分的な URL を指定できます。また、サーバのワイルドカードを含めたり、ポートを指定したりできます。

有効なプロトコル識別子は、http、https、cifs、imap4、pop3、および smtp です。URL にキーワード **any** を含めて、任意の URL を参照することもできます。アスタリスクを使用して、DNS 名のサブコンポーネントを表すことができます。

例　次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.company.com
```

次の例は、特定のファイルへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url
https://www.company.com/dir/file.html
```

次の例は、任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
show running-config access-list	適応型セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

accounting-mode

アカウンティング メッセージが単一のサーバに送信されるか（シングル モード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定するには、AAA サーバ コンフィギュレーション モードで **accounting-mode** コマンドを使用します。アカウンティング モードの指定を削除するには、このコマンドの **no** 形式を使用します。

accounting-mode {**simultaneous** | **single**}

構文の説明

simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。
single	単一のサーバにアカウンティング メッセージを送信します。

デフォルト

デフォルト値はシングル モードです。

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	透過	シングル	コンテキスト	システム
AAA サーバ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

単一のサーバにアカウンティング メッセージを送信するには、キーワード **single** を使用します。サーバ グループ内のすべてのサーバにアカウンティング メッセージを送信するには、キーワード **simultaneous** を使用します。

このコマンドは、アカウンティング（RADIUS または TACACS+）にサーバ グループが使用されている場合にのみ有効です。

例

次に、**accounting-mode** コマンドを使用して、グループ内のすべてのサーバにアカウンティング メッセージを送信する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	アカウンティング サービスをイネーブルまたはディセーブルにします。

aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始し、グループ内のすべてのホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-port

このホストの RADIUS アカウンティングに使用されるポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **accounting-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドでは、アカウンティング レコードの送信先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

accounting-port *port*

no accounting-port

構文の説明

port	RADIUS アカウンティング用のポート番号。値の範囲は 1 ～ 65535 です。

デフォルト

デフォルトでは、デバイスはアカウンティングのためにポート 1646 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS アカウンティングのデフォルトのポート番号（1646）が使用されます。

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	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティング サーバで 1646 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートに対してセキュリティ アプライアンスを設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、アカウンティング ポートを 2222 に設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがいずれのネットワーク サービスにアクセスしたかに関するレコードを保持します。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-server-group

アカウンティング レコード送信用の AAA サーバ グループを指定するには、さまざまなモードで **accounting-server-group** コマンドを使用します。アカウンティング サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、アカウンティングを使用して、ユーザがアクセスするネットワーク リソースを追跡します。

accounting-server-group *group_tag*

no accounting-server-group [*group_tag***]**

構文の説明

group_tag	設定済みのアカウンティング サーバまたはサーバ グループを指定します。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、アカウンティング サーバは設定されていません。

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	透過	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	•	—	•	—	—
Pop3s コンフィギュレーション	•	—	•	—	—
smtps コンフィギュレーション	•	—	•	—	—
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが、webvpn コンフィギュレーション モードではなく、トンネル グループ一般属性コンフィギュレーション モードで使用できるようになりました。

使用上のガイドライン

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性コンフィギュレーション モードの同等のコマンドに変換されます。

例

トンネル グループ一般属性コンフィギュレーション モードでの次の例では、IPSec LAN-to-LAN トンネル グループ「xyz」に対して「aaa-server123」という名前のアカウンティング サーバ グループを設定します。

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general-attributes
```

```
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)#
```

次に、POP3SSVRS という名前の一連のアカウンティング サーバを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

関連コマンド

コマンド	説明
aaa-server	認証、許可、およびアカウンティング サーバを設定します。