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

aaa accounting command

CLI で **show** 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** コマンドを使用します。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*

シンタックスの説明

tacacs+-server-tag	**aaa-server protocol** コマンドで指定したように、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は、特権の最低レベルを指定して、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。指定したレベルより下のコマンドは、セキュリティ アプライアンスで処理されません。

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
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、管理者が入力した **show** コマンド以外のコマンドが記録され、1 つまたは複数のアカウンティング サーバに送信されます。

例

次の例では、サポートされている全コマンドのアカウンティング レコードが生成され、そのレコードが adminserver というサーバ グループに送信されるように指定しています。

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

関連コマンド

コマンド	説明
aaa accounting	**aaa-server** コマンドで指定したサーバ上の TACACS+ または RADIUS のユーザ 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。
clear configure aaa	設定済みの AAA アカウンティングの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

管理者アクセス権の 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。管理者アクセス権の 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 {**http | serial| telnet | ssh | enable**} **console** *server-tag*

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

シンタックスの説明

enable	特権 EXEC モードの開始および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。
http	HTTP 接続で作成される管理セッションの確立および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管理セッションの確立および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** コマンドで定義したように、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 および TACACS+ です。
ssh	SSH で作成される管理セッションの確立および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 で作成される管理セッションの確立および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、管理者アクセス権の 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
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

サーバ グループの名前（事前に **aaa-server** コマンドで指定したもの）を指定する必要があります。

例

次の例では、すべての HTTP トランザクションに対してアカウンティング レコードが生成され、そのレコードが adminserver という名前のサーバに送信されるよう指定しています。

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

関連コマンド

コマンド	説明
aaa accounting match	**aaa-server** コマンドで指定したサーバ上の TACACS+ または RADIUS のユーザ 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 accounting command	管理者（ユーザ）によって入力された、各コマンドまたは指定した特権レベル以上のコマンドを記録し、アカウンティング サーバ（複数可）に送信するよう指定します。
clear configure aaa	設定済みの AAA アカウンティングの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 アプライアンス経由の TCP 接続または 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*

シンタックスの説明

exclude	サービスとアドレスが **include** コマンドですでに指定されている場合に、指定されたサービスと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と IP アドレスを指定します。**include** 文で指定されてい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インターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。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 を使用します。
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	（オプション）セキュリティの低いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。すべてのホストを指定するには、0 を指定します。
outside_mask	（オプション）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 を使用します。
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） • **ftp** • **http** • **https** • ***ssh*** • **telnet** • **tcp**/*port* • **udp**/*port*

デフォルト

デフォルトでは、管理者アクセス権の 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
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のものです。

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すべての TCP トラフィックおよび UDP トラフィックについて、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。このトラフィックが認証の対象にもなっている場合、AAA サーバはアカウンティング情報をユーザ名で管理できます。トラフィックが認証の対象になっていない場合、AAA サーバはアカウンティング情報を IP アドレスで管理できます。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、当該セッションでセキュリティ アプライアンスを通過したバイト数、使用されたサービス、および各セッションの継続時間が含まれています。

このコマンドを使用するには、**aaa-server** コマンドで AAA サーバを指定しておく必要があります。

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お勧めします。**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ないためです。

セキュリティ レベル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。この場合は、**aaa accounting match** コマンドを使用する必要があります。

例

次の例では、すべての TCP 接続でアカウンティングをイネーブルにしています。

```
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に対するアカウンティングをイネーブルにします。
aaa accounting command	管理者アクセス権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消去します。
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 アプライアンス経由の TCP 接続および 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*

シンタックスの説明

acl_name	**access-list** 名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 エントリが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 トラフィックに対してのみサポートされます。このコマンドを入力し、そのコマンドが他のプロトコルを許可するアクセス リストを参照している場合、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
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のものです。

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すべての TCP トラフィックおよび UDP トラフィックについて、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。このトラフィックが認証の対象にもなっている場合、AAA サーバはアカウンティング情報をユーザ名で管理できます。トラフィックが認証の対象になっていない場合、AAA サーバはアカウンティング情報を IP アドレスで管理できます。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、当該セッションでセキュリティ アプライアンスを通過したバイト数、使用されたサービス、および各セッションの継続時間が含まれています。

このコマンドを使用するには、**aaa-server** コマンドで AAA サーバを指定しておく必要があります。

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だけに送信されます。

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お勧めします。**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ないためです。

例

次の例では、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方法を示します。

```
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	コマンド内で IP アドレスを直接指定することで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 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**}

シンタックスの説明

exclude	サービスとアドレスが **include** コマンドですでに指定されている場合に、指定されたサービスと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と IP アドレスを指定します。**include** 文で指定されてい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インターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。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 を使用します。
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	（オプション）セキュリティの低いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。すべてのホストを指定するには、0 を指定します。
outside_mask	（オプション）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 を使用します。

server_tag	**aaa-server** コマンドで定義した 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） • **ftp** • **http** • **https** • ***ssh*** • **telnet** • **tcp**/*port*[-*port*] • **udp**/*port*[-*port*] • **icmp**/*type* • *protocol*[/*port*[-*port*]] どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。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
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のものです。

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お勧めします。**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ないためです。

セキュリティ レベル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。この場合は、**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。

ワンタイム認証

所定の IP アドレスを持つユーザは、認証セッションの期限が切れるまで、すべての規則およびタイプのいずれかで認証を 1 回受けるだけで済みます（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の継続中、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==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。この文字列が消去されるのは、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。

認証チャレンジの受信に必要なアプリケーション

どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。

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。

- FTP の場合はポート 21
- Telnet の場合はポート 23
- HTTP の場合はポート 80
- HTTPS の場合はポート 443

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 では、セキュリティ アプライアンスが認証プロンプトを生成します。

HTTP では、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 では、セキュリティ アプライアンスがカスタム 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改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

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 ページの変換規則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ような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

正しく認証されると、セキュリティ アプライアンスによって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手続きがある場合、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お勧めします。

FTP では、ユーザがセキュリティ アプライアンスのユーザ名、アットマーク（@）、FTP ユーザ名（name1@name2 形式）を入力するオプションがあります。パスワードを入力するとき、ユーザはセキュリティ アプライアンスのパスワードに続けてアットマーク（@）を入力し、次に FTP パスワードを入力します（password1@password2）。たとえば、次のように入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能が役立つのは、ファイアウォールをカスケードしていて、複数のログインが必要になる場合です。名前やパスワードが複数ある場合は、アットマーク（@）を複数使用して、それぞれを区切ります。

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、何回でもプロンプトが再表示される。
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 と HTTP

HTTP の認証では、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。実際のポート 80 宛てのトラフィックを検出した場合、マッピング ポートが何番であるかにかかわらず、セキュリティ アプライアンスはその HTTP 接続を代行受信し、認証を強制します。

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、ユーザが 10.48.66.155 にポート 889 でアクセスしようとすると、セキュリティ アプライアンスがトラフィックを代行受信して HTTP 認証を強制します。セキュリティ アプライアンスが HTTP 接続の確立を許可する前に、ユーザの Web ブラウザに 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 80 以外になっているとします。

```
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が表示されません。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には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は、**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。

インターフェイスに対して AAA をイーブルにすると、セキュリティ アプライアンスでの直接認証が次の URL で可能になります。

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 プロンプトを提供します。

例

次の例は、外部インターフェイスで内部 IP アドレスが 192.168.0.0、ネットマスクが 255.255.0.0、すべてのホストの外部 IP アドレスの TCP トラフィックを tacacs+ というサーバ グループを使用して認証します。2 行目のコマンドでは、外部インターフェイスで、内部アドレスが 192.168.38.0、すべてのホストの外部 IP アドレスの Telnet トラフィックを認証から除外しています。

```
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+
```

次の例は、*interface-name* パラメータの使用方法を示しています。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）が接続されています。

次の例では、内部ネットワークから外部ネットワーク宛てに送信される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宛てに送信される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宛てに送信される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宛てに送信される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宛てに送信される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	特権モードに入るときの認証をイネーブルまたはディセーブルにします。あるいは、指定した接続タイプでセキュリティ アプライアンスにアクセスする場合に、認証確認を要求します。
aaa authentication match	照合用のアクセス リストの名前（事前に **access-list** コマンドで定義したもの）を指定して、一致した場合に認証します。
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ことを許可する前に、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 protocol	グループ関連のサーバ アトリビュートを設定します。
aaa-server host	ホスト関連のアトリビュートを設定します。

aaa authentication console

SSH、HTTP、Telnet 接続を介して、またはセキュリティ アプライアンスの Console コネクタからセキュリティ アプライアンス コンソールにアクセスするときの認証サービス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 console** コマンドを使用します。このコマンドで、特権 EXEC モードへのアクセスもイネーブルになります。この認証サービス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** {*server-tag* [**LOCAL**] | **LOCAL**}

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

シンタックスの説明

enable	**enable** コマンドを使用して特権 EXEC モードで入力したエントリの認証をイネーブルにします。
http	HTTPS 接続の ASDM セッションの認証をイネーブルにします。HTTP の管理認証では、SDI サーバ グループのプロトコルをサポートしていません。
LOCAL	***LOCAL*** キーワードには、2 つの使用方法があります。ローカル データベースを使用するように指定する方法と、指定した認証サーバを利用できない場合にローカル データベースにフォールバックするように指定する方法です。
serial	シリアル コンソール インターフェイスで確立した管理セッションの認証をイネーブルにします。
server-tag	**aaa-server protocol** 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。 **LOCAL** というサーバ グループタグを指定すると、ローカルのユーザ データベースを使用できます。
ssh	SSH の管理セッションの認証をイネーブルにします。
telnet	Telnet 接続の管理セッションの認証をイネーブルにします。

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。

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
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のものです。

使用上のガイドライン

CLI 認証をイネーブルにした場合は、セキュリティ アプライアンスが、ログイン用のユーザ名とパスワードを入力するように求めるプロンプトを表示します。必要な情報を入力すると、ユーザ EXEC モードにアクセスできます。

特権 EXEC モードに入るには、**enable** コマンドか、**login** コマンド（ローカル データベースだけを使用している場合）を入力します。

イネーブル認証を設定した場合は、セキュリティ アプライアンスが、ユーザ名とパスワードを入力するように求めるプロンプトを表示します。イネーブル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、イネーブル認証を使用しないと、**enable** コマンドを入力した後で、特定のユーザとしてログインすることはありません。ユーザ名を維持したい場合は、イネーブル認証を使用してください。この機能は、コマンドの認証を行う場合、つまりユーザが入力できるコマンドを、ユーザ名で決める場合に特に便利です。

ローカル データベースを使って認証する場合は、**login** コマンドを使用できます。この場合は、ユーザ名が維持され、認証を有効にする設定は必要ありません。

セキュリティ アプライアンスで Telnet、SSH、または HTTP のユーザの認証を開始する前に、**telnet**、**ssh**、および **http** 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、セキュリティ アプライアンスと通信できる IP アドレスが決まります。Telnet 接続では、内部インターフェイスおよび IPSec を設定した外部インターフェイスからセキュリティ アプライアンス コンソールにアクセスできます。SSH の場合は、どのインターフェイスからでもセキュリティ アプライアンス コンソールにアクセスできます。

http キーワードは、HTTPS 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 ASDM クライアントを認証します。HTTP 認証は、AAA サーバを使用する場合だけ設定する必要があります。デフォルトでは、このコマンドを設定しなくても、ASDM は認証用にローカル データベースを使用します。HTTP 管理認証では、AAA サーバ グループ用に SDI プロトコルをサポートしていません。

認証用に AAA サーバ グループを使う場合は、セキュリティ アプライアンスで AAA サーバを利用できないときにローカル データベースをフォールバックとして使用するように設定できます。このためには、サーバ グループ名の次に **LOCAL** と入力します（**LOCAL** は必ず大文字で入力してください）。ローカル データベースのユーザ名とパスワードは、AAA サーバと同じものにすることをお勧めします。これは、セキュリティ アプライアンスのプロンプトには、どちらの方法で認証しているかが示されないからです。

ローカル データベースを主な認証方法（フォールバックなし）にすることもできます。この場合は、**LOCAL** だけを入力します。

HTTP 認証で要求できるユーザ名の最大長は、30 文字です。パスワードの最大長は 16 文字です。

次の表に、このコマンドで指定したオプションによって、セキュリティ アプライアンス コンソールへのアクセスを認証するときの処理がどのように異なるかを示します。

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	成功するまで何回でも試行できる。
SSH	3 回失敗するとアクセスが拒否される。
Telnet	成功するまで何回でも試行できる。
HTTP	成功するまで何回でも試行できる。

SSH での認証要求がタイムアウトになった（AAA サーバがダウンしているか利用できない）場合は、**pix** というユーザ名とイネーブル 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 パスワードはブランクです。この動作は、AAA が設定されていない状態でセキュリティ アプライアンスにログインする場合と異なります。AAA が設定されていない場合は、ログイン パスワード（**passwd** コマンドで設定）を使用します。

aaa authentication http console コマンド文を定義していない場合は、ASDM を使用して、ユーザ名とセキュリティ 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）を入力しなくてもセキュリティ アプライアンスにアクセスできます。**aaa** コマンドを定義した場合でも、HTTP の認証要求がタイムアウトしたとき（AAA サーバがダウンしているか利用できない）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。

例

次の例は、「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方法を示しています。

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

次の例では、サーバ グループ「AuthIn」を管理認証用に指定しています。

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

次の例は、**aaa authentication console** コマンドを使用して、グループ「srvgrp1」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するようにする方法を示しています。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config)# aaa authentication serial console srvgrp1 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	ユーザ認証用の AAA サーバ グループを指定します。
clear configure aaa	設定済みの AAA アカウンティングの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 authentication listener

ネットワーク ユーザを認証するために HTTP（S）リスニング 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 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 アプライアンスは直接接続や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**]

シンタックスの説明

http[s]	リッスンするプロトコル（HTTP または HTTPS のいずれか）を指定します。このコマンドはプロトコルごとに入力します。
port *portnum*	セキュリティ アプライアンスが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。
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、認証 Web ページにアクセスできるのはセキュリティ アプライアンス インターフェイス宛てのトラフィックだけとなります。
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。

デフォルト

デフォルトでは、イネーブルになっているリスナー サービスはなく、HTTP 接続は基本 HTTP 認証を使用します。リスナーをイネーブルにした場合、デフォルト 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している場合、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
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** コマンドまたは **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を受ける必要があるとき、セキュリティ アプライアンスは基本 HTTP 認証を使用します。HTTPS では、セキュリティ アプライアンスがカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードと共に設定した場合、セキュリティ アプライアンスはすべての HTTP（S）認証要求を、セキュリティ アプライアンスが提供する Web ページにリダイレクトします。

リダイレクションは基本方式を改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

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 ページの変換規則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ような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

redirect オプションを*含めずに* **aaa authentication listener** コマンドを入力した場合は、セキュリティ アプライアンスでの直接認証だけがイネーブルになり、通過トラフィックは基本 HTTP 認証を使用することになります。**redirect** オプションを含めると、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ていないトラフィック タイプを認証する場合に役立ちます。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。

例

次の例では、HTTP 接続および HTTPS 接続をデフォルト 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しています。

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

次の例では、直接セキュリティ アプライアンスに向かう認証要求を許可しています。通過トラフィックは基本 HTTP 認証を使用します。

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

次の例では、HTTP 接続および HTTPS 接続をデフォルトではない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しています。

```
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	
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	

aaa authentication match

セキュリティ アプライアンス経由のトラフィックを認証するには、グローバル コンフィギュレーション モードで **aaa authentication 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**}

シンタックスの説明

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
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のものです。

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お勧めします。**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ないためです。

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。

ワンタイム認証

所定の IP アドレスを持つユーザは、認証セッションの期限が切れるまで、すべての規則およびタイプのいずれかで認証を 1 回受けるだけで済みます（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の継続中、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==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。この文字列が消去されるのは、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。

認証チャレンジの受信に必要なアプリケーション

どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。

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。

- FTP の場合はポート 21
- Telnet の場合はポート 23
- HTTP の場合はポート 80
- HTTPS の場合はポート 443

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 では、セキュリティ アプライアンスが認証プロンプトを生成します。

HTTP では、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 では、セキュリティ アプライアンスがカスタム 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改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

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 ページの変換規則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ような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

正しく認証されると、セキュリティ アプライアンスによって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手続きがある場合、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お勧めします。

FTP では、ユーザがセキュリティ アプライアンスのユーザ名、アットマーク（@）、FTP ユーザ名（name1@name2 形式）を入力するオプションがあります。パスワードを入力するとき、ユーザはセキュリティ アプライアンスのパスワードに続けてアットマーク（@）を入力し、次に FTP パスワードを入力します（password1@password2）。たとえば、次のように入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能が役立つのは、ファイアウォールをカスケードしていて、複数のログインが必要になる場合です。名前やパスワードが複数ある場合は、アットマーク（@）を複数使用して、それぞれを区切ります。

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、何回でもプロンプトが再表示される。
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 と HTTP

HTTP の認証では、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。実際のポート 80 宛てのトラフィックを検出した場合、マッピング ポートが何番であるかにかかわらず、セキュリティ アプライアンスはその HTTP 接続を代行受信し、認証を強制します。

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、ユーザが 10.48.66.155 にポート 889 でアクセスしようとすると、セキュリティ アプライアンスがトラフィックを代行受信して HTTP 認証を強制します。セキュリティ アプライアンスが HTTP 接続の確立を許可する前に、ユーザの Web ブラウザに 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 80 以外になっているとします。

```
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が表示されません。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には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は、**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。

インターフェイスに対して AAA をイーブルにすると、セキュリティ アプライアンスでの直接認証が次の URL で可能になります。

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 プロンプトを提供します。

例

次の一連の例は、**aaa authentication match** コマンドの使用方法を示しています。

```
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+
```

この場合、次の 2 つのコマンドは同じ意味になります。

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

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 コマンド内のリストでは、**access-list** コマンド文を参照している部分が指定した順に処理されます。ここで、次のコマンドを入力するとします。

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

上のコマンドの後に、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** コマンド文グループにトラフィックが一致しているかどうかを確かめ、次に **yourlist** 内の **access-list** コマンド文グループに一致しているかどうかを確かめます。

関連コマンド

コマンド	説明
aaa authorization	LOCAL ユーザ認可サービスまたは 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。
access-list extended	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
clear configure aaa	設定済みの AAA アカウンティングの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 authentication secure-http-client

SSL をイネーブルにして、HTTP クライアントとセキュリティ アプライアンスの間でのユーザ名とパスワードの交換を保護するには、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** コマンドは、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ことを許可する前に、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 authentication secure-http-client

no aaa authentication secure-http-client

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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のものです。

使用上のガイドライン

aaa authentication secure-http-client コマンドは、（SSL を介して）HTTP クライアント認証を保護します。このコマンドは、HTTP カットスルー プロキシ認証に使用されます。

次に、**aaa authentication secure-http-client** コマンドの制限事項を示します。

- 実行時、許可される HTTPS 認証プロセスは最大で 16 個です。16 個の HTTPS 認証プロセスがすべて実行中である場合、認証を要求する 17 番目の新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されている（**uauth timeout** が 0 に設定されている）場合は、HTTPS 認証が機能しません。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。この現象を回避するには、**timeout uauth 0:0:1** コマンドを使用して、**uauth timeout** を 1 秒に設定します。ただし、この回避策ではウィンドウが 1 秒間開かれるため、このウィンドウを利用して、同じ送信元 IP アドレスからアクセスしてくる未認証のユーザがファイアウォールを通過する可能性があります。

- HTTPS 認証は SSL ポート 443 で発生するため、HTTP クライアントから HTTP サーバに向かうポート 443 上のトラフィックをブロックするように **access-list** コマンド文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、1 行目で Web トラフィックに対してスタティック PAT を設定しているため、2 行目を追加して、HTTPS 認証コンフィギュレーションをサポート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

次の例では、HTTP トラフィックがセキュアに認証されるように設定しています。

```
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* に適切な値を指定することを表します。

次のコマンドでは、HTTPS トラフィックがセキュアに認証されるように設定しています。

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

「...」は、*authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* に適切な値を指定することを表します。

（注） HTTPS トラフィックの場合、**aaa authentication secure-https-client** コマンドは不要です。

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

セキュリティ アプライアンス経由のトラフィックを TACACS+ サーバを使用したユーザ認可の対象にするか、対象から除外するかを指定するには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを ***include*** キーワードまたは ***exclude*** キーワードと共に使用します。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 {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

no aaa authorization {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

シンタックスの説明

authorization-service	認可の対象にする、または対象から除外するトラフィックのタイプを指定します。次のタイプがあります。 • **any**：すべてのトラフィックを認可します。 • **telnet**：Telnet のトラフィックを認可します。 • **ssh**：SSH のトラフィックを認可します。 • **ftp**：FTP のトラフィックを認可します。 • **http**：HTTP のトラフィックを認可します。 • **https**：HTTPS のトラフィックを認可します。 • **icmp**/*type*：指定したタイプの ICMP トラフィックを認可します。 • *proto*：指定した値または名前（**ip** や **igmp** など）の IP プロトコルを認可します。 • **tcp**/*port*[**-***port*]：指定したポートまたはポートの範囲の TCP トラフィックを認可します。すべての TCP トラフィックを認可するには、**0** に指定します。 • **udp**/*port*[**-***port*]：指定したポートまたはポートの範囲の UDP トラフィックを認可します。すべての UDP トラフィックを認可するには、**0** に指定します。 **（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、サーバが文字列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、ポート範囲を文字列としてサーバに送信します。実際には、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。ポート範囲を指定すると、サービスを個別に認可できません。
exclude	指定したサービスを認可から除外して、前に指定した規則の例外を作成します。
include	規則に合致したトラフィックを認可します。
inside-ip	認可が必要な接続の発信元または宛先となる内部（セキュリティ レベルが高い）のホストまたはネットワークの IP アドレスを指定します。このアドレスを **0** に設定すると、すべてのホストを指定できます。このコマンドでは、認可の適用対象にするインターフェイスとは無関係に、常にセキュリティの高い IP アドレスからセキュリティの低い IP アドレスの順に指定します。
inside-mask	*inside-ip* のネットワーク マスクを指定します。
interface-name	接続の開始側になるインターフェイスを指定します。

outside-ip	（オプション）トラフィックを認可する対象となる、外部の（セキュリティ レベルの低い）IP アドレスを指定します。すべてのホストを指定するには、***0*** を指定します。このコマンドでは、認可の適用対象にするインターフェイスとは無関係に、常にセキュリティの高い IP アドレスからセキュリティの低い IP アドレスの順に指定します。
outside-mask	（オプション）*outside-ip* のネットワーク マスク。
tacacs+-server-tag	**aaa-server protocol** コマンドで定義した TACACS+ 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
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** パラメータにより、ユーザが、特定のホスト（複数可）宛てのポートを指定して除外できるようになりました。

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、TACACS+ を使用してネットワーク アクセス認可を実行するように設定できます。

aaa authorization include コマンドや **exclude** コマンドの代わりに、**aaa authorization match** コマンドを使用することをお勧めします。**aaa authorization include** コマンドおよび **exclude** コマンドは、**aaa authorization match** 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。**aaa authorization match** コマンドは、アクセス リストを使用してトラフィックの一致を調べるため、この目的で使用するものとしては堅牢性の高いコマンドです。

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

認証の文と認可の文は、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、認可文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。特定の認可規則では、それに対応する認証は必要ありません。認証が必要となるのは、FTP、HTTP、または Telnet の場合だけで、認可クレデンシャルを入力するための対話型の方法がユーザに提供されます。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、認証セッションが期限切れになっていない場合、すべての規則およびタイプのいずれかで 1 回だけです。このため、トラフィックが認証文に一致した場合でも、認可は発生する可能性があります。

ユーザが認証されると、セキュリティ アプライアンスは認可規則をチェックして、一致するトラフィックがあるかどうかを調べます。トラフィックが認可文に一致した場合、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、そのトラフィックを許可するか拒否するかをユーザ プロファイルに基づいて判定し、セキュリティ アプライアンスに応答します。セキュリティ アプライアンスは、応答に含まれている認可規則を適用します。

ユーザに対してネットワーク アクセス認可を設定する方法については、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 番目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転送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 メッセージを示しています。

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

例

次の例では、TACACS+ プロトコルを使用しています。

```
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 serial console tplus1
```

この例では、最初のコマンド文で tplus1 という名前のサーバ グループを作成し、このグループ用に TACACS+ プロトコルを指定しています。2 番目のコマンドでは、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。その次の 3 つのコマンド文で指定しているのは、外部インターフェイスを経由する外部ホスト宛て接続を開始するユーザ全員を tplus1 サーバ グループで認証すること、正常に認証されたユーザに対してはどのサービスの使用も認可すること、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。最後のコマンド文では、セキュリティ アプライアンスのシリアル コンソールにアクセスするには、tplus1 サーバ グループから認証を受ける必要があることを指定しています。

次の例では、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します。

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

次の例では、内部ホストから内部インターフェイスに到着する、ICMP エコー応答パケットの認可をイネーブルにします。

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

このように設定すると、ユーザは Telnet、HTTP、または FTP を使用して認証を受けない限り、外部ホストを ping できなくなります。

次の例では、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）についてだけ認可をイネーブルにします。

```
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となる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 データベースにフォールバックするよう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+ の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 アカウンティングの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 command

管理アクセスのコマンドの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**]}

シンタックスの説明

LOCAL	ローカル コマンドの認可に、ローカル ユーザ データベースを使用することを指定します（特権レベルを使用）。TACACS+ サーバ グループ タグの後に **LOCAL** を指定すると、ローカル ユーザ データベースは、TACACS+ サーバ グループが利用できない場合のフォールバックとしてだけ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 protocol** 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

デフォルトでは、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ィセーブルになっています。

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
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)(1)	このコマンドが変更され、指定した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 データベースにフォールバックするよう管理認可を設定できるようになりました。

使用上のガイドライン

デフォルトでは、ログインすると、必要最低限のコマンドだけを使用できるユーザ EXEC モードにアクセスできるようになっています。**enable** コマンド（ローカル データベースを使用している場合は **login** コマンド）を入力すると、特権 EXEC モードにアクセスして、コンフィギュレーション コマンドを含む各種コマンドを使用できます。コマンドへのアクセスを制御する場合は、セキュリティ アプライアンスでコマンドの認可を設定して、どのコマンドをユーザが利用できるかを決めます。

次のコマンド認可方法のうちのいずれか一方を使用できます。

- ローカル データベース：**privilege** コマンドを使用して、セキュリティ アプライアンスのコマンドの特権レベルを設定します。ローカル ユーザが **enable** コマンド（**aaa authenticate enable console** コマンドでイネーブルにする）で認証を受けるか、**login** コマンドを入力してログインする場合は、セキュリティ アプライアンスが、このユーザをローカル データベース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。ローカルでのコマンド認可によって、それぞれのユーザが、ある特権レベルに置かれ、自分の特権レベル以下のコマンドを入力できるようになります。セキュリティ アプライアンスでは、コマンドに 16 レベル（0 ～ 15）のうちの 1 つを割り当てられます。デフォルトでは、各コマンドの特権レベルが 0 か 15 になっています。

（注） ローカルでのコマンド認可は、ローカル データベース内のユーザ、および CLI による認証やイネーブル認証なしで使用できます。この場合は、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力します。セキュリティ アプライアンスによって、特権レベルが 15 に設定されます。次に、各レベルのイネーブル パスワードを作成し、**enable** *n*（2 ～ 15）と入力したときに、セキュリティ アプライアンスによって該当するレベル *n* に設定されるようにします。これらのレベルは、ローカルでのコマンド認可をオンにしない限り使用されません。

- TACACS+ サーバ：ユーザまたはグループが CLI によるアクセスの認証を受けた後に使用できるコマンドを、TACACS+ サーバで設定します。ユーザが CLI で入力するすべてのコマンドが TACACS+ サーバでチェックされます。TACACS+ によるコマンドの認可をイネーブルした場合に、ユーザが CLI でコマンドを入力すると、セキュリティ アプライアンスは、そのコマンドとユーザ名を TACACS+ サーバに送信し、そのコマンドが認可されているかどうかを確かめます。

  TACACS+ によるコマンドの認可をイネーブルにする前に、TACACS+ サーバで定義されているユーザとしてセキュリティ アプライアンスにログインしていることと、セキュリティ アプライアンスの設定を続けるのに必要なコマンドの使用が認可されていることを確認してください。たとえば、全コマンドの使用が認可されている管理ユーザとしてログインします。他のユーザでログインしていると、ロックアウトされることがあります。

  TACACS+ サーバによるコマンドの認可を設定するときは、意図したとおりに認可機能が動作することを確認してから設定を保存してください。ただし、設定間違いが原因でロックアウトされた場合は、通常セキュリティ アプライアンスを再起動すると元どおりアクセスできるようになります。

  TACACS+ システムが安定していて信頼できることを確認してください。これには、通常、TACACS+ サーバ システムが完全な冗長構成になっていることと、セキュリティ アプライアンスへの完全な冗長接続があることが必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続しているサーバと、インターフェイス 2 に接続している別のサーバを含め、TACACS+ サーバが利用できない場合にローカルでのコマンド認可をフォールバックとして設定しておきます。

例

次の例は、tplus1 という名前の TACACS+ サーバ グループによるコマンド認可をイネーブルにする方法を示しています。

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

次の例は、tplus1 サーバ グループ内のすべてのサーバが利用できない場合に、ローカル ユーザ データベースにフォールバックするよう管理認可を設定する方法を示しています。

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

関連コマンド

コマンド	説明
aaa authorization	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
aaa-server host	ホスト関連のアトリビュートを設定します。
aaa-server protocol	グループ関連のサーバ アトリビュートを設定します。
clear configure aaa	設定済みの AAA アカウンティングの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 アプライアンス経由のトラフィックの TACACS+ サーバによるユーザ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。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*

シンタックスの説明

acl-name	認可するトラフィックを特定するアクセス リストの名前を指定します。**access-list** コマンドを参照してください。**permit** の ACE は、一致したトラフィックを認可することを、**deny** のエントリは認可から除外することを示します。
interface-name	接続の開始側になるインターフェイスを指定します。
server-tag	**aaa-server protocol** コマンドで定義した TACACS+ 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
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のものです。

使用上のガイドライン

セキュリティ アプライアンスでは、TACACS+ を使用してネットワーク アクセス認可を実行するように設定できます。

aaa authorization include コマンドや **exclude** コマンドの代わりに、**aaa authorization match** コマンドを使用することをお勧めします。**aaa authorization include** コマンドおよび **exclude** コマンドは、**aaa authorization match** 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。**aaa authorization match** コマンドは、アクセス リストを使用してトラフィックの一致を調べるため、この目的で使用するものとしては堅牢性の高いコマンドです。

認証の文と認可の文は、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、認可文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。特定の認可規則では、それに対応する認証は必要ありません。認証が必要となるのは、FTP、HTTP、または Telnet の場合だけで、認可クレデンシャルを入力するための対話型の方法がユーザに提供されます。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、認証セッションが期限切れになっていない場合、すべての規則およびタイプのいずれかで 1 回だけです。このため、トラフィックが認証文に一致した場合でも、認可は発生する可能性があります。

ユーザが認証されると、セキュリティ アプライアンスは認可規則をチェックして、一致するトラフィックがあるかどうかを調べます。トラフィックが認可文に一致した場合、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、そのトラフィックを許可するか拒否するかをユーザ プロファイルに基づいて判定し、セキュリティ アプライアンスに応答します。セキュリティ アプライアンスは、応答に含まれている認可規則を適用します。

ユーザに対してネットワーク アクセス認可を設定する方法については、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 番目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転送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 メッセージを示しています。

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

例

次の例では、tplus1 サーバ グループを **aaa** コマンドで使用しています。

```
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 match authen1 inside tplus1
hostname(config)#aaa accounting match acct1 inside tplus1
hostname(config)#aaa authorization match myacl inside tplus1
```

この例では、最初のコマンド文で、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 番目のコマンドでは、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 つのコマンド文では、内部インターフェイスを通過する、任意の外部ホスト宛てのすべての接続が、tplus1 サーバ グループを使用して認証され、かつアカウンティング データベースに記録されるように指定しています。最後のコマンド文では、myacl 内の ACE に一致するすべての接続が 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	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証の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 人のユーザまたは全ユーザの AAA 認可キャッシュと AAA 認証キャッシュを削除して、ユーザが次回に接続を作成するときに再認証を強制します。
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および認可の目的で認可サーバに提供されたユーザ名を表示します。また、ユーザ名がバインドされている IP アドレス、ユーザが認証されただけであるか、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 アプライアンスが所定のユーザ アカウントに対して許可するローカル ログイン試行の連続失敗回数を制限するには、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を及ぼします。この機能をディセーブルにして、ローカル ログイン試行が連続して何回失敗してもよいようにするには、このコマンドの **no** 形式を使用します。

aaa local authentication attempts max-fail *number*

シンタックスの説明

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。1 ～ 16 の数値を指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、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
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、ユーザが何回でも間違ったパスワードを入力できるようになります。

間違ったパスワードによるユーザのログイン試行が設定回数に達すると、ユーザはロックアウトされ、管理者によってユーザ名がアンロックされるまで、ログインに成功しません。ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

管理者は、デバイスからロックアウトされません。

ユーザが正常に認証された場合、またはセキュリティ アプライアンスがリブートした場合は、失敗試行回数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。

例

次の例は、**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 に設定する方法を示しています。

```
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 ステータスを消去し、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 ステータスを変更せずに、失敗したユーザ認証試行の回数を 0 にリセットします。
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

認証および認可の対象から免除する定義済みの MAC アドレス 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。**aaa mac-exempt** コマンドは、1 つだけ追加できます。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*

シンタックスの説明

id	**mac-list** コマンドで設定した MAC アドレス リストの番号を指定します。

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
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のものです。

使用上のガイドライン

aaa mac-exempt コマンドを使用するには、事前に **mac-list** コマンドを使用して MAC リストの番号を設定しておく必要があります。MAC リストにある permit のエントリは、その MAC アドレスの認証と認可を免除することを、deny のエントリは、認証と認可がイネーブルになっている場合に、その MAC アドレスを認証および認可する必要があることを示します。**aaa mac-exempt** コマンドは 1 回しか入力できないので、使用する MAC リストに、免除するすべての MAC アドレスが含まれていることを確認してください。

例

次の例では、1 つの MAC アドレスについて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、認証をバイパスしています。

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

次の例では、00a0.c95d.02b2 以外の MAC アドレスのグループの認証をバイパスしています。

```
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** コマンドで指定されている MAC アドレスのリストを表示します。
mac-list	MAC アドレスの認証や認可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 1 人あたりに許可する同時プロキシ接続の最大数を設定することで、uauth セッションの制限値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

シンタックスの説明

disable	プロキシは許可されません。
proxy_limit	ユーザ 1 人あたりに許可する同時プロキシ接続の数（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
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のものです。

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、その IP アドレスを認証の対象から除外するか、許容可能な未処理 AAA 要求の数を増やすことを検討してください。

例

次の例は、ユーザ 1 人あたりに許容可能な未処理認証要求の最大数を設定する方法を示しています。

```
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、または ASDM ユーザ認証をイネーブル化、ディセーブル化、または表示します。
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 アカウンティングの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 host

AAA サーバ グループの一部として AAA サーバを設定したり、ホスト固有の AAA サーバ パラメータを設定したりするには、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 モードに入ります。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。ホストの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*]

シンタックスの説明

(*interface-name***)**	（オプション）認証サーバが常駐するネットワーク 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何も指定しないと、デフォルトで **inside** になります（使用できる場合）。
key	（オプション）127 文字までの英数字のキーワードで、RADIUS サーバまたは TACACS+ サーバ上のキーと同じ値にします。アルファベットの大文字と小文字が区別されます。128 文字以降に入力された文字は、すべて無視されます。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やり取りする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 システムとサーバ システムの両方で同じにする必要があります。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サーバ名か、DNS 名を指定します。DNS 名の最大長は 128 文字、**name** コマンドで割り当てる名前の最大長は 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。**aaa-server protocol** コマンドで指定した名前と同じにします。
timeout *seconds*	（オプション）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
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 名をサポートするようになりました。

使用上のガイドライン

AAA サーバのコンフィギュレーションを制御するには、**aaa-server protocol** コマンドで AAA サーバ グループ プロトコルを定義してから、**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。

シングルモードでは最大 15 個のサーバ グループ、マルチモードではコンテキストごとに 4 個のサーバ グループを持つことができます。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きは、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 台ずつアクセスされます。

aaa-server host コマンドを入力したら、次に、ホスト特有のパラメータを設定します。

例

次の例では、「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 レルムを定義します。

（注） Kerberos レルム名に使用できるのは、数字と大文字のアルファベットのみです。セキュリティ アプライアンスでは、レルム名に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。必ず大文字のアルファベット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
```

次の例では、「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 に設定しています。

```
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 protocol	AAA サーバ グループを作成および修正します。
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 protocol

AAA サーバ グループを作成し、グループ固有および全グループのホストに共通した 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 protocol** コマンドを使用して、AAA サーバ グループ モードに入ります。このモードから、グループ パラメータを設定できます。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*

シンタックスの説明

server-tag	サーバ グループの名前。**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。
server-protocol	グループ内のサーバがサポートする AAA プロトコル。**kerberos**、**ldap**、**nt**、**radius**、**sdi**、または **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
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のものです。

使用上のガイドライン

AAA サーバのコンフィギュレーションを制御するには、**aaa-server protocol** コマンドで AAA サーバ グループ プロトコルを定義してから、**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。

シングルモードでは最大 15 個のサーバ グループ、マルチモードではコンテキストごとに 4 個のサーバ グループを持つことができます。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きは、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 台ずつアクセスされます。

aaa-server protocol コマンドを入力したら、次に、ホスト特有のパラメータを設定します。たとえば、AAA アカウンティングを行っている場合は、**accounting-mode** コマンドで同時アカウンティングを設定しない限り、アカウンティング情報はアクティブなサーバだけに送られます。

例

次の例は、**aaa-server protocol** コマンドを使用して、TACACS+ サーバ グループの詳細設定を変更する方法を示しています。

```
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 1 台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有効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無効になるまでに、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。

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

シンタックスの説明

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、午前 8 時は 8:00、午後 8 時は 20:00 とします。

デフォルト

開始日時を指定しない場合、permit 文または deny 文がただちに有効になります。最遅終了時刻は 23:59 31 December 2035 です。終了日時を指定しない場合、関連付けられている permit 文または deny 文はこの時刻まで有効です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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。その後、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

例

次の例では、2006 年 1 月 1 日午前 8 時に ACL が有効になります。

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

終了日時が指定されていないので、関連する ACL は無期限に有効になります。

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*** キーワードの設定をデフォルトに戻します。
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

装置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、暗号 CA トラストポイント コンフィギュレーション モードで **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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
暗号 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、IKE ピアは下位証明書と ID 証明書の両方を渡すことがあります。渡された下位証明書は、セキュリティ アプライアンスにインストールされていないことがあります。このコマンドを使用すると、装置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、装置は、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

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、トラストポイント central での下位証明書の受け入れをセキュリティ アプライアンスに許可しています。

```
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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

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*]

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

シンタックスの説明

access-list	アクセス リスト *ID*。
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	（オプション）ダウンロードしたユーザ 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
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のものです。

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、インターフェイス宛ての着信トラフィックに適用されます。**access-list** コマンド文に ***permit*** オプションを入力した場合は、セキュリティ アプライアンスはパケットの処理を続行します。**access-list** コマンド文に ***deny*** オプションを入力した場合は、セキュリティ アプライアンスはパケットを廃棄して、次の syslog メッセージを生成します。

```
%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ます。*per-user-override* オプション引数を指定しないと、セキュリティ アプライアンスは既存のフィルタリング動作を維持します。*per-user-override* を指定すると、セキュリティ アプライアンスは、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）内の ***permit*** ステータスまたは ***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 リスト内の permit ステータスまたは deny ステータスを上書きできるようにします。さらに、次の規則が適用されます。

- 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 リストが適用される。
- 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るが、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る。
- 既存のアクセス リスト ログ動作は同じである。たとえば、ユーザごとのアクセス リストによってユーザ 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、必ず **access-group** コマンドと共に使用してください。

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*** キーワードは、アクセス リストを、指定したインターフェイス上のトラフィックに適用します。***out*** キーワードは、アクセス リストを発信トラフィックに適用します。

（注） 1 つまたは複数の **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 文および deny 文）を削除すると、**access-group** コマンドが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 リストも、コメントだけを含むアクセス リストも参照できません。

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。

例

次の例は、**access-group** コマンドの使用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
```

この **static** コマンドでは、Web サーバ 10.1.1.3 にグローバル アドレス 209.165.201.3 を付与しています。**access-list** コマンドでは、すべてのホストがポート 80 を使用してグローバル アドレスにアクセスすることを許可しています。**access-group** コマンドでは、外部インターフェイスで受信するトラフィックに **access-list** コマンドを適用することを指定しています。

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。または、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

拒否フロー最大値到達メッセージ間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

シンタックスの説明

secs	拒否フロー最大値到達メッセージが生成される時間間隔。有効な値は 1 ～ 3600 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
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のものです。

使用上のガイドライン

access-list alert-interval コマンドは、syslog メッセージ 106101 を生成する時間間隔を設定します。syslog メッセージ 106101 は、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を警告します。拒否フローの最大数に達したとき、前回の 106101 メッセージが生成されてから *secs* 秒以上経過していた場合は、さらに 106101 メッセージが生成されます。

拒否フロー最大値到達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

次の例は、拒否フロー最大値到達メッセージ間の時間間隔を指定する方法を示しています。

```
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、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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトは 4096 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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のものです。

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、syslog メッセージ 106101 が生成されます。

例

次の例は、作成できる同時拒否フローの最大数を指定する方法を示しています。

```
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、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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリ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 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*}

シンタックスの説明

any	すべてのもの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	条件に合致している場合、アクセスを拒否します。
hex_number	EtherType を示す 0x600 以上の 16 ビット 16 進数値。
id	アクセス リストの名前または番号。
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	条件に合致している場合、アクセスを許可します。

デフォルト

デフォルトは次のとおりです。

- 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。
- ACL ロギングでは、拒否されたパケットについて syslog 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ときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 アプライアンスは、16 ビット 16 進数値で示された任意の EtherType を制御できます。EtherType ACL は、イーサネット V2 フレームをサポートしています。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 ユニットだけは例外で、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 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、両方向のトラフィックを通過させる場合は、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 では、MPLS ルータが、パケット転送用のラベル（アドレス）をネゴシエートできます）。

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*** に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。物理プロトコル トラフィック（オートネゴシエーションなど）だけが許可されます。

例

次の例は、EtherType アクセス リストを追加する方法を示しています。

```
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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリ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 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。1 つのアクセス リストに、同じアクセス リスト ID を持つ 1 つまたは複数の ACE が入っています。アクセス リストを使って、ネットワークへのアクセスを制御したり、各種機能で処理するトラフィックを指定したりします。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*]

シンタックスの説明

default	（オプション）ロギング方法をデフォルト（拒否パケットごとにシステム ログ メッセージ 106023 を送信）に設定します。
deny	条件を満たした場合に、パケットを拒否します。ネットワーク アクセスを制御する場合（**access-group** コマンドを使用）は、このキーワードでパケットがセキュリティ アプライアンスを通過しないようにします。クラスマップの検査を適用する場合（**class-map** と **inspect** コマンドを使用）は、このキーワードでトラフィックを検査の対象から免除します。機能の中には、ACE を拒否できないもの（NAT など）があります。詳しくは、アクセス リストを使用する各機能のコマンドの説明を参照してください。
dest_ip	パケットの送信先となるネットワークまたはホストの IP アドレスを指定します。単一の IP アドレスを指定するには、**host** キーワードに続けて IP アドレスを入力します。この場合は、マスクを入力しないでください。すべてのアドレスを指定するには、アドレスおよびマスクの代わりに **any** キーワードを入力します。
disable	（オプション）この ACE のロギングをディセーブルにします。
icmp_type	（オプション）使用するプロトコルが **icmp** の場合に、そのタイプを指定します。
id	アクセス リストの ID を 241 文字までの文字列または整数で指定します。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内で ID を区別しやすくするには、すべて大文字で指定します。
inactive	（オプション）ACE をディセーブルにします。イネーブルに戻すには、**inactive** キーワードなしで、ACE 全体を入力します。この機能を使うと、アクティブでない ACE のレコードをコンフィギュレーションに残しておけるので、イネーブルに戻しやすくなります。

interface *ifc_name*	送信元アドレスまたは宛先アドレスとしてのインターフェイス アドレスを指定します。 （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*	（オプション）システム ログ メッセージ 106100 を生成する間隔を指定します。有効な値は 1 ～ 600 秒です。デフォルトは 300 です。
level	（オプション）システム ログ メッセージ 106100 のレベル（0 ～ 7）を設定します。デフォルトは 6 です。
line *line-num*	（オプション）ACE の挿入先となる行の番号を指定します。行番号を指定しない場合、ACE はアクセス リストの末尾に追加されます。行番号は、コンフィギュレーションに保存されません。ACE を挿入する場所を指定するだけです。
log	（オプション）ネットワーク アクセスを制御（**access-group** コマンドでアクセス リストを適用）するときに、deny の ACE に一致するパケットのロギング オプションを設定します。引数なしで **log** キーワードを入力すると、デフォルトのレベル（6）のシステム ログ メッセージ 106100 がデフォルトの間隔（300 秒）で生成されます。log キーワードを入力しないと、システム ログ メッセージ 106023 のデフォルトのログが生成されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定する方法は、Cisco IOS ソフトウェアの **access-list** コマンドと異なります。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 マスクは 255.255.255.0）を使用します。一方、Cisco IOS のマスクでは、ワイルドカード ビット（0.0.0.255 など）を使います。
object-group *icmp_type_obj_grp_id*	（オプション）使用するプロトコルが **icmp** の場合に、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 グループの追加については、**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 グループの追加については、**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 グループの追加については、**object-group protocol** コマンドを参照してください。
object-group *service_obj_grp_id*	（オプション）プロトコルを **tcp** または **udp** に設定する場合に、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 グループの追加については、**object-group service** コマンドを参照してください。
operator	（オプション）発信元または宛先の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**：値の範囲。この演算子を使うときは、次の例のように、ポート番号を 2 つ指定します。 `range 100 200`

permit	条件を満たした場合に、パケットを許可します。ネットワーク アクセスを制御する場合（**access-group** コマンドを使用）は、このキーワードでパケットがセキュリティ アプライアンスを通過するようにします。クラス マップの検査を適用（**class-map** と **inspect** コマンドを使用）する場合は、このキーワードでパケットを検査の対象に含めます。
port	（オプション）プロトコルを **tcp** または **udp** に設定する場合に、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、Talk では、それぞれ TCP ポートを 1 つと UDP ポートを 1 つ定義する必要があります。TACACS+ では、TCP のポート 49 の定義が 1 つ必要です。
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 になります。
src_ip	パケットの送信元となるネットワークまたはホストの IP アドレスを指定します。単一の IP アドレスを指定するには、**host** キーワードに続けて IP アドレスを入力します。この場合は、マスクを入力しないでください。すべてのアドレスを指定するには、アドレスおよびマスクの代わりに **any** キーワードを入力します。
time-range *time_range_name*	（オプション）時間の範囲を決めて、各 ACE が特定の日時にアクティブになるようにします。時間範囲を定義する方法については、**time-range** コマンドを参照してください。

デフォルト

デフォルトは次のとおりです。

- ACE のログ機能によって、拒否パケットの syslog メッセージ 106023 が生成されます。拒否されたパケットを記録するには、deny の ACE が存在する必要があります。
- **log** キーワードを指定した場合は、syslog メッセージ 106100 のデフォルトのレベルは 6（情報）、間隔は 300 秒になります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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のものです。

使用上のガイドライン

指定した名前のアクセス リスト用に入力した各 ACE は、ACE の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 の順番は重要です。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めるときは、リストにある順番どおりに ACE を 1 つずつチェックしていきます。一致するものが見つかったら、残りの ACE は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 を作成した場合は、残りの ACE がまったくチェックされなくなります。

アクセス リストの最後には、暗黙的な拒否が設定されているので、明示的に許可しない限り、トラフィックを通過させることはできません。たとえば、セキュリティ アプライアンス経由で、特定のアドレスを除いた全ユーザにネットワークへのアクセスを許可するには、まず特定のアドレスの拒否を設定し、次に、他のすべてのアドレスを許可します。

NAT を使用する場合は、アクセス リストで指定する IP アドレスは、アクセス リストを関連付けているインターフェイスによって異なります。必ず、そのインターフェイスに接続するネットワークで有効なアドレスを使用してください。これは、着信と発信の両方のアクセス グループにあてはまります。使用するアドレスは、アクセスの方向ではなく、インターフェイス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 は、確立された双方向接続のすべてのトラフィックを許可するからです。一方、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 アプライアンスは、単方向のセッションを確立します。そのため、双方向の ICMP パケットを許可するアクセス リストを設定（発信元と宛先の両方のインターフェイスにアクセス リストを適用）するか、ICMP の検査エンジンをイネーブルにする必要があります。ICMP の検査エンジンは、ICMP セッションを双方向接続と見なします。

ICMP はコネクションレス型のプロトコルなので、双方向の ICMP パケットを許可するアクセス リストを設定（発信元と宛先の両方のインターフェイスにアクセス リストを適用）するか、ICMP の検査エンジンをイネーブルにする必要があります。ICMP 検査エンジンは、ICMP セッションをステートフル接続と見なします。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 のタイプについては、表 2-1 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（extended 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。インターフェイスにアクセス リストを適用する方法については、**access-group** コマンドを参照してください。

（注） アクセス リストの設定を変更し、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 リスト情報を使用したい場合は、**clear local-host** コマンドを使用して接続を消去します。

表 2-1 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

表 2-1　ICMP タイプのリテラル（続き）

ICMP タイプ	リテラル
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、このアクセス リストを適用するインターフェイスの全ホストからのセキュリティ アプライアンスへのアクセスを許可しています。

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

次のアクセス リストは、192.168.1.0/24 のホストから 209.165.201.0/27 のネットワークにアクセスできないようにしています。他のアドレスはすべて許可しています。

```
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
```

あるホストだけがアクセスできるようにする場合は、アクセスを限定する ACE を入力します。明示的に許可しない限り、デフォルトで他のすべてのトラフィックが拒否されます。

```
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 リストは、このアクセス リストを適用するインターフェイスの全ホストが 209.165.201.29 というアドレスの Web サイトにアクセスできないようにしています。この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
```

次のアクセス リストは、オブジェクト グループを使用して、内部ネットワークの数個のホストから、Web サーバのいくつかにアクセスできないようにしています。この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
```

あるネットワーク オブジェクト グループ（A）から別のネットワーク オブジェクト 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、次のように入力します。

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

時間ベースアクセス リストを実装するには、***time-range*** コマンドを使用して、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** コマンドを使用して、時間の範囲をアクセス リストにバインドします。次の例では、「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しています。

```
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)#
```

時間範囲を定義する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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
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。

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

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

シンタックスの説明

id	アクセス リストの名前。
line *line-num*	（オプション）コメントまたはアクセス コントロール エレメント（ACE）の挿入先となる行番号。
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
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のものです。

使用上のガイドライン

最大 100 文字（スペースや句読点を含む）をコメント テキストとして入力できます。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。空のコメントを入力することはできません。

コメントだけを含む ACL で **access-group** コマンドを使用することはできません。

例

次の例は、**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方法を示しています。

```
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、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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリ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 standard

アクセス リストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **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*}

シンタックスの説明

any	すべてのものへのアクセスを指定します。
deny	条件に合致している場合、アクセスを拒否します。説明については、「使用上のガイドライン」を参照してください。
host *ip_address*	ホスト IP アドレスへのアクセスを指定します。
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*	（オプション）ACE の挿入先となる行番号。
permit	条件に合致している場合、アクセスを許可します。説明については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトは次のとおりです。

- 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。
- ACL ロギングでは、拒否されたパケットについて syslog 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
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 コマンドと共に **deny** オプション キーワードを使用すると、パケットがセキュリティ アプライアンスを通過できなくなります。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。

TCP や UDP など、すべてのインターネット プロトコルに一致するよう *protocol* を指定するには、**ip** キーワードを使用します。

オブジェクト グループの設定方法については、**object-group** コマンドの項を参照してください。

アクセス リストをグループ化するには、**object-group** コマンドを使用します。

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場合のガイドラインは、次のとおりです。

- 32 ビットの 4 分割ドット付き 10 進数形式を使用する。
- アドレスとマスクを 0.0.0.0 0.0.0.0 にする場合は、短縮形の ***any*** キーワードを使用する。このキーワードは、IPSec では使用しないことをお勧めします。

マスクを 255.255.255.255 にする場合は、短縮形の ***host*** *address* を使用します。

例

次の例は、ファイアウォール経由の IP トラフィックを拒否する方法を示しています。

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

次の例は、条件に合致している場合に、ファイアウォール経由の IP トラフィックを許可する方法を示しています。

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

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 カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリ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 webtype

WebVPN 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*]]

シンタックスの説明

any	すべての IP アドレスを指定します。
any	（オプション）すべての URL を指定します。
deny	条件に合致している場合、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*	（オプション）syslog メッセージ 106100 を生成する時間間隔を指定します。有効値の範囲は 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*]	（オプション）ACE 用に syslog メッセージ 106100 が生成されるように指定します。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。使用できる演算子は、lt（小なり）、gt（大なり）、eq（同値）、neq（非同値）、および range（範囲）です。
permit	条件に合致している場合、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*	（オプション）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	（オプション）フィルタリングされる URL を指定します。

デフォルト

デフォルトは次のとおりです。

- 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。
- ACL ロギングでは、拒否されたパケットについて syslog 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ときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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、WebVPN フィルタリングを設定するために使用されます。指定する URL は、全体でも一部（ファイル指定なし）でもよく、サーバを示すワイルドカードを含めることも、ポートを指定することもできます。

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 ***any*** キーワードを含めて、すべての URL を指すことができます。アスタリスクを使用して、DNS 名のサブコンポーネントを指すこともできます。

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、すべての場所へのポート 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	トラフィックを EtherType に基づいて制御するためのアクセス 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、ファイアウォールを通過する 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 カウンタを消去します。
show running-config access-list	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 1 台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 グループ 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**}

シンタックスの説明

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	1 台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
AAA サーバ グループ	•	•	•	•	—

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

1 台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、***single*** キーワードを使用します。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、***simultaneous*** キーワードを使用します。

このコマンドは、アカウンティング（RADIUS または TACACS+）にサーバ グループを使用する場合に限り有効です。

例

次の例は、**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方法を示しています。

```
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 モードに入って、グループ内のすべてのホストに共通する、グループ固有の 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	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。

accounting-port

特定のホストの RADIUS アカウンティングに使用するポート番号を指定するには、AAA サーバ ホスト 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

シンタックスの説明

port	RADIUS アカウンティング用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1646 で RADIUS アカウンティングをリッスンします（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 ポート番号（1646）が使用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
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 サーバが 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、セキュリティ アプライアンスで適切なポートを設定する必要があります。

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

例

次の例では、ホスト「1.2.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、アカウンティング ポートを 2222 に設定しています。

```
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	ユーザがアクセスしたネットワーク サービスの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 モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド文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、トンネル グループ一般アトリビュート コンフィギュレーション モードで **accounting-server-group** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

accounting-server-group *server-group*

no accounting-server-group

シンタックスの説明

server-group	AAA サーバ グループの名前を指定します。デフォルトでは ***NONE*** になっています。

デフォルト

デフォルトでは、このコマンドの設定は ***NONE*** になっています。

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
トンネル グループ一般アトリビュート 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。
7.1(1)	このコマンドが、webvpn コンフィギュレーション モードからトンネル グループ一般アトリビュート コンフィギュレーション モードに変更されました。

使用上のガイドライン

すべてのトンネル グループ タイプにこのアトリビュートを適用できます。

例

トンネル グループ一般アトリビュート コンフィギュレーション モードに入る次の例では、IPSec LAN-to-LAN トンネル グループ「xyz」に「aaa-server123」という名前のアカウンティング サーバ グループを設定しています。

```
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)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

accounting-server-group（webvpn）

WebVPN または電子メール プロキシで使用するアカウンティング サーバ グループを指定するには、**accounting-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。コンフィギュレーションからアカウンティング サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、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

シンタックスの説明

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。グループ タグの最大長は 16 文字です。

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
Webvpn	•	•	—	—	•
Imap4s	•	•	—	—	•
Pop3s	•	•	—	—	•
SMTPS	•	•	—	—	•

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)	このコマンドは廃止されました。accounting-server-group コマンドは、トンネル グループ一般アトリビュート コンフィギュレーション モードで使用されるようになりました。

使用上のガイドライン

リリース 7.1(1) では、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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、WEBVPNACCT という名前のアカウンティング サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# accounting-server-group WEBVPNACCT
```

次の例は、POP3SSVRS という名前のアカウンティング サーバ グループを使用するように POP3S 電子メール プロキシを設定する方法を示しています。

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

関連コマンド

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