aaa accounting ～ accounting-server-group コマンド

aaa accounting

aaa-server host 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にしたり、ディセーブルにしたり、表示したりするには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。これら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 accounting {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

no aaa accounting {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

aaa accounting {**include** | **exclude**} *service interface-name server-tag*

no aaa accounting {**include** | **exclude**} *service interface-name server-tag*

シンタックスの説明

exclude	指定したサービスをアカウンティングから除外して、以前に記述したルールに対する例外を作成します。**exclude** パラメータでは、ユーザはサービスまたはプロトコル / ポートを指定して、特定のホスト（複数可）を除外できます。
foreign-ip	*local-ip* アドレスにアクセスするホストの 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 を使用します。*foreign-ip* アドレスは常に最も低いセキュリティ レベルのインターフェイスになります。
foreign-mask	*foreign-ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。IP アドレスが 0 の場合、0 を使用し、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名を指定します。アクセスが要求された場所と要求元を判別するには、*local-ip* アドレスと *foreign-ip* アドレスを組み合わせて *interface-name* を使用します。
include	指定したサービスに含む新しいルールを作成します。
local-ip	認証または許可するホストまたはホスト 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、すべてのホストを指定する **0** に設定し、アクセスが許可されるホストを認証サーバ側で決定させるようにできます。*local-ip* アドレスは常にセキュリティ レベルが最も高いインターフェイスになります。

local-mask	*local-ip* のネットワーク マスクを指定します。必ず、特定のマスク値を指定します。IP アドレスが 0 の場合、0 を使用し、ホストには 255.255.255.255 を使用します。
server-tag	**aaa-server host** コマンドで定義された AAA サーバ グループ タグを指定します。
service	アカウンティングを可能にするサービス / アクセス方式。アカウンティングはすべてのサービスに対して提供されますが、アカウンティングを 1 つまたは複数のサービスに制限できます。指定できる値は、**enable**、**http**、***ssh***、**telnet**、または *protocol*/*port* です。すべての TCP サービスに対してアカウンティングを提供するには、**enable** を使用します。UDP サービスに対してアカウンティングを提供するには、*protocol*/*port* 形式を使用します。

デフォルト

protocol/*port* では、TCP プロトコルは 6 と表示され、UDP プロトコルは 17 と表示されます。ポートは、TCP または UDP の宛先ポートです。ポートの値に 0（ゼロ）を使用すると、すべてのポートが指定されます。TCP または UDP 以外のプロトコルの場合、*port* は適用されず使用されません。

デフォルトでは、管理アクセスの AAA アカウンティングがディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	FWSM にこのコマンドが追加されました。

使用上のガイドライン

ユーザ アカウンティング サービスは、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。これらのレコードは、指定した AAA サーバ（複数可）に記録されます。アカウンティング情報は、同時アカウンティングをイネーブルにしている場合を除いて、サーバ グループ内のアクティブなサーバにだけ送信されます。

このコマンドを使用するには、まず **aaa-server** コマンドを使用して AAA サーバを指定する必要があります。

アクセス リストで指定された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するには、**aaa accounting match** コマンドを使用します。

（注）　**include** ステートメントで指定されていないトラフィックは処理されません。

アウトバウンド接続では、まず **nat** コマンドを使用して、FWSM にアクセスできる IP アドレスを判別します。インバウンド接続では、まず **static** と **access-list extended** コマンド ステートメントを使用して、外部ネットワークから FWSM を経由してアクセスできる内部 IP アドレスを判別します。

任意のホストからの接続を許可するには、ローカル IP アドレスとネットマスクを **0.0.0.0 0.0.0.0** または **0 0** としてコーディングします。同じ規則が、外部ホストの IP アドレスとネットマスクに適用されます。**0.0.0.0 0.0.0.0** は、外部ホストを指します。

例

次に、すべての接続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)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 mygroup
hostname(config)# aaa authorization include any inside 0 0 0 0 mygroup
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
hostname(config)# aaa authentication ssh console mygroup
```

この例では、IP アドレス 192.168.10.10 の認証サーバが内部インターフェイス上にあり、TACACS+ 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 ステートメントで指定しているのは、任意の外部ホストに対してアウトバウンド接続を開始するユーザ全員を TACACS+ 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許可すること、およびすべてのアウトバウンド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、FWSM コンソールに対する SSH アクセスには、TACACS+ サーバから認証を受ける必要があることを指定しています。

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ユーザ アカウンティングをイネーブルするために照合する必要がある、指定のアクセス リストの使用をイネーブルまたはディセーブルにします。
aaa accounting command	AAA アカウンティングの管理アクセスに対するサポートをイネーブルにします。
aaa-server host	ホストに関連する属性を設定します。
clear configure aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa accounting command

管理者が入力した各コマンドを FWSM がアカウンティング サーバに送信するようにコマンドのアカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを使用します。AAA コマンドの特権アカウンティングに対する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** コマンドは、アカウンティング レコードを生成するために、コマンドに関連付ける必要がある最低のレベルを指定します。

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

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

シンタックスの説明

server-tag	アカウンティング レコードが送信される TACACS+ サーバのサーバまたはグループ
privilege *level*	アカウンティング レコードを生成するために、コマンドに関連付ける必要がある最低のレベル。デフォルトの特権レベルは 0 です。

デフォルト

デフォルトの特権レベルは 0 です。デフォルトでは、管理アクセスの AAA コマンドの特権アカウンティングがディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

aaa accounting command コマンドを設定すると、管理者 / ユーザが入力した各コマンドが記録され、アカウンティング サーバ（複数可）に送信されます。オプションの ***privilege*** は、アカウンティング レコードを生成するために、コマンドに関連付ける必要がある最低の特権レベルを指定します。

このコマンドは、TACACS+ サーバにのみ適用されます。

aaa-server コマンドで指定し、このコマンドが適用されるサーバまたはグループの名前を指定する必要があります。

例

次に、特権レベルが 6 以上のコマンドのアカウンティング レコードを生成し、そのレコードを adminserver という名前のグループからサーバに送信するように指定する例を示します。

```
hostname(config)# aaa accounting command privilege 6 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で 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	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa accounting console

管理アクセス用の AAA アカウンティングに対する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。管理アクセス用のアカウンティングに対する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 {telnet | ssh | enable} console *server-tag*

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

シンタックスの説明

enable	特権 EXEC モードを開始および終了したときにマーク付けするアカウンティング レコードの生成をイネーブルまたはディセーブルにします。
server-tag	アカウンティング レコードが送信されるサーバまたはサーバ グループを指定します。有効なサーバ グループのプロトコルは、RADIUS および TACACS+ です。
ssh	SSH 上で作成される管理セッションを確立および終了したときにマーク付けするアカウンティング レコードの生成をイネーブルまたはディセーブルにします。
telnet	Telnet 上で作成される管理セッションを確立および終了したときにマーク付けするアカウンティング レコードの生成をイネーブルまたはディセーブルにします。

デフォルト

デフォルトでは、管理アクセスの AAA アカウンティングがディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	FWSM にこのコマンドが追加されました。
2.2(1)	このコマンドが LOCAL へのフォールバックをサポートするように変更されました。

使用上のガイドライン　**aaa-server** コマンドで指定したサーバ グループの名前を指定する必要があります。

例

次に、すべての Telnet トランザクションのアカウンティング レコードを生成し、そのレコードを adminserver という名前のサーバに送信するように指定する例を示します。

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

関連コマンド

コマンド	説明
aaa accounting match	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	指定した特権レベル以上で、管理者 / ユーザが入力したコマンド（複数可）が記録され、アカウンティング サーバ（複数可）に送信されるように指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa accounting match

アクセス リストで指定された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。アクセス リストで指定されたトラフィックに対する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** コマンドは、インターフェイス名とサーバ タグのほか、照合する必要があるアクセス リスト名を指定します。

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	照合する **access-list** 名を指定します。
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名を指定します。
server-tag	**aaa-server** コマンドで定義された AAA サーバ グループ タグを指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	FWSM にこのコマンドが追加されました。

使用上のガイドライン

acl-name は、**access-list** コマンドで定義されます。

ACL では、permit でアカウンティングが有効になり、deny でアカウンティングが無効になります。

AAA サーバ グループ タグは、**aaa-server** コマンドで定義されます。このコマンドを使用するには、まず **aaa-server** コマンドを使用して AAA サーバを指定する必要があります。

ユーザ アカウンティング サービスは、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。これらのレコードは、指定した AAA サーバ（複数可）に記録されます。アカウンティング情報は、同時アカウンティングをイネーブルにしている場合を除いて、サーバ グループ内のアクティブなサーバにだけ送信されます。**aaa accounting match** コマンドには、アカウンティング アクションを実行する前に照合するための ACL 名を指定する必要があります。

ACL 名は、数字または英数字名にすることができます。

例

次に、特定の ACL である acl2 に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。そのあとに、アクセス リストを表示する **show access-list** コマンドの出力を示します。

```
hostname(config) # aaa accounting match acl2 outside radserver1
hostname(config) # show access-list acl12
access-list acl12; 1 elements
access-list acl12 line 1 extended permit tcp any any (hitcnt=54021)
```

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で TACACS+ または RADIUS のユーザ アカウンティングをイネーブルにしたり、ディセーブルにしたり、表示したりします。
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 aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa authentication

FWSM を通過するトラフィックをユーザ認証の対象または除外にするには、グローバル コンフィギュレーション モードで ***include*** または ***exclude*** キーワードを指定して **aaa authentication** コマンドを使用します。ユーザ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。

認証では、有効なユーザ名とパスワードを要求することによって、アクセスを制御できます。FWSM を設定して、次の項目を認証できます。

- 次のセッションを含む、FWSM へのすべての管理接続：
  - Telnet
  - SSH
  - ASDM（HTTPS を使用）
  - VPN 管理アクセス
- **enable** コマンド
- FWSM 経由のネットワーク アクセス

各認証サーバには、1 つのユーザ プールがあります。複数の認証ルールとタイプで同じサーバを使用している場合、ユーザが 1 回認証を行えば、セッションの期限が終了するまですべてのルールとタイプで再び認証を行う必要がありません。たとえば、Telnet と FTP を認証するように FWSM を設定し、ユーザが正常に Telnet で認証された場合、セッションが存在するかぎり、ユーザは FTP でも認証を行う必要がありません。

aaa authentication include | **exclude** *authentication-service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*

no aaa authentication include | **exclude** *authentication-service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*

シンタックスの説明

authentication-service	選択されているサービス オプションに基づいて認証の対象または除外にするトラフィック タイプ
exclude	指定したサービスを認証から除外して、以前に記述したルールに対する例外を作成します。**exclude** パラメータは、以前の **except** オプションから改良され、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っています。
foreign-ip	（任意）認証を必要とする接続の送信元または宛先のいずれかである外部ホストの IP アドレス。***0*** は、すべてのホストを示します。
foreign-mask	（任意）*foreign-ip* のネットワーク マスク
include	指定したサービスに含む新しいルールを作成します。
interface-name	ユーザが認証を要求するインターフェイス名
local-ip	認証を必要とする接続の送信元または宛先のいずれかであるローカル / 内部ホストまたはホスト ネットワークの IP アドレス。このアドレスを **0** に設定して、すべてのホストを指定し、認証を受けるホストを認証サーバ側で決定させるようにできます。
local-mask	*local-ip* のネットワーク マスク
server-tag	AAA サーバ グループ タグは、**aaa-server** コマンドで定義されます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	FWSM にこのコマンドが追加されました。

使用上のガイドライン　トラフィックを認証の対象または除外にするには、**aaa-server** コマンドを使用して認証サーバを指定してから、**aaa authentication** コマンドを使用する必要があります。ローカル IP アドレスと外部 IP アドレスの各組み合わせでは、1 つの **aaa authentication** コマンドをインバウンド接続に、もう 1 つをアウトバウンド接続に使用できます。**aaa-server authentication** コマンドで IP アドレスが特定されるセッションは、FTP、Telnet、HTTP、または HTTPS を通じて接続を開始し、ユーザ名とパスワードの入力が求められます。ユーザ名とパスワードが、指定された認証サーバで確認された場合、FWSM で認証ホストとクライアント アドレス間の以降のトラフィックを許可します。

アクセスが要求された場所と要求元を判別するには、*interface-name*、*local-ip*、および *foreign-ip* 変数を使用します。*local-ip* アドレスは常にセキュリティ レベルが最も高いインターフェイスになり、*foreign-ip* アドレスはセキュリティ レベルが最も低いインターフェイスになります。

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

ローカル IP アドレス マスクおよび外部の IP アドレス マスクでは、IP アドレスが 0.0.0.0 の場合、***0*** を短縮形として使用できます。ホストに対しては、***255.255.255.255*** を使用します。

認証サーバは、ユーザがシステムにアクセスできるか否か、アクセス可能なサービス、ユーザによるアクセスが可能な IP アドレスを判別します。FWSM は FTP、HTTP、HTTPS、および Telnet のプロキシとして、証明書要求プロンプトを表示します。

（注）　カットスルー プロキシが設定されている場合、**nat** コマンドまたは **static** コマンドで **norandomseq** オプションを使用しているときでも、TCP セッション（Telnet、FTP、HTTP、または HTTPS）のシーケンス番号がランダム化される可能性があります。これは、AAA サーバが TCP セッションのプロキシと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。

ローカル アクセス認証

管理者を認証するように AAA サーバ（TACACS+、RADIUS、または LOCAL）を設定するには、アクセス認証サービスのオプションとして、Telnet アクセスの場合は **telnet**、SSH アクセスの場合は **ssh**、HTTP アクセスの場合は ***http***、イネーブル モードのアクセスの場合は **enable** のいずれかを選択します。

カットスルー認証

カットスルー プロキシと「トゥザボックス」認証では、**LOCAL** サーバ グループ タグを指定して、ローカル FWSM ユーザ認証のデータベースを使用することもできます。*server-tag* に **LOCAL** が指定され、ローカル ユーザのクレデンシャル 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.
```

逆に、コマンド内に **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は、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.
```

カットスルー認証サービスのオプションは、**telnet**、**ftp**、**http**、**https**、**icmp**/*type*、*proto*、**tcp**/*port*、および **udp**/*port* です。*proto* 変数には、サポートされている任意の IP プロトコル値または IP プロトコル名を指定できます。たとえば、**ip** または **igmp** を指定します。インタラクティブなユーザ認証が行われるのは、Telnet、FTP、HTTP または HTTPS トラフィックだけです。

AAA 用に FWSM がサポートしている認証ポートは、固定値です。

- FTP — ポート 21
- Telnet — ポート 23
- HTTP — ポート 80
- HTTPS — ポート 443

このため、認証の対象となるサービスのポートを再び割り当てる場合に、スタティック PAT を使用しないでください。つまり、認証するポートが既知の 3 ポートに当てはまらない場合、FWSM は接続を拒否し、サービスを認証しません。

type の ICMP メッセージ タイプ番号を入力して、特定の ICMP メッセージ タイプを認証の対象にしたり、除外したりできます。たとえば、**icmp/8** と入力すると、タイプ 8（エコー要求）ICMP メッセージが認証の対象または除外対象になります。

tcp/0 のオプションを使用すると、すべての TCP トラフィック（FTP、HTTP、HTTPS、および Telnet など）に対する認証がイネーブルになります。特定の *port* を指定した場合、指定した宛先ポートを持つトラフィックのみが認証の対象または除外対象となります。FTP、Telnet、HTTP、および HTTPS は、それぞれ **tcp/21**、**tcp/23**、**tcp/80**、および **tcp/443** と等しくなります。

ip を指定した場合、**include** および **exclude** のどちらを指定したかに応じて、すべての IP トラフィックが認証の対象または除外対象になります。すべての IP トラフィックを認証の対象にすると、次の処理が実行されます。

- ユーザを（発信元 IP に基づいて）認証する前は、FTP 要求、Telnet 要求、HTTP 要求、または HTTPS 要求を受信すると認証処理が発生し、他の IP 要求はすべて拒否されます。
- FTP 認証、Telnet 認証、HTTP 認証、HTTPS 認証、または仮想 Telnet 認証（**virtual** コマンドを参照）でユーザを認証すると、uauth がタイムアウトするまで、どのトラフィックに対しても認証処理が発生しなくなります。

認証のイネーブル化

aaa authentication コマンドを使用すると、次の機能をイネーブルまたはディセーブルにできます。

- LOCAL、TACACS+、または RADIUS サーバが提供するユーザ認証サービス。これらのサービスは、最初に **aaa-server** コマンドで指定する必要があります。FTP、Telnet、HTTP、または HTTPS を通じて接続を開始するユーザは、ユーザ名とパスワードを入力するように求められます。このユーザ名とパスワードが、指定した認証サーバで確認された場合、FWSM のカットスルー プロキシ機能は、送信元と宛先間で発生するそれ以降の FTP、Telnet、HTTP、または HTTPS トラフィックを許可します。

- Telnet、SSH、または HTTP を通じて FWSM コンソールにアクセスするための、管理認証サービス。Telnet アクセス前に **telnet** コマンドを使用する必要があります。SSH アクセスの前に **ssh** コマンドを使用する必要があります。

ユーザに表示される AAA 証明書要求プロンプトは、認証を受けて FWSM にアクセスできるサービスでそれぞれ異なります。

オプション	ログイン試行許可数	変更点
ftp	パスワードが正しくない場合、ただちに接続をドロップします。	FTP ユーザは、FTP プログラムからプロンプトを受け取ります。FTP の GUI（グラフィカル ユーザ インターフェイス）の一部には、チャレンジ値を表示しないものがあります。
http	ログインが正常に行われるまで繰り返しプロンプトが表示されます。	**aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザにはブラウザ自体が生成したポップアップ ウィンドウが表示されます。 **aaa authentication secure-http-client** を設定した場合は、ユーザ名とパスワードを収集するためのフォームがブラウザにロードされます。
telnet	4 回までログイン試行を許可し、違う場合はそれ以降の接続をドロップします。	Telnet コンソール接続の最初のコマンドライン プロンプトが表示される前

（注）　HTTP または HTTPS の場合、Web サーバと認証サーバがそれぞれ別ホスト上にある場合、正常な認証処理を実行するには **virtual** コマンドを使用します。

インターフェイス名は、**aaa authentication** コマンドで指定できます。たとえば、**aaa authentication include tcp outside 0 0** *server-tag* を指定した場合、FWSM は外部インターフェイスから発信された TCP 接続を認証します。

（注）　HTTP または HTTPS 認証の場合、認証されたあとは、FWSM uauth タイマーに小さい値が設定されている場合でも、ユーザ側で再認証が必要になることがありません。これは、ブラウザが [Basic=Uuhjksdkfhk==] の文字列をキャッシュして、特定のサイトへの後続のすべての接続に使用するためです。これがクリアされるのは、ユーザが Netscape Navigator または Internet Explorer のインスタンスをすべて終了して、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文字列はクリアされません。

TACACS+ サーバ および RADIUS サーバ

シングルモードでは最大 15 のサーバ グループ、マルチモードでは最大 4 つのサーバ グループを設定できます。各グループには、シングルモードの場合は最大 16 のサーバ、マルチモードの場合は最大 4 つのサーバを設定できます。可能なサーバは、TACACS+ または RADIUS サーバのいずれかです。**aaa-server** コマンドを使用して設定します。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。

FWSM で使用できる認証タイプは、ネットワークごとに 1 つだけです。たとえば、あるネットワークが認証に TACACS+ を使用して FWSM 経由で接続している場合、FWSM 経由で接続している別のネットワークでは RADIUS を使用して認証できますが、1 つのネットワークが TACACS+ と RADIUS の両方を使用して認証することはできません。

（注）　許可サーバが VPN 属性を実装した場合、FWSM は RADIUS 認証サーバから受信された VPN 属性を実装しません。たとえば、属性値ペア [tunnel-group=VPN] が RADIUS 認証と LDAP 許可で定義されている場合、LDAP サーバに設定されているすべての VPN リモート アクセス属性が VPN リモート アクセス トンネルで実装されます。RADIUS 認証サーバで定義されたこれらの属性は、無視されます。この動作は、トンネル グループの認証 / 許可パラメータに影響します。

例

次に、**aaa authentication** コマンドを使用する一部の例を示します。

例 1：

次の例は、[tacacs+] という名前のサーバを使用して、192.168.0.0 のローカル IP アドレスおよび 255.255.0.0 のネットマスクによる外部インターフェイスの TCP トラフィック、すべてのホストのリモート / 外部 IP アドレスによる外部インターフェイスの TCP トラフィックを認証の対象にします。2 番めのコマンドラインは、192.168.38.0 のローカル アドレスによる外部インターフェイスの Telnet トラフィック、すべてのホストのリモート / 外部 IP アドレスによる外部インターフェイスの Telnet トラフィックを認証から除外します。

```
hostname(config)# aaa authentication include tcp outside 192.168.0.0 255.255.0.0
0.0.0.0 0.0.0.0 tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0
0.0.0.0 0.0.0.0 tacacs+
```

例 2：

次の例では、*interface-name* パラメータの使用方法について説明します。FWSM 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に発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 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

例 3：

次の例では、内部ネットワークから境界ネットワークに発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 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

例 4：

次の例では、外部ネットワークから内部ネットワークに発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 outside 209.165.201.0 255.255.255.224
192.168.1.0 255.255.255.0 tacacs+
```

例 5：

次の例では、外部ネットワークから境界ネットワークに発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 outside 209.165.201.0 255.255.255.224
209.165.202.128 255.255.255.224 tacacs+
```

例 6：

次の例では、境界ネットワークから外部ネットワークに発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 inside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

例 7：

次の例では、外部インターフェイスを経由して接続を確立するときに、FWSM が 10.0.0.1 ～ 10.0.0.254 の IP アドレスを認証するように指定します。この例では、最初の **aaa authentication** コマンドがすべての FTP、HTTP、および Telnet セッションの認証を要求しています。2 番めの **aaa authentication** コマンドでは、ホスト 10.0.0.42 が認証を受けなくても送信接続を開始できるようにしています。この例は、**tacacs+** という名前のサーバ グループを使用します。

```
hostname(config)# nat (inside) 1 10.0.0.0 255.255.255.0
hostname(config)# aaa authentication include tcp inside 0 0 tacacs+
hostname(config)# aaa authentication exclude tcp inside 10.0.0.42 255.255.255.255
tacacs+
```

例 8：

次の例では、ネットワーク アドレス 209.165.201.0（サブネット マスク 255.255.255.224）を指定して、209.165.201.1 ～ 209.165.201.30 の範囲にある TCP IP アドレスへのインバウンド アクセスを許可します。**access-list** コマンドですべてのサービスが許可され、**aaa authentication** コマンドは、HTTP の認証を要求します。認証サーバは、内部インターフェイス上の IP アドレス 10.16.1.20 にあります。

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include http inside 0 0 0 0 AuthIn
```

関連コマンド

コマンド	説明
aaa authentication console	特権モードを開始するときの認証をイネーブルまたはディセーブルにするか、指定した接続タイプで FWSM にアクセスするときに認証確認を要求します。
aaa authentication match	照合を行って、一致した場合に認証を提供するアクセス リスト名（**access-list** コマンドで定義したアクセス リスト名）を指定します。
aaa authentication secure-http-client	HTTP 要求が FWSM を通過することを許可する前に、FWSM に対してセキュアなユーザ認証方法を提供します。
aaa-server protocol	グループに関連するサーバの属性を設定します。
aaa-server host	ホストに関連する属性を設定します。

aaa authentication challenge disable

FTP、Telnet、HTTP、または HTTPS の認証確認をディセーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication challenge disable** コマンドを使用します。FWSM をデフォルトの認証にリセットするには、このコマンドの **no** 形式を使用します。

aaa authentication {***ftp*** | ***telnet*** | ***http*** | ***https*** } ***challenge disable***

no aaa authentication {***ftp*** | ***telnet*** | ***http*** | ***https*** } ***challenge disable***

シンタックスの説明

ftp	FTP 接続の認証確認をディセーブルにします。
http	HTTP 接続の認証確認をディセーブルにします。
https	HTTPS 接続の認証確認をディセーブルにします。
telnet	Telnet 接続の認証確認をディセーブルにします。

デフォルト

デフォルトでは、**aaa authentication match** コマンドまたは **aaa authentication** [**include** | **exclude**] コマンドを使用して認証をイネーブルにすると、FTP、Telnet、HTTP、HTTPS で認証確認が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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM がユーザに対してユーザ名とパスワードの入力を要求するかどうかを設定できます。デフォルトでは、FWSM がプロンプトを表示し、AAA ルールによって、FTP、Telnet、HTTP、または HTTPS の新規セッションでトラフィックの認証が行われます。これらのうち 1 つ以上のプロトコルで、認証確認をディセーブルにする必要がある場合があります。その場合は、**aaa authentication challenge** コマンドを使用します。

特定のプロトコルで認証確認をディセーブルにすると、そのプロトコルを使用しているトラフィックは、既に認証済みのセッションに属している場合を除き、許可されません。この認証は、認証確認がイネーブルになっているプロトコルを使用しているトラフィックによって実行できます。たとえば、FTP で認証確認をディセーブルにすると、FWSM は、そのトラフィックが認証ルールに含まれている場合、FTP を使用した新規セッションを拒否します。認証確認がイネーブルになっているプロトコル（たとえば HTTP）を使用して新規セッションを確立した場合には、FTP トラフィックは許可されます。

例

次の例では、ネットワーク アドレス 209.165.201.0（サブネット マスク 255.255.255.224）を指定して、209.165.201.1 ～ 209.165.201.30 の範囲にある TCP IP アドレスへのインバウンド アクセスを許可しています。**access-list** コマンドはすべてのサービスを許可し、**aaa authentication** コマンドは認証を要求します。認証サーバは、内部インターフェイス上の IP アドレス 10.16.1.20 にあります。最後のコマンドは、FTP の認証確認をディセーブルにします。すなわち、**aaa authentication include** コマンドによって特定されるセッションのユーザは、FTP 以外、すなわち、Telnet、HTTP、または HTTPS によって認証を受けなければならなくなります。

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include tcp inside 0 0 0 0 AuthIn
hostname(config)# aaa authentication ftp challenge disable
```

関連コマンド

コマンド	説明
aaa authentication	トラフィックを包含または除外することによって、認証をイネーブルまたはディセーブルにします。
aaa authentication match	照合を行って、一致した場合に認証を提供するアクセス リスト名（access-list コマンドで定義したアクセス リスト名）を指定します。
aaa authentication secure-http-client	HTTP 要求が FWSM を通過することを許可する前に、FWSM に対してセキュアなユーザ認証方法を提供します。
aaa-server protocol	グループに関連するサーバの属性を設定します。
aaa-server host	ホストに関連する属性を設定します。

aaa authentication console

次の内容のいずれかを実行するには、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。

- SSH、HTTP、または Telnet 接続で FWSM コンソールにアクセスするための認証サービスをイネーブルにします。
- 特権モードへのアクセスをイネーブルにします。
- 指定したサーバ グループのリストまたはローカル 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証を設定します。

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 {**enable** | **telnet** | **ssh** | **http**} **console** *server-tag* [**LOCAL**]

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

シンタックスの説明

console	コンソールにアクセスするときに認証を要求するように指定します。
enable	特権モードを開始す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。有効なサーバ グループのプロトコルは、LOCAL、RADIUS、および TACACS+ です。
http	HTTP 上の管理セッションの認証をイネーブルまたはディセーブルにします。有効なサーバ グループのプロトコルは、LOCAL、RADIUS、および TACACS+ です。
LOCAL	***LOCAL*** キーワードには、2 つの使用方法があります。1 つめは、ローカル認証サーバの使用を指定し、2 つめは、指定された認証サーバを使用できない場合に、ローカル データベースへのフォールバックを指定できます。

server-tag	AAA サーバ グループ タグは、**aaa-server** コマンドで定義されます。
	
	LOCAL のサーバ グループ タグを指定することによって、ローカル FWSM ユーザ認証のデータベースを使用することもできます。*server-tag* に **LOCAL** が指定され、ローカル ユーザのクレデンシャル 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.`
	
	逆に、コマンド内に **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は、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.`

ssh	SSH 上の管理セッションの認証をイネーブルまたはディセーブルにします。有効なサーバ グループのプロトコルは、LOCAL、RADIUS、および TACACS+ です。
telnet	Telnet 上の管理セッションの認証をイネーブルまたはディセーブルにします。有効なサーバ グループのプロトコルは、LOCAL、RADIUS、および TACACS+ です。

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がディセーブルにされています。

aaa authentication http console *server-tag* コマンド ステートメントが定義されていない場合は、ユーザ名を指定せずに、FWSM のイネーブル パスワード（**password** コマンドで設定）を使用して FWSM（ASDM 経由）にアクセスできます。**aaa** コマンドを定義した場合でも、HTTP 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、使用不能になっていると考えられる）は、デフォルトの管理者のユーザ名とイネーブル パスワードを使用して FWSM 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。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	このコマンドが LOCAL へのフォールバックをサポートするように変更されました。

使用上のガイドライン

aaa authentication console コマンドは、特権モードを開始するときの認証をイネーブルまたはディセーブルにしたり、指定した接続タイプで FWSM にアクセスするときに認証確認を要求できるようにしたり、管理認証フォールバックをサポートしたりします。

Telnet アクセス前に **telnet** コマンドを使用する必要があります。SSH アクセスの前に **ssh** コマンドを使用する必要があります。

サーバ グループのプロトコルとして LOCAL を指定している場合を除いて、**aaa authentication console** コマンドを使用する場合、事前に **aaa-server** コマンドを使用して認証サーバを指定している必要があります。**aaa authentication console** コマンドは、RADIUS グループと TACACS+ グループをサポートしています。

「デフォルト」に記述されている内容の場合を除いて、HTTP 認証を使用している場合、FWSM は、**aaa authentication http console** コマンドを通じて、HTTP サーバの認証確認を要求します。

管理者が認証を求めるアクションを要求すると、FWSM は指定したグループのサーバとの認証セッションを開始します。システムがこのグループのサーバと通信できない場合。

指定したサーバ グループのすべてのサーバを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ように管理認証を設定するには、***LOCAL*** オプションを指定して、**aaa authentication** コマンドを使用します。この機能は、デフォルトでディセーブルです。

HTTP 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。

次の表に示されているように、**aaa authentication console** コマンドで選択したオプションに応じて、FWSM コンソールへの認証済みアクセスのプロンプト アクションは異なります。

オプション	ログイン試行許可数
enable	アクセス試行が 3 回失敗したときにアクセスを拒否します。
ssh	アクセス試行が 3 回失敗したときにアクセスを拒否します。
telnet	正常にログインするまで繰り返し表示されます。
http	正常にログインするまで繰り返し表示されます。

ssh オプションは、SSH ユーザ認証で使用される AAA サーバのグループを指定します。認証プロトコルと AAA サーバの IP アドレスは、**aaa-server** コマンド ステートメントで定義されます。

Telnet モデルと同様に、**aaa authentication ssh console** *server-tag* コマンド ステートメントを定義していない場合は、ユーザ名 ***pix*** と FWSM の Telnet パスワード（**passwd** コマンドで設定）を使用して FWSM コンソールにアクセスできます。**aaa** コマンドを定義した場合でも、SSH 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、使用不能になっていると考えられる）は、管理者の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 FWSM にアクセスできます。デフォルトでは、Telnet パスワードは **cisco** で、イネーブル パスワードは設定されていません。

ユーザに表示される AAA 証明書要求プロンプトは、認証を受けるために FWSM にアクセスできるサービス（Telnet、FTP、HTTP、HTTPS）でそれぞれ異なります。

- Telnet ユーザには、**auth-prompt** コマンドで変更できることを示すプロンプトが FWSM によって生成され表示されます。FWSM は、ログイン試行回数を制限していません。
- FTP ユーザは、FTP プログラムからプロンプトを受け取ります。ユーザの入力したパスワードが誤っている場合は、ただちに接続が中断されます。認証データベース上のユーザ名またはパスワードが、FTP を使用してアクセスするリモート ホスト上のユーザ名またはパスワードと異なる場合は、ユーザ名とパスワードを次の形式で入力します。

  ```
  authentication-user-name@remote-system-user-name
  authentication-password@remote-system-password
  ```

  FWSM 装置をデイジーチェーン接続している場合、Telnet 認証は装置が 1 台のときと同様に機能しますが、FTP および HTTP ユーザの場合は、パスワードとユーザ名ごとに「アットマーク」（@）文字を追加して、各デイジーチェーン システムのパスワードまたはユーザ名を入力する必要があります。ユーザは、デイジーチェーン接続されている装置の台数、およびパスワードの長さに応じて、63 文字までのパスワード制限を超えて入力できます。

  FTP の GUI（グラフィカル ユーザ インターフェイス）の一部には、チャレンジ値を表示しないものがあります。
- **aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザにはブラウザ自体が生成したポップアップ ウィンドウが表示されます。**aaa authentication secure-http-client** を設定した場合は、ユーザ名とパスワードを収集するためのフォームがブラウザにロードされます。どちらの場合でも、ユーザの入力したパスワードが誤っている場合は、ユーザは再入力を求められます。Web サーバと認証サーバがそれぞれ別ホスト上にある場合、正常な認証処理を実行するには **virtual** コマンドを使用します。

FWSM は、認証中に 7 ビット文字だけを受け入れます。認証後は、必要に応じて、クライアントとサーバで 8 ビット文字を使用してネゴシエートできます。認証中、FWSM は、Go-Ahead、Echo、および Network Virtual Terminal（NVT; ネットワーク仮想端末）だけをネゴシエートします。

HTTP 認証

「基本テキスト認証」または「NT チャレンジ」をイネーブルにした Microsoft IIS を実行しているサイトに対して HTTP 認証を使用すると、ユーザは Microsoft IIS サーバからアクセスを拒否されます。これは、ブラウザによって、[Authorization: Basic=Uuhjksdkfhk==] という文字列が HTTP GET コマンドに付加されるためです。この文字列には、FWSM 認証証明書が含まれます。

Microsoft Internet Information Service（IIS）サーバは、この証明書に応答して、Windows NT ユーザがサーバ上のアクセス制限付きページにアクセスしようとしているとみなします。FWSM のユーザ名とパスワードの組み合わせが、Microsoft IIS サーバ上の有効な Windows NT ユーザ名およびパスワードの組み合わせとまったく同じものである場合を除いて、この HTTP GET コマンドは拒否されます。

この問題を解決するために、FWSM には **virtual http** コマンドが用意されています。このコマンドは、ブラウザの初期接続を他の IP アドレスにリダイレクトしてユーザを認証したあとで、ユーザが要求した元の URL にブラウザをリダイレクトします。

認証されたあとは、FWSM uauth タイムアウトに小さい値が設定されている場合でも、ユーザ側で再認証が必要になることがありません。これは、ブラウザが [Authorization: Basic=Uuhjksdkfhk==] の文字列をキャッシュして、特定のサイトへの後続のすべての接続に使用するためです。これがクリアされるのは、ユーザが Netscape Navigator または Internet Explorer のインスタンスをすべて終了して、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文字列はクリアされません。

ユーザがインターネットを繰り返しブラウズする間、ブラウザは [Authorization: Basic=Uuhjksdkfhk==] 文字列を再送信して、ユーザを透過的に再認証します。

CU-SeeMe、Intel Internet Phone、MeetingPoint、MS NetMeeting などのマルチメディア アプリケーションは、内部から外部への H.323 セッションを確立する前に、バックグラウンドで HTTP サービスを起動します。

Netscape Navigator などのネットワーク ブラウザは、認証中にチャレンジ値を表示しません。このため、ネットワーク ブラウザから使用できるのはパスワード認証だけです。

（注） これらのアプリケーションの動作を妨げないようにするには、チャレンジされる全ポートを含めた包括的な送信 **aaa** コマンド ステートメント（**any** オプションを使用するものなど）を入力しないようにします。HTTP のチャレンジに使用するポートとアドレスは必要な分だけ設定し、ユーザ認証タイムアウトを設定するときは、大きめの値にします。マルチメディア プログラムの動作が妨げられると、内部からの送信セッションが確立したあとに、PC 上でエラーが発生したり、PC がクラッシュしたりする可能性があります。

TACACS+ サーバ および RADIUS サーバ

シングルモードでは最大 15 のグループ、マルチモードでは最大 4 つのグループを設定できます。各グループには、シングルモードの場合は最大 16 のサーバ、マルチモードの場合は最大 4 つのサーバを設定できます。可能なサーバは、TACACS+ または RADIUS サーバのいずれかです。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。

TACACS+ サーバでは、**aaa-server** コマンド用の鍵を指定していない場合は暗号化が使用できません。

FWSM が表示するタイムアウト メッセージは、RADIUS と TACACS+ のどちらの場合でも同じです。次のいずれかが発生した場合に、メッセージ [aaa server host machine not responding] を表示します。

- AAA サーバ システムがダウンしていたとき
- AAA サーバ システムは動作しているが、サービスが実行されていないとき

例

次に、**aaa authentication console** コマンドの使用例を示します。

例 1：

次の例では、[radius] サーバ タグを使用して、RADUIS サーバへの Telnet 接続に対して **aaa authentication console** コマンドを使用します。

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

例 2：

次の例では、管理認証用に [AuthIn] サーバ グループを指定します。

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

例 3 :

次の例では、グループ [svrgrp1] のすべてのサーバに障害が発生した場合に、LOCAL ユーザ データベースへのフォールバックに対して **aaa authentication console** コマンドを使用します。

```
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	ユーザ認証用に AAA サーバを指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa authentication match

aaa-server コマンドで指定したサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証のほか、ASDM ユーザ認証をイネーブルにするために照合する必要がある、指定のアクセス リストの使用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。指定したアクセス リストの照合に対する要件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** コマンドは、照合を行って、一致した場合に認証を提供するアクセス リスト名（access-list コマンドで定義されたアクセス リスト名）を指定します。

aaa authentication match *acl-name interface-name server-tag*

no aaa authentication match *acl-name interface-name server-tag*

シンタックスの説明

acl-name	**access-list** コマンド ステートメントの名前
interface-name	ユーザを認証するインターフェイス名
server-tag	AAA サーバ グループ タグは、**aaa-server** コマンドで定義されます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

LOCAL を指定している場合を除いて、**aaa authentication match** コマンドを使用する場合、事前に **aaa-server** コマンドを使用して認証サーバを指定し、**access-list** コマンドを使用して、名前が付けられたアクセス リストを定義している必要があります。送信元ポートを使用して一致するトラフィックを特定する **access-list** コマンド ステートメントを使用しないでください。**aaa authentication match** コマンドの一致基準では、送信元ポートがサポートされていません。

アクセスが要求された場所を定義するには、*interface-name* 変数を使用します。

カットスルー プロキシでは、***LOCAL*** のサーバ グループ タグを指定することによって、ローカル ユーザ認証のデータベースを使用することもできます。サーバ タグに ***LOCAL*** が指定され、ローカル ユーザの資格情報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 localisms.
```

逆に、コマンド内に ***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は、次の警告メッセージが表示されます。

```
Warning: local database is empty and there are still commands using 'LOCAL' for
authentication.
```

例

次の一連の例では、**aaa authentication match** コマンドの使用方法について説明します。

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 172.23.2.0 255.255.255.0
(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、その次のコマンドと同じです。

```
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 ステートメントのリストでは、**access-list** コマンド ステートメントの順序が重要です。次のコマンドを入力する場合は、その次のコマンドの前に入力します。

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

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

FWSM は、**mylist access-list** コマンド ステートメント グループで照合を試みてから、**yourlist access-list** コマンド ステートメント グループで照合を試みます。

関連コマンド

コマンド	説明
aaa authorization	LOCAL または TACACS+ ユーザ許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 aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA の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 FWSM 間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 ベースの Web 要求が FWSM を通過することを許可する前に、FWSM に対してセキュアなユーザ認証方法を提供します。

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、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.3(1)	このコマンドが追加されました。

使用上のガイドライン

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 プロキシ認証で使用されます。

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

- 許可される同時 HTTPS 認証プロセスは 16 個までです。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 番めの新しい 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 認証が機能しない場合があります。HTTPS 認証を受けたあと、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、同じ発信元 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 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、1 行めで 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 行めを追加して、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
```

- **aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザにはブラウザ自体が生成したポップアップ ウィンドウが表示されます。**aaa authentication secure-http-client** を設定した場合は、ユーザ名とパスワードを収集するためのフォームがブラウザにロードされます。どちらの場合でも、ユーザの入力したパスワードが誤っている場合は、ユーザは再入力を求められます。Web サーバと認証サーバがそれぞれ別ホスト上にある場合、正常な認証処理を実行するには **virtual** コマンドを使用します。

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。

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

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。
virtual telnet	FWSM の仮想サーバにアクセスします。

aaa authorization

指定したホストのサービスに対するユーザ許可をイネーブルまたはディセーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを使用します。指定したホストのユーザ許可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。認証サーバは、ユーザのアクセスが許可されるサーバを決定します。

aaa authorization {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

no aaa authorization {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

シンタックスの説明

exclude	指定したサービスを指定されたホストへの許可対象から除外して、以前に記述したルールに対する例外を作成します。
foreign-ip	*local-ip* アドレスにアクセスするホストの IP アドレス。すべてのホストを指定するには、0 を使用します。
foreign-mask	*foreign-ip* のネットワーク マスク。必ず、特定のマスク値を指定します。IP アドレスが 0 の場合、0 を使用し、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名アクセスが要求された場所と要求元を判別するには、*local-ip* アドレスと *foreign-ip* アドレスを組み合わせて *interface-name* を使用します。*local-ip* アドレスは常にセキュリティ レベルが最も高いインターフェイスになり、*foreign-ip* アドレスは常にセキュリティ レベルが最も低いインターフェイスになります。
include	指定したサービスに含む新しいルールを作成します。
local-ip	認証または許可するホストまたはホスト ネットワークの IP アドレス。このアドレスを **0** に設定して、すべてのホストを指定し、認証を受けるホストを認証サーバ側で決定させるようにできます。
local-mask	*local-ip* のネットワーク マスク。必ず、特定のマスク値を指定します。IP アドレスが 0 の場合、0 を使用し、ホストには 255.255.255.255 を使用します。
server-tag	**aaa-server** コマンドで定義された AAA サーバ グループ タグです。グループ タグ値に **LOCAL** を入力して、ローカルのコマンド許可特権レベルなど、ローカルのファイアウォール データベース AAA サービスを使用できます。
service	許可を要求するサービス。有効値は、**any**、**ftp**、**http**、**telnet**、または *protocol/port* です。すべての TCP サービスに対して許可を提供するには、**any** を使用します。UDP サービスに対して許可を提供するには、*protocol/port* 形式を*使用します*。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

IP アドレスを **0** にすると、「すべてのホスト」が指定されます。ローカル IP アドレスを **0** に設定すると、許可を受けるホストを許可サーバ側で決定させるようにできます。

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の許可がディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

コマンド許可と連携して使用する場合を除いて、**aaa authorization** コマンドでは事前に **aaa authentication** コマンドでの設定が必要です。ただし、**aaa authentication** コマンドには **aaa authorization** コマンドを使用する必要はありません。

FWSM は、認証が異なるプロトコルで実行されている場合にのみ、**aaa authorization** コマンドによる RADIUS 許可をサポートします。RADIUS サーバは、認証要求に対する応答とともに、許可情報を返します。**aaa authentication** コマンドの説明を参照してください。**aaa authorization** コマンドは、LOCAL サーバ（コマンドの許可でのみ）、RADIUS サーバ、または TACACS+ サーバで許可されています。FWSM に設定されていない場合でも、RADIUS サーバにダイナミック ACL を設定して、許可を提供できます。

VPN Authorization が LOCAL として定義されている場合、デフォルトのグループ ポリシーである DfltGrpPolicy に設定された属性が実装されます。これは、**tunnel-group** コマンドの設定に影響します。

IP アドレスごとに、1 つの **aaa authorization** コマンドが許可されます。**aaa authorization** で複数のサービスを許可する場合、サービス タイプに **any** パラメータを使用します。

最初の許可試行が失敗し、2 度めの試行でタイムアウトが発生した場合は、許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を再転送しないようにします。次の例は、Telnet での許可タイムアウト メッセージを示しています。

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

ユーザ許可サービスは、ユーザがアクセスできるネットワーク サービスを制御します。認証が完了したあと、アクセスの制限されているサービスにユーザがアクセスを試行すると、FWSM は指定された AAA サーバを使用してユーザのアクセス権を確認します。

（注） RADIUS 許可は、**access-list deny-flow-max** コマンド ステートメントと併せて使用する場合、および RADIUS サーバを **acl=***acl-name* ベンダー固有の識別子を使用して設定する場合にサポートされます。詳細については、**access-list deny-flow-max** コマンドのページと **authentication-port** コマンドのページを参照してください。

外部（宛先）IP アドレスを指定する場合、**0** を使用して、すべてのホストを指定します。宛先およびローカル マスクには、必ず特定のマスク値を指定します。IP アドレスが **0** の場合、**0** のマスクを使用し、ホストに対して **255.255.255.255** のマスクを使用します。

service パラメータ

指定されていないサービスは、暗黙的に許可されます。**aaa authentication** コマンド内に指定されたサービスは、許可を必要とするサービスには影響しません。

protocol/port では、次の値を指定できます。

- *protocol* — プロトコル（TCP の場合は 6、UDP の場合は 17、ICMP の場合は 1 など）

- *port* — TCP または UDP の宛先ポートまたはポート範囲。*port* には、ICMP タイプも入力できます。8 が ICMP echo または ping を表します。ポートの値に 0（ゼロ）を使用すると、すべてのポートが指定されます。ポート範囲を指定できるのは、TCP プロトコルと UDP プロトコルだけです。ICMP の場合は指定できません。TCP、UDP、および ICMP 以外のプロトコルの場合、*port* パラメータを使用しないでください。次に、ポート指定の例を示します。

  ```
  hostname(config)# aaa authorization include udp/53-1024 outside 0 0 0 0
  ```

  この例では、すべてのクライアントを対象として、内部インターフェイスに対する DNS lookup の許可をイネーブルにしています。さらに、53 ～ 1024 のポート範囲にあるほかのすべてのサービスへのアクセスを許可しています。

特定の許可ルールでは、それに対応する認証は必要ありません。認証が必要なのは、FTP、HTTP、または Telnet の場合だけです。これらのサービスでは、ユーザはインタラクティブな許可証明書の入力が可能です。

（注）　ポート範囲を指定すると、許可サーバで予期せぬ結果が生じる場合があります。FWSM は、サーバが具体的なポートに解析することを見込んで、ポート範囲を文字列でサーバに送信します。ただし、すべてのサーバがこのように動作するとは限りません。さらに、特定のサービスでユーザが許可されるようにする必要がある場合があります（これは、範囲が受け入れられる場合には、行われません）。

service オプションの有効値は、***telnet***、***ftp***、***http***、***https***、***tcp*** または ***0***、***tcp*** または *port*、***udp*** または *port*、***icmp*** または *port*、または *protocol* [/*port*] です。インタラクティブなユーザ認証が行われるのは、Telnet、FTP、HTTP、または HTTPS トラフィックだけです。

例

次に、TACACS+ プロトコルの使用例を示します。

```
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 ステートメントが 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 TACACS+ プロトコルを使用することを指定します。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り、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 ステートメントで指定しているのは、任意の外部ホストに対して外部インターフィスを経由する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許可すること、およびすべてのアウトバウンド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、FWSM コンソールに対する SSH アクセスには、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。

次に、外部インターフェイスから DNS lookup の許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 エコー応答パケットの許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 を使用して認証を受けないかぎり、外部ホストに 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）についてだけ許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	コマンドの実行が許可されるか否かを指定したり、指定したサーバグループのすべてのサーバがディセーブルにされている場合に、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許可を設定したりします。
aaa authorization match	特定の access-list コマンド名に対する LOCAL または TACACS+ ユーザ許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	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa authorization command

aaa authorization command コマンドは、コマンドの実行を許可対象とするか否かを指定します。コマンド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 command** コマンドを使用します。コマンドの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 command {LOCAL | *server-tag***}**

no aaa authorization command {**LOCAL |** *server-tag***}**

次の構文は、指定したサーバ グループのすべてのサーバがディセーブルにされている場合に、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許可を設定します。このオプションは、デフォルトではディセーブルです。

aaa authorization command *server-tag* [***LOCAL***]

no aaa authorization command *server-tag* [***LOCAL***]

シンタックスの説明

LOCAL	ローカル コマンドの許可（特権レベルを使用）に対して FWSM ローカル ユーザ データベースの使用を指定します。TACACS+ サーバ グループ タグのあとに **LOCAL** を指定した場合、TACACS+ サーバ グループが使用不可である場合に限り、コマンドの許可でローカル ユーザ データベースがフォールバックとしてのみ使用されます。
server-tag	TACACS+ 許可サーバに対して定義済みのサーバ グループ タグを指定します。**aaa-server** コマンドで定義された AAA サーバ グループ タグです。グループ タグ値に **LOCAL** を入力して、ローカルのコマンド許可特権レベルを使用することもできます。

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の許可がディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	AAA コンフィギュレーションに対する別の LOCAL 方式のサポートが追加されました。
3.1(1)	TACACS+ サーバ グループが一時的に使用できない場合の、LOCAL 許可へのフォールバックに対するサポートが追加されました。

使用上のガイドライン

コマンドの許可で使用する場合、**aaa authorization command** コマンドには、事前の **aaa authentication** コマンドでの設定は必要ありません。

aaa authorization コマンドは、TACACS+ サーバおよび LOCAL サーバ（コマンドの許可用）でサポートされていますが、RADIUS サーバではサポートされていません。

例

次に、tplus1 という名前の TACACS+ サーバ グループを使用して、コマンドの許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ように管理許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 authorization	ユーザ許可をイネーブルまたはディセーブルにします。
aaa-server host	ホストに関連する属性を設定します。
aaa-server protocol	グループに関連するサーバの属性を設定します。
clear configure aaa	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa authorization match

ユーザ許可サービスをイネーブルまたはディセーブルにするために照合する必要がある、指定のアクセス リストの使用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** コマンドを使用します。ユーザ許可サービスに対して、指定したアクセス 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。認証サーバは、ユーザのアクセスが許可されるサーバを決定します。

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	**access-list** コマンド ステートメントの名前を指定します。
interface-name	ユーザが認証を要求するインターフェイス名
server-tag	**aaa-server protocol** コマンドで定義された AAA サーバ グループ タグ

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
3.1(1)	このコマンドは、VPN 管理接続の許可に対する RADIUS サーバをサポートするように変更されました。

使用上のガイドライン

aaa authorization match コマンドでは事前に **aaa authentication** コマンドでの設定が必要です。ただし、**aaa authentication** コマンドには **aaa authorization** コマンドを使用する必要はありません。

aaa authorization コマンドは、RADIUS サーバまたは TACACS+ サーバで許可されています。**aaa authorization** コマンドによる RADIUS 許可では、FWSM に対する VPN 管理接続の許可のみをサポートしています。

ヒント　RADIUS には、認証応答で許可の属性を付加します。ネットワーク アクセスで RADIUS 認証をイネーブルにする場合は、RADIUS サーバにダイナミック ACL を設定して、許可を提供します。この場合、**aaa authorization** コマンドを使用する必要はありません。

最初の許可試行が失敗し、2 度めの試行でタイムアウトが発生した場合は、許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要求を再送信しないようにします。次の例は、Telnet での許可タイムアウト メッセージを示しています。

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

ユーザ許可サービスは、ユーザがアクセスできるネットワーク サービスを制御します。認証が完了したあと、アクセスの制限されているサービスにユーザがアクセスを試行すると、FWSM は指定された AAA サーバを使用してユーザのアクセス権を確認します。

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 ステートメントが tplus1 サーバ グループを TACACS+ グループとして定義します。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り、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 2 つのコマンド ステートメントで指定しているのは、内部インターフィスから任意の外部ホストに移動する接続を tplus1 サーバ グループで認証すること、およびこれらすべての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、myacl の ACE に一致する接続が tplus1 サーバ グループの AAA サーバの許可を受け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	ユーザ許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のパラメータをデフォルト値にリセットします。
clear uauth	ある特定のユーザまたはすべてのユーザの AAA 許可および認証キャッシュを削除します。次回接続を作成するときには再認証される必要が生じます。
show running-config aaa	AAA のコンフィギュレーションを表示します。
show uauth	認証および許可の目的で許可サーバに提供されているユーザ名、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

FWSM が所定のユーザ アカウントを許可するローカル ログイン連続失敗試行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 データベースの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 ログイン連続失敗試行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*

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、不正なパスワードの入力が許可される最大回数。この値の有効な範囲は、1 ～ 16 です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを省略すると、ローカル データベースが認証に使用されている場合に限り、ユーザが不正なパスワードを入力できる回数が無制限になります。

不正なパスワードによるログイン試行が設定数に達すると、ユーザはロックアウトされ、管理者がユーザ名のロックを解除するまで、正常にログインできません。ユーザ名がロックされるか、ロック解除されると、Syslog メッセージが生成されます。

装置から管理者をロックアウトすることはできません。

ユーザが正常に認証されるか、FWSM が再起動されると、失敗試行回数がゼロにリセットされ、ロックアウト ステータスが No にリセットされます。

例

次に、**aaa local authentication attempts max-limits** コマンドを使用して、最大失敗許可数を 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て、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 ステータスを変更することなく、ユーザ認証試行の失敗回数をゼロにリセットします。
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

事前に定義された MAC アドレスのリストの使用を認証および許可の対象から除外するように指定するには、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。MAC アドレス リストの使用を禁止するには、このコマンドの **no** 形式を使用します。**aaa mac-exempt** コマンドは、MAC アドレスのリストを認証および許可から除外します。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

シンタックスの説明

id	MAC アクセス リストの番号（**mac-list** コマンドで設定したものです）。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

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 アクセス リスト番号を設定します。認証が免除される MAC アドレスは、許可が自動的に免除されます。

例

次に、mac-exempt リストを指定する例を示します。

```
hostname(config)# aaa mac-exempt mac-list-6
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証を設定します。
aaa authorization	LOCAL または TACACS+ ユーザ認証サービスをイネーブルまたはディセーブルにします。
mac-list	初回一致の検索を使用した MAC アドレスのリストを追加します。これは MAC ベースの認証を実行する FWSM によって使用されます。

aaa proxy-limit

ユーザ 1 人に対して許可する同時プロキシ接続の最大数を設定するには、グローバル コンフィギュレーション モードで **aaa 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。ユーザ 1 人に対して 16 の同時プロキシ接続を許可するデフォルトのプロキシ制限値に戻すには、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

ディセーブル	プロキシを許可しません。
proxy_limit	ユーザ 1 人に対して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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

発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

次に、ユーザ 1 人に対して許可す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** コマンドで指定されたサーバ上で、LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルに設定したり、表示したりします。または ASDM ユーザ認証をイネーブルまたはディセーブルにしたり、表示したりします。
aaa authorization	ユーザ許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	設定した AAA アカウンティングの値を削除 / リセットします。
show running-config aaa	AAA のコンフィギュレーションを表示します。

aaa-server host

AAA サーバを設定したり、ホスト固有の AAA サーバの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場合、AAA サーバ ホスト モードを開始します。このモードでは、ホスト固有の AAA サーバの接続データを設定および管理できます。ホストの設定を削除するには、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* [*key*] [**timeout** *seconds*]

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

シンタックスの説明

(*interface-name*)	認証サーバが存在するネットワーク インターフェイス。このパラメータには、カッコが必要です。
key	（任意）127 文字までの英数字で構成されているキーワードで、RADIUS 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は区別されます。127 文字を超えて入力された文字は無視されます。このキーは、FWSM 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。キーは、FWSM 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、キーを追加したり、変更したりできます。
server-ip	AAA サーバの IP アドレス
server-tag	サーバ グループの記号名。他の AAA コマンドは、**aaa-server** コマンドの *server-tag* パラメータで定義された *server-tag* グループを参照します。
timeout *seconds*	（任意）要求のタイムアウト間隔。この値は、FWSM がプライマリ AAA サーバへの要求を断念するまでの時間です。スタンバイ AAA サーバが存在する場合、FWSM はバックアップ サーバに要求を送信します。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。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	Authentication Authorization Accounting（AAA; 認証、認可、アカウンティング）設定に関する別の LOCAL 方式をサポートするように、このコマンドが変更されました。

使用上のガイドライン

シングルモードでは最大 15 のグループ、マルチモードでは最大 4 つのグループを設定できます。各グループには、シングルモードの場合は最大 16 のサーバ、マルチモードの場合は最大 4 つのサーバを設定できます。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。

アカウンティングが有効になっている場合、**aaa-server protocol** コマンドで同時アカウンティングを指定している場合を除いて、アカウンティング情報はアクティブなサーバにだけ送信されます。

aaa-server コマンドはホスト単位のサーバ ポートの指定をサポートするように変更されたため、それぞれの動作が記述の内容のように変わり、これまでの FWSM で使用できた次のコマンド形式を徐々に廃止していくこととなりました。これは、RADIUS サーバを含むサーバ グループのみに適用されます。これらのコマンドは受け入れられますが、コンフィギュレーションには記述されません。

- **aaa-server radius-authport** [*auth-port*] **—** このコマンドは、すべての RADIUS サーバの *default* 認証ポートを制御します。これは、ホスト固有の認証ポートが指定されないと、このコマンドで指定された値が使用されることを意味します。このコマンドで値が指定されないと、デフォルトの RADIUS 認証ポート（1645）が使用されます。
- **aaa-server radius-acctport** [*acct-port*] **—** このコマンドは、前述の動作を RADIUS アカウンティング ポート（デフォルトの 1646）に適用します。

次に、すべてのホスト モードのコマンドを示します。使用できるのは、選択したサーバ グループの AAA サーバ タイプに適用されるコマンドだけです。詳細については、各コマンドの説明を参照してください。

コマンド	適用可能な AAA サーバ タイプ	デフォルト値
accounting-port	RADIUS	1646
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key[1]	RADIUS	—
	TACACS+	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 秒
	RADIUS	10 秒
sdi-pre-5-slave	SDI	—
sdi-version	SDI	sdi-5
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout[2]	すべて	10 秒

1. **aaa-server** コマンドで *key* パラメータを指定した場合、パラメータの効果は、ホスト モードで **key** コマンドを使用した場合と同じです。
2. **aaa-server** コマンドで ***timeout*** パラメータを指定した場合、パラメータの効果は、ホスト モードで **timeout** コマンドを使用した場合と同じです。

このリリースで **aaa-server** コマンドが変更されました。現在は、2 つの別個のコマンドに分かれていて、**aaa-server** *group-tag* **protocol** コマンドでグループ モードを開始し、**aaa-server host** コマンドでホスト モードを開始します。

例

次に、[1.2.3.4] のホストに [svrgrp1] という名前の SDI AAA サーバ グループを設定し、タイムアウト間隔を 6 秒、再試行間隔を 7 秒に設定し、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)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# sdi-version sdi-5
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server protocol	グループに固有の AAA サーバのパラメータを設定します。
clear configure aaa-server	すべての AAA サーバ コンフィギュレーションを削除します。
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について、AAA サーバの統計情報を表示します。

aaa-server protocol

グループに固有で、すべてのホストに共通の AAA サーバの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 モードを開始します。このモードでは、これらのグループの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 グループの記号名。他の AAA コマンドは、**aaa-server** コマンドの *server-tag* パラメータで定義された *server-tag* グループを参照します。
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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	Authentication Authorization Accounting（AAA; 認証、認可、アカウンティング）設定に関する別の LOCAL 方式をサポートするように、このコマンドが変更されました。

使用上のガイドライン

シングルモードでは最大 15 のグループ、マルチモードでは最大 4 つのグループを設定できます。各グループには、シングルモードの場合は最大 16 のサーバ、マルチモードの場合は最大 4 つのサーバを設定できます。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 アカウンティングが有効になっている場合、同時アカウンティングを設定している場合を除いて、アカウンティング情報はアクティブなサーバにだけ送信されます。

次の 2 つのコマンドを使用して AAA サーバのコンフィギュレーションを制御します。**aaa-server protocol** を使用して、AAA サーバ グループ モードを開始し、**aaa-server host** を使用して、AAA サーバ ホスト モードを開始します。さらに、**aaa-server protocol** コマンドを指定して開始するグループ モードは、**accounting-mode** コマンドと **reactivation-mode** コマンドによるアカウンティング モードとサーバ再アクティブ化機能をサポートしています。

グループ モードでサポートされているコマンドは、次のとおりです。

- **accounting-mode {simultaneous | single}**
- **no accounting-mode {simultaneous | single}**
- **reactivation-mode [depletion [deadtime** *minutes***] | timed]**
- **no reactivation-mode [depletion [deadtime** *minutes***] | timed]**
- **max-failed-attempts** *number*
- **no max-failed-attempts** *number*

これらのコマンドの詳細については、各コマンドの説明を参照してください。

例

```
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
hostname(config-aaa-server-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	特定の AAA サーバのパラメータを設定します。
accounting-mode	アカウンティング メッセージを 1 つのサーバだけに送信するか（シングル モード）、グループ内のすべてのサーバに送信するか（同時モード）を指定します。
reactivation-mode	障害が発生したサーバを再びアクティブにする方法を指定します。
max-failed-attempts	サーバ グループ内の個々のサーバが停止するまでに許容される障害回数を指定します。
clear configure aaa-server	すべての AAA サーバ コンフィギュレーションを削除します。
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について、AAA サーバの統計情報を表示します。

absolute

時間範囲が有効なとき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。この設定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。

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

no absolute [**end** *time date*] [**start** *time date*]

シンタックスの説明

date	「日 月 年」形式の日付を指定します（例：1 January 2006）。有効な年範囲は、1993 ～ 2035 です。
time	HH:MM の形式で時刻を指定します。たとえば、8:00 は午前 8 時、20:00 は午後 8 時です。

デフォルト

開始日時が指定されないと、permit または deny ステートメントが即座に有効になり、常に有効な状態になります。同様に、最大終了日時は、2035 年 12 月 31 日 23 時 59 分です。終了日時が指定されないと、対応する permit または deny ステートメントが永久に有効になります。

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	トランスペアレント	シングル	コンテキスト	システム
time-range コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

時間ベースの ACL を実行するには、***time-range*** コマンドを使用して、特定の時刻と曜日を定義します。さらに、**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。

```
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	FWSM を介して IP トラフィックを許可または拒否するポリシーを設定します。
periodic	時間範囲機能をサポートする機能に、週単位の反復する時間範囲を指定します。
time-range	時間に基づく FWSM のアクセス制御を定義します。

accept-subordinates

Subordinate Certification Authority（SCA; 下位認証局）の証明書がデバイスにインストールされていない場合に、FWSM がフェーズ 1 の IKE 交換で配信される SCA の証明書を受け入れるように設定するには、crypto 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、オンの状態です（下位認証が受け入れられます）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
crypto 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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

フェーズ 1 の処理では、IKE ピアが下位認証と ID 証明書の両方を渡す場合があり、下位認証は、FWSM にインストールされないことがあります。このコマンドを使用すると、管理者は、確立されたすべてのトラストポイントの SCA の証明書をすべて受け入れることなく、デバイスにトラストポイントとして設定されていない SCA の証明書をサポートできます。つまり、このコマンドを使用すると、デバイスはローカルにすべてのチェーンをインストールすることなく、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 crypto 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、FWSM がトラストポイント central の下位認証を受け入れるようにする例を示します。

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

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。インターフェイスからアクセス リストのマ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 リストの *id*
in	指定のインターフェイスで受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	指定のインターフェイスで送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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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、インターフェイスに着信するトラフィックに適用されます。**access-list** コマンド ステートメントに ***permit*** オプションを入力した場合、FWSM はパケットの処理を続行します。**access-list** コマンド ステートメントに ***deny*** オプションを入力した場合、FWSM 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 オプションは、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るようにします。*per-user-override* オプションの引数が指定されていない場合、FWSM は既存のフィルタリング動作を維持します。*per-user-override* が指定されている場合、FWSM は、ユーザに対応付けられたユーザ単位のアクセス リスト（ダウンロードされている場合）の ***permit*** または ***deny*** ステータスが、**access-group** コマンドに対応付けられたアクセス リストの permit または deny ステータスを上書きできるようにします。さらに、次のルールが適用されます。

- パケットが到着するときに、パケットに対応付けられたユーザ単位のアクセス リストがない場合、インターフェイスのアクセス リストが適用されます。
- ユーザ単位のアクセス 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ていますが、ユーザ単位の AAA セッションのタイムアウト値で上書きできます。
- 既存のアクセス リストのログ動作は、変わりません。たとえば、ユーザ単位のアクセス 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。ユーザ単位のアクセス リストのログ オプションには、まったく影響がありません。

access-list コマンドを使用する場合は、必ず **access-group** コマンドと併せて使用してください。

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

（注）　1 つまたは複数の **access-group** コマンドで参照されているアクセス リストから有効なエントリ（permit および deny ステートメント）をすべて削除すると、コンフィギュレーションから **access-group** コマンドが自動的に削除されます。**access-group** コマンドは、空白のアクセス リストまたはコメントだけが含まれるアクセス 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。

例

次に、**access-group** コマンドの使用例を示します。

```
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、すべてのホストに対して、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に受信するトラフィックに **access-list** コマンド文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 リストを作成したり、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。デフォルトの設定に戻すには、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	生成される拒否フローの最大メッセージの時間間隔を指定します。有効値は 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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。このメッセージは、FWSM が拒否フローの最大数に達したことを警告するものです。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。

生成される拒否フローの最大メッセージについては、**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	同時に作成できる拒否フローの最大数を指定します。
access-list extended	コンフィギュレーションにアクセス リストを追加し、それを FWSM を通過する IP トラフィックのポリシーの設定に使用します。
clear access-list	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 エントリを番号別に表示します。

access-list commit

manual-commit モードで、アクセス リストをコミットするには、グローバル コンフィギュレーション モードで **access-list commit** コマンドを使用します。

access-list commit

シンタックスの説明

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

このコマンドにはデフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

access-list mode コマンドを manual-commit に設定する場合、FWSM で使用される前に、手動でアクセス リストをコミットする必要があります。

（注）　manual-commit モードは、使用されていないアクセス リスト、または **access-group** コマンドで使用されているアクセス リストにだけ影響します。他のコンフィギュレーション コマンドで使用されているアクセス リストは、常に自動的にコミットされます。ただし、ACL モードが手動に設定されている場合は別です。その場合は、コミットされていない ACL を、Commit 機能、NAT、AAA に使用することはできません。

例

次に、アクセス リストと他のルールをコミットする例を示します。

```
fwsm/context(config)# access-list commit
```

関連コマンド

コマンド	説明
access-group	インターフェイスにアクセス リストをバインドします。
access-list extended	コンフィギュレーションにアクセス リストを追加して、FWSM を通過する IP トラフィックのポリシーを設定します。
access-list mode	manual-commit と auto-commit 間でアクセス リストのコミットメント モードを切り替えます。
clear access-list	アクセス リスト カウンタをクリアします。
object-group	コンフィギュレーションを最適化するのに使用できるオブジェクト グループを定義します。

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。デフォルトの設定に戻すには、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

デフォルトの値は、4096 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM で 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	コンフィギュレーションにアクセス リストを追加し、それを FWSM を通過する IP トラフィックのポリシーの設定に使用します。
clear access-list	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 エントリを番号別に表示します。
show running-config access-list	現在実行中のアクセス リスト設定を表示します。

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	任意の相手に対するアクセスを指定します。
bpdu	Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）に対するアクセスを指定します。デフォルトでは、BPDU が拒否されています。
deny	条件に一致した場合、アクセスを拒否します。
hex_number	EtherType を識別できる 0x600 以上の 16 ビット 16 進数
id	アクセス リストの名前または番号
ipx	IPX に対するアクセスを指定します。
mpls-multicast	MPLS マルチキャストに対するアクセスを指定します。
mpls-unicast	MPLS ユニキャストに対するアクセスを指定します。
permit	条件に一致した場合、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。

- アクセスを明確に許可しないかぎり、FWSM は発信元インターフェイスのパケットをすべて拒否します。
- アクセス リスト ロギングでは、拒否された非 IP パケットについて Syslog メッセージ 106027 が生成されます。拒否された非 IP パケットをロギングするには、必ず拒否非 IP パケットが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM は、16 ビットの 16 進数で識別される任意の EtherType を制御できます。EtherType のアクセス リストは、Ethernet V2 フレームをサポートしています。タイプ フィールドとは対照的な長さのフィールドを使用するため、アクセス リストは 802.3 形式のフレームを処理しません。アクセス リストで処理される BPDU は、唯一の例外です。BPDU は SNAP でカプセル化されています。また、FWSM は特別に BPDU を処理できるように設計されています。

EtherType はコネクションレス型なので、トラフィックを双方向に流すためには、両方のインターフェイスにアクセス リストを適用する必要があります。

MPLS を許可する場合、FWSM に接続した両方の MPLS ルータが LDP または TDP セッション用のルータ ID として FWSM 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って、LDP および TDP TCP 接続が FWSM を介して確立されるようにする必要があります（LDP および TDP によって、MPLS ルータはパケット転送用ラベル［アドレス］のネゴシエーションができます）。

インターフェイスの各方向に、各タイプ（拡張および 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することもできます。

（注） EtherType のアクセス リストが ***deny all*** に設定されている場合は、すべてのイーサネット フレームが廃棄されます。たとえば、自動ネゴシエーションなど、物理的なプロトコル トラフィックは、引き続き許可されます。

例

次に、EtherType のアクセス 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	インターフェイスにアクセス リストをバインドします。
clear access-list	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 リストを消去します。
show access-list	アクセス リスト エントリを番号別に表示します。
show running-config access-list	現在実行中のアクセス リスト設定を表示します。

access-list extended

Access Control Entry（ACE; アクセス制御エントリ）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 リストの ID を使用した 1 つまたは複数の ACE からなり、ネットワーク アクセスを制御したり、実行する多種多様な機能のトラフィックを指定したりするのに使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。すべてのアクセス リストを削除するには、**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	（任意）拒否された各パケットについてシステム ログ メッセージ 106023 を送信するデフォルトのロギング動作を設定します。
deny	条件に一致した場合、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）、このキーワードはパケットが FWSM を通過するのを防ぎます。アプリケーション検査をクラス マップに適用する場合（**class-map** コマンドと **inspect** コマンド）、このキーワードは検査からトラフィックを除外します。NAT など、一部の機能では、拒否 ACE を使用できません。アクセス リストを使用する各機能の詳細については、コマンド マニュアルを参照してください。
dest_ip	パケット宛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。IP アドレスの前に **host** キーワードを入力して、1 つのアドレスを指定します。この場合、マスクは入力しません。アドレスとマスクではなく、**any** キーワードを入力して、アドレスを指定します。
disable	（任意）この ACE のロギングをディセーブルにします。
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 リストの ID を、最長 241 文字の文字列または整数で指定します。ID は大文字と小文字を区別します。ヒント：すべての文字を大文字にすると、コンフィギュレーションに表示されるアクセス リストの ID が見やすくなります。
inactive	（任意）ACE をディセーブルにします。ACE を再イネーブルにするには、**inactive** キーワードを指定せずにすべての ACE を入力します。この機能は、ユーザがコンフィギュレーションに非アクティブの ACE のレコードを保持できるようにしているので、再イネーブルしやすくなっています。
interface *ifc_name*	送信元または宛先アドレスとしてインターフェイス アドレスを指定します。

interval *secs*	（任意）106100 のシステム ログ メッセージを生成するログ間隔を指定します。有効値は 1 ～ 600 秒です。デフォルトの値は、300 です。
level	（任意）106100 のシステム ログ メッセージ レベルを 0 ～ 7 の間で設定します。デフォルトのレベルは、6 です。
line *line-num*	（任意）ACE を挿入する行番号を指定します。ライン番号を指定しなかった場合、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は保存されません。行番号は、ACE を挿入する場所を指定するためのものです。
log	（任意）拒否 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）のパケットに一致する場合のロギング オプションを設定します。引数を指定せずに **log** キーワードを入力した場合、デフォルト間隔が 300 秒で、デフォルト レベルが 6 の、106100 のシステム ログ メッセージがイネーブルになります。log キーワードを入力しない場合、106023 のシステム ログ メッセージを使用した、デフォルトのロギングが行われます。
mask	IP アドレスのサブネット マスクネットワーク マスクを指定する場合、指定方法は、Cisco IOS ソフトウェアの **access-list** コマンドとは異なります。FWSM はネットワーク マスク（たとえば、Class C マスクの場合は 255.255.255.0）を使用します。Cisco IOS マスクは、ワイルドカード ビット（たとえば、0.0.0.255）を使用します。
object-group *icmp_type_obj_grp_id*	（任意）プロトコルが **icmp** の場合、ICMP タイプ オブジェクト グループの識別子を指定します。オブジェクト グループを追加する場合は、**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 グループの識別子を指定します。オブジェクト グループを追加する場合は、**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 グループの識別子を指定します。オブジェクト グループを追加する場合は、**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 グループの識別子を指定します。オブジェクト グループを追加する場合は、**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 —** less than：より小さい • **gt —** geater than：より大きい • **eq —** equal to：等しい • **neq —** not equal to：等しくない • **range —** 指定された値を含めた範囲。この演算子を使用する場合、たとえば、2 つのポート番号を指定します。 `range 100 200`
permit	条件に一致した場合、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）、このキーワードはパケットが FWSM を通過するのを許可します。アプリケーション検査をクラス マップに適用する場合（**class-map** コマンドと **inspect** コマンド）、このキーワードはパケットに検査を適用します。

port	（任意）プロトコルを **tcp** または **udp** に設定する場合、TCP または UDP ポートの整数または名前を指定します。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk のそれぞれには、TCP および UDP それぞれに対して 1 つの定義が必要です。TACACS+ には、TCP 上のポート 49 に対して 1 つの定義が必要です。
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。IP アドレスの前に **host** キーワードを入力して、1 つのアドレスを指定します。この場合、マスクは入力しません。アドレスとマスクではなく、**any** キーワードを入力して、アドレスを指定します。
time-range *time_range_name*	（任意）ACE に時間範囲を適用して、特定の日および週の時間に各 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対して、Syslog メッセージ 106023 を生成します。拒否されたパケットを記録する場合、必ず拒否 ACE が表示されます。
- **log** キーワードを指定する場合、Syslog メッセージ 106100 のデフォルト レベルは 6（通知）になり、デフォルトの間隔は 300 秒になります。

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

所定のアクセス リスト名に対して入力する各 ACE は、ACE に行番号を指定している場合を除いて、アクセス リストの末尾に追加されます。

ACE の順序は、重要です。FWSM がパケットを転送するか廃棄するかを判別する場合、FWSM は、エントリが表示されている順序に従って、各 ACE に対してパケットを照合します。一致したあとは、それ以上 ACE が確認されることはありません。たとえば、すべてのトラフィックを明示的に許可するアクセス リストの最初に ACE を作成した場合、それ以降のステートメントは確認されません。

暗黙の拒否ステートメントがアクセス リストの末尾に含まれているので、明示的に許可する場合を除いて、トラフィックは通過できません。たとえば、特定のアドレス以外のユーザ全員が FWSM を経由してネットワークにアクセスするようにするには、特定のアドレスを拒否してから、他のすべてのユーザを許可する必要があります。

NAT を使用する場合、アクセス リストに指定する IP アドレスは、アクセス リストが属するインターフェイスによって決まります。インターフェイスに接続した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。この注意事項は、インバウンドおよびアウトバウンド アクセス グループの両方に適用されます。使用するアドレスは方向によって左右されません。アドレスを決定付けるのはインターフェイスだけです。

TCP および UDP 接続では、リターン トラフィックを許可するためのアクセス リストを使用する必要はありません。FWSM は、確立済みの接続および双方向の接続でのすべてのリターン トラフィックを許可するからです。ただし、ICMP などのコネクションレス型プロトコルの場合は、FWSM が単一方向のセッションを確立するので、アクセス リストを使用して（送信元インターフェイスと宛先インターフェイスにアクセス リストを適用することによって）、双方向で ICMP を使用できるようにするか、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なので、アクセス リストを使用して（送信元インターフェイスと宛先インターフェイスにアクセス リストを適用することによって）、双方向で ICMP を使用できるようにするか、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 セッションをステートフル接続として扱います。ping を制御するには、**echo-reply**（**0**）（FWSM からホストへ）または **echo**（**8**）（ホストから FWSM へ）を指定します。ICMP タイプのリストについては、表 2-1 を参照してください。

インターフェイスの各方向に、各タイプ（拡張および 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 リストのコンフィギュレーションを変更し、新しいアクセス リストの情報が使用されるまで、既存の接続がタイムアウトするのを待機しない場合は、**clear local-host** コマンドを使用して、接続をクリアできます。

表 2-1 に、使用される 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（エコー応答）
3	unreachable（到達不能）
4	source-quench（送信元抑制）
5	redirect（リダイレクト）
6	alternate-address（代替アドレス）
8	echo（エコー）
9	router-advertisement（ルータ アドバタイズメント）
10	router-solicitation（ルータ送信請求）
11	time-exceeded（時間超過）
12	parameter-problem（パラメータの問題）
13	timestamp-request（タイムスタンプ要求）
14	timestamp-reply（タイムスタンプ応答）
15	information-request（情報要求）
16	information-reply（情報応答）

表 2-1　ICMP タイプのリテラル（続き）

ICMP タイプ	リテラル
17	mask-request（マスク要求）
18	mask-reply（マスク応答）
30	traceroute
31	conversion-error（変換エラー）
32	mobile-redirect（モバイル リダイレクト）

例

次のアクセス リストは、（アクセス リストが適用されるインターフェイス上の）すべてのホストに対して、FWSM の通過を許可します。

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

次のアクセス リストの例では、192.168.1.0/24 のホストに対して、209.165.201.0/27 ネットワークへのアクセスを禁止します。他のすべてのアドレスは許可されます。

```
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
```

一部のホストにアクセスを制限するには、制限を施した許可 ACE を入力します。デフォルトでは、明示的に許可されている場合を除いて、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、（アクセス リストが適用されるインターフェイス上の）すべてのホストに対して、アドレスが 209.165.201.29 の Web サイトへのアクセスを制限します。他のすべてのトラフィックは許可されます。

```
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 リストは、内部ネットワーク上の一部のホストに対して、一部の Web サーバへのアクセスを制限します。他のすべてのトラフィックは許可されます。

```
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（A）の 1 つのグループからネットワーク オブジェクト（B）の別のグループ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場合、次のようになります。

```
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、特定の日および週の時間を定義します。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。

関連コマンド

コマンド	説明
access-group	インターフェイスにアクセス リストをバインドします。
clear access-list	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	現在実行中のアクセス リスト設定を表示します。

access-list mode

manual-commit と auto-commit 間でコミットメント モードを切り替えるには、グローバル コンフィギュレーション モードで **access-list mode** コマンドを使用します。

access-list mode {**auto-commit** | **manual-commit**}

シンタックスの説明

auto-commit	ACE を追加するときに、アクセス リストを自動的にコミットします。
manual-commit	auto-commit をディセーブルにします。**access-list commit** コマンドを使用して、アクセス リストを手動でコミットする必要があります。

デフォルト

デフォルトは **auto-commit** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

アクセス リストに ACE を追加すると、FWSM はネットワーク プロセッサにアクセス リストをコミットすることによって、アクセス リストをアクティブにします。auto-commit モードの場合、最後の **access-list** コマンドを入力したあと、FWSM は短い時間待ってから、アクセス リストをコミットします。コミットメントが開始してから ACE を入力した場合、FWSM はコミットメントを打ち切り、新たな短い待機期間のあと、アクセス リストを再コミットします。FWSM はアクセス リストのコミット後に、次のようなメッセージを表示します。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

約 60K の ACE で構成される大型アクセス リストの場合、サイズに応じて、コミットに 3 ～ 4 分かかることがあります。

管理アプリケーションまたはスクリプトがアクセス リスト コミットメントをモニタして、エラーメッセージがないかどうか確認する必要がある場合、手動でアクセス リストをコミットできます。コンフィギュレーション コマンドで生じたエラーをモニタできない管理アプリケーションもあるので、ACE を追加した場合、コミットメント エラーが発生しても、管理アプリケーションがエラーを受け取らない場合もあります。ただし、管理アプリケーションがモードを manual-commit に設定した場合は、**access-list commit** コマンド（ランタイム コマンド）で発生するエラーをモニタできます。管理アプリケーションは、通常、このモードを自動的に manual-commit に設定します。

manual-commit をイネーブルにする場合、変更内容を追加するのか、削除するのかに関係なく、アクセス リストに加える変更内容を必ず手動でコミットしなければなりません。また、手動でアクセス リストをコミットしてから、インターフェイスに割り当てる必要があります（**access-group** コマンド）。アクセス リストが存在しなければ、FWSM はインターフェイスにアクセス リストを割り当てることができません。

ACE を削除して、変更内容をまだコミットしていない場合、**show running-config** コマンドは、ACE に [uncommitted deletion] のテキストを表示します。ACE を追加した場合は、追加した ACE に [uncommitted addition] のテキストが表示されます。

（注）　manual-commit モードは、使用されていないアクセス リスト、または **access-group** コマンドで使用されているアクセス リストにだけ影響します。他のコンフィギュレーション コマンドで使用されているアクセス リストは、常に自動的にコミットされます。ただし、ACL モードが手動に設定されている場合は別です。その場合は、コミットされていない ACL を、Commit 機能、NAT、AAA に使用することはできません。

例

次の例では、manual-commit モードを使用してトラフィックを中断することなく既存のアクセス リストを変更します。

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# clear configure access-list CHANGEME
fwsm(config)# access-list CHANGEME ...
! New ACE 1
fwsm(config)# access-list CHANGEME ...
! New ACE 2
fwsm(config)# ...
fwsm(config)# access-list CHANGEME ...
! New ACE N
fwsm(config)# access-list commit
```

次の例では、古いアクセス リストを削除して、別の名前の新しいアクセス リストを追加します。

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# clear config access-list old-acl
fwsm(config)# access-list new-acl Ö. : New ACE1
fwsm(config)# access-list new-acl Ö. : New ACE2
fwsm(config)# •Ö.
fwsm(config)# access-list new-acl Ö. : New ACEn
fwsm(config)# access-list commit
fwsm(config)# access-group new-acl in interface old-interface
```

前の例では、古いインターフェイス上でトラフィックがわずかに中断されます。中断される時間は、最後の 2 行のコマンド ラインでコミットを実行し、**access-group** コマンドを適用するのに必要な時間です。

次に、manual-commit モードの使用例を示します。

```
fwsm(config)# show access-list mode
ERROR: access-list <mode> does not exists
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
```

```
fwsm(config)# access-list commit
ERROR: access-list mode set to auto-commit; command ignored
fwsm(config)#
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
fwsm(config)#
fwsm(config)# access-list mode manual-commit
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted addition)
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
ERROR: access-list not committed, ignoring command
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# no access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted deletion)
fwsm(config)#
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)# #
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
fwsm(config)#
```

関連コマンド

コマンド	説明
access-list commit	manual-commit モードで、アクセス リストをコミットします。
access-list extended	コンフィギュレーションにアクセス リストを追加して、FWSM を通過する IP トラフィックのポリシーを設定します。
clear access-list	アクセス リスト カウンタをクリアします。
show access-list	アクセス リストのカウンタを表示します。
show access-list mode	システムのコンパイル モードを表示します。

access-list remark

access-list extended コマンドの前後に追加するコメント 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*

シンタックスの説明

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** コマンドの前後に追加するコメント テキスト

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。

使用上のガイドライン

コメント テキストは、スペースと句読点を含めて最長 100 文字です。コメント テキストには、スペース以外の文字を 1 つ以上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。

コメントだけからなる ACL には **access-group** コマンドを使用できません。

例

次に、**access-list** コマンドの前後に追加するコメント 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	コンフィギュレーションにアクセス リストを追加し、それを FWSM を通過する IP トラフィックのポリシーの設定に使用します。
clear access-list	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 エントリを番号別に表示します。
show running-config access-list	現在実行中のアクセス リスト設定を表示します。

access-list standard

アクセス リストを追加して、OSPF ルート（OSPF 再配布用のルート マップに使用可）の宛先 IP アドレスを特定するには、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	任意の相手に対するアクセスを指定します。
deny	条件に一致した場合、アクセスを拒否します。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。
host *ip_address*	ホストの IP アドレスに対する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 アドレスとサブネット マスクに対する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	条件に一致した場合、アクセスを許可します。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

デフォルトの設定は次のとおりです。

- アクセスを明確に許可しないかぎり、FWSM は発信元インターフェイスのパケットをすべて拒否します。
- 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ギングする場合、必ず拒否パケットが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

access-group コマンドとともに **deny** オプションを使用すると、パケットが FWSM を通過することが禁止されます。デフォルトでは、個々のアクセスを明確に許可しないかぎり、FWSM は発信元インターフェイスのパケットをすべて拒否します。

protocol を指定して、TCP および UDP を含むすべてのインターネット プロトコルに一致させる場合は、キーワード **ip** 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 リストをグループにまとめるには、**object-group** コマンドを使用します。

発信元アドレス、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注意事項は、次のとおりです。

- 32 ビットの 4 分割ドット付き 10 進数形式を使用してください。
- 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*** キーワードを使用します。このキーワードを、IPSec で使用することは推奨しません。

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

次に、ファイアウォールを通過する 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、条件が一致した場合に、ファイアウォールを通過する 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
```

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を最適化するのに使用できるオブジェクト グループを定義します。
clear access-list	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 エントリを番号別に表示します。
show running-config access-list	現在実行中のアクセス リスト設定を表示します。

accounting-mode

アカウンティング メッセージが 1 つのサーバ（single モード）に送信されるか、グループ内のすべてのサーバ（simultaneous モード）に送信されるかを指定するには、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 モードの指定を解除するには、このコマンドの **no** 形式を使用します。

accounting-mode simultaneous

accounting-mode single

no accounting-mode

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 つ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 single 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	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

1 つ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、サーバ グループがアカウンティング（RADIUS または TACACS+）に対して使用され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
```

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 モードを開始して、グループに固有で、グループ内のすべてのホストに共通の AAA サーバの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 サーバ コンフィギュレーションを削除します。
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について、AAA サーバの統計情報を表示します。

accounting-port

このホストの RADIUS アカウンティングで使用され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解除するには、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 アカウンティングのポート番号（1 ～ 65535 の範囲）

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待ち受けます（RFC 2058 に準拠）。ポートが指定されていない場合、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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	**aaa-server radius-acctport** コマンドに代わって、このコマンドが追加されました。

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している場合、**aaa-server** コマンドで RADIUS サービスを起動する前に、FWSM に適切なポートを設定する必要があります。

ヒント　RFC 2139 によって、RADIUS アカウンティングの標準ポートがポート 1813 に変更されました。

このコマンドは、RADIUS 用に設定されているサーバ グループでのみ有効です。

例

次に、ホスト [1.2.3.4] に [svrgrp1] という名前の RADIUS AAA サーバを設定する例を示します。タイムアウトを 9 秒、再試行間隔を 7 秒に設定し、アカウンティング ポート 2222 を設定します。

```
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 モードを開始して、ホスト固有の AAA サーバのパラメータを設定できるようにします。
clear configure aaa-server	コンフィギュレーションから AAA コマンド ステートメント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について、AAA サーバの統計情報を表示します。

accounting-server-group

アカウンティング レコードを送信する AAA サーバ グループを指定するには、tunnel-group general-attributes 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。デフォルトの設定に戻すには、このコマンドの ***no*** 形式を使用します。

[no] accounting-server-group *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。デフォルトは、***NONE*** です。

デフォルト

このコマンドのデフォルト設定は、***NONE*** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

すべてのトンネルグループ タイプにこの属性を適用できます。

例

次に、config-general コンフィギュレーション モードで、IPSec LAN 間トンネル 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 グループを設定する例を示します。

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
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 グループ設定を表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。