CHAPTER 2

A ～ B のコマンド

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化、ディセーブル化、または表示するには、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、以前に記述した規則に対する例外を作成します。**exclude** パラメータにより、特定のホスト（複数可）宛てのサービスまたはプロトコル / ポートを指定して除外できます。
foreign-ip	*local-ip* アドレスからのアクセス先となるホストの 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、セキュリティ レベルの最も低いインターフェイス上にあります。
foreign-mask	*foreign-ip* のネットワーク マスクを指定します。常に特定のマスク値を指定します。IP アドレスが 0 である場合は、0 を使用します。ホストには 255.255.255.255 を使用します。
interface-name	ユーザからの認証要求の送信元となるインターフェイス名を指定します。アクセスの要求元および送信者を指定するには、*interface-name* を *local-ip* アドレスおよび *foreign-ip* アドレスと組み合せて使用します。
include	指定したサービスに含む新しい規則を作成します。
local-ip	認証または認可を受けるホスト、またはホストのネットワークの IP アドレスを指定します。すべてのホストを指定して、アクセスが許可されるホストを認証サーバ側で決定するには、このアドレスを 0 に設定します。*local-ip* アドレスは、常に、セキュリティ レベルの最も高いインターフェイス上にあります。

local-mask	*local-ip* のネットワーク マスクを指定します。常に特定のマスク値を指定します。IP アドレスが 0 である場合は、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 タグを指定します。
service	アカウンティングが提供されるサービス（アクセス方式）。アカウンティングはすべてのサービスに提供されますが、特定のサービス（複数可）にだけ提供することもできます。指定できる値は、**enable**、**http**、***serial***、***ssh***、**telnet**、または *protocol*/*port* です。すべての TCP サービスにアカウンティングを提供するには、**enable** を使用します。アカウンティングを UDP サービスに提供するには、*protocol*/*port* 形式を使用します。

デフォルト

protocol/*port* 形式では、たとえば 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。ポート値を 0 にすると、すべてのポートを指定します。TCP および UDP 以外のプロトコルの場合、*port* は適用できないため、使用しないでください。

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。

コマンドのモード

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
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

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。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。

このコマンドを使用するには、事前に **aaa-server** コマンドを使用して 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した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。

（注） **include** 文によって指定されていないトラフィックは処理されません。

発信接続については、まず **nat** コマンドを使用して、セキュリティ アプライアンスにアクセスできる IP アドレスを定義します。着信接続については、まず **static** コマンド文と **access-list extended** コマンド文を使用して、外部ネットワークからセキュリティ アプライアンス経由でどの内部 IP アドレスにアクセスできるかを定義します。

あらゆるホストからの受信接続を許可する場合は、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** と記述します。外部ホストの IP アドレスとネットマスクについても、表記は同じです。すべての外部ホストを指定するには、**0.0.0.0 0.0.0.0** と記述します。

例

次の例では、すべての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 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 serial 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ること、および 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 つのコマンド文で指定しているのは、外部ホスト宛ての発信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、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にするために一致する必要のある特定のアクセス 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	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。
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 command

管理者によって入力された各コマンドをセキュリティ アプライアンスがアカウンティング サーバに送信するようにコマンド 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 特権コマンド 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** コマンドでは、アカウンティング レコードが生成されるコマンドに関連付けられている必要のある最低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 レコードの送信先となるサーバまたは TACACS+ サーバ グループ。
privilege *level*	アカウンティング レコードが生成されるコマンドに関連付けられている必要のある最低レベル。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、管理者アクセス権の AAA 特権コマンド アカウンティングはディセーブルになっています。

コマンドのモード

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
7.0(1)	このコマンドに管理オプションが追加されました。

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）によって入力され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。オプションで指定できる ***privilege*** は、アカウンティング レコードが生成されるコマンドに関連付けられている必要のある最低の特権レベルを示します。

このコマンドは、TACACS+ サーバだけに適用されます。

このコマンドを適用する先のサーバ名またはグループ名（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、特権レベル 6 以上のすべてのコマンド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 という名前のグループのサーバに送信されるよう指定しています。

```
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またはディセーブルにします。
http	HTTP を介して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またはディセーブルにします。
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 レコードの送信先とな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 プロトコルは、RADIUS および TACACS+ です。
ssh	SSH を介して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またはディセーブルにします。
telnet	Telnet を介して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。

コマンドのモード

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
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 match

アクセスリストで指定した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、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した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** コマンドでは、照合用のアクセスリスト名、およびインターフェイス名とサーバ タグを指定します。

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	トラフィックを照合する ACL の名前を指定します。この ACL に一致したトラフィックについて、セキュリティ アプライアンスがアカウンティングを実行します。*acl-name* 引数は、**access-list** コマンドで作成した ACL の名前である必要があります。
interface-name	ユーザからのアカウンティング要求の送信元となるインターフェイス名を指定します。
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。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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 accounting match コマンドでは、ACL を指定する必要があります。この ACL で許可されたトラフィックについて、セキュリティ アプライアンスがアカウンティング データを AAA サーバに送信します。セキュリティ アプライアンスは、ACL で許可されたトラフィックのアカウンティングを実行し、ACL で拒否されたトラフィックのアカウンティングを実行しません。

このコマンドを使用するには、事前に **aaa-server protocol** コマンドを使用して AAA サーバ グループ タグを作成しておく必要があります。

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 サーバに記録されます。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。詳細については、**accounting-mode** コマンドを参照してください。

例

次の例では、acl2 という名前の ACL 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してから、**show access-list** コマンドで ACL を表示しています。

```
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の TACACS+ または RADIUS のユーザ アカウンティングをイネーブル化、ディセーブル化、または表示します。
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

セキュリティ アプライアンス経由のトラフィックをユーザ認証の対象にするか、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 authentication** コマンドを ***include*** キーワードまたは ***exclude*** キーワードとともに使用します。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。セキュリティ アプライアンスでは、次の項目の認証を設定できます。

- 次のセッションを含む、セキュリティ アプライアンス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
- セキュリティ アプライアンス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。同じサーバで複数の認証規則および認証タイプを使用する場合、ユーザに必要な認証は、セッションが期限切れになるまでは、すべての規則とタイプに対して 1 回だけです。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、Telnet の認証に成功したユーザは、その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。

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*

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

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にするか、対象から除外するトラフィックのタイプ。
exclude	指定したサービスを認証から除外して、以前に記述した規則に対する例外を作成します。**exclude** パラメータでは、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ため、以前の **except** オプションよりも機能が向上しています。
foreign-ip	（オプション）認証を要求する接続の送信元または宛先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	（オプション）*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規則を作成します。
interface-name	ユーザからの認証要求の送信元となるインターフェイス名。
local-ip	認証を要求する接続の送信元または宛先であるローカル（内部）ホスト、またはホストのネットワークの IP アドレス。すべてのホストを指定して、認証を受けるホストを認証サーバ側で決定するには、このアドレスを **0** に設定します。
local-mask	*local-ip* のネットワーク マスク。
server-tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグ。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　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
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　トラフィックを認証の対象にするか、対象から除外するには、**aaa authentication** コマンドを使用する前に、**aaa-server** コマンドで認証サーバを指定しておく必要があります。ローカル IP アドレスと外部 IP アドレスの組み合せごとに、着信接続用の 1 つの **aaa authentication** コマンドと、発信接続用のもう 1 つの **aaa authentication** コマンドを指定できます。**aaa-server authentication** コマンドで指定した IP アドレスのセッションでは、FTP、Telnet、HTTP、または HTTPS を介した接続が開始されると、ユーザ名とパスワードが要求されます。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ると、セキュリティ アプライアンスは、認証ホストとクライアント アドレスの間で発生する以降のトラフィックを許可します。

アクセスの要求元および送信者を指定するには、*interface-name* 変数、*local-ip* 変数、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 レベルの最も高いインターフェイス上にあります。*foreign-ip* アドレスは、常に、セキュリティ レベルの最も低いインターフェイス上にあります。

（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。この場合は、**aaa authentication match** コマンドを使用する必要があります。

ローカル IP アドレスおよび外部 IP アドレスのマスクには、IP アドレスが 0.0.0.0 の場合の短縮表現として ***0*** を使用できます。ホストに対しては ***255.255.255.255*** を使用します。

ユーザがシステムにアクセスできるかどうか、どのサービスにアクセスできるか、およびどの IP アドレスにアクセスできるかは、認証サーバが決定します。セキュリティ アプライアンスは FTP、HTTP、HTTPS、および Telnet を代行処理して、クレデンシャル プロンプトを表示します。

（注）　カットスルー プロキシを設定する場合は、**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。

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のいずれかを選択します。つまり、シリアル コンソール アクセスの場合は ***serial***、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 アクセスの場合は **enable** を選択します。

カットスルー認証

カットスルー プロキシ認証と装置にアクセスする場合の認証では、サーバ グループ タグ **LOCAL** を使用することで、ローカルのセキュリティ アプライアンス ユーザ認証データベースも使用できます。*server-tag* に **LOCAL** を指定する場合、ローカル ユーザ クレデンシャル データベースが空のときは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。変数 *proto* 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** や **igmp** を指定します。対話型のユーザ認証は、Telnet トラフィック、FTP トラフィック、HTTP トラフィック、HTTPS トラフィックでだけトリガーします。

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

このため、スタティック PAT を使用して、認証の対象となるサービスのポートを再割り当てしないでください。認証するポートが既知の 3 ポートのいずれでもない場合、セキュリティ アプライアンスはサービスを認証せずに接続を拒否します。

ICMP メッセージ タイプ番号を *type* に入力すると、特定の ICMP メッセージ タイプを認証の対象にしたり、対象から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 オプションを指定すると、すべての TCP トラフィックが認証の対象になります。TCP トラフィックには、FTP、HTTP、HTTPS、および Telnet が含まれます。特定の *port* を指定すると、これに一致する宛先ポートが指定されたトラフィックだけが認証の対象または除外対象になります。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 を指定すると、**include** または **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（送信元 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る。
- 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る。

認証のイネーブル化

aaa authentication コマンドは、次の機能をイネーブルまたはディセーブルにします。

- LOCAL サーバ、TACACS+ サーバ、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 を介し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によって確認された場合、セキュリティ アプライアンスのカットスルー プロキシ機能により、送信元と宛先の間で発生する以降の FTP トラフィック、Telnet トラフィック、HTTP トラフィック、または HTTPS トラフィックが許可されます。
- Telnet、SSH、HTTP、またはシリアル コンソールを介してセキュリティ アプライアンス コンソールにアクセスするための、管理認証サービス。Telnet でアクセスする場合は、先に **telnet** コマンドを使用する必要があります。SSH でアクセスする場合は、先に **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 クレデンシャル要求プロンプトは、認証を受けてセキュリティ アプライアンスにアクセスできるサービス（Telnet、FTP、HTTP、および HTTPS）でそれぞれ異なります。

オプション	許可されるログイン試行の数	注意事項
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。	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 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	ログインが成功するまで、何回でもプロンプトが再表示される。	**aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザには、ブラウザ自身によって生成されたポップアップ ウィンドウが表示されます。**aaa authentication secure-http-client** が設定されている場合、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 回失敗すると接続がドロップされる。	Telnet コンソール接続の最初のコマンドライン プロンプトの前。

（注）　HTTP または HTTPS で、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* と指定した場合、セキュリティ アプライアンスは外部インターフェイスから送信される TCP 接続を認証します。

（注）　HTTP 認証または HTTPS 認証の場合、セキュリティ アプライアンスの uauth タイマー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 Netscape Navigator または Internet Explorer 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。

TACACS+ サーバと RADIUS サーバ

最大 15 個のシングルモード サーバ グループまたは 4 個のマルチモード 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。サーバは、**aaa-server** コマンドで設定した TACACS+ サーバまたは RADIUS サーバです。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。

セキュリティ アプライアンス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+ を使用してセキュリティ アプライアンス経由で接続している場合、セキュリティ アプライアンス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。しかし、1 つのネットワークで TACACS+ と RADIUS の両方を使用して認証することはできません。

（注） 認可サーバによって VPN アトリビュートが適用される場合、セキュリティ アプライアンスは、RADIUS 認証サーバによって適用される VPN アトリビュートを適用しません。これは、認証後に認可が行われるためです。たとえば、RADIUS 認証と LDAP 認可にアトリビュート値ペア「tunnel-group=VPN」が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 アトリビュートが VPN リモートアクセス トンネルに適用されます。RADIUS 認証サーバによって定義されているアトリビュートは無視されます。この動作は、トンネルグループ、webvpn、pop、imap、および smtps の認証パラメータおよび認可パラメータに影響を及ぼします。

例

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

例 1：

次の例では、ローカル IP アドレスが 192.168.0.0（ネットマスク 255.255.0.0）で、リモート（外部）IP アドレスが任意のホストである、外部インターフェイス上の TCP トラフィックを、「tacacs+」という名前のサーバによる認証の対象としています。2 番目のコマンドラインでは、ローカル アドレスが 192.168.38.0 で、リモート（外部）IP アドレスが任意のホストである、外部インターフェイス上の Telnet トラフィックを認証の対象外としています。

```
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 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 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 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 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 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、IP アドレス 10.0.0.1 ～ 10.0.0.254 が外部インターフェイス経由で接続を確立するときに、セキュリティ アプライアンスによる認証を受ける必要があるように指定しています。この例では、最初の **aaa authentication** コマンドで、すべての FTP セッション、HTTP セッション、および Telnet セッションの認証を要求しています。2 番目の **aaa authentication** コマンドでは、10.0.0.42 が認証を受けなくても発信接続を開始できるようにしています。この例では、**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 アドレスへの着信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を許可し、**aaa authentication** コマンドで HTTP に対する認証を要求します。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を提供します。
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

次のいずれかを行う場合は、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 接続、HTTP 接続、または Telnet 接続を介して、あるいはセキュリティ 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。
- 特権モードへのアクセスをイネーブルにする。
- 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する。

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**]

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

シンタックスの説明

console	コンソールへのアクセスに認証が必要であることを指定します。
enable	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。有効なサーバ グループ プロトコルは、LOCAL、RADIUS、および TACACS+ です。
http	HTTP を介した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 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。ローカル認証サーバを使用するように指定できます。また、指定した認証サーバが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指定できます。
serial	コンソールへのシリアル インターフェイス上で確立される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 プロトコルは、LOCAL、RADIUS、および TACACS+ です。

server-tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグ。
	
	カットスルー プロキシ認証と装置にアクセスする場合の認証では、サーバ グループ タグ **LOCAL** を使用することで、ローカルのセキュリティ アプライアンス ユーザ認証データベースも使用できます。*server-tag* に **LOCAL** を指定する場合、ローカル ユーザ クレデンシャル データベースが空のときは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 を介した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 プロトコルは、LOCAL、RADIUS、および TACACS+ です。
telnet	Telnet を介した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 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はディセーブルになっています。

aaa authentication http console *server-tag* コマンド文を定義していない場合は、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（**password** コマンドで設定）を入力しなくても、ASDM を通じてセキュリティ 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 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、到達不能になっていると考えられます）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。

help aaa コマンドを使用すると、**aaa authentication** コマンドのシンタックスと使用方法の要約が表示されます。

コマンドのモード

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
7.0	既存のコマンドです。セキュリティ アプライアンスで強化されました。

使用上のガイドライン

aaa authentication console コマンドは、特権モードに入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セキュリティ アプライアンスにアクセスするときに認証確認を要求できるようにします。あるいは、管理認証のフォールバックをサポートします。

Telnet でアクセスする場合は、先に **telnet** コマンドを使用する必要があります。SSH でアクセスする場合は、先に **ssh** コマンドを使用する必要があります。

serial キーワードを併用すると、コンフィギュレーションに対してシリアル コンソールから行われた変更の内容を syslog サーバに記録できます。

aaa authentication console コマンドを使用する場合は、サーバ グループ プロトコルとして LOCAL を指定しない限り、事前に **aaa-server** コマンドを使用して認証サーバを指定しておく必要があります。**aaa authentication console** コマンドでは、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」に記載されている場合を除き、HTTP 認証を使用する場合、
aaa authentication http console コマンドを指定すると、セキュリティ アプライアンスは HTTP サーバの認証確認を要求します。

認証を必要とするアクションが管理者から要求されると、セキュリティ アプライアンスは、指定したサーバ 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、このグループのどのサーバとも通信できない場合。

指定したサーバ 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、デフォルトではディセーブルになっています。

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。

次の表に示すように、セキュリティ アプライアンス コンソールに認証を受けてアクセスするときのプロンプトのアクションは、**aaa authentication** {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** *server-tag* コマンドでどのオプションを選択したかによって異なります。

オプション	許可されるログイン試行の数
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。

セキュリティ アプライアンス コンソールには、任意の内部インターフェイスおよび IPSec 設定済みの外部インターフェイスから Telnet アクセスできます。アクセス前に **telnet** コマンドを使用する必要があります。また、セキュリティ アプライアンス コンソールへの SSH アクセスについても、IPSec を設定していない任意のインターフェイスから実行できます。アクセス前に **ssh** コマンドを使用する必要があります。

ssh オプションには、SSH ユーザ認証に使用する AAA サーバのグループを指定します。認証プロトコルおよび AAA サーバの IP アドレスは、**aaa-server** コマンド文で指定します。

Telnet モデルの場合と同様に、**aaa authentication ssh console** *server-tag* コマンド文を定義していない場合は、ユーザ名 ***pix*** とセキュリティ アプライアンスの Telnet パスワード（**passwd** 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 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、到達不能になっていると考えられます）は、管理者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、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 クレデンシャル要求プロンプトは、認証を受けてセキュリティ アプライアンスにアクセスできるサービス（Telnet、FTP、HTTP、および HTTPS）でそれぞれ異なります。

- Telnet ユーザには、セキュリティ アプライアンスが生成するプロンプトが表示されます。このプロンプトは、**auth-prompt** コマンドで変更できます。セキュリティ アプライアンスは、ユーザに対して 4 回までのログイン試行を許可し、それでもユーザ名とパスワードが違う場合は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。ユーザの入力したパスワードが誤っている場合は、ただちに接続がドロップされます。認証データベース上のユーザ名およびパスワードが、FTP を使用してアクセスする宛先リモート ホスト上のユーザ名およびパスワードと異なっている場合は、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
  ```

  セキュリティ アプライアンス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。ただし、FTP ユーザと HTTP ユーザは、ユーザ名またはパスワードごとに @ を追加して、各デイジーチェーン システムのユーザ名とパスワード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 GUI 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、ブラウザ自身によって生成されたポップアップ ウィンドウが表示されます。
  aaa authentication secure-http-client が設定されている場合、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。

セキュリティ アプライアンスは、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、セキュリティ アプライアンスは、Go-Ahead、Echo、および 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、セキュリティ アプライアンスの認証クレデンシャルが含まれています。

Windows NT の Microsoft IIS サーバは、このクレデンシャルに応答して、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仮定します。セキュリティ アプライアンスのユーザ名およびパスワードが、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、セキュリティ アプライアンスには **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後で、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。

認証が終了した後は、セキュリティ アプライアンスの uauth タイムアウトが非常に小さな値に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はありません。これは、ブラウザが「Authorization: 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 Netscape Navigator または Internet Explorer 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。

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

CU-SeeMe、Intel インターネット電話、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** コマンド文（**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後に、PC 上でマルチメディア プログラムにエラーが発生したり、PC に障害が発生したりする可能性があります。

TACACS+ サーバと RADIUS サーバ

最大 15 個のシングルモード グループまたは 4 個のマルチモード 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。サーバは、TACACS+ サーバまたは RADIUS サーバです。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** コマンド用のキーを指定していない場合は暗号化が使用できません。

セキュリティ アプライアンス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る。
- 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。

例

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

例 1：

次の例は、サーバ タグ「radius」の RADIUS サーバへの Telnet 接続に対して **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
```

例 2：

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
```

例 3：

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 match

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、あるいは ASDM ユーザ認証をイネーブルにするために一致する必要のある特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。特定のアクセスリストと一致する必要がないようにするには、このコマンドの **no** 形式を使用します。**aaa authentication match** コマンドでは、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を提供します。

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** コマンド文の名前。
interface-name	ユーザの認証元となるインターフェイス名。
server-tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグ。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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 コマンドを使用する場合は、事前に **aaa-server** コマンドを使用して認証サーバを指定し（***LOCAL*** を指定する場合を除く）、**access-list** コマンドを使用して名前付きアクセスリストを定義しておく必要があります。トラフィックの選別基準として送信元ポートを使用する **access-list** コマンド文は使用しないでください。**aaa authentication match** コマンドの一致条件で、送信元ポートはサポートされていません。

アクセスの要求元を定義するには、*interface-name* 変数を使用します。

カットスルー プロキシでは、サーバ グループ タグ ***LOCAL*** を指定することで、ローカルのユーザ認証データベースも使用できます。server-tag に ***LOCAL*** を指定する場合、ローカル ユーザ クレデンシャル データベースが空のときは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 10.0.0.0 255.255.255.0 172.23.2.0 255.255.255.0
(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、**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まず検索し、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検索します。

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。

コマンドのモード

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
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
```

- **aaa authentication secure-http-client** が設定されていない場合、HTTP ユーザには、ブラウザ自身によって生成されたポップアップ ウィンドウが表示されます。
  aaa authentication secure-http-client が設定されている場合、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。

ヒント　**help aaa** コマンドを使用すると、**aaa authentication** コマンドのシンタックスと使用方法の要約が表示されます。

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は、**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

指定したホスト上でサービスに対するユーザ認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認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。ユーザがどのサービスへのアクセスを認可されるかは、認証サーバが決定します。

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、指定したホストに対する認可の対象から除外して、以前に記述した規則に対する例外を作成します。
foreign-ip	*local-ip* アドレスからのアクセス先となるホストの 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。常に特定のマスク値を指定します。IP アドレスが 0 である場合は、0 を使用します。ホストには 255.255.255.255 を使用します。
interface-name	ユーザからの認証要求の送信元となるインターフェイス名。アクセスの要求元および送信者を指定するには、*interface-name* を *local-ip* アドレスおよび *foreign-ip* アドレスと組み合せて使用します。*local-ip* アドレスは、常に、セキュリティレベルの最も高いインターフェイス上にあります。*foreign-ip* アドレスは、常に、セキュリティレベルの最も低いインターフェイス上にあります。
include	指定したサービスに含む新しい規則を作成します。
local-ip	認証または認可を受けるホスト、またはホストのネットワークの IP アドレス。すべてのホストを指定して、認証を受けるホストを認証サーバ側で決定するには、このアドレスを **0** に設定します。
local-mask	*local-ip* のネットワーク マスク。常に特定のマスク値を指定します。IP アドレスが 0 である場合は、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 タグ。グループ タグ値に **LOCAL** を入力して、ローカルのコマンド認可特権レベルなど、ローカルのファイアウォール データベース AAA サービスも使用できます。
service	認可を必要とするサービス。有効な値は、**any**、**ftp**、**http**、**telnet**、または *protocol/port* です。すべての TCP サービスに認可を提供するには、**any** を使用します。認可を UDP サービスに提供するには、*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

「すべてのホスト」を指定するには、IP アドレスを **0** にします。ローカル IP アドレスを **0** に設定すると、認可を受けるホストを認可サーバ側で決定できます。

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。

コマンドのモード

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
7.0(1)	このリリースで、このコマンドが変更されました。**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

コマンド認可とともに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** コマンドは **aaa authorization** コマンドを使用する必要はありません。

セキュリティ アプライアンスは、認証が別のプロトコルで行われる場合に限り、**aaa authorization** コマンドでの RADIUS 認可をサポートしています。RADIUS サーバは、認証要求への応答とともに認可情報を返します。**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（コマンド認可の場合だけ）に加えて、RADIUS または TACACS+ サーバで許可されます。RADIUS サーバでダイナミック ACL を設定して、認可を提供できます（その認可がセキュリティ アプライアンスに設定されていない場合でも）。

VPN 認可が LOCAL と定義されている場合は、デフォルト グループポリシー DfltGrpPolicy に設定されているアトリビュートが適用されます。これは、**tunnel-group** コマンドおよび **webvpn** コマンド内の設定に影響を及ぼします。

ヒント　**help aaa** コマンドを使用すると、**aaa authentication** コマンドのシンタックスと使用方法の要約が表示されます。

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認可するには、サービス タイプに **any** パラメータを使用します。

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
```

ユーザ認可サービスは、ユーザがどのネットワーク サービスにアクセスできるかを制御します。認証が完了した後、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、セキュリティ アプライアンスは指定された 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 認可は、**access-list deny-flow-max** コマンド文とともに使用する場合、また RADIUS サーバを **acl=***acl-name* ベンダー固有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-port** コマンドのページおよび **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、すべてのホストを指定するには **0** を使用します。宛先マスクとローカル 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** の場合はマスク **0** を使用し、ホストにはマスク **255.255.255.255** を使用します。

Service パラメータ

指定しないサービスは、暗黙的に認可されます。**aaa authentication** コマンド内で指定したサービスは、認可を必要とするサービスには影響しません。

protocol/port を使用する場合は、次の値を指定できます。

- *protocol*：プロトコル（例：6 は TCP、17 は UDP、1 は ICMP）。
- *port*：TCP または UDP の宛先ポートまたは宛先ポート範囲。*port* には、ICMP タイプも入力できます。8 が ICMP の echo または ping を表します。ポート値を 0 にすると、すべてのポートを指定します。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は、*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 の認可をイネーブルにして、さらに 53 ～ 1024 のポート範囲にある他のすべてのサービスへのアクセスを認可する方法を示しています。

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。

（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。

service オプションに有効な値は、***telnet***、***ftp***、***http***、***https***、***tcp*** または ***0***、***tcp*** または *port*、***udp*** または *port*、***icmp*** または *port*、あるいは *protocol* [/*port*] です。対話型のユーザ認証は、Telnet トラフィック、FTP トラフィック、HTTP トラフィック、HTTPS トラフィックでだけトリガーします。

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

aaa authorization command コマンドは、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。コマンド認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization command** コマンドを使用します。コマンド認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization command {LOCAL | *server-tag***}**

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

次のシンタックスでは、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。このオプションは、デフォルトではディセーブルになっています。

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 コマンドの認可に、特権レベルを使用してセキュリティ アプライアンスのローカル ユーザ データベースを使用することを指定します。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。
server-tag	TACACS+ 認可サーバの定義済みのサーバ グループ タグを指定します。**aaa-server** コマンドで定義した AAA サーバ グループ タグ。グループ タグ値に **LOCAL** を入力して、ローカルのコマンド認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、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。

コマンドのモード

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
7.0(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

aaa authorization command コマンドをコマンド認可に使用する場合は、**aaa authentication** コマンドによる事前のコンフィギュレーションは必要ありません。

aaa authorization コマンドは、TACACS+ サーバおよび LOCAL サーバ（コマンド認可の場合だけ）とともに使用できますが、RADIUS サーバとは使用できません。

ヒント　**help aaa** コマンドを使用すると、**aaa authorization** コマンドのシンタックスと使用方法の要約が表示されます。

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

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するために照合する必要のある特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。ユーザ認可サービスに特定のアクセスリストを使用しないようにするには、このコマンドの **no** 形式を使用します。ユーザがどのサービスへのアクセスを認可されるかは、認証サーバが決定します。

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** コマンド文の名前を指定します。
interface-name	ユーザからの認証要求の送信元となるインターフェイス名。
server-tag	**aaa-server protocol** コマンドで定義した AAA サーバ グループ タグ。グループ タグ値に **LOCAL** を入力して、ローカルのコマンド認可特権レベルなど、ローカルのセキュリティ アプライアンス データベース AAA サービスも使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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 authorization match コマンドでは、事前に **aaa authentication** コマンドでのコンフィギュレーションが必要です。ただし、**aaa authentication** コマンドでは、**aaa authorization** コマンドを使用する必要はありません。

セキュリティ アプライアンスは、認証が別のプロトコルで行われる場合に限り、**aaa authorization** コマンドでの RADIUS 認可をサポートしています。RADIUS サーバは、認証要求への応答とともに認可情報を返します。**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（コマンド認可の場合だけ）に加えて、RADIUS または TACACS+ サーバで許可されます。RADIUS サーバでダイナミック ACL を設定して、認可を提供できます（その認可がセキュリティ アプライアンスに設定されていない場合でも）。

ヒント　**help aaa** コマンドを使用すると、**aaa authorization match** コマンドのシンタックスと使用方法の要約が表示されます。

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
```

ユーザ認可サービスは、ユーザがどのネットワーク サービスにアクセスできるかを制御します。認証が完了した後、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、セキュリティ アプライアンスは指定された 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 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。

コマンドのモード

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
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除外する定義済みの 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。MAC アドレス 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。**aaa mac-exempt** コマンドは、MAC アドレスのリストを認証および認可の対象から除外します。

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です。この番号は、**mac-list** コマンドで設定したものです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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 アクセスリストの番号を設定しておく必要があります。認証が免除される MAC アドレスは、自動的に認可が免除されます。

例

次の例は、mac-exempt リストを指定する方法を示しています。

```
hostname(config)# aaa mac-exempt mac-list-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。
mac-list	最初に一致した時点で停止する検索処理を使用して、MAC アドレスのリストを追加します。このリストは、MAC ベースの認証を実行するセキュリティ アプライアンスによって使用されます。

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。

コマンドのモード

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
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 サーバを設定する、またはホスト固有の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト 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* [*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*)	（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。このパラメータにはカッコが必要です。
key	（オプション）127 文字までの英数字で構成されているキーワードで、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は区別されます。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。
server-ip	AAA サーバの IP アドレス。
server-tag	サーバ グループの識別名。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*	（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。

コマンドのモード

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
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 15 個のシングルモード グループまたは 4 個のマルチモード 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 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信されます。

セキュリティ アプライアンス バージョンの **aaa-server** コマンドは、ホストごとのサーバ ポートの指定をサポートしています。そのため、記載しているようなセマンティックの変更とともに、以前の PIX Firewall システムで使用できた次のコマンド形式が段階的に廃止されています（お勧めできません）。これは、RADIUS サーバを含むサーバ グループだけに適用されます。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書き込まれなくなります。

- **aaa-server radius-authport** [*auth-port*]：このコマンドは、すべての RADIUS サーバのデフォルトの認証ポートを制御します。つまり、ホスト固有の認証ポートを指定していない場合は、このコマンドで指定した値が使用されます。このコマンドで値を指定しなかった場合は、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、上記の動作を RADIUS アカウンティング ポート（デフォルトでは 1646）に適用します。

次に、ホスト モードのコマンドをすべて示します。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を使用できます。詳細については、個々のコマンドの説明を参照してください。

コマンド	適用できる AAA サーバ タイプ	デフォルト値
accounting-port	RADIUS	1646
acl-netmask-convert	RADIUS	standard
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

コマンド	適用できる AAA サーバ タイプ	デフォルト値
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout[2]	All	10 秒

1. **aaa-server** コマンドで *key* パラメータを指定すると、そのパラメータは、ホスト モードで **key** コマンドを使用する場合と同じ影響を及ぼします。
2. **aaa-server** コマンドで ***timeout*** パラメータを指定すると、そのパラメータは、ホスト モードで **timeout** コマンドを使用する場合と同じ影響を及ぼします。

このリリースで、**aaa-server** コマンドが変更されました。グループ モードに入るための **aaa-server** *group-tag* **protocol** と、ホスト モードに入るための **aaa-server host** という、2 つの別のコマンドになりました。

例

次の例では、ホスト「192.168.3.4」に対して「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)# aaa-server svrgrp1 host 192.168.3.4
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
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

グループ固有で、すべてのホストに共通の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server 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 グループの識別名。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

デフォルトの動作や値はありません。

コマンドのモード

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
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

最大 15 個のシングルモード グループまたは 4 個のマルチモード 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 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信されます。

AAA サーバ グループ モードに入るための **aaa-server protocol** と、AAA サーバ ホスト モードに入るための **aaa-server host** という 2 つのコマンドで、AAA サーバのコンフィギュレーションを制御します。さらに、**aaa-server protocol** コマンドを指定して入るグループ モードでは、**accounting-mode** コマンドおよび **reactivation-mode** コマンドによってアカウンティング モードおよびサーバ再有効化機能をサポートしています。

AAA サーバ 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**
- **reactivation-mode**
- **max-failed-attempts**

これらのコマンドの詳細については、個々のコマンドの説明を参照してください。

例

次の例は、**aaa-server protocol** コマンドを使用して、TACACS+ サーバ グループのコンフィギュレーションの詳細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
hostname(config-aaa-server-group)# exit
hostname(config)#
```

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。

コマンドのモード

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
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

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

関連コマンド

コマンド	説明
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元します。
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。

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。

コマンドのモード

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
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、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には、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場合、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*** ステータスが、**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** コマンドととも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。

コマンドのモード

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
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-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	アクセスリストのエントリを番号別に表示します。

access-list commit

手動コミット モードの場合に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、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

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
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 mode コマンドを手動コミットに設定した場合、セキュリティ アプライアンスがアクセスリストを使用できるようにするには、アクセスリストを手動でコミットする必要があります。

（注） 手動コミット モードは、未使用のアクセスリスト、または **access-group** コマンドで使用されるアクセスリストだけに影響を及ぼします。AAA、NAT、または他のコンフィギュレーション コマンドで使用されるアクセスリストは、常に自動的にコミットされます。たとえば、**access-group** と AAA に同じアクセスリストを使用する場合、AAA ではアクセスリストが自動的にコミットされますが、**access-group** では手動でコミットする必要があります。このため、**access-group** コマンドと他のコマンド（AAA や NAT など）で同じアクセスリストを共有する場合は、手動コミット モードを使用しないことをお勧めします。

例

次の例は、アクセスリストと他の規則をコミットする方法を示しています。

```
hostname(config)# access-list commit
```

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。
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。
access-list mode	アクセスリストのコミットメント モードを手動コミットと自動コミットの間で切り替えます。
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 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。

コマンドのモード

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
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-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	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。

コマンドのモード

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
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-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	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。アクセスリストは、同じアクセスリスト ID を持つ 1 つまたは複数の ACE で構成されています。アクセスリストは、ネットワーク アクセスの制御、またはさまざまな機能の動作対象となるトラフィックの指定に使用されます。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセスリスト全体を削除するには、**clear configure access-list** コマンドを使用します。

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

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

シンタックスの説明

default	（オプション）ロギングをデフォルト方式に設定します。デフォルトでは、拒否されたパケットごとにシステム ログ メッセージ 106023 が送信されます。
deny	条件に合致している場合、パケットを拒否します。ネットワーク アクセス（**access-group** コマンド）の場合、このキーワードによって、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。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** コマンドおよび **inspect** コマンド）、このキーワードにより、トラフィックが検査の対象から除外されます。一部の機能（NAT など）では、拒否 ACE を使用できません。詳細については、アクセスリストを使用する各機能のコマンド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。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
disable	（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）プロトコルが **icmp** の場合、ICMP タイプを指定します。
id	最大 241 文字の文字列または整数でアクセスリスト ID を指定します。ID では、大文字と小文字が区別されます。ヒント：コンフィギュレーション内でアクセスリスト ID を簡単に識別できるように、すべて大文字を使用してください。
inactive	（オプション）ACE をディセーブルにします。ACE を再びイネーブルにするには、**inactive** キーワードを付けずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、簡単に再びイネーブルにすることができます。

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。
interval *secs*	（オプション）106100 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。有効な値は 1 ～ 600 秒です。デフォルトは 300 です。
level	（オプション）106100 システム ログ メッセージのレベル 0 ～ 7 を設定します。デフォルト レベルは 6 です。
line *line-num*	（オプション）ACE の挿入先となる行番号を指定します。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 の挿入先を指定するだけです。
log	（オプション）拒否 ACE がネットワーク アクセス用のパケットに一致した場合のロギング オプションを設定します（**access-group** コマンドで適用されるアクセスリスト）。引数を付けずに **log** キーワードを入力すると、システム ログ メッセージ 106100 がデフォルト レベル（6）およびデフォルト間隔（300 秒）でイネーブルになります。log キーワードを入力しない場合は、システム ログ メッセージ 106023 を使用して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 マスクの指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なります。セキュリティ アプライアンスは、ネットワーク マスク（たとえば、クラス C マスクには 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*	（オプション）プロトコルが **icmp** の場合、ICMP タイプのオブジェクト グループの ID を指定します。このオブジェクト グループを追加する方法については、**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。このオブジェクト グループを追加する方法については、**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。このオブジェクト グループを追加する方法については、**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、サービス オブジェクト グループの ID を指定します。このオブジェクト グループを追加する方法については、**object-group service** コマンドを参照してください。
operator	（オプション）送信元または宛先によって使用されるポート番号を照合します。指定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**：～と等しい • **neq**：～と等しくない • **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します。次に例を示します。 `range 100 200`
permit	条件に合致している場合、パケットを許可します。ネットワーク アクセス（**access-group** コマンド）の場合、このキーワードによって、パケットがセキュリティ アプライアンスを通過できるようになります。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** コマンドおよび **inspect** コマンド）、このキーワードにより、パケットに検査が適用されます。

port	（オプション）プロトコルを **tcp** または **udp** に設定する場合、TCP ポートまたは UDP ポートを示す整数または名前を指定します。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk のそれぞれで、TCP に対して 1 つ、UDP に対して 1 つの定義が必要です。TACACS+ では、TCP 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。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。
time-range *time_range_name*	（オプション）ACE に時間範囲を適用することにより、各 ACE が週および 1 日の中の特定の時刻に有効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

デフォルトは次のとおりです。

- ACE 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、拒否 ACE が存在する必要があります。
- **log** 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、デフォルト間隔は 300 秒です。

コマンドのモード

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
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

所定のアクセスリスト名に対して入力する各 ACE は、ACE の行番号を指定しない限り、アクセスリストの末尾に付加されます。

ACE の順序は重要です。セキュリティ アプライアンスは、パケットを転送するかドロップするかを決める場合、エントリの記載順に、パケットを各 ACE と比較してチェックします。一致が見つかると、それ以降の 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、それ以降の文はチェックされません。

アクセスリストの末尾には、暗黙的な拒否があります。そのため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザがセキュリティ アプライアンス経由でネットワークにアクセスできるようにする場合は、特定のアドレスを拒否してから、他のすべてのアドレス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、アクセスリストが対応付けられるインターフェイスによって異なります。インターフェイスに接続されているネットワーク上で有効なアドレスを使用する必要があります。このガイドラインは、着信アクセス グループと発信アクセス グループの両方に適用されます。使用するアドレスは、方向によってではなく、インターフェイスによって決まります。

TCP 接続および UDP 接続の場合は、確立された双方向接続のすべてのリターン トラフィックが FWSM によって許可されるため、アクセスリストでリターン トラフィックを許可する必要はありません。ただし、コネクションレス型プロトコル（ICMP など）の場合、セキュリティ アプライアンスは単方向セッションを確立するため、（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り）アクセスリストが両方向の ICMP を許可するようにするか、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ICMP はコネクションレス型プロトコルであるため、（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り）アクセスリストが両方向の ICMP を許可するようにするか、または ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを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**）（セキュリティ アプライアンスからホストへ）または **echo**（**8**）（ホストからセキュリティ アプライアンスへ）を指定します。ICMP タイプのリストについては、表 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（拡張または EtherType）のアクセスリストを 1 つだけ適用できます。同じアクセスリストを複数のインターフェイスに適用することもできます。アクセスリストをインターフェイスに適用する方法の詳細については、**access-group** コマンドを参照してください。

（注） アクセスリストのコンフィギュレーションを変更した後、既存の接続がタイムアウトになるのを待たずに、新しいアクセスリスト情報を使用するには、**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、(アクセスリスト適用先のインターフェイス上の) すべてのホストがセキュリティ アプライアンスを通過できるようにしています。

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

次の例のアクセスリストは、192.168.1.0/24 上のホストが 209.165.201.0/27 ネットワークにアクセスできないようにしています。他のアドレスはすべて許可されます。

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

一部のホストだけにアクセスを許可するには、制限付きの許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他の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、(アクセスリスト適用先のインターフェイス上の) すべてのホストがアドレス 209.165.201.29 の Web サイトにアクセスできないようにしています。他のトラフィックはすべて許可されます。

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

オブジェクト グループを使用する次のアクセスリストは、内部ネットワーク上の一部のホストが一部の Web サーバにアクセスできないようにしています。他のトラフィックはすべて許可されます。

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

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。その後、**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 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 エントリ（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 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。

コマンドのモード

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
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 に対して **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 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-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	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。

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-group コマンドとともに **deny** 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することが禁止されます。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。

object-group コマンドを使用して、アクセスリストをグループ化できます。

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-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	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。

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

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 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。

コマンドのモード

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
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。

コマンドのモード

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
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 アプライアンスに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。これにより、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。

コマンドのモード

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
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

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

config-general 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
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-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

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、このコマンドは適切な電子メール 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。

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

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。

acl-netmask-convert

RADIUS サーバから受信したダウンロード可能な ACL 内のネットマスクをセキュリティ アプライアンスがどのように扱うかを指定するには、AAA サーバ ホスト モードで **acl-netmask-convert** コマンドを使用します。このモードにアクセスするには、**aaa-server host** コマンドを使用します。コマンドを削除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

シンタックスの説明

auto-detect	セキュリティ アプライアンスが、使用されているネットマスク表現のタイプを判断するように指定します。セキュリティ アプライアンスは、ワイルドカード ネットマスク表現を検出すると、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現だけが含まれていると見なすように指定します。ワイルドカード ネットマスク表現からの変換は行われません。
wildcard	セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現だけが含まれていると見なし、ACL のダウンロード時にその表現をすべて標準ネットマスク表現に変換するように指定します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は行われません。

コマンドのモード

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
7.0(1)(4)	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 サーバがワイルドカード形式のネットマスクを含むダウンロード可能な ACL を提供する場合は、wildcard キーワードまたは auto-detect キーワードとともに **acl-netmask-convert** コマンドを使用します。セキュリティ アプライアンスは、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると予想します。一方、Cisco Secure VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると予想します。ワイルドカード マスクでは、無視するビット位置には 1 が、一致する必要のあるビット位置には 0 が置かれます。**acl-netmask-convert** コマンドを使用すると、このような違いが、RADIUS サーバ上でダウンロード可能な ACL を設定する方法に及ぼす影響を最小限に抑えることができます。

auto-detect キーワードは、RADIUS サーバがどのように設定されているかわからない場合に役立ちます。ただし、ワイルドカード ネットマスク表現に「穴」があると、その表現が正しく検出されず、変換されません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットがどのような数値であっても許可し、Cisco VPN 3000 シリーズ コンセントレータで有効に使用できますが、セキュリティ アプライアンスはこの表現をワイルドカード ネットマスクとして検出できません。

例

次の例では、ホスト「192.168.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスク変換をイネーブルにして、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、認証ポートを 1650 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

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またはディセーブルにします。
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。これにより、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。

activation-key

セキュリティ アプライアンスのアクティベーション キーを変更し、セキュリティ アプライアンス上で運用されているアクティベーション キーをセキュリティ アプライアンスのフラッシュ パーティションに隠しファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

シンタックスの説明

activation-key-four-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。
activation-key-five-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

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
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

各要素の間にスペースを 1 つ入れて、4 つの要素で構成される 16 進数文字列として *activation-key-four-tuple* を入力します。または、各要素の間にスペースを 1 つ入れて、5 つの要素で構成される 16 進数文字列として、*activation-key-five-tuple* を入力します。次に例を示します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭部分の 0x 指定子は省略できます。値は、すべて 16 進数であると見なされます。

キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

例

次の例は、セキュリティ アプライアンスのアクティベーション キーを変更する方法を示しています。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

関連コマンド

コマンド	説明
show activation-key	アクティベーション キーを表示します。

address-pool

リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定するには、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 **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの ***no*** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

シンタックスの説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	(オプション)アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

このコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスを指定しない場合、このコマンドは、明示的に参照されていないすべてのインターフェイスのデフォルトを指定します。

例

config-general コンフィギュレーション モードに入る次の例では、IPSec リモートアクセス トンネルグループ xyz のリモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定しています。

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモートアクセス トンネルに使用する IP アドレス プールを設定します。
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-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

admin-context

システム コンフィギュレーションに管理コンテキ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 **admin-context** コマンドを使用します。システム コンフィギュレーションには、それ自身のネットワーク インターフェイスもネットワーク設定も含まれていません。システムは、ネットワーク リソースにアクセスする必要がある場合（セキュリティ アプライアンス ソフトウェアをダウンロードする場合や、管理者にリモート管理を許可する場合など）、管理コンテキストとして指定されているコンテキストの 1 つを使用します。

admin-context *name*

シンタックスの説明

name	最大 32 文字の文字列で名前を設定します。まだコンテキストを 1 つも定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。その後、**context** コマンドを使用して追加する最初のコンテキストは、指定した管理コンテキスト名である必要があります。 この名前では大文字と小文字が区別されます。したがって、たとえば「customerA」という名前と「CustomerA」という名前の 2 つコンテキストを持つことができます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンを使用することはできません。 「System」および「Null」（大文字および小文字）は予約されている名前であるため、使用できません。

デフォルト

マルチ コンテキスト モードの新しいセキュリティ アプライアンスでは、管理コンテキストは「admin」という名前です。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

コンテキスト コンフィギュレーションが内部フラッシュ メモリに常駐する限り、任意のコンテキストを管理コンテキストとして設定できます。

clear configure context コマンドを使用してすべてのコンテキストを削除しない限り、現在の管理コンテキストを削除することはできません。

例

次の例では、「administrator」を管理コンテキストとして設定しています。

```
hostname(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードに入ります。
show admin-context	現在の管理コンテキスト名を表示します。

alias

アドレスを手動で変換して DNS 応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** コマンドを削除するには、このコマンドの **no** 形式を使用します。このコマンドの機能は、外部 NAT コマンド（**dns** キーワード付きの **nat** コマンドや **static** コマンド）に置き換えられました。**alias** コマンドではなく、外部 NAT を使用することをお勧めします。

alias *interface_name mapped_ip real_ip* [*netmask*]

[no] alias *interface_name mapped_ip real_ip* [*netmask*]

シンタックスの説明

interface_name	マッピング IP アドレス宛てのトラフィックの入力インターフェイス名（またはマッピング IP アドレスからのトラフィックの出力インターフェイス名）を指定します。
mapped_ip	実際の IP アドレスの変換先となる IP アドレスを指定します。
real_ip	実際の IP アドレスを指定します。
netmask	（オプション）両方の IP アドレスのサブネット マスクを指定します。ホスト マスクの場合は **255.255.255.255** と入力します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

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
1.1(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

このコマンドは、宛先アドレスのアドレス変換を行う場合にも使用できます。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用することで、トラフィックを他のアドレス（209.165.201.30 など）にリダイレクトできます。

（注）　***alias*** コマンドを他のアドレスへの変換ではなく DNS の書き換えに使用する場合は、エイリアスがイネーブルなインターフェイス上で ***proxy-arp*** をディセーブルにします。***sysopt noproxyarp*** コマンドを使用して、セキュリティ アプライアンスが一般的な NAT 処理のために ***proxy-arp*** によって自分自身の方にトラフィックをプルしないようにしてください。

alias コマンドを変更または削除した後は、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルの中に、**alias** コマンドに含まれている「dnat」アドレスの A（アドレス）レコードが存在している必要があります。

alias コマンドには、2 つの使用方法があります。次に、その概要を示します。

- セキュリティ アプライアンスが *mapped_ip* 宛てのパケットを取得した場合、そのパケットを *real_ip* に送信するように **alias** コマンドを設定できる。
- セキュリティ アプライアンスが *real_ip* 宛てに DNS パケットを送信し、そのパケットがセキュリティ アプライアンスに戻ってきた場合、DNS パケットに変更を加えて、宛先ネットワーク アドレスを *mapped_ip* にするように **alias** コマンドを設定できる。

alias コマンドは、ネットワーク上の DNS サーバと自動的に対話して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

real_ip IP アドレスと *mapped_ip* IP アドレスにネットワーク アドレスを使用すると、ネット エイリアスを指定できます。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

static コマンドと **access-list** コマンドで **alias** コマンドの *mapped_ip* アドレスにアクセスするには、**access-list** コマンド内で、許可されるトラフィック送信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1
eq ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答は、セキュリティ アプライアンスによって 192.168.201.29 へと変更されます。セキュリティ アプライアンスで 209.165.200.225 ～ 209.165.200.254 をグローバル プール IP アドレスとして使用している場合、パケットはセキュリティ アプライアンスに SRC=209.165.201.2 および DST=192.168.201.29 として送信されます。セキュリティ アプライアンスは、アドレスを外部の SRC=209.165.200.254 および DST=209.165.201.29 に変換します。

例

次の例では、内部ネットワークに IP アドレス 209.165.201.29 が含まれています。このアドレスはインターネット上にあり、example.com に属しています。内部のクライアントが example.com にアクセスしても、パケットはセキュリティ　アプライアンスに到達しません。クライアントは、209.165.201.29 がローカルの内部ネットワーク上にあると判断するためです。

この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次の例では、内部の 10.1.1.11 にある Web サーバ、および 209.165.201.11 で作成された **static** コマンドを示しています。送信元ホストは、外部のアドレス 209.165.201.7 にあります。外部の DNS サーバには、次に示すとおり、www.example.com のレコードが登録されています。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは必要です。

次に、**alias** コマンドを使用する例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

セキュリティ アプライアンスは、内部クライアント用のネーム サーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host
209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

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。
clear configure alias	すべての **alias** コマンドをコンフィギュレーションから削除します。
show running-config alias	コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示します。
static	ローカル IP アドレスをグローバル IP アドレスに、またはローカル ポートをグローバル ポートにマッピングすることによって、1 対 1 のアドレス変換規則を設定します。

allocate-interface

セキュリティ コンテキストにインターフェイスを割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。コンテキストからインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [***visible*** | ***invisible***]

no allocate-interface *physical_interface*

allocate-interface *physical_interface.subinterface*[**-***physical_interface.subinterface*] [*map_name*[**-***map_name*]] [***visible*** | ***invisible***]

no allocate-interface *physical_interface.subinterface*[**-***physical_interface.subinterface*]

シンタックスの説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。

map_name	（オプション）マッピング名を設定します。
	
	map_name は、インターフェイス ID ではなく、インターフェイスを示す英数字のエイリアスで、コンテキスト内で使用できます。マッピング名を指定しない場合は、コンテキスト内でインターフェイス ID が使用されます。セキュリティを確保するため、コンテキストによって使用されているインターフェイスをコンテキスト管理者に知らせたくない場合があります。
	
	マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線だけを使用できます。たとえば、次のような名前を使用できます。
	
	`int0`
	
	`inta`
	
	`int_0`
	
	サブインターフェイスの場合は、マッピング名の範囲を指定できます。
	
	範囲の詳細については、「使用上のガイドライン」を参照してください。

physical_interface	インターフェイス ID（***gigabit*ethernet0/1** など）を設定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（オプション）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで物理インターフェイスのプロパティを表示できるようにします。

デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力でインターフェイス ID を表示できません。

コマンドのモード　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
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更
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　このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示の設定を変更するには、所定のインターフェイス ID でこのコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して、最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、セキュリティ アプライアンスによって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注）　透過モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをそのインターフェイスを通してフラッドしません。

ルーテッド モードでは、必要に応じて、同じインターフェイスを複数のコンテキストに割り当てることができます。透過モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成される必要がある。範囲の両端で、マッピング名のアルファベット部分が一致する必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力すると、コマンドが失敗します。
- マッピング名の数値部分には、サブインターフェイス範囲と同じ個数の数値が含まれる必要がある。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力すると、コマンドが失敗します。

例

次の例は、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる方法を示しています。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

シンタックスの説明

area_id	作成するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

作成するエリアには、パラメータが設定されていません。関連する area コマンドを使用して、エリア パラメータを設定します。

例

次の例は、エリア ID 1 の OSPF エリアを作成する方法を示しています。

```
hostname(config-router)# area 1
hostname(config-router)#
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
area nssa	エリアを準スタブ エリアとして定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。エリア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。

area *area_id* **authentication** [***message-digest***]

no area *area_id* **authentication** [***message-digest***]

シンタックスの説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
message-digest	（オプション）*area_id* によって指定されたエリアでの Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリア認証はディセーブルになっています。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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 OSPF エリアが存在しない場合は、このコマンドの入力時にそのエリアが作成されます。***message-digest*** キーワードを付けずに **area authentication** コマンドを入力すると、簡易パスワード認証がイネーブルになります。***message-digest*** キーワードを付けると、MD5 認証がイネーブルになります。

例

次の例は、エリア 1 の MD5 認証をイネーブルにする方法を示しています。

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area default-cost

スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* ***default-cost*** *cost*

no area *area_id* ***default-cost***

シンタックスの説明

area_id	デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
cost	スタブまたは NSSA に使用されるデフォルト サマリー ルートのコストを指定します。有効な値は 0 ～ 65535 です。

デフォルト

cost のデフォルト値は 1 です。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

例

次の例は、スタブまたは NSSA に送信されるサマリー ルートのデフォルト コストを指定する方法を示しています。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
area nssa	エリアを準スタブ エリアとして定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list** ***prefix*** *list_name* {***in*** | ***out***}

no area *area_id* ***filter-list prefix*** *list_name* {***in*** | ***out***}

シンタックスの説明

area_id	フィルタリングを設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
in	指定エリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定エリアから発信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

タイプ 3 LSA だけをフィルタリングできます。プライベート ネットワークに ASBR が設定されている場合は、ASBR がタイプ 5 LSA（プライベート ネットワークを記述）を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッドされます。

例

次の例では、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングします。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。エリアから NSSA 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。

area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

no area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

シンタックスの説明

area_id	NSSA として指定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR 上または NSSA ASBR 上に限り有効です。
metric *metric_value*	（オプション）OSPF デフォルト メトリック値を指定します。有効な値は 0 ～ 16777214 です。
metric-type {***1*** | ***2***}	（オプション）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • ***1*** : タイプ 1 • ***2*** : タイプ 2 デフォルト値は 2 です。
no-redistribution	（オプション）ルータが NSSA ABR である場合に、**redistribute** コマンドで通常エリアだけにルートをインポートし、NSSA エリアにはインポートしないときに使用します。
no-summary	（オプション）エリアを、サマリー ルートが投入されない準スタブ エリアにします。

デフォルト

デフォルトは次のとおりです。

- NSSA エリアは定義されていません。
- ***metric-type*** は 2 です。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

あるオプションをエリアに設定した後、別のオプションを指定すると、両方のオプションが設定されます。たとえば、次の 2 つのコマンドを別々に入力すると、コンフィギュレーション内では、両方のオプションが設定された 1 つのコマンドになります。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

例

次の例は、2 つのオプションを別々に設定すると、コンフィギュレーション内でどのように 1 つのコマンドになるかを示しています。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area range

エリアの境界でルートを統合および集約するには、ルータ コンフィギュレーション モードで **area range** 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。

area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

no area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

シンタックスの説明

address	サブネット範囲の IP アドレス。
advertise	（オプション）アドレス範囲ステータスを advertise に設定し、タイプ 3 要約リンクステート アドバタイズメント（LSA）を生成します。
area_id	範囲を設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（オプション）アドレス範囲ステータスを DoNotAdvertise に設定します。タイプ 3 要約 LSA の表示が抑止され、コンポーネント ネットワークは他のネットワークからは見えないままになります。

デフォルト

アドレス範囲ステータスは advertise に設定されます。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

area range コマンドは、ABR だけで使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つのサマリー ルートが ABR によって他のエリアにアドバタイズされます。エリアの境界でルーティング情報が凝縮されます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は、「経路集約」と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。これにより、OSPF は、多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* ***not-advertise*** コマンドは、***not-advertise*** オプション キーワードだけを削除します。

例

次の例は、ネットワーク 10.0.0.0 上のすべてのサブネット対する 1 つのサマリー ルート、およびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つのサマリー ルートが、ABR によって他のエリアにアドバタイズされるよう指定しています。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリア機能を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* [***no-summary***]

no area *area_id* [***no-summary***]

シンタックスの説明

area_id	スタブ エリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアが定義されていません。
- サマリー リンク アドバタイズメントがスタブ エリアに送信されます。

コマンドのモード

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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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

このコマンドは、スタブまたは NSSA に接続されている ABR だけで使用できます。

area stub と **area default-cost** という 2 つのスタブ エリア ルータ コンフィギュレーション コマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続されている ABR だけで **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成されるサマリー デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次の例では、指定したエリアをスタブ エリアとして設定しています。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定します。
area nssa	エリアを準スタブ エリアとして定義します。

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットする、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

no area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

シンタックスの説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
authentication	（オプション）認証タイプを指定します。
authentication-key *key*	（オプション）隣接ルーティング デバイスで使用するための OSPF 認証パスワードを指定します。
dead-interval *seconds*	（オプション）hello パケットを 1 つも受信しない場合に、隣接ルーティング デバイスがダウンしたことを宣言する前の間隔を設定します。有効な値は 1 ～ 65535 秒です。
hello-interval *seconds*	（オプション）インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。
md5 *key*	（オプション）最大 16 バイトの英数字によるキーを指定します。
message-digest	（オプション）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（オプション）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は 1 ～ 255 です。
null	（オプション）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されていれば上書きされます。
retransmit-interval *seconds*	（オプション）インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効な値は 1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（オプション）OSPF によるトポロジ変更の受信と最短パス優先（SPF）計算の開始との間の遅延時間（0 ～ 65535 秒）を指定します。デフォルトは 5 秒です。

デフォルト

デフォルトは次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- ***hello-interval*** *seconds*：10 秒。
- ***retransmit-interval*** *seconds*：5 秒。
- ***transmit-delay*** *seconds*：1 秒。
- ***dead-interval*** *seconds*：40 秒。
- ***authentication-key*** *key*：キーは事前に定義されていません。
- ***message-digest-key*** *key_id* ***md5*** *key*：キーは事前に定義されていません。

コマンドのモード　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
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
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　OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合、仮想リンクを確立することで接続を修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、***area*** *area_id* ***authentication*** コマンドでバックボーンに対して認証がイネーブルにされている場合にだけ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらかを指定するか、または両方とも指定しないでください。***authentication-key*** *key* または ***message-digest-key*** *key_id* ***md5*** *key* の後に指定するキーワードと引数はすべて無視されます。したがって、オプションの引数はすべて、上記のキーワードと引数の組み合せの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスはエリアに指定されている認証タイプを使用します。エリアに認証タイプが指定されていない場合、エリアのデフォルトは null 認証です。

（注）　仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンクからオプションを削除するには、削除するオプションを付けて、このコマンドの **no** 形式を使用します。仮想リンクを削除するには、**no area** *area_id* ***virtual-link*** コマンドを使用します。

例

次の例では、MD5 認証の仮想リンクを確立しています。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

arp

ARP テーブルにスタティック ARP 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 **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。スタティック ARP エントリは MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトしないため、ネットワーク問題の解決に役立つことがあります。透過ファイアウォール モードでは、ARP 検査でスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照してください）。

arp *interface_name ip_address mac_address* [***alias***]

no arp *interface_name ip_address mac_address*

シンタックスの説明

alias	（オプション）このマッピングに対してプロキシ ARP をイネーブルにします。セキュリティ アプライアンスは、このコマンドで指定された IP アドレスに対する ARP 要求を受信すると、セキュリティ アプライアンスの MAC アドレスで応答します。その後、その IP アドレスを持つホスト宛てのトラフィックを受信すると、セキュリティ アプライアンスはこのコマンドで指定されたホスト MAC アドレスにそのトラフィックを転送します。このキーワードは、たとえば、ARP を実行しないデバイスがある場合に役立ちます。 透過ファイアウォール モードの場合、このキーワードは無視され、セキュリティ アプライアンスはプロキシ ARP を実行しません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

ホストは IP アドレスによってパケットの宛先を指定しますが、イーサネット上での実際のパケット配信は、イーサネット MAC アドレスに依存しています。ルータまたはホストは、直接接続されているネットワーク上でパケットを配信する場合、IP アドレスに関連付けられている MAC アドレスを要求する ARP 要求を送信してから、その ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータは ARP テーブルを保持しているため、配信する必要のあるパケットごとに ARP 要求を送信する必要がありません。ARP テーブルは、ネットワーク上で ARP 応答が送信されるたびに動的にアップデートされます。また、一定期間使用されなかったエントリは、タイムアウトになります。エントリが間違っている場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合）、アップデートされる前にそのエントリがタイムアウトになります。

（注） 透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

例

次の例では、外部インターフェイス上で、10.1.1.1 のスタティック ARP エントリを MAC アドレス 0009.7cbe.2100 で作成しています。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	透過 ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp timeout

セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。ARP テーブルを再構築すると、自動的に、新しいホスト情報にアップデートされ、古いホスト情報が削除されます。ホスト情報が頻繁に変更されるため、タイムアウト値を小さくする必要がある場合もあります。

arp *timeout* *seconds*

no arp *timeout* *seconds*

シンタックスの説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

デフォルト

デフォルト値は 14,400 秒（4 時間）です。

コマンドのモード

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
既存	このコマンドは既存のものです。

例

次の例では、ARP タイムアウトを 5,000 秒に変更します。

```
hostname(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過 ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp-inspection

透過ファイアウォール モードで ARP 検査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 **arp-inspection** コマンドを使用します。ARP 検査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。ARP 検査では、すべての ARP パケットがスタティック ARP エントリ（**arp** コマンドを参照）と比較してチェックされ、一致しないパケットがブロックされます。この機能により、ARP スプーフィングを防止できます。

arp-inspection *interface_name* ***enable*** [***flood*** | ***no-flood***]

no arp-inspection *interface_name* ***enable***

シンタックスの説明

enable	ARP 検査をイネーブルにします。
flood	（デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットが、発信元インターフェイスを除くすべてのインターフェイスにフラッドされるように指定します。MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。 **（注）** 管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。
interface_name	ARP 検査をイネーブルにするインターフェイス。
no-flood	（オプション）スタティック ARP エントリに正確に一致しないパケットがドロップされるように指定します。

デフォルト

デフォルトでは、すべてのインターフェイスで ARP 検査がディセーブルになっています。すべての ARP パケットがセキュリティ アプライアンスを通過できます。ARP 検査をイネーブルにすると、デフォルトでは、まったく一致しない ARP パケットがフラッドされます。

コマンドのモード

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
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

ARP 検査をイネーブルにするには、事前に **arp** コマンドを使用してスタティック ARP エントリを設定しておく必要があります。

ARP 検査をイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較して、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致した場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットのエントリがスタティック ARP テーブル内のどのエントリとも一致しなかった場合、パケットをすべてのインターフェイスに転送（フラッド）するように、またはドロップするように、セキュリティ アプライアンスを設定できます。

（注） 管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。

ARP 検査により、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィングと呼ばれる）を防止できます。ARP スプーフィングは、「man-in-the-middle」攻撃をイネーブルにすることができます。たとえば、ホストがゲートウェイ ルータに ARP 要求を送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ところが、攻撃者はホストに、ルータの MAC アドレスではなく、攻撃者の MAC アドレスを含む別の ARP 応答を送信します。これで、攻撃者は、ルータに転送する前に、ホストのトラフィックをすべて代行受信できるようになります。

ARP 検査により、正しい MAC アドレスと、それに関連付けられている IP アドレスがスタティック ARP テーブル内にある限り、攻撃者が攻撃者の MAC アドレスで ARP 応答を送信できないことが保証されます。

（注） 透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

例

次の例では、外部インターフェイス上で ARP 検査をイネーブルにし、スタティック ARP エントリに一致しないすべての ARP パケットをドロップするようセキュリティ アプライアンスを設定しています。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP 検査のコンフィギュレーションを消去します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

シンタックスの説明

session	終了させるアクティブな ASDM セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm sessions** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**pdm disconnect** コマンドから **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのすべてのアクティブな ASDM セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM セッションにセッション ID 1 が割り当てられ、その後の新しいセッションには、セッション ID 3 から順番に ID が割り当てられます。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect** コマンドの入力前後に、**show asdm sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

asdm disconnect log_session *session*

シンタックスの説明

session	終了させるアクティブな ASDM ロギング セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm log_sessions** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
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

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

アクティブな各 ASDM セッションは、1 つまたは複数の ASDM ロギング セッションと関連付けられています。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶことがあります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

（注） 各 ASDM セッションは少なくとも 1 つの ASDM ロギング セッションを持っているため、**show asdm sessions** の出力と **show asdm log_sessions** の出力が同じになることがあります。

ASDM ロギング セッションを終了しても、残りのすべてのアクティブな ASDM ロギング セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM ロギング セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM ロギング セッションにセッション ID 1 が割り当てられ、その後の新しいロギング セッションには、セッション ID 3 から順番に ID が割り当てられます。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect log_sessions** コマンドの入力前後に、**show asdm log_sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm group

注意　このコマンドを手動で設定しないでください。**asdm group** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部用に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm group *real_grp_name real_if_name*

asdm group *ref_grp_name ref_if_name* ***reference*** *real_grp_name*

シンタックスの説明

real_grp_name	ASDM オブジェクト グループの名前。
real_if_name	指定のオブジェクト グループが関連付けられているインターフェイスの名前。
ref_grp_name	*real_grp_name* 引数で指定されたオブジェクト グループの変換された IP アドレスを含むオブジェクト グループの名前。
ref_if_name	着信トラフィックの宛先 IP アドレスが変換される元となるインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドが、**pdm group** コマンドから **asdm group** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asdm history enable

ASDM 履歴トラッキ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 **asdm history enable** コマンドを使用します。ASDM 履歴トラッキ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。

asdm history enable

no asdm history enable

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。

コマンドのモード

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
7.0(1)	このコマンドが、**pdm history enable** コマンドから **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって得られる情報は、ASDM 履歴バッファに格納されます。この情報を表示するには、**show asdm history** コマンドを使用します。この履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次の例では、ASDM 履歴トラッキングをイネーブルにしています。

```
hostname(config)# asdm history enable
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

ASDM ソフトウェア イメージを指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージ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。

asdm image *image_path*

no asdm image [*image_path*]

シンタックスの説明

image_path	セキュリティ アプライアンス上の ASDM イメージ ファイルのパス。たとえば、`flash:/asdm`。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドが、**pdm image** コマンドから **asdm image** コマンドに変更されました。

使用上のガイドライン

asdm image コマンドは、ASDM セッションの開始時に使用される ASDM ソフトウェア イメージを指定します。このコマンドがコンフィギュレーションに存在しない場合、ASDM セッションを開始できません。

フラッシュ メモリに複数の ASDM ソフトウェア イメージを格納できます。アクティブな ASDM セッションが存在している間に、**asdm image** コマンドを使用して新しい ASDM ソフトウェア イメージを指定しても、アクティブなセッションは中断しません。アクティブな ASDM セッションは、セッション開始時の ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用します。

ASDM 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。

例

次の例では、ASDM イメージを asdm.bin に設定しています。

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。

asdm location

注意　このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

シンタックスの説明

ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
netmask	*ip_addr* のサブネット マスク。
if_name	ASDM にアクセスするときに通過するインターフェイスの名前。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスおよびプレフィックス。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0(1)	このコマンドが、**pdm location** コマンドから **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。この ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*

no asr-group *group_id*

シンタックスの説明

group_id	非対称ルーティング グループ ID。有効な値は 1 ～ 32 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
インターフェイス コンフィギュレーション	•	•	—	•	—

コマンド履歴

リリース	変更
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

Active/Active フェールオーバーがイネーブルである場合、ロードバランシングのために、発信接続のリターン トラフィックがピア装置上のアクティブなコンテキストを介してルーティングされることがあります。このピア装置上で、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドでは、着信インターフェイスによるフローが見つからない場合、同じ asr グループのインターフェイスで着信パケットが再分類されます。再分類により、別のインターフェイスによるフローが見つかり、関連付けられているコンテキストがスタンバイ状態である場合、パケットは処理のためにアクティブな装置に転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーがイネーブルである必要があります。

ASR 統計情報を表示するには、**show interface detail** コマンドを使用します。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれています。

例

次の例では、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てています。

コンテキスト ctx1 のコンフィギュレーション

```
hostname/ctx1(config)# interface e2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション

```
hostname/ctx2(config)# interface e3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイス統計情報を表示します。

authentication

WebVPN または電子メール プロキシの認証方式を設定するには、**authentication** 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、このコマンドは適切な電子メール プロキシ モードで使用します。デフォルトの AAA に戻すには、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、ユーザを認証して、ユーザのアイデンティティを確認します。

authentication {**aaa** | **certificate** | **mailhost** | **piggyback**}

no authentication

シンタックスの説明

aaa	セキュリティ アプライアンスが設定済み AAA サーバに対してチェックするユーザ名とパスワードを提供します。
certificate	SSL ネゴシエーション中に証明書を提供します。
mailhost	リモート メール サーバを介した認証。mailhost を設定できるのは SMTPS だけです。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
piggyback	HTTPS WebVPN セッションがすでに存在する必要があります。ピギーバック認証は、電子メール プロキシだけで使用できます。

デフォルト

次の表は、WebVPN および電子メール プロキシのデフォルトの認証方式を示しています。

プロトコル	デフォルトの認証方式
WebVPN	AAA
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA

コマンドのモード　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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更
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　WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。その場合、ユーザは証明書およびユーザ名とパスワードを提供する必要があります。

電子メール プロキシ認証の場合、複数の認証方式を要求できます。

このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例　次の例は、WebVPN ユーザに対して認証のために証明書の提供を要求する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

authentication-port

特定のホストの RADIUS 認証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 **authentication-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、認証機能の割り当て先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定するものです。

authentication-port *port*

no authentication-port

シンタックスの説明

port	RADIUS 認証用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS 認証のデフォルト ポート番号（1645）が使用されます。

コマンドのモード

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
7.0(1)	このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。

使用上のガイドライン

RADIUS 認証サーバが 1645 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 アプライアンスに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、認証ポートを 1650 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)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

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またはディセーブルにします。
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。これにより、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。

authentication-server-group

ユーザ認証に使用する 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 モードで **authentication-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。

authentication-server-group [(*interface name*)] *server group* [***LOCAL*** | ***NONE***]

no authentication-server-group [(*interface name*)] *server group*

シンタックスの説明

interface name	（オプション）IPSec トンネルが終端するインターフェイスを指定します。
LOCAL	（オプション）通信障害のためにサーバ グループ内のすべてのサーバが無効になった場合に、認証がローカル ユーザ データベースに対して行われるように指定します。サーバ グループ名が ***LOCAL*** または ***NONE*** のいずれかである場合は、ここで ***LOCAL*** キーワードを使用しないでください。
NONE	（オプション）サーバ グループ名を NONE と指定します。認証が不要であることを示すには、サーバ グループ名として ***NONE*** キーワードを使用します。
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 ***LOCAL*** 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 ***LOCAL*** になっています。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
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

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

例

config-general コンフィギュレーション モードに入る次の例では、IPSec リモートアクセス トンネルグループ remotegrp に aaa-server456 という名前の認証サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
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-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

authentication-server-group (webvpn)

WebVPN またはいずれかの電子メール プロキシで使用する認証サーバ グループを指定するには、**authentication-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、このコマンドは適切な電子メール 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認証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、ユーザを認証して、ユーザのアイデンティティを確認します。

authentication-server-group *group tag*

no authentication-server-group

シンタックスの説明

group tag	設定済みの認証サーバまたはサーバ グループを指定します。認証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、認証サーバは設定されていません。

コマンドのモード

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
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 認証を設定する場合は、このアトリビュートも設定する必要があります。設定しないと、認証が必ず失敗します。

例

次の例は、WEBVPNAUTH という名前の認証サーバ 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)# authentication-server-group WEBVPNAUTH
```

次の例は、IMAP4SSVRS という名前の認証サーバ グループを使用するように IMAP4S 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)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

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。

authorization-dn-attributes

サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかを指定するには、トンネルグループ ipsec アトリビュート コンフィギュレーション モードで **authorization-dn-attributes** 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。

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | ***use-entire-name***}

no authorization-dn-attributes

シンタックスの説明

primary-attr	証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。
secondary-attr	（オプション）プライマリ アトリビュートが存在しない場合に、証明書から認可クエリー用の名前を生成するときに使用する追加のアトリビュートを指定します。
use-entire-name	セキュリティ アプライアンスがサブジェクト DN（RFC1779）全体を使用して名前を生成するように指定します。

デフォルト

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

コマンドのモード

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 ipsec 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
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　このアトリビュートは、IPSec リモートアクセス トンネル タイプだけに適用できます。

プライマリ アトリビュートとセカンダリ アトリビュートには、次のようなものがあります。

アトリビュート	定義
CN	Common Name（通常名）：個人、システムなどの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
O	Organization（組織）：会社、団体、機関、連合などの名前。
L	Locality（地名）：組織が置かれている市または町。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
C	Country（国または地域）：国または地域を示す 2 文字の短縮形。このコードは、ISO 3166 の国または地域の短縮形に準拠しています。
EA	E-mail address（電子メール アドレス）
T	Title（タイトル）
N	Name（名前）
GN	Given Name（名）
SN	Surname（姓）
I	Initials（イニシャル）
GENQ	Generational Qualifier（世代修飾子）
DNQ	Domain Name Qualifier（ドメイン名修飾子）
UID	User Identifier（ユーザ識別子）

例

config-ipsec コンフィギュレーション モードに入る次の例では、remotegrp という名前のリモートアクセス トンネルグループ（ipsec_ra）を作成し、IPSec グループ アトリビュートを指定して、通常名が認可用のユーザ名として使用されるように定義しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-ipsec)#
```

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	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

authorization-dn-attributes (webvpn)

認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定するには、**authorization-dn-attributes** 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、このコマンドは適切な電子メール プロキシ モードで使用します。このアトリビュートをコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

authorization-dn-attributes {*primary-attr*} **[***secondary-attr***] | use-entire-name}**

no authorization-dn-attributes

シンタックスの説明

primary-attr	デジタル証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。
secondary-attr	（オプション）デジタル証明書から認可クエリー用の名前を生成するときにプライマリ アトリビュートとともに使用する追加のアトリビュートを指定します。
use-entire-name	セキュリティ アプライアンスがサブジェクト DN 全体を使用して、デジタル証明書から認可クエリー用の名前を生成するように指定します。

デフォルト

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

コマンドのモード

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 IPSec アトリビュート	•	—	•	—	—
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更
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　次の表で、DN フィールドについて説明します。

DN フィールド	説明
C	Country（国または地域）
CN	Common Name（通常名）
DNQ	DN Qualifier（DN 修飾子）
EA	E-mail Address（電子メール アドレス）
GENQ	Generational Qualifier（世代修飾子）
GN	Given Name（名）
I	Initials（イニシャル）
L	Locality（地名）
N	Name（名前）
O	Organization（組織）
OU	Organizational Unit（組織ユニット）
SER	Serial Number（シリアル番号）
SN	Surname（姓）
SP	State/Province（州または都道府県）
T	Title（タイトル）
UID	User ID（ユーザ ID）
user-entire-name	DN 名全体を使用

例

次の例は、WebVPN ユーザが電子メール アドレス（プライマリ アトリビュート）および組織ユニット（セカンダリ アトリビュート）に基づいて認可されるように指定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-dn-attributes EA OU
```

関連コマンド

コマンド	説明
authorization-required	ユーザが接続前に正常に認可されることを必須とします。

authorization-required

ユーザが接続前に正常に認可されることを必須とするには、トンネルグループ ipsec アトリビュート コンフィギュレーション モードで **authorization-required** 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。

authorization-required

no authorization-required

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

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。

コマンドのモード

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 ipsec 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
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

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

例

config-ipsec コンフィギュレーション モードに入る次の例では、remotegrp という名前のリモートアクセス トンネルグループを介して接続するユーザが、完全な DN に基づく認可を受けることを必須としています。最初のコマンドでは、remotegrp という名前のリモート グループのトンネルグループ タイプを ipsec_ra（IPSec リモートアクセス）と設定しています。2 番目のコマンドで、指定したトンネルグループの config-ipsec コンフィギュレーション モードに入り、最後のコマンドで、指定したトンネルグループで認可が必要となるように指定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-required
hostname(config-ipsec)#
```

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	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

authorization-required (webvpn)

WebVPN ユーザまたは電子メール プロキシ ユーザが接続前に正常に認可されることを必須とするには、**authorization-required** 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、このコマンドは適切な電子メール プロキシ モードで使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

authorization-required

no authorization-required

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

デフォルトでは、authorization-required はディセーブルになっています。

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

例

次の例は、WebVPN ユーザが認可を受けることを必須とする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-required
```

関連コマンド

コマンド	説明
authorization-dn-attributes（webvpn）	認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定します。

authorization-server-group

ユーザ認可用の 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 モードで **authorization-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。

authorization-server-group *server group*

no authorization-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 ***no authorization-server-group*** になっています。

コマンドのモード

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	•	—	•	—	—

コマンド履歴

リリース	変更
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

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

VPN 認可が LOCAL と定義されている場合は、デフォルト グループポリシー DfltGrpPolicy に設定されているアトリビュートが適用されます。

例

config-general コンフィギュレーション モードに入る次の例では、「remotegrp」という名前の IPSec リモートアクセス トンネルグループに「aaa-server78」という名前の認可サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
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-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

authorization-server-group (webvpn)

WebVPN またはいずれかの電子メール プロキシで使用する認可サーバ グループを指定するには、**authorization-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、このコマンドは適切な電子メール 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認可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、認可を使用して、ユーザがネットワーク リソースに対して許可されるアクセス レベルを確認します。

authorization-server-group *group tag*

no authorization-server-group

シンタックスの説明

group tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認可サーバは設定されていません。

コマンドのモード

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
7.0(1)	このコマンドが導入されました。

例

次の例は、WebVPNpermit という名前の認可サーバ 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)# authorization-server-group WebVPNpermit
```

次の例は、POP3Spermit という名前の認可サーバ 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)# authorization-server-group POP3Spermit
```

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。

auth-prompt

セキュリティ アプライアンスを介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキ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。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

シンタックスの説明

accept	Telnet 経由のユーザ認証を受け入れる場合に、プロンプトとして *string* を表示します。
prompt	このキーワードの後に、AAA チャレンジ プロンプトの文字列を入力します。
reject	Telnet 経由のユーザ認証を拒否する場合に、プロンプトとして *string* を表示します。
string	235 文字または 31 単語（どちらか最初に達した方）までの英数字で構成される文字列。特殊文字、スペース、および句読点を使用できます。文字列を終了するには、疑問符を入力するか、**Enter** キーを押します。疑問符は文字列に含まれます。

デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示される。
- HTTP ユーザには `HTTP Authentication` が表示される。
- Telnet ユーザにはチャレンジ テキストが表示されない。

コマンドのモード

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
7.0(1)	セマンティックの小さな変更。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要である場合に、セキュリティ アプライアンスを介した HTTP アクセス、FTP アクセス、および Telnet アクセスに対して表示される AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

ユーザ認証が Telnet から発生する場合は、**accept** オプションと **reject** オプションを使用すると、認証試行が AAA サーバで受け入れられたか拒否されたかを示す異なるステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、セキュリティ アプライアンスはユーザに **auth-prompt accept** テキストを表示します（指定されている場合）。認証に失敗すると、**reject** テキストを表示します（指定されている場合）。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストだけが表示されます。**accept** テキストも **reject** テキストも表示されません。

（注）　Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Netscape Navigator では認証プロンプトに最大 120 文字、Telnet および FTP では最大 235 文字表示されます。

例

次の例では、認証プロンプトを「Please enter your username and password」という文字列に設定しています。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

コンフィギュレーションにこの文字列を追加すると、ユーザには次のプロンプトが表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、セキュリティ アプライアンスが認証試行を受け入れたときに表示するメッセージと、拒否したときに表示するメッセージを別々に指定することもできます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次の例では、認証が成功したときの認証プロンプトを「You’re OK.」という文字列に設定しています。

hostname(config)# auth-**prompt accept You’re OK.**

正常に認証されたユーザには、次のメッセージが表示されます。

```
You’re OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプト チャレンジ テキストがある場合、そのテキストを削除して、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-update device-id

Auto Update Server 用のセキュリティ アプライアンス デバイス ID 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 **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

シンタックスの説明

hardware-serial	セキュリティ アプライアンスのハードウェア シリアル番号を使用して、このデバイスを一意に識別します。
hostname	セキュリティ アプライアンスのホスト名を使用して、このデバイスを一意に識別します。
ipaddress [*if_name*]	セキュリティ アプライアンスの IP アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。
mac-address [*if_name*]	セキュリティ アプライアンスの MAC アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。
string *text*	デバイスを Auto Update Server に対して一意に識別するためのテキスト文字列を指定します。

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

デフォルト

デフォルトの ID はホスト名です。

コマンドのモード

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	•	•	•	—	—

例

次の例では、デバイス ID をシリアル番号に設定しています。

```
hostname(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update poll-period

セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。このパラメータをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

シンタックスの説明

poll_period	Auto Update Server をポーリングする頻度を分単位で指定します（1 ～ 35791）。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への最初の接続試行が失敗した後に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続を試行する間隔を分単位で指定します（1 ～ 35791）。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング間隔は 720 分（12 時間）です。

Auto Update Server への最初の接続試行が失敗した後に再接続を試行する回数は、デフォルトでは 0 です。

接続試行のデフォルト間隔は、5 分です。

コマンドのモード

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
7.0	このコマンドが導入されました。

例

次の例では、ポーリング間隔を 360 分に、リトライ回数を 1 回に、リトライ間隔を 3 分に設定しています。

```
hostname(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update server

Auto Update Server 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 **auto-update server** コマンドを使用します。Auto Update Server 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、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM のアップデートがないか調べます。

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

シンタックスの説明

url	Auto Update Server の場所を、シンタックス **http**[**s**]**:**[[*user:password@*]*location* [*:port*]] / *pathname* を使用して指定します。
interface	Auto Update Server に要求を送信する場合に使用するインターフェイスを指定します。
verify_certificate	Auto Update Server によって返される証明書を確認します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

設定できるサーバは 1 台だけです。

自動アップデート機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。

source *interface* 引数に指定したインターフェイスが、**management-access** コマンドで指定したインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネル経由で送信されます。

例

次の例では、Auto Update Server の URL を設定し、インターフェイス outside を指定しています。

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
management-access	セキュリティ アプライアンス上の内部管理インターフェイスにアクセスできるようにします。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update timeout

Auto Update Server へのアクセスに関するタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。このタイムアウト期間内に Auto Update Server にアクセスしないと、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トラフィックを停止させます。タイムアウトを設定することで、セキュリティ アプライアンスのイメージとコンフィギュレーションを常に最新の状態に保つことができます。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout *period*

no auto-update timeout [*period*]

シンタックスの説明

period	タイムアウト期間を分単位で指定します（1 ～ 35791）。デフォルトは 0 で、タイムアウトはありません。タイムアウトを 0 に設定することはできません。タイムアウトを 0 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。

デフォルト

デフォルトのタイムアウトは 0 で、セキュリティ アプライアンスはタイムアウトしないように設定されています。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

タイムアウト状態は、システム ログ メッセージ 201008 で報告されます。

例

次の例では、タイムアウトを 24 時間に設定しています。

```
hostname(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update server	Auto Update Server を指定します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

backup-servers

バックアップ サーバを設定するには、グループポリシー コンフィギュレーション モードで **backup-servers** コマンドを使用します。バックアップ 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。backup-servers アトリビュートを実行コンフィギュレーションから削除するには、引数を付けずにこのコマンドの **no** 形式を使用します。これにより、backup-servers の値を別のグループポリシーから継承できます。

IPSec バックアップ サーバにより、VPN クライアントは、プライマリ セキュリティ アプライアンスが利用できない場合に中央のサイトに接続できます。バックアップ サーバを設定すると、IPSec トンネルが確立されるときにセキュリティ アプライアンスがクライアントにサーバ リストをプッシュします。

backup-servers {server1 server2. . . . server10 | clear-client-config | keep-client-config}

no backup-servers [server1 server2. . . . server10 | clear-client-config | keep-client-config]

シンタックスの説明

clear-client-config	クライアントがバックアップ サーバを使用しないように指定します。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。
keep-client-config	セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないように指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。
server1 server 2.... server10	プライマリ セキュリティ アプライアンスが利用できない場合に VPN クライアントが使用するサーバのリストを入力します。各サーバをスペースで区切って優先度の高い順に並べます。サーバは、IP アドレスまたはホスト名で指定します。リストには 500 文字入力できますが、10 個のエントリしか含めることができません。

デフォルト

クライアントまたはプライマリ セキュリティ アプライアンス上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

コマンドのモード

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
グループポリシー	•	—	•	—	—

コマンド履歴

リリース	変更
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　バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンス上に設定します。セキュリティ アプライアンス上にバックアップ サーバを設定すると、セキュリティ アプライアンスはバックアップ サーバ ポリシーをグループ内のクライアントにプッシュし、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注）　ホスト名を使用する場合は、バックアップ DNS サーバとバックアップ WINS サーバを、プライマリ DNS サーバとプライマリ WINS サーバとは別のネットワーク上に置くことをお勧めします。同一ネットワーク上に置くと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得し、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報および WINS 情報がある場合、DHCP リースが期限切れになるまでクライアントをアップデートできません。さらに、ホスト名を使用するときに DNS サーバが利用できないと、重大な遅延が発生することがあります。

例　次の例は、「FirstGroup」という名前のグループポリシーに IP アドレス 10.10.10.1 および 192.168.10.14 のバックアップ サーバを設定する方法を指定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

セッション バナー、ログイン バナー、または「今日のお知らせ」バナーを設定するには、グローバル コンフィギュレーション モードで ***banner*** コマンドを使用します。指定したバナー キーワード（**exec**、**login**、または **motd**）のすべての行を削除するには、**no banner** コマンドを使用します。

banner {**exec | login | motd** *text*}

[no] banner {**exec | login | motd** [*text*]}

シンタックスの説明

exec	イネーブル プロンプトを表示する前に、バナーを表示するようにシステムを設定します。
login	ユーザが Telnet を使用してセキュリティ アプライアンスにアクセスしたときに、パスワード ログイン プロンプトを表示する前にバナーを表示するようにシステムを設定します。
motd	ユーザが最初に接続したときに「今日のお知らせ」バナーを表示するようにシステムを設定します。
text	表示するメッセージ テキスト行。

デフォルト

デフォルトでは、セッション バナー、ログイン バナー、および「今日のお知らせ」バナーは表示されません。

コマンドのモード

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
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

banner コマンドは、指定したキーワードに対応するバナーを表示するように設定します。*text* 文字列は、最初の空白文字（スペース）の後に続く、行末（復帰または改行（LF））までのすべての文字で構成されます。テキスト内にあるスペースはそのまま表示されます。ただし、CLI ではタブを入力できません。

先にバナーを消去しない限り、後続の *text* エントリは既存バナーの末尾に追加されます。

（注） トークン $(domain) と $(hostname) を使用すると、それぞれセキュリティ アプライアンスのドメイン名とホスト名に置き換えられます。コンテキスト コンフィギュレーションで $(system) トークンを入力すると、コンテキストはシステム コンフィギュレーションに設定されているバナーを使用します。

バナーを複数行にするには、追加する 1 行ごとに banner コマンドを新しく入力します。入力した行は、既存バナーの末尾に追加されていきます。RAM およびフラッシュ メモリの容量による限界を除いて、バナーの長さに制限はありません。

Telnet または SSH でセキュリティ アプライアンスにアクセスする場合、バナー メッセージの処理に必要なシステム メモリが十分にないときや、TCP 書き込みエラーが発生したときは、セッションが閉じます。exec バナーと motd バナーだけが、SSH を介したセキュリティ アプライアンスへのアクセスをサポートしています。login バナーは SSH をサポートしていません。

バナーを置き換えるには、**no banner** コマンドを使用してから、新しい行を追加します。

no banner {**exec** | **login** | **motd**} コマンドは、指定したバナー キーワードのすべての行を削除します。

no banner コマンドでは、テキスト文字列の一部だけを削除できません。このため、**no banner** コマンドの末尾に入力した *text* はすべて無視されます。

例

次の例は、**exec**、**login**、および **motd** の各バナーを設定する方法を示しています。

```
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

次の例は、**motd** バナーにもう 1 行を追加する方法を示しています。

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

関連コマンド

コマンド	説明
clear configure banner	すべてのバナーを削除します。
show running-config banner	すべてのバナーを表示します。

banner (group-policy)

リモート クライアントの接続時にリモート クライアント上でバナー（ウェルカム テキスト）を表示するには、グループポリシー コンフィギュレーション モードで **banner** コマンドを使用します。バナーを削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、バナーを別のグループポリシーから継承できます。バナーを継承しないようにするには、**banner none** コマンドを使用します。

banner {**value** *banner_string* | **none**}

no banner

（注）　VPN グループポリシーで複数のバナーを設定し、いずれかのバナーを削除すると、すべてのバナーが削除されます。

シンタックスの説明

none	バナーにヌル値を設定して、バナーを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーからバナーを継承しないようにします。
value *banner_string*	バナー テキストを設定します。文字列の最大サイズは 500 文字です。復帰を挿入するには、「\n」シーケンスを使用します。

デフォルト

デフォルトのバナーはありません。

コマンドのモード

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
グループポリシー	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例は、「FirstGroup」という名前のグループポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0(1).
```

blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、特権 EXEC モードで **blocks** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50% を超えることはありません。オプションで、メモリ サイズを手動で指定できます。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

シンタックスの説明

memory_size	（オプション）動的な値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50% を超える場合は、警告メッセージが表示されますが、値は受け入れられます。

デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは 2136 バイトです。

コマンドのモード

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
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

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

セキュリティ アプライアンスをリロードすると、メモリ割り当てがデフォルトに戻ります。

例

次の例では、ブロック診断用のメモリ サイズを増やしています。

```
hostname# blocks queue history enable
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やしています。

```
hostname# blocks queue history enable 3000
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やそうとしていますが、値が空きメモリを上回っています。

```
hostname# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やしていますが、値が空きメモリの 50% を超えています。

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

関連コマンド

コマンド	説明
clear blocks	システム バッファの統計情報を消去します。
show blocks	システム バッファの使用状況を表示します。

boot

システムが次回のリロードで使用するシステム イメージ、およびシステムが起動時に使用するコンフィギュレーション ファイルを指定するには、特権 EXEC モードで **boot** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

boot {**config** | ***system***} *url*

no boot {***config*** | ***system***} *url*

シンタックスの説明

config	システムがロードされるときに使用するコンフィギュレーション ファイルを指定します。
system	システムがロードされるときに使用するシステム イメージ ファイルを指定します。
url	コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL シンタックスを参照してください。 • ***disk0:/***[*path/*]*filename* このオプションは ASA プラットフォームだけに使用でき、内部フラッシュ カードを示します。***disk0*** の代わりに ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* このオプションは ASA プラットフォームだけで使用でき、外部フラッシュ カードを示します。 • ***flash:/***[*path/*]*filename* • ***tftp://***[*user*[*:password*]**@**]*server*[*:port*]**/**[*path/*]*filename*

デフォルト

boot config コマンドを指定しない場合は、スタートアップ コンフィギュレーションが非表示の場所に保存され、スタートアップ コンフィギュレーションを利用するコマンド（**show startup-config** コマンドや **copy startup-config** コマンド）だけで使用されます。

boot system コマンドにデフォルトはありません。BOOT 環境変数が設定されていない場合、システムは内部フラッシュ内を検索し、起動する最初の有効なイメージを探します。有効なイメージが見つからない場合、システム イメージはロードされず、システムは ROMMON モードまたは Monitor モードに入るまでブート ループ状態になります。

最大 4 つの **boot system** コマンド エントリを入力し、異なるイメージを指定して、順番に起動を試みることができます。セキュリティ アプライアンスは、最初に見つけた有効なイメージを起動します。

（注）　PIX プラットフォームの **boot system** コマンドは、TFTP ロケーションを使用したイメージのロードをサポートしていません。

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
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
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

boot config コマンドを使用する場合、現在動作中のメモリで CONFIG_FILE 環境変数を設定します。この変数は、システムが起動時にロードするコンフィギュレーション ファイルを指定します。

（注）　**boot system tftp:** コマンドは、1 つしか設定できず、最初に設定する必要があります。**no boot system** コマンドを発行しない限り、後続の複数の **boot system tftp:** コマンドは失敗します。

このグローバル コンフィギュレーション コマンドを使用する場合、影響を受けるのは実行コンフィギュレーションだけです。この環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、**write memory** コマンドまたは **copy** コマンドを使用します。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存すると、設定済みのファイルも実行コンフィギュレーションによって上書きされることに注意してください。そのため、この変数を変更して ***write memory*** コマンドを実行してから、新しいコンフィギュレーション ファイルを、設定した名前にコピーします。

システムは boot system コマンドを、コンフィギュレーション ファイルに入力した順に、保存および実行します。リロード時にそのコンフィギュレーションを実行するには、***write memory*** コマンドまたは ***copy*** コマンドを使用して、その環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存します。

ヒント　ASDM イメージ ファイルは、**asdm image** コマンドで指定します。

例

次の例は、起動時にセキュリティ アプライアンスが configuration.txt という名前のコンフィギュレーション ファイルをロードするように指定しています。

```
hostname(config)# boot config configuration.txt
```

関連コマンド

コマンド	説明
asdm image	ASDM ソフトウェア イメージを指定します。
show bootvar	ブート ファイルおよびブート コンフィギュレーションのプロパティを表示します。