aaa accounting ～ accounting-server-group コマンド

aaa accounting command

CLI で **show** コマンド以外のコマンドを入力したときに TACACS+ アカウンティング サーバにアカウンティング メッセージを送信するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを入力します。コマンド アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトの特権レベルは 0 です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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

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

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

関連コマンド

コマンド	説明
aaa accounting	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
clear configure aaa	設定した 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

管理者アクセスの AAA アカウンティングのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting console** コマンドを使用します。管理者アクセスの AAA アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

関連コマンド

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

aaa accounting include、exclude

ASA を介した TCP または UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting include** コマンドを使用します。アカウンティングからアドレスを除外するには、**aaa accounting exclude** コマンドを使用します。アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

outside_mask	(任意)外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
server_tag	**aaa-server host** コマンドで定義した AAA サーバ グループを指定します。
service	アカウンティングが必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**(すべての TCP トラフィックを指定します) • **ftp** • **http** • **https** • **ssh** • **Telnet** • **tcp/***port* • **udp/***port*

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

例

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

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

関連コマンド

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

aaa accounting match

ASA を介した TCP および UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting match** コマンドを使用します。トラフィックのアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

構文の説明

acl_name	ACL 名の一致によるアカウンティングが必要なトラフィックを指定します。ACL 内の permit エントリはアカウンティングの対象となり、deny エントリはアカウンティングから免除されます。このコマンドは、TCP トラフィックおよび UDP トラフィックについてのみサポートされます。このコマンドを入力し、他のプロトコルを許可する ACL をこのコマンドが参照している場合、警告メッセージが表示されます。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

例

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

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

関連コマンド

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

aaa authentication console

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

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

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

構文の説明

イネーブル化	**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証します。
http	HTTPS で ASA にアクセスする ASDM ユーザを認証します。デフォルトでは、ASDM は空白のユーザ名とイネーブル パスワードを受け入れ、このコマンドを設定しなくても認証にローカル データベースを使用することもできます。このコマンドは、空白のユーザ名とイネーブル パスワードによるログインを許可しません。 **aaa** コマンドが定義されているが、HTTPS 認証によってタイムアウトが要求される場合（AAA サーバがダウンしているか使用できないことを意味する）は、空白のユーザ名とイネーブル パスワードを使用して、ASA 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。

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

server-tag [**LOCAL**]	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。HTTPS 管理認証では AAA サーバ グループ用に SDI プロトコルがサポートされません。 *server-tag* 引数に加えて **LOCAL** キーワードを使用すると、AAA サーバを使用できない場合に、フォールバック方式としてローカル データベースを使用するように ASA を設定できます。**LOCAL** キーワードは大文字と小文字が区別されます。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、いずれの方式が使用されているかが示されないためです。
serial	シリアル コンソール ポートを使用して ASA にアクセスするユーザを認証します。
ssh	SSH を使用して ASA にアクセスするパスワードを持つユーザを認証します。ローカル **ユーザ名**の場合、**ssh authentication** コマンドを使用したパスワード認証の代わりに、公開キー認証を有効にすることができます。バージョン 9.6(2) および 9.7(1) では、**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。 9.6(1) 以前および 9.6(3)/9.8(1) 以降では、**aaa authentication ssh console LOCAL** コマンドを公開キー認証用に設定する必要はありません。このコマンドはパスワードを持つユーザにのみ適用され、LOCAL だけでなく任意のサーバ タイプを指定できます。たとえば、ローカル データベースを使用し、公開キー認証を利用できるユーザもいれば、RADIUS とともにパスワードを使用できるユーザもいます。
Telnet	Telnet を使用して ASA にアクセスするユーザを認証します。**aaa authentication telnet console** コマンドが定義されていない場合は、ASA のログイン パスワード（**password** コマンドで設定）で、ASA CLI にアクセスできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカル ユーザを定義する必要があります。ローカル ユーザを定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
9.6(2)	**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。
9.6(3)/9.8(1)	SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。AAA SSH 認証（**aaa authentication ssh console**）を明示的にイネーブルにする必要がなくなりました。ユーザに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトでイネーブルになります。さらに、AAA SSH 認証を明示的に設定すると、この設定はパスワード付きのユーザ名にのみ適用され、任意の AAA サーバ タイプを使用できます。

使用上のガイドライン

ASA で Telnet、SSH、または HTTPS ユーザを認証する前に、**telnet** コマンド、**ssh** コマンド、または **http** コマンドを使用して ASA へのアクセスを設定する必要があります。これらのコマンドでは、ASA との通信を許可する IP アドレスを指定します。

ASA へのログイン

ASA に接続した後、ログインしてユーザ EXEC モードにアクセスします。

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

特権 EXEC モードへのアクセス

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

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

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

ASDM へのアクセス

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

HTTPS 認証では AAA サーバ グループ用の SDI プロトコルがサポートされません。HTTPS 認証のユーザ名プロンプトの最大長は 30 文字です。パスワードの最大長は 16 文字です。

システム実行スペースでの AAA コマンドのサポートなし

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

許可されるログイン試行の回数

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

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

例

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

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

次に、サーバ グループ「AuthIn」を enable 認証用に指定する例を示します。

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

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

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

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザ認証に使用する AAA サーバを指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
ldap map-attributes	LDAP 属性を、ASA で認識できる RADIUS 属性にマッピングします。
service-type	ローカル ユーザの CLI アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication include、exclude

ASA を経由する接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication include** コマンドを使用します。認証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。認証からアドレスを除外するには、**aaa authentication exclude** コマンドを使用します。認証からアドレスを除外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。

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

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

構文の説明

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

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

一度だけの認証

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

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

認証確認を受けるために必要なアプリケーション

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

ASA が AAA 用にサポートしている認証ポートは固定値です。

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

ASA 認証プロンプト

Telnet および FTP の場合、ASA は認証プロンプトを生成します。

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

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

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

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

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

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

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

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

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

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

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

スタティック PAT および HTTP

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

たとえば、次のように、外部 TCP ポート 889 がポート 80（www）に変換され、関係するすべての ACL でこのトラフィックが許可されるとします。

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

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

次の例のように、ローカル ポートがポート 80 ではないとします。

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

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

ASA での直接認証

HTTP、HTTPS、Telnet、または FTP が ASA を通過することを許可せず、他のタイプのトラフィックに対しては認証を求める場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して ASA で直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL で ASA の直接認証を受けることができます。

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

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザは ASA 上で設定された所定の IP アドレスに Telnet で接続し、ASA が Telnet プロンプトを表示します。

例

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

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

次に、*interface-name* パラメータの使用方法を示す例を示します。ASA には、内部ネットワーク 192.168.1.0、外部ネットワーク 209.165.201.0（サブネット マスク 255.255.255.224）、および境界ネットワーク 209.165.202.128（サブネット マスク 255.255.255.224）があります。

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

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

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

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

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

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

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

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

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

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

関連コマンド

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

aaa authentication listener

HTTP/HTTPS リスニング ポートでネットワーク ユーザを認証できるようにするには、グローバル コンフィギュレーション モードで **aaa authentication listener** コマンドを使用します。リスニング ポートをイネーブルにすると、ASAでは直接接続に対して、およびオプションで通過トラフィックに対して認証ページを提供します。リスナーをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication listener {**http** | **https**} *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener {**http** | **https**} *interface_name* [**port** *portnum*] [**redirect**]

構文の説明

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

デフォルト

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

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

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。

使用上のガイドライン　**aaa authentication listener** コマンドを使用しないと、**aaa authentication match** または **aaa authentication include** コマンドの設定後に HTTP/HTTPS ユーザが ASA で認証する必要があるときに、ASA では基本 HTTP 認証が使用されます。HTTPS の場合、ASA はカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードを指定して設定すると、ASA により、すべての HTTP/HTTPS 認証要求は ASA によって提供される Web ページにリダイレクトされます。

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

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

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

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

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

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

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

例

次に、HTTP および HTTPS 接続をデフォルトのポートにリダイレクトするように ASA を設定する例を示します。

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
```

次に、ASA への直接認証要求を許可する例を示します。通過トラフィックによって基本 HTTP 認証が使用されます。

```
ciscoasa(config)# aaa authentication listener http inside
ciscoasa(config)# aaa authentication listener https inside
```

次に、HTTP および HTTPS 接続をデフォルト以外のポートにリダイレクトするように ASA を設定する例を示します。

```
ciscoasa(config)# aaa authentication listener http inside port 1100 redirect
ciscoasa(config)# aaa authentication listener https inside port 1400 redirect
```

関連コマンド

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

aaa authentication login-history

ログイン履歴の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 **aaa authentication login-history** コマンドを使用します。ログイン履歴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 login-history duration *days*

no aaa authentication login-history [**duration** *days*]

構文の説明

duration *days*	1 ～ 365 の範囲で日数を設定します。デフォルトは 90 です。

コマンドデフォルト

デフォルトは、90 日です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上の CLI 管理方式（SSH、Telnet、シリアル コンソール）でローカル AAA 認証をイネーブルにした場合、AAA サーバのユーザ名またはローカル データベースのユーザ名にこの機能が適用されます。

ASDM のログインは履歴に保存されません。

ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。

ログインの履歴データは、リロードされると保持されなくなります。

ログイン履歴を表示するには、**show aaa login-history** コマンドを使用します。

例

次に、ログイン履歴を 365 日に設定する例を示します。

```
ciscoasa(config)# aaa authentication login-history duration 365
```

ユーザがログインすると、以下の SSH の例のように、自身のログイン履歴が表示されます。

```
cugel@10.86.194.108's password:
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

関連コマンド

コマンド	説明
password-history	直前の **username** パスワードを保存します。ユーザはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザを設定します。

aaa authentication match

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

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

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

構文の説明

acl_name	拡張 ACL 名を指定します。
interface_name	ユーザを認証するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。
user-identity	アイデンティティ ファイアウォールにマッピングされるユーザ アイデンティティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**user-identity** キーワードが追加されました。

使用上のガイドライン

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

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

One-Time 認証

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

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

認証チャレンジの受信に必要なアプリケーション

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

ASA が AAA 用にサポートしている認証ポートは固定値です。

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

ASA 認証プロンプト

Telnet および FTP の場合、ASA は認証プロンプトを生成します。

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

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

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

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

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

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

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

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

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

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

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

スタティック PAT と HTTP

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

たとえば、次のように、外部 TCP ポート 889 がポート 80（www）に変換され、関係するすべての ACL でこのトラフィックが許可されるとします。

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

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

次の例のように、ローカル ポートがポート 80 ではないとします。

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

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

ASA での直接認証

HTTP、HTTPS、Telnet、または FTP が ASA を通過することを許可せず、他のタイプのトラフィックに対しては認証を求める場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して ASA で直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL でASAの直接認証を受けることができます。

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

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザは ASA 上で設定された所定の IP アドレスに Telnet で接続し、ASA が Telnet プロンプトを表示します。

例

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

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

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

このコンテキストでは、次のコマンドは

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

次のコマンドと同じです。

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

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

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

その後で、次のコマンドを入力します。

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

ASA は、まず **mylist** 内の **access-list** コマンド ステートメント グループに一致があるか確かめ、次に **yourlist** 内の **access-list** コマンド ステートメント グループに一致があるかを確かめます。

ASA を介した接続の認証をイネーブルにして、アイデンティティ ファイアウォール機能と照合するには、次のコマンドを入力してください。

```
ciscoasa(config)# aaa authenticate match access_list_name inside user-identity
```

関連コマンド

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

aaa authentication secure-http-client

SSL をイネーブルにし、HTTP クライアントと ASA の間のユーザ名とパスワードのセキュアな交換をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication secure-http-client** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication secure-http-client

no aaa authentication secure-http-client

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa authentication secure-http-client コマンドによって、ユーザの HTTP ベース Web 要求が ASA を通過するのを許可する前に、ASA に対するセキュアなユーザ認証方式が提供されます。このコマンドは、SSL による HTTP カットスルー プロキシ認証に使用されます。

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

- 実行時に、最大で 64 個の HTTPS 認証プロセスが許可されます。64 個の HTTPS 認証プロセスすべてが実行されている場合、認証を必要とする 65 番目の新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されると（**uauth timeout** が 0 に設定される）、HTTPS 認証は機能しない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この状況を回避するには、**timeout uauth 0:0:1** コマンドで **uauth timeout** を 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。
- HTTPS 認証は SSL ポート 443 で行われるため、HTTP クライアントから HTTP サーバ ポート 443 へのトラフィックをブロックするように、**access-list** コマンド ステートメントを設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、最初の行でスタティック PAT が Web トラフィックに対して設定されるため、HTTPS 認証コンフィギュレーションをサポートするために 2 番めの行を追加する必要があります。

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

例

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

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

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

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

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

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

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

関連コマンド

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

aaa authorization command

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

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

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

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

aaa authorization command コマンドでは、CLI でのコマンド実行が認可の対象かどうかを指定します。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。コマンドへのアクセスを制御する場合には、ASA にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

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

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

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

セキュリティ コンテキストとコマンド許可

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

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

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

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

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

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

  コマンド許可を設定する場合は、次の点を考慮します。

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

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

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

ローカル コマンド認可の前提条件

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

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

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

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

- RADIUS が認証に使用されている場合、**aaa authorization exec** コマンドを使用して、RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにすることができますが、必須ではありません。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可もイネーブルにします。
- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：**username** コマンドを使用して、ローカル データベース内のユーザを特権レベル 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。
- コマンド特権レベルの設定については、**privilege** コマンドを参照してください。

TACACS+ コマンド認可

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

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

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

TACACS+ サーバの設定については、CLI 設定ガイドを参照してください。

TACACS+ コマンド認可の前提条件

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

例

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

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

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

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

関連コマンド

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

aaa authorization exec

管理認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization exec** コマンドを使用します。管理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 exec {**authentication-server** | **LOCAL**} [**auto-enable**]

no aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

構文の説明

authentication-server	ユーザの認証に使用されたサーバから認可属性が取得されることを指定します。
auto-enable	十分な認可特権を持つ管理者が認証クレデンシャルを一度入力すると、特権 EXEC モードを開始できるようにします。
LOCAL	認証方法に関係なく、認可属性が ASA のローカル ユーザ データベースから取得されることを示します。

デフォルト

デフォルトでは、このコマンドはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(2)	**LOCAL** オプションが追加されました。
9.2(1)	**auto-enable** オプションが追加されました。
9.4(1)	この CLI は HTTP 以外の管理セッションにだけ適用されます。

使用上のガイドライン

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

no aaa authorization exec コマンドによる管理認可をディセーブルにする場合、次の点に注意してください。

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

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

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

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

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

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

- TACACS+ ユーザ:「service=shell」エントリで認可を要求し、サーバは次のように PASS または FAIL で応答します。
  - PASS、特権レベル 1 は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

- PASS、特権レベル 2 以上は、**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
- FAIL は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。

- ローカル ユーザ：**service-type** コマンドを設定します。これは、**username** コマンドのユーザ名コンフィギュレーション モードです。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、ローカル データベースを使用して管理認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization exec LOCAL
```

関連コマンド

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

aaa authorization http

ASDM の認可をイネーブルにするには、**aaa authorization http** コマンドを使用します。ASDM のユーザ名の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 http console LOCAL | <aaa-server-group>

[no] aaa authorization http console LOCAL | <aaa-server-group>

構文の説明

aaa-server-group	aaa サーバ　グループに対してすでに定義され、設定されたプロトコルは、LDAP、RADIUS、または TACACS+ である必要があります。プロトコルが LDAP、RADIUS、または TACACS+ でない場合は、コマンドに効力はありません。
console	管理認可用のサーバ グループを識別するには、このキーワードを指定します。
LOCAL	AAA プロトコル「local」に事前に定義されたサーバ タグです。

デフォルト

ASDM のユーザ名認証はデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、webvpn（ASA 1000v）をサポートしないプラットフォームや、No Payload Encryption（NPE）がイネーブルになっているプラットフォームでは使用できません。

例

```
5520-1(config)# aaa ?

configure mode commands/options:
  accounting      Configure user accounting parameters
  authentication  Configure user authentication parameters
  authorization   Configure user authorization parameters
  local           AAA Local method options
  mac-exempt      Configure MAC Exempt parameters
  proxy-limit     Configure number of concurrent proxy connections allowed per
                  user
5520-1(config)# aaa authorization ?

configure mode commands/options:
  command  Specify this keyword to allow command authorization to be configured
           for all administrators on all consoles
  exclude  Exclude the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  exec     Perform administrative authorization for console connections(ssh,
           telnet and enable) configured for authentication to RADIUS,
           LDAP, TACACS or LOCAL authentication servers.
  include  Include the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  match    Specify this keyword to configure an ACL to match
  http     Perform administrative authorization for http connections

5520-1(config)# aaa authorization http ?

configure mode commands/options:
  console  Specify this keyword to identify a server group for administrative
           authorization
5520-1(config)# aaa authorization http console ?
```

```
configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Name of RADIUS,LDAP or TACACS+ aaa-server group for administrative
         authorization
```

aaa authorization include、exclude

ASA を介した接続の認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization include** コマンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。認可からアドレスを除外するには、**aaa authorization exclude** コマンドを使用します。認可からアドレスを除外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。

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

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

構文の説明

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

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

デフォルト

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

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**exclude** パラメータを使用すると、ユーザは特定のホストに対して除外するポートを指定できます。

使用上のガイドライン

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

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

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

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

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

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

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

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

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

例

次に、TACACS+ プロトコルを使用する例を示します。

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

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

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

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

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

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

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

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

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

関連コマンド

コマンド	説明
aaa authorization command	コマンドの実行が認可の対象かどうかを指定します。または、指定したサーバ グループ内のすべてのサーバがディセーブルである場合に、ローカル ユーザ データベースへのフォールバックをサポートするように管理認可を設定します。
aaa authorization match	特定の access-list コマンド名に対して LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
clear configure aaa	設定した 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

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

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

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

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

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

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

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

例

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

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

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

関連コマンド

コマンド	説明
aaa authorization	ユーザ許可をイネーブルまたはディセーブルにします。
clear configure aaa	すべての AAA コンフィギュレーションのパラメータをデフォルト値にリセットします。
clear uauth	ある特定のユーザまたはすべてのユーザの AAA 許可および認証キャッシュを削除します。次回接続を作成するときには再認証の必要が生じます。
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および許可の目的で許可サーバに提供されているユーザ名、ユーザ名がバインドされている IP アドレス、およびユーザが認証されただけであるか、キャッシュされたサービスを持っているかを表示します。

aaa local authentication attempts max-fail

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

aaa local authentication attempts max-fail *number*

構文の説明

number	ユーザがロック アウトされるまでに間違ったパスワードを入力できる最大回数。この数の範囲は、1 ～ 16 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ローカル ユーザ データベースによる認証だけに影響します。このコマンドを省略すると、ユーザが間違ったパスワードを入力できる回数に制限は設けられません。

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

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

ユーザが正常に認証されるか、ASA がリブートされると、失敗試行回数は 0 にリセットされ、ロックアウト ステータスは No にリセットされます。

例

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

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

関連コマンド

コマンド	説明
clear aaa local user lockout	指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更することなく、ユーザ認証試行の失敗回数をゼロにリセットします。
show aaa local user	現在ロックされているユーザ名のリストを表示します。

aaa mac-exempt

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

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

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

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

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

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

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

関連コマンド

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

aaa proxy-limit

特定の IP アドレスの同時認証試行数を制限するには、グローバル コンフィギュレーション モードで **aaa proxy-limit** コマンドを使用します。デフォルトのプロキシ制限値に戻すには、このコマンドの **no** 形式を使用します。

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

構文の説明

disable	プロキシを許可しないことを指定します。
proxy_limit	ユーザごとに許可される同時プロキシ接続数（1 ～ 128）を指定します。

デフォルト

デフォルトのプロキシ制限値は 16 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

たとえば、ターミナル サーバに接続しているなどの理由で、同じ IP アドレスを使用する 2 人のユーザがブラウザまたは接続を開き、正確に同時に認証を開始しようとした場合、1 人のみが許可され、2 人目はブロックされます。

その IP アドレスからの最初のセッションは代行処理されて認証要求が送信され、もう 1 つのセッションはタイムアウトします。このことは、単一ユーザ名の接続数とは関係ありません。

例

次に、特定の IP アドレスについて未処理認証試行の最大数（同時）を設定する例を示します。

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

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上で、LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルに設定したり、表示したりします。または ASDM ユーザ認証をイネーブルまたはディセーブルにしたり、表示したりします。
aaa authorization	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	設定した 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

AAA サーバ グループを作成し、すべてのグループ ホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server** コマンドを使用します。指定したグループを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

protocol *server-protocol*	グループ内のサーバによってサポートされる AAA プロトコルを指定します。 • **http-form** • **kerberos** • **ldap** • **nt**（このオプションは、9.3(1) リリース以降は使用できないことに注意してください） • **radius** • **sdi** • **tacacs+**
server-tag	サーバ グループ名を指定します。**aaa-server host** コマンドで指定した名前と同じにします。他の AAA コマンドで、この AAA サーバ グループ名を参照します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	**http-form** プロトコルが追加されました。
8.2(2)	AAA サーバ グループの最大数が、シングル モードで 15 から 100 に増やされました。
8.4(2)	AAA サーバ グループ コンフィギュレーション モードで、**ad-agent-mode** オプションが追加されました。
9.3(1)	**nt** オプションが使用できなくなりました。Windows NT ドメイン認証のサポートが廃止されました。

使用上のガイドライン

シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。各グループには、シングルモードで最大 15 台、マルチモードで最大 4 台のサーバを含めることができます。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

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

RADIUS プロトコルを使用する場合、AAA サーバ グループ コンフィギュレーション モードでは、次のことに注意してください。

- クライアントレス SSL および AnyConnect セッションについてマルチセッション アカウンティングをイネーブルにするには、**interim-accounting-update** オプションを入力します。このオプションを選択すると、開始レコードと終了レコード以外に中間アカウンティング レコードが RADIUS サーバに送信されます。
- ASA と AD エージェントとの間の共有秘密を指定し、RADIUS サーバ グループにフル機能の RADIUS サーバではない AD エージェントを含めることを示すには、**ad-agent-mode** オプションを入力します。ユーザ アイデンティティに関連付けることができるのは、このオプションを使用して設定された RADIUS サーバ グループのみです。結果として、**ad-agent-mode** オプションを使用して設定されていない RADIUS サーバ グループを指定すると **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* コマンドが使用できなくなります。

(注) ASA では、**aaa-server protocol nt** コマンドが入力されたり、起動時にコンフィギュレーションから読み取られたりした場合には必ず、コンソールにメッセージが表示されます。このメッセージは、この認証方式が ASA の次のメジャー リリースで削除されることを示します。

例

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

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

関連コマンド

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

aaa-server active、fail

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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

例

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

```
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
ciscoasa# aaa-server active host 192.168.125.60
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

関連コマンド

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

aaa-server host

AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。ホスト コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトのタイムアウト値は 10 秒です。

デフォルトのインターフェイスは、inside です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	DNS 名のサポートが追加されました。
9.0(1)	ユーザ アイデンティティのサポートが追加されました。
9.9(2)	Radius サーバの IPv6 アドレッシングおよび Radius サーバへの接続のサポートが追加されました。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト コンフィギュレーション モードが開始されます。このモードから、ホスト固有の AAA サーバ接続データを指定および管理できます。

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

例

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

(注) Kerberos 領域名では数字と大文字だけを使用します。ASA は領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

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

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

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

次の例では、LDAP 検索に **aaa-server** *aaa_server_group_tag* コマンドを使用する際に、検索パスをターゲット グループに絞り込む方法を示しています。

```
ciscoasa(config)# aaa-server CISCO_AD_SERVER protocol ldap
ciscoasa(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
ciscoasa(config-aaa-server-host)# server-port 636
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password *
ciscoasa(config-aaa-server-host)# ldap-login-dn CISCO\username1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
```

(注) **ldap-group-base-dn** コマンドが指定されている場合、すべてのグループが LDAP ディレクトリ階層内のこのレベルの下に存在する必要があり、このパスの外部にグループが存在することはできません。

ldap-group-base-dn コマンドは、アクティブな user-identity ベースのポリシーが少なくとも 1 つ存在する場合にのみ有効です。

server-type microsoft コマンドはデフォルトではありませんが、設定する必要があります。

最初の **aaa-server** *aaa_server_group_tag* **host** コマンドは、LDAP 操作に使用されます。

関連コマンド

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

absolute

時間範囲が有効である場合に絶対時間を定義するには、時間範囲コンフィギュレーション モードで **absolute** コマンドを使用します。時間範囲に時間を指定しない場合は、このコマンドの **no** 形式を使用します。

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

no absolute

構文の説明

date	（オプション）日付を day month year 形式で指定します（たとえば、1 January 2006）。年の有効な範囲は、1993 ～ 2035 です。
end	（任意）時間範囲の終了日時を指定します。
start	（任意）時間範囲の開始日時を指定します。
time	（任意）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

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	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	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

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

```
ciscoasa(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	ASA 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。
デフォルト	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
定期	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 ASA のアクセス コントロールを定義します。

accept-subordinates

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

accept-subordinates

no accept-subordinates

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定はオンです（下位証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

関連コマンド

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

access-group

拡張 ACL または EtherType ACL を 1 つの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。ACL をインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

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

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

1 組のグローバル拡張ルールを 1 つのコマンドですべてのインターフェイスに適用するには、グローバル コンフィギュレーション モードで **access-group global** コマンドを使用します。設定済みのすべてのインターフェイスからグローバル ル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。

access-group *access_list* [**global**]

no access-group *access_list* [**global**]

構文の説明

access_list	拡張 ACL の名前。ブリッジ グループ メンバー インターフェイスの場合は、Ethertype ACL を指定することもできます。
control-plane	（オプション）ACL が to-the-box トラフィック用であるかどうかを指定します。たとえば、このオプションを使用し、ISAKMP をブロックすることによって、特定のリモート IP アドレスが ASA への VPN セッションを開始できないようにすることができます。to-the-box 管理トラフィック用のアクセス ルール（**http**、**ssh**、**telnet** などのコマンドで定義）は、**control-plane** オプションで適用される ACL よりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。このオプションは、**in** 方向にのみ使用可能です。
global	すべてのインターフェイスのすべてのトラフィックに ACL を適用します。
in	指定されたインターフェイスでインバウンド方向に ACL を適用します。
interface *interface_name*	ネットワーク インターフェイスの名前。 ルーテッド モードでは、ブリッジ仮想インターフェイス（BVI）とそのメンバー インターフェイスの両方に拡張 ACL を適用できます。トランスペアレント モードでは、メンバー インターフェイスにのみ拡張 ACL を適用できます。両方のモードでは、メンバー インターフェイスにのみ Ethertype ACL を適用できます。
out	指定されたインターフェイスでアウトバウンド方向に ACL を適用します。
per-user-override	（オプション）ダウンロード可能なユーザ ACL によって、インターフェイスに適用されている ACL を上書きできます。このオプションは、**in** 方向にのみ使用可能です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	このコマンドは、グローバル ポリシーをサポートするように変更されました。
9.7(1)	このコマンドは、ルーテッド モードで、BVI に拡張アクセス グループを適用し、ブリッジ グループ メンバー インターフェイスに Ethertype ACL を適用できるように変更されました。

使用上のガイドライン

インターフェイス固有のアクセス グループ ルールがグローバル ルールに優先されるため、パケットの分類時はインターフェイス固有のルールがグローバル ルールの前に処理されます。

ルーテッド モードでは、BVI とそのメンバー インターフェイスの両方にアクセス グループを適用した場合、優先順位は方向によって異なります。インバウンドでは、メンバー インターフェイスのアクセス グループが最初にチェックされ、次に BVI アクセス グループ、最後にグローバル グループがチェックされます。アウトバウンドでは、BVI アクセス グループが最初にチェックされ、次にメンバー インターフェイスのアクセス グループがチェックされます。

インターフェイス固有ルールの使用上のガイドライン

access-group コマンドは、インターフェイスに拡張 ACL をバインドします。ACL を作成するには、最初に **access-list extended** コマンドを使用する必要があります。

インターフェイスに対して着信または発信するトラフィックに ACL を適用できます。**access-list** コマンド ステートメントで **permit** オプションを入力すると、ASA によってパケットの処理は続行されます。**access-list** コマンド ステートメントで **deny** オプションを入力すると、ASA によってパケットが廃棄され、syslog message 106023（または、デフォルト以外のロギングを使用する ACE の場合には 106100）が生成されます。

インバウンド ACL の場合、**per-user-override** オプションを使用すると、ダウンロードされた ACL によって、インターフェイスに適用されている ACL を上書きできます。**per-user-override** オプションを指定しないと、ASA 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、ASA により、ユーザに関連付けられているユーザごとのアクセス リスト（ダウンロードされた場合）の **permit** または **deny** ステータスで、**access-group** コマンドに関連付けられている ACL の permit または deny ステータスを上書きできるようになります。さらに、次のルールが適用されます。

- パケットが到着した時点で、そのパケットに関連付けられているユーザごとの ACL がない場合、インターフェイス ACL が適用されます。
- ユーザごとの ACL は、**timeout** コマンドの **uauth** オプションで指定されたタイムアウト値によって管理されますが、このタイムアウト値は、ユーザごとの AAA セッション タイムアウト値によって上書きできます。
- 既存の ACL ログ動作は同じです。たとえば、ユーザごとの ACL が原因でユーザ 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。

デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、**no sysopt connection permit-vpn** コマンドを使用してこのバイパスをオフにする場合、動作は、グループ ポリシーに適用される **vpn-filter** があるかどうか、および **per-user-override** オプションを設定するかどうかによって異なります。

- **per-user-override** なし、**vpn-filter** なし: トラフィックはインターフェイス ACL と照合されます。
- **per-user-override** なし、**vpn-filter**: トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
- **per-user-override**、**vpn-filter**: トラフィックは VPN フィルタのみと照合されます。

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

グローバル ルールの使用上のガイドライン

access-group global コマンドは、ASA でトラフィックが到着するインターフェイスにかかわらず、すべてのトラフィックに対して 1 組のグローバル ルールを適用します。

すべてのグローバル ルールは、入力（着信）方向のトラフィックにのみ適用されます。グローバル ルールは出力（発信）トラフィックには適用されません。グローバル ルールが着信インターフェイス アクセス ルールと組み合わせて設定された場合、インターフェイス アクセス ルール（特定のルール）がグローバル アクセス ルール（一般のルール）よりも前に処理されます。

例

次に、**access-group global** コマンドを使用して、設定済みのすべてのインターフェイスに ACL を適用する例を示します。

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any

ciscoasa(config)# access-group acl-1 in interface outside
ciscoasa(config)# access-group acl-2 global
```

上記のルールでは、出力インターフェイスで 10.1.2.2 から 10.2.2.2 にトラフィックを通過させ、10.1.1.10 から 10.2.2.20 へのトラフィックはグローバル拒否ルールによりドロップします。この access-group コンフィギュレーションによって、分類テーブルに次のルールが追加されます（**show asp table classify** コマンドからの出力）。

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
```

```
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

次に、任意のアドレスから DMZ 内の HTTP サーバ（IP アドレス 10.2.2.2）へのグローバル アクセスを許可する例を示します。

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

上記のルールは、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への HTTP 接続を許可し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への HTTP 接続を許可します。

次に、グローバル ポリシーとインターフェイス ポリシーを一緒に使用する方法の例を示します。この例では、任意の内部ホストからサーバ（IP アドレス 10.2.2.2）へのアクセスは許可しますが、他のホストからサーバへのアクセスを拒否します。インターフェイス ポリシーが優先されます。

```
ciscoasa(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
ciscoasa(config)# access-list global_acl deny ip any host 10.2.2.2
ciscoasa(config)# access-group inside_acl in interface inside
ciscoasa(config)# access-group global_acl global
```

上記のルールは、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への SSH 接続を拒否し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への SSH 接続を許可します。

次に、NAT とグローバル アクセス コントロール ポリシーを一緒に機能させる方法の例を示します。この例では、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への 1 つの HTTP 接続を許可し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への別の HTTP 接続を許可し、外部ホスト 10.255.255.255 からホスト 172.31.255.255 への 1 つの HTTP 接続を（暗黙ルールによって）拒否します。

```
ciscoasa(config)# object network dmz-server host 10.1.1.2
ciscoasa(config)# nat (any, any) static 10.2.2.2
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

次に、NAT とグローバル アクセス コントロール ポリシーを一緒に機能させる方法の例を示します。この例では、ホスト 10.1.1.1 からホスト 192.168.0.0, への 1 つの HTTP 接続を許可し、ホスト 209.165.200.225 からホスト 172.16.0.0 への別の HTTP 接続を許可し、ホスト 10.1.1.1 からホスト 172.16.0.0 への 1 つの HTTP 接続を拒否します。

```
ciscoasa(config)# object network 10.1.1.1 host 10.1.1.1
ciscoasa(config)# object network 172.16.0.0 host 172.16.0.0
ciscoasa(config)# object network 192.168.0.0 host 192.168.0.0
ciscoasa(config)# nat (inside, any) source static 10.1.1.1 10.1.1.1 destination static
                  192.168.0.0 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip object 10.1.1.1 object 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip host 209.165.200.225 object 172.16.0.0
ciscoasa(config)# access-list global_acl deny ip any 172.16.0.0
ciscoasa(config)# access-group global_acl global
```

関連コマンド

コマンド	説明
access-list extended	拡張 ACL を作成します。
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	インターフェイスにバインドされている現在の ACL を表示します。

access-list alert-interval

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

access-list alert-interval *secs*

no access-list alert-interval

構文の説明

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

デフォルト

デフォルトは 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ACL deny ステートメントに **log** オプションを設定している場合、トラフィック フローが ACL ステートメントと一致すると、アプライアンスによってフロー情報がキャッシュされます。キャッシュの過負荷を避けるために、syslog メッセージ 106100 で示される統計情報のために保持されるキャッシュ拒否フローの最大数が設定されています。106100 が発行されてキャッシュがリセットされる前に最大数に達した場合は、拒否フローの最大数を超過したことを示す syslog メッセージ 106101 が発行されます。

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。拒否フローの最大数に達した場合、最後の syslog メッセージ 106101 が生成されてから *secs* 秒以上が経過すると、別の syslog メッセージ 106101 が生成されます。

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

例

次に、拒否フローの最大数メッセージの時間間隔を指定する例を示します。

```
ciscoasa(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	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL 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 ACL をクリアします。
show access-list	ACL エントリを番号で表示します。

access-list deny-flow-max

メッセージ 106100 の統計情報を計算するためにキャッシュ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 *number*

no access-list deny-flow-max *number*

構文の説明

number	syslog メッセージ 106100 の統計情報を計算するためにキャッシュする拒否フローの最大数。値は 1 ～ 4096 です。デフォルトは 4096 です。

デフォルト

デフォルトは 4096 です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン　ASA でキャッシュ拒否フローの最大数に達すると、syslog メッセージ 106101 が生成されます。

例　次に、キャッシュできる同時拒否フローの最大数を指定する例を示します。

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

関連コマンド

コマンド	説明
access-list alert-interval	メッセージ 106101 を発行する間隔を設定します。
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL 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 ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list ethertype

EtherType に基づいてトラフィックを制御する ACL 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。ACL 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**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number*}

構文の説明

any	すべてのトラフィックを許可または拒否します。
bpdu	ブリッジ プロトコル データ ユニットを許可または拒否します。 9.6(2) 以降では、このキーワードを使用しても意図した結果を得られません。代わりに、**dsap 0x42** 用のルールを書き込みます。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**bpdu** および **dsap 0x42** は **dsap bpdu** ルールに変換されます。
deny	トラフィックを拒否します。
dsap {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**}	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレス。ユーザが許可または拒否するアドレスを 16 進数（0x01 ～ 0xff）で含めます。 よく使用される値には、以下のキーワードも使用できます。 • **bpdu**：0x42（ブリッジ プロトコル データ ユニット）の場合。 • **ipx**：0xe0（Internet Packet Exchange（IPX）802.2 LLC）の場合。 • **isis**：0xfe（Intermediate System to Intermediate System（IS-IS））の場合。 • **raw-ipx**：0xff（Raw IPX 802.3 形式）の場合。
hex_number	0x600 以上の 16 ビットの 16 進数値として指定された特定の EtherType を含むトラフィックを許可または拒否します。
id	ACL の名前または番号を指定します。
eii-ipx	イーサネット II IPX 形式、EtherType 0x8137 を許可または拒否します。
ipx	IPX を許可または拒否します。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**ipx** は、**dsap ipx**、**dsap raw-ipx**、および **eii-ipx** に対して 3 つの異なるルールを設定するためのショートカットです。
isis	Intermediate System to Intermediate System（IS-IS）を許可または拒否します。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**isis** は **dsap isis** ルールに変換されます。
mpls-multicast	MPLS マルチキャストを許可または拒否します。
mpls-unicast	MPLS ユニキャストを許可または拒否します。
permit	トラフィックを許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(5)、9.1(2)	**isis** キーワードが追加されました。
9.6(2)	**dsap** *hex_address* キーワードが追加されました。**bpdu** キーワードは意図したトラフィックを照合しなくなりました。代わりに **dsap 0x42** を使用してください。
9.7(1)	ルーテッド モードのブリッジ グループ メンバー インターフェイスに Ethertype ACL を設定できるようになりました。
9.9(1)	次の点が変更されました。 • **dsap** キーワードに、よく使用されるプロトコルのための次の キーワードが追加されました：**dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}。 • **bpdu** キーワードは **dsap bpdu** キーワードに自動的に変換されます。 • **isis** キーワードは **dsap isis** キーワードに自動的に変換されます。 • **eii-ipx** キーワードが追加されました。 • **ipx** キーワードは、**dsap ipx**、**dsap raw-ipx**、および **eii-ipx** のための 3 つのルールに自動的に変換されます。

使用上のガイドライン

EtherType ACL は、EtherType を指定する 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。EtherType ルールは、16 ビットの 16 進数値で指定されるすべての EtherType および選択されたトラフィック タイプを制御します。

（注） EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE のすべてのトラフィックを明示的に拒否する場合、IP と ARP のトラフィックは拒否され、オート ネゴシエーションなどの物理プロトコル トラフィックだけが引き続き許可されます。

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるため、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- Intermediate System to Intermediate System（IS-IS）。
- IEEE 802.2 論理リンク制御パケット。宛先サービス アクセス ポイントのアドレスに基づいてアクセスを制御できます。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対するアクセス ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる場合は、着信インターフェイスと発信インターフェイスの両方にルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、Label Distribution Protocol および Tag Distribution Protocol の TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。interface は、ASA に接続されているインターフェイスです。

```
ciscoasa(config)# mpls ldp router-id interface force
```

または

```
ciscoasa(config)# tag-switching tdp router-id interface force
```

例

次に、EtherType ACL を追加する例を示します。

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit dsap 0x42
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、上記の例は次のように実行されます。

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
```

```
ciscoasa(config)# access-list ETHER ethertype permit bpdu
INFO: ethertype bpdu is saved to config as ethertype dsap bpdu

ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast

ciscoasa(config)# show access-list ETHER
access-list ETHER; 5 elements
access-list ETHER ethertype permit eii-ipx (hitcount=0)
access-list ETHER ethertype permit dsap ipx(hitcount=0)
access-list ETHER ethertype permit dsap raw-ipx(hitcount=0)
access-list ETHER ethertype permit dsap bpdu(hitcount=0)
access-list ETHER ethertype permit mpls-unicast (hitcount=0)

ciscoasa(config)# access-group ETHER in interface inside
```

関連コマンド

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

access-list extended

拡張 ACL にアクセス コントロール エントリ（ACE）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。ACE を削除するには、このコマンドの **no** 形式を使用します。

すべてのタイプのトラフィック、ポートなし:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

ポートベースのトラフィックの場合:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

ICMP トラフィック、ICMP タイプ:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**}[*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

構文の説明

access_list_name	ACL ID を最大 241 文字の文字列または整数として指定します。ID は、大文字と小文字が区別されます。 **ヒント** コンフィギュレーションで ACL ID を見やすくするには、すべて大文字を使用します。
deny	条件に合致している場合、パケットを拒否します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによって、パケットが ASA を通過しないようにします。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってトラフィックがインスペクションから免除されます。一部の機能では deny ACE の使用は許可されません。詳細については、ACL を使用する各機能のコマンド マニュアルを参照してください。

dest_address_argument	パケットの送信先の IP アドレスまたは FQDN を指定します。使用可能な引数は次のとおりです。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA では、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any**、**any4**、および **any6**：**any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。 • **interface** *interface_name* - ASA インターフェイスの名前を指定します。IP アドレスではなくインターフェイス名を使用して、トラフィックの送信元または宛先のインターフェイスに基づいてトラフィックを照合します。トラフィックの送信元がデバイス インターフェイスである場合、ACL に実際の IP アドレスを指定する代わりに interface キーワードを指定する必要があります。たとえば、このオプションを使用し、ISAKMP をブロックすることによって、特定のリモート IP アドレスが ASA への VPN セッションを開始できないようにすることができます。ASA を送信元または宛先とするすべてのトラフィック自体では、**access-group** コマンドを **control-plane** キーワードを指定して使用することが必要となります。 • **object** *nw_obj_id*：**object network** コマンドを使用して作成されたネットワーク オブジェクトを指定します。 • **object-group** *nw_grp_id*：**object-group network** コマンドを使用して作成されたネットワーク オブジェクト グループを指定します。
icmp_argument	（オプション）ICMP のタイプとコードを指定します。 • *icmp_type* [*icmp_code*]：ICMP タイプを名前または番号で指定し、そのタイプの ICMP コード（省略可能）を指定します。コードを指定しない場合は、すべてのコードが使用されます。 • **object-group** *icmp_grp_id*：**object-group service** コマンドまたは（非推奨）**object-group icmp** コマンドを使用して作成された ICMP/ICMP6 用のネットワーク オブジェクト グループを指定します。
inactive	（任意）ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。

line *line-num*	(任意)ACE を挿入する行番号を指定します。行番号を指定しなかった場合は、ACL の末尾に ACE が追加されます。行番号はコンフィギュレーションに保存されません。ACE の挿入場所を指定するだけです。
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(オプション)ネットワーク アクセスに関して ACE に一致するパケットが見つかったとき(**access-group** コマンドで ACL が適用されます)のロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル(6)とデフォルト間隔(300 秒)でシステム ログ メッセージ 106100 が有効になります。**log** キーワードを入力しないと、拒否されたパケットに対して、デフォルトのシステム ログ メッセージ 106023 が生成されます。ログ オプションは次のとおりです。 • *level*:0 ～ 7 の重大度。デフォルトは 6(情報)です。アクティブな ACE に対してこのレベルを変更する場合、新しいレベルは新規接続に適用され、既存の接続は引き続き前のレベルでロギングされます。 • **interval** *secs*:syslog メッセージ間の時間間隔(秒)。1 ～ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。 • **disable**:すべての ACE ロギングをディセーブルにします。 • **default**:メッセージ 106023 のロギングをイネーブルにします。この設定は、**log** オプションを含めないことと同じです。
permit	条件に合致している場合、パケットを許可します。ネットワーク アクセスの場合(**access-group** コマンド)、このキーワードによって、パケットが ASA を通過するようにします。クラス マップにアプリケーション インスペクションを適用する場合(**class-map** コマンドおよび **inspect** コマンド)、このキーワードによってインスペクションがパケットに適用されます。

port_argument	（任意：**tcp**、**udp**、**sctp** のみ）送信元ポートまたは宛先ポートを指定します。ポートを指定しなかった場合は、すべてのポートが照合されます。また、この引数を使用するのではなく、*protocol_argument* に指定するサービス オブジェクトのポートも指定できます。 使用可能な引数は次のとおりです。 • *operator port*：ポートの名前または番号（0 ～ 65535）。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。 – **lt**：より小さい – **gt**：より大きい – **eq**：等しい – **neq**：等しくない – **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200` DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。 • **object-group** *service_grp_id*：**object-group service** {**tcp** | **udp** | **tcp-udp**} コマンドを使用して作成されたサービス オブジェクト グループを指定します。これらのオブジェクト タイプは推奨されなくなりました。 ポート引数としてプロトコルおよびポートがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。これらのオブジェクトはプロトコル引数の一部として指定します。
protocol_argument	IP プロトコルを指定します。使用可能な引数は次のとおりです。 • *name* または *number*：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。**ip** を指定すると、すべてのプロトコルに適用されます。使用可能なオプションについては、CLI ヘルプを参照してください。 • **object-group** *protocol_grp_id*：**object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。 • **object** *service_obj_id*：**object service** コマンドを使用して作成されたサービス オブジェクトを指定します。TCP、UDP、SCTP、または ICMP サービス オブジェクトには、トラフィックを ACE と照合する際に使用するプロトコル、送信元ポートと宛先ポートの両方またはいずれか、あるいは ICMP のタイプとコードを含めることができます。ACE でポートとタイプを個別に設定する必要はありません。 • **object-group** *service_grp_id*：**object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。
sctp	SCTP にプロトコルを設定します。

security_group_argument	TrustSec 機能とともに使用し、送信元や宛先のアドレスに加えて、トラフィックを検出する条件となるセキュリティ グループを指定します。使用可能な引数は次のとおりです。 • **object-group-security** *security_obj_grp_id*:**object-group security** コマンドを使用して作成されたセキュリティ オブジェクト グループを指定します。 • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}:セキュリティ グループの名前またはタグを指定します。
source_address_argument	パケットの送信元の IP アドレスまたは FQDN を指定します。使用可能な引数は、*dest_address_argument* の説明にある引数と同じです。
tcp	TCP にプロトコルを設定します。
time-range *time_range_name*	(オプション)ACE をアクティブにする曜日と時刻を決定する時間範囲オブジェクトを指定します。時間範囲を含めない場合、ACE は常にアクティブです。時間範囲の定義については、**time-range** コマンドを参照してください。
udp	UDP にプロトコルを設定します。
user_argument	アイデンティティ ファイアウォール機能とともに使用し、送信元アドレスに加えて、トラフィックを検出する条件となるグループまたはユーザを指定します。使用可能な引数は次のとおりです。 • **object-group-user** *user_obj_grp_id*:**object-group user** コマンドを使用して作成されたユーザ オブジェクト グループを指定します。 • **user** {[*domain_nickname*\]*name* | **any** | **none**}:ユーザ名を指定します。ユーザ クレデンシャルを含むすべてのユーザを照合するには **any** を指定し、ユーザ名にマッピングされていないアドレスを照合するには **none** を指定してください。これらのオプションが特に役立つのは、**access-group** と **aaa authentication match** のポリシーを結合する場合です。 • **user-group** [*domain_nickname*\\]*user_group_name*:ユーザ グループ名を指定します。ドメインとグループ名を区切る 2 つの \\ に注意してください。

デフォルト

- deny ACE のデフォルトのロギングは、拒否されたパケットについてのみシステム ログ メッセージ 106023 を生成します。
- **log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6(情報)で、デフォルトの間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	NAT または PAT を使用するときは、さまざまな機能で、ACL でのマッピング アドレスおよびポートの使用が不要になります。これらの機能については、必ず変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。詳細については、「実際の IP アドレスを使用する機能」セクション（1-71ページ）を参照してください。
8.4(2)	送信元または宛先 IP アドレスに加えて、送信元と宛先に、アイデンティティ ファイアウォールのユーザおよびグループを使用できるようになりました。送信元と宛先に、**user**、**user-group**、および **object-group-user** のサポートが追加されました。
9.0(1)	送信元または宛先 IP アドレスに加えて、送信元と宛先に、TrustSec セキュリティ グループを使用できるようになりました。送信元または宛先に、**security-group** および **object-group-security** のサポートが追加されました。
9.0(1)	IPv6 のサポートが追加されました。any キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す any4 キーワードと、IPv6 のみのトラフィックを表す any6 キーワードが追加されました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせを指定できます。IPv4 と IPv6 間の変換に NAT を使用する場合、実際のパケットには、IPv4 アドレスと IPv6 アドレスの組み合わせは含まれません。ただし、多くの機能において、ACL では常に実際の IP アドレスが使用され、NAT マッピング アドレスは考慮されません。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。ACL の移行については、9.0 のリリース ノートを参照してください。
9.0(1)	ICMP コードのサポートが追加されました。プロトコルとして **icmp** を指定すると、*icmp_type* [*icmp_code*] を入力できます。
9.5(2)	**sctp** キーワードが追加されました。

使用上のガイドライン

1 つの ACL は、同じ ACL ID を持つ 1 つまたは複数の ACE で構成されます。ACL は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。特定の ACL 名に対して入力した各 ACE は、ACE で行番号を指定しない限り、その ACL の最後に追加されます。ACL 全体を削除するには、**clear configure access-list** コマンドを使用します。

ACE の順序

ACE の順序は重要です。ASA がパケットを転送するかドロップするかを決定する際、ASA は、エントリがリストされている順番で各 ACE を使用してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE を ACL の先頭に作成した場合は、残りのステートメントはチェックされません。

実際の IP アドレスを使用する機能

次のコマンドと機能では、実際の IP アドレスが ACL の中で使用されます。

- **access-group** コマンド
- モジュラ ポリシー フレームワークの **match access-list** コマンド
- ボットネット トラフィック フィルタの **dynamic-filter enable classify-list** コマンド
- AAA の **aaa ... match** コマンド
- WCCP の **wccp redirect-list group-list** コマンド

マッピング IP アドレスを使用する機能

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識されるマッピングされた値を使用します。

- IPsec ACL
- capture コマンドの ACL
- ユーザ単位 ACL
- ルーティング プロトコルの ACL
- 他のすべての機能の ACL

アイデンティティ ファイアウォール、FQDN、および TrustSec の ACL をサポートしない機能

次の機能は ACL を使用しますが、アイデンティティ ファイアウォール（ユーザ名またはグループ名を指定）、FQDN（完全修飾ドメイン名）、または TrustSec 値を含む ACL は使用できません。

- **route-map** コマンド
- VPN の **crypto map** コマンド
- VPN の **group-policy** コマンド、ただし、**vpn-filter** を除く
- WCCP
- DAP

例

次に示す ACL は ASA を通るすべてのホスト（ACL を適用するインターフェイス上の）を許可します。

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

次の ACL の例では、192.168.1.0/24 のホストが 209.165.201.0/27 のネットワークにアクセスすることを拒否します。その他のアドレスはすべて許可されます。

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

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

```
ciscoasa(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 ACL では、すべてのホスト（この ACL を適用するインターフェイス上の）からアドレス 209.165.201.29 の Web サイトへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(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 ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

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

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

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

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

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

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

次の ACL は、すべての ICMP トラフィックを許可します。

```
ciscoasa(config)# access-list abc extended permit icmp any any
```

次の ACL は、オブジェクト グループ「obj_icmp_1」のすべての ICMP トラフィックを許可します。

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

次の ACL は、ICMP タイプが 3、および ICMP コードが 4 の送信元ホスト 10.0.0.0 から宛先ホスト 10.1.1.1 への ICMP トラフィックを許可します。その他のタイプの ICMP トラフィックはすべて許可されません。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

次の ACL は、ICMP タイプが 3、および ICMP コードが任意の送信元ホスト 10.0.0.0 から宛先ホスト 10.1.1.1 への ICMP トラフィックを許可します。その他のタイプの ICMP トラフィックはすべて許可されません。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

関連コマンド

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

access-list remark

拡張、EtherType、または標準アクセス コントロール エントリの前後にコメントのテキストを指定するには、グローバル コンフィギュレーション モードで **access-list remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

id	ACL の名前
line *line-num*	(任意) コメントを挿入するライン番号
remark text	コメントのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

例

次に、ACL の末尾にコメント テキストを指定する例を示します。

```
ciscoasa(config)# access-list MY_ACL remark checklist
```

関連コマンド

コマンド	説明
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL 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 ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list rename

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

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

構文の説明

id	既存の ACL の名前。
rename *new_acl_id*	新しい ACL ID を最大 241 文字の文字列または整数として指定します。ID は、大文字と小文字が区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン　ACL が同じ名前に変更されると、ASA は、通知なしでこのコマンドを無視します。

例　次に、ACL の名前を TEST から OUTSIDE に変更する例を示します。

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

関連コマンド

コマンド	説明
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL 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 ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list standard

標準 ACL にアクセス コントロール エントリ（ACE）を追加するには、グローバル コンフィギュレーション モードで **access-list standard** コマンドを使用します。ACE 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** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

構文の説明

any4	任意の IPv4 アドレスに一致させます。
deny	条件に一致する場合、パケットを拒否または免除します
host *ip_address*	IPv4 ホスト アドレスを指定します(つまり、サブネット マスクは 255.255.255.255 です)。
id	ACL の名前または番号。
ip_address subnet_mask	IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
permit	条件に一致する場合、パケットを許可するか、または含みます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

標準 ACL は、ACL ID または名前が同じすべての ACE で構成されます。標準 ACL は、ルート マップや VPN フィルタなどの限られた数の機能に使用されます。標準 ACL は、IPv4 アドレスだけを使用して、宛先アドレスだけを定義します。

例

次に、標準 ACL にルールを追加する例を示します。

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list webtype

クライアントレス SSL VPN 接続をフィルタする Web タイプ ACL にアクセス コントロール エントリ（ACE）を追加するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。

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

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

access-list *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

構文の説明

deny	条件に一致する場合、アクセスを拒否します。
dest_address_argument	パケットの送信先 IP アドレスを指定します。宛先アドレス オプションは次のとおりです。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *dest_ip_address mask*：10.100.10.0 255.255.255.0 など、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address/prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any**、**any4**、および **any6**：**any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。
id	ACL の名前または番号を指定します。
inactive	（任意）ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。

log [[*level*] [**interval** *secs*] | **disable** | **default**]	(オプション)ACE に一致するパケットが見つかったときのロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル(6)とデフォルト間隔(300 秒)で VPN フィルタのシステム ログ メッセージ 106102 がイネーブルになります。**log** キーワードを入力しないと、デフォルトの VPN フィルタのシステム ログ メッセージ 106103 が生成されます。ログ オプションは次のとおりです。 • *level*:0 ～ 7 の重大度。デフォルトは 6(情報)です。 • **interval** *secs*:syslog メッセージ間の時間間隔(秒)。1 ～ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。 • **disable**:すべての ACE ロギングをディセーブルにします。 • **default**:メッセージ 106103 のロギングをイネーブルにします。この設定は、**log** オプションを含めないことと同じです。
operator port	(オプション)**tcp** を指定する場合は、宛先ポート。ポートを指定しなかった場合は、すべてのポートが照合されます。*operator* は次のいずれかになります。 • **lt**:より小さい • **gt**:より大きい • **eq**:等しい • **neq**:等しくない • **range**:値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200` *port* には、TCP ポートの番号(整数)または名前を指定できます。
permit	条件が一致した場合にアクセスを許可します。
time_range *name*	(オプション)ACE をアクティブにする曜日と時刻を決定する時間範囲オブジェクトを指定します。時間範囲を含めない場合、ACE は常にアクティブです。時間範囲の定義については、**time-range** コマンドを参照してください。
url {*url_string* | **any**}	照合する URL を指定します。すべての URL ベースのトラフィックを照合するには、**url any** を使用します。それ以外の場合、ワイルドカードを含めることができる URL 文字列を入力します。URL 文字列については、使用上のガイドラインを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- ACL ロギングによって、拒否されたパケットに対して syslog メッセージ 106103 が生成されます。
- オプションの **log** キーワードを指定した場合、syslog メッセージ 106102 のデフォルト レベルは 6(情報)です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

access-list webtype コマンドは、クライアントレス SSL VPN フィルタリングを設定するために使用されます。

URL の指定に関するヒントと制約事項は次のとおりです。

すべての URL を照合する場合は、**any** を選択します。

- 「permit url any」を指定すると、protocol://server-ip/path の形式を含むすべての URL が許可され、このパターンに一致しないポート転送などのトラフィックがブロックされます。暗黙的な拒否が発生しないよう、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE を使用してください。
- スマート トンネルと ica プラグインは、smart-tunnel:// と ica:// のタイプにのみ一致するため、「permit url any」を使用した ACL によって影響を受けることはありません。
- 使用できるプロトコルは、cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel://、および smtp:// です。プロトコルでワイルドカードを使用することもできます。たとえば、htt* は http および https に一致し、アスタリスク * はすべてのプロトコルに一致します。たとえば、*://*.example.com は、example.com ネットワークへのすべてのタイプの URL ベース トラフィックに一致します。
- smart-tunnel:// URL を指定すると、サーバ名だけを含めることができます。URL にパスを含めることはできません。たとえば、smart-tunnel://www.example.com は受け入れ可能ですが、smart-tunnel://www.example.com/index.html は受け入れ不可です。
- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。すべての http URL に一致させるには、http://*/* と入力します。
- 疑問符 ? は任意の 1 文字に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ と http://www.cisco.com:81/ の両方に一致させるには、**http://www.cisco.com:8[01]/** と入力します。

例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

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

次の例は、特定の Web ページへのアクセスを拒否する方法を示しています。

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

次の例は、特定サーバ上にある任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

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

関連コマンド

コマンド	説明
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	ASA で稼働中のアクセス リストのコンフィギュレーションを表示します。

accounting-mode

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

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

構文の説明

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

デフォルト

デフォルト値はシングル モードです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

単一のサーバにアカウンティング メッセージを送信するには、**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 グループが使用されている場合にのみ有効です。

例

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

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

関連コマンド

コマンド	説明
aaa accounting	アカウンティング サービスをイネーブルまたはディセーブルにします。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始し、グループ内のすべてのホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-port

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

accounting-port *port*

no accounting-port

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	Transparent	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、アカウンティング レコードの送信先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。RADIUS アカウンティング サーバで 1646 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートに対して ASA を設定する必要があります。

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

例

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

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

関連コマンド

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

accounting-server-group

アカウンティング レコード送信用の AAA サーバ グループを指定するには、さまざまなモードで **accounting-server-group** コマンドを使用します。アカウンティング サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

構文の説明

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

デフォルト

デフォルトでは、アカウンティング サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	Transparent	シングル	コンテキスト	システム
imap4s コンフィギュレーション（廃止）	• Yes	—	• Yes	—	—
pop3s コンフィギュレーション（廃止）	• Yes	—	• Yes	—	—
smtps コンフィギュレーション（廃止）	• Yes	—	• Yes	—	—
トンネル グループ一般属性コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードではなく、トンネル グループ一般属性コンフィギュレーション モードで使用できます。
9.5(2)	このコマンドは、imap4s モード、pop3s モード、および smtps モードについては廃止されました。
9.8(1)	このコマンドは、IPSec LAN-to-LAN（IPSec-12L）トンネル グループでは使用できなくなりました。実際、IPSec LAN-to-LAN ではサポートされていませんでした。

使用上のガイドライン

ASA では、アカウンティングを使用して、ユーザがアクセスするネットワーク リソースを追跡します。このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性コンフィギュレーション モードの同等のコマンドに変換されます。

例

次に、トンネル グループ一般属性コンフィギュレーション モードで、リモート アクセス トンネル グループ「xyz」に対して「aaa-server123」という名前のアカウンティング サーバ グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group xyz type remote-access
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

関連コマンド

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