aa - ac

aaa accoungting 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ー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+ サーバーまたはサーバーのグループを指定します。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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ーに送信されます。

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ー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 ユーザー 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ーで）。
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

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

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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ー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ー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 ユーザー 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ーで）。
aaa accounting command	管理者/ユーザー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 サーバー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	ユーザー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** コマンドによって定義される AAA サーバー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

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 サーバーまたは TACACS+ サーバーに送信できます。そのトラフィックも認証されている場合、AAA サーバーはユーザー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 サーバーは 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、ユーザー名、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 サーバー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

同じ設定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 Adaptive Security Device Manager（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 command	管理者アクセスのアカウンティングをイネーブルにします。
aaa-server host	AAA サーバーを設定します。
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	ユーザー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 サーバーグループを指定します。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 サーバーまたは TACACS+ サーバーに送信できます。そのトラフィックも認証されている場合、AAA サーバーはユーザー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 サーバーは 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、ユーザー名、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 サーバーを最初に指定する必要があります。

AAA サーバー 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ーグループ内のアクティブなサーバーにのみ送信されます。

aaa accounting match コマンドは、**aaa accounting include** および **exclude** コマンドと同じ設定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CLIにアクセスするユーザーを認証するか、**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ーを認証するには、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。認証を無効にするには、このコマンドの **no** 形式を使用します。

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

構文の説明

enable	**enable** コマンドを使用して特権EXECモードにアクセスするユーザーを認証します。
http	HTTPSでASAにアクセスするASDMユーザーを認証します。デフォルトでは、ASAは空白のユーザー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、空白のユーザー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サーバーがダウンしているか使用できないことを意味する）は、空白のユーザー名とイネーブルパスワードを使用して、AAA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 サーバーグループを指定します。HTTPS 管理認証では AAA サーバー 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 サーバー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 サーバーと同じユーザー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、ど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ーを認証します。
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ーを認証します。ローカル **username** 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** コマンドが必要です。 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ーのみに適用されます。また、LOCAL だけでなく、任意のサーバータイプを指定できます。たとえば、一部のユーザーはローカルデータベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。
telnet	Telnet を使用して ASA にアクセスするユーザーを認証します。**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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。

リリース	変更内容
8.4(2)	**pix** または **asa** ユーザー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、**username** コマンド（CLI）を入力するか **Configuration > Device Management > Users/AAA > User Accounts**（ASDM）を選択してローカルユーザーを定義する必要があります。ローカル データベースの代わりに AAA サーバー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** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに **username** 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ーの認証とパスワードを使用するユーザー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。ユーザーに **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ー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、明示的に AAA SSH 認証を設定すると、パスワードを持つユーザー名のみにこの認証が適用されます。また、AAA サーバー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 ユーザーを認証する前に、**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ー 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、ユーザー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、ユーザー名を入力しません。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 サーバーまたはローカル ユーザー データベースで定義されているユーザー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、特定のユーザーとしてログインしていません。ユーザー名を維持するには、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 によってユーザー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、ユーザー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、ブランクのユーザー名と **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（ユーザー名をブランクのままにしないで）ユーザー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 サーバー グループ用の SDI プロトコルがサポートされません。HTTPS 認証で要求できるユーザー名の最大長は、30 文字です。パスワードの最大長は 16 文字です。

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
enable	3回失敗するとアクセスが拒否される。
serial	成功するまで何回も試行できる。
ssh	3回失敗するとアクセスが拒否される。
telnet	成功するまで何回も試行できる。
http	成功するまで何回も試行できる。

例

次に、「radius」というサーバー タグの RADIUS サーバーへの 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、サーバー 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ーが利用できない場合に LOCAL ユーザー 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	ユーザー認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザー認証に使用する AAA サーバーを指定します。
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 ユーザーの 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 include** コマンドを使用します。認証を無効にするには、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	ユーザー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 ユーザー 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 サーバー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、ユーザー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。ユーザー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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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** コマンドと同じ設定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。

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 サーバーが TCP セッションを代行処理してユーザーを認証し、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 アドレスのユーザーは、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ーは、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ー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、ユーザーが 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、ユーザー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。ユーザー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。ユーザーがユーザー名とパスワードを入力できる内部 Web ページにユーザー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。ユーザーがユーザー名とパスワードを入力できる内部 Web ページにユーザー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ー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 と同じユーザー 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。宛先サーバーにも独自の認証がある場合、ユーザーは別のユーザー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、宛先サーバー用に別のユーザー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、ユーザー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 ユーザー名、アットマーク（@）、FTP ユーザー名（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る。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、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、ユーザーはポート 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、ユーザーの 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、ユーザー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ー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課す場合、 **aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して 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、ユーザーは 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ー 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ー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ー認証方式を提供します。
aaa-server	グループ関連のサーバー属性を設定します。
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ー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、直接認証ユーザー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ーは、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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 ユーザーが 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ー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 と同じユーザー 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、各ユーザーを ASA で直接認証できます。

（注） カットスループロキシの場合、ユーザーが認証ページからログアウトしても、接続はアクティブなままになります。接続を完全にクリアするには、ユーザーが SSH セッションからログアウトする必要があります。

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 listener no-logout-button	カットスルー プロキシのログイン ページからログアウト ボタンを削除します。
aaa authentication match	通過トラフィックのユーザー認証を設定します。
aaa authentication secure-http-client	SSL をイネーブルにし、HTTP クライアントと ASA の間のユーザー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 listener no-logout-button

カットスループロキシのポータルページからログアウトボタンを削除するには、グローバル コンフィギュレーション モードで **aaa authentication listener no-logout-button** コマンドを使用します。ログアウトボタンを復元する場合は、このコマンドの **no** 形式を入力します。

aaa authentication listener no-logout-button *interface_name*
no aaa authentication listener no-logout-button *interface_name*

構文の説明

interface_name 認証リスナーを有効にするインターフェイスを指定します。

コマンド デフォルト

デフォルトでは、ポータル ページにログアウト ボタンがあります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(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

デフォルトでは、カットスルー プロキシのポータル ページ（/netaccess/connstatus.html）には、接続ホストに対してカットスルー プロキシ セッションがすでにアクティブになっているときにアクセスされた場合、セッション情報とログアウト ボタンが表示されます。このコマンドを使用してログアウト ボタンを削除できます。

これは、ユーザーが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザーがログアウトすると、その IP アドレスのすべてのユーザーがログアウトされます。

例

次の例では、内部インターフェイスで HTTP および HTTPS リスナーを有効にし、認証が必要なすべての HTTP/HTTPS トラフィックをリダイレクトするように ASA を設定しています。

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

```
ciscoasa(config)# aaa authentication listener no-logout-button inside
```

関連コマンド

コマンド	説明
aaa authentication listener http/https	HTTP/HTTPS リスニング ポートでネットワーク ユーザーを認証できるようにします。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 サーバーのユーザー名またはローカル データベースのユーザー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
```

ユーザーがログインすると、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
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。
password-history	直前の **username** パスワードを保存します。ユーザー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 ユーザーを設定します。

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。認証を無効にするには、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	ユーザー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 ユーザー 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 サーバーグループを指定します。
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ー アイデンティティを指定します。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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** および **exclude** コマンドと同じ設定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 サーバーが TCP セッションを代行処理してユーザーを認証し、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 アドレスのユーザーは、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ーは、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ー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、ユーザーが 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、ユーザー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。ユーザー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。ユーザーがユーザー名とパスワードを入力できる内部 Web ページにユーザー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。ユーザーがユーザー名とパスワードを入力できる内部 Web ページにユーザー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ー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 と同じユーザー 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。宛先サーバーにも独自の認証がある場合、ユーザーは別のユーザー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、宛先サーバー用に別のユーザー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、ユーザー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ユーザー名、アットマーク（@）、FTPユーザー名（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る。

スタティック PAT および HTTP

HTTP認証では、スタティックPATが設定されている場合、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、ユーザーはポート 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、ユーザーの 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、ユーザー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ー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課す場合、 **aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して 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、ユーザーは 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** コマンドの使用例を示します。

```
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 acc**ess-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** 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	ユーザー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 の間のユーザー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。この機能を無効にするには、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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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、ユーザーの 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ー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、ユーザーが認証ページに正しいユーザー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ー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 サーバーポート 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ー上での、LOCAL、TACACS+、または RADIUS のユーザー認証をイネーブルにします。
virtual telnet	ASA 仮想サーバーにアクセスします。

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** [*server-tag + tacacs* | **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 ユーザー、RADIUS ユーザー、または LDAP ユーザー（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 はそのユーザーをローカルデータベース、RADIUS、または LDAP サーバーで定義されている特権レベルに所属させます。ユーザーは、ユーザー特権レベル以下のコマンドにアクセスできます。 TACACS+ サーバーグループタグの後に **LOCAL** を指定した場合、TACACS+ サーバー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 ユーザーデータベースがコマンド認可に使用されます。
tacacs+ server_tag	TACACS+ 認可サーバーの定義済みのサーバー グループ タグを指定します。**aaa-server** コマンドで定義した AAA サーバーグループタグです。

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	TACACS+ サーバー 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 サーバーまたは LDAP サーバー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ー 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、各ユーザー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認可方式

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 ユーザー、RADIUS ユーザー、または LDAP ユーザー（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 はそのユーザーをローカルデータベース、RADIUS、または LDAP サーバーで定義されている特権レベルに所属させます。ユーザーは、ユーザー特権レベル以下のコマンドにアクセスできます。すべてのユーザーは、初めてログインするときに、ユーザー 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。ユーザーは、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ーがなくても、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+ サーバー特権レベル：TACACS+ サーバーで、ユーザーまたはグループが 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 でユーザーが入力するすべてのコマンドは、TACACS+ サーバー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ー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ー名に関係なく、管理者 ID として常にデフォルトの enable_15 ユーザー名が使用されます。これにより、enable_15 ユーザーに対してコマンド許可が設定されていない場合や、enable_15 ユーザーの認可が前のコンテキスト セッションでのユーザー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ユーザー名を他のコンテキストで使用できるため、enable_15 ユーザー名でログインしたユーザーをコマンド 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 サーバーを使用する場合は、enable_15 ユーザー名を使用していたユーザーを追跡するために数台のサーバー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 ユーザー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 ユーザー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ー名を使用できます。

（注） システム実行スペースでは **aaa** コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

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、ユーザーが **enable** コマンドにアクセスした後にユーザー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 からの管理ユーザー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+ の各ユーザーの管理認可もイネーブルにします。
- 次に示すユーザー タイプごとの前提条件を確認してください。
- コマンド特権レベルの設定については、**privilege** コマンドを参照してください。

TACACS+ コマンド認可

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

TACACS+ サーバー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 を再始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+ サーバー システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバー プールに、インターフェイス 1 に接続された 1 つのサーバーとインターフェイス 2 に接続された別のサーバーを含めます。TACACS+ サーバー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 ユーザー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+ サーバーの設定については、CLI コンフィギュレーション 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+ サーバー 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 サーバー グループ内のすべてのサーバーが使用できない場合に、ローカル ユーザー 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。

コマンド	説明
aaa authorization exec	RADIUS からの管理ユーザー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ー属性を設定します。
enable	特権 EXEC モードを開始します。
ldap map-attributes	LDAP 属性を、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ーの 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	ユーザーの認証に使用されたサーバー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 のローカルユーザーデータベースから取得されることを示します。

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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、ユーザーの 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、ユーザーの 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+ ユーザーについて AAA サーバー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。

ユーザーが CLI、ASDM、または **enable** コマンドにアクセスするときにユーザーを認証するように **aaa authentication console** コマンド tを設定すると、ユーザー 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、認証したユーザーはすべてコンソールポートにアクセスできます。コマンド認可を設定した場合、コンソールユーザーにはコマンドの使用について引き続き制限が適用されます。

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

- LDAP マッピング済みユーザー：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 ユーザー：次の値のいずれかにマッピングする IETF RADIUS 数値型 **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。ユーザーは **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）ユーザーは、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** コマンドを設定している場合は CLI へのアクセスを許可しますが、 **aaa authentication http console** コマンドを設定している場合は ASDM への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** コマンドを使用して **enable** 認証を有効にしている場合、ユーザーは、**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+ ユーザー：「service=shell」エントリで認可を要求し、サーバーは次のように 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 以降は、**aaa authentication** {**telnet | ssh**} **console** コマンドを設定している場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定している場合は ASDM への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** コマンドを使用して認証を有効にしている場合、ユーザーは、**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。ユーザーは **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）。
- ローカルユーザー：**service-type** コマンドを設定します。これは、**username** コマンドのユーザー名コンフィギュレーション モードです。デフォルトでは、**service-type** は **admin** で、**aaa authentication console** コマンドで指定されたすべてのサービスに対してフルアクセスが許可されます。

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 ユーザーの制限 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 のユーザー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 サーバー 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ー 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ー タグです。

コマンド デフォルト

ASDM のユーザー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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

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 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	ユーザー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 サーバー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ーで生じる可能性があります。ASA では、サーバー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ーに送信します。すべてのサーバーがこのような変換を実行するとは限りません。また、ユーザー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。

コマンド 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ー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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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、ユーザー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** コマンドと同じ設定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。

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。ユーザー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ー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。

ユーザー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 はユーザー名を TACACS+ サーバーに送信します。TACACS+ サーバーは ASA に応答し、ユーザー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。

ユーザー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+ サーバー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ーで生じる可能性があります。ASA では、サーバー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ーに送信します。すべてのサーバーがこのような変換を実行するとは限りません。また、ユーザー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ーグループを作成し、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の認証サーバーが内部インターフェイス上にあること、およびtplus1サーバー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ーをtplus1サーバー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ー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サーバー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、ユーザーが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、指定したサーバーグループ内のすべてのサーバーがディセーブルである場合に、ローカルユーザー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+ユーザー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** コマンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization match *acl_name interface_name server_tag*
no aaa authorization match *acl_name interface_name server_tag*

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。**permit** 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、**deny** 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	ユーザー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** コマンドによって定義される AAA サーバーグループを指定します。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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** および **exclude** コマンドと同じ設定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。ユーザーが認可を

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ー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。

ユーザー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はユーザー名をTACACS+サーバーに送信します。TACACS+サーバーはASAに応答し、ユーザー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。

ユーザー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+サーバー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ーで生じる可能性があります。ASA では、サーバー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ーに送信します。すべてのサーバーがこのような変換を実行するとは限りません。また、ユーザー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 サーバー 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 サーバー 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 の認証サーバーが内部インターフェイス上にあること、および tplus1 サーバー 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 サーバー 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 サーバー グループ内の AAA サーバー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	ユーザー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	ある特定のユーザーまたはすべてのユーザーの 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ーに提供されているユーザー名、ユーザー名がバインドされている IP アドレス、およびユーザー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 kerberos import-keytab

Kerberos キータブファイルをインポートして、Kerberos サーバーの認証に使用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 kerberos import-keytab** コマンドを使用します。インポートされたキータブファイルを削除するには、**clear aaa kerberos keytab** コマンドを使用します。

aaa kerberos import-keytab *file*

構文の説明

url インポートするファイルのロケーションまたはURL。ファイルをインポートするためにサポートされているロケーションは次のとおりです。ロケーションに応じた完全なパスとファイル名を指定します。

- disk0:
- disk1:
- flash:
- ftp://
- http://
- https://
- scp://
- smb://
- tftp://

コマンド デフォルト

デフォルト値はありません。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(4)	このコマンドが追加されました。

使用上のガイドライン

validate-kdc コマンドを使用して、グループ内のサーバーを認証するように Kerberos AAA サーバーグループを設定できます。認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット（TGT）を取得してユーザーを検証した後、システムは **host**/*ASA_hostname* のユーザーに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバーは信頼できないと見なされ、ユーザーは認証されません。

KDC 認証を完了するには、次の手順を実行する必要があります。

1. （KDC 上。）ASA の Microsoft Active Directory にユーザーアカウントを作成します（**Start > Programs > Administrative Tools > Active Directory Users and Computers** に移動します）。たとえば、ASA の完全修飾ドメイン名（FQDN）が asahost.example.com の場合は、asahost という名前のユーザーを作成します。
2. （KDC 上。）FQDN とユーザーアカウントを使用して、ASA のホストサービスプリンシパル名（SPN）を作成します。

   ```
   C:> setspn -A HOST/asahost.example.com asahost
   ```

3. （KDC 上。）ASA の キータブファイルを作成します（わかりやすくするために改行を追加）。

   ```
   C:\Users\Administrator> ktpass /out new.keytab +rndPass
   /princ host/asahost@EXAMPLE.COM
   /mapuser asahost@example.com
   /ptype KRB5_NT_SRV_HST
   /mapop set
   ```

4. （ASA 上。）**aaa kerberos import-keytab** コマンドを使用して、キータブ（この例では new.keytab）を ASA にインポートします。
5. （ASA 上。）Kerberos AAA サーバーグループ設定に **validate-kdc** コマンドを追加します。キータブファイルは、このコマンドが含まれているサーバーグループでのみ使用されます。

（注） Kerberos 制約付き委任（KCD）とともに KDC 検証を使用することはできません。サーバーグループが KCD に使用されている場合、**validate-kdc** コマンドは無視されます。

例

次に、FTP サーバー上に存在する new.keytab というキータブをインポートし、Kerberos AAA サーバーグループで KDC 検証を有効にする例を示します。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
```

```
ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

関連コマンド

コマンド	説明
clear aaa kerberos keytab	インポートされた Kerberos キータブファイルをクリアします。
show aaa kerberos keytab	Kerberos キータブファイルに関する情報を表示します。
validate-kdc	Kerberos キー発行局（KDC）検証を実行するように Kerberos AAA サーバーグループを設定します。

aaa local authentication attempts max-fail

ASA で特定のユーザー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、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	ユーザーがロック 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。

コマンド デフォルト

このコマンドは、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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。
9.17(1)	ユーザーは 10 分後にロック解除され、特権レベル 15 のユーザーも影響を受けるようになりました。

使用上のガイドライン

このコマンドは、ローカル ユーザー 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、ユーザー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回数が設定回数に達すると、ユーザーはロック アウトされ、管理者がユーザー名のロックを解除するまで、または 10 分経過するまで、そのユーザーは正常にログインできません。ユーザー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。

ユーザー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	指定したユーザーのロックアウト 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	ユーザーのロックアウト ステータスを変更することなく、ユーザー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ー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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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	ユーザー認証をイネーブルにします。
aaa authorization	ユーザー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	ユーザー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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 サーバーである場合は、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 サーバー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 人のユーザー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、単一ユーザー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ー上で、LOCAL、TACACS+、または RADIUS ユーザー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 ユーザー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+ ユーザー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 サーバーを指定します。
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 sdi import-node-secret

RSA Authentication Manager からエクスポートしたノードシークレットファイルを SDI AAA サーバーグループで使用するためにインポートするには、グローバル コンフィギュレーション モードで **aaa sdi import-node-secret** コマンドを使用します。ノードシークレットファイルを削除するには、**clear aaa sdi node-secret** コマンドを使用します。

aaa sdi import-node-secret *filepath rsa_server_address password*

構文の説明

filepath	RSA Authentication Manager からエクスポートして解凍されたノードシークレットファイルへの完全なパス。ファイルをインポートするためにサポートされているロケーションは次のとおりです。ロケーションに応じた完全なパスとファイル名を指定します。 • disk0: • disk1: • flash: • ftp:// • http:// • https:// • scp:// • smb:// • tftp://
rsa_server_address	ノードシークレットが属する RSA Authentication Manager サーバーの IP アドレスまたは完全修飾ホスト名。
password	エクスポート時にファイルを保護するために使用されるパスワード。

コマンド デフォルト

デフォルト値はありません。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.15(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

RSA Authentication Manager（SecurID）サーバーによって生成されたノードシークレットファイルを手動でインポートできます。

RSA Authentication Manager サーバーからノードシークレットファイルをエクスポートする必要があります。詳細については、RSA Authentication Manager のドキュメントを参照してください。次に、解凍したファイルを ASA にアップロードするか、このコマンドを使用してインポートできるサーバーに配置します。

例

次に、rsaam.example.com サーバーの nodesecret.rec ファイルをインポートする例を示します。パスワードは mysecret です。

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret

nodesecret.rec imported successfully
ciscoasa#
```

関連コマンド

コマンド	説明
clear aaa sdi node-secret	インポートされた SDI ノードシークレットファイルをクリアします。
show aaa sdi node-secrets	インポートされたノードシークレットファイルがある SecurID サーバーに関する情報を表示します。

aaa-server

AAA サーバーグループを作成し、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 サーバー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ー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**（認証およびサーバー管理プロトコル（ACE）を使用する RSA SecurID） • **tacacs+**
server-tag	サーバー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 サーバー グループ名を参照します。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 サーバー 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 サーバー 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。
9.13(1)	許可されるサーバー グループ数の制限は、シングル モードでは 100 から 200 に、マルチ モードでは 4 から 8 に増加しました。また、グループ内のサーバー数の制限は、マルチ モードで 4 から 8 に増加しました。シングル モードでのグループごとのサーバー数の制限は 16 であり、変更されていません。

使用上のガイドライン

シングル モードで最大 100 個のサーバー グループ、またはマルチ モードでコンテキストごとに 4 つのサーバー グループを持つことができます。9.13(1) 以降では、制限はシングルモードでは 200 グループ、マルチモードでは 8 グループに増加しています。

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 台のサーバーを含めることができます。9.13(1) 以降では、マルチモードの制限はグループあたり 8 台のサーバーです。ユーザーがログインすると、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ーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

aaa-server コマンドで AAA サーバーグループプロトコルを定義することによって AAA サーバー 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ーをグループに追加します。**aaa-server protocol** コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

RADIUS プロトコルを使用する場合、AAA サーバー 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 クライアント 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有効にするには、**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 サーバーに送信されます。
- ASA と AD エージェントとの間の共有秘密を指定し、RADIUS サーバーグループにフル機能の RADIUS サーバーではない 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。ユーザー 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 サーバー 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 サーバー 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。

例

次に、**aaa-server** コマンドを使用して、TACACS+ サーバー 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ーに送信されるか（シングル モード）、グループ内のすべてのサーバーに送信されるか（同時モード）を指定します。
reactivation-mode	障害の発生したサーバーを再度アクティブにする方式を指定します。
max-failed-attempts	サーバー グループ内の所定のサーバーが非アクティブ化されるまでに、そのサーバー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 サーバー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 サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

aaa-server active、fail

障害とマークされたAAAサーバー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ー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	サーバーをアクティブ状態に設定します。
fail	サーバーを障害状態に設定します。
host	ホストの IP アドレス名または IP アドレスを指定します。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS名を使用してサーバー名を指定します。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 サーバーの IP アドレスを指定します。
server_tag	サーバー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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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ーは、グループ内のすべてのサーバー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ーに障害が発生した後に、サーバーはすべて再度アクティブにされます。

例

次に、サーバー 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 サーバー グループを作成および変更します。
clear configure aaa-server	AAA サーバー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 サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

aaa-server host

AAA サーバーを AAA サーバーグループの一部として設定し、ホスト固有の AAA サーバー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）認証サーバー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** となります（使用可能な場合）。 （注） インターフェイスを使用してホストを設定後、インターフェイスを変更する必要がある場合は、最初に **no** フォームを使用して host コマンドを削除する必要があります。その後、正しいインターフェイスで新しいホストエントリを追加できます。最初にコマンドを削除せずにインターフェースを変更しようとすると、変更は受け入れられますが無視されます。
key	（任意）127 文字までの大文字と小文字が区別される英数字のキーワードを指定します。RADIUS サーバーまたは TACACS+ サーバー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 とサーバー間でデータを暗号化するために使われ、ASA とサーバー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ー名を指定します。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。 DNS 名を使用すると、名前が IP アドレスに解決されるのは、最初にサーバーを作成したとき、または障害状態からアクティブ状態に戻ったときに、サーバーがアクティブに移行した場合だけです。名前の存続可能時間（TTL）が期限切れになったため、名前が解決されません。
server-ip	AAA サーバーの IP アドレスを指定します。
server-tag	サーバー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 サーバーへの要求を断念します。スタンバイ AAA サーバーが存在する場合、ASA は要求をそのバックアップサーバーに送信します。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。

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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)	ユーザー 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 サーバーの IPv6 アドレッシングおよび Radius サーバーへの接続のサポートが追加されました。
9.13(1)	許可されるサーバー グループ数の制限は、シングル モードでは 100 から 200 に、マルチ モードでは 4 から 8 に増加しました。また、グループ内のサーバー数の制限は、マルチ モードで 4 から 8 に増加しました。シングル モードでのグループごとのサーバー数の制限は 16 であり、変更されていません。

使用上のガイドライン

aaa-server コマンドで AAA サーバーグループを定義することによって AAA サーバー 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ー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 サーバー 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 サーバー接続データを指定および管理できます。

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 台のサーバーを含めることができます。9.13(1) 以降では、マルチモードの制限はグループあたり 8 台のサーバーです。ユーザーがログインすると、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ーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

例

次に、「watchdogs」という名前の Kerberos AAA サーバー グループを設定し、そのグループに AAA サーバーを追加し、そのサーバーの 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 サーバー グループを設定し、そのグループに AAA サーバーを追加し、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。

デフォルトではない **server-type microsoft** コマンドを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 サーバー グループを作成および変更します。
clear configure aaa-server	AAAサーバー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サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

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、特定の日時および曜日を定義します。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。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいて 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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

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ー 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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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、ユーザーに関連付けられているユーザー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ーごとの ACL がない場合、インターフェイス ACL が適用されます。
- ユーザーごとの 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、ユーザーごとの 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、ユーザーごとの ACL が原因でユーザー 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。ユーザー 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。ユーザーごとのアクセス 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。

- [No **per-user-override**, no **vpn-filter**]：トラフィックはインターフェイス ACL と照合されます。
- [No **per-user-override**, **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 サーバー（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ー（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ー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。

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。

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 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** のルールを記述します。 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、**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。ユーザー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 では、ブリッジ プロトコル データ ユニット。 • **ipx** 0xe0 では、Internet Packet Exchange（IPX）802.2 LLC。 • **isis** 0xfe では、Intermediate System to Intermediate System（IS-IS） • **raw-ipx** 0xff では、Raw IPX 802.3 形式。
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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 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。

コマンド	説明
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 ［ **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 ［ **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 ［ **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 の両方のトラフィックを指定します。**any4** は IPv4 トラフィックのみを指定します。**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を指定します。 • **object-group-network-service** *name*：ネットワークサービス オブジェクトの名前を指定します。

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（廃止予定）**object-group icmp** コマンドを使用して作成された ICMP/ICMP6 用の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 のシビラティ（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** オプションを指定しないのと同じです。

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。プロトコルとポートを指定するネットワークサービス オブジェクトを使用する場合は、この引数でポートを指定しないでください。
	
	使用可能な引数は次のとおりです。
	
	• オペレータポート: ポート名またはポート番号（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**：小なり
	
	  • **gt**：大なり
	
	  • **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。プロトコルとポートを指定するネットワーク サービス オブジェクトを使用する場合は、この引数で **ip** 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ネットワークオブジェクトを指定します。 • **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 グループを指定します。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ネットワークオブジェクトを指定します。 • **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ーを指定します。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ーオブジェクトグループを指定します。
- **user** {[*domain_nickname*\\]*name* | **any** | **none**}：ユーザー名を指定します。ユーザーク レデンシャルを含むすべてのユーザーを照合するには **any** を指定し、ユーザー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*：ユーザー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。

コマンド 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 のデフォルトのシビラティ（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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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」を参照してください。

リリース	変更内容
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ー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。送信元と宛先に、**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。
9.17(1)	**object-group-network-service** 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 **match access-list** コマンド

- ボットネット トラフィック フィルタ **dynamic-filter enable classify-list** コマンド
- AAA **aaa ... match** コマンド
- WCCP **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 ACL
- ユーザー単位 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（ユーザー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 **crypto map** コマンド
- VPN **group-policy** コマンド（**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 サーバー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
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
remarktext	コメントのテキスト。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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。

コマンド	説明
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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

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 では、 IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

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 の両方のトラフィックを指定します。**any4** は IPv4 トラフィックのみを指定します。**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 のシビラティ（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** オプションを指定しないのと同じです。
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**：小なり • **gt**：大なり • **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に一致させるには、**url any** を使用します。そうでない場合は、URL 文字列を入力します。URL 文字列には、ワイルドカードを含めることができます。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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

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」と指定すると、「プロトコル://サーバー IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。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、サーバー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/ および 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、特定サーバー上にある任意の 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ーに送信されるか（シングルモード）、グループ内のすべてのサーバーに送信されるか（同時モード）を指定するには、AAA サーバー 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ーにアカウンティング メッセージを送信します。
single	単一のサーバーにアカウンティング メッセージを送信します。

コマンド 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。

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

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

単一のサーバー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。サーバー グループ内のすべてのサーバー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+）にサーバー 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ー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 サーバー 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 サーバー パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバー 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 サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー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 サーバー 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。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

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 サーバー 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ーで 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ー 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 サーバーを設定し、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	ユーザー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 サーバー 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 サーバー 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 サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー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 サーバー 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ー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 サーバーまたはサーバー グループを指定します。アカウンティング サーバーを設定するには、**aaa-server** コマンドを使用します。

コマンド デフォルト

デフォルトでは、アカウンティング サーバー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。

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

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。

リリース	変更内容
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、ユーザー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 サーバー 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 サーバーを設定します。

acl-netmask-convert

aaa-server host コマンドを使用してアクセスする RADIUS サーバーからダウンロード可能な ACL に受信したネットマスクを ASA でどのように処理するかを指定するには、AAA サーバー ホスト コンフィギュレーション モードで acl-netmask-convert コマンドを使用します。ASA の指定した動作を解除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert { **auto-detect** | **standard** | **wildcard** }
no acl-netmask-convert

構文の説明

auto-detect	ASA は、使用されているネットマスク表現のタイプを判断しようとします。ASA によってワイルドカード ネットマスク表現が検出された場合は、標準ネットマスク表現に変換されます。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	ASA は、RADIUS サーバーから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
wildcard	ASA は、RADIUS サーバーから受信したダウンロード可能な ACL にワイルドカードネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

コマンド デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は実行されません。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

RADIUS サーバーから提供されるダウンロード可能な ACL にワイルドカード形式のネットマスクが含まれている場合は、wildcard または auto-detect キーワードを指定して **acl-netmask-convert**

コマンドを使用します。ASA は、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカードネットマスク表現が含まれていると想定します。ワイルドカードマスクでは、無視するビット位置に 1、照合するビット位置に 0 が配置されます。**acl-netmask-convert** コマンドを使用すると、このような相違が RADIUS サーバー上のダウンロード可能な ACL の設定方法に与える影響を最小限に抑えることができます。

RADIUS サーバーの設定方法が不明な場合は、**auto-detect** キーワードが役立ちます。ただし、「穴」があるワイルドカードネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカードネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可し、Cisco VPN 3000 シリーズ コンセントレータでは有効に使用できます。ただし、ASA では、この表現をワイルドカードネットマスクとして検出できません。

例

次に、ホスト「192.168.3.4」に「srvgrp1」という名前の RADIUS AAA サーバーを設定し、ダウンロード可能な ACL のネットマスクの変換をイネーブルにして、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 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 192.168.3.4
ciscoasa
(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
aaa authentication	aaa-server コマンドまたは ASDM ユーザー認証により指定されたサーバー上の LOCAL、TACACS+、または RADIUS ユーザー認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバー 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 サーバー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。

コマンド	説明
show running-config aaa-server	すべてのAAAサーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルのAAAサーバー統計情報を表示します。

action

アクセスポリシーをセッションに適用するか、またはセッションを終了するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **action** コマンドを使用します。セッションをリセットしてアクセスポリシーをセッションに適用するには、このコマンドの **no** 形式を使用します。

action { **continue** | **terminate** }
no action { **continue** | **terminate** }

構文の説明

continue	アクセス ポリシーをセッションに適用します。
terminate	接続を切断します。

コマンド デフォルト

デフォルト値は continue 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	• 対応	• 対応	• 対応	—	—

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

選択したすべての DAP レコードでセッションにアクセスポリシーを適用するには、**continue** キーワードを使用します。選択した DAP レコードのいずれかで接続を切断するには、**terminate** キーワードを使用します。

例

次に、Finance という DAP ポリシーのセッションを切断する例を示します。

```
ciscoasa (config)#
config-dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
 action terminate
```

```
ciscoasa
(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

action cli command

イベント マネージャ アプレットでアクションを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **action cli command** コマンドを使用します。設定したアクションを削除するには、**no action** *n* コマンドを入力します。

action *n* **cli command "** コマンド **"**
no action *n*

構文の説明

“*command* ”	コマンド名を指定します。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。このコマンドは、特権レベル 15（最高）を持つユーザーとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。コマンドで使用可能な場合は、**noconfirm** オプションを使用します。
n	アクション ID を指定します。有効な ID の範囲は 0 ～ 42947295 です。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

イベント マネージャ アプレットでアクションを設定するには、このコマンドを使用します。

例

次に、イベント マネージャ アプレットでアクションを設定する例を示します。

```
hostname (config-applet)#
action 1 cli command “show version”
```

関連コマンド

コマンド	説明
description	アプレットについて説明します。
event manager run	イベント マネージャ アプレットを実行します。
show event manager	設定された各イベントマネージャ アプレットの統計情報を表示します。
debug event manager	イベント マネージャのデバッグ トレースを管理します。

action-uri

Webサーバーの URI を指定して、シングルサインオン（SSO）認証用のユーザー名とパスワードを受信するには、AAA サーバー ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。

action-uri *string*
no action-uri

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string 認証プログラムの URI。複数行に入力できます。各行の最大文字数は 255 です。URI 全体の最大文字数は、2048 文字です。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

これはHTTP フォームのコマンドを使用した SSO です。URI（ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトな文字列です。これらのコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、ソフトウェア プログラムなどがあります。URI の最も一般的な形式は、Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式またはサブセットで、URL と呼ばれます。

ASA の WebVPN サーバーでは、POST 要求を使用して、認証 Web サーバーに SSO 認証要求を送信できます。これを行うには、HTTP POST 要求を使用して、認証 Web サーバー上のアクション URI にユーザー名とパスワードを渡すように ASA を設定します。**action-uri** コマンドでは、ASA が POST 要求を送信する Web サーバー上の認証プログラムの場所と名前を指定します。

認証 Web サーバー上のアクション URI を見つけるには、ブラウザで直接 Web サーバーのログイン ページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバーのアクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時に ASA によって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それよりも少ない文字を各行に入力できます。

（注） ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、www.example.com の URI を指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

（注） アクション URI にホスト名とプロトコルを含める必要があります。上記の例では、これらは URI の最初にある http://www.example.com に含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバーとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザー パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。

コマンド	説明
user-parameter	SSO認証用にユーザー名を送信する必要があるHTTP POST要求のパラメータの名前を指定します。

activate-tunnel-group-script

このコマンドは、tunnel-group sub-mode で username-from-certificate が設定されている場合に、ASDM によって生成されたスクリプト ファイルをリロードするために内部で使用されます。

（注） このコマンドは、ASA CLI では使用しないでください。

activation-key

ASA にライセンス アクティベーション キーを入力するには、特権 EXEC モードで **activation-key** コマンドを使用します。

activation-key [**noconfirm** *activation_key*] **activate** | **deactivate** }

構文の説明

activate	時間ベースのアクティベーションキーをアクティブ化します。**activate** はデフォルト値です。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。
activation_key	アクティベーションキーを ASA に適用します。*activation_key* は、各要素の間にスペースを 1 つ入れた 5 つの要素から構成される 16 進数のストリングです。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。 1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。
deactivate	時間ベースのアクティベーション キーを非アクティブ化します。非アクティブ化した場合でも、アクティベーションキーは ASA にインストールされたままです。後で **activate** キーワードを使用してアクティブ化できます。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブステートでインストールされます。
noconfirm	（オプション）確認を求めるプロンプトを表示せずにアクティベーション キーを入力します。

コマンド デフォルト

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。インストールされているライセンスを特定するには、**show activation-key** コマンドを参照してください。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	

コマンド履歴

リリース	変更内容
7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
7.1(1)	SSL VPN ライセンスが追加されました。
7.2(1)	5000 ユーザーの SSL VPN ライセンスが ASA 5550 以降に対して追加されました。
7.2(2)	• ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。 • VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートします。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
8.0(2)	• Advanced Endpoint Assessment ライセンスが追加されました。 • VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされます。
8.0(3)	AnyConnect クライアント for Mobile ライセンスが追加されました。
8.0(4)/8.1(2)	時間ベース ライセンスが追加されました。
8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
8.0(4)	UC Proxy セッション ライセンスが追加されました。

リリース	変更内容
8.2(1)	• ボットネット トラフィック フィルタ ライセンスが追加されました。 • AnyConnect Essentials ライセンスが追加されました。デフォルトで、ASA は AnyConnect Essentials ライセンスを使用します。これをディセーブルにして他のライセンスを使用するには、**no anyconnect-essentials** コマンドを使用します。 • SSL VPN の共有ライセンスが追加されました。
8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
8.3(1)	• フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 • 時間ベース ライセンスがスタッカブルになりました。 • IME ライセンスが追加されました。 • 時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できます。 • **activate** キーワードまたは **deactivate** キーワードを使用して、時間ベースライセンスをアクティブ化または非アクティブ化できます。

リリース	変更内容
8.4(1)	• ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。 • ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。 • ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000 K から 2,000 K へ • ASA 5580-40：2,000 K から 4,000 K へ • ASA 5585-X（SSP-10 搭載）：750 K から 1,000 K へ • ASA 5585-X（SSP-20 搭載）：1,000 K から 2,000 K へ • ASA 5585-X（SSP-40 搭載）：2,000 K から 4,000 K へ • ASA 5585-X（SSP-60 搭載）：2,000 K から 10,000 K へ • ASA 5580 の場合、AnyConnect VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • ASA 5580 の場合、その他の VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 • Other VPN ライセンス（以前の IPsec VPN）にはサイトツーサイト セッションが追加されました。 • ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイドコミュニケーションと VPN 機能を無効にしています。

使用上のガイドライン

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要になります。機能ライセンスごとに個別の製品アクティベーション キーを購入する必要があります。たとえば、基本ライセンスがある場合は、Advanced Endpoint Assessment 用と追加の SSL VPN セッション用に別々のキーを購入する必要があります。

製品認証キーを取得した後、次のいずれかの URL の Cisco.com でキーを登録する必要があります。

• Cisco.com の登録済みユーザーの場合は、次の Web サイトを使用します。

http://www.cisco.com/go/license

- Cisco.com の登録済みユーザーではない場合は、次の Web サイトを使用します。

http://www.cisco.com/go/license/public

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。
- 共有ライセンスは、マルチ コンテキスト モードではサポートされていません。

フェールオーバーのガイドライン

- 共有ライセンスは、アクティブ/アクティブ モードではサポートされていません。
- フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。

旧バージョンの ASA ソフトウェアは、各ユニット上のライセンスが一致する必要がありました。バージョン 8.3(1) から、同一のライセンスをインストールする必要がなくなりました。通常、ライセンスをプライマリ ユニット専用に購入します。アクティブ/スタンバイ フェールオーバーでは、セカンダリ ユニットがアクティブになるとプライマリ ライセンスを継承します。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。

- ASA 5505 および 5510 では、両方の装置に Security Plus ライセンスが必要です。基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ装置ではフェールオーバーをイネーブルにできません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2* より前に追加された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーションキーの互換性は存続します。ただし、*8.2* 以降に追加された機能ライセンスをアクティブ化した場合は、アクティベーションキーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、より堅牢な時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり追加されました。

- 複数の時間ベースのアクティベーションキーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベースキーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
- フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

その他のガイドラインと制限事項

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーションキーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要がある場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- すべてのライセンス タイプをアクティブ化できますが、たとえば、マルチ コンテキスト モードおよびVPNなど一部の機能には相互互換性がありません。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。SSL VPN フル ライセンス、SSL VPN 共有ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスがこれらのライセンスの代わりに使用されます。設定の AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用するように復元するには、**no anyconnect-essentials** コマンドを使用します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。<xref> に、リロードが必要なライセンスを示します。

表 *1*:永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
ASA 5505 および ASA 5510	基本ライセンスと Security Plus ライセンスの切り替え
すべてのモデル	暗号化ライセンスの変更
すべてのモデル	永続ライセンスのダウングレード（たとえば、10個のコンテキストから 2 個のコンテキストへ）。

例

次に、ASA のアクティベーションキーを変更する例を示します。

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

次に、**activation-key** コマンドの出力例を示します。ここでは、新しいアクティベーションキーが古いアクティベーションキーと異なる場合のフェールオーバーに対する出力が示されています。

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada
Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
 in the new activation key:
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y
]
Flash permanent activation key was updated with the requested key.
```

次に、ライセンス ファイルの出力例を示します。

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520
Failover                        : Enabled
VPN-DES                         : Enabled
VPN-3DES-AES                    : Enabled
Security Contexts               : 10
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.
Platform = asa
123456789JA: yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.
Platform = asa
123456789JA: yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

関連コマンド

コマンド	説明
anyconnect-essentials	AnyConnect Essentials ライセンスをイネーブルまたはディセーブルにします。
show activation-key	アクティベーション キーを表示します。
show version	ソフトウェア バージョンおよびアクティベーション キーを表示します。

activex-relay

クライアントレスポータルに ActiveX を必要とするアプリケーションを埋め込むには、グループポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードで **activex-relay** コマンドを使用します。デフォルトのグループポリシーから **activex-relay** コマンドを継承するには、このコマンドの **no** 形式を使用します。

activex-relay { **enable** | **disable** }
no activex-relay

構文の説明

enable	WebVPN セッションの ActiveX をイネーブルにします。
disable	WebVPN セッションの ActiveX をディセーブルにします。

コマンド 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

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

オブジェクトタグがある HTML コンテンツ（画像、オーディオ、ビデオ、Java アプレット、ActiveX、PDF、またはフラッシュなど）に対する ActiveX をユーザーが WebVPN ブラウザから起動できるようにするには、**activex-relay enable** コマンドを使用します。これらのアプリケーションでは、WebVPN セッションを使用して ActiveX コントロールをダウンロードおよびアップロードします。ActiveX リレーは、WebVPN セッションが閉じるまで有効です。Microsoft OWA 2007 などを使用する場合は、ActiveX をディセーブルにする必要があります。

（注） これらには同じ機能があるため、スマートトンネルをディセーブルにしても、**activex-relay enable** コマンドによってスマートトンネルのログが生成されます。

次に、特定のグループ ポリシーに関連付けられている WebVPN セッションの ActiveX コントロールをイネーブルにする例を示します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

次に、特定のユーザー名に関連付けられている WebVPN セッションの ActiveX コントロールをディセーブルにする例を示します。

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。