Cisco IOS セキュリティ コマンド リファレンス：コマンド A ～ C、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 11 日

最終更新：2013 年 01 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

aaa authentication banner ～ aaa group server tacacs+

aaa authentication banner

ユーザのログイン時に表示されるパーソナライズされたバナーを設定するには、グローバル コンフィギュレーション モードで **aaa authentication banner** コマンドを使用します。 バナーを削除するには、このコマンドの no 形式を使用します。

aaa authentication banner *dstringd*

no aaa authentication banner

構文の説明

d	文字列がバナーとして表示されるシステムに通知するための文字列の先頭と末尾のデリミタ。デリミタには、拡張ASCII文字セットの任意の文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト文字列には使用できません。
string	デリミタとして使用されるもの以外の文字グループ。 表示可能な文字の最大数は 2996 文字です。

コマンド デフォルト

イネーブルになっていません

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3(4)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

ユーザのシステムへのログイン時に表示されるパーソナライズされたメッセージを作成するには、**aaa authentication banner** コマンドを使用します。 ユーザのログイン時のデフォルト メッセージは、このメッセージまたはバナーに置き換えられます。

ログイン バナーを作成するには、デリミタを設定する必要があります。デリミタはシステムに通知され、デリミタに続くテキストストリングはバナーとして表示され、テキストストリング自体が表示されます。デリミタは、バナーの末尾を示すために、テキストストリングの末尾で繰り返されます。 デリミタには、拡張 ASCII 文字セットの任意の文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト文字列には使用できません。

（注） TACACS+ が方式リストの最初にある場合、AAA 認証バナー メッセージは表示されません。

例

次に、**aaa authentication banner** が設定されていない場合のデフォルトのログイン メッセージを示します。 （RADIUS はデフォルト ログイン認証方式として指定されます）。

```
aaa new-model
aaa authentication login default group radius
```

この設定によって、次の標準出力が作成されます。

```
User Verification Access
Username:
Password:
```

次に、ユーザがシステムにログインしたときに表示されるログイン バナー（この場合、「Unauthorized use is prohibited.」というフレーズ）を設定する例を示します。 この場合、アスタリスク（*）記号は、デリミタとして使用されます。 （RADIUS はデフォルト ログイン認証方式として指定されます）。

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

この設定によって、次のログイン バナーが生成されます。

```
Unauthorized use is prohibited.
Username:
```

関連コマンド

コマンド	説明
aaa authentication fail-message	ユーザがログインに失敗したときに表示されるパーソナライズされたバナーを設定します。

aaa authentication dot1x

IEEE 802.1X を実行するインターフェイスで 1 つまたは複数の認証、許可、アカウンティング（AAA）方式を指定するには、グローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x {**default**| *listname*} *method1* [*method2 ...*]

no aaa authentication dot1x {**default**| *listname*} *method1* [*method2 ...*]

構文の説明

default	ユーザのログイン時のデフォルトの方式リストとして、この引数に続くリストされた認証方式を使用します。
listname	ユーザのログイン時に試行される認証方式のリストに名前を付けるために使用する文字列。
method1 [*method2...*]	次の少なくとも 1 つのキーワード • **enable**：認証にイネーブル パスワードを使用します。 • **group radius**：認証にすべての RADIUS サーバのリストを使用します。 • **line**：認証にライン パスワードを使用します。 • **local**：認証にローカルなユーザ名データベースを使用します。 • **local-case**：認証に大文字小文字を区別するローカル ユーザ名データベースを使用します。 • **none**：認証を使用しません。 クライアントは、クライアントが提供する情報を使用しないで、スイッチによって自動的に認証されます。

コマンド デフォルト

認証は実行されません。

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(6)EA2	このコマンドが Cisco イーサネット スイッチ ネットワーク モジュールに追加されました。
12.2(15)ZJ	このコマンドが、Ciscoイーサネット スイッチ モジュールのプラットフォーム Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズに実装されました。
12.3(2)XA	このコマンドが Cisco 806、Cisco 831、Cisco 836、Cisco 837、Cisco 1701、Cisco 1710、Cisco 1721、Cisco 1751-V、および Cisco 1760 の Cisco ルータ プラットフォームに追加されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。 Cisco 1751、Cisco 2610XM - Cisco 2611XM、Cisco 2620XM - Cisco 2621XM、Cisco 2650XM - Cisco 2651XM、Cisco 2691、Cisco 3640、Cisco 3640A、および Cisco 3660 のプラットフォームにルータのサポートが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために一定の順序で試みる方式のリストを指定します。 実際に 802.1x に準拠している唯一の方式は、クライアント データが RADIUS 認証サーバに対して確認される **group radius** 方式です。 その他の方式は、ローカルで設定されているデータを使用して、AAA をイネーブルにしてクライアントを認証します。 たとえば **local** および **local-case** 方式では、Cisco IOS コンフィギュレーション ファイルに保存されているユーザ名とパスワードを使用します。 **enable** 方式および **line** 方式は、認証に **enable** パスワードと **line** パスワードを使用します。

group radius を指定する場合、**radius-server host** グローバル コンフィギュレーション コマンドを入力して、RADIUS サーバを設定する必要があります。 RADIUS サーバを使用していない場合、**local** 方式または **local-case** 方式を使用できます。これらは、ローカル ユーザ名データベースにアクセスして、認証を実行します。 **enable** 方式または **line** 方式を指定すると、クライアントにパスワードを提供してスイッチにアクセスできます。

設定された認証方式のリストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

例

次に、AAA をイネーブルにして 802.1X の認証リストを作成する例を示します。 この認証は、最初に RADIUS サーバとの交信を試みます。 この操作でエラーが返された場合、ユーザは認証なしで、アクセスが許可されます。

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

関連コマンド

コマンド	説明
debug dot1x	802.1X デバッグ情報を表示します。
identity profile default	アイデンティティ プロファイルを作成し、dot1x プロファイル コンフィギュレーション モードを開始します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。
show dot1x (EtherSwitch)	スイッチまたは指定したインターフェイスの 802.1X 統計情報、管理ステータス、動作状態を表示します。

aaa authentication fail-message

ユーザがログインに失敗したときに表示されるパーソナライズされたバナーを設定するには、グローバル コンフィギュレーション モードで **aaa authentication fail-message** コマンドを使用します。 ログイン失敗メッセージを削除するには、このコマンドの no 形式を使用します。

aaa authentication fail-message *dstringd*

no aaa authentication fail-message

構文の説明

d	文字列がバナーとして表示されるシステムに通知するための文字列の先頭と末尾のデリミタ。デリミタには、拡張ASCII文字セットの任意の文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト文字列には使用できません。
string	デリミタとして使用されるもの以外の文字グループ。 表示可能な文字の最大数は 2996 文字です。

コマンド デフォルト

イネーブルになっていません

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3(4)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

ユーザがログインに失敗したときに表示されるパーソナライズされたメッセージを作成するには、**aaa authentication fail-message** コマンドを使用します。 デフォルトのログイン失敗メッセージは、このメッセージに置き換えられます。

failed-login バナーを作成するには、デリミタを設定する必要があります。デリミタはシステムに通知され、デリミタに続くテキストストリングはバナーとして表示され、テキストストリング自体が表示されます。デリミタは、バナーの末尾を示すために、テキストストリングの末尾で繰り返されます。 デリミタには、拡張 ASCII 文字セットの任意の文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキスト文字列には使用できません。

例

次に、**aaa authentication banner** および **aaa authentication fail-message** が設定されていない場合のデフォルトのログイン メッセージおよびログイン失敗メッセージを示します。 （RADIUS はデフォルト ログイン認証方式として指定されます）。

```
aaa new-model
aaa authentication login default group radius
```

この設定によって、次の標準出力が作成されます。

```
User Verification Access
Username:
Password:
% Authentication failed.
```

次に、ログイン バナー（「Unauthorized use is prohibited.」）およびログイン失敗メッセージ（「Failed login. Try again.」）の両方を設定する例を示します。 ログイン メッセージは、ユーザがシステムにログインしたときに表示されます。 ログイン失敗メッセージは、ユーザがシステムへのログインを試みて失敗したときに表示されます（デフォルトのログイン認証方式として RADIUS が指定されています）。この例では、アスタリスク（*）記号がデリミタとして使用されています。

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

この設定で、次のログイン バナーと失敗ログイン バナーが生成されます。

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

関連コマンド

コマンド	説明
aaa authentication banner	ユーザがログインしたときに表示されるパーソナライズされたバナーを設定します。

aaa authentication login

ログイン時に認証、許可、アカウンティング（AAA）認証を設定するには、グローバル コンフィギュレーション モードで **aaa authentication login** コマンドを使用します。 AAA 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication login {**default**| *list-name*} **[passwd-expiry]** *method1* [*method2 ...*]

no aaa authentication login {**default**| *list-name*} **[passwd-expiry]** *method1* [*method2 ...*]

構文の説明

default	ユーザのログイン時のデフォルトの方式リストとして、このキーワードに続くリストされた認証方式を使用します。
list-name	ユーザがログインするときにアクティブ化される認証方式リストに、名前を付けるときに使用する文字列。詳細については、「使用上のガイドライン」の項を参照してください。
passwd-expiry	ローカル認証リストのパスワードのエージングをイネーブルにします。 （注） **passwd-expiry** キーワードを機能させるには、**radius-server vsa send authentication** コマンドが必要です。
method1 [*method2...*]	認証アルゴリズムが一定の順序で試みる方式のリスト。 1 つ以上の方式を入力する必要があります。また最高 4 つの方式を入力できます。 次の表に、方式キーワードを示します。

コマンド デフォルト

ログイン時の AAA 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
10.3	このコマンドが導入されました。

リリース	変更内容
12.0(5)T	このコマンドが変更されました。 認証の方式として**group radius**、**group tacacs+**、および **local-case** キーワードが追加されました。
12.4(6)T	このコマンドが変更されました。 **password-expiry** キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。 認証の方式として **cache** *group-name* キーワードおよび引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M に統合されました。
15.1(1)T	このコマンドが変更されました。 **group ldap** キーワードが追加されました。
Cisco IOS XE Release 3.1S	このコマンドが Cisco IOS XE Release 3.1S に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
15.0(1)S	このコマンドが Cisco IOS Release 15.0(1)S に統合されました。

使用上のガイドライン

default キーワードが設定されていない場合、ローカル ユーザ データベースだけがチェックされます。 これは、次のコマンドと同じ結果になります。

```
aaa authentication login default local
```

（注） コンソール上では、**default** キーワードが設定されていない場合、認証チェックなしでログインが成功します。

aaa authentication login コマンドで作成したデフォルトおよびオプション リストの名前は、**login authentication** コマンドで使用されます。

特定のプロトコルに対し、**aaa authentication login** *list-name method* コマンドを入力してリストを作成します。 *list-name* 引数は、ユーザがログインするときにアクティブ化される認証方式のリストに名前を指定するのに使用する文字列です。 *method* 引数には、認証アルゴリズムが一定の順序で試みる方式のリストを指定します。 aaa authentication login, （9 ページ）セクションでは、

list-name 引数に使用できない認証方式のリストを示します。また、次の表に方式のキーワードを示します。

回線にリストが割り当てられていない場合に使用するデフォルト リストを作成するには、**login authentication** コマンドをデフォルト引数で使用します。その後、デフォルトの状況で使用する方式を使用します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 すべての方法でエラーが返されても、認証が成功するようにするには、コマンド ラインの最後の方式として **none** を指定します。

回線に対して認証が明示的に設定されていない場合、デフォルトではアクセスが拒否され、認証は実行されません。 現在設定されている認証方式のリストを表示するには、**more system:running-config** コマンドを使用します。

list-name 引数に使用できない認証方式

list-name 引数に使用できない認証方式は次のとおりです。

- **auth-guest**
- **enable**
- **guest**
- **if-authenticated**
- **if-needed**
- **krb5**
- **krb-instance**
- **krb-telnet**
- **line**
- **local**
- **none**
- **radius**
- **rcmd**
- **tacacs**
- **tacacsplus**

（注） 次の表に、以前に定義された一連の RADIUS サーバまたは TACACS+ サーバを参照する **group radius**、**group tacacs +**、**group ldap**、および **group***group-name* 方式を示します。 ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンド、**aaa group server ldap** コマンド、および **aaa group server tacacs+** コマンドを使用します。

次の表に、方式のキーワードを示します。

表 *1*：*aaa authentication login* 方法のキーワード

キーワード	説明
cache *group-name*	キャッシュ サーバ グループを認証に使用します。
enable	認証にイネーブル パスワードを使用します。このキーワードは使用できません。
group *group-name*	認証に **aaa group server radius** コマンドまたは **aaa group server tacacs+** コマンドで定義された RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。
group ldap	認証にすべての Lightweight Directory Access Protocol（LDAP）サーバのリストを使用します。
group radius	認証にすべての RADIUS サーバのリストを使用します。
group tacacs+	認証にすべての TACACS+ サーバのリストを使用します。
krb5	Kerberos 5 を認証に使用します。
krb5-telnet	ルータへの接続に Telnet を使用する場合、Kerberos 5 Telnet 認証プロトコルを使用します。
line	認証にライン パスワードを使用します。
local	認証にローカルなユーザ名データベースを使用します。
local-case	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
none	認証を使用しません。
passwd-expiry	ログイン リストを使用してパスワード エージングをサポートします。

例

次に、*MIS-access* と呼ばれる AAA 認証リストを作成する例を示します。 この認証は、まず TACACS+サーバに接続を試みます。サーバが見つからない場合は、TACACS+がエラーを返し、AAA はイネーブル パスワードの使用を試みます。（サーバにイネーブル パスワードが設定されていないため）この試みがエラーを返す場合、ユーザは認証なしでのアクセスが許可されます。

```
aaa authentication login MIS-access group tacacs+ enable none
```

次に、同じリストを作成する例を示します。ただし、他のリストが指定されていない場合、すべてのログイン認証に使用されるデフォルトのリストが設定されます。

```
aaa authentication login default group tacacs+ enable none
```

次に、Telnet を使用してルータに接続する場合、ログイン時の認証に Kerberos 5 Telnet 認証プロトコルを使用するように設定する例を示します。

```
aaa authentication login default krb5
```

次に、crypto クライアントに AAA を使用することによってパスワード エージングを設定する例を示します。

```
aaa authentication login userauthen passwd-expiry group radius
```

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
login authentication	ログインに対する AAA 認証をイネーブルにします。

aaa authorization

ネットワークへのユーザ アクセスを制限する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 authorization** コマンドを使用します。 パラメータを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization {**auth-proxy**| **cache**| **commands** *level*| **config-commands**| **configuration**| **console**| **exec**| **ipmobile**| **multicast**| **network**| **policy-if**| **prepaid**| **radius-proxy**| **reverse-access**| **subscriber-service**| **template**} {**default**| *list-name*} [*method1* [*method2 ...*]]

no aaa authorization {**auth-proxy**| **cache**| **commands** *level*| **config-commands**| **configuration**| **console**| **exec**| **ipmobile**| **multicast**| **network**| **policy-if**| **prepaid**| **radius-proxy**| **reverse-access**| **subscriber-service**| **template**} {**default**| *list-name*} [*method1* [*method2 ...*]]

構文の説明

auth-proxy	認証プロキシ サービスの許可を実行します。
cache	認証、許可、アカウンティング（AAA）サーバを設定します。
commands	指定した特権レベルですべてのコマンドの許可を実行します。
level	許可が必要な特定のコマンド レベル。 有効な値は 0 ～ 15 です。
config-commands	許可を実行して、コンフィギュレーションモードで入力されるコマンドが許可されるかどうかを確認します。
configuration	AAA サーバからコンフィギュレーションをダウンロードします。
console	AAA サーバのコンソール許可をイネーブルにします。
exec	許可を実行して、EXEC シェルを実行することがユーザに許可されているかどうかを確認します。 この機能では、autocommand の情報など、ユーザ プロファイルの情報が返されます。
ipmobile	モバイル IP サービスの許可を実行します。
multicast	AAA サーバからマルチキャスト コンフィギュレーションをダウンロードします。

network	シリアル ライン インターネット プロトコル（SLIP）、PPP（ポイントツーポイント プロトコル）、PPP ネットワーク コントロール プログラム（NCP）、AppleTalk Remote Access（ARA）など、すべてのネットワーク関連サービス要求について許可を実行します。
policy-if	diameter ポリシー インターフェイス アプリケーションの許可を実行します。
prepaid	diameter プリペイド サービスの許可を実行します。
radius-proxy	プロキシ サービスの許可を実行します。
reverse-access	リバース Telnet などのリバース アクセス接続の許可を実行します。
subscriber-service	Virtual Private Dialup Network（VPDN）などの iEdge 加入者サービスの許可を実行します。
template	AAA サーバのテンプレート許可をイネーブルにします。
default	このキーワードに続く許可方式のリストを許可のデフォルト方式リストとして使用します。
list-name	許可方式リストの名前の指定に使用する文字列です。
method1 [*method2...*]	（任意）許可に使用する 1 つまたは複数の許可方式を指定します。方式は、次の表に示すキーワードのいずれかである可能性があります。

コマンド デフォルト

すべてのアクションに対する許可がディセーブルになります（キーワード **none** と同等）。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。

リリース	変更内容
12.0(5)T	このコマンドが変更されました。 許可の方式として **group radius** および **group tacacs+** キーワードが追加されました。
12.2(28)SB	このコマンドが変更されました。 許可の方式として **cache** *group-name* キーワードおよび引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.0(1)M	このコマンドが、Cisco IOS Release 15.0(1)M に統合されました。
15.1(1)T	このコマンドが変更されました。 **group ldap** キーワードが追加されました。

使用上のガイドライン

許可をイネーブルにし、ユーザが特定の機能にアクセスしたときに使用できる許可方式を定義する名前付き方式リストを作成するには、**aaa authorization** コマンドを使用します。 許可の方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。 方式リストは、順番に使用される許可方式（RADIUS、TACACS+ など）を説明する名前付きリストです。 方式リストを使用すると、許可に使用するセキュリティ プロトコルを 1 つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。 Cisco IOS ソフトウェアでは、特定のネットワーク サービスについてユーザを許可するために最初の方式が使用されます。その方式が応答しない場合、方式リストの次の方式が選択されます。 このプロセスは、リスト内の許可方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。 このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

特定の許可タイプの **aaa authorization** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線（この許可タイプが適用される）にデフォルトの方式リストが自動的に適用されます（定義された方式リストによって、デフォルトの方式リストが上書きされます）。デフォルトの方式リストが定義されていない場合は許可が実行されません。 RADIUS サーバからの IP プールのダウンロードの許可など、アウトバウンド許可を実行するには、デフォルトの許可方式リストを使用する必要があります。

list-name および *method* 引数の値を入力してリストを作成するには、**aaa authorization** コマンドを使用します。ここで、*list-name* はこのリストの名前（すべての方式名を除く）の指定に使用する文字列で、*method* には、一定の順序で試みる許可方式のリストを指定します。

（注） 次の表に、以前に定義された一連の RADIUS サーバまたは TACACS+ サーバを参照する **group** *group-name*、**group ldap**、**group radius**、および **group tacacs +** 方式を示します。 ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。 サーバの名前付きグループを作成するには、**aaa group server radius** コマンド、**aaa group server ldap** コマンド、および **aaa group server tacacs+** コマンドを使用します。

次の表に、方式のキーワードを示します。

表 *2*：*aaa authorization* 方式

キーワード	説明
cache *group-name*	許可にキャッシュ サーバ グループを使用します。
group *group-name*	アカウンティングに **server group** *group-name* コマンドで定義される RADIUS または TACACS+ サーバのサブセットを使用します。
group ldap	認証にすべての Lightweight Directory Access Protocol（LDAP）サーバのリストを使用します。
group radius	認証に **aaa group server radius** コマンドで定義されるすべての RADIUS サーバのリストを使用します。
group tacacs+	認証に **aaa group server tacacs+** コマンドで定義されるすべての TACACS+ サーバのリストを使用します。
if-authenticated	ユーザが認証されると、ユーザが要求した機能にアクセスすることを許可します。 （注） **if-authenticated** 方式は終了方式です。したがって、これが方式としてリストされている場合、この方式の後にリストされている方式は評価されません。
local	許可にローカル データベースを使用します。

キーワード	説明
none	許可が実行されないことを示します。

Cisco IOS ソフトウェアは、次の許可の方式をサポートしています。

- Cache Server Groups：ルータがユーザに固有の権限を許可するキャッシュ サーバ グループを照会します。
- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従って、ローカル データベースに問い合わせて、ユーザに固有の権限を許可します。 ローカル データベースでは制御できるのは、一部の機能だけです。
- None：ネットワーク アクセス サーバは、許可情報を要求しません。許可は、この回線またはインターフェイスで実行されません。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバ グループからの許可情報を要求します。 RADIUS 許可では、属性を関連付けることでユーザに固有の権限を定義します。属性は適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。
- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと許可情報を交換します。 TACACS+ 許可は、属性値（AV）ペアを関連付けることでユーザに固有の権限を定義します。属性ペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。

方式リストは、要求されている許可のタイプによって異なります。 AAA は 5 種類の許可をサポートしています。

- コマンド：ユーザが実行する EXEC モード コマンドに適用されます。 コマンドの許可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、許可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用します。
- ネットワーク：ネットワーク接続に適用します。 ネットワーク接続には、PPP、SLIP、または ARA 接続を含めることができます。

（注） 先頭に **do** コマンドを追加した EXEC コマンドを含むグローバル コンフィギュレーション コマンドを許可するには、**aaa authorization config-commands** コマンドを設定する必要があります。

- リバース アクセス：リバース Telnet セッションに適用します。
- コンフィギュレーション：AAA サーバからダウンロードされるコンフィギュレーションに適用します。

名前付き方式リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。

許可コマンドにより、許可プロセスの一部としてRADIUSまたはTACACSデーモンに送信される一連のAVペアを含む要求パケットが発生します。 デーモンは、次のいずれかのアクションを実行できます。

- 要求をそのまま受け入れます。
- 要求を変更します。
- 要求と許可を拒否します。

サポートされるRADIUS属性のリストについては、「RADIUS属性」モジュールを参照してください。 サポートされるTACACS+ AVペアのリストについては、「TACACS+属性値ペア」モジュールを参照してください。

（注） **disable**、**enable**、**exit**、**help**、および**logout**の5つのコマンドは、特権レベル0に関連付けられています。 特権レベルのAAA許可を1以上に設定した場合、これらの5つのコマンドは特権レベル コマンドのセットに含まれません。

例

次に、PPPを使用するシリアル回線にRADIUS許可が使用されるように指定するmygroupという名前のネットワーク許可方式リストを定義する例を示します。 RADIUSサーバが応答しない場合、ローカル ネットワーク許可が実行されます。

```
aaa authorization network mygroup group radius local
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa group server radius	各種のRADIUSサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa group server tacacs+	各種のTACACS+サーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。

コマンド	説明
radius-server host	RADIUS サーバ ホストを指定します。
tacacs-server host	TACACS+ ホストを指定します。
username	ユーザ名をベースとした認証システムを構築します。

aaa dnis map accounting network

AAAアカウンティングに使用される特定の認証、許可、アカウンティング（AAA）サーバグループに着信番号情報サービス（DNIS）番号をマッピングするには、グローバル コンフィギュレーション モードで **aaa dnis map accounting network** コマンドを使用します。名前付きサーバ グループから DNIS マッピングを削除するには、このコマンドの **no** 形式を使用します。

aaa dnis map *dnis-number* **accounting network** [**start-stop**| **stop-only**| **none**] **[broadcast] group** *groupname*

no aaa dnis map *dnis-number* **accounting network**

構文の説明

dnis-number	DNIS の番号。
start-stop	（任意）定義されたセキュリティ サーバ グループがプロセスの開始時に「アカウンティング開始」通知を送信し、プロセスの終了時に「アカウンティング停止」通知を送信することを示します。「アカウンティング開始」レコードはバックグラウンドで送信されます（要求されたユーザ プロセスは、「アカウンティング開始」通知をアカウンティング サーバから受信したかどうかにかかわらず開始されます）。
stop-only	（任意）定義されたセキュリティ サーバ グループが要求されたユーザ プロセスの終了時に「アカウンティング停止」通知を送信することを示します。
none	（任意）定義されたセキュリティ サーバ グループがアカウンティング通知を送信しないことを示します。
broadcast	（任意）複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
group *groupname*	下の表で説明されているキーワードの少なくとも 1 個。

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。

コマンド履歴

リリース	変更内容
12.0(7)T	このコマンドが導入されました。
12.1(1)T	• オプションの **broadcast** キーワードが追加されました。 • 複数のサーバ グループを指定する機能が追加されました。 • 複数のサーバ グループに対応するために、コマンドの名前が **aaa dnis map accounting network group** から **aaa dnis map accounting network** に変更されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドは、特定のDNISを使用してネットワークに電話をかけているユーザのアカウンティング要求をサーバ グループが処理できるように、特定の AAA サーバ グループに DNIS 番号を割り当てることができます。 このコマンドを使用するには、まず AAA をイネーブルにし、AAA サーバ グループを定義して、DNIS マッピングをイネーブルにする必要があります。

次の表に、アカウンティング方式のキーワードについての説明を示します。

表 *3*：*AAA* アカウンティング方式

キーワード	説明
group radius	認証に **aaa group server radius** コマンドで定義されるすべてのRADIUSサーバのリストを使用します。
group tacacs+	認証に **aaa group server tacacs+** コマンドで定義されるすべての TACACS+ サーバのリストを使用します。
group group-name	*group-name* サーバ グループで定義したように、アカウンティングのためのRADIUSサーバまたは TACACS+ サーバのサブセットを使用します。

上の表に、以前に定義された一連の RADIUS サーバまたは TACACS+ サーバを参照する **group radius** および **group tacacs +** 方式を示します。 ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。 サーバの名前付きグループを作成するには、**aaa group server radius** コマンドおよび **aaa group server tacacs+** コマンドを使用します。

例

次に、group1 と呼ばれる RADIUS サーバ グループに DNIS 番号 7777 をマッピングする例を示します。 サーバ グループ group1 は、DNIS 7777 で電話をかけるユーザのアカウンティング要求に対して RADIUS サーバ 172.30.0.0 を使用します。

```
aaa new-model
radius-server host 172.30.0.0 acct-port 1646 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 accounting network group group1
```

関連コマンド

コマンド	説明
aaa dnis map authentication ppp group	特定の認証サーバ グループに DNIS 番号をマッピングします。
aaa dnis map enable	DNIS に基づいて、AAA サーバの選択をイネーブルにします。
aaa group server	複数のサーバ ホストを別々のリストと別々の方式にグループ分けします。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

aaa dnis map authentication group

AAAアカウンティングに使用される特定の認証サーバ グループ（認証、許可、アカウンティング（AAA）認証に使用されるサーバ グループ）に着信番号識別サービス（DNIS）番号をマッピングするには、AAA サーバ グループ コンフィギュレーション モードで **aaa dnis map authentication group** コマンドを使用します。 定義済みのサーバ グループから DNIS 番号を削除するには、このコマンドの **no** 形式を使用します。

aaa dnis map *dnis-number* **authentication** {**ppp| login**} **group** *server-group-name*

no aaa dnis map *dnis-number* **authentication** {**ppp| login**} **group** *server-group-name*

構文の説明

dnis-number	DNIS の番号。
ppp	PPP 認証方式をイネーブルにします。
login	文字モード認証をイネーブルにします。
server-group-name	サーバ グループに関連付けられているセキュリティ サーバのグループの名前を指定するのに使用する文字列。

コマンド デフォルト

DNIS 番号はサーバ グループにマッピングされません。

コマンド モード

AAA-server-group の設定

コマンド履歴

リリース	変更内容
12.0(7)T	このコマンドが導入されました。
12.1(3)XL1	このコマンドは **login** キーワードが追加され、文字モード認証を含むように変更されました。
12.2(2)T	**login** キーワードのサポートが Cisco IOS Release 12.2(2)T に追加され、このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 7200 プラットフォームに実装されました。

リリース	変更内容
12.2(8)T	このコマンドが、IGX8400 プラットフォーム用の Cisco 806、Cisco 828、Cisco 1710、Cisco SOHO 78、Cisco 3631、Cisco 3725、Cisco 3745、および Cisco URM に実装されました。
12.2(11)T	このコマンドが Cisco AS5300 および Cisco AS5800 プラットフォームに実装されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

特定の DNIS を使用してネットワークに電話をかけているユーザのアカウンティング要求をサーバ グループが処理できるように、特定の AAA サーバ グループに DNIS 番号を割り当てるには、**aaa dnis map authentication group** コマンドを使用します。 **aaa dnis map authentication group** コマンドを使用するには、まず AAA をイネーブルにし、AAA サーバ グループを定義して、DNIS マッピングをイネーブルにする必要があります。

例

次に、group1 と呼ばれる RADIUS サーバ グループに DNIS 番号 7777 をマッピングする例を示します。 サーバ グループ group1 は、DNIS 7777 で電話をかけるユーザの認証要求に対して RADIUS サーバ 172.30.0.0 を使用します。

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 aaa dnis map enable
 aaa dnis map 7777 authentication ppp group group1
 aaa dnis map 7777 authentication login group group1
```

関連コマンド

コマンド	説明
aaa dnis map accounting network group	特定のアカウンティング サーバ グループに DNIS 番号をマッピングします。
aaa dnis map enable	DNIS に基づいて、AAA サーバの選択をイネーブルにします。

コマンド	説明
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

aaa group server radius

各種の RADIUS サーバ ホストを別個のリストと別個の方式にグループ化するには、グローバル コンフィギュレーション モードで **aaa group server radius** コマンドを入力します。 コンフィギュレーション リストからグループ サーバを削除するには、このコマンドの **no** 形式を入力します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。 *group-name* 引数として使用できない語句のリストについては、次の表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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.0(5)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

認証、許可、アカウンティング（AAA）サーバグループ機能は、既存のサーバホストをグループ化する手段を導入します。 この機能を使用して、設定されているサーバホストのサブセットを選択し、それらのホストを特定のサービスに使用できます。

グループ サーバは、特定のタイプのサーバ ホストのリストです。 現在サポートされているサーバ ホストのタイプは RADIUS サーバ ホストと TACACS+ サーバ ホストです。 グループ サーバ

は、グローバル サーバ ホスト リストと併せて使用されます。 グループ サーバには、選択したサーバ ホストの IP アドレスが一覧表示されます。

次の表に、*group-name* 引数として使用できない語句を示します。

表 *4*：*group-name* 引数として使用できない語句

語句
auth-guest
enable
guest
if-authenticated
if-needed
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

例

次に、3 つのメンバ サーバからなる radgroup1 という AAA グループ サーバを設定する例を示します。

```
aaa group server radius radgroup1
 server 10.1.1.1 auth-port 1700 acct-port 1701
 server 10.2.2.2 auth-port 1702 acct-port 1703
 server 10.3.3.3 auth-port 1705 acct-port 1706
```

（注） auth-port と acct-port が指定されていない場合、auth-port のデフォルト値は 1645、acct-port のデフォルト値は 1646 です。

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

aaa group server tacacs+

各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化するには、グローバル コンフィギュレーション モードで **aaa group server** tacacs+ コマンドを使用します。 コンフィギュレーション リストからサーバ 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 group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。 *group-name* 引数として使用できない語句のリストについては、次の表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

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(5)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.2(54)SG	このコマンドが、Cisco IOS Release 12.2(54)SG に統合されました。
Cisco IOS XE Release 3.2S	このコマンドが変更されました。 IPv6 のサポートが追加されました。

使用上のガイドライン

認証、許可、アカウンティング（AAA）サーバグループ機能は、既存のサーバホストをグループ化する手段を導入します。この機能を使用して、設定されているサーバホストのサブセットを選択し、それらのホストを特定のサービスに使用できます。

サーバ グループは、特定のタイプのサーバ ホストのリストです。 現在サポートされているサーバ ホストのタイプは RADIUS サーバ ホストと TACACS+ サーバ ホストです。 サーバ グループは、グローバル サーバ ホスト リストと併せて使用されます。 サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

次の表に、*group-name* 引数値に使用できないキーワードを示します。

表 *5*：*group-name* 引数として使用できない語句

語句
auth-guest
enable
guest
if-authenticated
if-needed
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

例

次に、3 つのメンバ サーバからなる tacgroup1 という AAA グループ サーバを設定する例を示します。

```
aaa group server tacacs+ tacgroup1
server 10.1.1.1
server 10.2.2.2
server 10.3.3.3
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。
aaa authentication login	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
tacacs-server host	TACACS+ ホストを指定します。

aaa nas port extended ～ address ipv6（TACACS+）

aaa nas port extended

NAS-Port 属性を RADIUS IETF 属性 26 で置換し、拡張フィールド情報を表示するには、グローバル コンフィギュレーション モードで **aaa nas port extended** コマンドを使用します。 拡張フィールド情報を表示しない場合は、このコマンドの **no** 形式を使用します。

aaa nas port extended

no aaa nas port extended

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

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

各スロットに複数のインターフェイス（ポート）があるプラットフォームの場合、シスコ RADIUS 実装では、インターフェイスを区別できる固有の NAS-Port 属性を提供しません。 たとえば、デュアル PRI インターフェイスがスロット 1 にある場合、Serial1/0:1 と Serial1/1:1 の両方のコールは、RADIUS IETF の NAS-Port 属性に関連付けられた 16 ビットのフィールド サイズ制限により、NAS-Port = 20101 として表示されます。

この場合の解決策は、ベンダー固有属性（RADIUS IETF 属性 26）で NAS-Port 属性を置換することです。 シスコのベンダー ID は 9 であり、Cisco-NAS-Port 属性はサブタイプ 2 です。 ベンダー固有属性（VSA）を有効にするには、**radius-server vsa send** コマンドを入力します。 ベンダー固有属性のポート情報を提供および設定するには、**aaa nas port extended** コマンドを使用します。

標準の NAS-Port 属性（RADIUS IETF 属性 5）は以降も送信されます。 この情報を送信しない場合、**no radius-server attribute nas-port** コマンドを使用して停止できます。 このコマンドを設定すると、標準の NAS-Port 属性は送信されなくなります。

例

次に、RADIUS が拡張インターフェイス情報を表示するように指定する例を示します。

```
radius-server vsa send
aaa nas port extended
```

関連コマンド

コマンド	説明
radius-server extended-portnames	NAS-Port 属性の拡張インターフェイス情報を表示します。
radius-server vsa send	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバを設定します。

aaa new-model

認証、許可、アカウンティング（AAA）アクセス コントロール モデル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 new-model** コマンドを発行します。 AAA アクセス コントロール モデル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 new-model

no aaa new-model

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

AAA がディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.4(4)T	IPv6 のサポートが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXI	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

このコマンドは、AAA アクセス コントロール システムをイネーブルにします。

例

次に、AAA を初期化する例を示します。

```
aaa new-model
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa authentication arap	TACACS+ を使用して ARAP の AAA 認証方式をイネーブルにします。
aaa authentication enable default	AAA 認証をイネーブルにして、ユーザが特権コマンドレベルにアクセスできるかどうかを確認します。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

aaa route download

スタティック ルート ダウンロード機能をイネーブルにし、ダウンロード間隔を設定するには、グローバル コンフィギュレーション モードで **aaa route download** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

構文の説明

time	（任意）ダウンロード間隔（分単位）。 有効な範囲は 1 ～ 1440 分です。
authorization *method-list*	（任意）スタティック ルート ダウンロード用の RADIUS 許可要求が送信される名前付き方式リストを指定します。 これらの属性が設定されていない場合、すべての RADIUS 許可要求はデフォルトの方式リストで指定されたサーバに送信されます。

コマンド デフォルト

デフォルトのダウンロード（更新）間隔は 720 分です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.0(3)T	このコマンドが導入されました。
12.1	このコマンドが Cisco IOS Release 12.1 に統合されました。
12.2(8)T	**authorization** キーワードが追加されました。*method-list* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。

使用上のガイドライン

このコマンドは、ルータの名前が *hostname* の場合に、許可、認証、アカウンティング（AAA）サーバからスタティック ルートの詳細をダウンロードするために使用されます。 スタティック ルートの AAA サーバに渡される名前は *hostname-1*、*hostname-2* ～ *hostname-n* です。ルータは、インデックスが失敗し、ルートがそれ以上ダウンロードできなくなるまで、スタティック ルートをダウンロードし続けます。

例

次に、AAA ルートの更新期間を 100 分に設定する例を示します。

```
aaa route download 100
```

次に、AAA ルートの更新期間を 10 分に設定し、方式リストの名前「list1」で指定されたサーバにスタティック ルート ダウンロード要求を送信する例を示します。

```
aaa route download 10 authorization list1
```

関連コマンド

コマンド	説明
aaa authorization configuration default	TACACS+ または RADIUS を使用して AAA サーバからスタティック ルート設定情報をダウンロードします。
clear ip route download	AAA サーバからダウンロードされたスタティック ルートをクリアします。
show ip route	すべてのスタティック IP ルート、または AAA ルート ダウンロード機能を使用してインストールされたスタティック IP ルートを表示します。

aaa server radius dynamic-author

デバイスを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシーサーバとの相互作用を実行するように設定するには、グローバル コンフィギュレーション モードで **aaa server radius dynamic-author** コマンドを使用します。 このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

aaa server radius dynamic-author

no aaa server radius dynamic-author

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

デバイスは、外部ポリシー サーバとの相互作用を実行するときにサーバとして機能しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(28)SB	このコマンドが導入されました。
12.4	このコマンドが、Cisco IOS Release 12.4 に統合されました。
Cisco IOS XE Release 2.6	このコマンドが、Cisco IOS XE Release 2.6 に統合されました。
12.2(5)SXI	このコマンドが、Cisco IOS Release 12.2(5)SXI に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

動的許可は、外部ポリシーサーバがデバイスに動的に更新情報を送信できます。 **aaa server radius dynamic-author** コマンドが設定されている場合は、動的許可ローカル サーバ コンフィギュレーション モードが開始されます。 このモードでは、RADIUS アプリケーション コマンドを設定できます。

Intelligent Services Gateway（ISG）用の動的許可

ISG は、加入者別およびサービス別の情報が格納されたポリシー サーバと呼ばれる外部デバイスと連携動作します。 ISG は、ISG デバイスと外部ポリシー サーバ間の相互作用の 2 つのモデル（初期許可と動的許可）をサポートしています。

動的許可モデルでは、外部ポリシー サーバは、ISG に対して動的にポリシーを送信できます。 これらの処理は、（サービスの選択を通じて）加入者がインバンド方式で開始することも、管理者の操作を通じて開始することもできます。また、アプリケーションはアルゴリズムに基づいてポリシーを変更できます（たとえば、1 日の特定の時間に、セッションの Quality of Service（QoS）を変更します）。 このモデルは、Change of Authorization（CoA）RADIUS 拡張によって容易になります。 CoA は、RADIUS にピアツーピア機能を導入しました。これにより、ISG と外部ポリシー サーバをそれぞれ RADIUS クライアントとサーバとして機能させることができます。

例

次に、IP アドレス 10.12.12.12 のクライアントと相互作用を実行する場合に、ISG が AAA サーバとして機能するように設定する例を示します。

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

関連コマンド

コマンド	説明
auth-type（ISG）	サーバの許可タイプを指定します。
client	デバイスに CoA および切断要求を送信する RADIUS クライアントを指定します。
default	RADIUS アプリケーション コマンドをデフォルトに設定します。
domain	ユーザ名のドメイン オプションを指定します。
ignore	特定のパラメータを無視するように動作を上書きします。
port	ローカル RADIUS サーバがリッスンするポートを指定します。
server-key	RADIUS クライアントと共有する暗号キーを指定します。

access-list（IP 標準）

標準 IP アクセス リストを定義するには、グローバル コンフィギュレーション モードで **access-list** コマンドの標準バージョンを使用します。標準アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *access-list-number* {**deny**| **permit**} *source* [*source-wildcard*] [**log** [*word*]]

no access-list *access-list-number*

構文の説明

access-list-number	アクセス リスト番号。 1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数です。
deny	条件に一致する場合、アクセスを拒否します。
permit	条件が一致した場合にアクセスを許可します。
source	パケットの送信元のネットワークまたはホストの番号。送信元を指定する場合、代わりに次の 2 つの方法を使用できます。 • 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用します。
source-wildcard	（任意）送信元に適用されるワイルドカード ビット。送信元のワイルドカードを指定する場合、次の 2 つの方法を使用できます。 • 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。 無視するビット位置には 1 を入力します。 • **any** キーワードを、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* の短縮形として使用します。

log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。（コンソールに記憶されるメッセージのレベルは **logging console** コマンドで制御します）。 このログ メッセージに含まれるものには、アクセス リスト番号、パケットが許可されたか拒否されたか、送信元アドレス、パケット数、さらに、該当する場合は、ユーザ定義のクッキーまたはルータが生成したハッシュ値があります。メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で許可または拒否されたパケット数を含めて生成されます。 ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。 この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。 そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。
word	（任意）ログ メッセージに追加されるユーザ定義のクッキー。 クッキーには次の制約があります。 • 文字以外は使用できません。 • 16進表記で開始することはできません（0x など）。 • **reflect**、**fragment**、**time-range** キーワード、およびこれらのキーワードのサブセットと同じにはできません。 • 英数字以外は使用できません。 ユーザ定義のクッキーはアクセス コントロール エントリ（ACE）の syslog エントリに加えられ、syslog エントリを生成したアクセス コントロール リスト内で ACE を一意に識別します。

コマンド デフォルト

アクセス リストは、デフォルトで、すべてに対する暗黙の拒否ステートメントです。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
10.3	このコマンドが導入されました。
11.3(3)T	**log** キーワードが追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の12.2SXリリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(22)T	**log** キーワードに *word* 引数が追加されました。

使用上のガイドライン

アクセス条件を慎重に計画し、アクセス リストの末尾にある暗黙の拒否ステートメントに注意してください。

アクセス リストは、インターフェイスでのパケット送信の制御、vty アクセスの制御、ルーティング アップデートの内容の制限に使用できます。

すべてのアクセス リストの内容を表示するには、**show access-lists** EXEC コマンドを使用します。

1 つのアクセス リストの内容を表示するには、**show ip access-list** EXEC コマンドを使用します。

注意

このコマンドの拡張には下位互換性があります。Cisco IOS Release 10.3 以前のリリースからの移行ではアクセス リストが自動的に変換されます。 ただし、Release 10.3 以前のリリースでは、これらの拡張との上位互換性はありません。 そのため、アクセスリストをこれらのイメージに保存してから、Release 10.3 以前のソフトウェアを使用すると、そのアクセス リストは正しく解釈されません。 **この状態は、深刻なセキュリティ上の問題が発生する可能性があります。** これらのイメージをブートする前に、以前のコンフィギュレーション ファイルを保存してください。

例

次に、標準アクセス リストで、3 つの特定のネットワーク上のホストだけにアクセスを許可する例を示します。 ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リスト ステートメントに一致しない送信元アドレスのホストはすべて拒否されます。

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

ワイルドカードがすべてゼロの場合、ワイルドカードを省略することで、大量の個別アドレスを簡単に指定できます。 したがって、次の 2 つのコンフィギュレーション コマンドは実質的に同一です。

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

次に、標準アクセス リストで、10.29.2.64 ～ 10.29.2.127 の範囲の IP アドレスを持つデバイスにアクセスを許可する例を示します。 この範囲にない送信元アドレスを持つすべてのパケットは拒否されます。 また、ロギング メカニズムがイネーブルになり、各 syslog エントリに SampleUserValue という語句が追加されます。

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

関連コマンド

コマンド	説明
access-list	着信接続および発信接続を特定の（シスコデバイスへの）vty とアクセス リスト内のアドレスとの間に制限します。
access-list（IP 拡張）	拡張 IP アクセス リストを定義します。
access-list remark	番号付き IP アクセス リスト内のエントリに有益なコメント（注釈）を書き込みます。
deny（IP）	パケットが名前付きアクセス リストを渡さない条件を設定します。

コマンド	説明
distribute-list in（IP）	アップデートで受信するネットワークをフィルタリングします。
distribute-list out（IP）	更新でのネットワークのアドバタイズを抑制します。
ip access-group	インターフェイスへのアクセスを制御します。
ip access-list logging hash-generation	ACE syslog エントリのハッシュ値の生成をイネーブルにします。
permit（IP）	パケットが名前付きアクセスリストを渡す条件を設定します。
remark（IP）	名前付き IP アクセス リスト内のエントリに有益なコメント（注釈）を書き込みます。
show access-lists	現在の IP およびレート制限アクセス リストの内容を表示します。
show ip access-list	現在のすべての IP アクセス リストの内容を表示します。

address ipv6（config-radius-server）

RADIUS サーバのアカウンティングおよび認証パラメータの IPv6 アドレスを設定するには、RADIUS サーバ コンフィギュレーション モードで **address ipv6** コマンドを使用します。 指定した RADIUS サーバのアカウンティングおよび認証パラメータを削除するには、このコマンドの **no** 形式を使用します。

address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

no address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

構文の説明

hostname	RADIUS サーバ ホストのドメイン ネーム システム（DNS）名。
ipv6address	RADIUS サーバの IPv6 アドレス。
acct-port *port*	（任意）アカウンティング要求の RADIUS アカウンティング サーバにユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトのポートは 1646 です。
alias {*hostname* | *ipv6address*}	（任意）このサーバにエイリアスを指定します。 エイリアスは IPv6 アドレスまたはホスト名を指定できます。エイリアスはこのサーバに 8 つまで設定できます。
auth-port *port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。デフォルトのポートは 1645 です。

コマンド デフォルト

RADIUS サーバのアカウンティングおよび認証パラメータは設定されていません。

コマンド モード

RADIUS サーバ コンフィギュレーション（config-radius-server）

コマンド履歴

リリース	変更内容
15.2(2)T	このコマンドが導入されました。

使用上のガイドライン

このコマンドにアクセスする前に、**aaa new-model** コマンドを設定する必要があります。

Cisco TrustSec（CTS）機能は、Secure RADIUS を使用して、認証、許可、セッション アソシエーション、暗号化、およびトラフィック フィルタリングの処理を規定します。

エイリアスを RADIUS サーバに設定する前に、サーバの IPv6 アドレスまたは DNS 名を設定する必要があります。 これは、**address ipv6** コマンドおよび *hostname* 引数を使用して行います。 その後、**address ipv6** コマンド、**alias** キーワードおよび *hostname* 引数を使用してエイリアスを設定できます。

例

次に、RADIUS サーバのアカウンティングおよび認証パラメータを設定する例を示します。

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812
```

関連コマンド

コマンド	説明
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
address ipv4	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
radius server	RADIUS サーバ コンフィギュレーションの名前を指定し、RADIUS サーバ コンフィギュレーション モードを開始します。

address ipv6（TACACS+）

TACACS+ サーバの IPv6 アドレスを設定するには、TACACS+ サーバ コンフィギュレーション モードで **address ipv6** コマンドを使用します。 IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

address ipv6 *ipv6-address*

no address ipv6 *ipv6-address*

構文の説明

ipv6-address	秘密 TACACS+ サーバ ホスト。

コマンド デフォルト

TACACS+ サーバは設定されていません。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

tacacs server コマンドを使用して TACACS+ サーバをイネーブルにした後で、address ipv6（TACACS+）コマンドを使用します。

例

次に、server1 という名前の TACACS+ サーバの IPv6 アドレスを指定する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。

address ipv6（TACACS+）

authentication command bounce-port ignore ～ auth-type

authentication command bounce-port ignore

ルータが RADIUS 許可変更（CoA）bounce port コマンドを無視するように設定するには、グローバル コンフィギュレーション モードで **authentication command bounce-port ignore** コマンドを使用します。 デフォルト ステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command bounce-port ignore

no authentication command bounce-port ignore

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

ルータが RADIUS CoA bounce port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが導入されました。
12.2(33)SXI4	このコマンドが、Cisco IOS Release 12.2(33)SXI4 に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

RADIUS CoA bounce port コマンドが RADIUS サーバから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）の再ネゴシエーションが開始されます。 この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。

authentication command bounce-port ignore コマンドは、ルータが RADIUS CoA bounce port コマンドを無視し、認証ポートに接続されているホストのリンク フラップの発生を防ぐように設定します。

例

次に、ルータが RADIUS CoA bounce port コマンドを無視するように設定する例を示します。

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

関連コマンド

コマンド	説明
authentication command disable-port ignore	ルータが RADIUS サーバの CoA **disable port** コマンドを無視するように設定します。

authentication command disable-port ignore

ルータがRADIUSサーバの許可変更（CoA）disable portコマンドを無視するように設定するには、グローバル コンフィギュレーション モードで **authentication command disable-port ignore** コマンドを使用します。 デフォルト ステータスに戻すには、このコマンドの **no** 形式を使用します。

authentication command disable-port ignore

no authentication command disable-port ignore

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

ルータが RADIUS CoA disable port コマンドを受け入れます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(52)SE	このコマンドが導入されました。
12.2(33)SXI4	このコマンドが、Cisco IOS Release 12.2(33)SXI4に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)Tに統合されました。

使用上のガイドライン

RADIUS サーバの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。 ルータが RADIUS サーバの CoA disable port コマンドを無視し、この認証ポートの認証ポートおよびその他のホストが切断されないように設定するには、**authentication command disable-port ignore** コマンドを使用します。

例

次に、ルータが CoA **disable port** コマンドを無視するように設定する例を示します。

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

関連コマンド

コマンド	説明
authentication command bounce-port ignore	ルータが RADIUS サーバの CoA bounce port コマンドを無視するように設定します。

authentication control-direction

ポートの認証制御の方向を設定するには、インターフェイス コンフィギュレーション モードで **authentication control-direction** 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。

authentication control-direction {**both**| **in**}

no authentication control-direction

構文の説明

both	ポートで双方向制御をイネーブルにします。
in	ポートで単方向制御をイネーブルにします。

コマンド デフォルト

ポートは双方向モードに設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

IEEE 802.1x 標準は、nonauthenticated クライアントとネットワーク リソース間のトラフィックをブロックするために実装されます。 これは、nonauthenticated クライアントがオーセンティケータ以外のネットワーク上のデバイスと通信できないことを意味します。 リバースは true です。ただし、ポートが単方向制御ポートとして設定されている場合を除きます。

単方向ステート

IEEE 802.1x 標準は、ネットワーク上のデバイスがクライアントを「起動」してクライアントが再認証され続けるように、単方向制御ポートを定義します。 **authentication control-direction in** コマンドを使用してポートを単方向に設定すると、ポートはスパニングツリー フォワーディング ステートに変更され、ネットワーク上のデバイスがクライアントを起動して強制的に再認証を行わせることが許可されます。

双方向ステート

authentication control-direction both コマンドを使用してポートを双方向に設定すると、ポートへのアクセスが両方向で制御されます。 この場合、ポートはパケットを送受信しません。

例

次の例では、単方向制御をイネーブルにする方法を示します。

```
Switch(config-if)# authentication control-direction in
```

次に、双方向制御をイネーブルにする例を示します。

```
Switch(config-if)# authentication control-direction both
```

authentication event fail

ユーザ クレデンシャルが認識されないときの認証エラーを Auth Manager が処理する方法を指定するには、インターフェイス コンフィギュレーション モードで **authentication event fail** 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。

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id*| **next-method**}

no authentication event fail

構文の説明

retry *retry-count*	（任意）認証が最初に失敗した後に試行される認証方式の回数を指定します。
action	不正なユーザ クレデンシャルによって認証が失敗した後に実行するアクションを指定します。
authorize vlan *vlan-id*	認証の試行が失敗した後に、ポートの制限付き VLAN を許可します。
next-method	認証の試行が失敗した後に呼び出される次の認証方式を指定します。 認証方式の順序は、**authentication order** コマンドによって指定されます。

コマンド デフォルト

認証は最初の試行が失敗した後に 2 回試行されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

dot1x 認証方式だけが、この認証失敗のタイプをシグナリングできます。

例

次に、認証試行に 3 回失敗した後、ポートが制限付き VLAN に割り当てられるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event fail retry 3 action authorize vlan 40

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event no-response action	ホストが応答しないことにより認証が失敗した場合に実行するアクションを指定します。
authentication order	試行する認証方式の順序を指定します。

authentication event server alive action reinitialize

以前は到達不能だった認証、許可、アカウンティング（AAA）サーバが使用可能になった場合に、許可された Auth Manager セッションを再初期化するには、インターフェイス コンフィギュレーション モードで **authentication event server alive action reinitialize** 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。

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

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

セッションは再初期化されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

以前は到達不能だった AAA サーバが使用可能になった場合は、**authentication event server alive action reinitialize** コマンドを使用して、許可されたセッションを再初期化します。

例

次に、以前は到達不能だったAAAサーバが使用可能になった場合に、許可されたセッションが再初期化されるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event server dead action authorize	AAA サーバが到達不能の場合に、許可されたセッションの処理方法を指定します。

authentication event server dead action authorize

認証、許可、アカウンティング（AAA）サーバが到達不能になった場合にAuth Managerセッションを許可するには、インターフェイス コンフィギュレーション モードで **authentication event server dead action authorize** 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。

authentication event server dead action authorize vlan *vlan-id*

no authentication event server dead action authorize

構文の説明

vlan *vlan-id*	認証の試行が失敗した後に、ポートの制限付きVLAN を許可します。

コマンド デフォルト

セッションは許可されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。

使用上のガイドライン

AAA サーバが使用できない場合でも、**authentication event server dead action authorize** コマンドを使用してセッションを許可できます。

例

次に、AAAサーバが到達不能になった場合に、ポートがVLANに割り当てられるように指定する例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication event server alive action reinitialize	以前は到達不能だった AAA サーバが使用可能になったときに、許可されたセッションを再初期化します。

authentication fallback

Web 認証フォールバック方式をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication fallback** コマンドを使用します。 Web 認証フォールバック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。

authentication fallback *fallback-profile*

no authentication fallback

構文の説明

fallback-profile	Web 認証フォールバック プロファイルの名前。

コマンド デフォルト

Web 認証フォールバックはイネーブルではありません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

Web 認証フォールバック プロファイルを指定するには、**authentication fallback** コマンドを使用します。 プロファイルの詳細を指定するには、**fallback profile** コマンドを使用します。

例

次に、ポートにフォールバック プロファイルを指定する例を示します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

関連コマンド

コマンド	説明
fallback profile	Web 認証のプロファイルを指定します。

authentication host-mode

ホストの制御ポートへのアクセスを許可するには、インターフェイス コンフィギュレーション モードで**authentication host-mode** 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。

authentication host-mode {**single-host**| **multi-auth**| **multi-domain**| **multi-host**} **[open]**

no authentication host-mode

構文の説明

single-host	常に 1 つのクライアントだけがポートで認証できるように指定します。複数のクライアントが検出された場合、セキュリティ違反が発生します。
multi-auth	常に複数のクライアントがポートで認証できるように指定します。
multi-domain	ドメイン（DATA または VOICE）ごとに、一度に 1 つのクライアントだけが認証できるように指定します。
multi-host	最初のクライアントが認証されると、それ以降のすべてのクライアントのアクセスが許可されるように指定します。
open	（任意）ポートが開くように指定します。つまり、アクセス制限はありません。

コマンド デフォルト

ポートへのアクセスは許可されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

このコマンドを使用する前に、**authentication port-control** コマンドをキーワード **auto** で使用する必要があります。

multi-host モードでは、すべてのホストのネットワーク アクセスが許可されるように、接続されたホストのうち 1 つだけが正常に許可される必要があります。 ポートが無許可ステートになった場合（再認証が失敗した場合、または Extensible Authentication Protocol over LAN（EAPOL）-Logoff メッセージを受信した場合）は、接続されたすべてのクライアントがネットワーク アクセスを拒否されます。

例

次に、**multi-host** モードで認証をイネーブルにする例を示します。

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

関連コマンド

コマンド	説明
authentication port-control	インターフェイスに関する情報を表示します。

authentication open

このポートでオープン アクセスをイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication open** コマンドを使用します。 このポートでオープン アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication open

no authentication open

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

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドがサポートされるようになりました。

使用上のガイドライン

オープン アクセスを使用すると、認証の実行前にクライアントまたはデバイスがネットワークにアクセスできます。

show authentication 特権 EXEC コマンドを入力することにより、設定を確認できます。

このコマンドは、ポートに対してのみ **authentication host-mode** *session-type* **open** グローバル コンフィギュレーション コマンドよりも優先されます。

例

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Router(config-if)# authentication open
Router(config-if)#
```

次の例では、ポートに対してオープン アクセスをイネーブルにする方法を示します。

```
Router(config-if)# no authentication open
Router(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。

authentication order

ポートで Auth Manager がクライアントの認証を試行する順序を指定するには、インターフェイス コンフィギュレーション モードで **authentication order** コマンドを使用します。 デフォルトの認証順序に戻すには、このコマンドの **no** 形式を使用します。

authentication order {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication order

構文の説明

dot1x	IEEE 802.1X 認証を指定します。
mab	MAC ベースの認証（MAB）を指定します。
webauth	Web ベースの認証を指定します。

コマンド デフォルト

デフォルトの認証順序は **dot1x**、**mab**、および **webauth** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

authentication order コマンドを使用して、実行する認証方式を明示的に指定し、その実行する順序を指定します。 各方式は一度だけリストに入力できます。**webauth** の後に方式をリストすることはできません。

例

次に、ポートに認証順序を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1
```

```
Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

関連コマンド

コマンド	説明
authentication priority	ポートでの認証方式のプライオリティを指定します。

authentication periodic

ポートの自動再認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **authentication periodic** コマンドを使用します。 ディセーブルにするには、このコマンドの **no** 形式を使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**dot1x reauthentication** コマンドが、**authentication periodic** コマンドに置き換えられました。

authentication periodic

no authentication periodic

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

再認証はディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポートの自動再認証をイネーブルにするには、**authentication periodic** コマンドを使用します。 再認証の試行間隔を設定するには、**authentication timer reauthenticate** コマンドを使用します。

例

次に、再認証をイネーブルにし、試行間隔を 1800 秒に設定する例を示します。

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 1800
```

関連コマンド

コマンド	説明
authentication timer reauthenticate	許可ポートの再認証の試行間隔を指定します。

authentication port-control

制御ポートの許可ステートを設定するには、インターフェイスコンフィギュレーションモードで **authentication port-control** コマンドを使用します。 ポート制御値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。

（注） Cisco IOS Release 12.2(33)SXI から、**dot1x port-control** コマンドが、**authentication port-control** コマンドに置き換えられました。

authentication port-control {**auto**| **force-authorized**| **force-unauthorized**}

no authentication port-control

構文の説明

auto	ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのは Extensible Authentication Protocol over LAN（EAPOL）フレームだけです。
force-authorized	インターフェイスの IEEE 802.1X をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。**force-authorized** キーワードはデフォルトです。
force-unauthorized	クライアントからの認証試行をすべて無視し、ポートを強制的に無許可ステートに変更して、このインターフェイス経由のすべてのアクセスを拒否します。

コマンド デフォルト

ポートは認証情報の交換なしで許可されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポート制御の設定を確認するには、**show interfaces** コマンドを使用するか、ディスプレイの 802.1X Port Summary セクションの Status カラムを確認します。 enabled ステータスは、ポート制御値が auto または force-unauthorized に設定されていることを意味します。

ポートのリンク ステートがダウンからアップに移行するか、または EAPOL-Start フレームを受信すると、認証プロセスが開始されます。 システムはクライアントの識別情報を要求して、クライアントと認証サーバ間で認証メッセージのリレーを開始します。

例

次に、クライアントの許可ステータスが認証プロセスによって決定されるように指定するコマンドの例を示します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ethernet0/2

Router(config-if)# authentication port-control auto
```

関連コマンド

コマンド	説明
show interfaces	制御ポートの許可ステートを設定します。

authentication priority

ポートで認証方式のプライオリティを指定するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。 デフォルトに戻るには、**no** 形式のコマンドを使用します。

authentication priority {**dot1x** [**mab**| **webauth**] [**webauth**]| **mab** [**dot1x**| **webauth**] [**webauth**]| **webauth**}

no authentication priority

構文の説明

dot1x	IEEE 802.1X 認証を指定します。
mab	MAC ベースの認証を指定します。
webauth	Web ベースの認証を指定します。

コマンド デフォルト

デフォルトのプライオリティ順は **dot1x**、**mab**、および **webauth** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

authentication order コマンドは、認証方式を試行する順序を指定します。 これはデフォルトのプライオリティ順です。 デフォルトのプライオリティを上書きし、高いプライオリティの方式が認証方式の実行に割り込むことを許可するには、**authentication priority** コマンドを使用します。

例

次に、ポートで認証順序と認証のプライオリティの設定に使用するコマンドの例を示します。

```
Router# configure terminal
Router(config)# interface fastethernet0/1
```

```
Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

関連コマンド

コマンド	説明
authentication order	ポートでAuth Managerがクライアントの認証を試行する順序を指定します。

authentication timer inactivity

非アクティブな Auth Manager セッションが終了するまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **authentication timer inactivity** コマンドを使用します。 非アクティビティ タイマ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。

authentication timer inactivity {*seconds*| **server**}

no authentication timer inactivity

構文の説明

seconds	Auth Manager セッションが終了してポートが無許可になる前に許可される非アクティビティ期間（秒単位）。 有効な範囲は 1 ～ 65535 です。
server	非アクティビティ期間が認証、許可、アカウンティング（AAA）サーバのアイドル タイムアウト値（RADIUS 属性 28）によって定義されるように指定します。

コマンド デフォルト

非アクティビティ タイマーはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

非アクティブ セッションの再認証を回避するには、**authentication timer inactivity** コマンドを使用して、非アクティビティ タイマーを、**authentication timer reauthenticate** コマンドで設定された再認証間隔よりも短い間隔に設定します。

例

次に、ポートの非アクティビティ間隔を 900 秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

関連コマンド

コマンド	説明
configuration timer reauthenticate	Auth Manager が、許可ポートの再認証の試行を開始するまでの時間を指定します。
authentication timer restart	Auth Manager が無許可ポートの認証の試行を開始するまでの間隔を指定します。

authentication timer reauthenticate

Auth Manager が許可ポートの再認証を試行する間隔を指定するには、インターフェイス コンフィギュレーション モードで **authentication timer reauthenticate** コマンドを使用します。 再認証間隔をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

authentication timer reauthenticate {*seconds*| **server**}

no authentication timer reauthenticate

構文の説明

seconds	再認証間隔（秒単位）。 デフォルト値は 3600 です。
server	再認証の試行間隔が、認証、許可、アカウンティング（AAA）サーバのセッション タイムアウト値（RADIUS 属性 27）で定義されるように指定します。

コマンド デフォルト

自動再認証間隔は 3600 秒に設定されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

許可ポートの自動再認証間隔を設定するには、**authentication timer reauthenticate** コマンドを使用します。 **authentication timer inactivity** コマンドを使用して非アクティビティ間隔を設定する場合は、再認証間隔を非アクティビティ間隔よりも長く設定します。

例

次に、ポートの再認証間隔を 1800 秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer reauthenticate 1800

Switch(config-if)# end
```

関連コマンド

コマンド	説明
authentication periodic	自動再認証をイネーブルにします。
authentication timer inactivity	Auth Manager が非アクティブ セッションを終了するまでの間隔を指定します。
authentication timer restart	Auth Manager が無許可ポートの認証の試行を開始するまでの間隔を指定します。

authentication timer restart

Auth Manager が無許可ポートの認証の試行を開始するまでの期間を指定するには、インターフェイス コンフィギュレーション モードで **authentication timer restart** コマンドを使用します。 間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

authentication timer restart *seconds*

no authentication timer restart

構文の説明

seconds	無許可ポートの認証試行間隔（秒単位）。 指定できる範囲は 1 ～ 65535 です。 デフォルトは 60 です。

コマンド デフォルト

無許可ポートの認証の試行は行われません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

無許可ポートの認証試行間隔を指定するには、**authentication timer restart** コマンドを使用します。 デフォルト インターバルは 60 秒です。

例

次に、認証タイマーの間隔を 120 秒に設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

関連コマンド

コマンド	説明
authentication timer inactivity	Auth Manager が無許可ポートの認証の試行を開始するまでの期間を指定します。
configuration timer reauthenticate	Auth Manager が、許可ポートの再認証の試行を開始するまでの時間を指定します。

authentication violation

ポートでセキュリティ違反が発生したときに実行するアクションを指定するには、インターフェイス コンフィギュレーション モードで **authentication violation** コマンドを使用します。 デフォルトのアクションに戻すには、このコマンドの **no** 形式を使用します。

authentication violation {**restrict**| **shutdown**}

no authentication violation

構文の説明

restrict	セキュリティ違反が発生したドメインに対してポートがトラフィックを制限するように指定します。
shutdown	セキュリティ違反に対してポートがシャットダウンするように指定します。

コマンド デフォルト

セキュリティ違反が発生すると、ポートはシャット ダウンします。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI	このコマンドが導入されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。

使用上のガイドライン

ポートでセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

例

次に、セキュリティ違反が発生したときに GigabitEthernet インターフェイスがトラフィックを制限するように設定する例を示します。

```
Switch(config)# interface GigabitEthernet6/2
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

auth-type

動的に認証または認証解除されるデバイスにポリシーを設定するには、アイデンティティ プロファイル コンフィギュレーション モードで **auth-type** コマンドを使用します。 指定されたポリシーを削除するには、このコマンドの **no** 形式を使用します。

auth-type {**authorize| not-authorize**} **policy** *policy-name*

no auth-type {**authorize| not-authorize**} **policy** *policy-name*

構文の説明

authorize	ポリシーは、すべての許可済みデバイスに指定されます。
not-authorize	ポリシーは、すべての許可されていないデバイスに指定されます。
policy *policy-name*	アイデンティティ ポリシー名が、関連付けられた認証結果に適用されるように指定します。

コマンド デフォルト

ポリシーは、許可済みまたは許可されていないデバイスには設定されません。

コマンド モード

アイデンティティ プロファイルの設定

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

このコマンドは、ネットワーク アクセス デバイスによってデバイスが動的に認証または認証解除される場合、およびデバイスにその認証結果に適用する必要があるポリシーの名前が必要である場合に使用されます。

例

次に、すべての動的に認証されたホストに対してアイデンティティ ポリシー「grant」に802.1x認証を適用する例を示します。

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを作成します。
identity profile dot1x	802.1xアイデンティティ プロファイルを作成します。

clear dot1x ～ clear eap

clear dot1x

802.1X インターフェイス情報をクリアするには、特権 EXEC モードで **clear dot1x** コマンドを使用します。

clear dot1x {**all**| **interface interface-name**}

構文の説明

all	すべてのインターフェイスの 802.1X 情報をクリアします。
interface interface-name	指定したインターフェイスの 802.1X 情報をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(25)SEE	このコマンドが、Cisco IOS Release 12.2(25)SEE に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

例

次の設定は、すべてのインターフェイスで 802.1X 情報がクリアされることを示します。

```
Router# clear dot1x all
```

次の設定は、イーサネット 0 インターフェイスで 802.1X 情報がクリアされることを示します。

```
Router# clear dot1x interface ethernet 0
```

show dot1x コマンドを入力して、情報が削除されたことを確認することができます。

関連コマンド

コマンド	説明
debug dot1x	802.1X デバッグ情報を表示します。
identity profile default	アイデンティティ プロファイルを作成し、アイデンティティ プロファイル コンフィギュレーション モードを開始します。
show dot1x	アイデンティティ プロファイルの詳細を表示します。

clear eap

スイッチまたは指定されたポートの拡張認証プロトコル（EAP）情報を削除するには、特権EXECモードで **clear eap** コマンドを使用します。

clear eap [**sessions** [**credentials** *credentials-name*| **interface** *interface-name*| **method** *method-name*| **transport** *transport-name*]]

構文の説明

sessions	（任意）スイッチまたは指定されたポートのEAP セッションをクリアします。
credentials *credentials-name*	（任意）指定されたプロファイルの EAP クレデンシャル情報だけをクリアします。
interface *interface-name*	（任意）指定されたインターフェイスの EAP クレデンシャル情報だけをクリアします。
method *method-name*	（任意）指定された方式の EAP クレデンシャル情報だけをクリアします。
transport *transport-name*	（任意）指定された下位レイヤの EAP クレデンシャル情報だけをクリアします。

コマンド デフォルト

すべてのアクティブな EAP セッションがクリアされます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(25)SEE	このコマンドが導入されました。
12.4(6)T	このコマンドが、Cisco IOS Release 12.4(6)T に統合されました。

使用上のガイドライン

clear eap コマンドを **session** キーワードで使用して、すべてのカウンタをクリアできます。また、**credentials**、**interface**、**method**、または **transport** キーワードを使用して、指定された情報だけをクリアすることもできます。

例

次に、EAP 情報をクリアする例を示します。

```
Router# clear eap sessions
```

次に、指定されたプロファイルの EAP セッション情報をクリアする例を示します。

```
Router# clear eap sessions credentials type1
```

関連コマンド

コマンド	説明
show eap registrations	EAP 登録情報を表示します。
show eap sessions	アクティブな EAP セッション情報を表示します。

client ～ crl

client

デバイスに許可変更（CoA）および切断要求を送信する RADIUS クライアントを指定するには、動的許可ローカル サーバ コンフィギュレーション モードで **client** コマンドを使用します。 こ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。

client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

no client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

構文の説明

name	RADIUS クライアントのホスト名。
ip-address	RADIUS クライアントの IP アドレス。
key	（任意）デバイスと RADIUS クライアントの間で共有される RADIUS キーを設定します。
0	（任意）暗号化されていないキーが後ろに続くように指定します。
7	（任意）暗号化されたキーが後ろに続くように指定します。
word	（任意）暗号化されていないサーバ キー
vrf *vrf-id*	（任意）クライアントの仮想ルーティングおよびフォワーディング（VRF）ID。

コマンド デフォルト

CoA および切断要求はドロップされます。

コマンド モード

動的許可ローカル サーバ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(28)SB	このコマンドが導入されました。
Cisco IOS XE Release 2.6	このコマンドが、Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

デバイス（ルータなど）は、外部ポリシー サーバがルータに動的に更新を送信できるように設定できます。 この機能は、CoA RADIUS 拡張によって容易になります。 CoA は、RADIUS にピアツーピア機能を導入しました。これにより、ルータと外部ポリシー サーバをそれぞれ RADIUS クライアントとサーバとして機能させることができます。 **client** コマンドを使用して、ルータがサーバとして機能する RADIUS クライアントを指定します。

例

次に、ルータが、IP アドレス 10.0.0.1 の RADIUS クライアントから要求を受け入れるように設定する例を示します。

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

関連コマンド

コマンド	説明
aaa server radius dynamic-author	外部ポリシー サーバとの相互作用が容易になるように、ISG を AAA サーバとして設定します。

crl

公開キー インフラストラクチャ（PKI）トラストプールの証明書失効リスト（CRL）クエリーおよび CRL キャッシュ オプションを指定するには、ca-trustpool コンフィギュレーション モードで **crl** コマンドを使用します。 デフォルトの動作に戻し、証明書に埋め込まれている URL をルータが確認するようにするには、このコマンドの **no** 形式を使用します。

crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

no crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

構文の説明

cache	CRL キャッシュ オプションを指定します。
delete-after	タイムアウト後にキャッシュから CRL を削除します。
minutes	キャッシュから CRL を削除する前に待機する時間を分単位で指定します。範囲は 1 ～ 43200 分です。
none	CRLがキャッシュされないように指定します。
query *url*	CRL をクエリーするために認証局（CA）サーバによって発行される URL を指定します。

コマンド デフォルト

CRL はクエリーされません。CRL キャッシュ パラメータは設定されていません。

コマンド モード

ca-trustpool コンフィギュレーション（ca-trustpool）

コマンド履歴

リリース	変更内容
15.2(2)T	このコマンドが導入されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

このコマンドを設定する前に、**crypto pki trustpool policy** コマンドをイネーブルにして ca-trustpool コンフィギュレーション モードを開始する必要があります。

crl query コマンドは、CDP が Lightweight Directory Access Protocol（LDAP）形式の場合に使用されます。これは、証明書内の CDP の場所が、ディレクトリ内の CRL 分散ポイント（CDP）が置かれている場所だけを示すことを意味します。つまり、CDP は実際のクエリーの場所を示しません。

Cisco IOS ソフトウェアでは、ピア証明書を確認するために証明書が取り消されないように CRL をクエリーします（たとえば、インターネット キー交換（IKE）または Secure Sockets Layer（SSL）ハンドシェイク中に）。 クエリーは、CRL のダウンロードに使用される証明書の CDP 拡張を探します。 このクエリーが失敗した場合は、CA サーバから直接 CRL をクエリーするために Simple Certificate Enrollment Protocol（SCEP）GetCRL メカニズムが使用されます（一部の CA サーバはこの方式をサポートしていません）。

Cisco IOS ソフトウェアは、次の CDP エントリをサポートしています。

- HTTP URL + ホスト名 （例：http://myurlname/myca.crl）。
- HTTP URL + IPv4 アドレス （例：http://10.10.10.10:81/myca.crl）。
- LDAP URL + ホスト名 （例：ldap://CN=myca、O=cisco）。
- LDAP URL + IPv4 アドレス （例：ldap://10.10.10.10:3899/CN=myca、O=cisco）。
- LDAP/X.500 DN （例：CN=myca、O=cisco）。

Cisco IOS には、CDP を検索するための完全な URL が必要です。

例

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

関連コマンド

コマンド	説明
cabundle url	PKI トラストプール CA バンドルをダウンロードする URL を設定します。
chain-validation	PKI トラストプールの、ピアの証明書からルート CA 証明書までのチェーン バリデーションをイネーブルにします。

コマンド	説明
crypto pki trustpool import	CA 証明書バンドルを PKI トラストプールに手動でインポート（ダウンロード）し、既存の CA バンドルを更新または置換します。
crypto pki trustpool policy	PKI トラストプールのポリシーパラメータを設定します。
default	ca-trustpool コンフィギュレーション コマンドの値をデフォルトにリセットします。
match	PKI トラストプールの証明書マップの使用をイネーブルにします。
ocsp	PKI トラストプールの OCSP 設定を指定します。
revocation-check	PKI トラストプール ポリシーが使用される場合の失効チェックをディセーブルにします。
show	ルータの PKI トラストプール ポリシーを ca-trustpool コンフィギュレーション モードで表示します。
show crypto pki trustpool	PKI トラストプールの CRL 取得、OCSP ステータス、または CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。
source interface	PKI トラストプールの CRL 取得、OCSP ステータス、または CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。
storage	ルータ上の、PKI トラストプール証明書が保存されるファイルシステムの場所を指定します。

コマンド	説明
vrf	CRL 取得に使用する VRF インスタンスを指定します。

crypto ca authenticate ～ crypto ca trustpoint

crypto ca aunticate

（注） Cisco IOS Release 12.3(7)T および 12.2(18)SXE から、このコマンドが **crypto pki authenticate** コマンドに置き換えられました。

（CA の証明書を取得することによって）認証局を認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。

crypto ca authenticate *name*

構文の説明

name	CA 名を指定します。 これは、**crypto ca identity** コマンドを使用して CA を宣言した際と同じ名前を指定します。

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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3 T	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ルータで最初に CA サポートを設定する場合に必要です。

このコマンドは、CA の公開キーを含む CA の自己署名証明書を取得することで、ルータに対して CA を認証します。 CA では、証明書が自己署名されるため、このコマンドを実行するときは、CA 管理者に問い合わせて、CA の公開キーを手作業で認証する必要があります。

RA モードを使用する場合（**enrollment mode ra** コマンドを使用する場合）は、**crypto ca authenticate** コマンドを発行すると、登録局の署名と暗号化証明書が CA と CA 証明書から返されます。

このコマンドはルータ コンフィギュレーションに保存されません。 ただし、受信した CA（および RA）証明書に埋め込まれている公開キーについては、RSA 公開キー レコード（「RSA 公開キー チェーン」と呼ばれます）の一部としてコンフィギュレーションに保存されます。

このコマンドを発行した後で CA がタイムアウト期間内に応答しない場合は、このコマンドが停滞しないように端末制御が返されます。 これが発生した場合、コマンドを再入力する必要があります。 Cisco IOS ソフトウェアは、西暦 2049 年より後に設定された CA 証明書の有効期限を認識しません。 CA 証明書の有効期限が西暦 2049 年より後に期限切れになるように設定すると、CA サーバの認証の試行時に次のエラー メッセージが表示されます。

error retrieving certificate :incomplete chain

これと同様のエラー メッセージを受け取った場合は CA 証明書の有効期限を確認してください。 CA 証明書の有効期限が西暦 2049 年より後に設定されている場合は、有効期限を西暦 2049 年より前に設定し直す必要があります。

例

次に、ルータが CA の証明書を要求する例を示します。 CA は証明書を送信し、ルータは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。 CA 管理者は、CA 証明書のフィンガープリントを表示することもできるので、CA 管理者が実際に見ているものと、ルータの画面に表示されるものとを比較する必要があります。 ルータの画面のフィンガープリントと、CA 管理者が表示するフィンガープリントが一致した場合、証明書は有効です。

```
Router(config)#
crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
```

関連コマンド

コマンド	説明
debug crypto pki transactions	CA とルータ間の相互作用（メッセージ タイプ）のトレースのデバッグ メッセージを表示します。
show crypto pki certificates	証明書、CA の証明書、および RA 証明書に関する情報を表示します。

crypto ca enroll

（注） Cisco IOS Release 12.3(7)T および 12.2(18)SXE から、このコマンドが **crypto pki enroll** コマンドに置き換えられました。

認証局からルータの証明書を取得するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。 現在の登録要求を削除するには、このコマンドの **no** 形式を使用します。

crypto ca enroll *name*

no crypto ca enroll *name*

構文の説明

name	CA 名を指定します。 **crypto pki trustpoint** コマンドを使用して CA を宣言したときと同じ名前を使用します。

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

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3 T	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべてのルータの RSA キー ペアに対して CA からの証明書を要求します。 このタスクは、CA を使用した登録とも呼ばれます。 （理論的には、証明書の登録と取得は 2 つの別々のイベントですが、このコマンドが発行される際はこれらの両方が発生します）。

ルータは、ルータ上の各 RSA キー ペアに対して CA からの署名付き証明書が必要です。以前に汎用キーを作成している場合、このコマンドにより、1 組の汎用 RSA キー ペアに対応する 1 つの証明書が取得されます。 特殊用途キーを以前に作成している場合、このコマンドにより、この特殊用途の RSA キー ペアそれぞれに対応する 2 つの証明書が取得されます。

キーに対する証明書をすでに持っている場合は、このコマンドを完了できません。代わりに、まず既存の証明書の削除を求めるプロンプトが表示されます（**no certificate** コマンドで既存の証明書を削除できます）。

crypto ca enroll コマンドは、ルータ コンフィギュレーションには保存されません。

（注） **crypto ca enroll** コマンドを発行した後、証明書を受信する前にルータがリブートした場合は、コマンドを再発行する必要があります。

プロンプトへの応答

crypto ca enroll コマンドを発行すると、次の作業を求められます。

まず、チャレンジ パスワードを作成するように求められます。 このパスワードの長さは最大 80 文字です。 このパスワードは、ルータの証明書を取り消す場合に必要です。 CA 管理者に証明書を無効にするよう依頼する場合は、不正なまたは誤った失効要求からの保護としてこのチャレンジ パスワードを入力する必要があります。

（注） このパスワードはどこにも保存されないため、覚えておく必要があります。

パスワードを忘れた場合は、CA 管理者によってルータの証明書を取り消すことができる場合がありますが、ルータの管理者 ID の手動による認証が必要になる場合もあります。

また、取得した証明書にルータのシリアル番号を含めるかどうかを指示するように求められます。シリアル番号は IP セキュリティまたはインターネット キー交換には使用されませんが、CA によって証明書の認証または後で特定のルータに証明書を関連付けるために使用される場合があります（保存されるシリアル番号は、本体ケースではなく内部ボードのシリアル番号であることに注意してください）。シリアル番号を含める必要があるかどうかを CA 管理者に問い合わせてください。 不明な場合は、シリアル番号を含めてください。

通常、IP アドレスは含めません。これは、IP アドレスが特定のエンティティに証明書をより厳密にバインドするためです。 また、ルータが移動すると、新しい証明書を発行する必要があります。 最後に、ルータには複数の IP アドレスがありますが、いずれも IPSec で使用されることはありません。

IP アドレスを含めることが必要であることを示す場合、IP アドレスのインターフェイスを指定するように求められます。 このインターフェイスは、クリプト マップ セットを適用するインターフェイスに対応している必要があります。 複数のインターフェイスにクリプト マップ セットを適用する場合は、**crypto map local-address** コマンドで指定するインターフェイスを指定します。

例

次に、汎用 RSA キー ペアを持つルータが CA からの証明書を要求する例を示します。 ルータが証明書フィンガープリントを表示する場合、管理者は、番号を検査する CA 管理者に問い合わせてこの番号を確認します。 フィンガープリントが正しければ、ルータ管理者は証明書を受け入れます。

ルータ管理者が要求を送信してから、証明書がルータによって実際に届くまで遅延が発生する場合があります。 遅延の量はCAの動作方法によって異なります。

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

その後、ルータがCAから証明書を受け取ると、次の確認メッセージが表示されます。

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

必要に応じて、ルータ管理者はCA管理者とともに表示されたフィンガープリントを確認できます。

証明書要求に問題があり、証明書が許可されない場合、代わりに次のメッセージがコンソールに表示されます:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

証明書のサブジェクト名は、RSAキー ペアの名前と同じになるように自動的に割り当てられます。 上記の例では、RSAキー ペアの名前が「myrouter.example.com.」（ルータが割り当てた名前）になっています。

特殊用途キーを持つルータの証明書を要求する場合は、上記の例と同じですが、CAによって2つの証明書が返されることもあります。 ルータが2つの証明書を受け取る場合は、同じ確認メッセージを表示します。

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

関連コマンド

コマンド	説明
debug crypto pki messages	CAとルータ間の相互作用（メッセージ ダンプ）の詳細のデバッグ メッセージを表示します。
debug crypto pki transactions	CAとルータ間の相互作用（メッセージ タイプ）のトレースのデバッグ メッセージを表示します。

コマンド	説明
show crypto pki certificates	証明書、CA の証明書、および RA 証明書に関する情報を表示します。

crypto ca trustpoint

（注） Cisco IOS Release 12.3(8)T、12.2(18)SXD、および 12.2(18)SXE から、**crypto ca trustpoint** コマンドが **crypto pki trustpoint** コマンドに置き換えられました。 詳細については、**crypto pki trustpoint** コマンドを参照してください。

ルータが使用する認証局（CA）を宣言するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。 CA に関連するすべての ID 情報および証明書を削除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

構文の説明

name	CA の名前を作成します （以前に CA を宣言していて、その特性を更新する場合は、以前に作成した名前を指定します）。

コマンド デフォルト

このコマンドを使用して CA を宣言するまで、ルータは CA を認識しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。
12.2(15)T	**match certificate** サブコマンドが導入されました。
12.3(7)T	このコマンドが **crypto pki trustpoint** コマンドに置き換えられました。 **crypto ca trusted-root** または **crypto ca trustpoint** コマンドも入力はできますが、コマンドはコンフィギュレーション内に「crypto pki trustpoint」として書き込まれます。

使用上のガイドライン

自己署名ルート CA または下位 CA となる CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。 **crypto ca trustpoint** コマンドを発行すると、ca-trustpoint コンフィギュレーション モードが開始されます。

次のサブコマンドを使用して、トラストポイント CA の特性を指定できます。

- **crl**：証明書失効リスト（CRL）をクエリーし、ピアの証明書が失効していないことを確認します。
- **default**（**ca-trustpoint**）：ca-trustpool コンフィギュレーション モードのサブコマンドの値をデフォルトにリセットします。
- **enrollment**：登録パラメータを指定します（任意）。
- **enrollment http-proxy**：HTTP を使用し、プロキシ サーバ経由で CA にアクセスします。
- **match certificate**：**crypto ca certificate map** コマンドで定義された証明書ベースのアクセス コントロール リスト（ACL）を関連付けます。
- **primary**：特定のトラストポイントをルータのプライマリ トラストポイントとして割り当てます。
- **root**：CA を取得するための簡易ファイル転送プロトコル（TFTP）を定義し、CA 証明書に保存されるサーバ名とファイル名の両方を指定します。

（注） Cisco IOS Release 12.2(8)T 以降では、**crypto ca identity** および **crypto ca trusted-root** コマンドは、その機能が **crypto ca trustpoint** コマンドに統合され、置き換えられました。 **crypto ca identity** または **crypto ca trusted-root** コマンドも入力はできますが、コンフィギュレーション モードおよびコマンドは、コンフィギュレーション内に「**crypto ca trustpoint**」として書き込まれます。

例

次に、「ka」という名前の CA を宣言し、登録および CRL パラメータを指定する例を示します。

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

次に、**crypto ca certificate map** コマンドで定義され、**crypto ca | pki trustpoint** コマンドの **match certificate** サブコマンドに含まれる「Group」というラベルを持つ、証明書ベースのアクセス コントロール リスト（ACL）の例を示します。

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

関連コマンド

コマンド	説明
crl	CRL をクエリーし、ピアの証明書が失効していないことを確認します。
default（ca-trustpoint）	ca-trustpoint コンフィギュレーション サブコマンドの値をデフォルトにリセットします。
enrollment	CA の登録パラメータを指定します。
enrollment http-proxy	HTTP を使用し、プロキシ サーバ経由で CA にアクセスします。
primary	特定のトラストポイントをルータのプライマリ トラストポイントとして割り当てます。
root	TFTP を使用して CA 証明書を取得します。

crypto key generate rsa

crypto key generate rsa

Rivest, Shamir, and Adelman（RSA）キー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**general-keys**| **usage-keys**| **signature**| **encryption**] [**label** *key-label*] **[exportable]** [**modulus** *modulus-size*] [**storage** *devicename* **:**] **[redundancy]** [**on** *devicename* **:**]

構文の説明

general-keys	（任意）デフォルトで汎用キー ペアが生成されるように指定します。
usage-keys	（任意）2 つの RSA 特殊用途キー ペア（1 つの暗号化ペアと 1 つのシグニチャ ペア）が生成されるように指定します。
signature	（任意）生成される RSA 公開キーが署名用の特殊用途キーになるように指定します。
encryption	（任意）生成される RSA 公開キーが暗号化用の特殊用途キーになるように指定します。
label *key-label*	（任意）RSA キー ペアのエクスポート時に使用される名前を指定します。 キー ラベルが指定されていない場合は、ルータの完全修飾ドメイン名（FQDN）が使用されます。
exportable	（任意）RSA キー ペアをルータなどの別のシスコ デバイスにエクスポートできるように指定します。

modulus *modulus-size*	（任意）キー モジュラスの IP サイズを指定します。 デフォルトでは、認証局（CA）キーのモジュラス サイズは 1024 ビットです。 推奨される CA キーのモジュラスは 2048 ビットです。 CA キーのモジュラスの範囲は 350 ～ 4096 ビットです。 （注） Cisco IOS XE Release 2.4 および Cisco IOS Release 15.1(1)T から、秘密キー操作の最大キー サイズは 4096 ビットに拡張されました。 これより前のリリースの秘密キー操作の最大値は 2048 ビットです。
storage *devicename* **:**	（任意）キー ストレージの場所を指定します。ストレージデバイスの名前の後にはコロン（:）を付けます。
redundancy	（任意）キーがスタンバイ CA に同期するように指定します。
on *devicename* **:**	（任意）Universal Serial Bus（USB）トークン、ローカル ディスク、または NVRAM など、指定されたデバイスに RSA キー ペアが作成されるように指定します。 装置の名前の後にはコロン（:）を付けます。 USB トークン上で作成されるキーは、2048 ビット以下である必要があります。

コマンド デフォルト

RSA キー ペアは存在しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3	このコマンドが導入されました。
12.2(8)T	*key-label* 引数が追加されました。
12.2(15)T	**exportable** キーワードが追加されました。

リリース	変更内容
12.2(18)SXD	このコマンドが、Cisco IOS Release 12.2(18)SXD に統合されました。
12.4(4)T	**storage** キーワードおよび *devicename* **:** 引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(11)T	**storage** キーワードおよび *devicename* **:** 引数が、Cisco 7200VXR NPE-G2 プラットフォームに実装されました。 **signature**、**encryption** および **on** キーワードと *devicename* **:** 引数が追加されました。
12.4(24)T	IPv6 セキュア ネイバー探索（SeND）のサポートが追加されました。
XE 2.4	秘密キー操作の最大 RSA キー サイズが 2048 ビットから 4096 ビットに拡張されました。
15.0(1)M	このコマンドが変更されました。 **redundancy** キーワードが追加されました。
15.1(1)T	このコマンドが変更されました。 **modulus** キーワードの値の範囲が 360 ～ 2048 ビットから 360 ～ 4096 ビットに拡張されました。

使用上のガイドライン

（注） セキュリティ上の脅威と、これに対抗するための暗号テクノロジーは、絶えず変化しています。 最新のシスコの暗号化に関する推奨事項の詳細については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。

このコマンドは、シスコデバイス（ルータなど）の RSA キーペアを生成するために使用します。

RSA キーはペアで生成されます。1 つは公開 RSA キーで、もう 1 つは秘密 RSA キーです。

このコマンドの発行時に、ルータに RSA キーがすでに設定されている場合は、警告が表示され、既存のキーを新しいキーと置き換えるよう求めるプロンプトが表示されます。

（注） このコマンドを発行する前に、ルータにホスト名および IP ドメイン名が設定されていることを確認します（**hostname** および **ip domain-name** コマンドを使用）。 ホスト名および IP ドメイン名なしで **crypto key generate rsa** コマンドを完了することはできません （名前付きのキーペアのみを生成する場合を除きます）。

（注） RSA キーなしでルータのキー ペアを生成すると、セキュア シェル（SSH）によって RSA キー ペアが生成される場合があります。 追加のキー ペアは、SSH のみが使用し、{*router_FQDN*}.server などの名前が付けられます。 たとえば、ルータの名前が「router1.cisco.com」の場合は、キーの名前が「router1.cisco.com.server」になります。

このコマンドはルータ コンフィギュレーションに保存されません。ただし、このコマンドによって生成された RSA キーは、次回に NVRAM にコンフィギュレーションが書き込まれる際に NVRAM のプライベート コンフィギュレーションに保存されます（ユーザには表示されません。また、別のデバイスにバックアップもされません）。

（注） コンフィギュレーションが NVRAM に保存されない場合、生成されたキーは次回のルータのリロード時に失われます。

RSA キー ペアには特殊用途キーと汎用目的キーの 2 つのタイプがあり、これらは相互に排他的です。 RSA キー ペアを生成する場合、特殊用途キーまたは汎用目的キーのいずれかを選択するように求められます。

特殊用途キー

特殊用途キーを生成すると、RSA キーが 2 ペア生成されます。 一方のペアは、認証方式として RSA シグニチャを指定するインターネット キー交換（IKE）ポリシーで使用され、もう一方のペアは、認証方式として RSA 暗号キーを指定する IKE ポリシーで使用されます。

CA は、RSA シグニチャを指定する IKE ポリシーでのみ使用され、RSA 暗号化ナンスを指定する IKE ポリシーでは使用されません （ただし、複数の IKE ポリシーを指定し、一方のポリシーに RSA シグニチャを指定し、もう一方のポリシーに RSA 暗号化ナンスを指定することはできます）。

IKE ポリシーに両方のタイプの RSA 認証方式を使用する場合は、特殊用途キーを生成します。 特殊用途キーを使用すると、各キーは不必要に暴露されなくなります （特殊用途キーを使用しない場合、1 つのキーが両方の認証方式に使用されるため、そのキーが暴露される危険性が高くなります）。

汎用目的キー

汎用目的キーを生成すると、RSA キーが 1 ペアだけ生成されます。 このペアは、RSA シグニチャまたは RSA 暗号化キーのいずれかを指定する IKE ポリシーで使用されます。 したがって、汎用目的キー ペアは、特殊用途キー ペアよりも頻繁に使用される可能性があります。

名前付きのキー ペア

key-label 引数を使用して名前付きのキー ペアを生成する場合は、**usage-keys** キーワードまたは **general-keys** キーワードを指定する必要があります。 名前付きのキー ペアを使用すると、複数の RSA キー ペアを持つことが可能になり、Cisco IOS ソフトウェアがアイデンティティ証明書ごとに異なるキー ペアを維持できます。

モジュラス長

RSA キーを生成すると、モジュラス長を入力するように求められます。 モジュラス長が長いほど、セキュリティが強力になります。 ただし、モジュラス長が長いほど生成に時間がかかり（次の表の生成時間の例を参照）、使用するのに時間がかかります。

表 *6*：モジュラス長による *RSA* キーの生成時間の例

ルータ	360 ビット	512 ビット	1024 ビット	2048 ビット（最大）
Cisco 2500	11 秒	20 seconds	4 分 38 秒	1 時間以上
Cisco 4700	1 秒未満	1 秒	4 秒	50 秒

Cisco IOS ソフトウェアは、4096 ビットより大きいモジュラスはサポートしません。 512 ビット未満の長さは、通常は推奨されません。 モジュラスが短いと IKE で適切に機能しない場合があるため、少なくとも 2048 ビット以上のモジュラスを使用することを推奨します。

（注） Cisco IOS Release 12.4(11)T の時点では、最大 4096 ビットまでのピアの公開 RSA キーのモジュラス値が自動的にサポートされます。 秘密 RSA キーの最大モジュラス値は 4096 ビットです。したがって、ルータが生成またはインポートできる RSA 秘密キーの最大サイズは、4096 ビットです。 ただし、RFC 2409 では、RSA 暗号化の秘密キーのサイズを 2048 ビット以下に制限しています。 CA に対して推奨されるモジュラスは 2048 ビット、クライアントに対して推奨されるモジュラスは 2048 ビットです。

RSA キーが暗号化ハードウェアによって生成されるときは、追加の制限が適用される場合があります。 たとえば、RSA キーが Cisco VPN Services Port Adapter（VSPA）によって生成される場合は、RSA キーのモジュラスの最小値は 384 ビットで、64 の倍数である必要があります。

RSA キーの保管場所の指定

crypto key generate rsa コマンドを **storage** *devicename* **:** キーワードおよび引数で発行すると、RSA キーは指定されたデバイスに保存されます。 この場所は、**crypto key storage** コマンドの設定に優先します。

RSA キーを生成するデバイスの指定

Cisco IOS Release 12.4(11)T 以降のリリースでは、RSA キーを生成するデバイスを指定できます。サポートされているデバイスには、NVRAM、ローカルディスク、および USB トークンがあります。 ルータに設定済みで利用可能な USB トークンがある場合、USB トークンは、ストレージデバイスだけでなく暗号化デバイスとして使用することもできます。 USB トークンを暗号化デバイスとして使用すると、トークンでクレデンシャルのキー生成、署名、認証などの RSA 操作を実行できます。 秘密キーは決して USB トークンから出ないようになっており、エクスポートできません。 公開キーはエクスポート可能です。

on *devicename* **:** キーワードおよび引数を使用すると、設定済みの利用可能な USB トークンで RSA キーが生成される場合があります。 USB トークン上に常駐するキーは、生成された段階でトークンの永続的な保管場所に保存されます。 USB トークンで生成されるキーの数は、使用可能な空き

領域によって制限されます。USB トークンでキーを生成するときに使用可能な空き領域がない場合は、次のメッセージが表示されます。

```
% Error in generating keys:no available resources
```

キーの削除操作を行うと、トークンに保存されているキーは、永続的な保管場所からただちに削除されます（トークン上に常駐していないキーは、**copy** またはそれに類するコマンドが発行されると、トークン以外の保管場所で保存や削除が行われます）。

USB トークンの設定の詳細については、『Cisco IOS Security Configuration Guide, Release 12.4T』の「Storing PKI Credentials」の章を参照してください。 トークン上の RSA クレデンシャルの使用の詳細については、『Cisco IOS Security Configuration Guide, Release 12.4T』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章を参照してください。

デバイスでの RSA キーの冗長性の生成の指定

エクスポート可能な場合にだけ、既存のキーの冗長性を指定できます。

例

次に、「ms2」というラベルの USB トークンでの汎用 1024 ビット RSA キー ペアの生成と、それとともに表示される暗号エンジンのデバッギング メッセージの例を示します。

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

これで、「ms2」というラベルが付けられた、トークン上のキーを登録に使用できます。

次に、特殊用途 RSA キーを生成する例を示します。

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用目的 RSA キーを生成する例を示します。

（注） 特殊用途キーと汎用目的キーの両方は生成できません。いずれか一方だけを生成できます。

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用目的 RSA キー ペア「exampleCAkeys」を生成する例を示します。

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

次に、「usbtoken0:」の RSA キーの保管場所を「tokenkey1」に指定する例を示します。

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

次に、**redundancy** キーワードを指定する例を示します。

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

キーの名前は MYKEYS になります。

汎用目的キーのキー モジュラスのサイズを 360 ～ 2048 の

範囲で選択します。 512 より大きいサイズのキー モジュラスを選択した場合は生成に

数分かかる場合があります。

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

関連コマンド

コマンド	説明
copy	特権 EXEC モードで copy コマンドを使用して、送信元から宛先にファイルをコピーします。
crypto key storage	RSA キー ペアのデフォルトの保管場所を設定します。
debug crypto engine	暗号エンジンに関するデバッグ メッセージを表示します。
hostname	ネットワーク サーバのホスト名を指定または修正します。
ip domain-name	デフォルトのドメイン名を定義して、未修飾のホスト名（ドット付き 10 進表記で記載されていない名前）を完成します。
show crypto key mypubkey rsa	ルータの RSA 公開キーを表示します。
show crypto pki certificates	PKI 証明書、認証局、および登録局証明書に関する情報を表示します。