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。