Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ システム セキュリティ コマンド リファレンス リリース 4.3.x

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/

Text Part Number: OL-28471-01-J

【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

はじめに

このマニュアルでは、Cisco IOS XR ソフトウェアでシステム セキュリティを表示および設定するために使用されるコマンドについて説明します。 システム セキュリティの設定情報および例については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』を参照してください。

ここでは、次のトピックについて取り上げます。

マニュアルの変更履歴

次の表に、初版後、本書に行われた変更の履歴を示します。

表 *1*：マニュアルの変更履歴

リビジョン	日付	変更点
OL-28471-01-J	2012 年 12 月	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定するこ

ともできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

認証、許可、アカウンティング コマンド

ここでは、認証、許可、アカウンティング（AAA）サービスを設定するために使用されるコマンドについて説明します。

AAA の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Configuring AAA Services on* 」モジュールを参照してください。

aaa accounting

アカウンティングの方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。 システムからリスト名を削除するには、このコマンドの **no** 形式を使用します。

aaa accounting {**commands**| **exec**| **network**} {**default**| **list-name**} {**start-stop**| **stop-only**} {**none**| **method**}

no aaa accounting {**commands**| **exec**| **network**} {**default**| **list-name**}

構文の説明

commands	EXEC シェル コマンドに対してアカウンティングをイネーブルにします。
exec	EXEC セッションのアカウンティングをイネーブルにします。
network	Internet Key Exchange（IKE; インターネットキー交換）や Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）など、すべてのネットワーク関連サービス要求に対するアカウンティングをイネーブルにします。
default	このキーワードに続くアカウンティング方式のリストをアカウンティング サービスのデフォルト方式リストとして使用します。
list-name	アカウンティング方式リストの名前の指定に使用する文字列です。
start-stop	プロセスの開始時に「start accounting」通知を送信し、プロセスの終了時に「stop accounting」通知を送信します。 要求されたユーザ プロセスは、「start accounting」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。
stop-only	要求されたユーザ プロセスの終了時に「stop accounting」通知を送信します。
none	アカウンティングを使用しません。
method	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：すべての TACACS+ サーバのリストをアカウンティングに使用します。 • **group radius**：すべての RADIUS サーバのリストをアカウンティングに使用します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットをアカウンティングに使用します。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa accounting コマンドを使用して、回線単位またはインターフェイス単位で使用できる、特定のアカウンティング方式を定義するデフォルトまたは名前付き方式リストを作成します。 方式リストには方式を 4 つまで指定できます。 リスト名を回線（console、aux、または vty テンプレート）に適用して、その回線でアカウンティングをイネーブルにすることができます。

Cisco IOS XR ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式の両方をサポートします。 ルータからセキュリティ サーバにアカウンティング レコードの形でユーザ アクティビティが報告され、そのレコードはセキュリティ サーバに保存されます。

アカウンティング方式リストには、アカウンティングの実行方法が定義されます。このリストを使用して、特定のタイプのアカウンティング サービスに固有の回線またはインターフェイスに使用する特定のセキュリティ プロトコルを指定できます。

最小限のアカウンティングを行うには、要求されたユーザ プロセスのあとで「stop accounting」通知を送信するよう、**stop-only** キーワードを付加します。 さらに詳細なアカウンティングを行うには、TACACS+ が要求されたプロセスの開始時に「start accounting」通知を送信し、プロセスのあとで「stop accounting」通知を送信するよう、**start-stop** キーワードを付加できます。 アカウンティング レコードは、TACACS+ サーバだけに保存されます。

要求されたユーザ プロセスは、「start accounting」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。

（注） このコマンドは、TACACS または拡張 TACACS には使用できません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、デフォルトの commands アカウンティング方式リストを定義する例を示します。この例では、TACACS+ セキュリティ サーバにより、stop-only 制限付きのアカウンティング サービスが提供されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting commands default stop-only group tacacs+
```

関連コマンド

コマンド	説明
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa accounting system default

認証、許可、アカウンティング（AAA）システム アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting system default** コマンドを使用します。システム アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting system default {**start-stop**| **stop-only**} {**none**| **method**}

no aaa accounting system default

構文の説明

start-stop	システム起動時に「start accounting」通知を送信し、システム シャットダウンまたはリロード時に「stop accounting」通知を送信します。
stop-only	システム シャットダウンまたはリロード時に「stop accounting」通知を送信します。
none	アカウンティングを使用しません。
method	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：すべての TACACS+ サーバのリストをアカウンティングに使用します。 • **group radius**：すべての RADIUS サーバのリストをアカウンティングに使用します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットをアカウンティングに使用します。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システムアカウンティングには、名前付きアカウンティング リストは使用されません。定義できるのは、デフォルト リストだけです。

デフォルトの方式リストが、自動的にすべてのインターフェイスまたは回線に適用されます。 デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

方式リストには方式を 4 つまで指定できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ルータの最初の起動時に「start accounting」レコードが TACACS+ サーバに送信されるようにする例を示します。 また、ルータのシャットダウンまたはリロード時には「stop accounting」レコードが送信されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting system default start-stop group tacacs+
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa accounting system rp-failover

RP フェールオーバーまたは RP スイッチオーバー開始または停止アカウンティング メッセージを送信するためのアカウンティング リストを作成するには、**aaa accounting system rp-failover** コマンドをグローバル コンフィギュレーション モードで使用します。 RP フェールオーバーに対するシステム アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting system rp-failover {*list_name* {**start-stop| stop-only**}| **default** {**start-stop| stop-only**}}

no aaa accounting system rp-failover {*list_name* {**start-stop| stop-only**}| **default** {**start-stop| stop-only**}}

構文の説明

list_name	アカウンティング リスト名を指定します。
default	デフォルトのアカウンティング リストを指定します。
start-stop	開始および停止のレコードをイネーブルにします。
stop-only	停止レコードだけをイネーブルにします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 4.2.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、デフォルトのアカウンティング リストに対して **aaa accounting system rp-failover** コマンドを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# aaa accounting system rp-failover default start-stop none
```

関連コマンド

コマンド	説明
aaa attribute format	AAA 属性形式の名前を作成します。

aaa accounting update

定期的な中間アカウンティング レコードがアカウンティング サーバに送信されるようにするには、グローバル コンフィギュレーション モードで **aaa accounting update** コマンドを使用します。中間アカウンティングのアップデートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting update {**newinfo**| **periodic** *minutes*}

no aaa accounting update

構文の説明

newinfo	（任意）当該のユーザに関して報告する新しいアカウンティング情報があるときは常に、中間アカウンティング レコードをアカウンティング サーバに送信します。
periodic *minutes*	（任意）*minutes* 引数によって定義されているとおりに、中間アカウンティング レコードを定期的にアカウンティング サーバに送信します。この引数は、分数を指定する整数です。 範囲は、1 ～ 35791394 分です。

コマンド デフォルト

AAA のアカウンティングのアップデートはディセーブルになります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

newinfo キーワードを使用すると、報告する新しいアカウンティング情報があるたびに中間アカウンティング レコードがアカウンティング サーバに送信されます。 たとえば、IP Control Protocol（IPCP; IP 制御プロトコル）がリモート ピアとの IP アドレス ネゴシエーションを完了した時点でこのようなレポートが送信されます。 中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

periodic キーワードを使用すると、中間アカウンティング レコードは *minutes* 引数で定義されているとおりに定期的に送信されます。 中間アカウンティング レコードには、アカウンティング レコードが送信される時点までにそのユーザに関して記録されたすべてのアカウンティング情報が含まれます。

newinfo キーワードと **periodic** キーワードを両方使用すると、報告する新しいアカウンティング情報があるたびに中間アカウンティング レコードがアカウンティング サーバに送信され、さらに *minutes* 引数で定義されているとおりにアカウンティング レコードが定期的にアカウンティング サーバに送信されます。 たとえば、**aaa accounting update** コマンドに **newinfo** キーワードと **periodic** キーワードを設定すると、現在ログインしているすべてのユーザによって定期的な中間アカウンティング レコードの生成が続けられると同時に、新たにユーザがログインすると、newinfo アルゴリズムに基づいてアカウンティング レコードが生成されます。

注意 多数のユーザがネットワークにログインしているときに **aaa accounting update** コマンドに **periodic** キーワードを指定すると、大きな輻輳が生じる場合があります。

periodic キーワードと **newinfo** キーワードは相互に排他的であるため、一度に設定できるキーワードはいずれか 1 つです。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、定期的な中間アカウンティング レコードを 30 分間隔で RADIUS サーバに送信する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting update periodic 30
```

次に、報告する新しいアカウンティング情報があるときに、中間アカウンティング レコードを RADIUS サーバに送信する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting update newinfo
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa authentication

認証の方式リストを作成するには、グローバル コンフィギュレーション モードまたは管理コンフィギュレーション モードで **aaa authentication** コマンドを使用します。 この認証方式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**| **ppp**} {**default**| *list-name*| **remote**} *method-list*

no aaa authentication {**login**| **ppp**} {**default**| *list-name*| **remote**} *method-list*

構文の説明

login	ログインの認証を設定します。
ppp	ポイントツーポイント プロトコルの認証を設定します。
default	このキーワードに続く認証方式のリストを認証のデフォルト方式リストとして使用します。
list-name	認証方式リストの名前の指定に使用する文字列です。
remote	このキーワードに続く認証方式リストを、所有者なしのリモートのセキュア ドメイン ルータにおける管理認証のデフォルト方式リストとして使用します。 **remote** キーワードは **login** キーワードと一緒に使用できますが、**ppp** キーワードとは一緒に使用できません。 （注） **remote** キーワードは管理プレーンだけで使用できます。
method-list	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：設定されたすべての TACACS+ サーバのリストを認証に使用する方式リストを指定します。 • **group radius**：設定されたすべての RADIUS サーバのリストを認証に使用する方式リストを指定します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを認証に使用する方式リストを指定します。 • **local**：ローカル ユーザ名データベース方式を認証に使用する方式リストを指定します。 ユーザ名がローカル グループで定義されていない場合、AAA 方式がローカル方式以外にロールオーバーされます。 • **line**：回線パスワードを認証に使用する方式リストを指定します。

コマンド デフォルト

デフォルトでは、すべてのポートにローカル認証が適用されます。

管理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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authentication コマンドを使用して、一連の認証方式、つまり方式リストを作成します。 方式リストには方式を 4 つまで指定できます。 *method list* は、一連の認証方式（TACACS+ または RADIUS など）を示す名前付きリストです。 後続の認証方式は、最初の方式が失敗した場合ではなく、使用不可能な場合にだけ使用されます。

別の名前付き方式リストが明示的に指定されている場合を除き、すべてのインターフェイスの認証にデフォルトの方式リストが適用されます。別のリストが明示的に指定されている場合は、デフォルト リストが上書きされます。

コンソールおよび vty のアクセスについては、認証が設定されていない場合、デフォルトのローカル方式が適用されます。

（注）

- このコマンドの **group tacacs+**、**group radius**、および **group** *group-name* の各形式は、あらかじめ定義された一連の TACACS+ サーバまたは RADIUS サーバを指します。
- ホスト サーバを設定するには、**tacacs-server host** コマンドまたは **radius-server host** コマンドを使用します。
- サーバの名前付きサブセットを作成するには、**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドを使用します。
- **login** キーワード、**remote** キーワード、**local** オプション、および **group** オプションは、管理コンフィギュレーション モードでだけ使用できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、グローバル コンフィギュレーション モードでデフォルトの認証方式リストを指定し、コンソールの認証をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authentication login default group tacacs+
```

次に、管理コンフィギュレーション モードでリモートの認証方式リストを指定し、コンソールの認証をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router (admin)# configure
RP/0/RSP0/CPU0:router(admin-config)# aaa authentication login remote local group tacacs+
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。
aaa group server radius, （22 ページ）	複数の RADIUS 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 group server tacacs+, （25 ページ）	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。
login authentication, （45 ページ）	ログインに対する AAA 認証をイネーブルにします。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

aaa authorization

許可の方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを使用します。 機能に対する許可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization {**commands**| **eventmanager**| **exec**| **network**} {**default**| *list-name*} {**none**| **local**| **group** {**tacacs+**| **radius**| *group-name*}}

no aaa authorization {**commands**| **eventmanager**| **exec**| **network**} {**default**| *list-name*}

構文の説明

commands	すべての EXEC シェル コマンドに対する許可を設定します。
eventmanager	イベント マネージャ（障害マネージャ）を許可するための許可方式を適用します。
exec	対話型（EXEC）セッションに対する許可を設定します。
network	PPPやインターネットキー交換（IKE）などのネットワーク サービスに対する許可を設定します。
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。
none	許可を使用しません。 **none** を指定すると、後続の許可方式は試行されません。ただし、タスク IDの許可は常に必要であり、ディセーブルにはできません。
local	ローカルの許可を使用します。 この許可方式は、コマンドの許可には使用できません。
group tacacs+	設定されているすべての TACACS+ サーバのリストを許可に使用します。
group radius	設定されているすべての RADIUS サーバのリストを許可に使用します。この許可方式は、コマンドの許可には使用できません。
group *group-name*	**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを許可に使用します。

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（**none** キーワードと同等）。

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authorization コマンドを使用して、回線単位またはインターフェイス単位で使用できる特定の許可方式を定義する方式リストを作成します。 方式リストには方式を 4 つまで指定できます。

（注） ここに示すコマンドの許可は、タスクに基づいた許可ではなく、外部の AAA サーバで実行される許可に適用します。

許可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、一連の許可方式（TACACS+ など）を記述した名前付きリストです。 方式リストを使用して、許可に 1 つまたは複数のセキュリティ プロトコルを指定し、最初の方式が失敗した場合のバックアップ システムを確保することができます。 Cisco IOS XR ソフトウェアでは、特定のネットワーク サービスに対してユーザを許可するために、リスト内の最初の方式が使用されます。この方式が応答に失敗すると、Cisco IOS XR ソフトウェアでは方式リスト内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との通信に成功するまで、または定義されている方式を使い果たすまで続行されます。

（注） Cisco IOS XR ソフトウェアでは、前の方式から応答がない（障害ではない）場合にだけ、次に指定された方式を使って許可が試みられます。 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。

Cisco IOS XR ソフトウェアは、次の許可方式をサポートします。

- **none**：ルータから許可情報の要求はありません。この回線やインターフェイスに対する許可は行われません。
- **local**：ローカル データベースを許可に使用します。
- **group tacacs+**：設定されているすべての TACACS+ サーバのリストを許可に使用します。
- **group radius**：設定されているすべての RADIUS サーバのリストを許可に使用します。
- **group group-name**：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを許可に使用します。

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。 Cisco IOS XR ソフトウェアは、次の 4 つのタイプの AAA 許可をサポートします。

- **コマンドの許可**：ユーザが実行する EXEC モード コマンドに適用されます。 コマンドの許可では、すべての EXEC モード コマンドに対する許可が試みられます。

（注） 「コマンド」の許可は、認証時に設定されたタスク プロファイルに基づく「タスクベース」の許可とは異なります。

- **EXEC の許可**：EXEC セッションの開始に対する許可が適用されます。

（注） **exec** キーワードは、障害マネージャ サービスの許可に使用されなくなりました。 障害マネージャ サービスの許可には、**eventmanager** キーワード（障害マネージャ）を使用します。 **exec** キーワードは、EXEC の許可に使用します。

- **ネットワークの許可**：IKE などのネットワーク サービスの許可が適用されます。
- **イベント マネージャの許可**：イベント マネージャ（障害マネージャ）を許可するための許可方式が適用されます。 TACACS+ を使用することも、locald を使用することもできます。

（注） イベント マネージャ（障害マネージャ）を許可するには、**exec** キーワードの代わりに **eventmanager** キーワード（障害マネージャ）を使用します。

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。 方式リストを定義した場合、定義した方式のいずれかを実行するには、まず特定の回線またはインターフェイスに方式リストを適用する必要があります。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、TACACS+ の許可を使用するように指定する listname1 というネットワーク許可方式リストを定義する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authorization commands listname1 group tacacs+
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。

aaa default-taskgroup

リモートの TACACS+ 認証と RADIUS 認証の両方のタスク グループを指定するには、グローバル コンフィギュレーション モードで **aaa default-taskgroup** コマンドを使用します。 このデフォルト タスク グループを削除するには、このコマンドの **no** 形式を入力します。

aaa default-taskgroup *taskgroup-name*

no aaa default-taskgroup

構文の説明

taskgroup-name	既存のタスク グループの名前です。

コマンド デフォルト

リモート認証には、デフォルトのタスク グループは割り当てられません。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa default-taskgroup コマンドを使用して、リモート TACACS+ 認証に既存のタスク グループを指定します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、リモート TACACS+ 認証のデフォルト タスク グループとして taskgroup1 を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa default-taskgroup taskgroup1
```

aaa group server radius

各種の RADIUS サーバ ホストを別個のリスト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** コマンドを使用します。 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。

コマンド デフォルト

このコマンドはディセーブルになります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa group server radius コマンドを使用して、既存のサーバ ホストをグループ化します。そうすることにより、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、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 グループは、選択されているサーバ ホストの IP アドレスまたはホスト名を示します。

また、サーバ グループには、各エントリが一意の ID を持っていれば、同一サーバに複数のホスト エントリを組み込むことができます。 IP アドレスとユーザ データグラム プロトコル（UDP）ポート番号を組み合わせることで、一意の ID が作成されます。この情報を使用して、固有の認証、許可、アカウンティング（AAA）サービスを提供する RADIUS ホストとして各ポートを個別に定義できます。 つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。 たとえば、同一の RADIUS サーバの 2 つの異なるホスト エントリを同一のサービスに対して設定すると、2 つ目のホスト エントリは最初のホスト エントリをバックアップする自動

スイッチオーバーとして機能します。この場合、最初のホストエントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じデバイス上の 2 つ目のホスト エントリでアカウンティング サービスを試行します。RADIUS ホストエントリは、サーバ グループに設定された順序で試行されます。

サーバ グループのメンバはすべて同じタイプ、つまり RADIUS であることが必要です。

サーバ グループには、radius や tacacs の名前を付けることはできません。

このコマンドを実行すると、サーバ グループ コンフィギュレーション モードが開始されます。server コマンドを使用して、特定の RADIUS サーバを定義済みのサーバ グループに関連付けることができます。

タスク ID

タスク ID	操作
aaa	read, write

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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius radgroup1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.5 auth-port 1700 acct-port 1701
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.10 auth-port 1702 acct-port 1703
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.20 auth-port 1705 acct-port 1706
```

（注） **auth-port** *port-number* および **acct-port** *port-number* キーワードおよび引数が指定されていない場合、**auth-port** キーワードの *port-number* 引数のデフォルト値は 1645、**acct-port** キーワードの *port-number* 引数のデフォルト値は 1646 です。

関連コマンド

コマンド	説明
key（RADIUS）, （41 ページ）	ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。
radius source-interface, （66 ページ）	RADIUS で、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスが使用されるようにします。

コマンド	説明
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server（RADIUS）, （73 ページ）	RADIUS サーバを定義済みのサーバ グループに関連付けます。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

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** 形式を入力します。

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。

コマンド デフォルト

このコマンドはディセーブルになります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

AAA サーバグループ機能により、既存のサーバ ホストをグループ化する手段が追加されます。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。

aaa group server tacacs+ コマンドを実行すると、サーバ グループ コンフィギュレーション モードが開始されます。 **server** コマンドを実行すると、特定の TACACS+ サーバが定義済みのサーバ グループに関連付けることができます。

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。 サポートされているサーバ ホストのタイプは、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 ホストのリストと一緒に使用します。 サーバ グループは、選択されているサーバ ホストの IP アドレスまたはホスト名を示します。

サーバ グループには、radius や tacacs の名前を付けることはできません。

（注） グループ名方式では、定義済みの一連の TACACS+ サーバを参照します。 ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。

タスク ID

タスク ID	操作
aaa	read, write

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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tacgroup1
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.226
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.227
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.228
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。
server（TACACS+）, （76 ページ）	外部 TACACS+ サーバのホスト名または IP アドレスを指定します。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

accounting（回線）

特定の回線または回線グループに対して認証、許可、アカウンティング（AAA）アカウンティング サービスをイネーブルにするには、回線テンプレート コンフィギュレーション モードで **accounting** コマンドを使用します。 AAA アカウンティング サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

accounting {**commands**| **exec**} {**default**| *list-name*}

no accounting {**commands**| **exec**}

構文の説明

commands	すべての EXEC シェル コマンドに対して、選択した回線におけるアカウンティングをイネーブルにします。
exec	EXEC セッションのアカウンティングをイネーブルにします。
default	**aaa accounting** コマンドで作成されるデフォルトの方式リストの名前です。
list-name	使用するアカウンティング方式リストの名前を指定します。 リストは、**aaa accounting** コマンドで作成されます。

コマンド デフォルト

アカウンティングはディセーブルです。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa accounting コマンドをイネーブルにして、特定のタイプのアカウンティングに対して名前付きアカウンティング方式リストを定義（またはデフォルトの方式リストを使用）したあと、アカウンティング サービスを実行する該当の回線に、定義済みのリストを適用する必要があります。 **accounting** コマンドを使用して、選択した回線または回線グループに指定の方式リストを適用し

ます。 このように方式リストを指定しないと、選択した回線または回線グループにアカウンティングが適用されません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、回線テンプレート *configure* でアカウンティング方式リスト *listname2* を使用するコマンド アカウンティング サービスをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# accounting commands listname2
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。

authorization

特定の回線または回線グループに対して認証、許可、アカウンティング（AAA）の許可をイネーブルにするには、回線テンプレート コンフィギュレーション モードで **authorization** コマンドを使用します。 許可をディセーブルにするには、このコマンドの **no** 形式を使用します。

authorization {**commands**| **exec**} {**default**| *list-name*}

no authorization {**commands**| **exec**}

構文の説明

commands	選択した回線におけるすべてのコマンドの許可をイネーブルにします。
exec	対話型（EXEC）セッションに対する許可をイネーブルにします。
default	**aaa authorization** コマンドで作成されたデフォルトの方式リストを適用します。
list-name	使用する許可方式リストの名前を指定します。 リスト名を指定しない場合は、デフォルト名が使用されます。 リストは **aaa authorization** コマンドで作成されます。

コマンド デフォルト

許可はディセーブルになります。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authorization コマンドを使用して、特定のタイプの許可に対して名前付き許可方式リストを定義（またはデフォルトの方式リストを使用）したあと、許可を実行する該当の回線に、定義済みのリストを適用する必要があります。 **authorization** コマンドを使用して、指定の方式リスト

（または、方式リストを指定していない場合はデフォルトの方式リスト）を選択した回線または回線グループに適用します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、回線テンプレート *configure* で方式リスト *listname4* を使用するコマンド許可をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# authorization commands listname4
```

関連コマンド

コマンド	説明
aaa authorization, （16 ページ）	許可の方式リストを作成します。

deadtime（サーバグループ コンフィギュレーション）

RADIUSサーバ グループ レベルでデッドタイム値を設定するには、サーバグループ コンフィギュレーション モードで **deadtime** コマンドを使用します。 デッドタイムを 0 に設定するには、このコマンドの **no** 形式を使用します。

deadtime *minutes*

no deadtime

構文の説明

minutes	RADIUS サーバがトランザクション要求によってスキップされる時間を最長 1440（24 時間）まで分単位で表したものです。 指定できる範囲は 1 ～ 1440 です。

コマンド デフォルト

デッドタイムは 0 に設定されます。

コマンド モード

サーバグループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバ グループに設定されたデッドタイム値は、グローバルに設定されたデッドタイム値を上書きします。サーバグループ コンフィギュレーションでデッドタイムを省略した場合は、マスターリストの値が継承されます。サーバグループを設定しない場合、グループ内のすべてのサーバにデフォルト値 0 が適用されます。 デッドタイムを 0 に設定すると、サーバに dead のマークは付きません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、RADIUS サーバ グループ group1 が認証要求への応答に失敗したときの **deadtime** コマンドに対して、1 分のデッドタイムを指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
RP/0/RSP0/CPU0:router(config-sg-radius)# deadtime 1
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	複数の RADIUS 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。
radius-server dead-criteria time, （50 ページ）	RADIUS サーバに dead マークを付けるための 1 つまたは両方の基準を強制的に使用します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間を分単位で定義します。

description（AAA）

設定時にタスク グループまたはユーザ グループの説明を作成するには、タスク グループ コンフィギュレーション モードまたはユーザ グループ コンフィギュレーション モードで **description** コマンドを使用します。 タスク グループの説明またはユーザ グループの説明を削除するには、このコマンドの **no** 形式を使用します。

description *string*

no description

構文の説明

string	タスク グループまたはユーザ グループを説明する文字列です。

コマンド デフォルト

なし

コマンド モード

タスク グループ コンフィギュレーション

ユーザ グループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスクまたはユーザ グループ コンフィギュレーション サブモードで **description** コマンドを使用して、タスクまたはユーザ グループの説明をそれぞれ定義します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タスク グループの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# description this is a sample taskgroup
```

次に、ユーザ グループの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# description this is a sample user group
```

関連コマンド

コマンド	説明
taskgroup, （125 ページ）	タスク グループ コンフィギュレーション モードにアクセスし、一連のタスク ID に関連付けることでタスク グループを設定します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、一連のタスク グループに関連付けることでユーザ グループを設定します。

group（AAA）

ユーザをグループに追加するには、ユーザ名コンフィギュレーション モードで **group** コマンドを使用します。 グループからユーザを削除するには、このコマンドの **no** 形式を使用します。

group {**root-system**| **root-lr**| **netadmin**| **sysadmin**| **operator**| **cisco-support**| **serviceadmin**| *group-name*}**no group** {**root-system**| **root-lr**| **netadmin**| **sysadmin**| **operator**| **cisco-support**| **serviceadmin**| *group-name*}

構文の説明

root-system	事前定義された root-system グループにユーザを追加します。 root-system 権限を持つユーザだけがこのオプションを使用できます。
root-lr	事前定義された root-lr グループにユーザを追加します。 root-system 権限または root-lr 権限を持つユーザだけがこのオプションを使用できます。
netadmin	事前定義されたネットワーク管理者グループにユーザを追加します。
sysadmin	事前定義されたシステム管理者グループにユーザを追加します。
operator	事前定義されたオペレータ グループにユーザを追加します。
cisco-support	事前定義されたシスコ サポート担当者グループにユーザを追加します。
serviceadmin	事前定義されたサービス管理者グループにユーザを追加します。
group-name	すでに **usergroup** コマンドで定義されている名前付きユーザ グループにユーザを追加します。

コマンド デフォルト

なし

コマンド モード

ユーザ名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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

定義済みの root-system グループは、root-system ユーザだけが管理の設定時に指定できます。

ユーザ名コンフィギュレーション モードで **group** コマンドを使用します。 ユーザ名コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで username, （135 ページ） コマンドを使用します。

管理コンフィギュレーション モードで **group** コマンドを使用する場合に指定できるキーワードは、root-system および cisco-support に限られます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ グループ operator を user1 というユーザに割り当てる例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# group operator
```

関連コマンド

コマンド	説明
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
usergroup, （133 ページ）	ユーザ グループを設定し、そのユーザ グループを一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーション モードにアクセスし、新しいユーザにユーザ名を設定して、そのユーザのパスワードとアクセス許可を設定します。

inherit taskgroup

タスク グループで別のタスク グループのアクセス許可を取得できるようにするには、タスク グループ コンフィギュレーション モードで **inherit taskgroup** コマンドを使用します。

inherit taskgroup {*taskgroup-name*| **netadmin**| **operator**| **sysadmin**| **cisco-support**| **root-lr**| **root-system**| **serviceadmin**}

構文の説明

taskgroup-name	アクセス許可を継承する元のタスク グループの名前です。
netadmin	ネットワーク管理者タスク グループからアクセス許可を継承します。
operator	オペレータ タスク グループからアクセス許可を継承します。
sysadmin	システム管理者タスク グループからアクセス許可を継承します。
cisco-support	Cisco サポート タスク グループからアクセス許可を継承します。
root-lr	root-lr タスク グループからアクセス許可を継承します。
root-system	root-system タスク グループからアクセス許可を継承します。
serviceadmin	サービス管理者タスク グループからアクセス許可を継承します。

コマンド デフォルト

なし

コマンド モード

タスク グループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

inherit taskgroup コマンドを使用して、あるタスク グループから別のタスク グループにアクセス許可（タスク ID）を継承します。 継承元のタスク グループが変更されると、ただちに継承元のグループ内に反映されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タスク グループ tg2 のアクセス許可がタスク グループ tg1 に継承される例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup tg1
RP/0/RSP0/CPU0:router(config-tg)# inherit taskgroup tg2
RP/0/RSP0/CPU0:router(config-tg)# end
```

inherit usergroup

ユーザ グループで別のユーザ グループの特性を取得できるようにするには、ユーザ グループ コンフィギュレーション モードで **inherit usergroup** コマンドを使用します。

inherit usergroup *usergroup-name*

構文の説明

usergroup-name	アクセス許可が継承される元のユーザ グループの名前です。

コマンド デフォルト

なし

コマンド モード

ユーザ グループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

各ユーザ グループは、そのグループのユーザに適用できる一連のタスク グループが関連付けられます。 タスク グループは、タスク ID の集合によって定義されます。 タスク グループには、各アクション クラスに対応したタスク ID リストが含まれます。 ユーザに対するタスク アクセス許可は、そのユーザが属するユーザ グループに関連付けられたタスク グループから（EXEC または XML セッションの開始時に）取得されます。

ユーザ グループは、別のユーザ グループからの継承をサポートします。 **inherit usergroup** コマンドを使用して、あるユーザ グループから別のユーザ グループにアクセス許可（タスク ID 属性）をコピーします。「コピー先」のユーザ グループは継承元のグループのプロパティを継承し、これらのグループに指定されているすべてのタスク ID の集合を形成します。 たとえば、ユーザ グループ A がユーザ グループ B を継承すると、ユーザ グループ A のタスク マップは A と B の集合になります。 循環インクルードは検出され、拒否されます。 ユーザ グループは、root-system ユーザ、root-sdr ユーザ、netadmin ユーザなどの事前定義されたグループからプロパティを継承できません。 継承元のユーザグループが変更されると、継承元のグループ内にただちに反映されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、purchasing ユーザ グループが sales ユーザ グループのプロパティを継承できるようにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup purchasing
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup sales
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	タスク グループ コンフィギュレーション モードでタスク グループの説明を作成するか、ユーザ グループ コンフィギュレーション モードでユーザ グループの説明を作成します。
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。
usergroup, （133 ページ）	一連のタスク グループに関連付けるように、ユーザ グループを設定します。

key（RADIUS）

ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **key**（**RADIUS**）コマンドを使用します。

key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

no key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
clear-text-key	暗号化されていない（クリアテキスト）ユーザ パスワードを指定します。

コマンド デフォルト

サブモードの **key** コマンドでは、定義されている場合はデフォルトでグローバル コンフィギュレーション モードの **radius-server key** コマンドが使用されます。 グローバル キーも定義されていない場合、この設定は完了しません。

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、暗号キーを anykey に設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# key anykey
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の RADIUS サーバ ホストを別個のリストにグループ化します。
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。

key（TACACS+）

AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定するには、TACACS ホスト コンフィギュレーション モードで**key（TACACS+）**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。

key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

no key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
auth-key	AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。

コマンド デフォルト

なし

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

TACACS+ パケットは、キーを使って暗号化されます。このキーは、TACACS+ デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、**tacacs-server key** コマンドで設定されているキーが上書きされます。

このキーを使用して、TACACS+ から発信されるパケットを暗号化します。パケットが正しく復号化されるよう、このキーは外部 TACACS+ サーバに設定されているキーと一致している必要があります。 一致しない場合は、復号化に失敗します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、暗号キーを anykey に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# key anykey
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。
tacacs-server key, （117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+通信に使用される認証および暗号キーをグローバルに設定します。

login authentication

ログインに対する認証、許可、アカウンティング（AAA）の認証をイネーブルにするには、回線テンプレート コンフィギュレーション モードで **login authentication** コマンドを使用します。 デフォルトの認証設定に戻すには、このコマンドの **no** 形式を使用します。

login authentication {**default**| *list-name*}

no login authentication

構文の説明

default	**aaa authentication login** コマンドで設定されている、デフォルトの AAA 認証方式リストです。
list-name	認証に使用する方式リストの名前です。 このリストは、**aaa authentication login** コマンドで指定します。

コマンド デフォルト

このコマンドでは、**aaa authentication login** コマンドで設定されたデフォルトが使用されます。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

login authentication コマンドは、ログイン時に試行される AAA 認証方式のリスト名を指定した AAA と一緒に使用する、回線単位のコマンドです。

注意 **aaa authentication login** コマンドで設定されていない *list-name* 値を使用した場合、その設定は拒否されます。

login authentication コマンドの **no** 形式を入力すると、このコマンドに **default** キーワードを使用した場合と同じ結果になります。

このコマンドを実行する前に、**aaa authentication login** グローバル コンフィギュレーション コマンドを使用して認証プロセスのリストを作成します。

タスク ID

タスク ID	操作
aaa	read, write
tty-access	read, write

例

次に、回線テンプレート *template1* にデフォルトの AAA 認証を使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template1
RP/0/RSP0/CPU0:router(config-line)# login authentication default
```

次に、回線テンプレート *template2* に AAA 認証リスト *list1* を使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template2
RP/0/RSP0/CPU0:router(config-line)# login authentication list1
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを作成します。

password（AAA）

ユーザにログインパスワードを作成するには、ユーザ名コンフィギュレーションモードまたは回線テンプレート コンフィギュレーション モードで **password** コマンドを使用します。 パスワードを削除するには、このコマンドの **no** 形式を使用します。

password {**[0]**| **7** *password*}

no password {**0**| **7** *password*}

構文の説明

0	（任意）暗号化されていないクリアテキスト パスワードが続くことを指定します。
7	暗号化パスワードが続くことを指定します。
password	「lab」など、ログインするユーザが入力する暗号化されていないパスワードのテキストを指定します。 暗号化が設定されている場合、パスワードはユーザに表示されません。 最長で 253 文字まで入力できます。

コマンド デフォルト

パスワードは暗号化されていないクリア テキストです。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

パスワードは暗号化かクリア テキストのいずれかのタイプを指定できます。

パスワードで保護された回線で EXEC プロセスが開始されると、パスワードの入力を求められます。ユーザが正しいパスワードを入力すると、プロンプトが実行されます。ユーザがパスワードの入力に 3 回失敗すると、プロセスは終了し、端末がアイドル状態に戻ります。

パスワードは双方向に暗号化されており、復号化できるパスワードを必要とする PPP などのアプリケーションに使用する必要があります。

（注） **show running-config** コマンドに **0** オプションが使用されていると、クリアテキストのログインパスワードが常に暗号化形式で表示されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザに暗号化されていないパスワード *pwd1* を設定する例を示します。 **show** コマンドの出力には、パスワードが暗号化形式で表示されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# password 0 pwd1
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user1
 password 7 141B1309
```

関連コマンド

コマンド	説明
group（AAA）, （35 ページ）	ユーザをグループに追加します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、ユーザ グループを設定して一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーションモードにアクセスし、新しいユーザにユーザ名とパスワードを設定し、そのユーザのアクセス許可を付与します。

コマンド	説明
line	指定された回線テンプレートの回線テンプレート コンフィギュレーション モードが開始されます。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。

radius-server dead-criteria time

ルータがRADIUSサーバから有効なパケットを最後に受信してから、サーバにdeadマークが付くまでに最低限経過する必要のある時間を秒単位で指定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria time** コマンドを使用します。 設定された基準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。

radius-server dead-criteria time *seconds*

no radius-server dead-criteria time *seconds*

構文の説明

seconds	秒単位の時間です。 範囲は、1 ～ 120 秒です。 *seconds* 引数を設定していない場合、サーバのトランザクション レートによって 10 ～ 60 秒になります。 （注） 時間基準は、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

seconds 引数を設定していない場合、サーバのトランザクション レートによって 10 ～ 60 秒になります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

（注） **radius-server deadtime** コマンドの前に **radius-server dead-criteria time** コマンドを設定すると、**radius-server dead-criteria time** コマンドが実行されない場合があります。

ルータが起動してからパケットの受信がなく、タイムアウトになると、時間基準は満たされたものとして処理されます。

seconds 引数を指定していない場合、時間はデフォルトに設定されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server dead-criteria time** コマンドに対し、RADIUS サーバに dead マークを付けるための dead-criteria 条件として時間を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria time 5
```

関連コマンド

コマンド	説明
radius-server dead-criteria tries, （52 ページ）	ルータで連続何回タイムアウトが発生したら、RADIUS サーバに dead マークを付けるかを指定します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間の長さを分単位で定義します。
show radius dead-criteria, （99 ページ）	dead サーバの検出基準の情報を表示します。

radius-server dead-criteria tries

RADIUS サーバに dead マークが付くまでにルータで発生する連続タイムアウト回数を指定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria tries** コマンドを使用します。 設定された基準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。

radius-server dead-criteria *tries*

no radius-server dead-criteria *tries*

構文の説明

tries	1 ～ 100 のタイムアウト回数。 *tries* 引数を設定しない場合は、サーバのトランザクション レートと設定されている再送信回数によって、連続タイムタウト回数は 10 ～ 100 となります。 （注） 試行基準は、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

tries 引数を設定しない場合は、サーバのトランザクション レートと設定されている再送信回数によって、連続タイムタウト回数は 10 ～ 100 となります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバが認証とアカウンティングの両方を実行する場合、両方のパケットのタイプが数値に含まれます。 構造が適切でないパケットは、タイムアウトされたものとしてカウントされます。 最初の送信と再送信を含むすべての送信がカウントされます。

（注） **radius-server deadtime** コマンドの前に **radius-server dead-criteria tries** コマンドを設定すると、**radius-server dead-criteria tries** コマンドが実行されない場合があります。

tries 引数が指定されていない場合、試行回数はデフォルトに設定されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server dead-criteria tries** コマンドに対し、RADIUS サーバに dead マークを付けるための dead-criteria 条件として試行回数を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria tries 4
```

関連コマンド

コマンド	説明
radius-server dead-criteria time, （50 ページ）	ルータが RADIUS サーバから有効なパケットを最後に受信してから、サーバに dead マークが付くまでに経過する必要のある時間を秒単位で定義します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間の長さを分単位で定義します。
show radius dead-criteria, （99 ページ）	dead サーバの検出基準の情報を表示します。

radius-server deadtime

一部のサーバが使用できない場合に RADIUS の応答時間を短縮し、使用できないサーバがただちにスキップされるようにするには、グローバル コンフィギュレーション モードで **radius-server deadtime** コマンドを使用します。 デッドタイムを 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime *value*

no radius-server deadtime *value*

構文の説明

value	RADIUS サーバがトランザクション要求によってスキップされる時間を最長 1440（24 時間）まで分単位で表したものです。 指定できる範囲は 1 ～ 1440 です。 デフォルト値は 0 です。

コマンド デフォルト

デッド タイムは 0 に設定されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

他すべてのサーバに dead マークが付いている場合、また、ロールオーバー方式が存在しない場合以外は、指定の時間内に追加要求が発生すると、dead マークの付いた RADIUS サーバはスキップされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server deadtime** コマンドに対し、認証要求への応答に失敗した RADIUS サーバのデッドタイムを 5 分に指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server deadtime 5
```

radius-server host

RADIUS サーバ ホストを指定するには、グローバル コンフィギュレーション モードで **radius-server host** コマンドを使用します。 指定した RADIUS ホ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。

radius-server host {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no radius-server host {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

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）名です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対してユーザ データグラム プロトコル（UDP）宛先ポートを指定します。0 に設定すると、そのホストは認証に使用されません。 指定しない場合、ポート番号はデフォルトの 1645 になります。
acct-port *port-number*	（任意）アカウンティング要求に対して UDP 宛先ポートを指定します。0 に設定すると、そのホストはアカウンティングに使用されません。 指定しない場合、ポート番号はデフォルトの 1646 になります。
timeout *seconds*	（任意）ルータが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）です。 この設定によって、**radius-server timeout** コマンドのグローバル値は上書きされます。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。 1 ～ 1000 の範囲の値を入力します。 デフォルトは 5 です。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数です。 この設定によって、**radius-server retransmit** コマンドのグローバル設定は上書きされます。 再送信値が指定されていない場合は、グローバル値が使用されます。 1 ～ 100 の範囲の値を入力します。 デフォルトは 3 です。

key *string*	（任意）ルータと RADIUS サーバ間で使用される認証および暗号キーを指定します。 この設定によって、**radius-server key** コマンドのグローバル設定は上書きされます。 キー文字列を指定しない場合、グローバル値が使用されます。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に、**radius-server host** コマンド構文の最後の項目として設定します。これは、先頭のスペースは無視されますが、キーの中と末尾のスペースは使用されるためです。 キーにスペースを使用する場合は、引用符自体がキーの一部でない限り、そのキーを引用符で囲まないでください。

コマンド デフォルト

RADIUS ホストは指定されません。グローバルの**radius-server** コマンド値を使用します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

複数の **radius-server host** コマンドを使用して、複数のホストを指定できます。 Cisco IOS XR ソフトウェアにより、指定の順序でホストが検索されます。

ホスト固有のタイムアウト値、再送信値、またはキー値が指定されていない場合は、グローバル値が各ホストに適用されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、*host1* を RADIUS サーバとして設定し、アカウンティングと認証の両方にデフォルト ポートを使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host host1host1
```

次に、host1 という RADIUS ホストで認証要求の宛先ポートとしてポート 1612 を設定し、アカウンティング要求の宛先ポートとしてポート 1616 を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host host1 auth-port 1612 acct-port 1616
```

回線を入力するとすべてのポート番号がリセットされるため、ホストを指定し、1 つの回線のアカウンティング ポートと認証ポートを設定する必要があります。

次に、RADIUS サーバとして IP アドレス 172.29.39.46 のホストを設定し、許可ポートおよびアカウンティング ポートとしてポート 1612 と 1616 を使用し、タイムアウト値を 6、再送信値を 5 にそれぞれ設定して、さらに RADIUS サーバのキーと一致する暗号キーとして「rad123」を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host 172.29.39.46 auth-port 1612 acct-port
1616 timeout 6 retransmit 5 key rad123
```

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

次に、RADIUS サーバ host1 を認証には使用せずにアカウンティングに使用するように設定し、RADIUS サーバ host2 をアカウンティングには使用せずに認証に使用するように指定する例を示します。

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#radius-server host host1.example.com auth-port 0
RP/0/RSP0/CPU0:router(config)#radius-server host host2.example.com acct-port 0
```

関連コマンド

コマンド	説明
aaa accounting subscriber	アカウンティングの方式リストを作成します。
aaa authentication subscriber	認証の方式リストを作成します。
aaa authorization subscriber	許可の方式リストを作成します。
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定します。

コマンド	説明
radius-server timeout, （64 ページ）	サーバホストが応答するまでルータが待機する間隔を設定します。

radius-server key

ルータと RADIUS デーモン間のすべての RADIUS 通信に対して認証および暗号キーを設定するには、グローバル コンフィギュレーション モードで **radius-server key** コマンドを使用します。 キ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。

radius-server key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

no radius-server key

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
clear-text-key	暗号化されていない（クリアテキスト）共有キーを指定します。

コマンド デフォルト

認証および暗号キーはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

入力したキーは、RADIUS サーバで使用されるキーと一致する必要があります。 先頭のスペースはすべて無視されますが、キーの中間および末尾のスペースは使用できます。 キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、クリアテキスト キーを「samplekey」に設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 0 samplekey
```

次の例では、暗号化共有キーを「anykey」に設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 7 anykey
```

radius-server retransmit

Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定するには、グローバル コンフィギュレーション モードで **radius-server retransmit** コマンドを使用します。 再送信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。

radius-server retransmit *retries*

no radius-server retransmit

構文の説明

retries	再送信の最大試行回数です。 範囲は 1 ～ 100 です。 デフォルトは 3 です。

コマンド デフォルト

RADIUS サーバには 3 回まで、または応答が受信されるまで再送信されます。

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
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

RADIUS クライアントでは、すべてのサーバに対して再送信が試みられ、それぞれがタイムアウトになってから再送信カウントが増加します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、再送信カウンタ値を 5 回に指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server retransmit 5
```

関連コマンド

コマンド	説明
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。

radius-server timeout

タイムアウトになるまでルータがサーバ ホストの応答を待機する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 **radius-server timeout** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

radius-server timeout *seconds*

no radius-server timeout

構文の説明

seconds	タイムアウトの間隔を指定する秒数です。 範囲は、1 ～ 1000 です。

コマンド デフォルト

radius-server timeout のデフォルト値は 5 秒です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius-server timeout コマンドを使用して、タイムアウトになるまでルータがサーバ ホストの応答を待機する秒数を設定します。

タスク ID

タスク ID	操作
aaa	read, write

例

この例では、インターバル タイマーを 10 秒に変更します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server timeout 10
```

radius source-interface

すべての発信 RADIUS パケットに対して RADIUS が指定されたインターフェイスまたはサブインターフェイスの IP アドレスを使用するようにするには、グローバル コンフィギュレーション モードで **radius source-interface** コマンドを使用します。 指定されたインターフェイスだけがデフォルトにならないようにし、すべての発信 RADIUS パケットに使用されないようにするには、このコマンドの **no** 形式を使用します。

radius source-interface *interface* [**vrf** *vrf_name*]

no radius source-interface *interface*

構文の説明

interface-name	RADIUS がすべての発信パケットに使用するインターフェイスの名前です。
vrf *vrf-id*	割り当てられている VRF の名前を指定します。

コマンド デフォルト

特定のソース インターフェイスが設定されていない場合、インターフェイスがダウン状態にある場合、またはインターフェイスに IP アドレスが設定されていない場合は、IP アドレスが自動的に選択されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius source-interface コマンドを使用して、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスを設定します。インターフェイスまたはサブインターフェイスがアップ状態である限り、このアドレスが使用されます。 このように、RADIUS

サーバでは IP アドレスのリストを保持する代わりに、すべてのネットワーク アクセス クライアントに対して 1 つの IP アドレス エントリを使用できます。

指定されたインターフェイスまたはサブインターフェイスには、IP アドレスが関連付けられている必要があります。指定のインターフェイスまたはサブインターフェイスにIPアドレスが設定されていないか、そのインターフェイスがダウン状態にある場合、RADIUS はデフォルトに戻ります。これを回避するには、インターフェイスまたはサブインターフェイスにIPアドレスを追加するか、そのインターフェイスをアップ状態にします。

特に、ルータに多数のインターフェイスやサブインターフェイスがあり、特定のルータからのすべての RADIUS パケットに同じ IP アドレスが含まれるようにする場合は、**radius source-interface** コマンドが役立ちます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、すべての発信 RADIUS パケットに対して RADIUS がサブインターフェイス s2 の IP アドレスを使用するようにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius source-interface Loopback 10 vrf vrf-1
```

retransmit（RADIUS）

サーバが応答しない場合や、応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **retransmit** コマンドを使用します。

retransmit *retries*

no retransmit *retries*

構文の説明

retries	*retries* 引数は、再送信値を指定します。 範囲は 1 ～ 100 です。 再送信値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

デフォルト値は 3 です。

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、再送信値を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
```

```
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# retransmit 100
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の RADIUS サーバ ホストを別個のリストにグループ化します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。

secret

Message Digest 5（MD5）で暗号化されたシークレットを設定して暗号化されたユーザ名に関連付けるには、ユーザ名コンフィギュレーション モードまたは回線テンプレート コンフィギュレーション モードで **secret** コマンドを使用します。 セキュア シークレットを削除するには、このコマンドの **no** 形式を使用します。

secret {**[0]** *secret-login*| **5** *secret-login*}

no secret {**0**| **5**} *secret-login*

構文の説明

0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 MD5 暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。 それ以外の場合、パスワードは暗号化されません。
5	暗号化された MD5 パスワード（シークレット）が続くことを指定します。
secret-login	ユーザのログイン ID と一緒に MD5 で暗号化されたパスワードとして保存される、ユーザが入力する英数字のテキスト文字列です。 最長で 253 文字まで入力できます。 （注） 入力する文字は、MD5 暗号化標準に準拠する必要があります。

コマンド デフォルト

パスワードは指定されません。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

Cisco IOS XR ソフトウェアでは、ログインに使用するユーザ名とパスワードに Message Digest 5（MD5）暗号化を設定できます。 MD5 暗号化は、暗号化されたパスワードの逆送信を不可能にする一方向ハッシュ関数であり、強力な暗号化保護を可能にします。 MD5 暗号化を使用すると、クリアテキスト パスワードを取得できません。 したがって、MD5 で暗号化されたパスワードは、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）など、クリアテキスト パスワードの取得を必要とするプロトコルと一緒には使用できません。

セキュア シークレット ID のタイプは暗号化（5）とクリア テキスト（0）のいずれかを指定できます。 0 も 5 も選択しなかった場合、入力したクリアテキスト パスワードは暗号化されません。

パスワードで保護された回線で EXEC プロセスが開始されると、シークレットの入力を求めるプロンプトが表示されます。 ユーザが正しいシークレットを入力すると、プロンプトが実行されます。 ユーザがシークレットの入力に 3 回失敗すると、端末はアイドル状態に戻ります。

シークレットは一方向の暗号化なので、復号可能なシークレットを必要としないログイン アクティビティに使用します。

MD5 パスワードの暗号化がイネーブルであることを確認するには、**show running-config** コマンドを使用します。 コマンド出力に「username name secret 5」という行が表示された場合は、拡張パスワード セキュリティがイネーブルです。

（注） **0** オプションを使用して暗号化されていないパスワードを指定すると、**show running-config** コマンドを実行してもログイン パスワードはクリアテキストで表示されません。 「例」の項を参照してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ *user2* にクリアテキスト シークレット「lab」を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user2
RP/0/RSP0/CPU0:router(config-un)# secret 0 lab
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user2
 secret 5 $1$DTmd$q7C6fhzje7Cc7Xzmu2Frx1
!
end
```

関連コマンド

コマンド	説明
group（AAA）， （35 ページ）	ユーザをグループに追加します。

コマンド	説明
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、ユーザ グループを設定して一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーション モードにアクセスし、新しいユーザにユーザ名とパスワードを設定し、そのユーザのアクセス許可を付与します。

server（RADIUS）

特定の RADIUS サーバを定義済みのサーバ グループに関連付けるには、RADIUS サーバグループ コンフィギュレーション モードで **server** コマンドを使用します。 関連付けられたサーバをサーバ グループから削除するには、このコマンドの **no** 形式を使用します。

server {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

no server {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポートを指定します。 *port-number* 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。 デフォルトは 1645 です。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 *port-number* 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。 デフォルトは 1646 です。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

RADIUS サーバグループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server コマンドを使用して、特定の RADIUS サーバを定義済みのサーバ グループに関連付けることができます。

サーバを識別する方法は、AAA サービスを提供する方法に応じて 2 種類あります。 IP アドレスを使用して単純にサーバを識別する方法と、オプションの **auth-port** キーワードおよび **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを識別する方法があります。

オプションのキーワードを使用すると、ネットワーク アクセス サーバにより、IP アドレスと特定の UDP ポート番号に基づいてグループ サーバに関連付けられている RADIUS セキュリティ サーバおよびホスト インスタンスが識別されます。 IP アドレスと UDP ポート番号の組み合わせによって一意の ID を作成し、特定の AAA サービスを提供する RADIUS ホスト エントリとして各ポートを個々に定義できます。 たとえば、同一の RADIUS サーバの 2 つの異なるホスト エントリを同一のサービス（アカウンティングなど）に対して設定すると、2 番目に設定したホスト エントリは最初のホスト エントリをバックアップする自動スイッチオーバーとして機能します。 この場合、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します （試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、同一のサービス、つまり認証とアカウンティングに設定されている同一の RADIUS サーバ上の 2 つの異なるホスト エントリを使用する例を示します。 2 番目に設定されているホスト エントリは、最初のホスト エントリをバックアップするスイッチオーバーとして機能します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
```

関連コマンド

コマンド	説明
aaa group server radius, （22 ページ）	複数の RADIUS 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。

コマンド	説明
deadtime（サーバグループ コンフィギュレーション），（31 ページ）	RADIUS サーバ グループ レベルでデッドタイム値を設定します。
server-private（RADIUS），（78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

server（TACACS+）

特定のTACACS+サーバを定義済みのサーバ グループに関連付けるには、TACACS+サーバグループ コンフィギュレーション モードで**server**コマンドを使用します。 関連付けられたサーバをサーバ グループから削除するには、このコマンドの **no** 形式を使用します。

server {*hostname*| *ip-address*}

no server {*hostname*| *ip-address*}

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	サーバ ホストの IP アドレスです。

コマンド デフォルト

なし

コマンド モード

TACACS+ サーバグループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク IDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server コマンドを使用して、特定の TACACS+ サーバを定義済みのサーバ グループに関連付けることができます。 サーバは設定時にアクセス可能である必要はありません。 あとで、認証、許可、アカウンティング（AAA）の設定に使用される方式リストから、設定済みのサーバ グループを参照できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、IP アドレス 192.168.60.15 の TACACS+ サーバをサーバ グループ tac1 に関連付ける例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tac1
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の TACACS+ サーバ ホストを別個のリストにグループ化します。

server-private（RADIUS）

グループ サーバに対して、プライベート RADIUS サーバの IP アドレスを設定するには、RADIUS サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを AAA グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対するユーザデータグラムプロトコル（UDP）宛先ポートを指定します。 *port-number* 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。 デフォルト値は 1645 です。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 *port-number* 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。 デフォルト値は 1646 です。
timeout *seconds*	（任意）再送信するまでにルータが RADIUS サーバの応答を待機する秒数を指定します。 この設定によって、**radius-server timeout** コマンドのグローバル値は上書きされます。タイムアウト値が指定されていない場合は、グローバル値が使用されます。 *seconds* 引数は、タイムアウト値を秒単位で指定します。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 この設定によって、**radius-server transmit** コマンドのグローバル設定は上書きされます。 *retries* 引数は、再送信値を指定します。 範囲は 1 ～ 100 です。 再送信値が指定されていない場合は、グローバル値が使用されます。

key *string*	（任意）ルータとRADIUSサーバ上で稼働するRADIUSデーモン間で使用される認証および暗号キーを指定します。この設定によって、**radius-server key** コマンドのグローバル設定は上書きされます。キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

RADIUS サーバグループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。VRFインスタンス間ではIPアドレスの重複が可能です。プライベート サーバ（プライベート アドレスを持つサーバ）はサーバ グループ内で定義して、他のグループからは非表示のままにすることができます。一方、グローバル プール（デフォルトの RADIUS サーバグループなど）内のサーバは、IPアドレスとポート番号を使って参照できます。このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

auth-port キーワードと **acct-port** キーワードのどちらを使用しても、RADIUS サーバグループ プライベート コンフィギュレーション モードが開始されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、group1 RADIUS グループ サーバを定義して、これにプライベート サーバを関連付け、RADIUS サーバグループ プライベート コンフィギュレーション モードを開始する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# exit
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)#
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	複数の RADIUS 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。
radius-server key, （60 ページ）	ルータと RADIUS デーモン間のすべての RADIUS 通信に対する認証および暗号キーを設定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定します。
radius-server timeout, （64 ページ）	タイムアウトになるまでにルータがサーバ ホストの応答を待機する間隔を設定します。
key（RADIUS）, （41 ページ）	ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

server-private（TACACS+）

グループ サーバに対して、プライベートTACACS+サーバのIPアドレスを設定するには、TACACS+サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを AAA グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*hostname*| *ip-address*} [**port** *port-number*] [**timeout** *seconds*] [**key** *string*]

no server-private {*hostname*| *ip-address*}

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	TACACS+ サーバ ホストの IP アドレスです。
port *port-number*	（任意）サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。 有効なポート番号の範囲は 1 ～ 65535 です。
timeout *seconds*	（任意）認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を秒で指定します。 このオプションによって、**tacacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。 範囲は 1 ～ 1000 です。 デフォルト値は 5 です。
key *string*	（任意）ルータと TACACS+ サーバ上で稼働する TACACS+ デーモン間で使用される認証および暗号キーを指定します。 このキーは **tacacs-server key** コマンドのグローバル設定を書き換えます。 キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

port-name 引数が指定されていない場合、標準ポート 49 がデフォルトで使用されます。

seconds 引数が指定されていない場合、5 秒がデフォルトで使用されます。

コマンド モード

TACACS+ サーバグループ 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
リリース 4.1.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 VRF インスタンス間では IP アドレスの重複が可能です。 プライベート サーバ（プライベート アドレスを持つサーバ）はサーバ グループ内で定義して、他のグループからは非表示のままにすることができます。一方、グローバル プール（デフォルトの TACACS+ サーバ グループなど）内のサーバは、IP アドレスとポート番号を使って参照できます。 このように、サーバ グループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、myserver TACACS+ グループ サーバを定義して、プライベート サーバを関連付け、TACACS+ サーバ グループ プライベート コンフィギュレーション モードを開始する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 key a_secret
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 port 51
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)# exit
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 port 300
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)#
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	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。
tacacs-server key, （117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+通信に使用される認証および暗号キーを設定します。
tacacs-server timeout, （119 ページ）	タイムアウトになるまでにルータがサーバ ホストの応答を待機する間隔を設定します。

コマンド	説明
key（TACACS+），（43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
timeout（TACACS+），（129 ページ）	認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。
vrf（TACACS+），（143 ページ）	AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照情報を設定します。

show aaa

インターネットキー交換（IKE）セキュリティ プロトコル グループ、ユーザ グループ、ローカル ユーザ、ログイン トレース、タスク グループに関する情報を表示したり、システム内のすべての IKE グループ、ユーザ グループ、ローカル ユーザ、タスク グループに関連付けられたすべてのタスク ID を一覧表示したり、指定の IKE グループ、ユーザ グループ、ローカル ユーザ、タスク グループのすべてのタスク ID を一覧表示したりするには、EXEC モードで **show aaa コマンド**を使用します。

show aaa {**ikegroup** *ikegroup-name*| **login trace**| **usergroup** [*usergroup-name*]| **trace**| **userdb** [*username*]| **task supported**| **taskgroup** [**root-lr**| **netadmin**| **operator**| **sysadmin**| **root-system**| **service-admin**| **cisco-support**| **t** *askgroup-name*]}

構文の説明

ikegroup	すべての IKE グループの詳細を表示します。
ikegroup-name	（任意）詳細が表示される IKE グループです。
login trace	ログイン サブシステムに関するトレース データを表示します。
usergroup	すべてのユーザ グループの詳細を表示します。
root-lr	（任意）ユーザグループ名です。
netadmin	（任意）ユーザグループ名です。
operator	（任意）ユーザグループ名です。
sysadmin	（任意）ユーザグループ名です。
root-system	（任意）ユーザグループ名です。
cisco-support	（任意）ユーザグループ名です。
usergroup-name	（任意）ユーザグループ名です。
trace	AAA サブシステムに関するトレース データを表示します。
userdb	すべてのローカル ユーザと各ユーザが属するユーザグループの詳細を表示します。
username	（任意）詳細を表示する対象のユーザです。
task supported	使用可能なすべての AAA タスク ID を表示します。

taskgroup	すべてのタスク グループの詳細を表示します。 （注） taskgroup のキーワードについては、オプションの usergroup name キーワード リストを参照してください。
taskgroup-name	（任意）詳細を表示する対象のタスク グループ。

コマンド デフォルト

引数を入力しない場合は、すべてのユーザ グループ、すべてのローカル ユーザ、またはすべてのタスク グループの詳細が表示されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システム内のすべての IKE グループ、ユーザ グループ、ローカル ユーザ、またはタスク グループの詳細を表示するには、**show aaa** コマンドを使用します。 オプションの *ikegroup-name*、*usergroup-name*、*username*、または *taskgroup-name* 引数を使用して、それぞれ指定の IKE グループ、ユーザ グループ、ユーザ、またはタスク グループの詳細を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**ikegroup** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa ikegroup

IKE Group ike-group
        Max-Users = 50
IKE Group ikeuser
        Group-Key = test-password
        Default Domain = cisco.com
IKE Group ike-user
```

次に、**usergroup** コマンドを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa usergroup operator

User group 'operator'
  Inherits from task group 'operator'
User group 'operator' has the following combined set
of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

次に、タスク グループ netadmin に対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa taskgroup netadmin

Task group 'netadmin'

Task group 'netadmin' has the following combined set
  of task IDs (including all inherited groups):

Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ
Task:                 dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:    ethernet-services  : READ
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:                l2vpn  : READ    WRITE    EXECUTE    DEBUG
Task:                   li  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ
Task:             mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:          mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:            multicast  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ
Task:              pos-dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ                                (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ                                (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、オペレータに対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク グループ operator には、次に示すように、継承されるすべてのグループを含む一連のタスク ID が組み合わされています。

```
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

次に、ルート システムに対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク グループ root system には次に示すように、継承されるすべてのグループを含む一連のタスク ID が組み合わされています。

```
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa acl  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  admin atm  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services           bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp boot  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot bundle  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle    cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt services  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services           crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                crypto   diag  : READ    WRITE    EXECUTE    DEBUG
Task:                  diag  drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               drivers ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access     fabric  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem          fr  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  host-services  : READ    WRITE    EXECUTE    DEBUG
Task:         host-services           hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  interface  : READ    WRITE    EXECUTE    DEBUG
Task:            interface inventory  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:           ip-services          ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                  ipv4 ipv6  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:                ipv6 isis  : READ    WRITE    EXECUTE    DEBUG
Task:                isis  logging  : READ    WRITE    EXECUTE    DEBUG
Task:             logging     lpts  : READ    WRITE    EXECUTE    DEBUG
Task:                lpts  monitor  : READ    WRITE    EXECUTE    DEBUG
Task:             monitor mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-ldp static  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-static te  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te multicast  : READ    WRITE    EXECUTE    DEBUG
Task:             multicast netflow  : READ    WRITE    EXECUTE    DEBUG
Task:             netflow network  : READ    WRITE    EXECUTE    DEBUG
Task:             network     ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                ospf ouni  : READ    WRITE    EXECUTE    DEBUG
Task:                ouni pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:            pkg  pos-mgmt dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                 ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                 qos  : READ    WRITE    EXECUTE    DEBUG
Task:                 rib  : READ    WRITE    EXECUTE    DEBUG
Task:                 rip  : READ    WRITE    EXECUTE    DEBUG
Task:            root-lr  : READ    WRITE    EXECUTE    DEBUG
Task:         root-system  : READ    WRITE    EXECUTE    DEBUG
Task:           route-map  : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                snmp  : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:              static  : READ    WRITE    EXECUTE    DEBUG
Task:              sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:              system  : READ    WRITE    EXECUTE    DEBUG
Task:           transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:              tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:           universal  : READ    WRITE    EXECUTE    DEBUG
Task:                vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、**userdb** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa userdb

Username lab (admin plane)
User group root-system
User group cisco-support
Username acme
User group root-system
```

次に、**task supported** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク ID はアルファベット順に表示されます。

```
RP/0/RP0/CPU0:router# show aaa task supported

aaa
acl
admin
atm
basic-services
bcdl
bfd
bgp
boot
bundle
cdp
cef
cisco-support
config-mgmt
config-services
crypto
diag
disallowed
drivers
eigrp
ext-access
fabric
fault-mgr
```

```
filesystem
firewall
fr
hdlc
host-services
hsrp
interface
inventory
ip-services
ipv4
ipv6
isis
logging
lpts
monitor
mpls-ldp
mpls-static
mpls-te
multicast
netflow
network
ospf
ouni
pkg-mgmt
pos-dpt
ppp
qos
rib
rip
User group root-systemlr
root-system
route-map
route-policy
sbc
snmp
sonet-sdh
static
sysmgr
system
transport
tty-access
tunnel
universal
vlan
vrrp
```

関連コマンド

コマンド	説明
show user, （108 ページ）	現在ログインしているユーザに対してイネーブルになっているタスク ID を表示します。

show radius

システムに設定されている RADIUS サーバの情報を表示するには、EXEC モードで **show radius** コマンドを使用します。

show radius

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバが設定されていない場合、出力は表示されません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius コマンドを使用して、設定されている RADIUS サーバごとの統計情報を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius

Global dead time: 0 minute(s)

Server: 1.1.1.1/1645/1646  is UP
  Timeout: 5 sec, Retransmit limit: 3
  Authentication:
    0 requests, 0 pending, 0 retransmits
```

```
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt

Server: 2.2.2.2/1645/1646  is UP
  Timeout: 10 sec, Retransmit limit: 3
  Authentication:
    0 requests, 0 pending, 0 retransmits
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *2*：*show radius* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。
Timeout	タイムアウトになるまでにルータがサーバホストの応答を待機する秒数です。
Retransmit limit	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数です。

関連コマンド

コマンド	説明
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数を指定します。
radius-server timeout, （64 ページ）	サーバホストが応答するまでルータが待機する間隔を設定します。

show radius accounting

RADIUS アカウンティング サーバとポートの情報および詳細な統計情報を取得するには、EXEC モードで **show radius accounting** コマンドを使用します。

show radius accounting

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバがルータに設定されていない場合、出力は空になります。 カウンタ（要求や保留など）に対するデフォルト値の場合、RADIUS サーバは定義されただけでまだ使用されていないため、値はすべてゼロになります。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、サーバ単位で表示される **show radius accounting** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius accounting

Server: 12.26.25.61, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

```
Server: 12.26.49.12, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.38.28.18, port: 29199
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *3*：*show radius accounting* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート、アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
show radius authentication, （95 ページ）	RADIUS 認証サーバおよびポートの情報と詳細な統計情報を取得します。

show radius authentication

RADIUS 認証サーバおよびポートの情報と詳細な統計情報を取得するには、EXEC モードで **show radius authentication** コマンドを使用します。

show radius authentication

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバがルータに設定されていない場合、出力は空になります。 カウンタ（要求や保留など）に対するデフォルト値の場合、RADIUS サーバは定義されただけでまだ使用されていないため、値はすべてゼロになります。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius authentication** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius authentication

Server: 12.26.25.61, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

```
Server: 12.26.49.12, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.38.28.18, port: 21099
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *4*：*show radius authentication* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート、アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
show radius accounting, （93 ページ）	RADIUS アカウンティング サーバおよびポートの情報と詳細な統計情報を取得します。

show radius client

Cisco IOS XR ソフトウェアで RADIUS クライアントの一般情報を取得するには、EXEC モードで **show radius client** コマンドを使用します。

show radius client

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

カウンタ（無効なアドレスなど）のデフォルト値は 0 です。 Network Access Server（NAS; ネットワーク アクセス サーバ）の ID は、ルータで定義されているホスト名です。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius client コマンドを実行すると、NAS に認識されないサーバなど、無効な RADIUS サーバから受信した認証およびアカウンティングの応答が表示されます。 また、**show radius client** コマンドによって、RADIUS 認証クライアント、アカウンティング クライアント、またはその両方のホスト名または NAS ID が表示されます。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius client** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius client
```

```
Client NAS identifier:                          miniq
Authentication responses from invalid addresses:      0
Accounting responses from invalid addresses:          0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *5*：*show radius client* フィールドの説明

フィールド	説明
Client NAS identifier	RADIUS 認証クライアントの NAS ID を識別します。

関連コマンド

コマンド	説明
server（RADIUS），（73 ページ）	特定の RADIUS サーバを定義済みのサーバ グループに関連付けます。
show radius，（91 ページ）	システムに設定されている RADIUS サーバの情報を表示します。

show radius dead-criteria

デッド サーバの検出基準に関する情報を取得するには、EXEC モードで **show radius dead-criteria** コマンドを使用します。

show radius dead-criteria host *ip-addr* [**auth-port** *auth-port*] [**acct-port** *acct-port*]

構文の説明

host *ip-addr*	設定されている RADIUS サーバの名前または IP アドレスを指定します。
auth-port *auth-port*	（任意）RADIUS サーバに対する認証ポートを指定します。 デフォルト値は 1645 です。
acct-port *acct-port*	（任意）RADIUS サーバに対するアカウンティング ポートを指定します。 デフォルト値は 1646 です。

コマンド デフォルト

時間と試行回数のデフォルト値は、1 つの値に固定されません。時間の場合は 10 ～ 60 秒、試行回数の場合は 10 ～ 100 回の範囲で算出されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius dead-criteria** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius dead-criteria host 12.26.49.12 auth-port 11000 acct-port
 11001

Server: 12.26.49.12/11000/11001
Dead criteria time: 10 sec (computed) tries: 10 (computed)
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *6*：*show radius dead-criteria* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。
Timeout	タイムアウトになるまでにルータがサーバホストの応答を待機する秒数です。
Retransmits	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数です。

関連コマンド

コマンド	説明
radius-server dead-criteria time, （50 ページ）	RADIUS サーバに dead マークを付けるための 1 つまたは両方の基準を強制的に使用します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間を分単位で定義します。

show radius server-groups

システムに設定されているRADIUSサーバ グループの情報を表示するには、EXECモードで**show radius server-groups** コマンドを使用します。

show radius server-groups [*group-name* **[detail]**]

構文の説明

group-name	（任意）サーバ グループの名前です。プロパティが表示されます。
detail	（任意）すべてのサーバ グループのプロパティを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius server-groups コマンドを使用して、グループ名、グループ内のサーバ数、名前付きサーバ グループ内のサーバのリストなど、設定されている各 RADIUS サーバ グループの情報を表示します。 設定されているすべての RADIUS サーバのグローバル リストも、認証およびアカウンティングのポート番号と一緒に表示されます。

タスク ID

タスク ID	操作
aaa	read

例

このグループに対してグループ レベルのデッドタイムが定義されていない場合、継承されるグローバル メッセージが表示されます。グループ レベルのデッドタイム値が定義されている場合はその値が表示され、このメッセージは省略されます。 次に、**show radius server-groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups

Global list of servers
  Contains 2 server(s)
    Server 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp1' has 2 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 2 server(s)
    Server 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp-priv' has 1 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
    Server 3.3.3.3/1645/1646 [private]
```

次に、グループ「radgrp1」に含まれるすべてのサーバ グループのプロパティの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp1 detail

Server group 'radgrp1' has 2 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 2 server(s)
      Server 1.1.1.1/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
      Server 2.2.2.2/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

次に、グループ「raddgrp-priv」に含まれるすべてのサーバ グループのプロパティの詳細な出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp-priv detail

Server group 'radgrp-priv' has 1 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 1 server(s)
      Server 3.3.3.3/1645/1646 [private]
```

```
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *7*：*show radius server-groups* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
vrf（RADIUS），（141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

show tacacs

システムに設定されている TACACS+ サーバの情報を表示するには、EXEC モードで **show tacacs** コマンドを使用します。

show tacacs

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show tacacs コマンドを使用して、設定されている各 TACACS+ サーバの統計情報を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show tacacs** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show tacacs

Server:1.1.1.1/21212 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

Server:2.2.2.2/21232 opens=0 closes=0 aborts=0 errors=0
```

```
        packets in=0 packets out=0
        status=up single-connect=false
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *8*：*show tacacs* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス。
opens	外部サーバに対して開くソケットの数です。
closes	外部サーバに対して閉じるソケットの数です。
aborts	途中で中断された TACACS+ 要求の数です。
errors	外部サーバからのエラー応答の数です。
packets in	外部サーバから受信した TCP パケットの数です。
packets out	外部サーバに送信された TCP パケットの数です。

show tacacs server-groups

システムに設定されている TACACS+ サーバ グループの情報を表示するには、EXEC モードで **show tacacs server-groups** コマンドを使用します。

show tacacs server-groups

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show tacacs server-groups コマンドを使用して、グループ名、グループ内のサーバ数、名前付きサーバ グループ内のサーバのリストなど、設定されている各 TACACS+ サーバ グループの情報を表示します。 設定されているすべての TACACS+ サーバのグローバル リストも表示されます。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show tacacs server-groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show tacacs server-groups

Global list of servers
  Server 12.26.25.61/23456
  Server 12.26.49.12/12345
```

```
  Server 12.26.49.12/9000
  Server 12.26.25.61/23432
  Server 5.5.5.5/23456
  Server 1.1.1.1/49
Server group 'tac100' has 1 servers
Server 12.26.49.12
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *9*：*show tacacs server-groups* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス。

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

show user

現在ログインしているユーザに関連付けられているすべてのユーザ グループとタスク ID を表示するには、EXEC モードで **show user** コマンドを使用します。

show user [**all**| **authentication**| **group**| **tasks**]

構文の説明

all	（任意）現在ログインしているユーザに関するすべてのユーザ グループとタスク ID を表示します。
authentication	（任意）現在ログインしているユーザの認証方式パラメータを表示します。
group	（任意）現在ログインしているユーザに関連付けられているユーザ グループを表示します。
tasks	（任意）現在ログインしているユーザに関連付けられているタスク ID を表示します。 **tasks** キーワードを使用した出力例では、予約済みのタスクが示されています。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show user コマンドを使用して、現在ログインしているユーザに関連付けられているすべてのユーザ グループとタスク ID を表示します。

タスク ID

タスク ID	操作
none	—

例

次に、**show user** コマンドの認証方式パラメータの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user authentication

local
```

次に、**show user** コマンドのグループの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user group

root-system
```

次に、**show user** コマンドのグループとタスクに関するすべての情報の出力例を示します。

```
RP/0/RSP0/CPU0:router# show user all
Username: lab
Groups: root-system
Authenticated using method local
User lab has the following Task ID(s):

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                  admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                   ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                   qos  : READ    WRITE    EXECUTE    DEBUG
Task:                   rib  : READ    WRITE    EXECUTE    DEBUG
Task:                   rip  : READ    WRITE    EXECUTE    DEBUG
Task:               root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:             route-map  : READ    WRITE    EXECUTE    DEBUG
Task:          route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                   sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                  snmp  : READ    WRITE    EXECUTE    DEBUG
Task:              sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:                 static  : READ    WRITE    EXECUTE    DEBUG
Task:                 sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:                 system  : READ    WRITE    EXECUTE    DEBUG
Task:              transport  : READ    WRITE    EXECUTE    DEBUG
Task:            tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:                 tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:              universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                   vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                   vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、**show user** コマンドのタスクの一覧とどのタスクが予約されているかの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user tasks

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:           interface  : READ    WRITE    EXECUTE    DEBUG
Task:           inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:              pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:           root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

関連コマンド

コマンド	説明
show aaa, （85 ページ）	選択されているユーザ グループ、ローカル ユーザ、またはタスク グループに関するタスク マップを表示します。

single-connection

単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信するには、TACACS ホスト コンフィギュレーション モードで **single-connection** コマンドを使用します。 別個の接続を使用するすべての新しいセッションに対して単一の TCP 接続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。

single-connection

no single-connection

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

デフォルトでは、セッションごとに別個の接続が使用されます。

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

single-connection コマンドを使用すると、複数の TCP 接続を使用してサーバに要求が送信された場合に可能な数よりも、多くの TACACS 操作を TACACS+ サーバで処理することができます。

この機能をイネーブルにするには、使用されている TACACS+ サーバが単一接続モードをサポートしている必要があります。それ以外の場合はネットワーク アクセス サーバと TACACS+ サーバ間の接続がロックアップするか、非認証のエラーが発生します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、TACACS+ サーバ（IP アドレス 209.165.200.226）との単一の TCP 接続を設定し、すべての認証、許可、アカウンティング要求でこの TCP 接続が使用されるようにする例を示します。この設定は、TACACS+ サーバも単一接続モードで設定されている場合に限り機能します。TACACS+ サーバを単一接続モードで設定する方法については、各サーバのマニュアルを参照してください。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# single-connection
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs-server host

TACACS+ホストサーバを指定するには、グローバル コンフィギュレーション モードで**tacacs-server host** コマンドを使用します。 指定された名前または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。

tacacs-server host host-name [**port port-number**] [**timeout seconds**] [**key** [**0**| **7**] **auth-key**] **[single-connection]**

no tacacs-server host *host-name* [*port port-number*]

構文の説明

host-name	TACACS+ サーバのホスト名またはドメイン名または IP アドレス。
port *port-number*	（任意）サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。 有効なポート番号の範囲は 1 ～ 65535 です。
timeout *seconds*	（任意）認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。 この設定によって、**acacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。 有効なタイムアウトの範囲は、1 ～ 1000 秒です。 デフォルトは 5 です。
key [**0** | **7**] *auth-key*	（任意）AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。 TACACS+ パケットは、このキーを使って暗号化されます。 このキーはTACACS+デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、**tacacs-server key** コマンドで設定されているキーが上書きされます。 （任意）**0**の入力により、暗号化されていない（クリアテキスト）キーが続くことを指定します。 （任意）**7** の入力により、暗号キーが続くことを指定します。 *auth-key* 引数は、AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。
single-connection	（任意）単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信します。 デフォルトでは、セッションごとに別個の接続が使用されます。

コマンド デフォルト

TACACS+ ホストは指定されません。

port-name 引数が指定されていない場合、標準ポート 49 がデフォルトで使用されます。
seconds 引数が指定されていない場合、5 秒がデフォルトで使用されます。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

key キーワードには文字列（改行のないテキスト）ではなく行（改行付きのテキスト）が使用されるため、このキーワードは最後に入力する必要があります。 ユーザが Enter キーを押すまでのテキストと改行は、キーの一部として使用されます。

複数の **tacacs-server host** コマンドを使用して、追加のホストを指定できます。 Cisco IOS XR ソフトウェアでは、指定の順序でホストが検索されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、IP アドレス 209.165.200.226 の TACACS+ ホストを指定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)#
```

次に、**show run** コマンドによって、**tacacs-server host** コマンドのデフォルト値を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show run

Building configuration...
!! Last configuration change at 13:51:56 UTC Mon Nov 14 2005 by lab
!
tacacs-server host 209.165.200.226 port 49
 timeout 5
!
```

次に、ルータがポート番号 51 の TACACS+ サーバ ホスト host1 を参照するように指定する例を示します。 この接続における要求のタイムアウト値は 30 秒で、暗号キーは a_secret です。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host host1 port 51 timeout 30 key a_secret
```

関連コマンド

コマンド	説明
key（TACACS+）, （43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
single-connection, （112 ページ）	単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信します。
tacacs-server key, （117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+通信に使用される認証および暗号キーをグローバルに設定します。
tacacs-server timeout, （119 ページ）	ルータがサーバホストの応答を待機する間隔をグローバルに設定します。
timeout（TACACS+）, （129 ページ）	認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。

tacacs-server key

ルータと TACACS+ デーモン間のすべての TACACS+ 通信に対して認証および暗号キーを設定するには、グローバル コンフィギュレーション モードで **tacacs-server key** コマンドを使用します。キ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。

tacacs-server key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

no tacacs-server key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
auth-key	AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。

コマンド デフォルト

なし

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

入力するキー名は、TACACS+ デーモンで使用するキーと一致する必要があります。 キー名は、個別にキーが指定されていないすべてのサーバに適用されます。 すべての先頭のスペースは無視されますが、キーの中と後続のスペースは使用されます。 キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

キー名は、次のガイドラインに沿っている場合に限り有効です。

- *clear-text-key* 引数のあとに **0** キーワードを指定する必要があります。

- *encrypted-key* 引数のあとに **7** キーワードを指定する必要があります。

TACACS サーバ キーは、個々の TACACS サーバにキーが設定されていない場合に限り使用されます。個々のTACACSサーバにキーを設定すると、このグローバルなキー設定は常に上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、認証および暗号キーを key1 に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server key key1
```

関連コマンド

コマンド	説明
key（TACACS+）, （43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs-server timeout

サーバがサーバホストの応答を待機する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 **tacacs-server timeout** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

構文の説明

seconds	タイムアウトの間隔（秒単位）を指定する 1 ～ 1000 の整数です。

コマンド デフォルト

5 秒

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

この TACACS+ サーバのタイムアウトは、個々の TACACS+ サーバにタイムアウトが設定されていない場合に限り使用されます。 個々の TACACS+ サーバにタイムアウトの間隔が設定されている場合は常に、このグローバルなタイムアウト設定が上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、インターバル タイマーを 10 秒に変更する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server timeout 10
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs source-interface

すべての発信 TACACS+ パケットに対して選択したインターフェイスの送信元 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **tacacs source-interface** コマンドを使用します。 指定したインターフェイス IP アドレ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。

tacacs source-interface *type path-id* [**vrf** *vrf-id*]

no tacacs source-interface *type path-id*

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
vrf *vrf-id*	割り当てられている VRF の名前を指定します。

コマンド デフォルト

特定のソース インターフェイスが設定されていない場合、インターフェイスがダウン状態にある場合、またはインターフェイスにIPアドレスが設定されていない場合は、IPアドレスが自動的に選択されます。

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
リリース 3.7.2	このコマンドが追加されました。
リリース 4.1.0	**vrf** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius source-interface コマンドを使用して、すべての発信 TACACS+ パケットに対して指定するインターフェイスの IP アドレスを設定します。インターフェイスがアップ状態である限り、このアドレスが使用されます。 このように、TACACS+ サーバでは IP アドレスのリストを保持する代わりに、ネットワーク アクセス クライアントに関連付けられた 1 つの IP アドレス エントリを使用できます。

特に、ルータに多数のインターフェイスがあり、特定のルータからのすべての TACACS+ パケットに同一の IP アドレスが含まれるようにする場合は、このコマンドが役立ちます。

指定したインターフェイスに IP アドレスが設定されていないか、そのインターフェイスがダウン状態にある場合、TACACS+ は、送信元インターフェイスの設定が使用されないものとして処理します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、すべての発信 TACACS+ パケットに指定するインターフェイスの IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tacacs source-interface GigabitEthernet 0/0/0/29 vrf abc
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	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。

task

タスク ID をタスク グループに追加するには、タスク グループ コンフィギュレーション モードで **task** コマンドを使用します。 タスク グループからタスク ID を削除するには、このコマンドの **no** 形式を使用します。

task {**read**| **write**| **execute**| **debug**} *taskid-name*

no task {**read**| **write**| **execute**| **debug**} *taskid-name*

構文の説明

read	名前付きタスク ID に対して読み取り専用特権をイネーブルにします。
write	名前付きタスク ID に対して書き込み特権をイネーブルにします。「write」という用語には read の意も含まれます。
execute	名前付きタスク ID に対して実行特権をイネーブルにします。
debug	名前付きタスク ID に対してデバッグ特権をイネーブルにします。
taskid-name	タスク ID の名前です。

コマンド デフォルト

新しく作成したタスク グループには、タスク ID は割り当てられません。

コマンド モード

タスク グループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク グループ コンフィギュレーション モードで **task** コマンドを使用します。 タスク グローバル コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで **taskgroup** コマンドを使用します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、config-services タスク ID に対して実行特権をイネーブルにし、そのタスク ID をタスク グループ taskgroup1 に関連付ける例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup taskgroup1
RP/0/RSP0/CPU0:router(config-tg)# task execute config-services
```

関連コマンド

コマンド	説明
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。

taskgroup

タスク グループを一連のタスク ID に関連付けるように設定するには、また、タスク グローバル コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **taskgroup** コマンドを使用します。 タスク 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。

taskgroup *taskgroup-name* [**description** *string*| **task** {**read**| **write**| **execute**| **debug**} *taskid-name*| **inherit taskgroup** *taskgroup-name*]

no taskgroup *taskgroup-name*

構文の説明

taskgroup-name	特定のタスク グループの名前です。
description	（任意）名前付きタスク グループの説明を作成できます。
string	（任意）タスク グループの説明に使用する文字列です。
task	（任意）タスク ID が名前付きタスク グループに関連付けられることを指定します。
read	（任意）名前付きタスク ID で読み取りアクセスだけが許可されることを指定します。
write	（任意）名前付きタスク ID で読み取りおよび書き込みアクセスだけが許可されることを指定します。
execute	（任意）名前付きタスク ID で実行アクセスが許可されることを指定します。
debug	（任意）名前付きタスク ID でデバッグ アクセスだけが許可されることを指定します。
taskid-name	（任意）タスクの名前：タスク ID です。
inherit taskgroup	（任意）名前付きタスク グループからアクセス許可をコピーします。
taskgroup-name	（任意）アクセス許可を継承する元のタスク グループの名前です。

コマンド デフォルト

デフォルトでは、事前定義された 5 つのユーザ グループが使用可能になります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク グループには、アクション タイプごとに一連のタスク ID が設定されます。 システムでまだ参照されているタスク グループを削除すると、警告が表示され、削除は拒否されます。

グローバル コンフィギュレーション モードから、設定されているすべてのタスク グループを表示できます。 ただし、タスク グループ コンフィギュレーション モードでは、設定されているすべてのタスク グループを表示できるとは限りません。

キーワードや引数なしで **taskgroup** コマンドを入力すると、タスク グループ 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、**description**、**inherit**、**show**、および **task** の各コマンドを使用できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、BGP 読み取りアクセス権をタスク グループ alpha に割り当てる例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# task read bgp
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	タスク コンフィギュレーション モードでタスク グループの説明を作成します。
task, （123 ページ）	タスク ID をタスク グループに追加します。

timeout（RADIUS）

ルータが RADIUS サーバの応答を待機し、再送信するまでの秒数を指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **timeout** コマンドを使用します。 このコマンドをディセーブルにして、デフォルトのタイムアウト値の 5 秒に戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	タイムアウト値（秒単位）です。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

seconds：5

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タイムアウト値の秒数を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# timeout 500
```

関連コマンド

コマンド	説明
radius-server timeout, （64 ページ）	タイムアウトになるまでにルータがサーバホストの応答を待機する間隔を設定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

timeout（TACACS+）

認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定するには、TACACS ホスト コンフィギュレーション モードで **timeout**（TACACS+）コマンドを使用します。 このコマンドをディセーブルにして、デフォルトのタイムアウト値の 5 秒に戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	タイムアウト値（秒単位）です。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

seconds：5

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

timeout（TACACS+）コマンドによって、**tacacs-server timeout** コマンドで設定されたグローバルのタイムアウト値が、このサーバに限り上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タイムアウト値の秒数を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# timeout 500
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

timeout login response

サーバがログインに対する応答を待機する間隔を設定するには、回線テンプレート コンフィギュレーション モードで **timeout login response** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

timeout login response *seconds*

no timeout login response *seconds*

構文の説明

seconds	タイムアウトの間隔（秒単位）を指定する 0 ～ 300 の整数です。

コマンド デフォルト

seconds：30

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

回線テンプレート コンフィギュレーション モードで **timeout login response** コマンドを使用して、タイムアウト値を設定します。 このタイムアウト値は、入力した回線テンプレートが適用されるすべての端末回線に適用されます。 このタイムアウト値は、コンソール回線にも適用できます。 タイムアウト値の時間が経過すると、ユーザに再びプロンプトが表示されます。 再試行は 3 回まで可能です。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、インターバル タイマーを 20 秒に変更する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template alpha
RP/0/RSP0/CPU0:router(config-line)# timeout login response 20
```

関連コマンド

コマンド	説明
login authentication, （45 ページ）	ログインに対する AAA 認証をイネーブルにします。

usergroup

ユーザ グループを設定し、そのグループを一連のタスク グループに関連付けるには、また、ユーザ グループ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **usergroup** コマンドを使用します。 ユーザ グループを削除するには、またはタスク グループと指定されたユーザ グループとの関連付けを削除するには、このコマンドの **no** 形式を使用します。

usergroup *usergroup-name*

no usergroup *usergroup-name*

構文の説明

usergroup-name	ユーザ グループの名前です。 *usergroup-name* 引数には 1 つの単語だけ使用できます。 スペースと引用符は使用できません。

コマンド デフォルト

デフォルトでは、事前定義された 5 つのユーザ グループが使用可能になります。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ユーザ グループは、タスク グループなど一連のユーザに対するコマンド パラメータによって設定されます。 特定のユーザ グループを削除するには、**usergroup** コマンドの **no** 形式を使用します。 ユーザ グループ自体を削除するには、このコマンドをパラメータなしの **no** 形式で実行します。 システムでまだ参照されているユーザ グループを削除すると、警告が表示され、削除は拒否されます。

別のユーザ グループからアクセス権をコピーするには、inherit usergroup, （39 ページ） コマンドを使用します。 ユーザ グループは親グループに継承され、これらのグループに指定されているすべてのタスク ID の集合を形成します。 循環インクルードは検出され、拒否されます。 ユーザ グ

ループは、root-system や owner-sdr などの事前定義されたグループのプロパティを継承できません。

グローバル コンフィギュレーション モードから、設定されているすべてのユーザ グループを表示できます。 ただし、ユーザグループ コンフィギュレーション モードでは、設定されているすべてのユーザ グループを表示できるとは限りません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ グループ beta からユーザ グループ alpha にアクセス権を追加する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup beta
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	設定時にタスク グループの説明を作成します。
inherit usergroup, （39 ページ）	ユーザ グループが別のユーザ グループからアクセス権を取得できるようにします。
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。

username

新しいユーザにユーザ名とパスワードを設定し、そのユーザに対してアクセス権を付与するには、また、ユーザ名コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードまたは管理コンフィギュレーション モードで **username** コマンドを使用します。データベースからユーザを削除するには、このコマンドの **no** 形式を使用します。

username *user-name* [**password** {**[0]| 7**} *password*| **secret** {**[0]| 5**} *password*| **group** *usergroup-name*]

no username *user-name* [**password** {**0| 7**} *password*| **secret** {**0| 5**} *password*| **group** *usergroup-name*]

構文の説明

user-name	ユーザ名。*user-name* 引数に指定できるのは、1 つの単語だけです。 スペースと引用符は使用できません。
password	（任意）名前付きユーザにパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 シスコ独自の暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
7	（任意）暗号化パスワードが続くことを指定します。
password	（任意）「*lab*」など、ログインするユーザが入力する暗号化されていないパスワードのテキストを指定します。 暗号化が設定されている場合、パスワードはユーザに表示されません。 最長で 253 文字まで入力できます。
secret	（任意）名前付きユーザに対して、MD5 で保護されたパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 MD5 暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
5	（任意）暗号化パスワードが続くことを指定します。
group	（任意）名前付きユーザをユーザ グループに関連付けることができます。
usergroup-name	（任意）**usergroup** コマンドで定義されているとおりのユーザ グループの名前。

コマンド デフォルト

グローバル ユーザ名は定義されません。

管理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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

（注） 1 人のユーザが、単独のグループとしてシスコ サポート特権を持つことはできません。

username コマンドを使用して、ユーザを識別し、ユーザ名コンフィギュレーション モードを開始します。 パスワードとユーザ グループの割り当ては、グローバル コンフィギュレーション モードかユーザ名コンフィギュレーション サブモードのいずれかで実行できます。 アクセス権（タスク ID）を割り当てるには、定義されている 1 つまたは複数のユーザ グループにユーザを関連付けます。

グローバル コンフィギュレーション モードから、設定されているすべてのユーザ名を表示できます。 ただし、ユーザ名コンフィギュレーション モードでは、設定されているすべてのユーザ名を表示できるとは限りません。

各ユーザは、管理ドメイン内で一意のユーザ名によって識別されます。 各ユーザは、少なくとも 1 つのユーザ グループのメンバーであることが必要です。 ユーザ グループを削除すると、そのグループに関連付けられたユーザが孤立する場合があります。 AAA サーバでは孤立したユーザも認証されますが、ほとんどのコマンドは許可されません。

デフォルトでは、ローカル ログイン認証用に **username** コマンドが特定のユーザに関連付けられます。 また、TACACS+ ログイン認証用に TACACS+ サーバのデータベースにユーザとパスワードを設定することもできます。 詳細については、aaa authentication, （13 ページ） コマンドの説明を参照してください。

事前定義された root-system グループは、管理の設定時に root-system ユーザだけが指定できます。

（注） ローカル ネットワーキング デバイスをリモートのチャレンジ ハンドシェーク認証プロトコル（CHAP）の要求に応答できるようにするには、一方の **username** コマンド エントリを、他方のネットワーキング デバイスにすでに割り当てられているホスト名エントリと同一にする必要があります。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、グローバル コンフィギュレーション モードで **username** コマンドを実行したあとに使用できるコマンドの例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# ?
```

clear	コミットされていない設定をクリアします。
commit	設定変更を実行コンフィギュレーションにコミットします。
describe	実際に処理を行わず、コマンドについて説明します。
do	exec コマンドを実行します。
exit	このサブモードを終了します。
group	このユーザがメンバであるユーザ グループです。
no	コマンドを無効にするか、またはデフォルト値を設定します。
password	このユーザのパスワードを指定します。
pwd	現在のサブモードを開始するために使用するコマンドです。
root	グローバル コンフィギュレーション モードに戻ります。
secret	このユーザの安全なパスワードを指定します。
show	設定内容を表示します。

```
RP/0/RSP0/CPU0:router(config-un)#
```

次に、グローバル コンフィギュレーション モードでユーザ名 *user1* にクリアテキスト パスワード *password1* を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# password 0 password1
```

次に、管理コンフィギュレーション モードでユーザ *user1* に MD5 で保護されたシークレットを設定する例を示します。

```
RP/0/RSP0/CPU0:P1(admin-config)# username user1
RP/0/RSP0/CPU0:P1(admin-config-un)# secret 0 lab
RP/0/RSP0/CPU0:P1(admin-config-un)# commit
RP/0/RSP0/CPU0:May  6 13:06:43.205 : config[65723]: %MGBL-CONFIG-6-DB_COMMIT_ADMIN :
Configuration committed by user 'cisco'. Use 'show configuration commit changes 2000000005'
 to view the changes.
RP/0/RSP0/CPU0:P1(admin-config-un)# exit
RP/0/RSP0/CPU0:P1(admin-config)# show run username
username user1 secret 5 $1$QB03$3H29k3ZT.0PMQ8GQQKXCF0
!
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを定義します。
group（AAA）, （35 ページ）	ユーザをグループに追加します。
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
secret, （70 ページ）	ユーザに対してセキュア ログイン用のシークレットを作成します。

users group

ユーザ グループとその特権を回線に関連付けるには、回線テンプレート コンフィギュレーション モードで **users group** コマンドを使用します。 ユーザ グループと回線の関連付けを削除するには、このコマンドの **no** 形式を使用します。

users group {*usergroup-name*| **cisco-support**| **netadmin**| **operator**| **root-lr**| **root-system**| **sysadmin**}

no users group {*usergroup-name*| **cisco-support**| **netadmin**| **operator**| **root-lr**| **root-system**| **serviceadim**| **sysadmin**}

構文の説明

usergroup-name	ユーザ グループの名前です。 *usergroup-name* 引数には 1 つの単語だけ使用できます。 スペースと引用符は使用できません。
cisco-support	その回線を介してログインしているユーザにシスコ サポート担当者の特権を与えることを指定します。
netadmin	その回線を介してログインしているユーザにネットワーク管理者の特権を与えることを指定します。
operator	その回線を介してログインしているユーザにオペレータの特権を与えることを指定します。
root-lr	その回線を介してログインしているユーザにルート論理ルータ（LR）の特権を与えることを指定します。
root-system	その回線を介してログインしているユーザにルート システムの特権を与えることを指定します。
serviceadmin	その回線を介してログインしているユーザにサービス管理者グループの特権を与えることを指定します。
sysadmin	その回線を介してログインしているユーザにシステム管理者の特権を与えることを指定します。

コマンド デフォルト

なし

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

users group コマンドを使用して、ユーザ グループとその特権を回線に関連付けます。つまり、その回線にログインしているユーザには、特定のユーザ グループの特権が与えられます。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、回線テンプレート *vty* を使って vty-pool が作成された場合、vty を介してログインしているユーザにオペレータの特権が与えられます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authen login vty-authen line
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# line template vty
RP/0/RSP0/CPU0:router(config-line)# users group operator
RP/0/RSP0/CPU0:router(config-line)# login authentication
```

vrf（RADIUS）

AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を設定するには、RADIUS サーバグループ コンフィギュレーション モードで **vrf** コマンドを使用します。 サーバ グループがグローバル（デフォルト）ルーティング テーブルを使用できるようにするには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf *vrf-name*

構文の説明

vrf-name	VRF に割り当てる名前です。

コマンド デフォルト

デフォルトの VRF が使用されます。

コマンド モード

RADIUS サーバグループ 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

vrf コマンドを使用して、AAA RADIUS サーバ グループに VRF を指定し、ダイヤルアップ ユーザが異なるルーティング ドメインの AAA サーバを使用できるようにします。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、**vrf** コマンドの使用方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# vrf wal-mart
```

関連コマンド

コマンド	説明
radius source-interface, （66 ページ）	RADIUS で、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスが使用されるようにします。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

vrf（TACACS+）

AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を設定するには、TACACS+サーバグループ コンフィギュレーション モードで**vrf**コマンドを使用します。 サーバ グループがグローバル（デフォルト）ルーティング テーブルを使用できるようにするには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf *vrf-name*

構文の説明

vrf-name	VRF に割り当てる名前です。

コマンド デフォルト

デフォルトの VRF が使用されます。

コマンド モード

TACACS+ サーバグループ 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
リリース 4.1.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

vrf コマンドを使用して、AAA TACACS+ サーバ グループに VRF を指定し、ダイヤルアップ ユーザが異なるルーティング ドメインの AAA サーバを使用できるようにします。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**vrf** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 9.27.10.6
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# vrf abc
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	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。
server（TACACS+）, （76 ページ）	すべての発信 TACACS+ パケットに対して、選択したインターフェイスの発信元 IP アドレスを指定します。
server-private（TACACS+）, （82 ページ）	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。

IPSec コマンド

このモジュールでは、IPSec のコマンドについて説明します。

（注） 次に示す IPSec のコマンドを使用できるのは、<platform>-k9sec.pie がインストールされている場合のみです。

clear crypto ipsec sa

特定のセキュリティ アソシエーション（SA）、または IP Security（IPSec）セキュリティ アソシエーションデータベース（SADB）内のすべての SA を削除するには、EXEC モードで **clear crypto ipsec sa** コマンドを使用します。

clear crypto ipsec sa {*sa-id*| **all**}

構文の説明

sa-id	SA の識別子。 IPSec では、1 ～ 64,500 セッションがサポートされます。
all	IPsec SADB のすべての IPSec SA を削除します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SA は IPsec 内のデータ フローのセキュリティを確保するために確立されます。 **clear crypto ipsec sa** コマンドは、アクティブな IPSec セッションを削除するときや、強制的に新しい IPSec SA を再確立するときに使用します。 通常、ピア間の SA の確立は、IPsec に代わってインターネット キー交換（IKE）を通してネゴシエートされます。

タスク ID

タスク ID	操作
crypto	execute

例

次の例では、ID 100 の SA を SADB から削除する方法を示します。

```
RP/0/RSP0/CPU0:router# clear crypto ipsec sa 100
```

関連コマンド

コマンド	説明
show crypto ipsec sa, （151 ページ）	現在の SA によって使用されている設定を表示します。

description（IPsec プロファイル）

IPSecプロファイルの説明を作成するには、**description** コマンドをプロファイル コンフィギュレーション モードで使用します。 プロファイルの説明を削除するには、このコマンドの **no** 形式を使用します。

description *string*

no description

構文の説明

string	IPSec プロファイルを説明する文字列。

コマンド デフォルト

なし

コマンド モード

Crypto IPSec プロファイル

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

IPSec プロファイルの説明を作成するには、プロファイル コンフィギュレーション サブモード内で **description** コマンドを使用します。

タスク ID

タスク ID	操作
profile configuration	read, write

例

次の例では、プロファイルの説明を作成する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/RSP0/CPU0:router(config-newprofile)# description this is a sample profile
```

interface tunnel-ip（GRE）

総称ルーティングカプセル化（GRE）のトンネルインターフェイスを設定するには、グローバル コンフィギュレーション モードで **interface tunnel-ip** コマンドを使用します。 IP トンネル インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface tunnel-ip *number*

no interface tunnel-ip *number*

構文の説明

number	インターフェイスのインスタンス番号。 範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

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
リリース 3.9.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
interface	read, write

例

次の例では、**interface tunnel-ip** コマンドの使用方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 50000
RP/0/RSP0/CPU0:router(config-if)#
```

show crypto ipsec sa

ラック/スロット/モジュールの場所に基づいてセキュリティ アソシエーション（SA）の情報を表示するには、EXEC モードで **show crypto ipsec sa** コマンドを使用します。

show crypto ipsec sa [*sa-id*| **peer** *ip-address*| **profile** *profile-name*| **detail**| **fvrf** *fvrf-name*| **ivrf** *ivrf-name*| **location** *node-id*]

構文の説明

sa-id	（任意）SA の識別子。 範囲は 1 ～ 64500 です。
peer *ip-address*	（任意）リモート（PC）側で使用される IP アドレス。 無効な IP アドレスを入力することはできません。
profile *profile-name*	（任意）セキュリティ プロファイルの名前を英数字で指定します。 文字範囲は 1 ～ 64 です。 プロファイル名が重複していてはなりません。
detail	（任意）追加の動的 SA 情報を表示します。
fvrf *fvrf-name*	（任意）前面扉仮想ルーティングおよび転送（FVRF）のすべての既存の SA が fvrf-name と同じであることを指定します。
ivrf *ivrf-name*	（任意）内部仮想ルーティングおよび転送（IVRF）のすべての既存の SA が ivrf-name と同じであることを指定します。
location *node-id*	（任意）SA が指定の場所で設定されることを指定します。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

任意指定の引数やキーワードを使用しない場合は、フロー内のすべての SA が表示されます。 フロー内の SA は、プロトコル（カプセル化セキュリティ ペイロード（ESP）または認証ヘッダー（AH））および方向（インバウンドまたはアウトバウンド）ごとに表示されます。

detail キーワードを指定すると、ソフトウェア暗号化エンジン内で設定された SA のみの追加情報が表示されます。 SA は、tunnel-ipsec と transport を使用して設定されます。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ipsec sa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa

SSA id:          510
Node id:        0/1/0
SA Type:        MANUAL
interface:      service-ipsec22
profile  :      p7
local  ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.255/512/0)
remote ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.0/512/0)
local crypto endpt: 0.0.0.0, remote crypto endpt: 0.0.0.0, vrf default

 #pkts tx         :0                     #pkts rx         :0
 #bytes tx        :0                     #bytes rx        :0
 #pkts encrypt    :0                     #pkts decrypt    :0
 #pkts digest     :0                     #pkts verify     :0
 #pkts encrpt fail:0                     #pkts decrpt fail:0
 #pkts digest fail:0                     #pkts verify fail:0
 #pkts replay fail:0
 #pkts tx errors  :0                     #pkts rx errors  :0

outbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
inbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *10* : *show crypto ipsec sa* のフィールドの説明

フィールド	説明
SA id	SA の識別子。
interface	インターフェイスの識別子。
profile	セキュリティ プロファイルの名前を指定する英数字の文字列。
local ident	ローカル ピアの IP アドレス、マスク、プロトコル、およびポート。
remote ident	リモート ピアの IP アドレス、マスク、プロトコル、およびポート。
outbound esp sas	アウトバウンド ESP の SA。
inbound esp sas	インバウンド ESP の SA。
transform	SA で使用されるトランスフォーム。
sa lifetime	SA で使用されるライフタイム値。

次の出力例は、**show crypto ipsec sa** コマンドの **profile** キーワードで pn1 というプロファイルを指定した場合のものです。

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa profile pn1

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

次の出力例は、**show crypto ipsec sa** コマンドで **peer** キーワードを指定した場合のものです。

```
RP/0/RSP0/CPU0:router# show crypto ipsec sa peer 172.19.72.120

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

show crypto ipsec summary

IP セキュリティ（IPSec）のサマリー情報を表示するには、**show crypto ipsec summary** コマンドを EXEC モードで使用します。

show crypto ipsec summary

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ipsec summary** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ipsec summary

# * Attached to a transform indicates a bundle

# Active IPSec Sessions: 1

SA  Interface       Local Peer/Port   Remote Peer/Port  FVRF    Profile  Transform Lifetime
------------------------------------------------------------------------------------------
502 tunnel-ipsec100 70.70.70.2/500    60.60.60.2/500    default ipsec1   esp-3des  esp
3600/100000000
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *11*：*show crypto ipsec summary* のフィールドの説明

フィールド	説明
SA	セキュリティ アソシエーションの識別子。
Node	ノードの識別子。
Local Peer	ローカル ピアの IP アドレス。
Remote Peer	リモート ピアの IP アドレス
FVRF	SA の前面扉仮想ルーティングおよび転送（FVRF）。 FVRF がグローバルの場合は、出力の f_vrf が空のフィールドとして表示されます
Mode	プロファイル モードのタイプ。
Profile	使用中の暗号化プロファイル。
Transform	使用中のトランスフォーム。
Lifetime	ライフタイム値（秒単位）の後に KB 数が続きます。

show crypto ipsec transform-set

設定済みのトランスフォームセットを表示するには、EXECモードで**show crypto ipsec transform-set**コマンドを使用します。

show crypto ipsec transform-set [*transform-set-name*]

構文の説明

transform-set-name	（任意）*transform-set-name* 引数で指定された値を持つ IPSec トランスフォーム セットが表示されます。

コマンド デフォルト

デフォルト値はありません。デフォルトでは、すべての使用可能なトランスフォームセットが出力されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トランスフォームを指定しない場合は、すべてのトランスフォームが表示されます。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ipsec transform-set** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ipsec transform-set
```

```
Transform set combined-des-sha: {esp-des esp-sha-hmac}
Transform set tsfm2: {esp-md5-hmac esp-3des }
        Mode: Transport
Transform set tsfm1: {esp-md5-hmac esp-3des }
        Mode: Tunnel
Transform set ts1: {esp-des  }
        Mode: Tunnel
```

キーチェーン管理コマンド

ここでは、キーチェーン管理を設定するために使用されるコマンドについて説明します。

キーチェーン管理の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Keychain Management on Cisco ASR 9000 Series Router*」設定モジュールを参照してください。

accept-lifetime

キーチェーンの認証キーが有効なキーとして受信される期間を設定するには、キー コンフィギュレーション モードで **accept-lifetime** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

accept-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

no accept-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

構文の説明

start-time	キーが有効になる開始時間を *hh:mm:ss* 日月年の形式で指定します。 範囲は 0:0:0 ～ 23:59:59 です。 日付の範囲は 1 ～ 31 です。 年の範囲は 1993 ～ 2035 です。
duration *duration value*	（任意）キーのライフタイムを秒で指定します。 範囲は、1～2147483646 です。
infinite	（任意）有効になった後、そのキーが期限切れにならないことを示します。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 日月年の形式で指定します。 範囲は 0:0:0 ～ 23:59:59 です。

コマンド デフォルト

なし

コマンド モード

キー 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
system	read, write

例

次に、**accept-lifetime** コマンドの使用例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

関連コマンド

コマンド	説明
key（キーチェーン）, （166 ページ）	キーチェーンのキーを作成または変更します。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
key-string（キーチェーン）, （170 ページ）	キー文字列のテキストを指定します。
send-lifetime, （172 ページ）	有効なキーを送信します。
show key chain, （174 ページ）	キーチェーンを表示します。

accept-tolerance

ピアが使用する受け入れキーの許容値、つまり受け入れ可能な限度を秒で指定するには、キーチェーン コンフィギュレーション モードで **accept-tolerance** 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。

accept-tolerance [*value*| **infinite**]

no accept-tolerance [*value*| **infinite**]

構文の説明

value	（任意）秒で示される許容値の範囲。 範囲は、1 ～ 8640000 です。
infinite	（任意）指定された許容値が無限であることを示します。この受け入れキーは期限切れになりません。 無限の許容限度は、受け入れキーが常に受け入れ可能であり、ピアが使用する際に検証されることを意味します。

コマンド デフォルト

デフォルト値は、許容しないことを意味する 0 です。

コマンド モード

キーチェーン 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

accept-tolerance コマンドを設定しない場合、許容値は 0 に設定されます。

キーが有効なライフタイムの範囲外にある場合でも、許容限度内にあればそのキーは受け入れ可能と判断されます（たとえば、ライフタイムの開始前やライフタイムの終了後など）。

タスク ID

タスク ID	操作
system	read, write

例

次に、**accept-tolerance** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

関連コマンド

コマンド	説明
accept-lifetime, （160 ページ）	有効なキーを受け入れます。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
show key chain, （174 ページ）	キーチェーンを表示します。

cryptographic-algorithm

キーIDに設定されたキー文字列を使用して、パケットに適用する暗号化アルゴリズムを選択するには、キーチェーンおよびキー コンフィギュレーション モードで **cryptographic-algorithm** 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。

cryptographic-algorithm [**HMAC-MD5**| **HMAC-SHA1-12**| **HMAC-SHA1-20**| **MD5**| **SHA-1**]

no cryptographic-algorithm [**HMAC-MD5**| **HMAC-SHA1-12**| **HMAC-SHA1-20**| **MD5**| **SHA-1**]

構文の説明

HMAC-MD5	HMAC-MD5 をダイジェスト サイズ 16 バイトの暗号化アルゴリズムとして設定します。
HMAC-SHA1-12	HMAC-SHA1-12 をダイジェスト サイズ 12 バイトの暗号化アルゴリズムとして設定します。
HMAC-SHA1-20	HMAC-SHA1-20 をダイジェスト サイズ 20 バイトの暗号化アルゴリズムとして設定します。
MD5	MD5 をダイジェスト サイズ 16 バイトの暗号化アルゴリズムとして設定します。
SHA-1	SHA-1-20 をダイジェスト サイズ 20 バイトの暗号化アルゴリズムとして設定します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

暗号化アルゴリズムを設定しない場合、MAC 計算と API 検証は無効になります。

各プロトコルがサポートする暗号化アルゴリズムは次のとおりです。

- ボーダー ゲートウェイ プロトコル（BGP）は HMAC-MD5 と HMAC-SHA1-12 だけをサポート
- Intermediate System-to-Intermediate System（IS-IS）は HMAC-MD5 だけをサポート
- Open Shortest Path First（OSPF）は MD5 だけをサポート

タスク ID

タスク ID	操作
system	read, write

例

次に、**cryptographic-algorithm** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

関連コマンド

コマンド	説明
accept-lifetime, （160 ページ）	有効なキーを受け入れます。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
show key chain, （174 ページ）	キーチェーンを表示します。

key（キーチェーン）

キーチェーンのキーを作成または変更するには、キーチェーンのキー コンフィギュレーション モードで **key** 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。

key *key-id*

no key *key-id*

構文の説明

key-id	48 ビット整数型のキー ID。範囲は 0 ～ 281474976710655 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ボーダー ゲートウェイ プロトコル（BGP）のキーチェーン設定では、*key-id* 引数の範囲は 0 ～ 63 でなければなりません。 この範囲が 63 の値を超えると、BGP キーチェーンの操作は拒否されます。

タスク ID

タスク ID	操作
system	read, write

例

次に、**key** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)#
```

関連コマンド

コマンド	説明
accept-lifetime, （160 ページ）	有効なキーを受け入れます。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
key-string（キーチェーン）, （170 ページ）	キー文字列のテキストを指定します。
send-lifetime, （172 ページ）	有効なキーを送信します。
show key chain, （174 ページ）	キーチェーンを表示します。

key chain（キーチェーン）

キーチェーンを作成または変更するには、グローバル コンフィギュレーション モードで **key chain** 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。

key chain *key-chain-name*

no key chain *key-chain-name*

構文の説明

key-chain-name	キーチェーンの名前を指定します。 最大文字数は 48 です。

コマンド デフォルト

デフォルトの動作または値はありません。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ボーダー ゲートウェイ プロトコル（BGP）のキーチェーンは、ネイバー、セッション グループ、またはネイバー グループとして設定できます。 BGP はこのキーチェーンを使用して、ヒットしないキー更新を認証にインプリメントできます。

タスク ID

タスク ID	操作
system	read, write

例

次の例は、キーチェーン名 isis-keys が **key chain** コマンド用であることを示しています。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)#
```

関連コマンド

コマンド	説明
accept-lifetime,（160 ページ）	有効なキーを受け入れます。
accept-tolerance,（162 ページ）	キーチェーンのキーを受け入れる際の許容値を設定します。
key（キーチェーン）,（166 ページ）	キーチェーンのキーを作成または変更します。
key-string（キーチェーン）,（170 ページ）	キー文字列のテキストを指定します。
send-lifetime,（172 ページ）	有効なキーを送信します。
show key chain,（174 ページ）	キーチェーンを表示します。

key-string（キーチェーン）

キーのテキスト文字列を指定するには、キーチェーンのキー コンフィギュレーション モードで **key-string** 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。

key-string [**clear**| **password**] *key-string-text*

no key-string [**clear**| **password**] *key-string-text*

構文の説明

clear	キー文字列をクリアテキスト形式で指定します。
password	キーを暗号化形式で指定します。
key-string-text	キーのテキスト文字列。パーサー プロセスによって暗号化されてから、設定に保存されます。 テキスト文字列には、次の文字制限があります。 • プレーン テキストのキー文字列：最小 1 文字、最大 32 文字。 • 暗号化されたキー文字列：最小 4 文字、上限はなし。

コマンド デフォルト

デフォルト値は clear です。

コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

コマンド履歴

リリース	変更内容
リリース 3.3.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

暗号化パスワードが有効であるためには、次の条件を満たしている必要があります。

- 文字列に 4 文字以上の偶数個の文字が含まれている。
- パスワード文字列の最初の 2 文字は 10 進数、残りの文字は 16 進数である。
- 最初の 2 桁は 53 以下である。

次の例は、どちらも有効な暗号化パスワードです。

1234abcd

または

50aefd

タスク ID

タスク ID	操作
system	read, write

例

次に、**keystring** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router:# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

関連コマンド

コマンド	説明
accept-lifetime, （160 ページ）	有効なキーを受け入れます。
key（キーチェーン）, （166 ページ）	キーチェーンのキーを作成または変更します。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
send-lifetime, （172 ページ）	有効なキーを送信します。
show key chain, （174 ページ）	キーチェーンを表示します。

send-lifetime

有効なキーを送信し、ピアのローカル ホストからの情報を認証するには、キーチェーンおよびキー コンフィギュレーション モードで**send-lifetime** 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。

send-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

no send-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

構文の説明

start-time	キーが有効になる開始時間を *hh:mm:ss* 日月年の形式で指定します。 範囲は 0:0:0 ～ 23:59:59 です。 日付の範囲は 1 ～ 31 です。 年の範囲は 1993 ～ 2035 です。
duration *duration value*	（任意）キーのライフタイムを秒で指定します。
infinite	（任意）一旦有効になると、そのキーは期限切れにならないことを示します。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 日月年の形式で指定します。 範囲は 0:0:0 ～ 23:59:59 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
system	read, write

例

次に、**send-lifetime** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain isis-keys
RP/0/RSP0/CPU0:router(config-isis-keys)# key 8
RP/0/RSP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

関連コマンド

コマンド	説明
accept-lifetime,（160 ページ）	有効なキーを受け入れます。
key（キーチェーン），（166 ページ）	キーチェーンのキーを作成または変更します。
key chain（キーチェーン），（168 ページ）	キーチェーンを作成または変更します。
key-string（キーチェーン），（170 ページ）	キー文字列のテキストを指定します。

show key chain

キーチェーンを表示するには、EXEC モードで **show key chain** コマンドを使用します。

show key chain *key-chain-name*

構文の説明

key-chain-name	指定したキーチェーンのキーの名前です。 最大文字数は32です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
system	read

例

セキュアなキー ストレージが使用可能になった場合は、ユーザにマスターパスワードの入力を要求し、暗号化してからキー ラベルを表示するのが、キーチェーン管理にとっては望ましい方法です。 次の例では、**show key chain** コマンドに対して暗号化キー ラベルだけが表示されます。

```
RP/0/RSP0/CPU0:router# show key chain isis-keys

Key-chain: isis-keys/ -

accept-tolerance -- infinite
Key 8 -- text "8"
```

```
cryptographic-algorithm -- MD5
Send lifetime:   01:00:00, 29 Jun 2006 - Always valid  [Valid now]
Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

関連コマンド

コマンド	説明
accept-lifetime, （160 ページ）	有効なキーを受け入れます。
accept-tolerance, （162 ページ）	キーチェーンのキーを受け入れる際の許容値を設定します。
key（キーチェーン）, （166 ページ）	キーチェーンのキーを作成または変更します。
key chain（キーチェーン）, （168 ページ）	キーチェーンを作成または変更します。
key-string（キーチェーン）, （170 ページ）	キー文字列のテキストを指定します。
send-lifetime, （172 ページ）	有効なキーを送信します。

合法的傍受コマンド

ここでは、合法的傍受（LI）を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

キーチェーン管理の概念、設定作業、および例の詳細については、「*Implementing Lawful Intercept on Cisco ASR 9000 Series RouterSoftware*」設定モジュールを参照してください。

lawful-intercept disable

合法的傍受機能をディセーブルにするには、グローバル コンフィギュレーション モードで **lawful-intercept disable** コマンドを使用します。 合法的傍受機能を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

lawful-intercept disable

no lawful-intercept disable

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

合法的傍受機能はデフォルトでイネーブルです。

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
リリース 4.1.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

合法的傍受をディセーブルにすると、すべてのメディエーション デバイスおよび関連する TAP が削除されます。

タスク ID

タスク ID	操作
li	read, write

例

次に、**lawful-intercept disable** コマンドの使用例を示します。

```
RP/0/RSP0/CPU0:router(config)# lawful-intercept disable
```

管理プレーン保護コマンド

ここでは、管理プレーン保護（MPP）を設定するために使用されるコマンドについて説明します。

キーチェーン管理の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の、「*Implementing Management Plane Protection on* Cisco ASR 9000 Series Router」モジュールを参照してください。

address ipv4（MPP）

管理トラフィックがインターフェイス上で許可されるピア IPv4 アドレスを設定するには、インターフェイス ピア コンフィギュレーション モードで **address ipv4** コマンドを使用します。 以前このインターフェイスに設定された IP 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 ipv4 {*peer-ip-address*| *peer-ip-address*/ *length*}

no address ipv4 {*peer-ip-address*| *peer-ip-address*/ *length*}

構文の説明

peer-ip-address	このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレス。 実質的には、このアドレスは、設定済みインターフェイスで着信する管理トラフィックのソース アドレスです。
peer ip-address/length	ピア IPv4 アドレスのプレフィックス。 • IPv4：*A.B.C.D./length* • IPv6：*X.X:X.X*

コマンド デフォルト

特定のピアが設定されていない場合は、すべてのピアが許可されます。

コマンド モード

インターフェイス ピア 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
system	read, write

例

次に、管理トラフィックにピア IPv4 アドレス 10.1.0.0 とプレフィックス 16 を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inbandout-of-band
RP/0/RSP0/CPU0:router(config-mpp-inbandoutband)# interface GigabitEthernet POS 0/16/10/12
RP/0/RSP0/CPU0:router(config-mpp-inbandoutband-GigabitEthernet0_1_1_1POS0_6_0_2)# allow
Telnet TFTP peer
RP/0/RSP0/CPU0:router(config-telnettftp-peer)# address ipv4 10.1.0.0/16ipv6 33::33
```

関連コマンド

コマンド	説明
address ipv6（MPP）, （183 ページ）	このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレスを設定します。
allow, （185 ページ）	インターフェイスを、特定またはすべてのプロトコルに対してすべてのピアアドレスを許可するインバンドまたはアウトオブバンドインターフェイスとして設定します。
control-plane, （188 ページ）	コントロール プレーンを設定します。
inband, （190 ページ）	インバンドインターフェイスまたはプロトコルを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

address ipv6（MPP）

管理トラフィックがインターフェイス上で許可されるピア IPv6 アドレスを設定するには、インターフェイス ピア 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。 以前このインターフェイスに設定された IP 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 {*peer-ip-address*| *peer-ip-address*/*length*}

構文の説明

peer-ip-address	このインターフェイス上で管理トラフィックが許可されるピア IPv6 アドレス。 実質的には、このアドレスは、設定済みインターフェイスで着信する管理トラフィックのソース アドレスです。
s*peer ip-address/length*	ピア IPv6 アドレスのプレフィックス。

コマンド デフォルト

特定のピアが設定されていない場合は、すべてのピアが許可されます。

コマンド モード

インターフェイス ピア 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
system	read, write

例

次に、管理トラフィックにピア IPv6 アドレス 33::33 を設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface
            GigabitEthernet 0/1/1/2

RP/0/RSP0/CPU0:router(config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RSP0/CPU0:router(config-tftp-peer)# address ipv6 33::33
```

関連コマンド

コマンド	説明
address ipv4（MPP）, （180 ページ）	このインターフェイス上で管理トラフィックが許可されるピア IPv4 アドレスを設定します。
allow, （185 ページ）	インターフェイスを、特定またはすべてのプロトコルに対してすべてのピア アドレスを許可するインバンドまたはアウトオブバンドインターフェイスとして設定します。
control-plane, （188 ページ）	コントロール プレーンを設定します。
inband, （190 ページ）	インバンドインターフェイスまたはプロトコルを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

allow

インターフェイスを、特定またはすべてのプロトコルに対してすべてのピア アドレスを許可するインバンドまたはアウトオブバンド インターフェイスとして設定するには、管理プレーン保護インバンド インターフェイス コンフィギュレーション モードまたは管理プレーン保護アウトオブバンド インターフェイス コンフィギュレーション モードで **allow** コマンドを使用します。 インターフェイス上でプロトコルを不許可にするには、このコマンドの **no** 形式を使用します。

allow {*protocol*| **all**} **[peer]**

no allow {*protocol*| **all**} **[peer]**

構文の説明

protocol	次に示す特定のプロトコルのトラフィックに対してピア フィルタリングを許可するよう設定されたインターフェイス。 • HTTP（S） • SNMP（バージョンも） • セキュア シェル（v1 および v2） • TFTP • Telnet • XML
all	プロトコルのリストで指定されたすべての管理トラフィックに対してピア フィルタリングを許可するインターフェイスを設定します。
peer	（任意）インターフェイスのピア アドレスを設定します。 ピアは、トラフィックがメイン ルータに到着する可能性がある隣接ルータ インターフェイスを意味します。

コマンド デフォルト

デフォルトでは、管理プロトコルは管理インターフェイス以外のどのインターフェイス上でも許可されません。

コマンド モード

管理プレーン保護インバンド インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.0.0	XML キーワードが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

インターフェイスに対して特定のプロトコルを許可すると、トラフィックはそのプロトコルに対してだけ許可され、その他の管理トラフィックはすべてドロップされます。

インターフェイスをインバンドまたはアウトオブバンドとして設定すると、指定したプロトコルのトラフィックまたはすべてのプロトコル トラフィックがインターフェイス上で許可されます。インバンドまたはアウトオブバンドとして設定されていないインターフェイスは、プロトコル トラフィックをドロップします。

IOS-XR XML API は、外部の管理アプリケーションが使用するためにルータにプログラマチック インターフェイスを提供します。 このインターフェイスは、XML形式の要求および応答ストリームを使用するルータ設定とモニタリングのメカニズムを提供します。 管理サービスの 1 つとして、XML は MPP を適用できる必要があります。 XML MPP のデータを保護するために、XML キーワードがコマンドに追加されました。

タスク ID

タスク ID	操作
system	read, write

例

次に、すべてのインバンド インターフェイスに対してすべての管理プロトコルを設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-inband-all)# allow all
```

次に、アウトオブバンド インターフェイスに TFTP プロトコルのピア フィルタリングを設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
```

```
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface GigabitEthernet 0/1/1/2
RP/0/RSP0/CPU0:router(config-mpp-outband-GigabitEthernet0_1_1_2)# allow TFTP peer
RP/0/RSP0/CPU0:router(config-tftp-peer)#
```

次に、XML のピアのインバンド インターフェイスで MPP のサポートを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-ctrl-mpp)# inband interface all allow xml peer address ipv4
172.10.10.1
```

関連コマンド

コマンド	説明
control-plane, （188 ページ）	コントロール プレーンを設定します。
inband, （190 ページ）	インバンドインターフェイスまたはプロトコルを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

control-plane

コントロールプレーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **control-plane** コマンドを使用します。 コントロール プレーン モードでの設定をすべて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。

control-plane

no control-plane

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

コントロール プレーン コンフィギュレーション モードを開始するには、**control-plane** コマンドを使用します。

タスク ID

タスク ID	操作
system	read, write

例

次に、**control-plane** コマンドを使用してコントロール プレーン コンフィギュレーション モードを開始する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)#
```

関連コマンド

コマンド	説明
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。

inband

インバンド インターフェイスを設定し、管理プレーン保護インバンド コンフィギュレーション モードを開始するには、管理プレーン保護コンフィギュレーション モードで **inband** コマンドを使用します。インバンド コンフィギュレーション モードでの設定をすべて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。

inband

no inband

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

管理プレーン保護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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

管理プレーン保護コンフィギュレーション モードを開始するには、**inband** コマンドを使用します。

タスク ID

タスク ID	操作
system	read, write

例

次に、**inband** コマンドを使用して管理プレーン保護インバンド コンフィギュレーション モードを開始する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)#
```

関連コマンド

コマンド	説明
control-plane, （188 ページ）	コントロール プレーンを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

interface（MPP）

特定またはすべてのインターフェイスをインバンドまたはアウトオブバンド インターフェイスとして設定するには、管理プレーン保護インバンド コンフィギュレーション モードまたは管理プレーン保護アウトオブバンド コンフィギュレーション モードで **interface** コマンドを使用します。インターフェイス モードでの設定をすべて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。

interface {*type interface-path-id*| **all**}

no interface {*type interface-path-id*| **all**}

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
interface-path-id	仮想インターフェイス インスタンス。 数字の範囲は、インターフェイス タイプによって異なります。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
all	管理トラフィックを許可するよう、すべてのインターフェイスを設定します。

コマンド デフォルト

なし

コマンド モード

管理プレーン保護アウトオブバンド 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

管理プレーン保護インバンドインターフェイス コンフィギュレーション モードまたは管理プレーン保護アウトオブバンド インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを使用します。

instance 引数については、管理イーサネット インターフェイスをインバンド インターフェイスとして設定できません。

タスク ID

タスク ID	操作
system	read, write

例

次に、MPP にすべてのインバンド インターフェイスを設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# inband
RP/0/RSP0/CPU0:router(config-mpp-inband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-inband-all)#
```

次に、MPP にすべてのアウトオブバンド インターフェイスを設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# interface all
RP/0/RSP0/CPU0:router(config-mpp-outband-all)#
```

関連コマンド

コマンド	説明
allow, （185 ページ）	インターフェイスを、特定またはすべてのプロトコルに対してすべてのピア アドレスを許可するインバンドまたはアウトオブバンドインターフェイスとして設定します。
control-plane, （188 ページ）	コントロール プレーンを設定します。
inband, （190 ページ）	インバンドインターフェイスまたはプロトコルを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。

コマンド	説明
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

management-plane

プロトコルを許可または不許可にするよう管理プレーン保護を設定するには、コントロール プレーン コンフィギュレーション モードで **management-plane** コマンドを使用します。 管理プレーン モードでの設定をすべて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。

management-plane

no management-plane

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

コントロール プレーン 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

管理プレーン保護コンフィギュレーション モードを開始するには、**management-plane** コマンドを使用します。

タスク ID

タスク ID	操作
system	read, write

例

次に、**management-plane** コマンドを使用して管理プレーン保護コンフィギュレーション モードを開始する例を示します。

```
RR/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)#
```

out-of-band

アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンドコンフィギュレーションモードを開始するには、管理プレーン保護コンフィギュレーションモードで **out-of-band** コマンドを使用します。 管理プレーン保護アウトオブバンド コンフィギュレーション モードでの設定をすべて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。

out-of-band

no out-of-band

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

管理プレーン保護アウトオブバンド 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

管理プレーン保護アウトオブバンドコンフィギュレーション モードを開始するには、**out-of-band** コマンドを使用します。

アウトオブバンドは、管理プロトコル トラフィックの転送または処理だけを許可するインターフェイスを意味します。アウトオブバンド管理インターフェイスは、ネットワーク管理トラフィックだけを受信するようネットワーク オペレータによって定義されます。 これには、転送（またはカスタマー）トラフィックによってルータの管理が妨害されないという利点があります。

タスク ID

タスク ID	操作
system	read, write

例

次に、**out-of-band** コマンドを使用して管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)#
```

関連コマンド

コマンド	説明
control-plane, （188 ページ）	コントロール プレーンを設定します。
inband, （190 ページ）	インバンドインターフェイスまたはプロトコルを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。
vrf（MPP）, （202 ページ）	アウトオブバンドインターフェイスのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）リファレンスを設定します。

show mgmt-plane

インターフェイスのタイプやインターフェイス上でイネーブルにするプロトコルなど、管理プレーンに関する情報を表示するには、EXEC モードで **show mgmt-plane** コマンドを使用します。

show mgmt-plane [**inband**| **out-of-band**] [**interface** *type interface-path-id*| **vrf**]

構文の説明

inband	（任意）データ転送パケットだけでなく管理パケットも処理するインバンド管理インターフェイス コンフィギュレーションを表示します。インバンド管理インターフェイスは、共有管理インターフェイスとも呼ばれています。
out-of-band	（任意）アウトオブバンドインターフェイス コンフィギュレーションを表示します。アウトオブバンドインターフェイスは、ネットワーク管理トラフィックだけを受信するよう、ネットワーク オペレータによって定義されます。
interface	（任意）指定されたインターフェイス上で許可されるすべてのプロトコルを表示します。
type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
interface-path-id	仮想インターフェイス インスタンス。 数字の範囲は、インターフェイス タイプによって異なります。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
vrf	（任意）アウトオブバンド インターフェイスのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送リファレンスを設定します。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

vrf キーワードは、アウトオブバンド VRF コンフィギュレーションに対してだけ有効です。

タスク ID

タスク ID	操作
system	read

例

次のサンプル出力は、MPP でインバンドまたはアウトオブバンドインターフェイスとして設定されるすべてのインターフェイスを示しています。

```
RR/0/RSP0/CPU0:router# show mgmt-plane

Management Plane Protection

inband interfaces
----------------------

interface - GigabitEthernet0_1_1_0
        ssh configured -
                All peers allowed
        telnet configured -
                peer v4 allowed - 10.1.0.0/16
        all configured -
                All peers allowed
interface - GigabitEthernet0_1_1_0
        telnet configured -
                peer v4 allowed - 10.1.0.0/16

interface - all
        all configured -
                All peers allowed

outband interfaces
----------------------
interface - GigabitEthernet0_1_1_0
        tftp configured -
                peer v6 allowed - 33::33
```

次のサンプル出力は、アウトオブバンド インターフェイスの Virtual Private Network (VPN) routing and forwarding（VRF; バーチャル プライベート ネットワーク（VPN）および転送）リファレンスを示しています。

```
RR/0/RSP0/CPU0:router# show mgmt-plane out-of-band vrf

Management Plane Protection -
        out-of-band VRF - my_out_of_band
```

関連コマンド

コマンド	説明
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。

vrf（MPP）

アウトオブバンド インターフェイスのバーチャル プライベート ネットワーク（VPN）および転送（VRF）リファレンスを設定するには、管理プレーン保護アウトオブバンド コンフィギュレーション モードで **vrf** コマンドを使用します。 VRF 名を使用する前に VRF 定義を削除するには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf *vrf-name*

構文の説明

vrf-name	VRF に割り当てる名前です。

コマンド デフォルト

インターフェイスをアウトオブバンドとして設定するには、VRF の概念を使用する必要があります。 アウトオブバンド コンフィギュレーションで VRF が設定されていない場合、インターフェイスはデフォルトの VRF になります。

コマンド モード

管理プレーン保護アウトオブバンド 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

VRF リファレンスが設定されていない場合は、デフォルト名の MPP_OUTBAND_VRF が使用されます。

VRF を参照するアウトオブバンド コンフィギュレーションがあり、その VRF が削除された場合は、すべての MPP バインディングが削除されます。

タスク ID

タスク ID	操作
system	read

例

次に、VRF を設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vrf my_out_of_band
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)# exit
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv6 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)# commit
RP/0/RSP0/CPU0:router(config-vrf-af)# end
RR/0/RSP0/CPU0:router#
```

次に、MMP の VRF 定義を設定する例を示します。

```
RR/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# control-plane
RP/0/RSP0/CPU0:router(config-ctrl)# management-plane
RP/0/RSP0/CPU0:router(config-mpp)# out-of-band
RP/0/RSP0/CPU0:router(config-mpp-outband)# vrf my_out_of_band
```

関連コマンド

コマンド	説明
control-plane, （188 ページ）	コントロール プレーンを設定します。
interface（MPP）, （192 ページ）	特定またはすべてのインバンドまたはアウトオブバンド インターフェイスを設定します。
management-plane, （195 ページ）	プロトコルを許可または不許可にする管理プレーン保護を設定します。
out-of-band, （197 ページ）	アウトオブバンドインターフェイスまたはプロトコルを設定し、管理プレーン保護アウトオブバンド コンフィギュレーション モードを開始します。
show mgmt-plane, （199 ページ）	管理プレーンを表示します。

公開キー インフラストラクチャ コマンド

ここでは、公開キーインフラストラクチャ（PKI）を設定するために使用されるコマンドについて説明します。

PKI の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Certification Authority Interoperability on Cisco ASR 9000 Series Router*」モジュールを参照してください。

clear crypto ca certificates

コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアするには、EXEC モードで **clear crypto ca certificates** コマンドを使用します。

clear crypto ca certificates *trustpoint*

構文の説明

trustpoint	トラストポイント名。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータが、新しいコンフィギュレーション ファイルを使用してロードされており、新しいコンフィギュレーションファイルに対応するトラストポイントが設定されていない場合は、**clear crypto ca certificates** コマンドを使用して、コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアします。

clear crypto ca certificates コマンドにより、Certification Authority（CA; 認証局）およびルータの両方の証明書がシステムから削除されます。

タスク ID

タスク ID	操作
crypto	execute

例

次に、コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto ca certificates tp_1
```

clear crypto ca crl

ルータに保存されているすべての Certificate Revocation Lists（CRL; 証明書失効リスト）をクリアするには、EXEC モードで **clear crypto ca crl** コマンドを使用します。

clear crypto ca crl

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに保存されているすべての CRL をクリアするには、**clear crypto ca crl** コマンドを使用します。 その結果、ルータは認証局（CA）に承認され、証明書を確認する着信要求に対する新しい CRL をダウンロードします。

タスク ID

タスク ID	操作
crypto	execute

例

次に、ルータに保存されているすべての CRL をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca crls

CRL Entry
==============================================
  Issuer : cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
```

```
  Last Update : [UTC] Wed Jun  5 02:40:04 2002
  Next Update : [UTC] Wed Jun  5 03:00:04 2002
  CRL Distribution Point :
ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

RP/0/RSP0/CPU0:router# clear crypto ca crl
RP/0/RSP0/CPU0:router# show crypto ca crls
```

関連コマンド

コマンド	説明
show crypto ca crls, （260 ページ）	ルータの CRL に関する情報を表示します。

crl optional（トラストポイント）

他のピアの証明書が、対応するCRLを取得しなくても受け付けられるようにするには、トラストポイント コンフィギュレーション モードで **crl optional** コマンドを使用します。 ルータが証明書を受け付ける前にCRL チェックを必須とするデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

crl optional

no crl optional

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

ルータは、他のIPセキュリティ ピアの証明書を受け付ける前に、対応するCRLを取得しており、それをチェックしている必要があります。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータがピアから証明書を受け取ると、対応するCRLがないかメモリを検索します。ルータが対応する CRL を見つけた場合は、その CRL が使用されます。 見つからなかった場合は、ルータはピアの証明書での指定に従って、認証局（CA）またはCRL Distribution Point（CDP; CRL 分散ポイント）のどちらかから CRL をダウンロードします。 次に、ルータはCRL をチェックして、ピアから送信された証明書が無効になっていないことを確認します。 証明書がCRLに表示されている場合、ルータは証明書を受け付けることができず、ピアを認証できません。CRLをダウンロードしないで、証明書を無効として処理するようルータに指示するには、**crl optional** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA を宣言して、CRL を取得しないでルータが証明書を受け付けることを許可します。 またこの例では、非標準のリトライ期間とリトライ回数も指定します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RSP0/CPU0:router(config-trustp)# crl optional
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry count, （236 ページ）	ルータが証明書要求を再送信する回数を指定します。
enrollment retry period, （238 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment url, （242 ページ）	CA の URL を指定します。

crypto ca authenticate

認証局（CA）の証明書を取得することでCAを認証するには、EXECモードで**crypto ca authenticate**コマンドを使用します。

crypto ca authenticate *ca-name*

構文の説明

ca-name	CA サーバ名

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータで最初にCA サポートを設定する際は、**crypto ca authenticate** コマンドが必要です。

このコマンドは、CA の公開キーを含むCA 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。 自己署名のルートCA の場合は、CA がそれ自体の証明書に署名するため、このコマンドを使用する際にCA 管理者に連絡して、CA 公開キーを手動で認証する必要があります。 証明書のフィンガープリントの照合は、アウトオブバンド（電話機での通話など）で行われます。

ルートCA の認証前に、第 2 レベルの CA の認証を行う必要があります。

crypto ca authenticateコマンドを発行した後、指定されたタイムアウト期間までにCAが応答しない場合、もう一度端末コントロールを取得して、コマンドを再入力する必要があります。

タスク ID

タスク ID	操作
crypto	execute

例

CAによって証明書が送信され、ルータから、証明書のフィンガープリント（一意のID）をチェックすることで証明書を確認するよう管理者にプロンプトが表示されます。 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。 画面のフィンガープリントが、CA管理者によって表示されているフィンガープリントと一致した場合は、その証明書を有効な証明書として受け付ける必要があります。

次の例では、ルータによるCA証明書の要求を示します。

```
RP/0/RSP0/CPU0:router# crypto ca authenticate msiox
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Certificate has the following attributes:
   Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

Do you accept this certificate? [yes/no]: yes


RP/0/RSP0/CPU0:router#:Apr 10 00:28:52.324 : cepki[335]: %SECURITY-CEPKI-6-INFO : certificate
 database updated
Do you accept this certificate? [yes/no] yes
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
show crypto ca certificates, （258 ページ）	ご使用の証明書およびCAの証明書に関する情報を表示します。

crypto ca cancel-enroll

現在の登録要求をキャンセルするには、EXEC モードで **crypto ca cancel-enroll** コマンドを使用します。

crypto ca cancel-enroll *ca-name*

構文の説明

ca-name	認証局（CA）の名前。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイント コンフィギュレーション モードで rsakeypair, （248 ページ） コマンドによって定義されているルータの Rivest, Shamir, and Adelman（RSA）キー ペアの証明書を CA から要求するには、**crypto ca enroll** コマンドを使用します。 現在のトラストポイントに対して rsakeypair, （248 ページ） コマンドが設定されていない場合は、登録にはデフォルトの RSA キー ペアが使用されます。 このタスクは、CA を使用した登録とも呼ばれます。 現在の登録要求をキャンセルするには、**crypto ca cancel-enroll** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次に、myca という名前の CA から現在の登録要求をキャンセルする例を示します。

```
RP/0/RSP0/CPU0:router# crypto ca cancel-enroll myca
```

関連コマンド

コマンド	説明
crypto ca enroll, （217 ページ）	CA からルータの証明書を取得します。
rsakeypair, （248 ページ）	トラストポイントに対する名前付きの RSA キーペアを指定します。

crypto ca enroll

認証局（CA）からルータの証明書を取得するには、EXEC モードで **crypto ca enroll** コマンドを使用します。

crypto ca enroll *ca-name*

構文の説明

ca-name	CA サーバ名

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイント コンフィギュレーション モードで rsakeypair, （248 ページ） コマンドによって定義されているルータの Rivest, Shamir, and Adelman（RSA）キー ペアの証明書を CA から要求するには、**crypto ca enroll** コマンドを使用します。 現在のトラストポイントに対して rsakeypair, （248 ページ） コマンドが設定されていない場合は、登録にはデフォルトの RSA キー ペアが使用されます。 このタスクは、CA を使用した登録とも呼ばれます。 （証明書の登録と取得は、2 つの個別のイベントですが、**crypto ca enroll** コマンドが発行された場合はこれら両方のイベントが発生します）。手動登録を行った場合、この 2 つのイベントは個別に発生します。

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、このコマンドを設定できません。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 （既存の証明書を削除するには、**no**

crypto ca trustpoint コマンドを使用してトラストポイント コンフィギュレーションを削除します）。

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。

タスク ID

タスク ID	操作
crypto	execute

例

次に、**crypto ca enroll** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# crypto ca enroll msiox
% 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 you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
    Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7
RP/0/RSP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RSP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
rsakeypair, （248 ページ）	トラストポイントに対する名前付きのRSA キーペアを指定します。

crypto ca import

認証局（CA）証明書を、TFTP、SFTP、または端末でのカットアンドペーストを使用して手動でインポートするには、EXEC モードで **crypto ca import** コマンドを使用します。

crypto ca import *name* **certificate**

構文の説明

name **certificate**	認証局（CA）の名前。この名前には、crypto ca trustpoint, （221 ページ）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

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	execute

例

次に、CA 証明書をカット アンド ペーストを使用してインポートする例を示します。この例では、証明書は myca という名前です。

```
RP/0/RSP0/CPU0:router# crypto ca import myca certificate
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
show crypto ca certificates, （258 ページ）	証明書と認証局（CA）証明書に関する情報を表示します。

crypto ca trustpoint

信頼できるポイントを選択した名前で設定するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。 信頼できるポイントの設定を解除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *ca-name*

no crypto ca trustpoint *ca-name*

構文の説明

ca-name	CA の名前。

コマンド デフォルト

なし

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。

このコマンドを使用して、選択した名前で信頼できるポイントを設定できるので、ルータはピアに対して発行された証明書を確認できます。 ルータは、ピアに対して証明書を発行した CA に登録する必要はありません。

crypto ca trustpoint コマンドを実行するとトラストポイント コンフィギュレーション モードが開始され、このモードで次のコマンドを使用して CA の特性を指定できます。

- crl optional（トラストポイント）, （211 ページ） コマンド：対応する CRL を取得しなくても他のピアの証明書が受け付けられます。
- enrollment retry count, （236 ページ） コマンド：ルータによって送信される、証明書要求のリトライ回数。 オプション。

- enrollment retry period, （238 ページ） コマンド：（任意）ルータが証明書要求のリトライを送信するまでの待機時間。
- enrollment terminal, （240 ページ） コマンド：ルータと認証局（CA）間がネットワーク接続されていない場合に、証明書要求と証明書を手動でカット アンド ペーストします。
- enrollment url, （242 ページ） コマンド：（任意）CA の URL。
- ip-address（トラストポイント）, （244 ページ） コマンド：証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレス
- query url, （246 ページ） コマンド：証明書失効リスト（CRL）が発行されるディレクトリ サーバの URL。「ldap://」で始まる文字列だけが受け付けられます。
  CA が Lightweight Directory Access Protocol（LDAP）をサポートしている場合に限り必要です。
- rsakeypair, （248 ページ） コマンド：このトラストポイントに対する名前付きの Rivest, Shamir, and Adelman（RSA）キー ペア。
- serial-number（トラストポイント）, （250 ページ） コマンド：証明書要求内のルータのシリアル番号。
- sftp-password（トラストポイント）, （252 ページ） コマンド：FTP セキュア パスワード。
- sftp-username（トラストポイント）, （254 ページ） コマンド：FTP セキュア ユーザ名。
- subject-name（トラストポイント）, （256 ページ） コマンド：証明書要求内の件名。

タスク ID

タスク ID	操作
crypto	execute

例

次に、**crypto ca trustpoint** コマンドを使用してトラストポイントを作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password xxxxxx
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url
sftp://192.168..254.254/tftpboot/tmordeko/CAcert
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair label-2
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。

コマンド	説明
enrollment retry count, （236 ページ）	ルータが証明書要求を再送信する回数を指定します。
enrollment retry period, （238 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment terminal, （240 ページ）	カットアンドペーストによる手動での証明書登録を指定します。
enrollment url, （242 ページ）	CA の URL を指定します。
query url, （246 ページ）	CRL 分散ポイントの LDAP の URL を指定します。
rsakeypair, （248 ページ）	このトラストポイントに対する名前付きのRSA キー ペアを指定します。
sftp-password（トラストポイント）, （252 ページ）	FTP パスワードを保護します。
sftp-username（トラストポイント）, （254 ページ）	FTP ユーザ名を保護します。

crypto key generate dsa

Digital Signature Algorithm（DSA; デジタル署名アルゴリズム）キー ペアを生成するには、EXEC モードで **crypto key generate dsa** コマンドを使用します。

crypto key generate dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに対して DSA キー ペアを作成するには、**crypto key generate dsa** コマンドを使用します。

DSA キーはペアで作成されます。1 つは DSA 公開キー、もう 1 つは DSA 秘密キーです。

このコマンドの発行時に、ルータにすでにDSAキーが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プロンプトが表示されます。

生成された DSA キーを削除するには、**crypto key zeroize dsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次に、512 ビットの DSA キーを生成する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key generate dsa
The name for the keys will be: the_default
    Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
Choosing a key modulus
How many bits in the modulus [1024]: 512
Generating DSA keys...
Done w/ crypto generate keypair
[OK]
```

関連コマンド

コマンド	説明
crypto key zeroize dsa, （230 ページ）	ルータから DSA キー ペアを削除します。
show crypto key mypubkey dsa, （262 ページ）	ルータの DSA 公開キーを表示します。

crypto key generate rsa

Rivest, Shamir, and Adelman（RSA）キー ペアを作成するには、EXEC モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**usage-keys| general-keys**] [*keypair-label*]

構文の説明

usage-keys	（任意）署名および暗号化用に個別の RSA キー ペアを作成します。
general-keys	（任意）署名および暗号化用に汎用の RSA キー ペアを作成します。
keypair-label	（任意）RSA キー ペアに名前を付ける RSA キー ペアのラベル。

コマンド デフォルト

RSA キー ペアは存在しません。 **usage-keys** キーワードが使用されていない場合、汎用キーが作成されます。 RSA ラベルが指定されていない場合、キーはデフォルトの RSA キーとして生成されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。

RSA キーはペアで作成されます。1 つは RSA 公開キー、もう 1 つは RSA 秘密キーです。

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。 このコマンドによって生成されるキーは、セキュア NVRAM（ユーザには表示されず、別のデバイスにもバックアップされません）に保存されます。

RSA キーを削除するには、**crypto key zeroize rsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次に、RSA キー ペアを作成する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key generate rsa

The name for the keys will be: the_default

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[1024]: <return>
RP/0/RSP0/CPU0:router#
```

関連コマンド

コマンド	説明
crypto key zeroize rsa, （232 ページ）	ルータ用の RSA キー ペアを削除します。
show crypto key mypubkey rsa, （264 ページ）	ルータの RSA 公開キーを表示します。

crypto key import authentication rsa

Rivest, Shamir, and Adelman（RSA）方式を使用して公開キーをインポートするには、EXEC モードで **crypto key import authentication rsa** コマンドを使用します。

crypto key import authentication rsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.9.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

まず、ssh-keygen などのキー生成メカニズムを使用して UNIX クライアント上に RSA 公開キーと秘密キーのキーペアを生成する必要があります。 キーサイズの範囲は、512 ～ 2048 ビットです。

次に、公開キーをボックスに正しくインポートするために、公開キーを Base64 エンコード（バイナリ）形式に変換する必要があります。 nvram ボックスに保存できるキーの数は、個々のキー サイズによって異なります。 このサイズは、ユーザ定義の変数です。

公開キーが生成されると、RSA ベースの認証をイネーブルにするルータ上にキーを配置する必要があります。

タスク ID

タスク ID	操作
crypto	execute

例

次に、公開キーをインポートする例を示します。

```
RP/RSP0/0/CPU0:k2#crypto key import authentication rsa
```

crypto key zeroize dsa

デジタル署名アルゴリズム（DSA）キー ペアをルータから削除するには、EXEC モードで **crypto key zeroize dsa** コマンドを使用します。

crypto key zeroize dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータによって以前生成された DSA キー ペアを削除するには、**crypto key zeroize dsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次に、ルータから DSA キーを削除する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key zeroize dsa
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

関連コマンド

コマンド	説明
crypto key generate dsa, （224 ページ）	DSA キー ペアを作成します。
show crypto key mypubkey dsa, （262 ページ）	ルータの DSA 公開キーを表示します。

crypto key zeroize rsa

ルータからすべての Rivest, Shamir, and Adelman（RSA）キーを削除するには、EXEC モードで **crypto key zeroize rsa** コマンドを使用します。

crypto key zeroize rsa [*keypair-label*]

構文の説明

keypair-label	（任意）削除する RSA キー ペアを指定します。

コマンド デフォルト

キー ペアのラベルが指定されていない場合は、デフォルトの RSA キー ペアが削除されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータによって以前生成されたすべての RSA キーを削除するには、**crypto key zeroize rsa** コマンドを使用します。 このコマンドの実行後、次の 2 つのタスクを追加で実行する必要があります。

- 認証局（CA）の管理者に、CA でルータの証明書を無効にするよう依頼する。このとき、当初 crypto ca enroll, （217 ページ） コマンドを使用してルータの証明書を取得する際に作成したチャレンジ パスワードを CA に提供する必要があります。
- **clear crypto ca certificates** コマンドを使用して、設定から証明書を手動で削除する。

タスク ID

タスク ID	操作
crypto	execute

例

次に、以前生成された汎用 RSA キー ペアを削除する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key zeroize rsa key1
% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

関連コマンド

コマンド	説明
clear crypto ca certificates, （207 ページ）	コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられた証明書をクリアします。
crypto ca enroll, （217 ページ）	CA からルータの証明書を取得します。
crypto key generate rsa, （226 ページ）	RSA キー ペアを生成します。
show crypto key mypubkey rsa, （264 ページ）	ルータの RSA 公開キーを表示します。

description（トラストポイント）

トラストポイントの説明を作成するには、トラストポイント コンフィギュレーション モードで **description** コマンドを使用します。トラストポイントの説明を削除するには、このコマンドの **no** 形式を使用します。

description *string*

no description

構文の説明

string	トラストポイントを説明する文字ストリング

コマンド デフォルト

デフォルトの説明は空白です。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイントの説明を作成するには、トラストポイント コンフィギュレーション モードで **description** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、トラストポイントの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# description this is the primary trustpoint
```

enrollment retry count

ルータが認証局（CA）へ証明書要求を再送信する回数を指定するには、トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。 リトライ回数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。

enrollment retry count *number*

no enrollment retry count *number*

構文の説明

number	ルータが前回の要求で証明書を受け取っていない場合に、証明書要求を再送信する回数。 範囲は 1 ～ 100 です。

コマンド デフォルト

リトライ回数が指定されていない場合、デフォルト値は 10 です。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

証明書の要求後、ルータは CA からの証明書の受け取りを待機します。 指定された時間（リトライ期間）内にルータが証明書を受け取らなかった場合、ルータは再度証明書要求を送信します。 ルータは、有効な証明書を受け取るか、CA から登録エラーが返されるか、または設定されているリトライ回数を超えるまで、要求を送信し続けます。

リトライ回数をデフォルトの 10 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。 リトライ回数を 0 に設定すると、リトライが無制限に行われます。 ルータは、有効な証明書を受け取るまで CA の証明書要求を送信します（リトライ回数は無制限）。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、CA を宣言してリトライ期間を 10 分に変更し、リトライ回数を 60 回に変更する例を示します。 ルータは、証明書を受け取るか、最初の要求の送信後約 10 時間が経過するかのどちらか早い方まで、10 分おきに証明書要求を再送信します（10 分 x 60 回 = 600 分 = 10 時間）。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 60
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry period, （238 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment url, （242 ページ）	認証局（CA）の場所を、CA の URL で指定します。

enrollment retry period

証明書要求をリトライするまでの待機期間を指定するには、トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。 リトライ期間をデフォルトの 1 分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。

enrollment retry period *minutes*

no enrollment retry period *minutes*

構文の説明

minutes	ルータから認証局（CA）へ行われる証明書要求をリトライするまでの期間（分単位）。 範囲は 1 ～ 60 分です。

コマンド デフォルト

minutes：*1*

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

証明書の要求後、ルータは CA からの証明書の受け取りを待機します。 指定された時間（リトライ期間）内にルータが証明書を受け取らなかった場合、ルータは再度証明書要求を送信します。ルータは、有効な証明書を受け取るか、CA から登録エラーが返されるか、または設定されているリトライ回数を超えるまで、要求を送信し続けます。

ルータは、有効な証明書を受け取るまで、CA に証明書要求を送信します（デフォルトでは、ルータは要求を 10 回送信しますが、**enrollment retry count** コマンドを使用して、リトライ回数を変更できます）。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、CA を宣言してリトライ期間を 5 分に変更する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 5
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry count, （236 ページ）	ルータが証明書要求を再送信する回数を指定します。

enrollment terminal

カットアンドペーストによる手動登録を指定するには、トラストポイント コンフィギュレーション モードで **enrollment terminal** 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。

enrollment terminal

no enrollment terminal

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータと認証局（CA）間がネットワーク接続されていない場合、証明書要求と証明書を手動でカット アンド ペーストできます。 **enrollment terminal** コマンドがイネーブルの場合、ルータのコンソール端末に証明書要求が表示され、これにより発行された証明書を端末上で入力できます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、カット アンド ペーストにより証明書の登録を手動で指定する例を示します。 この例で、CA のトラストポイントは myca です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment terminal
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。

enrollment url

認証局（CA）の場所を CA の URL で指定するには、トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。 設定から CA の URL を削除するには、このコマンドの **no** 形式を使用します。

enrollment url *CA-URL*

no enrollment url *CA-URL*

構文の説明

CA-URL	CA サーバの URL。 URL ストリングの先頭は、http://CA_name であることが必要です。CA_name はホストのドメイン ネーム システム（DNS）の名前、または CA の IP アドレス（例：http://ca-server）です。 CA で CA cgi-bin スクリプトの場所が /cgi-bin/pkiclient.exe（デフォルトの CA cgi-bin スクリプトの場所）でない場合は、非標準スクリプトの場所も、http://CA-name/script-location（script-location は CA スクリプトのフル パス）の形式で URL に含める必要があります。

コマンド デフォルト

なし

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

CA の URL を指定するには、**enrollment url** コマンドを使用します。 このコマンドは、**crypto ca trustpoint** コマンドを使用して CA を宣言する際に必要です。 CA スクリプトがデフォルトの cgi-bin スクリプトの場所にロードされない場合は、URL に CA スクリプトの場所を含める必要があります。 CA スクリプトの場所については、CA 管理者に問い合わせます。

次の表に、使用可能な登録方式を示します。

表 *12*：証明書の登録方式

登録方式	説明
SFTP	SFTP: ファイル システムを使用した登録
TFTP[1]	TFTP: ファイル システムを使用した登録

1 登録に TFTP を使用している場合は、URL を tftp://certserver/file_specification の形式で指定する必要があります。（ファイルの指定は任意です）。

TFTP による登録では、登録要求が送信され、CA の証明書とルータの証明書が取得されます。URL でファイルが指定されている場合、ルータはそのファイルに拡張子を追加します。

CA の URL を変更するには、**enrollment url** コマンドを繰り返し実行して、以前の URL を上書きします。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA の宣言に必要な最小限の絶対設定を示します。

```
RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#
            crypto ca trustpoint myca RP/0/RSP0/CPU0:router(config-trustp)#
            enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

関連コマンド

コマンド	説明
crl optional（トラストポイント），（211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint,（221 ページ）	信頼できるポイントを選択した名前で設定します。
ip-address（トラストポイント），（244 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。

ip-address（トラストポイント）

証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定するには、トラストポイント コンフィギュレーション モードで **ip-address** コマンドを使用します。デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

ip-address {*ip-address*| **none**}

no ip-address {*ip-address*| **none**}

構文の説明

ip-address	証明書要求内に含まれるドット付き IP アドレス
none	IP アドレスを証明書要求内に含まないことを指定します。

コマンド デフォルト

証明書の登録時に、IP アドレスを要求するプロンプトが表示されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ip-address コマンドを使用して、指定されたインターフェイスの IP アドレスを証明書要求に含めたり、IP アドレスを証明書要求に含めないよう指定します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、Ethernet 0 インターフェイスの IP アドレスをトラストポイント フロッグの証明書要求に含める例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

次に、IP アドレスを証明書要求に含めない例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems,
C=US
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
```

関連コマンド

コマンド	説明
crl optional（トラストポイント），（211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint,（221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url,（242 ページ）	認証局（CA）の場所を、CA の URL で指定します。
serial-number（トラストポイント），（250 ページ）	証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。
subject-name（トラストポイント），（256 ページ）	証明書要求の所有者名を指定します。

query url

Lightweight Directory Access Protocol（LDAP）プロトコルのサポートを指定するには、トラストポイント コンフィギュレーション モードで **query url** コマンドを使用します。 設定からクエリーの URL を削除するには、このコマンドの **no** 形式を使用します。

query url *LDAP-URL*

no query url *LDAP-URL*

構文の説明

LDAP-URL	LDAP サーバの URL（ldap://another-server など）。 この URL は、ldap://server-name の形式であることが必要です（server-name はホストのドメイン ネーム システム（DNS）名または LDAP サーバの IP アドレス）。

コマンド デフォルト

ルータ証明書の CRLDistributionPoint 拡張子に提示されている URL が使用されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

LDAP は、ルータが証明書失効リスト（CRL）を取得する際に使用されるクエリー プロトコルです。 認証局（CA）の管理者は、CA が LDAP をサポートしているかどうかを把握している必要があります。CA が LDAP をサポートしている場合は、CA 管理者が証明書と証明書失効リストを取得する LDAP の場所を指示できます。

クエリーの URL を変更するには、**query url** コマンドを繰り返し実行して、以前の URL を上書きします。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA が LDAP をサポートしている場合に CA の宣言に必要な設定を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。

rsakeypair

このトラストポイントに対して名前付きの Rivest, Shamir, and Adelman（RSA）キー ペアを指定するには、トラストポイント コンフィギュレーション モードで **rsakeypair** コマンドを使用します。RSA キー ペア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。

rsakeypair *keypair-label*

no rsakeypair *keypair-label*

構文の説明

keypair-label	RSA キー ペアに名前を付ける RSA キー ペアのラベル

コマンド デフォルト

RSA キー ペアが指定されていない場合、このトラストポイントにはデフォルトの RSA キーが使用されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このトラストポイントに **crypto key generate rsa** コマンドを使用して生成された、名前付きの RSA キー ペアを指定するには、**rsakeypair** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、トラストポイント myca に対して名前付きの RSA キー ペア key1 を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair key1
```

関連コマンド

コマンド	説明
crypto key generate rsa, （226 ページ）	RSA キー ペアを生成します。

serial-number（トラストポイント）

ルータのシリアル番号を証明書要求に含めるかどうかを指定するには、トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。 デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

serial-number [none]

no serial-number

構文の説明

none	（任意）証明書要求にシリアル番号を含めないよう指定します。

コマンド デフォルト

証明書の登録時に、シリアル番号を要求するプロンプトが表示されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

serial-number コマンドを使用する前に、**crypto ca trustpoint** コマンドをイネーブルにする必要があります。このコマンドにより、ルータが使用し、トラストポイント コンフィギュレーション モードを開始する認証局（CA）が宣言されます。

このコマンドを使用して、証明書要求でルータのシリアル番号を指定するか、**none** キーワードを使用して、証明書要求にシリアル番号を含めないよう指定します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、ルート証明書の要求でシリアル番号を省略する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
RP/0/RSP0/CPU0:router(config-trustp)# serial-number none
RP/0/RSP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems, C=US
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url, （242 ページ）	認証局（CA）の場所を、CA の URL で指定します。
ip-address（トラストポイント）, （244 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。
subject-name（トラストポイント）, （256 ページ）	証明書要求の所有者名を指定します。

sftp-password（トラストポイント）

FTP パスワードを保護するには、トラストポイント コンフィギュレーション モードで **sftp-password** 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。

sftp-password {*clear text*| **clear** *text*| **password** *encrypted string*}

no sftp-password {*clear text*| **clear** *text*| **password** *encrypted string*}

構文の説明

clear text	クリアテキストのパスワードで、表示目的のためだけに暗号化されます。
password *encrypted string*	パスワードを暗号化形式で入力します。

コマンド デフォルト

デフォルトでは *clear text* 引数が使用されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

パスワードは暗号化形式で保存され、プレーンテキストとしては保存されません。 コマンドライン インターフェイス（CLI）には、パスワード入力を指定するためのプロビジョニング（クリアおよび暗号化など）が含まれます。

SFTP プロトコルの一部として、ユーザ名とパスワードが必要です。 sftp:// というプレフィックスで始まる URL を指定する場合、トラストポイントで **sftp-password** コマンドに対するパラメータを設定する必要があります。 設定しなかった場合、証明書の手動登録に使用する証明書を SFTP サーバから取得できません。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、FTP パスワードを暗号化形式で保護する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
sftp-username（トラストポイント）, （254 ページ）	FTP ユーザ名を保護します。

sftp-username（トラストポイント）

FTPユーザ名を保護するには、トラストポイント コンフィギュレーション モードで**sftp-username**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。

sftp-username *username*

no sftp-username *username*

構文の説明

username	ユーザ名。

コマンド デフォルト

なし

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク IDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

sftp-username コマンドが使用されるのは、URL のプレフィックスに sftp:// が含まれる場合だけです。 プレフィックスで sftp:// が指定されていない場合、SFTP を使用した証明書の手動登録は失敗します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、FTP ユーザ名を保護する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
sftp-password（トラストポイント）, （252 ページ）	FTP パスワードを保護します。

subject-name（トラストポイント）

証明書要求で件名を指定するには、トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。 設定から件名をクリアするには、このコマンドの **no** 形式を使用します。

subject-name *x.500-name*

no subject-name *x.500-name*

構文の説明

x.500-name	（任意）証明書要求で使用される件名を指定します。

コマンド デフォルト

x.500-name 引数が指定されていない場合は、デフォルトの件名である fully qualified domain name（FQDN; 完全修飾ドメイン名）が使用されます。

コマンド モード

トラストポイント 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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

subject-name コマンドを使用する前に、**crypto ca trustpoint** コマンドをイネーブルにする必要があります。このコマンドにより、お使いのルータが使用し、トラストポイント コンフィギュレーション モードを開始する認証局（CA）が宣言されます。

subject-name コマンドは、自動登録に設定できる属性であるため、このコマンドを発行すると、登録時に件名を要求するプロンプトが表示されなくなります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、フロッグ証明書に件名を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （211 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （221 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url, （242 ページ）	認証局（CA）の場所を、CA の URL で指定します。
ip-address（トラストポイント）, （244 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。
serial-number（トラストポイント）, （250 ページ）	証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。

show crypto ca certificates

ご使用の証明書および認証局（CA）証明書に関する情報を表示するには、EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

次の証明書に関する情報を表示するには、**show crypto ca certificates** コマンドを使用します。

- ご使用の証明書（CA に要求した場合。**crypto ca enroll** コマンドを参照）
- CA 証明書（証明書を受け取っている場合。**crypto ca authenticate** コマンドを参照）

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ca certificates** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca certificates
Trustpoint       : msiox
================================================
```

```
CAa certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Router certificate
  Status         : Available
  Key usage      : Signature
  Serial Number  : 38:6B:C6:B8:00:04:00:00:01:45
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:30:03 UTC Mon Apr 10 2006
  Validity End   : 08:40:03 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX
Router certificate
  Status         : Available
  Key usage      : Encryption
  Serial Number  : 38:6D:2B:A7:00:04:00:00:01:46
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:31:34 UTC Mon Apr 10 2006
  Validity End   : 08:41:34 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: msiox
```

関連コマンド

コマンド	説明
crypto ca authenticate, （213 ページ）	CA の証明書を取得することにより、CA を認証します。
crypto ca enroll, （217 ページ）	CA からルータの証明書を取得します。
crypto ca import, （219 ページ）	認証局（CA）証明書を、TFTP、SFTP、または端末でのカット アンド ペーストを通じて、手動でインポートします。
crypto ca trustpoint, （221 ページ）	トラストポイントを選択した名前で設定します。

show crypto ca crls

ローカル キャッシュの証明書失効リスト（CRL）に関する情報を表示するには、EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ca crls** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca crls
CRL Entry
================================================
Issuer : cn=xyz-w2k-root,ou=HFR,o=Cisco System,l=San Jose,st=CA,c=US
Last Update : [UTC] Thu Jan 10 01:01:14 2002
Next Update : [UTC] Thu Jan 17 13:21:14 2002
CRL Distribution Point :
http://xyz-w2k.cisco.com/CertEnroll/xyz-w2k-root.crl
```

関連コマンド

コマンド	説明
clear crypto ca crl, （209 ページ）	ルータに保存されているすべての CRL をクリアします。

show crypto key mypubkey dsa

ルータの Directory System Agent（DSA）公開キーを表示するには、EXEC モードで **show crypto key mypubkey dsa** コマンドを使用します。

show crypto key mypubkey dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto key mypubkey dsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey dsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 17:33:23 UTC Thu Sep 18 2003
Data :
3081F230 81AA0605 2B0E0302 0C3081A0 02020200 024100C8 A36B6179 56B8D620
1F77595C 32EF3004 577A9F79 0A8ABDA4 89FB969D 35C04E7E 5491ED4E 120C657C
610576E5 841696B6 0948846C C92F56E5 B4921458 70FC4902 1500AB61 5C0D63D3
EB082BB9 F16030C5 AA0B5D1A DFE50240 73F661EA 9F579E77 B413DBC4 9047B4F2
```

```
10A1CFCB 14D98B57 3E0BBA97 9B5120AD F52BBDC7 15B63454 8CB54885 92B6C9DF
7DC27768 FD296844 42024945 5E86C81A 03430002 4071B49E F80F9E4B AF2B62E7
AA817460 87EFD503 C668AD8C D606050B 225CC277 7C0A0974 8072D7D7 2ADDDE42
329FE896 AB015ED1 3A414254 6935FDCA 0043BA4F 66
```

関連コマンド

コマンド	説明
crypto key generate dsa, （224 ページ）	DSA キー ペアを作成します。
crypto key zeroize dsa, （230 ページ）	ルータからすべての DSA キーを削除します。

show crypto key mypubkey rsa

ルータの Rivest、Rivest, Shamir, and Adelman（RSA）公開キーを表示するには、EXEC モードで **show crypto key mypubkey rsa** コマンドを使用します。

show crypto key mypubkey rsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto key mypubkey rsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4D164D F6EDB78B 926B1DDE 0383027F BA71BCC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4BA71BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
```

```
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6F40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCE8F3DF DD1327D8 C1C30C45 2EEB4981 B1B48D2B 1AF14665 178058FB 8F6BB6BB
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF EC8E5822 9B020301 0001
```

関連コマンド

コマンド	説明
crypto key generate rsa, （226 ページ）	RSA キー ペアを生成します。
crypto key zeroize rsa, （232 ページ）	ルータからすべての RSA キーを削除します。

Software Authentication Manager コマンド

ここでは、Software Authentication Manager（SAM）を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

SAM の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Configuring Software Authentication Manager on* Cisco ASR 9000 Series Router」モジュールを参照してください。

sam add certificate

証明書テーブルに新しい証明書を追加するには、EXEC モードで **sam add certificate** コマンドを使用します。

sam add certificate *filepath location* {**trust**| **untrust**}

構文の説明

filepath	証明書のソース ロケーションへの絶対パス。
location	証明書の保管場所。 **root**、**mem**、**disk0**、**disk1**、または**ルータ上の他のフラッシュ デバイス名**のいずれかを使用します。
trust	Software Authentication Manager（SAM）による検証を行わずに、証明書を証明書テーブルに追加します。ルート証明書を追加するには、**trust** キーワードを使用する必要があります。ルート証明書は、**untrust** キーワードを使用して追加できません。
untrust	SAM が証明書を検証してから証明書テーブルに追加します。ルート証明書は、**untrust** キーワードを使用して追加できません。ルート証明書を追加するには、**trust** キーワードを使用する必要があります。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

セキュリティ上の理由から、**sam add certificate** コマンドはネットワーキング デバイスのコンソール ポートまたは AUX ポート以外からは発行できません。このコマンドは、ネットワーキング デバイスの他のインターフェイスへの Telnet 接続からは発行できません。

証明書は、ネットワークデバイスにコピーしなければ、証明書テーブルに追加できません。 証明書テーブルに証明書がすでに存在する場合は、SAM が追加を拒否します。

ルート証明書を追加する場合は、次の注意事項に従ってください。

- ルート ロケーションに追加できるのは、Certificate Authority（CA; 認証局）ルート証明書だけです。
- ルート証明書を追加するには、**trust** キーワードを使用する必要があります。 ルート証明書は、**untrust** キーワードを使用して追加できません。

trust キーワードを使用すると、信頼できるソースから新しい証明書を受信したので、SAM による検証を行わなくても十分に信頼できると見なされます。 信頼できるソースから証明書を取得する 1 例は、ユーザ認証を要求する CA サーバ（Cisco.com など）から証明書をダウンロードする場合です。 別の例は、個人の認識票のチェックなどによって確認できる個人またはエンティティからの証明書を取得する場合です。 SAM が提供する検証による保護を実行しない場合、他の有効なプロセスによって証明書の識別情報および整合性を確認する必要があります。

メモリ（**mem**）ロケーションに追加された証明書は、メモリにインストールされているソフトウェアを検証します。 **disk0** ロケーションまたは **disk1** ロケーションに追加された証明書は、それぞれこれらのデバイスを検証します。

（注） 証明書の失効を示すメッセージが表示されて **sam add certificate** コマンドが失敗する場合、ネットワーキング デバイスのクロックが正しく設定されていない可能性があります。 **show clock** コマンドを使用して、クロックが正常に設定されているかを確認します。

タスク ID

タスク ID	操作
crypto	execute

例

次に、最初に証明書の検証を行わずに、/bootflash/ca.bin にある証明書をルート ロケーションの証明書テーブルに追加する例を示します。

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/ca.bin root trust

SAM: Successful adding certificate /bootflash/ca.bin
```

次に、検証後に、/bootflash/css.bin にある証明書をメモリ（**mem**）ロケーションの証明書テーブルに追加する例を示します。

```
RP/0/RSP0/CPU0:router# sam add certificate /bootflash/css.bin mem untrust

SAM: Successful adding certificate /bootflash/css.bin
```

関連コマンド

コマンド	説明
sam delete certificate, （271 ページ）	証明書テーブルから証明書を削除します。
show sam certificate, （278 ページ）	証明書の場所など、証明書テーブル内の情報を表示します。
show clock	ネットワーキングデバイスのクロック情報を表示します。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。

sam delete certificate

証明書テーブルから証明書を削除するには、EXEC モードで **sam delete certificate** コマンドを使用します。

sam delete certificate *location certificate-index*

構文の説明

location	証明書の保管場所。**root**、**mem**、**disk0**、**disk1**、または**ルータ上の他のフラッシュ デバイス名**のいずれかを使用します。
certificate-index	1 ～ 65000 の範囲の番号。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

セキュリティ上の理由から、**sam delete certificate** コマンドはネットワーキング デバイスのコンソール ポート以外からは発行できません。このコマンドは、ネットワーキング デバイスの他のインターフェイスへの Telnet 接続からは発行できません。

インデックス番号を使用して証明書を表示するには、**show sam certificate summary** コマンドを使用します。

無意識のうちに認証局（CA）証明書を削除してはいけないので、CA 証明書を削除しようとすると、Software Authentication Manager（SAM）がユーザに確認を求めます。

システムに保存されている証明書がすでに有効ではない場合（たとえば、証明書が失効した場合）、**sam delete certificate** コマンドを使用してリストから証明書を削除できます。

タスク ID

タスク ID	操作
crypto	execute

例

次に、インデックス番号 2 で識別される証明書をメモリ ロケーションから削除する例を示します。

```
RP/0/RSP0/CPU0:router# sam delete certificate mem 2

SAM: Successful deleting certificate index 2
```

次に、インデックス番号 1 で識別される証明書のルート ロケーションからの削除をキャンセルする例を示します。

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): N
SAM: Delete certificate (index 1) canceled
```

次に、インデックス番号 1 で識別される証明書をルート ロケーションから削除する例を示します。

```
RP/0/RSP0/CPU0:router# sam delete certificate root 1

Do you really want to delete the root CA certificate (Y/N): Y
SAM: Successful deleting certificate index 1
```

関連コマンド

コマンド	説明
sam add certificate, （268 ページ）	証明書テーブルに新しい証明書を追加します。
show sam certificate, （278 ページ）	証明書の保存場所など、証明書テーブル内の情報を表示します。

sam prompt-interval

Software Authentication Manager（SAM）が起動時に異常な状況を検出したときに、ユーザに入力を求めた後で待機するインターバルを設定し、指定されたインターバル内にユーザからの入力を受信しなかった場合のSAMの応答方法を決定するには、グローバル コンフィギュレーション モードで **sam promptinterval** コマンドを使用します。 プロンプト インターバルおよび応答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。

sam promptinterval *time-interval* {**proceed| terminate**}

no sam promptinterval *time-interval* {**proceed| terminate**}

構文の説明

time-interval	プロンプト時間。0 ～ 300 秒の範囲です。
proceed	プロンプト インターバルが終了したとき、SAM が「yes」を受信したように応答させます。
terminate	プロンプトインターバルが終了したとき、SAMが「no」を受信したように応答させます。

コマンド デフォルト

SAM のデフォルトの応答は、10 秒間待機してから認証タスクを終了させます。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

起動時のSAMの初期化中に失効した証明書などシステムが例外条件を検出した時に実行するアクションを制御するには、**sam prompt-interval** コマンドを使用します。 次のメッセージは、認証局（CA）証明書が失効したという異常な状況を検出した場合に表示されます。

```
SAM detects expired CA certificate. Continue at risk (Y/N):
```

ユーザがプロンプトに対して応答するまで、または **sam prompt-interval** コマンドによって制御されるインターバルが終了するまでのいずれか早いイベントを待機します。 プロンプトに対して「N」と応答すると、起動プロセスは完了できますが、パッケージはインストールできません。

次のメッセージは、Code Signing Server（CSS; コード サイニング サーバ）証明書が失効したという異常な状況を検出した場合に表示されます。

```
SAM detects CA certificate (Code Signing Server Certificate Authority) has expired. The
validity period is Oct 17, 2000 01:46:24 UTC - Oct 17, 2015 01:51:47 UTC. Continue at risk?
 (Y/N) [Default:N w/in 10]:
```

プロンプトに対して応答しないと、SAM は指定されたインターバルが終了するまで待機し、（**proceed** キーワードまたは **terminate** キーワードのいずれかを使用して）**sam prompt-interval** コマンドで指定されたアクションを実行します。

proceed キーワードを使用してこのコマンドを入力した場合、SAM は指定されたインターバルが終了するまで待機し、ユーザがプロンプトに対して「yes」と応答したように続行します。

terminate キーワードを使用してコマンドを入力した場合、SAM は指定されたインターバルが終了するまで待機し、ユーザがプロンプトに対して「no」と応答したように続行します。 このようにコマンドを使用することによって、システム コンソールが無人の場合にシステムが無期限に待機しないようにさせます。

（注） ソフトウェアが起動した後に、このコマンドを使って *time-interval* 引数を設定しても無効です。この値が適用されるのは、起動時だけです。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、プロンプトに対するユーザの応答を SAM に 30 秒間待機させ、要求された SAM プロセス タスクを終了させる方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# sam promptinterval 30 terminate
```

関連コマンド

コマンド	説明
show sam sysinfo, （292 ページ）	SAM の現在のステータス情報を表示します。

sam verify

Message Digest 5（MD5）ハッシュ アルゴリズムを使用してフラッシュ メモリ カードのソフトウェア コンポーネントの整合性を確認し、送信中に改ざんされていないことを保証するには、EXEC モードで **sam verify** コマンドを使用します。

sam verify {*location*| *file-system*} {**MD5**| **SHA** [*digest*]}

構文の説明

location	フラッシュ メモリ カード スロットの名前。disk0 または disk1 のいずれかです。
file-system	確認対象のファイルへの絶対パス。
MD5	単方向のハッシュ アルゴリズムを指定し、指定されたソフトウェア コンポーネントの 128 ビットのハッシュ（またはメッセージ ダイジェスト）を生成します。
SHA	セキュア ハッシュ アルゴリズム（264 ビット未満の長さのメッセージを受け取り、160 ビットのメッセージ ダイジェストを生成するハッシュ アルゴリズム）を指定します。大きいメッセージ ダイジェストは、ブルートフォース コリジョンおよび反転攻撃に対するセキュリティを提供します。
digest	（任意）ハッシュ アルゴリズムによって生成されるメッセージ ダイジェストは、ソフトウェア コンポーネントの整合性を確認する際に比較されます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

所定のデバイス用にメッセージ ダイジェストを生成するには、**sam verify** コマンドを使用します。メッセージ ダイジェストは、フラッシュ メモリ カード上のソフトウェアが送信中に改ざんされていないことを確認するのに有用です。 このコマンドによって、送信時と受信時のソフトウェアの整合性を比較するために使用できるハッシュ コードが生成されます。

たとえば、ソフトウェアがプリインストールされているフラッシュ メモリ カードと以前に生成された MD5 メッセージ ダイジェストがある場合、**sam verify** コマンドを使用してソフトウェアの整合性を確認できます。

`sam verify` *device* `MD5` *digest*
device 引数は、フラッシュ デバイスを指定します。 *digest* 引数は、ソフトウェアのオリジネータから供給されたメッセージ ダイジェストを指定します。

このメッセージ ダイジェストと **sam verify** コマンドによって生成されたメッセージ ダイジェストが一致した場合、ソフトウェア コンポーネントは有効です。

（注） フラッシュ メモリ カードにロードされている一連のファイルとは異なるファイルを使用して、宛先ネットワーキング デバイスでフラッシュ メモリ コードのコンテンツについてハッシュ コードを計算する必要があります。 権限のないユーザが同じソフトウェア バージョンを使用して目的とする（一致する）ハッシュ コードを生成し、それによって誰かが新しいソフトウェアを改ざんしたように偽装できます。

タスク ID

タスク ID	操作
crypto	execute

例

ここでは、不一致に対する Software Authentication Manager（SAM）の応答を示すための、第 3 の **sam verify** コマンドを示します。このコマンドは、メッセージ ダイジェストが不一致であることを示すメッセージとともに発行されます。 次の例は、MD5 を使用してスロット 0 のフラッシュ メモリ カード上のファイル システム全体についてメッセージ ダイジェストを生成し、ダイジェスト比較を実行するための入力値としてこれらのメッセージ ダイジェストを使用する方法を示します。

```
RP/0/RSP0/CPU0:router# sam verify disk0: MD5

Total file count in disk0: = 813
082183cb6e65a44fd7ca95fe8e93def6

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 082183cb6e65a44fd7ca95fe8e93def6

Total file count in disk0: = 813
Same digest values

RP/0/RSP0/CPU0:router# sam verify disk0: MD5 3216c9282d97ee7a40b78a4e401158bd

Total file count in disk0: = 813
Different digest values
```

次の例は、MD5 を使用してメッセージ ダイジェストを生成し、これらのメッセージ ダイジェストをダイジェスト比較を実行するための入力値として使用する方法を示します。

```
RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5
```

```
38243ffbbe6cdb7a12fa9fa6452956ac
RP/0/RSP0/CPU0:router# sam verify disk0: /crl_revoked.bin MD5 38243ffbbe6cdb7a12fa9fa6452956ac
Same digest values
```

show sam certificate

証明テーブル内の情報を表示するには、EXEC モードで **show sam certificate** コマンドを使用します。

構文の説明

detail	選択された（*location* 引数および *certificate-index* 引数で指定された）テーブル エントリのすべての属性を表示します。
location	表示するエントリの保存場所を指定します。 次のいずれかの値を使用します。 • **root**：証明書は、ルート デバイスに保存されます。 • **mem**：証明書は、メモリに保存されます。 • *device-name*：証明書は、指定されたデバイスに保存されます。 disk0、disk1、またはルータ上の他のフラッシュ デバイス名を使用します。 フラッシュ デバイス名は、**show filesystem** コマンドを使用して検索できます。
certificate-index	表示する証明書テーブル内のエントリのインデックス番号。1 ～ 65000 の範囲です。
brief	証明書テーブル内のエントリの属性のサブセットを表示します。
location	表示するエントリの保存場所を指定します。 次のいずれかの値を使用します。 • **all**：すべての証明書の属性のサブセットを表示します。 • **root**：ルートデバイスに保存されるすべての証明書の属性のサブセットを表示します。 • **mem**：メモリに保存されるすべての証明書の属性のサブセットを表示します。 • *device-name*：指定されたデバイスに保存されるすべての証明書の属性のサブセットを表示します。 disk0、disk1、またはルータ上の他のフラッシュ デバイス名を使用します。 フラッシュ デバイス名は、**show filesystem** コマンドを使用して検索できます。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システムに保存されているすべての証明書を表示するときは、**show sam certificate** コマンドを使用します。 属性は、認証番号、認証フラグ、シリアル番号、サブジェクト名、発行元、バージョン、発行アルゴリズム、発効日と失効日、公開キー、およびシグニチャです。

認証番号を取得するには、*certificate-index* 引数を使用します。 **brief** キーワードと **all** キーワードを使用した場合、テーブル内のすべてのエントリに対して、選択されたすべての属性が表示されます。

タスク ID

タスク ID	操作
none	—

例

次の例では、ルート ロケーションに 1 つの証明書が存在し、ディスク 0 に 1 つの証明書が存在します。 次の出力例は、**show sam certificate** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam certificate
            brief

            all

-------------------- SUMMARY OF CERTIFICATES -------------------

Certificate Location    :root
Certificate Index       :1
Certificate Flag        :VALIDATED
  Serial Number  :32:E0:A3:C6:CA:00:39:8C:4E:AC:22:59:1B:61:03:9F
  Subject Name   :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct 17 01:46:24 2000
  Validity End   :[UTC] Sat Oct 17 01:51:47 2015
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED
```

```
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate %20Authority.crl
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *13*：*show sam certificate summary all* フィールドの説明

フィールド	説明
Certificate Location	証明書の場所。**root**、**mem**、**disk0**、**disk1**、または他のフラッシュ デバイス名のいずれかです。
Certificate Index	Software Authentication Manager が証明書に自動的に割り当てるインデックス番号。
Certificate Flag	TRUSTED、VALIDATED、EXPIRED、または REVOKED のいずれかです。
Serial Number	発行元によって割り当てられた、証明書の一意のシリアル番号。
Subject Name	証明書の発行対象エンティティの名前。
Issued By	証明書を発行したエンティティの名前。

show sam certificate コマンドを実行した結果である次の出力例は、特定の SAM の詳細の表示方法を示します。

```
RP/0/RSP0/CPU0:router# show sam certificate detail mem 1
-------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2003
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
```

```
 Public Key BER (294 bytes):
30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
35 02 03 01 00 01                                    [5.....]
 Certificate signature (256 bytes):
67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m..............]
b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y.............e.]
e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
e1 ea 3b 27 50 42 08 d6 71 eb 66 37 b1 f5 f6 5d      [..;'PB..q.f7...]]
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *14*：*show sam certificate detail mem 1* フィールドの説明

フィールド	説明
Certificate Location	証明書の場所。**root**、**mem**、**disk0**、または**disk1**のいずれかです。
Certificate Index	SAM が証明書に自動的に割り当てたインデックス番号。
Certificate Flag	TRUSTED、VALIDATED、EXPIRED、または REVOKED のいずれかです。
Serial Number	発行元によって割り当てられた、証明書の一意のシリアル番号。
Subject Name	証明書の発行対象エンティティの名前。
Issued By	証明書を発行したエンティティの名前。

フィールド	説明
Version	証明書の ITU-T X.509 バージョン。 バージョンは、1（X.509v1）、2（X.509v2）、または 3（X.509v3）です。
Issuing Algorithm	発行元が証明書のサインに使用したハッシュおよび公開キーアルゴリズム。
Public Key	証明書のサブジェクト公開キー。
Certificate signature	証明書の暗号化されたハッシュ値（またはシグニチャ）。 証明書のハッシュ値は、発行元の秘密キーを使用して暗号化されます。

show sam crl

Certificate Revocation List（CRL; 証明書失効リスト）テーブル内の情報を表示するには、EXEC モードで **show sam crl** コマンドを使用します。

show sam crl {**summary**| **detail** *crl-index*}

構文の説明

summary	テーブル内のすべてのエントリについて、選択された属性を表示します。
detail	（特に *crl-index* 引数によって）選択されたテーブル エントリの属性をすべて表示します。
crl-index	エントリのインデックス番号。1 ～ 65000 の範囲です。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システムに現在保存されている失効した証明書をすべて表示する場合は、**show sam crl** コマンドを使用します。 属性は、CRL インデックス番号、発行元、および更新情報です。

CRL インデックス番号を取得するには、**summary** キーワードを使用します。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、**summary** キーワードを使用して **show sam crl** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam crl summary

---------------------- SUMMARY OF CRLs --------------------------

CRL Index       :1
Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O =
Cisco,
  L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                     Sep 09, 2002 03:50:41 GMT
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *15*：*show sam crl summary* フィールドの説明

フィールド	説明
CRL Index	エントリのインデックス番号。1 ～ 65000 の範囲です。インデックス番号は、証明書失効リスト テーブルに保存されます。
Issuer	この CRL を発行した認証局（CA）。
Including updates of	CRL テーブルに含まれる、この CA が発行した CRL のバージョン。

次の出力例は、**detail** キーワードを使用して **show sam crl** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam crl detail 1

------------------------------------------------------------------

CRL Index      :1

-------------- CERTIFICATE REVOCATION LIST (CRL) -----------------

Issuer:CN = Code Sign Server Certificate Manager, OU = Cisco HFR mc , O = Cisco,
 L = San Jose, ST = CA, C = US, EA =<16> iosmx-css-cert@cisco.com
Including updates of:
                    Sep 09, 2002 03:50:41 GMT
Revoked certificates include:

   Serial #:61:2C:5C:83:00:00:00:00:00:44, revoked on Nov 03, 2002 00:59:02 GMT
   Serial #:21:2C:48:83:00:00:00:00:00:59, revoked on Nov 06, 2002 19:32:51 GMT
------------------------------------------------------------------------------
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *16* : *show sam crl detail* フィールドの説明

フィールド	説明
CRL Index	エントリのインデックス番号。1 ～ 65000 の範囲です。インデックス番号は、証明書失効リスト テーブルに保存されます。
Issuer	この CRL を発行した CA。
Including updates of	CRL テーブルに含まれる、この CA が発行した CRL のバージョン。
Revoked certificates include	失効した証明書のリスト。証明書のシリアル番号および証明書の失効日時を含みます。

show sam log

Software Authentication Manager（SAM）ログ ファイルの内容を表示するには、EXEC モードで **show sam log** コマンドを使用します。

show sam log [*lines-number*]

構文の説明

lines-number	（任意）表示する SAM ログ ファイルの行数。0 ～ 200 の範囲です。0 は、ログ ファイル内のすべての行を表示し、200 は、最新の 200 行（ログ ファイル内の行数が 200 未満の場合は、存在する行数）を表示します。

コマンド デフォルト

lines-number 引数を使用しない **show sam log** コマンドは、ログ ファイル内のすべての行を表示します。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SAM ログ ファイルは、失効した証明書または無効な証明書、テーブル ダイジェストの不一致、および SAM サーバの再起動など、SAM テーブルに対する変更を記録します。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、**show sam log** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam log

06/16/02 12:03:44 UTC Added certificate in table root/1 CN = Certificate Manage, 0x01
06/16/02 12:03:45 UTC SAM server restarted through router reboot
06/16/02 12:03:47 UTC Added CRL in table CN = Certificate Manage, updated at Nov 10, 2001
   04:11:42 GMT
06/16/02 12:03:48 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:16:16 UTC SAM server restarted through router reboot
06/16/02 12:25:02 UTC SAM server restarted through router reboot
06/16/02 12:25:04 UTC Added certificate in table mem:/1 CN = Certificate Manage, 0x1e
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:39:30 UTC SAM server restarted through router reboot
06/16/02 12:40:57 UTC Added certificate in table mem/1 CN = Certificate Manage, 0x1e

33 entries shown
```

出力の各行は、テーブルの変更、失効した証明書または無効な証明書、テーブル ダイジェストの不一致、または SAM サーバの再起動など、ログに記録された特定のイベントを示します。

show sam package

ネットワーキング デバイスにインストールされている特定パッケージのソフトウェアの認証に使用された証明書に関する情報を表示するには、EXEC モードで **show sam package** コマンドを使用します。

show sam package *package-name*

構文の説明

package-name	メモリ デバイス（**disk0:**、**disk1:**、**mem**: など）およびファイルへのファイル システム パスなどソフトウェア パッケージの場所。インストール マネージャ パッケージの名前およびロケーション情報を表示するには、**show install all** コマンドを使用します。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ソフトウェア パッケージのインストール場所および名前を表示するには、**show install all** コマンド（たとえば、mem:ena-base-0.0.0 または disk1:crypto-exp-lib-0.4.0）を使用します。次に、**show sam package** コマンドを使用して、インストールされているパッケージの認証に使用された証明書に関する情報を表示します。 **show sam package** コマンドは、**detail** キーワードを使用して **show sam certificate** コマンドを使用した場合と同じ情報を表示します。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、**show sam package** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam package mem:12k-rp-1.0.0

------------------------------------------------------------

Certificate Location    :mem
Certificate Index       :1
Certificate Flag        :VALIDATED

----------------------- CERTIFICATE ------------------------
  Serial Number  :01:27:FE:79:00:00:00:00:00:05
  Subject Name   :
        cn=Engineer code sign certificate
  Issued By      :
        cn=Code Signing Server Certificate Authority,o=Cisco,c=US
  Validity Start :[UTC] Tue Oct  9 23:14:28 2001
  Validity End   :[UTC] Wed Apr  9 23:24:28 2002
  CRL Distribution Point

file://\\CodeSignServer\CertEnroll\Code%20Signing%20Server%20Certificate
%20Authority.crl
  Version 3 certificate
  Issuing Algorithm:MD5withRSA
  Public Key BER (294 bytes):
 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01      [0.."0...*.H.....]
 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01      [........0.......]
 00 be 75 eb 9b b3 d9 cb 2e d8 c6 db 68 f3 5a ab      [..u.........h.Z.]
 0c 17 d3 84 16 22 d8 18 dc 3b 13 99 23 d8 c6 94      [....."...;..#...]
 91 15 15 ec 57 ea 68 dc a5 38 68 6a cb 0f 4b c2      [....W.h..8hj..K.]
 43 4b 2d f9 92 94 93 04 df ff ca 0b 35 1d 85 12      [CK-.........5...]
 99 e9 bd bc e2 98 99 58 fe 6b 45 38 f0 52 b4 cb      [.......X.kE8.R..]
 a9 47 cd 22 aa ce 70 0e 4c 9b 48 a1 cf 0f 4a db      [.G."..p.L.H...J.]
 35 f5 1f 20 b7 68 cb 71 2c 27 01 84 d6 bf 4e d1      [5.. .h.q,'....N.]
 ba e1 b2 50 e7 f1 29 3a b4 85 3e ac d7 cb 3f 36      [...P..):..>...?6]
 96 65 30 13 27 48 84 f5 fe 88 03 4a d7 05 ed 72      [.e0.'H.....J...r]
 4b aa a5 62 e6 05 ac 3d 20 4b d6 c9 db 92 89 38      [K..b...= K.....8]
 b5 14 df 46 a3 8f 6b 05 c3 54 4d a2 83 d4 b7 02      [...F..k..TM.....]
 88 2d 58 e7 a4 86 1c 48 77 68 49 66 a1 35 3e c4      [.-X....HwhIf.5>.]
 71 20 aa 18 9d 9f 1a 38 52 3c e3 35 b2 19 12 ad      [q .....8R<.5....]
 99 ad ce 68 8b b0 d0 29 ba 25 fd 1e e0 5d aa 12      [...h...).%...]..]
 9c 44 89 63 89 62 e3 cb f3 5d 5f a3 7c b7 b9 ef      [.D.c.b...]_.|...]
 01 89 5b 33 35 a8 81 60 38 61 4e d8 4f 6a 53 70      [..[35..`8aN.OjSp]
 35 02 03 01 00 01                                    [5.....]
  Certificate signature (256 bytes):
 67 f6 12 25 3f d4 d2 dd 6a f7 3e 55 b8 9f 33 53      [g..%?...j.>U..3S]
 20 4d d1 17 54 08 8a 70 22 35 92 59 9c 03 9c 0f      [ M..T..p"5.Y....]
 ce 46 3c 06 74 d0 a9 8e b1 88 a2 35 b3 eb 1b 00      [.F<.t......5....]
 5c 6d bb 1d b5 ad 17 19 f2 c6 96 87 9b e7 15 01      [\m..............]
 b2 04 af 7d 92 60 d9 ee ef bc 60 4e 2e af 84 e2      [...}.`....`N....]
 42 fe 07 71 7e fc ee ee f5 d1 6d 71 e7 46 f0 97      [B..q~.....mq.F..]
 e0 e8 b3 0e f9 07 e0 de 6e 36 5a 56 1e 80 10 05      [........n6ZV....]
 59 d9 88 ba f7 a3 d1 f6 cd 00 12 9f 90 f0 65 83      [Y.............e.]
 e9 0f 76 a4 da eb 1b 1b 2d ea bd be a0 8a fb a7      [..v.....-.......]
 a5 18 ff 9f 5c e9 99 66 f0 d3 90 ae 49 3f c8 cc      [....\..f....I?..]
 32 6b db 64 da fd f5 42 ea bc f3 b0 8a 2f 17 d8      [2k.d...B...../..]
 cf c0 d8 d4 3a 41 ae 1d cf 7a c6 a6 a1 65 c2 94      [....:A...z...e..]
 8a ba ea d3 da 3e 8a 44 9b 47 35 10 ab 61 1b 4f      [.....>.D.G5..a.O]
 82 dd 59 16 d5 f2 1d f3 c2 08 cc 1c 7f ab be 9c      [..Y.............]
 be 52 73 ea e0 89 d7 6f 4d d0 d8 aa 3d 50 d6 b0      [.Rs....oM...=P..]
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *17* : ***show sam package*** フィールドの説明

フィールド	説明
Certificate Location	証明書の場所。**root**、**mem**、**disk0**、または**disk1** のいずれかです。
Certificate Index	Software Authentication Manager（SAM）が証明書に自動的に割り当てるインデックス番号。
Certificate Flag	TRUSTED、VALIDATED、EXPIRED、または REVOKED のいずれかです。
Serial Number	発行元によって割り当てられた、証明書の一意のシリアル番号。
Subject Name	証明書の発行対象エンティティの名前。
Issued By	証明書を発行したエンティティの名前。
Version	証明書の ITU-T X.509 バージョン。 バージョンは、1（X.509v1）、2（X.509v2）、または 3（X.509v3）です。
Issuing Algorithm	発行元が証明書のサインに使用したハッシュおよび公開キーアルゴリズム。
Public Key	証明書のサブジェクト公開キー。
Certificate signature	証明書の暗号化されたハッシュ値（またはシグニチャ）。 証明書のハッシュ値は、発行元の秘密キーを使用して暗号化されます。

関連コマンド

コマンド	説明
show install	ソフトウェアパッケージのインストール場所および名前を表示します。 **all** キーワードを使用して、すべての場所からアクティブなパッケージを表示できます。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。
show sam certificate, （278 ページ）	SAM 証明書テーブル内の情報を表示します。

show sam sysinfo

Software Authentication Manager（SAM）の現在の設定を表示するには、EXEC モードで **show sam sysinfo** コマンドを使用します。

show sam sysinfo

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SAM の設定を確認するには、**show sam sysinfo** コマンドを使用します。

ディスプレイには、SAM のステータス、現在のプロンプト インターバル設定、および現在のプロンプトのデフォルト応答が表示されます。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、**show sam sysinfo** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show sam sysinfo

Software Authentication Manager System Information
==========================================
Status                  : running
```

```
Prompt Interval         : 10 sec
Prompt Default Response : NO
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *18* : *show sam sysinfo* フィールドの説明

フィールド	説明
Status	running または not running のいずれか。 SAM が稼働していなければ、システム マネージャによってこの状態が検出され、SAM の再起動が試行されます。既定の再試行回数を実行しても、問題が発生するために SAM を再起動できない場合、SAM は再起動されません。 このような場合は、Cisco Technical Assistance Center（TAC）の担当者にご連絡ください。
Prompt Interval	プロンプト インターバルの現在の設定。 インターバルは、0～300秒の範囲に設定できます。出力例に示されている値（10秒）は、デフォルトです。
Prompt Default Response	ユーザがプロンプトに対して応答する前にプロンプト インターバルが終了した場合に SAM が実行するアクションを指定する現在の設定。ユーザがプロンプトに対して応答しない場合、SAM は指定されたインターバルが終了するまで待機し、（**proceed** キーワードまたは **terminate** キーワードのいずれかを使用して）**sam prompt-interval** コマンドで指定されたアクションを実行します。 **proceed** キーワードを使用して **sam promptinterval** コマンドを入力すると、**show sam sysinfo** コマンドに「Yes」と表示させます。つまり、SAMによって実行されるデフォルトのアクションは、プロンプトインターバルが終了するまで待機し、ユーザから「yes」を受信したように応答します。 **terminate** キーワードを使用して **sam promptinterval** コマンドを入力すると、**show sam sysinfo** コマンドに「No」と表示させます。つまり、SAM によって実行されるデフォルトのアクションは、プロンプトインターバルが終了するまで待機し、ユーザから「no」を受信したように応答します。

関連コマンド

コマンド	説明
sam prompt-interval, （273 ページ）	異常な状況を検出したときに、ユーザに入力を求めた後で SAM が待機するインターバルを設定し、指定されたインターバル内にユーザからの入力を受信しなかった場合の SAM の応答方法を決定します。

セキュア シェル コマンド

ここでは、セキュア シェル（SSH）を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

SSH の概念、設定作業、および例の詳細については 『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』 の 「*Implementing Secure Shell on* Cisco ASR 9000 Series Router Software」設定モジュールを参照してください。

clear ssh

着信または発信のセキュア シェル（SSH）接続を終了するには、EXEC モードで **clear ssh** コマンドを使用します。

clear ssh {*session-id*| **outgoing** *session-id*}

構文の説明

session-id	**show ssh** コマンドの出力で表示される着信接続のセッション ID 番号。範囲は 0 ～ 1024 です。
outgoing *session-id*	**show ssh** コマンドの出力で表示される発信接続のセッション ID 番号を指定します。 指定できる範囲は 1 ～ 10 です。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

着信または発信の SSH 接続を切断するには、**clear ssh** コマンドを使用します。 着信接続は、ローカル ネットワーキング デバイス上で実行している SSH サーバによって管理されます。 発信接続は、ローカル ネットワーキング デバイスから開始されます。

接続のセッション ID を表示するには、**show ssh** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次の例では、**show ssh** コマンドを使用して、ルータへのすべての着信接続と発信接続を表示します。 そのあと、**clear ssh** コマンドを使用して、ID 番号が 0 の着信セッションを終了します。

```
RP/0/RSP0/CPU0:router# show ssh

SSH version: Cisco-2.0
session     pty  location   state       userid     host         ver
-----------------------------------------------------------------------
Incoming sessions
0           vty0 0/33/1  SESSION_OPEN   cisco   172.19.72.182   v2
1           vty1 0/33/1  SESSION_OPEN   cisco   172.18.0.5      v2
2           vty2 0/33/1  SESSION_OPEN   cisco   172.20.10.3     v1
3           vty3 0/33/1  SESSION_OPEN   cisco   3333::50        v2

Outgoing sessions
1               0/33/1  SESSION_OPEN    cisco   172.19.72.182   v2
2               0/33/1  SESSION_OPEN    cisco   3333::50        v2

RP/0/RSP0/CPU0:router# clear ssh 0
```

関連コマンド

コマンド	説明
show ssh, （306 ページ）	ルータへの着信接続と発信接続を表示します。

sftp

セキュア FTP（SFTP）クライアントを起動するには、EXEC モードで **sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] *source-filename dest-filename* [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。ユーザ名のあとにアットマーク（@）が必要です。
hostname:remote-filename	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。 ホスト名のあとにコロン（:）が必要です。
source-filename	SFTP の発信元（パスを含む）
dest-filename	SFTP の宛先（パスを含む）
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。 詳細については、疑問符（**?**）オンラインヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンラインヘルプを参照してください。
vrf *vrf-name*	発信元インターフェイスに対応づける VRF の名前を指定します。

コマンド デフォルト

username 引数を省略した場合、ルータのログイン名が使用されます。 *hostname* 引数を省略した場合、ファイルはローカルにあると見なされます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SFTP では、ルータとリモート ホストの間でファイルの安全な（および認証された）コピーを行うことができます。 **copy** コマンドと同様に、**sftp** コマンドは EXEC モードでしか実行できません。

ユーザ名を省略すると、ルータのログイン名がデフォルトとして使用されます。 ホスト名を省略すると、ファイルはローカルにあると見なされます。

sftp コマンドで発信元インターフェイスを指定すると、**sftp** インターフェイスが、**ssh client source-interface** コマンドで指定されたインターフェイスよりも優先されます。

ファイルの宛先がローカルパスの場合、すべての発信元ファイルがリモートホスト上になければなりません。その逆の場合も同様です。

複数の発信元ファイルが存在する場合、宛先は、すでに存在するディレクトリでなければなりません。 それ以外の場合、宛先には、ディレクトリ名または宛先ファイル名のいずれかを指定できます。 ファイルの発信元をディレクトリ名にはできません。

ファイルを複数のリモート ホストからダウンロードする場合、つまり、発信元に複数のリモートホストを指定すると、SFTP クライアントによって SSH インスタンスがホストごとに生成されます。そのため、ユーザ認証を複数回要求されることがあります。

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の例では、ユーザ *abc* がファイル *ssh.diff* を SFTP サーバ *ena-view1* から *disk0* にダウンロードします。

```
RP/0/RSP0/CPU0:router# sftp abc@ena-view1:ssh.diff disk0
```

次の例では、ユーザ *abc* が、disk 0:/sam_* で示される複数のファイルをリモート SFTP サーバ ena-view1 上の /users/abc/ にアップロードします。

```
RP/0/RSP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *run* を *disk0a:* からローカル SFTP サーバ上の *disk0:/v6copy* にダウンロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]:disk0a:/run disk0:/V6copy
Connecting to 2:2:2::2...
Password:

disk0a:/run
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (338172)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0:/V6copy

Directory of disk0:

70144       -rwx  308413      Sun Oct 16 23:06:52 2011  V6copy

2102657024 bytes total (1537638400 bytes free)
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *v6copy* を *disk0:* からローカル SFTP サーバ上の *disk0a:/v6back* にアップロードします。

```
RP/0/RSP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:

/disk0:/V6copy
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (421329)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/v6back

Directory of disk0a:

66016       -rwx  308413      Sun Oct 16 23:07:28 2011  v6back

2102788096 bytes total (2098987008 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile* を *disk0:* からローカル SFTP サーバ上の *disk0a:/sampfile_v4* にダウンロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile disk0a:/sampfile_v4
Connecting to 2.2.2.2...
Password:

disk0:/sampfile
  Transferred 986 Bytes
  986 bytes copied in 0 sec (493000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/sampfile_v4

Directory of disk0a:

131520      -rwx  986         Tue Oct 18 05:37:00 2011  sampfile_v4

502710272 bytes total (502001664 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile_v4* を *disk0a:* からローカル SFTP サーバ上の *disk0:/sampfile_back* にアップロードします。

```
RP/0/RSP0/CPU0:router#sftp disk0a:/sampfile_v4 admin@2.2.2.2:disk0:/sampfile_back
Connecting to 2.2.2.2...
Password:

disk0a:/sampfile_v4
  Transferred 986 Bytes
  986 bytes copied in 0 sec (564000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0:/sampfile_back

Directory of disk0:

121765      -rwx  986         Tue Oct 18 05:39:00 2011  sampfile_back

524501272 bytes total (512507614 bytes free)
```

関連コマンド

コマンド	説明
ssh client source-interface, （315 ページ）	すべての発信SSH接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
ssh client vrf, （317 ページ）	SSH クライアントで使用される新しい VRF を設定します。

sftp（インタラクティブ モード）

ユーザがセキュア FTP（SFTP）クライアントを起動できるようにするには、EXEC モードで **sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。ユーザ名のあとにアットマーク（@）が必要です。
hostname:remote-filename	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。 ホスト名のあとにコロン（:）が必要です。
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイスタイプ。詳細については、疑問符（**?**）オンラインヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
vrf *vrf-name*	発信元インターフェイスに対応づける VRF の名前を指定します。

コマンド デフォルト

username 引数を省略した場合、ルータのログイン名が使用されます。 *hostname* 引数を省略した場合、ファイルはローカルにあると見なされます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.9.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SFTP クライアントは、インタラクティブ モードで、ユーザがサポートされているコマンドを入力できるセキュアな SSH チャネルを作成します。 ユーザがインタラクティブ モードで SFTP クライアントを起動すると、SFTP クライアント プロセスによってセキュアな SSH チャネルが作成され、ユーザがサポートされているコマンドを入力できるエディタが開きます。

複数の要求を SFTP サーバに送信してコマンドを実行することができます。 サーバに対する「未確認」または未処理の要求に数の制限はありませんが、サーバは便宜上これらの要求をバッファリングするか、またはキューに入れる場合があります。 このため、要求の順番に論理的な順序があることがあります。

インタラクティブ モードでサポートされる UNIX ベース コマンドは次のとおりです。

- bye
- **cd** *<path>*
- **chmod** *<mode> <path>*
- exit
- **get** *<remote-path> [local-path]*
- help
- **ls** *[-alt] [path]*
- **mkdir <path>**
- **put** *<local-path> [remote-path]*
- pwd
- quit
- **rename <old-path> <new-path>**
- **rmdir <path>**
- **rm <path>**

次のコマンドはサポートされません。

- lcd、lls、lpwd、lumask、lmkdir
- ln、symlink
- chgrp、chown
- !、！コマンド
- ?
- mget、mput

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の例では、ユーザ *admin* が IPv6 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]

Connecting to 2:2:2::2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/admin
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/admin/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

次の例では、ユーザ *abc* が IPv4 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RSP0/CPU0:router#sftp abc@2.2.2.2
Connecting to 2.2.2.2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/abc
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

関連コマンド

コマンド	説明
ssh client source-interface, （315 ページ）	すべての発信SSH接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
ssh client vrf, （317 ページ）	SSH クライアントで使用される新しい VRF を設定します。

show ssh

ルータへのすべての着信接続と発信接続を表示するには、EXEC モードで **show ssh** コマンドを使用します。

show ssh

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

セキュア シェル（SSH）Version 1（SSHv1; SSH バージョン 1）と SSH Version 2（SSHv2; SSH バージョン 2）のすべての着信接続と発信接続を表示するには、**show ssh** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、SSH がイネーブルのときに **show ssh** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show ssh

SSH version: Cisco-2.0

id pty      location      state        userid        host            ver
------------------------------------------------------------------------
Incoming sessions
```

```
0 vty0       0/RSP0/CPU0    SESSION_OPEN    cisco       172.19.72.182    v2
1 vty1       0/RSP0/CPU0    SESSION_OPEN    cisco       172.18.0.5       v2
2 vty2       0/RSP0/CPU0    SESSION_OPEN    cisco       172.20.10.3      v1
3 vty3       0/RSP0/CPU0    SESSION_OPEN    cisco       3333::50         v2

Outgoing sessions

1            0/RSP0/CPU0    SUSPENDED       root        172.19.72.182    v2
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *19*：*show ssh* フィールドの説明

フィールド	説明
id	着信および発信 SSH 接続のセッション ID。
pty	着信セッションに割り当てられた仮想端末ID。発信 SSH 接続の場合は Null になります。
location	着信接続の場合、SSH サーバが稼働している場所を示します。 発信接続の場合、location は、SSH セッションがどのルート プロセッサから開始されるかを示します。
state	接続の現在の SSH 状態。
userid	ルータへ、またはルータからの接続に使用される認証、許可、アカウンティング（AAA）ユーザ名
host	リモート ピアの IP アドレス
ver	接続タイプが SSHv1 と SSHv2 のいずれであるかを示します。

関連コマンド

コマンド	説明
show sessions	開いている Telnet 接続または rlogin 接続に関する情報を表示します。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。
show ssh session details, （308 ページ）	ルータへのすべての着信と発信の SSHv2 接続について、詳細を表示します。

show ssh session details

すべての着信と発信のセキュア シェル バージョン2（SSHv2）接続について詳細を表示するには、EXEC モードで **show ssh session details** コマンドを使用します。

show ssh session details

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータへの SSHv2 接続の詳細レポートを表示するには、**show ssh session details** コマンドを使用します。このレポートには、特定のセッションに選択された暗号化に関する情報が含まれます。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、着信と発信のすべての SSHv2 接続の詳細を表示するために、**show ssh session details** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show ssh session details

SSH version: Cisco-2.0
session     key-exchange   pubkey   incipher   outcipher    inmac     outmac
--------------------------------------------------------------------------------
```

```
Incoming Session

0           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5

Outgoing connection

1           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *20*：*show ssh session details* フィールドの説明

フィールド	説明
session	着信および発信 SSH 接続のセッション ID。
key-exchange	相互に認証するために両方のピアによって選択されたキー交換アルゴリズム。
pubkey	キー交換用に選択された公開キー アルゴリズム。
incipher	Rx トラフィック用に選択された暗号化。
outcipher	Tx トラフィック用に選択された暗号化。
inmac	Rx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。
outmac	Tx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。

関連コマンド

コマンド	説明
show sessions	開いている Telnet 接続または rlogin 接続に関する情報を表示します。
show ssh, （306 ページ）	ルータへのすべての着信接続と発信接続を表示します。

ssh

セキュア シェル（SSH）クライアント接続を開始し、SSH サーバへの発信接続をイネーブルにするには、EXEC モードで **ssh** コマンドを使用します。

ssh [**vrf vrf-name**] {**ipv4-address| ipv6-address| hostname**} [**username** *user-id*] [**cipher des** {**128-cbc| 192-cbc| 256-cbc**}][**source-interface** *type interface-path-id*][**command***command-name*]

構文の説明

ipv4-address	A:B:C:D 形式の IPv4 アドレス。
ipv6-address	X:X::X 形式の IPv6 アドレス。
hostname	リモート ノードのホスト名。 このホスト名に IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、IPv6 アドレスが使用されます。
username *user-id*	（任意）SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用するユーザ名を指定します。 ユーザ ID を省略すると、デフォルトとして現在のユーザ ID が使用されます。
cipher des	（任意）暗号スイート。 Version 1（v1; バージョン 1）接続に対してだけ有効です。 暗号スイートを **cipher des** オプションで指定しなければ、トリプル データ暗号規格（トリプル DES）がデフォルトの暗号スイートとして使用されます。 SSHv2 は、3DES だけをサポートします（プロトコルは、128 ビット以上の暗号だけをサポートします）。 SSHv1 は、DES（56 ビット）と 3DES（168 ビット）の両方の暗号スイートをサポートします。
source interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
command	（任意）リモート コマンドを指定します。 このキーワードを追加すると、SSHv2 サーバにインタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行するよう要求します。

command name	リモート コマンド キーワードの名前。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 3.9.1	**command** キーワードのサポートが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

発信クライアント接続を行うには、**ssh** コマンドを使用します。 SSH クライアントにより、リモート ピアへの SSHv2 接続が試みられます。 リモート ピアで SSHv1 サーバしかサポートされていない場合、リモート サーバへの SSHv1 接続が内部生成されます。 リモート ピアのバージョンの検出と適切なクライアント接続の生成のプロセスは、ユーザからは見えません。

ssh コマンドで **source-interface** キーワード を指定すると、**ssh** インターフェイスが **ssh client source-interface** コマンド（ssh client source-interface, （315 ページ））で指定されたインターフェイスよりも優先されます。

SSHv2 サーバがインタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行できるようにするには、**command** キーワードを使用します。

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の出力例は、発信 SSH クライアント接続をイネーブルにするために、**ssh** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# sshremote-host username userabc

Password:
Remote-host>
```

関連コマンド

コマンド	説明
show ssh, （306 ページ）	ルータへのすべての着信接続と発信接続を表示します。

ssh client knownhost

サーバ公開キー（pubkey）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 **ssh client knownhost** コマンドを使用します。 サーバ pubkey の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。

ssh client knownhost device:/**filename**

no ssh client knownhost device:/**filename**

構文の説明

device:/ *filename*	ファイル名の完全なパス（たとえば、slot0:/server_pubkey）。 コロン（:）とスラッシュ（/）が必要です。

コマンド デフォルト

なし

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバ *pubkey* は、クライアント側で全員が知る公開キーとキーのオーナーしか知らない秘密キーの 2 つのキーを使用する暗号化システムです。 証明書がない場合、サーバ pubkey は、アウトオブバンド セキュア チャネルを介してクライアントに転送されます。 クライアントでは、この pubkey がローカル データベースに保存され、セッション構築ハンドシェイクのキー ネゴシエーションの初期段階にサーバから提供されたキーと比較されます。 キーが一致しない、またはクライアントのローカル データベースにキーが見つからない場合、セッションを許可するか拒否するかを確認するプロンプトが表示されます。

サーバ pubkey が、アウトオブバンド セキュア チャネルを介して最初に取得されたときに、ローカル データベースに保存されることが動作の前提条件になっています。 このプロセスは、UNIX 環境でセキュア シェル（SSH）の実装に採用されている現行のモデルと同じです。

タスク ID

タスク ID	操作
crypto	read, write

例

次の出力例は、**ssh client knownhost** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RSP0/CPU0:host1# exit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

すべての発信セキュア シェル（SSH）接続に選択されたインターフェイスの発信元IPアドレスを指定するには、グローバル コンフィギュレーション モードで **ssh client source-interface** コマンドを使用します。指定したインターフェイスIPアドレ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。

ssh client source-interface *type interface-path-id*

no ssh client source-interface *type interface-path-id*

構文の説明

type	インターフェイス タイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。

コマンド デフォルト

発信元インターフェイスは使用されません。

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

指定したインターフェイスの IP アドレスをすべての発信 SSH 接続に対して設定するには、**ssh client source-interface** コマンドを使用します。 このコマンドを設定しなければ、ソケットが接続されるときの TCP の発信元 IP アドレスは、使用される発信インターフェイスに基づいて選択されます。つまり、サーバに到達するために必要なルートに基づきます。 このコマンドは、SSH

セッションだけでなく、セキュア シェル ファイル転送プロトコル（SFTP）セッション上でも発信シェルに適用されます。これらのセッションでは、転送に ssh クライアントが使用されます。

source-interface の設定は、同じアドレス ファミリ内のリモート ホストへの接続にしか影響しません。 システム データベース（Sysdb）により、コマンドで指定されたインターフェイスに、対応する（同じファミリ内の）IP アドレスが設定されているかどうか検証されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、すべての発信 SSH 接続に対して管理イーサネット インターフェイスの IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client source-interface MgmtEth 0/RSP0/CPU0/0
```

ssh client vrf

SSH クライアントで使用される新しい VRF 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 **ssh client vrf** コマンドを使用します。 指定した VRF を削除するには、このコマンドの **no** 形式を使用します。

ssh client vrf *vrf-name*

no ssh client vrf *vrf-name*

構文の説明

vrf-name	SSH クライアントが使用する VRF の名前を指定します。

コマンド デフォルト

なし

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
リリース 3.8.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSH クライアントには VRF を 1 つだけ設定できます。

特定の VRF が SSH クライアント用に設定されていない場合、ssh client knownhost, （313 ページ）、ssh client source-interface, （315 ページ） などの他の SSH クライアント関連のコマンドを適用する際にデフォルトの VRF が使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、指定された VRF から起動するように設定されている SSH クライアントの例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client vrf green
```

関連コマンド

コマンド	説明
ssh client dscp <0 ～ 63 の値>	SSH クライアントは発信パケットの DSCP 値の設定をサポートします。 設定されていない場合、（クライアントとサーバ両方の）パケット内に設定されるデフォルト DSCP 値は 16 です。

ssh server

セキュア シェル（SSH）サーバを起動し、そのサーバで使用するために 1 つ以上の VRF 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 **ssh server** コマンドを使用します。 SSH サーバが指定された VRF の接続をこれ以上受信しないようにするには、このコマンドの **no** 形式を使用します。

ssh server [**vrf vrf-name| v2**]

no ssh server [**vrf vrf-name| v2**]

構文の説明

vrf *vrf-name*	SSH サーバが使用する VRF の名前を指定します。 VRF の最大長は 32 文字です。 （注） VRF が指定されていない場合、デフォルトの VRF が使用されます。
v2	SSH サーバ バージョンを強制的に 2 だけにします。

コマンド デフォルト

デフォルトの SSH サーバ バージョンは 2（SSHv2）です。着信 SSH クライアント接続が SSHv1 に設定されると、1（SSHv1）になります。

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
リリース 3.7.2	このコマンドが追加されました。
リリース 3.8.0	**vrf** キーワー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

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSH サーバは少なくとも 1 つの VRF に対して設定する必要があります。 デフォルトを含め、設定済みのすべての VRF を削除すると、SSH サーバのプロセスは停止します。 **ssh client knownhost**、**ssh client source-interface** などの他のコマンドを適用する際に SSH クライアントに特定の VRF を設定していない場合、デフォルトの VRF が使用されます。

SSH サーバは、ポート 22 で着信クライアント接続を待ち受けます。このサーバでは、IPv4 と IPv6 の両方のアドレス ファミリに対してセキュア シェル バージョン 1（SSHv1）と SSHv2 の両方の着信クライアント接続が処理されます。セキュア シェル バージョン 2 の接続だけを許可するには、ssh server v2, （327 ページ） コマンドを使用します。

SSH サーバが起動し、稼働中であることを確認するには、**show process sshd** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、SSH サーバが起動され、VRF「green」の接続を受信します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server
```

関連コマンド

コマンド	説明
show processes	SSH サーバに関する情報を表示します。詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。
ssh server v2, （327 ページ）	SSH サーバ バージョンを強制的に 2（SSHv2）だけにします。
ssh server dscp <0 ～ 63 の値>	SSH サーバは発信パケットの DSCP 値の設定をサポートします。設定されていない場合、（クライアントとサーバ両方の）パケット内に設定されるデフォルト DSCP 値は 16 です。

ssh server logging

SSH サーバのロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **ssh server logging** コマンドを使用します。 SSH サーバのロギングを停止するには、このコマンドの **no** 形式を使用します。

ssh server logging

no ssh server logging

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

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
リリース 3.8.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSHv2 クライアント接続だけが許可されます。

ロギングを設定すると、次のメッセージが表示されます。

- Warning: The requested term-type is not supported
- SSH v2 connection from %s succeeded (*user:%s, cipher:%s, mac:%s, pty:%s*)

警告メッセージは、サポートされていない端末タイプを使用して接続しようとした場合に表示されます。 Cisco IOS XR ソフトウェアを実行しているルータがサポートするのは vt100 端末タイプだけです。

2 番めのメッセージでログインに成功したことを確認します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、SSH サーバのロギングの開始例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server logging
```

関連コマンド

コマンド	説明
ssh server, （319 ページ）	SSH サーバを開始します。

ssh server rate-limit

1 分間あたりに許可される着信セキュア シェル（SSH）接続要求の数を制限するには、グローバル コンフィギュレーション モードで **ssh server rate-limit** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server rate-limit *rate-limit*

no ssh server rate-limit

構文の説明

rate-limit	1 分間あたりに許可される着信 SSH 接続要求の数。 範囲は 1 ～ 120 です。

コマンド デフォルト

rate-limit：1 分間あたり 60 個の接続要求

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
リリース 3.7.2	このコマンドが追加されました。

コマンド履歴

リリース	変更内容
リリース 2.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

着信 SSH 接続要求を設定レートに制限するには、**ssh server rate-limit** コマンドを使用します。 このレート制限を超える接続要求は、SSH サーバから拒否されます。 レート制限の変更は、確立している SSH セッションには影響しません。

たとえば、*rate-limit* 引数を 30 に設定すると、1 分間で 30 個の要求が許可されます。より正確には、接続の行われる間隔が 2 秒に制限されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、着信 SSH 接続要求の制限を 1 分あたり 20 に設定する方法です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

許可される同時着信セキュア シェル（SSH）セッションの数を設定するには、グローバル コンフィギュレーション モードで **ssh server session-limit** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server session-limit *sessions*

no ssh server session-limit

構文の説明

sessions	ルータで許可される着信 SSH セッションの数。 有効な範囲は 1 ～ 1024 です。

コマンド デフォルト

sessions：ルータあたり 64

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

許可される同時着信 SSH 接続の制限を設定するには、**ssh server session-limit** コマンドを使用します。 発信接続はこの制限に含まれません。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、着信 SSH 接続の制限を 50 に設定する方法です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server session-limit 50
```

ssh server v2

SSHサーババージョンを強制的に2（SSHv2）だけにするには、グローバル コンフィギュレーション モードで **ssh server v2** コマンドを使用します。 SSHv2 の SSH サーバを停止するには、このコマンドの **no** 形式を使用します。

ssh server v2

no ssh server v2

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSHv2 クライアント接続だけが許可されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、SSH サーバ バージョンを SSHv2 に限定して開始する方法です。

```
 RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# ssh server v2
```

関連コマンド

ssh timeout

認証、許可、アカウンティング（AAA）ユーザ認証のタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。 タイムアウト値をデフォルト時間に設定するには、このコマンドの **no** 形式を使用します。

ssh timeout *seconds*

no ssh timeout *seconds*

構文の説明

seconds	ユーザ認証の時間（秒単位）。 範囲は 5 ～ 120 です。

コマンド デフォルト

seconds：30

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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

AAA に対するユーザ認証のタイムアウト値を設定するには、**ssh timeout** コマンドを使用します。 設定された時間内にユーザ自身の認証が AAA に対してできないと、接続は中断されます。 値を設定しなければ、30 秒のデフォルト値が使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、AAA ユーザ認証のタイムアウト値が 60 秒に設定されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh timeout 60
```

Secure Socket Layer プロトコル コマンド

ここでは、Secure Socket Layer（SSL）プロトコルを設定するために使用されるコマンドについて説明します。

SSL の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Secure Socket Layer on* Cisco ASR 9000 Series Router」を参照してください。

show ssl

アクティブな Secure Socket Layer（SSL）セッションを表示するには、EXEC モードで **show ssl** コマンドを使用します。

show ssl [*process-id*]

構文の説明

process-id	（任意）SSL アプリケーションの Process ID（PID; プロセス ID）。 範囲は 1 ～ 1000000000 です。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

特定のプロセスを表示するには、プロセス ID 番号を入力します。 特定のプロセス ID 番号を取得するには、コマンドラインまたはシェルから **run pidin** を入力します。

引数を省略すると、SSL を実行しているすべてのプロセスが表示されます。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、**show ssl** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show ssl

PID         Method      Type        Peer                Port    Cipher-Suite
==========================================================================

1261711     sslv3       Server      172.16.0.5          1296    DES-CBC3-SHA
```

次の表に、この出力で表示されるフィールドの説明を示します。

表 *21*：*show ssl* のフィールドの説明

フィールド	説明
PID	SSL アプリケーションのプロセス ID。
Method	プロトコル バージョン（sslv2、sslv3、sslv23、または tlsv1）。
Type	SSL クライアントまたはサーバ。
Peer	SSL ピアの IP アドレス。
Port	SSL トラフィックが送信されるポート番号。
Cipher-Suite	SSL トラフィックに選択される正確な暗号スイート。 最初の部分は暗号化を示し、2 番目の部分はハッシュまたは整合性の方法を示します。 表示例では、暗号化は Triple DES、整合性（メッセージ ダイジェスト アルゴリズム）は SHA になります。

関連コマンド

コマンド	説明
run pidin	実行中のすべてのプロセスのプロセス ID を表示します。

トラフィック ストーム制御コマンド

ここでは、Virtual Private LAN Service（VPLS）ブリッジ ドメイン下でトラフィック ストーム制御を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

トラフィック ストーム制御の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Traffic Storm Control*」モジュールを参照してください。

storm-control

VPLSブリッジ下のアクセス回路またはアクセス疑似回線（PW）上でトラフィック ストーム制御をイネーブルにするには、l2vpn ブリッジ グループ ブリッジドメイン アクセス回路コンフィギュレーション モードまたは l2vpn ブリッジ グループ ブリッジドメイン疑似回線コンフィギュレーション モードで **storm-control** コマンドを使用します。 トラフィック ストーム制御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。

storm-control {**broadcast| multicast| unknown-unicast**} **pps** *value*

no storm-control {**broadcast| multicast| unknown-unicast**} **pps**

構文の説明

broadcast	ブロードキャスト トラフィックのトラフィック ストーム制御を設定します。
multicast	マルチキャスト トラフィックのトラフィック ストーム制御を設定します。
unknown-unicast	不明のユニキャスト トラフィックのトラフィック ストーム制御を設定します。 • トラフィック ストーム制御は、ブリッジ プロトコル データ ユニット（BPDU）パケットには適用されません。 すべての BPDU パケットは、トラフィック ストーム制御が設定されていないものとして処理されます。 • トラフィック ストーム制御は、内部の通信パケットと制御パケット、ルート アップデート、SNMP 管理トラフィック、Telnet セッション、またはルータ宛てのその他のパケットには適用されません。
pp s *value*	指定したトラフィック タイプに 1 秒あたりのパケット数のストーム制御しきい値を設定します。 有効値の範囲は 1 ～ 160000 です。

コマンド デフォルト

トラフィック ストーム制御は、デフォルトではディセーブルに設定されています。

コマンド モード

l2vpn ブリッジ グループ ブリッジドメイン アクセス回路コンフィギュレーション

l2vpn ブリッジ グループ ブリッジドメイン疑似回線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
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

トラフィック ストーム制御では、過剰なトラフィックによるブリッジの遮断が防止されることにより、VPLS ブリッジ下においてレイヤ 2 ポート セキュリティが提供されます。 トラフィック ストーム制御は、VPLS ブリッジ下の AC と PW 上でイネーブルにすることができます。 トラフィック ストーム制御では、ポート上の着信トラフィック レベルが監視され、1 秒のインターバルのうちにパケット数が設定したしきい値レベルに到達すると、トラフィックがドロップされます。

AC と PW のポートごとに、ブロードキャスト、マルチキャスト、および不明のユニキャストの 3 種類のトラフィックに対するトラフィック ストーム制御をイネーブルにできます。

しきい値は、1 秒あたりのパケット数のレートで設定されます。 指定されたトラフィック タイプのパケット数が、設定されたしきい値レベルに到達すると、そのポートにそれ以降に着信するそのトラフィック タイプのパケットは、1 秒のインターバルの残り時間がなくなるまでドロップされます。 新しい 1 秒のインターバルが開始されると、その指定されたタイプのトラフィックはポートを通過できるようになります。

この 1 秒のインターバルは、ハードウェアに設定されるため、変更できません。 各 1 秒のインターバルで許可されるパケットの最大数を設定するには、**pps** キーワードを使用します。

ドロップ カウンタには、しきい値に到達したことによりドロップされたパケットの累積数が維持されます。

ブリッジ下のすべての設定されたトラフィック ストーム制御しきい値とストーム制御ドロップ カウンタの現在値を表示するには、**show l2vpn bridge-domain** コマンドを使用します。

タスク ID

タスク ID	操作
l2vpn	read, write

例

次の例では、疑似回線上の 2 つのトラフィック ストーム制御しきい値をイネーブルにします。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group csco
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# neighbor 1.1.1.1 pw-id 100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# storm-control broadcast pps 4500
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# storm-control multicast pps 500
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# commit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-pw)# end
```

関連コマンド

コマンド	説明
show l2vpn bridge-domain	bridge-domain に関する情報と統計情報を表示します。

索 引

L

M

O

P

Q

R

S

T

U

V