



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 4.2.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/>

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.



目次

はじめに ix

マニュアルの変更履歴 ix

マニュアルの入手方法およびテクニカル サポート ix

認証、許可、アカウントिंग コマンド 1

aaa accounting 4

aaa accounting system default 7

aaa accounting update 9

aaa authentication 11

aaa authorization 14

aaa default-taskgroup 18

aaa group server radius 20

aaa group server tacacs+ 23

accounting (回線) 25

authorization 27

deadtime (サーバグループ コンフィギュレーション) 29

description (AAA) 31

group (AAA) 33

inherit taskgroup 35

inherit usergroup 37

key (RADIUS) 39

key (TACACS+) 41

login authentication 43

password (AAA) 45

radius-server dead-criteria time 48

radius-server dead-criteria tries 50

radius-server deadtime 52

radius-server host 54

radius-server key	58
radius-server retransmit	60
radius-server timeout	62
radius source-interface	64
retransmit (RADIUS)	66
secret	68
server (RADIUS)	71
server (TACACS+)	74
server-private (RADIUS)	76
server-private (TACACS+)	80
show aaa	83
show radius	89
show radius accounting	91
show radius authentication	93
show radius client	95
show radius dead-criteria	97
show radius server-groups	99
show tacacs	102
show tacacs server-groups	104
show user	106
single-connection	110
tacacs-server host	112
tacacs-server key	115
tacacs-server timeout	117
tacacs source-interface	119
task	121
taskgroup	123
timeout (RADIUS)	125
timeout (TACACS+)	127
timeout login response	129
usergroup	131
username	133
users group	137
vrf (RADIUS)	139
vrf (TACACS+)	141

インターネット キー交換セキュリティ プロトコル コマンド 143

- accounting (IKE) 145
- address 147
- authentication (IKE ポリシー) 149
- clear crypto isakmp 152
- clear crypto isakmp call admission statistics 154
- clear crypto isakmp errors 156
- clear crypto session 158
- crypto isakmp 160
- crypto isakmp call admission limit 161
- crypto isakmp identity 163
- crypto isakmp keepalive 166
- crypto isakmp peer 168
- crypto isakmp policy 170
- crypto isakmp policy-set 173
- crypto isakmp profile 175
- crypto keyring 177
- crypto logging 179
- description (IKE ポリシー) 180
- description (ISAKMP ポリシーセット) 182
- description (ISAKMP ピア) 184
- description (キーリング) 186
- encryption (IKE ポリシー) 188
- group (IKE ポリシー) 190
- hash (IKE ポリシー) 192
- keepalive (ISAKMP プロファイル) 194
- keyring 196
- key-string (IKE) 198
- lifetime (IKE ポリシー) 200
- local-address (キーリング) 202
- match identity (ISAKMP ポリシーセット) 204
- match identity (ISAKMP プロファイル) 206
- policy (ISAKMP ポリシーセット) 209
- pre-shared-key 211

rsa-pubkey	213
self-identity	215
set interface tunnel-ipsec	217
set ipsec-profile	219
show crypto isakmp call admission statistics	221
show crypto isakmp errors	224
show crypto isakmp key	232
show crypto isakmp peers	234
show crypto isakmp policy	236
show crypto isakmp profile	239
show crypto isakmp sa	241
show crypto isakmp stats	244
show crypto key pubkey-chain rsa	248
show crypto session	251
キーチェーン管理コマンド	255
accept-lifetime	256
accept-tolerance	258
cryptographic-algorithm	260
key (キーチェーン)	262
key chain (キーチェーン)	264
key-string (キーチェーン)	266
send-lifetime	268
show key chain	270
合法的傍受コマンド	273
lawful-intercept disable	274
管理プレーン保護コマンド	275
address ipv4 (MPP)	276
address ipv6 (MPP)	279
allow	281
control-plane	284
inband	286
interface (MPP)	288
management-plane	291
out-of-band	293
show mgmt-plane	295

vrf (MPP)	298
公開キー インフラストラクチャ コマンド	301
clear crypto ca certificates	303
clear crypto ca crl	305
crl optional (トラストポイント)	307
crypto ca authenticate	309
crypto ca cancel-enroll	311
crypto ca enroll	313
crypto ca import	315
crypto ca trustpoint	317
crypto key generate dsa	320
crypto key generate rsa	322
crypto key import authentication rsa	324
crypto key zeroize dsa	326
crypto key zeroize rsa	328
description (トラストポイント)	330
enrollment retry count	332
enrollment retry period	334
enrollment terminal	336
enrollment url	338
ip-address (トラストポイント)	340
query url	342
rsakeypair	344
serial-number (トラストポイント)	346
sftp-password (トラストポイント)	348
sftp-username (トラストポイント)	350
subject-name (トラストポイント)	352
show crypto ca certificates	354
show crypto ca crls	356
show crypto key mypubkey dsa	358
show crypto key mypubkey rsa	360
Software Authentication Manager コマンド	363
sam add certificate	364
sam delete certificate	367

sam prompt-interval	369
sam verify	371
show sam certificate	374
show sam crl	379
show sam log	382
show sam package	384
show sam sysinfo	388
セキュア シェル コマンド	391
clear ssh	392
sftp	394
sftp (インタラクティブ モード)	398
show ssh	402
show ssh session details	404
ssh	406
ssh client knownhost	409
ssh client source-interface	411
ssh client vrf	413
ssh server	415
ssh server logging	417
ssh server rate-limit	419
ssh server session-limit	421
ssh server v2	423
ssh timeout	424
Secure Socket Layer プロトコル コマンド	427
show ssl	428
トラフィック ストーム制御コマンド	431
storm-control	432



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, ix ページ
- マニュアルの入手方法およびテクニカル サポート, ix ページ

マニュアルの変更履歴

初版後このマニュアルに加えられた技術的な変更の履歴をこの表に示します。

表 1: マニュアルの変更履歴

リビジョン	日付	変更点
OL-26051-02-J	2012 年 6 月	Cisco IOS XR リリース 4.2.1 用に再発行されました。
OL-26051-01	2011 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、アカウントिंग コマンド

ここでは、認証、許可、アカウントिंग（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, 4 ページ](#)
- [aaa accounting system default, 7 ページ](#)
- [aaa accounting update, 9 ページ](#)
- [aaa authentication, 11 ページ](#)
- [aaa authorization, 14 ページ](#)
- [aaa default-taskgroup, 18 ページ](#)
- [aaa group server radius, 20 ページ](#)
- [aaa group server tacacs+, 23 ページ](#)
- [accounting \(回線\), 25 ページ](#)
- [authorization, 27 ページ](#)
- [deadtime \(サブグループ コンフィギュレーション\), 29 ページ](#)
- [description \(AAA\), 31 ページ](#)
- [group \(AAA\), 33 ページ](#)
- [inherit taskgroup, 35 ページ](#)
- [inherit usergroup, 37 ページ](#)
- [key \(RADIUS\), 39 ページ](#)
- [key \(TACACS+\), 41 ページ](#)
- [login authentication, 43 ページ](#)

- password (AAA) , 45 ページ
- radius-server dead-criteria time, 48 ページ
- radius-server dead-criteria tries, 50 ページ
- radius-server deadtime, 52 ページ
- radius-server host, 54 ページ
- radius-server key, 58 ページ
- radius-server retransmit, 60 ページ
- radius-server timeout, 62 ページ
- radius source-interface, 64 ページ
- retransmit (RADIUS) , 66 ページ
- secret, 68 ページ
- server (RADIUS) , 71 ページ
- server (TACACS+) , 74 ページ
- server-private (RADIUS) , 76 ページ
- server-private (TACACS+) , 80 ページ
- show aaa, 83 ページ
- show radius, 89 ページ
- show radius accounting, 91 ページ
- show radius authentication, 93 ページ
- show radius client, 95 ページ
- show radius dead-criteria, 97 ページ
- show radius server-groups, 99 ページ
- show tacacs, 102 ページ
- show tacacs server-groups, 104 ページ
- show user, 106 ページ
- single-connection, 110 ページ
- tacacs-server host, 112 ページ
- tacacs-server key, 115 ページ
- tacacs-server timeout, 117 ページ
- tacacs source-interface, 119 ページ
- task, 121 ページ

- [taskgroup, 123 ページ](#)
- [timeout \(RADIUS\) , 125 ページ](#)
- [timeout \(TACACS+\) , 127 ページ](#)
- [timeout login response, 129 ページ](#)
- [usergroup, 131 ページ](#)
- [username, 133 ページ](#)
- [users group, 137 ページ](#)
- [vrf \(RADIUS\) , 139 ページ](#)
- [vrf \(TACACS+\) , 141 ページ](#)

aaa accounting

アカウント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トングをイネーブルにします。
exec	EXEC セッションのアカウント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ト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トング方式のリストをアカウント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。
<i>list-name</i>	アカウント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」通知がアカウントング 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	アカウントングを使用しません。
<i>method</i>	AAA システムアカウント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。 <ul style="list-style-type: none"> • group tacacs+ : すべての TACACS+ サーバのリストをアカウントングに使用します。 • group radius : すべての RADIUS サーバのリストをアカウントングに使用します。 • 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トングに使用します。

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	変更箇所
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、特定のアカウント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ト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、アカウントングに 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 サーバにアカウントング 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。

アカウントング方式リストには、アカウント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トング 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。

最小限のアカウントングを行うには、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トングを行うには、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。アカウントング 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`」通知がアカウントング 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` アカウント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トング 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, (14 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、アカウントング (AAA) システムアカウント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。システムアカウント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」通知を送信しません。
none	アカウントングを使用しません。
method	AAA システムアカウント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。 <ul style="list-style-type: none"> • group tacacs+ : すべての TACACS+ サーバのリストをアカウントングに使用します。 • group radius : すべての RADIUS サーバのリストをアカウントングに使用します。 • 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トングに使用します。

コマンド デフォルト

AAA アカウント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	変更箇所
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。

システムアカウントングには、名前付きアカウント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、アカウント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, (11 ページ)	認証の方式リストを作成します。
aaa authorization, (14 ページ)	許可の方式リストを作成します。

aaa accounting update

定期的な中間アカウントングレコードがアカウント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。中間アカウント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トング情報があるときは常に、中間アカウントングレコードをアカウントングサーバに送信します。
periodic minutes	(任意) <i>minutes</i> 引数によって定義されているとおりに、中間アカウントングレコードを定期的にアカウント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 のアカウント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	変更箇所
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トング情報があるたびに中間アカウントングレコードがアカウント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。中間アカウントングレコードには、リモートピアに使用されるネゴシエーション済み IP アドレスが含まれます。

periodic キーワードを使用すると、中間アカウントングレコードは *minutes* 引数で定義されているとおりに定期的送信されます。中間アカウントングレコードには、アカウント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ト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トング情報があるたびに中間アカウントングレコードがアカウント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トングレコードが定期的にアカウント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ト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ト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トングレコードを 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トング情報があるときに、中間アカウントングレコードを 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)	アカウントングの方式リストを作成します。
aaa authorization , (14 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。
<i>list-name</i>	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せん。
<i>method-list</i>	AAA システム アカウントिंग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。 <ul style="list-style-type: none"> • 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 モデル

グローバルでは、**aaa authentication** の位置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	変更箇所
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)	アカウントングの方式リストを作成します。
aaa authorization, (14 ページ)	許可の方式リストを作成します。
aaa group server radius, (20 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+, (23 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, (43 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, (112 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。
<i>list-name</i>	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 モデル

このコマンドのオプションは、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	変更箇所
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)	アカウント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

<i>taskgroup-name</i>	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	変更箇所
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

<i>group-name</i>	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	変更箇所
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、アカウントング (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ト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ト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) , (39 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 , (64 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) , (66 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) , (71 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) , (76 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) , (125 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) , (139 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。



(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)	アカウントングの方式リストを作成します。
aaa authentication , (11 ページ)	認証の方式リストを作成します。
aaa authorization , (14 ページ)	許可の方式リストを作成します。
server (TACACS+) , (74 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 , (112 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、アカウントング (AAA) アカウント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 アカウント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トングをイネーブルにします。
exec	EXEC セッションのアカウント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。
<i>list-name</i>	使用するアカウント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

アカウント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	変更箇所
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トングに対して名前付きアカウント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、アカウント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トिंग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* でアカウントING方式リスト *listname2* を使用するコマンドアカウントING 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)	アカウントING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、アカウントング（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。
<i>list-name</i>	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	変更箇所
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 , (14 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

<i>minutes</i>	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	変更箇所
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+ , (23 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 , (48 ページ)	RADIUS サーバに <code>dead</code> 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 , (52 ページ)	RADIUS サーバに <code>dead</code> 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	変更箇所
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 , (123 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 , (131 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	変更箇所
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**, (133 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) , (45 ページ)	ユーザのログインパスワードを作成します。
usergroup , (131 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 , (133 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

<i>taskgroup-name</i>	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	変更箇所
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
```


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) , (31 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 , (123 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 , (131 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 <i>clear-text-key</i>	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 <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>clear-text-key</i>	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	変更箇所
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+ , (23 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 , (58 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) , (66 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) , (76 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) , (125 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 <i>clear-text-key</i>	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 <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>auth-key</i>	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	変更箇所
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する必要があります。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 , (112 ページ)	TACACS+ ホストを指定します。
tacacs-server key , (115 ページ)	ルータと TACACS+ デモン間のすべての 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、アカウントング（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。
<i>list-name</i>	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	変更箇所
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 , (11 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。
<i>password</i>	「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	変更箇所
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) , (33 ページ)	ユーザをグループに追加します。
usergroup , (131 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 , (133 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、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』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が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

<i>seconds</i>	秒単位の時間です。範囲は、1 ～ 120 秒です。 <i>seconds</i> 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	変更箇所
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, (50 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, (52 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, (97 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

<i>tries</i>	1 ~ 100 のタイムアウト回数。 <i>tries</i> 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、連続タイムアウト回数は 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せん。

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、連続タイムアウト回数は 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	変更箇所
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ト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, (48 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がある時間を秒単位で定義します。
radius-server deadtime, (52 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, (97 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 minutes

no radius-server deadtime minutes

構文の説明

<i>minutes</i>	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

コマンド履歴

リリース	変更箇所
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。

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
```

関連コマンド

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) , (29 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。
radius-server dead-criteria time , (48 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。
show radius dead-criteria , (97 ページ)	dead サーバの検出基準の情報を表示します。

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

<i>hostname</i>	RADIUS サーバホストのドメインネームシステム (DNS) 名です。
<i>ip-address</i>	RADIUS サーバホストの IP アドレスです。
auth-port <i>port-number</i>	(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 <i>port-number</i>	(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 <i>seconds</i>	(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 <i>retries</i>	(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せん。

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	変更箇所
	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。

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、アカウント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、アカウント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ト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ト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
```

アカウント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トングに使用するように設定し、RADIUS サーバ *host2* をアカウント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 , (4 ページ)	アカウントングの方式リストを作成します。
aaa authentication , (11 ページ)	認証の方式リストを作成します。
aaa authorization , (14 ページ)	許可の方式リストを作成します。
radius-server key , (58 ページ)	ルータおよび RADIUS デモン間のすべての 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 , (60 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
<code>radius-server timeout</code> , (62 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 <i>clear-text-key</i>	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 <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>clear-text-key</i>	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

コマンド履歴

リリース	変更箇所
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 次に、クリアテキストキーを「samplekey」に設定する例を示します：

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

次に、暗号化共有キーを「anykey」に設定する例を示します：

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

関連コマンド

コマンド	説明
key (RADIUS) , (39 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。
server-private (RADIUS) , (76 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。

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	変更箇所
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。

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 , (58 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) , (66 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) , (76 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。

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

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

変更箇所

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。

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

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

関連コマンド

コマンド	説明
radius-server key , (58 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。
server-private (RADIUS) , (76 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) , (125 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。

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-name* [*vrf vrf-id*]

no radius source-interface

構文の説明

<i>interface-name</i>	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。
<i>vrf vrf-id</i>	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	変更箇所
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。

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
```

関連コマンド

コマンド	説明
aaa group server tacacs+, (23 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, (58 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)

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	変更箇所
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+ , (23 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) , (76 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) , (125 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。
<i>secret-login</i>	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	変更箇所
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イク認証プロトコル) 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せん。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$q7C6fhzje7Cc7Xzmu2Fr1
  !
end
```

関連コマンド

コマンド	説明
group (AAA) , (33 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) , (45 ページ)	ユーザのログインパスワードを作成します。
usergroup , (131 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 , (133 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

<i>hostname</i>	サーバ ホスト名の指定に使用する文字列です。
<i>ip-address</i>	RADIUS サーバホストの IP アドレスです。
auth-port <i>port-number</i>	(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。 <i>port-number</i> 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 <i>port-number</i>	(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。 <i>port-number</i> 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	変更箇所
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（アカウントングなど）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ト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トングサービス用に設定されている 2 番目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ト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, (20 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) , (29 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) , (76 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

<i>hostname</i>	サーバホスト名の指定に使用する文字列です。
<i>ip-address</i>	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	変更箇所
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、アカウントिंग (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+, (23 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

<i>hostname</i>	サーバ ホスト名の指定に使用する文字列です。
<i>ip-address</i>	RADIUS サーバホストの IP アドレスです。
auth-port <i>port-number</i>	(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。 <i>port-number</i> 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 <i>port-number</i>	(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。 <i>port-number</i> 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 <i>seconds</i>	(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。 <i>seconds</i> 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 <i>retries</i>	(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。 <i>retries</i> 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
- アカウントングポート : 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	変更箇所
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+, (23 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, (58 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, (60 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, (62 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), (39 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), (66 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), (125 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), (139 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

<i>hostname</i>	サーバ ホスト名の指定に使用する文字列です。
<i>ip-address</i>	TACACS+ サーバホストの IP アドレスです。
port <i>port-number</i>	(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 <i>seconds</i>	(任意) 認証、許可、アカウントング (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 <i>string</i>	(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	変更箇所
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+, (23 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, (115 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, (117 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+) , (41 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+) , (127 ページ)	認証、許可、アカウントング (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+) , (141 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。
<i>ikegroup-name</i>	(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。
<i>usergroup-name</i>	(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。
<i>username</i>	(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	変更箇所
	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
```

show aaa

```

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, (106 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	変更箇所
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
```

show radius

```

    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/アカウントリング要求の 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) , (139 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, (60 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, (62 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	変更箇所
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
```

show radius accounting

```
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、アカウントリング要求の 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)	アカウントリングの方式リストを作成します。
aaa authentication , (11 ページ)	認証の方式リストを作成します。
show radius authentication , (93 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	変更箇所
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
```

show radius authentication

```
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、アカウントリング要求の 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)	アカウントリングの方式リストを作成します。
aaa authentication, (11 ページ)	認証の方式リストを作成します。
show radius accounting, (91 ページ)	RADIUS アカウントリ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	変更箇所
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トING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、アカウントING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) , (71 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 , (89 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ト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	変更箇所
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/アカウントング要求の 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, (48 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, (52 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

<i>group-name</i>	(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	変更箇所
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ト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「radgrp-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/アカウントング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
vrf (RADIUS) , (139 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

変更箇所

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

変更箇所

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 , (112 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表示されています。

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	変更箇所
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する必要があります。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
```

show user

```

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:          bcndl : 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 , (83 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

変更箇所

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、アカウントング要求でこの 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 , (112 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

<i>host-name</i>	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 <i>port-number</i>	(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 <i>seconds</i>	(任意) 認証、許可、アカウントング (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] <i>auth-key</i>	(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。 <i>auth-key</i> 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ず。

コマンド デフォルト

TACACS+ ホストは指定されません。

コマンド モード

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。
グローバルコンフィギュレーション
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。

コマンド履歴

リリース	変更箇所
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+) , (41 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, (110 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, (115 ページ)	ルータと TACACS+ デモン間のすべての 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, (117 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+) , (127 ページ)	認証、許可、アカウントング (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 <i>clear-text-key</i>	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 <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>auth-key</i>	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	変更箇所
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+) , (41 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, (112 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

変更箇所

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 , (112 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

<i>type</i>	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。
<i>path-id</i>	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 (?) オンライン ヘルプ機能を使用します。
<i>vrf vrf-id</i>	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	変更箇所
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+, (23 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。
<i>taskid-name</i>	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	変更箇所
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 , (123 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

<i>taskgroup-name</i>	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。
<i>string</i>	(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。
<i>taskid-name</i>	(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。
<i>taskgroup-name</i>	(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	変更箇所
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) , (31 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 , (121 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	変更箇所
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 , (62 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) , (66 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) , (76 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、アカウントング (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	変更箇所
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 , (112 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	変更箇所
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, (43 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

<i>usergroup-name</i>	ユーザグループの名前です。 <i>usergroup-name</i> 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	変更箇所
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**, (37 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) , (31 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 , (37 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 , (123 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

<i>user-name</i>	ユーザ名。 <i>user-name</i> 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。
<i>password</i>	(任意) 「 <i>lab</i> 」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。
<i>usergroup-name</i>	(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 モデル

グローバル コンフィギュレーション モードで定義されません。

管理コンフィギュレーション

コマンド履歴

リリース	変更箇所
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](#)、(11 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 ハンドシェイク 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.0PMQ8GQQKXCFO
!
```

関連コマンド

コマンド	説明
aaa authentication, (11 ページ)	認証の方式リストを定義します。
group (AAA) , (33 ページ)	ユーザをグループに追加します。
password (AAA) , (45 ページ)	ユーザのログインパスワードを作成します。
secret, (68 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**| **serviceadmin**| **sysadmin**}

構文の説明

<i>usergroup-name</i>	ユーザグループの名前です。 <i>usergroup-name</i> 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	変更箇所
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	変更箇所
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 , (64 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) , (76 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	変更箇所
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+ , (23 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+) , (74 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+) , (80 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。



インターネットキー交換セキュリティプロトコルコマンド

ここでは、インターネットキー交換 (IKE) セキュリティプロトコル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。

IKE 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 Internet Key Exchange Security Protocol on Cisco ASR 9000 Series Router*」を参照してください。

- [accounting \(IKE\)](#) , 145 ページ
- [address](#), 147 ページ
- [authentication \(IKE ポリシー\)](#) , 149 ページ
- [clear crypto isakmp](#), 152 ページ
- [clear crypto isakmp call admission statistics](#), 154 ページ
- [clear crypto isakmp errors](#), 156 ページ
- [clear crypto session](#), 158 ページ
- [crypto isakmp](#), 160 ページ
- [crypto isakmp call admission limit](#), 161 ページ
- [crypto isakmp identity](#), 163 ページ
- [crypto isakmp keepalive](#), 166 ページ
- [crypto isakmp peer](#), 168 ページ
- [crypto isakmp policy](#), 170 ページ
- [crypto isakmp policy-set](#), 173 ページ
- [crypto isakmp profile](#), 175 ページ
- [crypto keyring](#), 177 ページ

- [crypto logging](#), 179 ページ
- [description \(IKE ポリシー\)](#), 180 ページ
- [description \(ISAKMP ポリシーセット\)](#), 182 ページ
- [description \(ISAKMP ピア\)](#), 184 ページ
- [description \(キーリング\)](#), 186 ページ
- [encryption \(IKE ポリシー\)](#), 188 ページ
- [group \(IKE ポリシー\)](#), 190 ページ
- [hash \(IKE ポリシー\)](#), 192 ページ
- [keepalive \(ISAKMP プロファイル\)](#), 194 ページ
- [keyring](#), 196 ページ
- [key-string \(IKE\)](#), 198 ページ
- [lifetime \(IKE ポリシー\)](#), 200 ページ
- [local-address \(キーリング\)](#), 202 ページ
- [match identity \(ISAKMP ポリシーセット\)](#), 204 ページ
- [match identity \(ISAKMP プロファイル\)](#), 206 ページ
- [policy \(ISAKMP ポリシーセット\)](#), 209 ページ
- [pre-shared-key](#), 211 ページ
- [rsa-pubkey](#), 213 ページ
- [self-identity](#), 215 ページ
- [set interface tunnel-ipsec](#), 217 ページ
- [set ipsec-profile](#), 219 ページ
- [show crypto isakmp call admission statistics](#), 221 ページ
- [show crypto isakmp errors](#), 224 ページ
- [show crypto isakmp key](#), 232 ページ
- [show crypto isakmp peers](#), 234 ページ
- [show crypto isakmp policy](#), 236 ページ
- [show crypto isakmp profile](#), 239 ページ
- [show crypto isakmp sa](#), 241 ページ
- [show crypto isakmp stats](#), 244 ページ
- [show crypto key pubkey-chain rsa](#), 248 ページ
- [show crypto session](#), 251 ページ

accounting (IKE)

ISAKMP プロファイルを介して接続するすべてのピアについて認証、許可、アカウントिंग (AAA) サービスをイネーブルにするには、ISAKMP プロファイル 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。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。

accounting *list-name*

no accounting

構文の説明

<i>list-name</i>	クライアント アカウンティング リストの名前。最大長は 127 文字です。
------------------	---------------------------------------

コマンド デフォルト

デフォルト値は **no accounting** です。

コマンド モード

ISAKMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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, write

例

次に、アカウントリングリス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 isakmp profile vpnprofile  
RP/0/RSP0/CPU0:router(config-isa-prof)# accounting aaalist
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。

address

手動で設定するリモートピアの Rivest, Shamir, and Adelman (RSA) 公開キーの IP アドレスを指定するには、公開キー コンフィギュレーション モードで **address** コマンドを使用します。リモートピアの 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 *ip-address*

no address *ip-address*

構文の説明

<i>ip-address</i>	手動で設定するピアのリモート RSA 公開キーの IP アドレス
-------------------	----------------------------------

コマンドモード

なし
公開キー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

次に手動で設定する IP Security (IPSec) ピアの RSA 公開キーを指定するには、**address** コマンドを使用します。

RSA キーの指定が終了したら、公開キー コンフィギュレーション モード プロンプトで **quit** と入力してグローバル コンフィギュレーション モードに戻る必要があります。

タスク ID

タスク ID	操作
crypto	read, write

address

例

次に、IPSec ピアの RSA 公開キーを手動で指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey name host.vpn.com
RP/0/RSP0/CPU0:router(config-pubkey)# address 10.5.5.1
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
```

関連コマンド

コマンド	説明
key-string (IKE) , (198 ページ)	リモート ピアの RSA 公開キーを指定します。
rsa-pubkey , (213 ページ)	IKE 認証時の暗号化またはシグニチャに使用される Rivest, Shamir, and Adelman (RSA) 手動キーを定義します。
show crypto key pubkey-chain rsa , (248 ページ)	ルータに保存されているピアの RSA 公開キーを表示します。

authentication (IKE ポリシー)

インターネットキー交換 (IKE) ポリシー内の認証方式を指定するには、**ISAKMP** ポリシー コンフィギュレーション モードで **authentication** コマンドを使用します。認証方式をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

authentication {pre-share|rsa-sig|rsa-encr}

no authentication {pre-share|rsa-sig|rsa-encr}

構文の説明

pre-share	認証方式として事前共有キーを指定します。
rsa-sig	認証方式として RSA シグニチャを指定します。
rsa-encr	認証方式として Rivest, Shamir, and Adelman (RSA) 暗号化ナンスを指定します。

コマンド デフォルト

RSA シグニチャ

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

IKE ポリシーは、IKE ネゴシエーション時に使用される一連のパラメータを定義したものです。IKE ポリシーの認証方式を指定するには、**authentication** コマンドを使用します。事前共有キーを指定した場合は、これらの事前共有キーも個別に設定する必要があります。

RSA 暗号化ナンスを指定した場合は、各ピアが他のピアの RSA 公開キーを持っていることを確認する必要があります (**address**、**rsa-pubkey**、および **key-string** コマンドを参照)。

RSA シグニチャを指定した場合は、Certification Authority (CA; 認証局) から証明書を取得するためにピア ルータを設定する必要があります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、認証方式として事前共有キーを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication pre-share
```

次に、認証方式として RSA 暗号キーを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-encr
```

次に、認証方式として RSA シグニチャを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-sig
```

関連コマンド

コマンド	説明
address , (147 ページ)	手動で設定するリモート ピアのリモート RSA 公開キーの IP アドレスを指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュアルゴリズムを指定します。
key-string (IKE) , (198 ページ)	リモート ピアの RSA 公開キーを指定します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。

コマンド	説明
rsa-pubkey, (213 ページ)	IKE 認証時の暗号化またはシグニチャに使用される Rivest, Shamir, and Adelman (RSA) 手動キーを定義します。
show crypto isakmp policy, (236 ページ)	各 IKE ポリシーのパラメータを表示します。

clear crypto isakmp

アクティブなインターネットキー交換 (IKE) 接続をクリアするには、EXEC モードで **clear crypto isakmp** コマンドを使用します。

clear crypto isakmp [*connection-id*]

構文の説明

connection-id (任意) クリアする接続の名前。範囲は 1 ~ 64000 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	変更箇所
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)

connection-id 引数を使用しない場合は、このコマンドの発行時に既存のすべての IKE 接続がクリアされます。

タスク ID

タスク ID	操作
crypto	実行

例

次に、インターフェイス 172.21.114.123 および 172.21.114.67 で接続された 2 つのピア間の IKE 接続をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp sa
vrf          dst          src          state         conn-id      nodeid
-----
default      172.21.114.123  172.21.114.67 QM_IDLE      1            0
default      172.0.0.2        172.0.0.1    QM_IDLE      8            0

RP/0/RSP0/CPU0:router# configure
Enter configuration commands, one per line.  End with CNTL/Z.

RP/0/RSP0/CPU0:router# clear crypto isakmp 1
RP/0/RSP0/CPU0:router# show crypto isakmp sa

vrf          dst          src          state         conn-id      nodeid
-----
default      172.0.0.2        172.0.0.1    QM_IDLE      8            0
```

関連コマンド

コマンド	説明
show crypto isakmp sa , (241 ページ)	ピアにおける現在のすべての IKE SA を表示します。

clear crypto isakmp call admission statistics

ISAKMP コール アドミッション 統計情報をクリアするには、EXEC モードで **clear crypto isakmp call admission statistics** コマンドを使用します。

clear crypto isakmp call isakmp call admission statistics

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

変更箇所

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

実行

例

次に、コールアドミッション統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto isakmp call admission statistics
```

関連コマンド

コマンド	説明
show crypto isakmp call admission statistics , (221 ページ)	IKE プロトコルに対する Call Admission Control (CAC; コールアドミッション制御) の設定を表示します。

clear crypto isakmp errors

Internet Security Association and Key Management Protocol (ISAKMP) エラーの統計情報をクリアするには、EXEC モードで **clear crypto isakmp errors** コマンドを使用します。

clear crypto isakmp error

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

変更箇所

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

実行

例

次に、ISAKMP エラー統計情報をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp errors
```

```
Control Plane Errors
```

```
-----
ERR NO MEMORY.....0
INVALID CERT.....0
CRYPTO FAILURE.....0
SA NOT AUTH.....0
AUTHENTICATION FAILED.....0
GROUP AUTHOR FAILED.....0
```

```

USER AUTHEN REJECTED.....0
LOCAL ADDRESS FAILURE.....0
FAILED TO CREATE SKEYID.....0
RSA PUBLIC KEY NOT FOUND.....0
RETRANSMISSION LIMIT.....0
MALFORMED MESSAGE.....0
QUICK MODE TIMER EXPIRED.....0
KEY NOT FOUND IN PROFILE.....0
PROFILE NOT FOUND.....0
PRESHARED KEY NOT FOUND.....0
PHASE2 PROPOSAL NOT CHOSEN.....0
POLICY MISMATCH.....0
NO POLICY FOUND.....0
PACKET PROCESS FAILURE.....0

Warnings
-----
CERT DOESNT MATCH ID.....0
CERT ISNT TRUSTED ROOT.....0
PACKET NOT ENCRYPTED.....0
UNRELIABLE INFO MSG.....0
NO SA.....0
BAD DOI SA.....0
UNKNOWN EXCHANGE TYPE.....0
OUTGOING PKT TOO BIG.....0
INCOMING PKT TOO BIG.....0

Informational
-----
CAC DROPS.....0
DEFAULT POLICY ACCEPTED.....0

RP/0/RSP0/CPU0:router# clear crypto isakmp errors
    
```

関連コマンド

コマンド	説明
show crypto isakmp errors	トンネルの確立時に発生する ISAKMP エラーを表示します。

clear crypto session

暗号化セッション (IP セキュリティ [IPSec] およびインターネットキー交換 [IKE] セキュリティ アソシエーション [SA]) を削除するには、EXEC モードで **clear crypto session** コマンドを使用します。

clear crypto session [*user username*| *group group*| *interface*| *ivrf vrf-name*| *local ip-address*| *fvrp vrf-name*| *remote ip-address*]

構文の説明

user <i>username</i>	(任意) ユーザの名前を指定します。
group <i>group</i>	(任意) グループの識別名を指定します。
interface	(任意) インターフェイスの名前を指定します。
ivrf <i>vrf-name</i>	(任意) クリアされる 内部 VRF (IVRF) セッションを指定します。
local <i>ip-address</i>	(任意) ローカル暗号化エンドポイントの暗号化セッションをクリアします。 <i>ip-address</i> 引数は、ローカル暗号化エンドポイントの IP アドレスです。
fvrp <i>vrf-name</i>	(任意) Front Door Virtual Routing and Forwarding (FVRF; 前面扉仮想ルーティングおよび転送) セッションを指定します。
remote <i>ip-address</i>	(任意) リモート IKE ピアの暗号化セッションをクリアします。 <i>ip-address</i> 引数は、リモート IKE ピアの IP アドレスです。

コマンド デフォルト

キーワードを指定しないで **clear crypto session** コマンドを入力した場合は、既存のすべてのセッションがクリアされます。IPSec SA が最初に削除されます。次に、IKE SA が削除されます。リモート ポートのデフォルト値は 500 です。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
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。

特定の暗号化セッションまたはすべてのセッションのサブセットをクリアするには、ローカルインターフェイス、ローカル IP アドレス、リモート IP アドレス（およびポート）、FVRF 名、または IVRF 名などのセッション固有のパラメータを指定する必要があります。

ローカル IP アドレスがパラメータとして指定された場合は、その IP アドレスをローカル暗号化エンドポイント（IKE ローカルアドレス）として共有するすべてのセッション（とその IKE SA および IPSec SA）が削除されます。

タスク ID

タスク ID	操作
crypto	実行

例

次に、すべての暗号化セッションを削除する例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto session
```

次に、"blue" という名前の FVRF の暗号化セッションが削除される例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto session fvrf blue
```

次に、ローカル エンドポイント 10.1.1.1 の暗号化セッションが削除される例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto session local 10.1.1.1
```

関連コマンド

コマンド	説明
description (ISAKMP ピア) , (184 ページ)	インターネットキー交換 (IKE) ピアの説明を追加します。
show crypto session , (251 ページ)	アクティブな暗号セッションのステータス情報を表示します。

crypto isakmp

ピア ルータでインターネットキー交換 (IKE) をグローバルに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 **crypto isakmp** コマンドを使用します。ピアで IKE 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。

crypto isakmp

no crypto isakmp

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

IKE 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	変更箇所
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。

IKE は 個々のインターフェイスに対してイネーブルにする必要はありませんが、ルータのすべてのインターフェイスに対してグローバルにイネーブルにします。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、1 つのピアの IKE をディセーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp
RP/0/RSP0/CPU0:router(config)# no crypto isakmp
```

crypto isakmp call admission limit

複数のメトリックに基づいて着信または発信セッション要求を拒否するには、グローバル コンフィギュレーション モードで **crypto isakmp call admission limit** 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。

crypto isakmp call admission limit {cpu {total percent| ike percent}| in-negotiation-sa number| sa number}
no crypto isakmp call admission limit {cpu {total percent| ike percent}| in-negotiation-sa number| sa number}

構文の説明

cpu	新しいコールを受け入れるための CPU 使用率の合計リソース制限を指定します。
total percent	新しいコールを受け入れるための最大合計 CPU 使用率を指定します。percent 引数の範囲は 1 ~ 100 です。
ike percent	新しいコールを受け入れるための最大 IKE CPU 使用率を指定します。percent 引数の範囲は 1 ~ 100 です。
in-negotiation-sa number	IKE が新しい SA 要求の拒否を開始するまでにルータが確立できる、ネゴシエーション中（初期）IKE セキュリティ アソシエーション（SA）の最大数を指定します。number 引数の範囲は 1 ~ 100000 です。
sa number	IKE が新しい SA 要求の拒否を開始するまでにルータが確立できる、アクティブな IKE SA の最大数を指定します。ネゴシエーション中の接続数に制限を設定できます。このタイプの接続は、認証と実際の確立よりも前の、アグレッシブ モードの IKE SA またはメイン モードの SA を意味します。number 引数の範囲は 1 ~ 100000 です。

コマンド デフォルト

in-negotiation-sa キーワードのデフォルト値は 1000 SA に設定されています。

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	変更箇所
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。

ネゴシエーションを処理するのに十分なシステムリソースが存在しない場合、IKESA の要求は拒否されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、**crypto isakmp call admission limit** 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)# crypto isakmp call admission limit cpu ike 30
```

関連コマンド

コマンド	説明
crypto ipsec profile	IPSec プロファイルを設定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。

crypto isakmp identity

インターネットキー交換 (IKE) プロトコルへの参加時にルータで使用される識別情報を指定するには、グローバル コンフィギュレーション モードで **crypto isakmp identity** コマンドを使用します。Internet Security Association Key Management Protocol (ISAKMP) 識別情報をデフォルト値 (address) 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。

crypto isakmp identity {address| hostname}

no crypto isakmp identity

構文の説明

address	ISAKMP 識別情報を、IKE ネゴシエーション時にリモート ピアと通信するインターフェイスの IP アドレスに設定します。
hostname	ISAKMP 識別情報を、ドメイン名と連結されたホスト名 (例: myhost.example.com) に設定します。

コマンド デフォルト

IP アドレスが ISAKMP 識別情報に使用されます。

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	変更箇所
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 アドレスまたはホスト名のいずれかによって ISAKMP 識別情報を指定するには、**crypto isakmp identity** コマンドを使用します。原則として、ピアの識別情報はすべて同じ方法で (IP アドレスまたはホスト名のいずれかで) 設定してください。

事前共有キーを指定する場合は必ず ISAKMP 識別情報を設定します。

IKE ネゴシエーションに 1 つのインターフェイスだけ (したがって、1 つの IP アドレスだけ) がピアによって使用され、その IP アドレスが既知である場合は、**address** キーワードを使用します。

ピア上の複数のインターフェイスが IKE ネゴシエーションに使用される可能性がある場合、またはインターフェイスの IP アドレスが未知である場合（ダイナミックに割り当てられる IP アドレスなど）は、**hostname** キーワードを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、2つのピアで事前共有キーを使用し、両方の ISAKMP 識別情報を IP アドレスに設定する例を示します。

ローカルピア（10.0.0.1）で、ISAKMP 識別情報が設定され、事前共有キーが指定されます。

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 192.168.1.33 key presharedkey
```

リモートピア（192.168.1.33）で、ISAKMP 識別情報が設定され、同じ事前共有キーが指定されません。

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity address
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.0.0.1 key presharedkey
```



(注)

前の例で、**crypto isakmp identity** コマンドが実行されなかった場合、ISAKMP 識別情報は IP アドレス（デフォルトの識別情報）に設定されたままになります。

次に、2つのピアで事前共有キーを使用し、両方の ISAKMP 識別情報をホスト名に設定する例を示します。

ローカルピアで、ISAKMP 識別情報が設定され、事前共有キーが指定されます。

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname remoterouter.example.com key presharedkey
```

リモートピアで、ISAKMP 識別情報が設定され、同じ事前共有キーが指定されます。

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp identity hostname
RP/0/RSP0/CPU0:router(config)# crypto keyring keyring1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname localrouter.example.com key presharedkey
```

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。

コマンド	説明
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。
local-address (キーリング), (202 ページ)	ISAKMP キーリング設定の範囲を、ローカルターミネーションアドレスに限定します。
pre-shared-key , (211 ページ)	IKE 認証の事前共有キーを定義します。

crypto isakmp keepalive

インターネットキー交換 (IKE) セキュリティ アソシエーション (SA) 機能を使用して 2 つの IP セキュリティ (IPSec) ピア間の接続切断を検出するメカニズムを提供するには、グローバル コンフィギュレーション モードで **crypto isakmp keepalive** 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。

crypto isakmp keepalive seconds retry-seconds

no crypto isakmp keepalive

構文の説明

<i>seconds</i>	キープアライブ メッセージの間隔を指定する秒数。範囲は 10 ～ 3600 です。
<i>retry-seconds</i>	キープアライブが失敗した場合の再試行の間隔を指定する秒数。範囲は 2 ～ 60 です。

コマンド デフォルト

このコマンドで指定されない限り、IKE はキープアライブ メッセージを送信しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

4 回試行してもピアからキープアライブ 応答メッセージを受け取らなかった場合、IKE はピアとの接続が切断されたと判断します。

タスク ID

タスク ID	操作
crypto	read, write

例

キープアライブメッセージの間隔を 20 秒に設定し、キープアライブが失敗した場合の再試行の間隔を 20 秒に設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure  
RP/0/RSP0/CPU0:router(config)# crypto isakmp keepalive 20
```

関連コマンド

コマンド	説明
crypto isakmp identity , (163 ページ)	IKE プロトコルへの参加時にルータが使用する識別情報を指定します。

crypto isakmp peer

インターネットキー交換 (IKE) 用に IP セキュリティ (IPSec) ピア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 **crypto isakmp peer** 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。

crypto isakmp peer {address *ip-address*| hostname *hostname*} [**description** *line*| vrf *vrf-name*]

no crypto isakmp peer {address *ip-address*| hostname *hostname*} [**description** *line*| vrf *vrf-name*]

構文の説明

address <i>ip-address</i>	ピア ルータの IP アドレスを指定します。
hostname <i>hostname</i>	ピアのホスト名を指定します。
description <i>line</i>	(任意) IKE ピアの説明を指定します。ピアの説明に使用できる文字の最大数は 80 文字です。
vrf <i>vrf-name</i>	(任意) ピアから到達可能な VPN ルーティングおよび転送 (VRF) ルーティング テーブルを指定します。 <i>vrf-name</i> 引数は、VPN ルーティングおよび転送 (VRF) 設定時に定義された FVRF 名と一致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

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	変更箇所
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。

ISAKMP ピア コンフィギュレーション モードを開始するには、**crypto isakmp peer** コマンドを使用します。

IP アドレスで識別されるピアに、意味のある名前または説明を付与することができます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、ピアのアドレスが 40.40.40.2 で名前が citeA である場合の例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp peer address 40.40.40.2
RP/0/RSP0/CPU0:router(config-isakmp-peer)# description citeA
RP/0/RSP0/CPU0:router(config-isakmp-peer)# commit

RP/0/RSP0/CPU0:router# show crypto isakmp peers
Peer: 60.60.60.2 Port: 500 Local: 70.70.70.2 vrf: default
  UDP encapsulate: False
  SA information:
    Connection ID: 2
    State: QM_IDLE
    Phase 1 ID: IPV4_ADDR 60.60.60.2

Peer: 40.40.40.2 Port: 500 Local: 50.50.50.2 vrf: default
  Description: peerA
  UDP encapsulate: False
  SA information:
    Connection ID: 1
    State: QM_IDLE
    Phase 1 ID: IPV4_ADDR 40.40.40.2
```

関連コマンド

コマンド	説明
description (ISAKMP ピア) , (184 ページ)	インターネットキー交換 (IKE) ピアの説明を追加します。
show crypto isakmp peers, (234 ページ)	ピアの構造を表示します。

crypto isakmp policy

インターネットキー交換 (IKE) ポリシーを定義するには、グローバル コンフィギュレーション モードで **crypto isakmp policy** コマンドを使用します。IKE ポリシーを削除するには、このコマンドの **no** 形式を使用します。

crypto isakmp policy priority

no crypto isakmp policy priority

構文の説明

<i>priority</i>	IKE ポリシーを一意に識別し、保護ポリシーにプライオリティを割り当てる値。1～10000の整数を使用します (1が最高で10000が最低のプライオリティ)。
-----------------	---

コマンド デフォルト

デフォルト ポリシーがあり、常に最低のプライオリティが設定されています。デフォルト ポリシーには、暗号化、ハッシュ、認証、Diffie-Hellman グループ、およびライフタイムパラメータのデフォルト値が含まれています (パラメータのデフォルトについては、「使用上のガイドライン」を参照してください)。IKE ポリシーを作成する際に、値を指定しない場合は特定のパラメータのデフォルトが使用されます。

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	変更箇所
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。

IKE ネゴシエーション時に使用するパラメータを指定するには、**crypto isakmp policy** コマンドを使用します (これらのパラメータによって IKE セキュリティ アソシエーション [SA] が作成されます)。

crypto isakmp policy コマンドにより、ISAKMP ポリシー 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、ポリシーのパラメータを指定するために次のコマンドを使用できません。

- **authentication** (IKE ポリシー) , (149 ページ) コマンド : デフォルト値が Rivest, Shamir, and Adelman (RSA) シグニチャになるように指定します。
- **description** (IKE ポリシー) , (180 ページ) コマンド : IKE ポリシーの説明を作成します。
- **encryption** (IKE ポリシー) , (188 ページ) コマンド : 次の規格のいずれかに従って保護スイートの暗号化アルゴリズムを設定します。
- **group** (IKE ポリシー) , (190 ページ) コマンド : デフォルト値が 768 ビット Diffie-Hellman になるように指定します。
- **hash** (IKE ポリシー) , (192 ページ) コマンド : デフォルト値が SHA-1 になるように指定します。
- **lifetime** (IKE ポリシー) , (200 ページ) コマンド : デフォルト値が 86,400 秒 (1 日) になるように指定します。

ポリシーに対してこれらのコマンドのいずれかを指定しない場合、そのパラメータのデフォルト値が使用されます。

IP セキュリティ (IPSec) に参加する各ピアに複数の IKE ポリシーを設定できます。IKE ネゴシエーションが開始されると、リモートピアに指定された最高プライオリティのポリシーから順に、両方のピアに設定された共通のポリシーの検索が試行されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、ピアに 2 つのポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# hash md5
RP/0/RSP0/CPU0:router(config-isakmp)# authentication rsa-sig
RP/0/RSP0/CPU0:router(config-isakmp)# group 2
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 5000
RP/0/RSP0/CPU0:router(config-isakmp)# exit
```

```
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 20
RP/0/RSP0/CPU0:router(config-isakmp)# authentication pre-share
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 10000
RP/0/RSP0/CPU0:router(config-isakmp)# exit
```

結果として次のようなポリシーが設定されます。

```
Protection suite priority 15
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Message Digest 5
  authentication method: Rivest-Shamir-Adelman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
```

```

hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman Group: #1 (768 bit)
lifetime: 10000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman Group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit

```

IKE ポリシー 15 が最高のプライオリティで、デフォルト ポリシーが最低のプライオリティです。

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
description (IKE ポリシー) , (180 ページ)	ISAKMP ポリシーの説明を指定します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュ アルゴリズムを指定します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。
show crypto isakmp policy , (236 ページ)	各 IKE ポリシーのパラメータを表示します。

crypto isakmp policy-set

ISAKMP 保護スイート用のポリシーセットを定義するには、グローバル コンフィギュレーション モードで **crypto isakmp policy-set** コマンドを使用します。以前に設定されたポリシーセットをキャンセルするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy-set *policy-name*

no crypto isakmp policy-set *policy-name*

構文の説明

<i>policy-name</i>	ポリシー セットの名前。
--------------------	--------------

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	変更箇所
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。

このコマンドを使用すると、ISAKMP ポリシー セット 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
crypto	read, write

例

次に、リモートアクセスのユーザが特定の ISAKMP ポリシーにアクセスできないように制限するために、ローカル アドレスに基づいて ISAKMP ポリシー セットを定義する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy-set mypolicy
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)#
```

関連コマンド

コマンド	説明
description (ISAKMP ポリシーセット) , (182 ページ)	ISAKMP ポリシーセットの説明です。
match identity (ISAKMP ポリシーセット) , (204 ページ)	SVI トンネル ソースを作成します。この手順で識別された IP にユーザが接続すると、定義済みの暗号化アルゴリズムが動作するようになります。
policy (ISAKMP ポリシーセット) , (209 ページ)	事前設定されたポリシーを使用するためのプライオリティを指定します。

crypto isakmp profile

ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査するには、グローバル コンフィギュレーション モードで **crypto isakmp profile** コマンドを使用します。名前付き暗号化 ISAKMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

crypto isakmp profile {profile-name| local profile-name}

no crypto isakmp profile {profile-name| local profile-name}

構文の説明

local	ローカルが送信元または終端であるトラフィックに使用されるプロファイルを指定します。 (注) ローカルが送信元または宛先であるトラフィックを定義する場合は、ISAKMP プロファイルに local キーワードが使用されます。このトラフィックはルートプロセッサ (RP) によって復号化または暗号化されます。
profile-name	ユーザ プロファイルの名前。ユーザ プロファイルを RADIUS サーバに関連付けるには、ユーザ プロファイル名が識別されている必要があります。

コマンド デフォルト

なし

コマンド モード

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	変更箇所
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。

ローカルが送信元または宛先であるトラフィックを定義する場合は、ISAKMP プロファイルに **local** キーワードが使用されます。このトラフィックは、Cisco IPSec VPN SPA ではなく、ルートプロセッサ (RP) によって復号化または暗号化されます。

ISAKMP プロファイルに定義された識別情報と突き合わせて（インターネットキー交換 [IKE] の識別子 [ID] ペイロードに指定されたとおりに）識別情報が一致した場合に、ピアは ISAKMP プロファイルにマッピングされます。1つの ISAKMP プロファイルに一意にマッピングするには、2つの ISAKMP プロファイルが同じ識別情報と一致しないようにする必要があります。ピアの識別情報が2つの ISAKMP プロファイルと一致する場合、その設定は無効です。プロファイルが完全であるためには、ISAKMP プロファイルに少なくとも1つの **match identity** コマンドが定義されていることも必要です。

ISAKMP プロファイルを設定する前に、プロファイルに使用されるキーリングを設定する必要があります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、ISAKMP プロファイルを定義し、ピアの識別情報を照合する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local profile1vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity address 10.1.1.0/24group vpngrpou
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-service-ipsec 1
```

関連コマンド

コマンド	説明
isakmp authorization list	インターネットキー交換 (IKE) 対話の許可に使用される許可リストを指定します。
keepalive (ISAKMP プロファイル) , (194 ページ)	ゲートウェイが Dead Peer Detection (DPD) メッセージをピアに送信できるようにします。
self-identity	ローカル IKE がリモートピアに対して IKE 自身を識別させるために使用する ID を定義します。
set interface tunnel-ipsec , (217 ページ)	インターフェイスインスタンスを事前定義します。
set ipsec-profile , (219 ページ)	IPSec プロファイルを事前定義します。
show crypto isakmp profile , (239 ページ)	ルータに定義されている ISAKMP プロファイルをすべてリストします。

関連コマンド

crypto keyring

IKE 認証時の暗号キーリングを定義するには、グローバルコンフィギュレーションモードで **crypto keyring** コマンドを使用します。キーリングを削除するには、このコマンドの **no** 形式を使用します。

crypto keyring *keyring-name* [*vrf fvrf-name*]

no crypto keyring *keyring-name* [*vrf fvrf-name*]

構文の説明

<i>keyring-name</i>	暗号キーリングの名前。キーリング名の最大長は 32 文字です。
<i>vrf fvrf-name</i>	(任意) キーリングの参照先となる前面扉仮想ルーティングおよび転送 (FVRF) 名を指定します。 <i>fvrf-name</i> 引数は、仮想ルーティングおよび転送 (VRF) 設定時に定義された FVRF 名と一致する必要があります。

コマンド デフォルト

vrf キーワードが定義されない場合、キーリングの参照先はグローバル VRF 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	変更箇所
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。

キーリングは、事前共有キーおよび RSA 公開キーのリポジトリです。キーリングはグローバルコンフィギュレーションモードで使用されます。このプロファイルに対応付けられるキーリングにピアのキーが定義されている場合、ISAKMP プロファイルはピアの認証を正常に完了します。

キーリング コンフィギュレーション モードを開始するには、**crypto keyring** 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、**crypto keyring** 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)# crypto keyring vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnsecret
```

関連コマンド

コマンド	説明
crypto isakmp identity , (163 ページ)	インターネットキー交換 (IKE) プロトコルへの参加時にルータが使用する識別情報を指定します。
description (キーリング), (186 ページ)	キーリングの説明を作成します。
local-address (キーリング), (202 ページ)	ISAKMP キーリング設定の範囲を、ローカルターミネーションアドレスまたはインターフェイスに限定します。
pre-shared-key , (211 ページ)	IKE 認証の事前共有キーを定義します。
rsa-pubkey , (213 ページ)	アドレスまたはホスト名によって Rivest, Shamir, and Adelman (RSA) 公開キーを定義します。

crypto logging

暗号化トンネルのアップまたはダウンメッセージの表示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 **crypto logging** コマンドを使用します。このオプション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。

crypto logging tunnel-status

no crypto logging tunnel-status

構文の説明

tunnel-status	トンネルステータスのロギングをイネーブルにします。
---------------	---------------------------

コマンド デフォルト

デフォルトではディセーブルになっています。

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	変更箇所
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, write

例

次に、**crypto logging** 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)# crypto logging tunnel-status
```

description (IKE ポリシー)

インターネットキー交換 (IKE) ポリシーの説明を作成するには、ISAKMP ポリシー 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。IKE ポリシー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 IKE ポリシーを説明する文字ストリング。

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	変更箇所
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。

IKE ポリシーの説明を作成するには、ISAKMP ポリシー 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
crypto	read, write

例

次に、IKE ポリシー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 isakmp policy 15  
RP/0/RSP0/CPU0:router(config-isakmp)# description this is a sample IKE policy
```

description (ISAKMP ポリシーセット)

ISAKMP ポリシーセットの説明を作成するには、ISAKMP ポリシー 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。ISAKMP ポリシーセッ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 IKE ポリシー セットを説明する文字ストリングです。

コマンド デフォルト

なし

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

IKE ポリシーセットの説明を作成するには、ISAKMP ポリシーセット 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
crypto	read, write

例

次に、IKE ポリシー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 isakmp policy-set pol1
RP/0/RSP0/CPU0:router(config-isakmp-pol-set)# description this is a sample IKE policy-set
```

関連コマンド

コマンド	説明
crypto isakmp policy-set , (173 ページ)	ISAKMP 保護スイートのポリシーセットを定義します。
match identity (ISAKMP ポリシーセット) , (204 ページ)	事前設定されたポリシーセットと一致する識別情報に基づいて、SVI トンネルソースを作成します。
policy (ISAKMP ポリシーセット) , (209 ページ)	事前設定されたポリシーのルーティングプライオリティを指定します。

description (ISAKMP ピア)

インターネットキー交換 (IKE) ピアの説明を追加するには、ISAKMP ピア 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。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 *string*

構文の説明

string IKE ピアに付与する説明。最大数は 80 文字です。

コマンド デフォルト

なし

コマンド モード

ISAKMP ピア コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

ネットワーク アドレス変換 (NAT) デバイスの背後に「配置」された IKE ピアは一意に識別することができないため、同じピアの説明を共有する必要があります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、IKE ピアに「connection from site A」という説明を追加する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp peer address 10.2.2.9
RP/0/RSP0/CPU0:router(config-isakmp-peer)# description connection from site A
```

関連コマンド

コマンド	説明
clear crypto session, (158 ページ)	ISAKMP グループおよびユーザの暗号化セッション IPSec および IKE SA を削除します。
crypto isakmp peer, (168 ページ)	インターネットキー交換 (IKE) 用に IP セキュリティ (IPSec) ピアをイネーブルにします。
show crypto isakmp peers, (234 ページ)	ピアの構造を表示します。
show crypto session, (251 ページ)	アクティブな暗号セッションのステータス情報を表示します。
auto-update client	ISAKMP グループおよびユーザの暗号化セッション IPSec および IKE SA を削除します。

description (キーリング)

キーリングの1行説明を作成するには、キーリング 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。キーリング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 キーリング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

キーリング コンフィギュレーション

コマンド履歴

リリース

変更箇所

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, write

例

次に、キーリング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 keyring vpnkey
RP/0/RSP0/CPU0:router (config-keyring)# description this is a sample keyring
```

関連コマンド

コマンド	説明
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。

encryption (IKE ポリシー)

インターネットキー交換 (IKE) ポリシー内の暗号化アルゴリズムを指定するには、ISAKMP ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。暗号化アルゴリズム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。

encryption {des|3des|aes|aes 192|aes 256}

no encryption

構文の説明

des	暗号化アルゴリズムとして 56 ビット DES-CBC を指定します。このオプションがデフォルト値です。
3des	暗号化アルゴリズムとして 168 ビット Digital Encryption Standard (DES; デジタル暗号化規格) を指定します。
aes	暗号化アルゴリズムとして 128 ビット Advanced Encryption Standard (AES) を指定します。
aes 192	暗号化アルゴリズムとして 192 ビット AES を指定します。
aes 256	暗号化アルゴリズムとして 256 ビット AES を指定します。

コマンド デフォルト

56 ビット DES-CBC 暗号化アルゴリズム (**des**) です。

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

IKE ポリシーは、IKE ネゴシエーション時に使用される一連のパラメータを定義したものです。IKE ポリシーの暗号化アルゴリズムを指定するには、**encryption** 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、3DES暗号化アルゴリズムを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# encryption 3des
```

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュアルゴリズムを指定します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。
show crypto isakmp policy , (236 ページ)	各 IKE ポリシーのパラメータを表示します。

group (IKE ポリシー)

インターネットキー交換 (IKE) ポリシー内の Diffie-Hellman ID を指定するには、ISAKMP ポリシー 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。Diffie-Hellman グループ ID 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。

group {1|2|5}

no group

構文の説明

1	768 ビット Diffie-Hellman グループを指定します。このオプションがデフォルトです。
2	1024 ビット Diffie-Hellman グループを指定します。
5	1536 ビット Diffie-Hellman グループを指定します。

コマンド デフォルト

デフォルトは 768 ビット Diffie-Hellman (グループ 1) です

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

IKE ポリシーは、IKE ネゴシエーション時に使用される一連のパラメータを定義したものです。IKE ポリシーの Diffie-Hellman グループを指定するには、**group (IKE ポリシー)** 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、1024 ビット Diffie-Hellman グループを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# group 2
```

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュアルゴリズムを指定します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。
show crypto isakmp policy , (236 ページ)	各 IKE ポリシーのパラメータを表示します。

hash (IKE ポリシー)

インターネットキー交換 (IKE) ポリシー内のハッシュ アルゴリズムを指定するには、ISAKMP ポリシー コンフィギュレーション モードで **hash** コマンドを使用します。ハッシュ アルゴリズムをデフォルトの SHA-1 ハッシュ アルゴリズム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。

hash {sha|md5}

no hash

構文の説明

sha	ハッシュ アルゴリズムとして SHA-1 (Hashed Message Authentication Code [HMAC]) を指定します。このオプションがデフォルトです。
md5	ハッシュ アルゴリズムとして Message Digest 5 (MD5) (HMAC バリエント) を指定します。

コマンド デフォルト

SHA-1 ハッシュ アルゴリズム

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

IKE ポリシーのハッシュ アルゴリズムを指定するには、**hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用される一連のパラメータを定義したものです。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、MD5 ハッシュ アルゴリズムを指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# Crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# hash md5
```

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。
show crypto isakmp policy , (236 ページ)	各 IKE ポリシーのパラメータを表示します。

keepalive (ISAKMP プロファイル)

ゲートウェイが Dead Peer Detection (DPD) メッセージをピアに送信できるようにするには、ISAKMP プロファイル コンフィギュレーション モードで **keepalive** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

keepalive disable

no keepalive

構文の説明

disable キープアライブのグローバル宣言をディセーブルにします。

コマンド デフォルト

キープアライブはイネーブルです。

コマンド モード

ISAKMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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, write

例

次に、**keepalive** 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)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# keepalive disable
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。

keyring

ISAKMP プロファイルとともにキーリングを設定するには、ISAKMP プロファイル コンフィギュレーション モードで **keyring** コマンドを使用します。ISAKMP プロファイルからキーリングを削除するには、このコマンドの **no** 形式を使用します。

keyring *kr-name1* [*kr-name2* [*kr-name3* [*kr-name4* [*kr-name5* [*kr-name6*]]]]]

no keyring *kr-name1* [*kr-name2* [*kr-name3* [*kr-name4* [*kr-name5* [*kr-name6*]]]]]

構文の説明

<i>kr-name1</i>	キーリング 1 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致する必要があります。
<i>kr-name2</i>	キーリング 2 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致する必要があります。
<i>kr-name3</i>	キーリング 3 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致する必要があります。
<i>kr-name4</i>	キーリング 4 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致する必要があります。
<i>kr-name5</i>	キーリング 5 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致する必要があります。
<i>kr-name6</i>	キーリング 6 の名前です。これはグローバル コンフィギュレーションで定義されたキーリング名と一致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 ISAKMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

このプロファイルに対応付けられるキーリングにピアのキーが定義されている場合、ISAKMP プロファイルはピアの認証を正常に完了します。少なくとも 1 つのキーリングを定義する必要があります。

ISAKMP プロファイルでは 1 つまたは複数のキーリングを定義できます。たとえば、IKE ピア エンドポイントがパブリックアドレス空間にほとんどないのに対して、他のものは IKE ローカルエンドポイントとして前面扉仮想ルーティングおよび転送 (FVRF) スペースにある場合は、複数のキーリングを使用できます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、vpnkeyring をキーリング名に設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# keyring vpnkeyring
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザ セッションを監査します。
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。
show crypto isakmp profile , (239 ページ)	ルータに定義されている ISAKMP プロファイルをすべてリストします。

例

次に、IPSec ピアの RSA 公開キーを手動で指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey address 10.5.5.1
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
```

関連コマンド

コマンド	説明
rsa-pubkey, (213 ページ)	アドレスまたはホスト名によってRivest, Shamir, and Adelman (RSA) 公開キーを定義します。
show crypto key pubkey-chain rsa, (248 ページ)	ルータに保存されているピアの RSA 公開キーを表示します。

lifetime (IKE ポリシー)

インターネットキー交換 (IKE) セキュリティ アソシエーション (SA) のライフタイムを指定するには、ISAKMP ポリシー コンフィギュレーション モードで **lifetime** コマンドを使用します。SA のライフタイム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。

lifetime seconds

no lifetime

構文の説明

<i>seconds</i>	期限切れになるまでに各 SA が存在する時間 (秒単位)。60 ~ 86400 秒の整数を使用します。
----------------	---

コマンド デフォルト

86400 秒 (1 日)

コマンド モード

ISAKMP ポリシー コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

期限切れになるまでに IKE SA が存在する時間を指定するには、**lifetime** コマンドを使用します。

IKE はネゴシエーションの開始時に、最初に自身のセッション用のセキュリティ パラメータに同意します。その後、同意済みのパラメータが各ピアで SA によって参照されます。SA は、SA のライフタイムが期限切れになるまで各ピアによって保持されます。SA が期限切れになるまで、SA は次の IKE ネゴシエーションで再利用することができるので、新しい IP セキュリティ (IPSec) SA が設定される際の時間を節約できます。

IPSec の設定時間を節約するには、IKE SA のライフタイムを長めに設定します。ただし、ライフタイムが短いほど、この SA の攻撃者への露出は制限されます。SA が長く使用されるほど、攻撃者はより多くの暗号化トラフィックを収集できるようになり、それが攻撃に使用される可能性が高くなります。



(注) ローカル ピアがリモート ピアとの IKE ネゴシエーションを開始する際に、ライフタイムが等しくない場合は、ライフタイムが短いほうの IKE ポリシーが選択されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、SA ライフタイムを 600 秒に指定した（他のパラメータはすべてデフォルトに設定された）IKE ポリシーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp policy 15
RP/0/RSP0/CPU0:router(config-isakmp)# lifetime 600
```

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュアルゴリズムを指定します。
show crypto isakmp policy , (236 ページ)	各 IKE ポリシーのパラメータを表示します。


```
RP/0/RSP0/CPU0:router(config-keyring)# local-address 130.40.1.1
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 0.0.0.0 0.0.0.0 key mykey
```

関連コマンド

コマンド	説明
crypto isakmp identity , (163 ページ)	インターネットキー交換 (IKE) プロトコルへの参加時にルータが使用する識別情報を指定します。
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。

match identity (ISAKMP ポリシーセット)

SVI トンネルソースを作成するには、ISAKMP ポリシーセット コンフィギュレーション モードで **match identity** コマンドを使用します。識別情報を削除するには、このコマンドの **no** 形式を使用します。

match identity local-address *IP address*

no match identity local-address *IP address*

構文の説明

local-address	これにより、リモート ピア用の SVI トンネル ソースが作成されます。
<i>IP address</i>	SVI トンネル ソースの IP プレフィックスです。

コマンド デフォルト

なし

コマンド モード

ISAKMP ポリシーセット コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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。

ISAKMP プロファイル コンフィギュレーションには、少なくとも 1 つの **match identity** コマンドが必要です。ISAKMP プロファイルに定義された識別情報と突き合わせて (IKE 交換の ID ペイロードに指定されたとおりに) 識別情報が一致した場合に、ピアは ISAKMP プロファイルにマッピングされます。1 つの ISAKMP プロファイルに一意にマッピングするには、2 つの ISAKMP プロファイルが同じ識別情報と一致しないようにする必要があります。ピアの識別情報が 2 つの ISAKMP プロファイルと一致する場合、その設定は無効です。

このコマンドで識別される IP アドレスには、特定の暗号化アルゴリズムが事前設定されている必要があります、それが 1 つだけ動作していることが必要です。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、**match identity** (ISAKMP ポリシーセット) コマンドを設定する例を示します。

```
/CPU0:router(config)# crypto isakmp policy-set ps2
/CPU0:router(config-isakmp-pol-set)# policy 60 61
/CPU0:router(config-isakmp-pol-set)# match identity local-address 12.13.51.1
```

関連コマンド

コマンド	説明
crypto isakmp policy-set , (173 ページ)	ISAKMP 保護スイートのポリシーセットを定義します。
policy (ISAKMP ポリシーセット) , (209 ページ)	事前設定されたポリシーのルーティングプライオリティを指定します。
description (ISAKMP ポリシーセット) , (182 ページ)	ISAKMP ポリシーセットの説明を作成します。

match identity (ISAKMP プロファイル)

ISAKMP プロファイルでピアの識別情報を照合するには、ISAKMP プロファイル コンフィギュレーション モードで **match identity** コマンドを使用します。識別情報を削除するには、このコマンドの **no** 形式を使用します。

```
match identity {group group-name| address address [mask] vrf [fvr]} host hostname| host domain
domain-name| user username| user domain domain-name}
```

```
no match identity {group group-name| address address [mask] vrf [fvr]} host hostname| host domain
domain-name| user username| user domain domain-name}
```

構文の説明

group <i>group-name</i>	識別子 (ID) タイプ ID_KEY_ID と一致する Unity グループを指定します。RSA シグニチャを使用する場合、 <i>group-name</i> 引数は Distinguished Name (DN; 認定者名) の Organizational Unit (OU; 組織ユニット) フィールドと一致します。
address <i>address</i>	<i>address</i> 引数を ID タイプ ID_IPV4_ADDR と照合します。
<i>mask</i>	<i>mask</i> 引数はアドレスの範囲を指定するのに使用されます。
vrf	ピアの前面扉 VPN ルーティングおよび転送 (FVRF) を指定します。
<i>fvr</i>	<i>fvr</i> 引数は、前面扉 VPN ルーティングおよび転送 (FVRF) バーチャルプライベートネットワーク (VPN) 領域のアドレスと一致します。
host <i>hostname</i>	Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) がドメイン名で終わるタイプ ID_FQDN と一致する識別情報を指定します。
host domain <i>domain-name</i>	タイプ ID_FQDN と一致する識別情報を指定します。ドメイン名は <i>domain-name</i> 引数と同じです。
user <i>username</i>	FQDN と一致する識別情報を指定します。
user domain <i>domain-name</i>	タイプ ID_USER_FQDN と一致する識別情報を指定します。 user domain キーワードが存在する場合、タイプ ID_USER_FQDN の識別情報を持ち、 <i>domain-name</i> で終わるすべてのユーザが照合されます。

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 ISAKMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

ISAKMP プロファイル コンフィギュレーションには、少なくとも 1 つの **match identity** コマンドが必要です。ISAKMP プロファイルに定義された識別情報と突き合わせて (IKE 交換の ID ペイロードに指定されたとおりに) 識別情報が一致した場合に、ピアは ISAKMP プロファイルにマッピングされます。1 つの ISAKMP プロファイルに一意にマッピングするには、2 つの ISAKMP プロファイルが同じ識別情報と一致しないようにする必要があります。ピアの識別情報が 2 つの ISAKMP プロファイルと一致する場合、その設定は無効です。



(注)

tunnel-ipsec インターフェイスを設定するには、ローカル ISAKMP プロファイルを設定する必要があります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、**match identity** コマンド用の vpngroup としてグループを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local_tunnel_ipsec
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity address 10.1.1.6/32 vrf default
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-ipsec3001
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。

コマンド	説明
self-identity	ローカル IKE がリモートピアに対して IKE 自身を識別させるために使用する ID を定義します。
set interface tunnel-ipsec, (217 ページ)	インターフェイスインスタンスを事前定義します。
set ipsec-profile, (219 ページ)	IPSec プロファイルインスタンスを事前定義します。

policy (ISAKMP ポリシーセット)

事前設定されたポリシーのルーティングプライオリティを指定するには、ISAKMP ポリシーセットサブモード内で **policy** コマンドを使用します。プライオリティをキャンセルするには、このコマンドの **no** 形式を使用します。

policy *policy number*

no **policy**

構文の説明

policy number 1 ~ 10000 で、範囲の最低値が最も高いプライオリティを表します。

コマンド デフォルト

なし

コマンド モード

ISAKMP ポリシーセット コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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, write

例

次に、ルーティング ポリシーのプライオリティを設定する例を示します。

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

policy (ISAKMP ポリシーセット)

```
RP/0/RSP0/CPU0:router (config)# crypto isakmp policy-set p1
RP/0/RSP0/CPU0:router (config-isakmp-pol-set)# policy pol2
```

関連コマンド

コマンド	説明
description (ISAKMP ポリシーセット) , (182 ページ)	ISAKMP ポリシー セットを定義します。
crypto isakmp policy-set , (173 ページ)	ISAKMP 保護スイートのポリシーセットを定義します。
match identity (ISAKMP ポリシーセット) , (204 ページ)	SVI トンネル ソースを作成します。

pre-shared-key

IKE 認証用の事前共有キーを定義するには、キーリング コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

pre-shared-key {address *address* [*mask*] | hostname *hostname*} key *key*

no pre-shared-key {address *address* [*mask*] | hostname *hostname*} key *key*

構文の説明

address <i>address</i>	リモート ピアの IP アドレスまたはサブネットとマスクを指定します。
<i>mask</i>	(任意) <i>mask</i> 引数はアドレスの範囲と一致します。デフォルト値は 255.255.255.255 です。
hostname <i>hostname</i>	ピアの完全修飾ドメイン名 (FQDN) を指定します。
key <i>key</i>	事前共有キーを指定します。

コマンド デフォルト

なし

コマンド モード

キーリング コンフィギュレーション

コマンド履歴

リリース	変更箇所
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, write

例

次に、IP アドレスとホスト名を使用して事前共有キーを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key address 10.72.23.11 key vpnkey
RP/0/RSP0/CPU0:router(config-keyring)# pre-shared-key hostname www.vpn.com key vpnkey
```

関連コマンド

コマンド	説明
crypto isakmp identity , (163 ページ)	インターネットキー交換 (IKE) プロトコルへの参加時にルータが使用する識別情報を指定します。
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。

rsa-pubkey

IKE 認証時の暗号化またはシグニチャに使用される Rivest, Shamir, and Adelman (RSA) 手動キーを定義するには、キーリング コンフィギュレーション モードで **rsa-pubkey** 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。

rsa-pubkey {*address address*| *name fqdn*} [*encryption*| *signature*]

no rsa-pubkey {*address address*| *name fqdn*} [*encryption*| *signature*]

構文の説明

address <i>address</i>	リモート ピアの RSA 公開キーの IP アドレスを指定します。 <i>address</i> 引数は、手動で設定するリモート ピアのリモート RSA 公開キーの IP アドレスです。
name <i>fqdn</i>	ピアの完全修飾ドメイン名 (FQDN) を指定します。
encryption	(任意) 手動キーが暗号化に使用されるように指定します。
signature	(任意) 手動キーがシグニチャに使用されるように指定します。 signature キーワードがデフォルトです。

コマンド デフォルト

キーはシグニチャに使用されます。

コマンド モード

キーリング コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

公開キー コンフィギュレーション モードを開始するには、**rsa-pubkey** コマンドを使用します。他の IP Security (IPSec) ピアの RSA 公開キーを手動で指定する必要がある場合は、このコマンドを使用します。ピア ルータで IKE ポリシーの認証方式として RSA 暗号化ナンスを設定するときは、他のピアのキーを指定する必要があります。

RSA キーの指定が終了したら、**quit** と入力してグローバルコンフィギュレーションモードに戻る必要があります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、IPSec ピアの RSA 手動キーが指定されている例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto keyring vpnkeyring
RP/0/RSP0/CPU0:router(config-keyring)# rsa-pubkey name host.vpn.com
RP/0/RSP0/CPU0:router(config-pubkey)# key-string 005C300D 06092A86 4886F70D 01010105
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
quit
```

関連コマンド

コマンド	説明
address , (147 ページ)	手動で設定するリモート ピアの Rivest, Shamir, and Adelman (RSA) 公開キーの IP アドレスを指定します。
crypto keyring , (177 ページ)	IKE 認証時の暗号キーリングを定義します。
key-string (IKE) , (198 ページ)	リモート ピアの Rivest, Shamir, and Adelman (RSA) 公開キーを手動で指定します。

self-identity

ローカル IKE がリモート ピアに自身を識別させるために使用する識別情報を定義するには、ISAKMP プロファイル コンフィギュレーション モードで **self-identity** コマンドを使用します。IKE 用に定義された ISAKMP 識別情報を削除するには、このコマンドの **no** 形式を使用します。

```
self-identity {address| fqdn| user-fqdn user-fqdn}
```

```
no self-identity {address| fqdn| user-fqdn user-fqdn}
```

構文の説明

address	ローカル エンドポイントの IP アドレスを指定します。
fqdn	ホストの完全修飾ドメイン名 (FQDN) を指定します。
user-fqdn user-fqdn	リモート エンドポイントに送信されるユーザ FQDN を指定します。

コマンド デフォルト

ISAKMP 識別情報が ISAKMP プロファイル コンフィギュレーション に定義されていない場合、グローバル コンフィギュレーション がデフォルトになります。

コマンド モード

ISAKMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

self-identity コマンドが定義されていない場合、IKE はグローバルに設定された値を使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、IKE 識別情報がユーザ FQDN 「user@vpn.com」 である例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# self-identity user-fqdn user@vpn.com
```

関連コマンド

コマンド	説明
crypto isakmp profile, (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。

set interface tunnel-ipsec

ローカルが送信元または終端であるトラフィック用のトンネルモードIPSec サービスアソシエーション (SA) についてIKEがネゴシエートする際に、仮想インターフェイスインスタンスを事前定義するには、ISAKMP プロファイル照合コンフィギュレーションモードで **set interface tunnel-ipsec** 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。

set interface tunnel-ipsec *intf-index*

no set interface tunnel-ipsec *intf-index*

構文の説明

intf-index 仮想インターフェイス インデックスを指定します。範囲は 0 ~ 4294967295 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

ISAKMP プロファイル照合コンフィギュレーション

コマンド履歴

リリース	変更箇所
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。

インターフェイスは **set interface** コマンドを使用して事前定義する必要があります。そうしないと、IKE SA を確立できません。

ローカルエンドポイントが IKE の応答側である場合、定義済みのインターフェイスは、ピアの識別情報に応じて検索されます。ローカルエンドポイントが IKE の発信側である場合、定義済みのインターフェイスは、使用する適切な ISAKMP プロファイルを検索するために使用されます。したがって、複数の ISAKMP プロファイルには仮想インターフェイスを事前定義できません。



(注) **set interface tunnel-ipsec** コマンドは、ローカル ISAKMP プロファイルだけに使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、インターフェイス インスタンスを事前定義する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity group vpngroup
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set interface tunnel-ipsec 50
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。
match identity (ISAKMP ポリシーセット) , (204 ページ)	ISAKMP プロファイルのピアの ID を照合します。
set ipsec-profile , (219 ページ)	IPSec プロファイル インスタンスを事前定義します。

set ipsec-profile

ローカルが送信元または終端であるトラフィック用のトランスポートモードIPSec サービスアソシエーション (SA) についてIKEがネゴシエートする際に、プロファイルインスタンスを事前定義するには、プロファイル照合コンフィギュレーションモードで **set ipsec-profile** 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。

set ipsec-profile *profile-name*

no set ipsec-profile *profile-name*

構文の説明

profile-name IPsec プロファイルの名前です。

コマンド デフォルト

なし

コマンド モード

ISAKMP プロファイル照合コンフィギュレーション

コマンド履歴

リリース	変更箇所
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 プロファイルは、トランスポートモードIPSec SAのネゴシエーション時に **set ipsec-profile** または **set interface tunnel-ipsec** コマンドを使用して事前定義する必要があります。そうしないと、IKE SA を確立できません。

ローカルエンドポイントがIKEの応答側である場合、定義済みのインターフェイスは、ピアの識別情報に応じて検索されます。ローカルエンドポイントがIKEの発信側である場合、定義済みのインターフェイスは、使用する適切なISAKMPプロファイルを検索するために使用されます。したがって、複数のISAKMPプロファイルには仮想インターフェイスを事前定義できません。



(注) 識別情報のプロファイルは、選択された仮想インターフェイスに基づいて決定されます。ローカル ISAKMP プロファイルだけがサポートされるため、この場合は tunnel-ipsec だけです。

ローカル エンドポイントが IKE の発信側である場合、定義されたプロファイルまたはインターフェイスは、正しい ISAKMP プロファイルを選択するために使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、IPSec プロファイル インスタンスを事前定義する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto isakmp profile local vpnprofile
RP/0/RSP0/CPU0:router(config-isa-prof)# match identity group vpngroup
RP/0/RSP0/CPU0:router(config-isa-prof-match)# set ipsec-profile myprofile
```

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。
match identity (ISAKMP ポリシーセット) , (204 ページ)	ISAKMP プロファイルのピアの ID を照合します。
set interface tunnel-ipsec , (217 ページ)	ローカルを送信元または終端とするトラフィックのトンネルモード IPSec サービスアソシエーション (SA) について IKE がネゴシエートする際に、インターフェイスインスタンスを事前定義します。

show crypto isakmp call admission statistics

IKE プロトコルのコールアドミッション制御（CAC）統計情報をモニタするには、EXEC モードで **show crypto isakmp call admission statistics** コマンドを使用します。

show crypto isakmp call admission statistics

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	変更箇所
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 isakmp call admission statistics** コマンドの設定を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp call admission statistics
```

```
-----
Crypto Call Admission Control Statistics
-----
IKE Active SA Limit: 1, IKE In-Negotiation SA limit: 2
Total CPU usage limit: 100, IKE CPU usage limit: 100
Total IKE SA Count: 0, active: 0, negotiating: 0
Incoming IKE Calls: 24      , accepted 24      , rejected 0
Outgoing IKE Calls: 16      , accepted 6      , rejected 10
```

show crypto isakmp call admission statistics

Total Calls: 40
 Rejected IKE Calls: 10, resources low 0, limit exceeded 10
 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 10 : show crypto isakmp call admission statistics フィールドの説明

フィールド	説明
IKE Active SA Limit	デフォルト値の 0 には、制限がありません。
In-Negotiation SA limit	デフォルト値は 1000 です。
Total IKE SA Count	IKE SA の数。
active	アクティブな SA の数。
negotiating	ネゴシエートされる SA 要求の数。
Incoming IKE Calls	着信 IKE SA 要求の数。着信 IKE コール数は、受け入れられた要求と拒否された要求の合計と同じです。
accepted	受け入れられた着信または発信 IKE SA 要求の数。
rejected	拒否された着信または発信 IKE SA 要求の数。
Outgoing IKE Calls	発信 IKE SA 要求の数。発信 IKE コール数は、受け入れられた要求と拒否された要求の合計と同じです。
Total Calls	合計コール数は、着信 IKE コール数と発信 IKE コール数の合計と同じです。
Rejected IKE Calls	拒否された IKE 要求の数。拒否された IKE コール数は、リソース低下と制限超過の合計数と同じです。
resources low	システムリソースの低下、または事前設定されたシステムリソース制限の超過を理由に拒否された IKE 要求の数。
limit exceeded	SA 制限に達したために拒否された IKE SA 要求の数。

関連コマンド

コマンド	説明
clear crypto isakmp call admission statistics , (154 ページ)	ISAKMP コールアドミッション統計情報をクリアします。

show crypto isakmp errors

トンネルの確立時に発生した Internet Security Association and Key Management Protocol (ISAKMP) エラーを表示するには、EXEC モードで **show crypto isakmp errors** コマンドを使用します。

show crypto isakmp errors

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

変更箇所

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 isakmp errors** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp errors

Control Plane Errors
-----
ERR NO MEMORY.....0
INVALID CERT.....0
CRYPTO FAILURE.....0
SA NOT AUTH.....0
AUTHENTICATION FAILED.....0
GROUP AUTHOR FAILED.....0
USER AUTHEN REJECTED.....0
```

```

LOCAL ADDRESS FAILURE.....0
FAILED TO CREATE SKEYID.....0
RSA PUBLIC KEY NOT FOUND.....0
RETRANSMISSION LIMIT.....0
MALFORMED MESSAGE.....0
QUICK MODE TIMER EXPIRED.....0
KEY NOT FOUND IN PROFILE.....0
PROFILE NOT FOUND.....0
PRESHARED KEY NOT FOUND.....0
PHASE2 PROPOSAL NOT CHOSEN.....0
POLICY MISMATCH.....0
NO POLICY FOUND.....0
PACKET PROCESS FAILURE.....0

Warnings
-----
CERT DOESNT MATCH ID.....0
CERT ISNT TRUSTED ROOT.....0
PACKET NOT ENCRYPTED.....0
UNRELIABLE INFO MSG.....0
NO SA.....0
BAD DOI SA.....0
UNKNOWN EXCHANGE TYPE.....0
OUTGOING PKT TOO BIG.....0
INCOMING PKT TOO BIG.....0

Informational
-----
CAC DROPS.....0
DEFAULT POLICY ACCEPTED.....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 11 : *show crypto isakmp errors* フィールドの説明

フィールド	説明
ERR NO MEMORY	メモリ割り当ての失敗が発生し、そのプロセスを自動的に回復できませんでした。 正しく動作させるためには、プロセスを再開する必要があります。メモリが何度も枯渇する場合は、より大きなメモリ構成にアップグレードできます。
INVALID CERT	リモートピアから付与された証明書が失効または期限切れになったか（証明書が無効）、証明書のシグニチャチェックに失敗しました（不良なシグニチャ）。 リモートピアのCAに連絡し、考えられる不良なCA証明書を報告することを推奨します。
CRYPTO FAILURE	IKEは、暗号化または復号化サービスから返された失敗を検出しました。 リモートピアの管理者に連絡することを推奨します。

フィールド	説明
SA NOT AUTH	リモートピアとのIKEセキュリティアソシエーションが認証されませんでした。ピアはクイックモード交換の開始を試みました。交換は、認証されたセキュリティアソシエーションでだけ実行する必要があります。 ピアの管理者に連絡することを推奨します。
AUTHENTICATION FAILED	IKEプロセスはリモートピアとのセキュリティアソシエーションを認証できませんでした。 ピアの管理者に連絡することを推奨します。
GROUP AUTHOR FAILED	グループの許可が失敗しました。 AAAの接続を確認することを推奨します。
USER AUTHEN REJECTED	ピアとのフェーズ1.5 (Xauth) の処理が失敗しました。 配信されたパスワードがクライアントのものと一致していることを確認する必要があります。それでも解決しない場合は、受け取った正確なログメッセージを用意して Cisco Technical Support にお問い合わせください。
LOCAL ADDRESS FAILURE	クライアントへのIPアドレスの割り当てに失敗しました。 IPローカルプールが定義され、少なくとも1つのフリーアドレスが含まれていることを確認する必要があります。さらに、 show crypto isakmp profile コマンドから特定のプールが適切なISAKMPプロファイルに割り当てられていることを確認します。それでも解決しない場合は、受け取った正確なログメッセージを用意して Cisco Technical Support にお問い合わせください。
FAILED TO CREATE SKEYID	SKEYIDの生成に失敗しました。 Cisco Technical Support に連絡することを推奨します。
RSA PUBLIC KEY NOT FOUND	RSAキーの照会に失敗しました。 証明書の件名を確認できます。

フィールド	説明
RETRANSMISSION LIMIT	再送の制限を超えました。 管理者に連絡することを推奨します。
MALFORMED MESSAGE	受信したすべての ISAKMP メッセージには、すべてのコンポーネントのペイロードタイプが有効であり、個々の長さの合計が受信メッセージの合計長と等しいことを確認するために、簡単な健全性チェックが実行されます。このメッセージは健全性チェックに失敗しました。 連続した不良メッセージは Denial of Service (DoS; サービス拒絶) 攻撃を示す可能性があります。 ピアの管理者に連絡することを推奨します。
QUICK MODE TIMER EXPIRED	必ずしもクイック モードを開始してフェーズ 2 を開始するまで待機できるとは限りません。 ほとんどの場合、フェーズ 2 の開始に失敗する理由はプロセスがフェーズ I を完了できなかったからです。その場合は、このメッセージの直前に表示される別のメッセージがログに記録されている必要があります。
KEY NOT FOUND IN PROFILE	メイン モードでは、ID ペイロードは MM5 と MM6 でだけ交換されます。キーリング情報はネゴシエーションのより早い段階で必要となるので、ピアのアドレスに基づいて検索されます。選択されたキーリングがそのピア用に ISAKMP プロファイルに定義されたキーリングと一致しない場合に、このエラーが表示されます。 キーが存在するキーリングが ISAKMP プロファイルに対応付けられていることを確認する必要があります。

フィールド	説明
PROFILE NOT FOUND	<p>次の説明が表示されます。</p> <ul style="list-style-type: none"> • ピアの識別情報と一致する ISAKMP プロファイルが見つかりません。これは RESPONDER モードにだけ該当します。 • インターフェイス名と一致する ISAKMP プロファイルが見つかりません。これは INITIATOR モードにだけ該当します。 • ピアの識別情報がインターフェイスに関連付けられた ISAKMP プロファイルと一致しません。これは INITIATOR モードにだけ該当します。 <p>次の推奨事項が表示されます。</p> <ul style="list-style-type: none"> • ピアの ID と一致する ISAKMP プロファイルが存在することを確認する必要があります。 • ISAKMP プロファイルが適切なインターフェイスに対応付けられていることを確認する必要があります。 • インターフェイスに対応付けられている ISAKMP プロファイルが、ピアの識別情報と一致することを確認する必要があります。
PRESHARED KEY NOT FOUND	<p>事前共有キーの検出に失敗しました。 管理者に連絡することを推奨します。</p>
PHASE2 PROPOSAL NOT CHOSEN	<p>ピアとのフェーズ 2 パラメータのネゴシエーションが失敗しました。 ピアの管理者に連絡することを推奨します。</p>
POLICY MISMATCH	<p>ピアとのフェーズ 1 ポリシーパラメータのネゴシエーションが失敗しました。 ピアの管理者に連絡することを推奨します。</p>

フィールド	説明
NO POLICY FOUND	<p>次のどの方法でもピアのキーを取得できませんでした。</p> <ul style="list-style-type: none"> • 事前共有キー • RSA キー • 証明書 <p>管理者に連絡することを推奨します。</p>
PACKET PROCESS FAILURE	<p>このエラーメッセージは重大なエラー状態を示します。これは内部エラーに起因する可能性があります。</p> <p>Cisco Technical Support に連絡することを推奨します。</p>
CERT DOESNT MATCH ID	<p>識別情報が証明書から収集できる情報と一致しないことが示されました。</p> <p>セッションが開始されない場合は、リモートピアまたは管理者に連絡することができます。</p>
CERT ISNT TRUSTED ROOT	<p>IKE フェーズ I シグニチャの検証時に、発信側は CA 証明書のリストを送信します。この警告は、リストにある CA がいずれも信頼できるルートではない場合に、応答側によって出力されます。</p> <p>(注) 複数の cert-req ペイロードが存在する可能性があるため、これは必ずしもエラーとは限りません。</p> <p>セッションが開始されない場合は、リモートピアまたは管理者に連絡することができます。</p>
PACKET NOT ENCRYPTED	<p>受信パケットはピアによって暗号化されている必要がありますが、暗号化されませんでした。</p> <p>リモートピアの管理者に連絡することを推奨します。</p>
UNRELIABLE INFO MSG	<p>ピアが認証される前に INFO メッセージを受信したことが、信頼できないと判断される理由です。</p> <p>リモートピアの管理者に連絡することを推奨します。</p>

フィールド	説明
NO SA	<p>このパケット用のセキュリティアソシエーションが存在しません。これは SA を確立するピアからの初期オファーではありません。これらのエラーはサービス拒絶攻撃を示す可能性があります。</p> <p>リモートピアまたは管理者に連絡することを推奨します。</p>
BAD DOI SA	<p>SA オファーにはメッセージ解析のために DOI フィールドが必要です。DOI が不明の SA オファーは解析できません。</p> <p>この状況が続く場合は、リモートピアの管理者に連絡できます。</p>
UNKNOWN EXCHANGE TYPE	<p>IKE は、定義された交換に基づいてメッセージに関するアクションを実行します。不明な交換でメッセージが受信されています。</p> <p>問題が一時的なものではないと思われる場合は、ピアの管理者に連絡できます。</p>
OUTGOING PKT TOO BIG	<p>最大許容 UDP パケットサイズを上回る ISAKMP パケットを送信しようとしています。これは極めて多数の IKE ポリシーが発信側から提示されていた場合に発生する可能性があります。</p> <p>設定された ISAKMP ポリシーの数を減らすことを試みることができます。</p>
INCOMING PKT TOO BIG	<p>パケットサイズは 3,000 に制限されています。ピアが大きな情報を送信すると、強制的に大きなバッファの割り当てが必要となります (サービス拒絶 (DoS) など)。</p> <p>リモートピアまたは管理者に連絡することを推奨します。</p>

フィールド	説明
CAC DROPS	<p>コールアドミッション制御 (CAC) ポリシーがデバイスに設定されています。その結果、エラーメッセージに記載された理由で IKE SA 要求が拒否されました。</p> <p>要求が拒否された理由に応じて、システムへの負荷を減らして新しい IKE SA 要求を処理できるようにするか、さらに必要な場合は最大許容 IKE セッションを増やすことができます。</p>
DEFAULT POLICY ACCEPTED	<p>ローカルに設定されたポリシーがピアのポリシーと一致しなかったため、デフォルトポリシーが使用されています。</p> <p>これが実際に使用すべき ISAKMP ポリシーであるかどうかを確認できます。デフォルトポリシーを使用しないようにするには、ピアのポリシーと一致するようにローカルポリシーを再設定することができます。</p>

関連コマンド

コマンド	説明
clear crypto isakmp errors	ISAKMP エラーの統計情報をクリアします。

show crypto isakmp key

ルータの Internet Security Association and Key Management Protocol (ISAKMP) 事前共有キーを表示するには、EXEC モードで **show crypto isakmp key** コマンドを使用します。

show crypto isakmp key

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

変更箇所

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、IP ホスト名およびアドレスと事前共有キーを表示する例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp key
```

```
Keyring      Hostname/Address  Preshared Key
K1           3.3.3.1          rd26
K2           5.5.5.5          ex22
K2           tzvi.cisco.com   ppp
```

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 12 : *show crypto isakmp key* フィールドの説明

フィールド	説明
Hostname/Address	ルータの IP ホスト名またはアドレス
Preshared Key	ルータの ISAKMP 事前共有キー

show crypto isakmp peers

ピアの構造を表示するには、EXEC モードで **show crypto isakmp peers** コマンドを使用します。

show crypto isakmp peers [*ip-address*] **vrf** *vrf-name*]

構文の説明

<i>ip-address</i>	(任意) ピアの IP アドレス。
vrf <i>vrf-name</i>	(任意) ピアの前面扉 VRF を指定します。 <i>vrf-name</i> 引数は、VRF に割り当てる名前です。

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	変更箇所
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 isakmp peers** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp peers
Peer: 10.0.83.1   Port: 4500   Local: 30.0.0.4   vrf: default
  UDP encapsulate: True
  SA information:
```

```

Connection ID: 1
State: QM_IDLE
Phase 1 ID: DER_ASN1_DN srbu

```

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 crypto isakmp peers* フィールドの説明

フィールド	説明
Connection ID	インターネットキー交換 (IKE) ID。
State	さまざまな状態の出力表示。各状態の詳細については、 表 17: モードの状態 (242 ページ) を参照してください。
Phase1 ID	インターネットキー交換 (IKE) ID。

関連コマンド

コマンド	説明
crypto isakmp peer , (168 ページ)	インターネットキー交換 (IKE) 用に IP セキュリティ (IPSec) ピアをイネーブルにします。
description (ISAKMP ピア) , (184 ページ)	インターネットキー交換 (IKE) ピアの説明を追加します。
show crypto session , (251 ページ)	アクティブな暗号セッションのステータス情報を表示します。

show crypto isakmp policy

各インターネットキー交換 (IKE) ポリシーのパラメータを表示するには、EXEC モードで **show crypto isakmp policy** コマンドを使用します。

show crypto isakmp policy

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

変更箇所

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、2 つの IKE ポリシー (プライオリティはそれぞれ 15 および 20) を設定したあとの **show crypto isakmp policy** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp policy

Protection suite priority 15
  encryption algorithm: DES - Data Encryption Standard (56 bit keys)
  hash algorithm: Message Digest 5
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime: 5000 seconds, no volume limit
Protection suite priority 20
```

```

encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: preshared Key
Diffie-Hellman Group: #1 (768 bit)
lifetime: 10000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys)
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman Group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit

```



(注) 出力ではライフタイムに「no volume limit」と表示されていますが、現在設定できるのは、時限ライフタイム（86,400秒など）だけです。ボリューム制限によるライフタイムは設定できません。

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 crypto isakmp policy フィールドの説明

フィールド	説明
encryption algorithm	IKE ポリシー内の暗号化アルゴリズム
hash algorithm	IKE ポリシー内のハッシュ アルゴリズム
authentication method	IKE ポリシーで使用される認証方式
Diffie-Hellman group	IKE ポリシーの Diffie-Hellman グループ ID
lifetime	期限切れになるまでにセキュリティアソシエーション (SA) が存在する時間 (秒単位)

関連コマンド

コマンド	説明
authentication (IKE ポリシー) , (149 ページ)	IKE ポリシー内の認証方式を指定します。
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
encryption (IKE ポリシー) , (188 ページ)	IKE ポリシー内の暗号化アルゴリズムを指定します。
group (IKE ポリシー) , (190 ページ)	IKE ポリシー内部での Diffie-Hellman グループの識別番号を指定します。
hash (IKE ポリシー) , (192 ページ)	IKE ポリシー内のハッシュアルゴリズムを指定します。

show crypto isakmp policy

コマンド	説明
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。

show crypto isakmp profile

ルータに定義されているすべての ISAKMP プロファイルを表示するには、EXEC モードで **show crypto isakmp profile** コマンドを使用します。

show crypto isakmp profile [**interface** *intf-name* | **ipsec-profile** *ipsec-prof-name* | **tag** *isakmp-prof-name*]

構文の説明

interface <i>intf-name</i>	(任意) IPsec 照合 ID のインターフェイスごとに ISAKMP プロファイルを表示します。
ipsec-profile <i>ipsec-prof-name</i>	(任意) IPsec 照合 ID の IPsec プロファイルごとに ISAKMP プロファイルを表示します。
tag <i>isakmp-prof-name</i>	(任意) 名前ごとに ISAKMP プロファイルを表示します。

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	変更箇所
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 isakmp profile** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp profile

ISAKMP Profile: isakmp-prof2
  Keyring(s): kr2
  Identities matched are:
    Address: 10.0.2.1 255.255.255.255 fvrf: green
    Interface: service-ipsec2

ISAKMP Profile: isakmp-prof1
  Keyring(s): kr1
  Identities matched are:
    Group: srbu
    Interface: service-grel
```

次の表に、**show crypto isakmp profile** コマンドのフィールドを示します。

表 15 : **show crypto isakmp profile** フィールドの説明

フィールド	説明
ISAKMP Profile	ISAKMP プロファイルの名前。
Keyring(s)	キーリングの名前です。これはグローバルコンフィギュレーションで定義されたキーリング名と一致する必要があります。
Identities matched are	ISAKMP プロファイルで照合できるすべての識別情報です。

関連コマンド

コマンド	説明
crypto isakmp profile , (175 ページ)	ISAKMP プロファイルを定義し、IPSec ユーザセッションを監査します。
keyring , (196 ページ)	ISAKMP プロファイルとともにキーリングを定義します。

show crypto isakmp sa

ピアにおける現在のすべてのインターネットキー交換（IKE）セキュリティ アソシエーション（SA）を表示するには、EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [*connection ID*]

構文の説明

connection ID (任意) IKE SA ID です。有効な範囲は 1 ～ 65535 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	変更箇所
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。

ID のリストを表示するには、*connection ID* 引数を使用します。

タスク ID

タスク ID	操作
crypto	read

例

次に、IKE ネゴシエーションが 2 つのピア間で正常に完了したあとの **show crypto isakmp sa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto isakmp sa vrf
dst src state conn-id nodeid -----
-----
----- default 30.0.0.4 10.0.83.1 QM_IDLE 1 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 16 : show crypto isakmp sa フィールドの説明

フィールド	説明
vrf	VRF ごとの ISAKMP SA 詳細を表示するための Virtual Route Forwarding (VRF; 仮想ルート転送)。
dst	宛先の IP アドレス。
src	発信元の IP アドレス。
conn-id	接続 ID。
nodeid	ノード ID。

次の表に、show crypto isakmp sa コマンドの出力に表示される可能性のあるさまざまな状態を示します。Internet Security Association and Key Management Protocol (ISAKMP) SA が存在するときは、ほとんどの場合、休止状態 (QM_IDLE) です。長い交換の間に、いくつかの MM_xxx 状態が観察される可能性があります。

表 17 : モードの状態

状態 : メイン モード交換	説明
MM_NO_STATE	ISAKMP SA は作成済みですが、他にはまだ何も発生していません。この段階では「仮性」で、状態はありません。
MM_SA_SETUP	ピアは ISAKMP SA のパラメータに同意しました。
MM_KEY_EXCH	ピアは Diffie-Hellman 公開キーを交換して共有秘密を生成しました。ISAKMP SA は認証されていないままです。
MM_KEY_AUTH	ISAKMP SA は認証済みです。ルータがこの交換を開始した場合、この状態はすぐに QM_IDLE に移行し、クイック モード交換が開始されます。
状態 : アグレッシブ モード交換	説明

状態：メインモード交換	説明
AG_NO_STATE	ISAKMP SA は作成済みですが、他にはまだ何も発生していません。この段階では「仮性」で、状態はありません。
AG_INIT_EXCH	ピアはアグレッシブモードで最初の交換を実行しましたが、SA は認証されていません。
AG_AUTH	ISAKMP SA は認証済みです。ルータがこの交換を開始した場合、この状態はすぐにQM_IDLE に移行し、クイックモード交換が開始されます。
状態：クイックモード交換	説明
QM_IDLE	ISAKMP SA はアイドル状態です。Iピアとは認証されたままですが、後続のクイックモード交換用に使用される可能性があります。休止状態です。

関連コマンド

コマンド	説明
crypto isakmp policy , (170 ページ)	IKE ポリシーを定義します。
lifetime (IKE ポリシー) , (200 ページ)	IKE SA のライフタイムを指定します。
show crypto isakmp stats , (244 ページ)	ISAKMPセキュリティアソシエーション (SA) の数を表示します。
show crypto isakmp stats , (244 ページ)	ISAKMPセキュリティアソシエーション (SA) の詳細を表示します。

show crypto isakmp stats

ISAKMP のグローバル統計情報を表示するには、EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats [*vrf vrf-name*]

構文の説明

vrf vrf-name (任意) VPNルーティングおよび転送 (VRF) インスタンスごとの ISAKMP 統計情報を指定します。 *vrf-name* 引数は、VRF に割り当てる名前です。

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	変更箇所
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 インスタンスごとの ISAKMP 統計情報を表示するには、**show crypto isakmp stats** コマンドを使用します。VRF インスタンスが指定されない場合は、VRF インスタンスの統計情報デフォルトが表示されます。

show crypto isakmp stats コマンドにより、次のグローバル統計情報が出力されます。

- アクティブな ISAKMP SA
- 現在ネゴシエーション中の ISAKMP
- 同時 ISAKMP SA の最大数
- 同時に確立される SA の最大数
- 期限切れになった SA の数

タスク ID

タスク ID	操作
crypto	read

例

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

```
RP/0/RSP0/CPU0:router# show crypto isakmp stats
VRF ISAKMP statistics:
    Active Tunnels:                0
    Previous Tunnels:              0
    In Octets:                     0
    In Packets:                   0
    In Drop Packets:               0
    In Notifys Messages:          0
    In Phase2 Exchanges:          0
    In Phase2 Exchange Invalids:  0
    In Phase2 Exchange Rejects:   0
    In Phase2 SA Delete Requests: 0
    Out Octets:                   0
    Out Packets:                  0
    Out Drop Packets:             0
    Out Notifys Messages:         0
    Out Phase2 Exchanges:         0
    Out Phase2 Exchange Invalids: 0
    Out Phase2 Exchange Rejects:  0
    Out Phase2 SA Delete Requests: 0
    Initiator Tunnels:            0
    Initiator Tunnel Setup Fails: 0
    Responder Tunnel Setup Fails: 0
    Sys Cap Fails:                0
    Auth Failures:                0
    Decryption Fails:             0
    Hash Valid Fails:             0
    No SA Fails:                  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 18 : **show crypto isakmp stats** フィールドの説明

フィールド	説明
Active Tunnels	現在アクティブな IPSec フェーズ 1 IKE トンネルの数
Previous Tunnels	以前にアクティブだった IPSec フェーズ 1 IKE トンネルの合計数
In Octets	現在アクティブおよび以前にアクティブだったすべての IPSec フェーズ 1 IKE トンネルが受信した合計オクテット数

フィールド	説明
In Packets	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが受信した合計パケット数
In Phase2 Exchanges	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが受信した IPsec フェーズ 2 交換の合計数
In Phase2 Exchange Invalids	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが受信し、無効であることを検出した IPsec フェーズ 2 交換の合計数
In Phase2 Exchange Rejects	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが受信し、拒否した IPsec フェーズ 2 交換の合計数
In Phase2 SA Delete Requests	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが受信した、IPsec フェーズ 2 セキュリティアソシエーションの削除要求の合計数
Out Octets	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信した合計オクテット数
Out Packets	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 トンネルが送信した合計パケット数
Out Drop Packets	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信処理中にドロップしたパケットの合計数
Out Notifys Messages	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信した通知の合計数
Out Phase2 Exchanges	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信した IPsec フェーズ 2 交換の合計数

フィールド	説明
Out Phase2 Exchange Invalids	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 トンネルが送信し、無効であることを検出した IPsec フェーズ 2 交換の合計数
Out Phase2 Exchange Rejects	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信し、拒否した IPsec フェーズ 2 交換の合計数
Out Phase2 SA Delete Requests	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルが送信した、IPsec フェーズ 2 SA の削除要求の合計数
Initiator Tunnels	ローカルで開始された IPsec フェーズ 1 IKE トンネルの合計数
Initiator Tunnel Setup Fails	ローカルで開始され、アクティブにされなかった IPsec フェーズ 1 IKE トンネルの合計数
Responder Tunnel Setup Fails	リモートで開始され、アクティブにされなかった IPsec フェーズ 1 IKE トンネルの合計数
Sys Cap Fails	現在アクティブおよび以前にアクティブだったすべての IPsec フェーズ 1 IKE トンネルの処理中に発生した、システムキャパシティ障害の合計数
Auth Failures	現在および以前のすべての IPsec フェーズ 1 IKE トンネルが失敗した認証の合計数
Decryption Fails	現在および以前のすべての IPsec フェーズ 1 IKE トンネルが失敗した復号化の合計数
Hash Valid Fails	現在および以前のすべての IPsec フェーズ 1 IKE トンネルが失敗したハッシュ検証の合計数
No SA Fails	現在および以前のすべての IPsec フェーズ 1 IKE トンネルの処理中に発生した、存在しないセキュリティ アソシエーションの障害の合計数

show crypto key pubkey-chain rsa

ルータに保存されているピアの Rivest, Shamir, and Adelman (RSA) 公開キーを表示するには、EXEC モードで **show crypto key pubkey-chain rsa** コマンドを使用します。

show crypto key pubkey-chain rsa [*name key-name* | *address key-address*]

構文の説明

name <i>key-name</i>	(任意) 特定の公開キーの名前を表示します。
address <i>key-address</i>	(任意) 特定の公開キーのアドレスを表示します。

コマンド デフォルト

ルータに保存されているすべての RSA 公開キーが表示されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
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 RSA 公開キーを表示するには、このコマンドを使用します。表示には、ルータで手動で設定されたピアの RSA 公開キー、および他の手段によって（認証局サポートが設定されている場合は、証明書によってなど）ルータで受信されたキーが含まれます。

ルータを再起動した場合、証明書によって取得された公開キーは失われます。ルータが再度証明書を要求し、その際に公開キーが再度取得されるためです。

ルータに保存されている特定の RSA 公開キーの詳細を表示するには、**name** または **address** キーワードを使用します。

キーワードを指定しない場合、このコマンドではルータに保存されているすべての RSA 公開キーのリストが表示されます。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto key pubkey-chain rsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa
Codes: M - Manually Configured, C - Extracted from certificate
```

```
Code Usage      IP-Address      VRF              Keyring          Name
M   Encrypt
M   Signing      5.5.5.5         green            K2               example.cisco.com
```

次に、手動で設定された、**somerouter** という名前のピアの専用 RSA 公開キーの例を示します。この例には、ピア証明書から取得した 3 つのキー（peer routerA 用の 2 つの専用キーと peer routerB 用の 1 つの汎用キー）も示されています。

例では証明書サポートが使用されています。証明書サポートが使用されていない場合、どのピアのキーも Code 列に「C」と表示されず、すべて手動で設定されることが必要になります。

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 crypto key pubkey-chain rsa** フィールドの説明

フィールド	説明
Code	ルータ上で手動で設定された RSA 公開キー（M）と、証明書などの他の手段によってルータで受信されたキー（C）。
Usage	生成された RSA キーのタイプ。
IP-address	RSA キーが設定されているローカルまたはリモートピアの IP アドレス。
VRF	キーリングの仮想ルート転送（VRF）。
Keyring	暗号キーリングの名前。グローバルキーはデフォルトのキーリングに表示されます。
Name	ローカルまたはリモートピアの名前。

次に、**name** キーワードで公開キーに somerouter.example.com という名前を付けている、**show crypto key pubkey-chain rsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa name somerouter.example.com

Key name: somerouter.example.com
Key address: 10.0.0.1
Usage: Signature Key
Source: Manual
Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 10.0.0.1
Usage: Encryption Key
Source: Manual
Data:
 00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```



(注) 例の **Source** フィールドに表示されている「**Manual**」は、キーがピアからの証明書で受信したものではなく、ルータ上で手動で設定されたものであることを意味します。

次に、アドレス 192.168.10.3 の **show crypto key pubkey-chain rsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key pubkey-chain rsa address 192.168.10.3

Key name: routerB.example.com
Key address: 192.168.10.3
Usage: General Purpose Key
Source: Certificate
Data:
 0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
 58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
 0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

例の **Source** フィールドに表示されている「**Certificate**」は、キーが他方のルータからの証明書を受けてルータで受信したものであることを意味します。

show crypto session

アクティブな暗号化セッションのステータス情報を表示するには、EXEC モードで **show crypto session** コマンドを使用します。

show crypto session [**detail**] **fvr**f **fvr**f-name [**detail**] | **group** **group** name | **groups** | **interface** **interface**-name | **ivrf** **ivrf**-name | **local** IP address [**fvr**f **fvr**f-name | **detail**] | **profile** **profile** name [**detail**] | **remote** IP-address [**detail**] | **port** **remote**-port | **fvr**f **fvr**f-name | **user** **username** [**detail**] | **users**]

構文の説明

detail	(任意) セッションに関するより詳細な情報を表示します。たとえば、インターネットキー交換 (IKE) セキュリアソシエーション (SA) の機能、接続 ID、IKE SA の残りのライフタイム、IP セキュリティ (IPSec) フローの着信または発信の暗号化または復号化パケット数、ドロップされたパケットの数、IPSec SA のライフタイム (キロバイト/秒単位) などが含まれます。
fvr f fvr f-name	(任意) 前面扉仮想ルーティングおよび転送 (FVRF) セッションのステータス情報を表示します。 <i>fvr</i> f-name 引数は、FVRF に割り当てられた名前です。
group group name	(任意) バーチャルプライベートネットワーク (VPN) デバイスで現在アクティブなグループの識別名の使用状況を表示します。 <i>group</i> name 引数は、グループの識別名です。
groups	(任意) バーチャルプライベートネットワーク (VPN) デバイスで現在アクティブなすべての接続グループの使用状況を表示します。
interface interface -name	<ul style="list-style-type: none"> • Cisco ASR 9000 シリーズルータではサービスが動作しません。デフォルトのインターフェイスは tunnel-ipsec です。または IPSec トンネル サービス インターフェイスを指定します。
ivrf ivrf -name	(任意) 内部 VRF (IVRF) セッションのステータス情報を表示します。 <i>ivrf</i> -name 引数は、内部 VRF の名前です。
local IP address	(任意) ローカル暗号化エンドポイントの暗号化セッションに関するステータス情報を表示します。 <i>IP</i> -address 引数は、ローカル暗号化エンドポイントの IP アドレスです。
profile profile name	(任意) ルータに定義されている Internet Security Association and Key Management Protocol (ISAKMP) プロファイルを表示します。 <i>profile</i> name 引数は、ISAKMP プロファイルの名前です。

remote IP address	(任意) リモートセッションの暗号化セッションに関するステータス情報を表示します。 <i>IP address</i> 引数は、リモート暗号化エンドポイントの IP アドレスです。
port remote-port	(任意) リモート暗号化エンドポイントの暗号化セッションに関するステータス情報を表示します。 <i>remote-port</i> 引数は 1 ~ 65535 です。 デフォルト値は 500 です。
user username	(任意) 接続ユーザの使用状況を表示します。 <i>user name</i> 引数は、ユーザの名前です。
users	(任意) すべての接続ユーザの使用状況を表示します。

コマンド デフォルト

キーワードを指定しないで **show crypto session** コマンドを入力した場合は、既存のすべてのセッションがクリアされます。 ポートのデフォルト値は 500 です。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
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可能性がある場合は、AAA 管理者にお問い合わせください。

show crypto session コマンドを使用して、すべてのアクティブな ISAKMP セッションと、各セッションの IKE および IPSec SA のリストを取得できます。 次のリストが含まれます。

- Interface
- IPSec SA を作成したピアに関連付けられた IKE SA
- セッションのフローにサービスを提供する IPSec SA

(同じセッションの) 同じピアには、複数の IKE または IPSec SA が確立されます。 その場合、IKE ピアの説明は、ピアと関連付けられている IKE SA と、セッションのフローのサービスを提供している IPSec SA 用に、異なる値で繰り返されます。

タスク ID

タスク ID	操作
crypto	read

例 次に、**show crypto session** コマンドのフィールドリストの例を示します。

```
RP/0/RSP0/CPU0:router# show crypto session

Interface:      service-ipsec1
Profile:        prof1
ISAKMP policy:  10
Fvrf:          default
Ivrf:          default
Peer:          21.21.21.21/500
Ike SAs:        1
  IKE SA : conn-id 1 local 100.100.100.1/500 remote 21.21.21.21/500  QM_IDLE

Interface:      service-ipsec4
Username:       cisco
InterfaceProfile:  tunnel-ipsec3001ezvpnIke
ProfileGroup:   TUNNEL_IPSECgroup-a
Assigned address: 10.0.0.1
ISAKMP policy: 1020
Fvrf:          default
Ivrf:          default
Peer:          10192.1168.110.52/500
Ike SAs:        1
IPsec FlowsSAs: 1
  IKE SA : conn-id 1 2 local 10135.135.1135.1.6/500 remote 10192.1168.110.52/500  QM_IDLE
  IPSEC FLOW 1510: permit ipv4 100.70.2080.20/2550.2550.2550.255 0
10.70.2080.21/255.255.255.255
  Active SAs 2
```

次に、セッションの詳細情報の例を示します。

```
Interface:      tunnelservice-ipsec3001gre1
Profile:        TUNNEL_IPSECisakmp-prof1
ISAKMP policy: 10
Fvrf:          default
Ivrf:          default
Peer:          1040.140.140.62/500
Ike SAs:        1
IPsec FlowsSAs: 1
  IKE SA : conn-id 2 1 local 1050.150.150.52/500 remote 1040.140.140.62/500  QM_IDLE
  IPSEC FLOW 2501: permit ipv4 10gre 50.750.20850.2/255.255.255.255
1040.740.20840.2/255.255.255.255
  Active SAs 2
  Inbound: #pkts dec'ed 5 0 drop 0 life (KB/Sec) 10000000099354592/32492414
  Outbound: #pkts encdec'ed 5 655653 drop 0 life (KB/Sec) 10000000099354592/32492414
```

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 crypto session** フィールドの説明

フィールド	説明
Interface	暗号化セッションが関連付けられるインターフェイス。

show crypto session

フィールド	説明
IKE SA	IKE SA についての情報が提供されます。たとえば、ローカルおよびリモートアドレスおよびポート、SA のステータス、SA の機能、暗号化エンジンの接続 ID、IKE SA の残りのライフタイムなどが含まれます。
IPSEC FLOW	IPSec で保護されたトラフィック フローに関する情報のスナップショット。たとえば、フローの内容、存在する IPSec SA の数、SA の送信元、暗号化または復号化パケットまたはドロップパケットの数、IPSec SA の残りのライフタイム (キロバイト/秒単位) などが含まれます。

関連コマンド

コマンド	説明
clear crypto session , (158 ページ)	暗号化セッション (IP セキュリティ [IPSec] およびインターネットキー交換 [IKE] セキュリティ アソシエーション [SA]) を削除します。
description (ISAKMP ピア), (184 ページ)	インターネットキー交換 (IKE) ピアの説明を追加します。
show crypto isakmp peers , (234 ページ)	ピアの構造を表示します。



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, 256 ページ](#)
- [accept-tolerance, 258 ページ](#)
- [cryptographic-algorithm, 260 ページ](#)
- [key \(キーチェーン\), 262 ページ](#)
- [key chain \(キーチェーン\), 264 ページ](#)
- [key-string \(キーチェーン\), 266 ページ](#)
- [send-lifetime, 268 ページ](#)
- [show key chain, 270 ページ](#)

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

<i>start-time</i>	キーが有効になる開始時間を <i>hh:mm:ss</i> 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 <i>duration value</i>	(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。
<i>end-time</i>	(任意) キーが期限切れとなる時刻を <i>hh:mm:ss</i> 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	変更箇所
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) , (262 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) , (264 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) , (266 ページ)	キー文字列のテキストを指定します。
send-lifetime , (268 ページ)	有効なキーを送信します。
show key chain , (270 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

<i>value</i>	(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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
key chain (キーチェーン), (264 ページ)	キーチェーンを作成または変更します。
show key chain , (270 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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
key chain (キーチェーン), (264 ページ)	キーチェーンを作成または変更します。
show key chain , (270 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	変更箇所
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せん。

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 , (256 ページ)	有効なキーを受け入れます。
key chain (キーチェーン), (264 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), (266 ページ)	キー文字列のテキストを指定します。
send-lifetime , (268 ページ)	有効なキーを送信します。
show key chain , (270 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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
accept-tolerance , (258 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), (262 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), (266 ページ)	キー文字列のテキストを指定します。
send-lifetime , (268 ページ)	有効なキーを送信します。
show key chain , (270 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。
<i>key-string-text</i>	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。 <ul style="list-style-type: none"> 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	変更箇所
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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
key (キーチェーン), (262 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), (264 ページ)	キーチェーンを作成または変更します。
send-lifetime , (268 ページ)	有効なキーを送信します。
show key chain , (270 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

<i>start-time</i>	キーが有効になる開始時間を <i>hh:mm:ss</i> 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 <i>duration value</i>	(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。
<i>end-time</i>	(任意) キーが期限切れとなる時刻を <i>hh:mm:ss</i> 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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
key (キーチェーン), (262 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), (264 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), (266 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	変更箇所
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 , (256 ページ)	有効なキーを受け入れます。
accept-tolerance , (258 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。
cryptographic-algorithm , (260 ページ)	暗号化アルゴリズムを選択します。
key (キーチェーン), (262 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), (264 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), (266 ページ)	キー文字列のテキストを指定します。
send-lifetime , (268 ページ)	有効なキーを送信します。

■ `show key chain`



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 Router Software*」設定モジュールを参照してください。

- [lawful-intercept disable](#), 274 ページ

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

変更箇所

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、すべてのメディア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

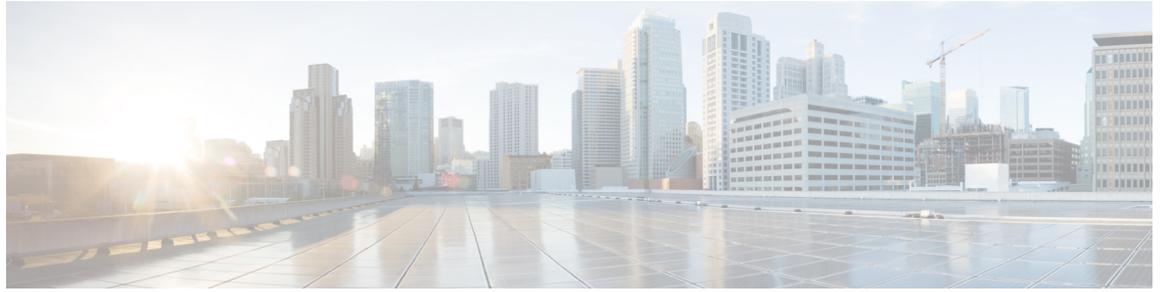
li

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 \(MPP\)](#) , 276 ページ
- [address ipv6 \(MPP\)](#) , 279 ページ
- [allow](#), 281 ページ
- [control-plane](#), 284 ページ
- [inband](#), 286 ページ
- [interface \(MPP\)](#) , 288 ページ
- [management-plane](#), 291 ページ
- [out-of-band](#), 293 ページ
- [show mgmt-plane](#), 295 ページ
- [vrf \(MPP\)](#) , 298 ページ

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

<i>peer-ip-address</i>	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。
<i>peer ip-address/length</i>	ピア IPv4 アドレスのプレフィックス。 <ul style="list-style-type: none"> • IPv4 : <i>A.B.C.D./length</i> • IPv6 : <i>X.X:X.X</i>

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	変更箇所
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) , (279 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 , (281 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 , (284 ページ)	コントロールプレーンを設定します。
inband , (286 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) , (288 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 , (291 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 , (293 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 , (295 ページ)	管理プレーンを表示します。

■ address ipv4 (MPP)

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

<i>peer-ip-address</i>	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。
<i>peer ip-address/length</i>	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	変更箇所
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) , (276 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 , (281 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 , (284 ページ)	コントロールプレーンを設定します。
inband , (286 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) , (288 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 , (291 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 , (293 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 , (295 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

<i>protocol</i>	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。 <ul style="list-style-type: none"> • 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ネイバー 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	変更箇所
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 , (284 ページ)	コントロールプレーンを設定します。
inband , (286 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) , (288 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 , (291 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 , (293 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 , (295 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

変更箇所

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, (291 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

変更箇所

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 , (284 ページ)	コントロールプレーンを設定します。
interface (MPP) , (288 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 , (291 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 , (293 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 , (295 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

<i>type</i>	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。
<i>interface-path-id</i>	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 (?) オンライン ヘルプ機能を使用します。
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	変更箇所
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 , (281 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 , (284 ページ)	コントロールプレーンを設定します。
inband , (286 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 , (291 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 , (293 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 , (295 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	変更箇所
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	変更箇所
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 , (284 ページ)	コントロールプレーンを設定します。
inband , (286 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) , (288 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 , (291 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 , (295 ページ)	管理プレーンを表示します。
vrf (MPP) , (298 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 (?) オンライン ヘルプ機能を使用します。
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	変更箇所
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 , (291 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

<i>vrf-name</i>	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	変更箇所
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 , (284 ページ)	コントロールプレーンを設定します。
interface (MPP) , (288 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 , (291 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 , (293 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 , (295 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, 303 ページ](#)
- [clear crypto ca crt, 305 ページ](#)
- [crl optional \(トラストポイント\), 307 ページ](#)
- [crypto ca authenticate, 309 ページ](#)
- [crypto ca cancel-enroll, 311 ページ](#)
- [crypto ca enroll, 313 ページ](#)
- [crypto ca import, 315 ページ](#)
- [crypto ca trustpoint, 317 ページ](#)
- [crypto key generate dsa, 320 ページ](#)
- [crypto key generate rsa, 322 ページ](#)
- [crypto key import authentication rsa, 324 ページ](#)
- [crypto key zeroize dsa, 326 ページ](#)
- [crypto key zeroize rsa, 328 ページ](#)
- [description \(トラストポイント\), 330 ページ](#)
- [enrollment retry count, 332 ページ](#)
- [enrollment retry period, 334 ページ](#)
- [enrollment terminal, 336 ページ](#)
- [enrollment url, 338 ページ](#)

- [ip-address \(トラストポイント\)](#) , 340 ページ
- [query url](#) , 342 ページ
- [rsakeypair](#) , 344 ページ
- [serial-number \(トラストポイント\)](#) , 346 ページ
- [sftp-password \(トラストポイント\)](#) , 348 ページ
- [sftp-username \(トラストポイント\)](#) , 350 ページ
- [subject-name \(トラストポイント\)](#) , 352 ページ
- [show crypto ca certificates](#) , 354 ページ
- [show crypto ca crls](#) , 356 ページ
- [show crypto key mypubkey dsa](#) , 358 ページ
- [show crypto key mypubkey rsa](#) , 360 ページ

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	変更箇所
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	実行

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
```

clear crypto ca crt

```
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 crt
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, (356 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、それをチェックする必要があります。

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	変更箇所
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 がい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, (317 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, (332 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, (334 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, (338 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

<i>ca-name</i>	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	変更箇所
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	実行

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, (317 ページ)	信頼できるポイントを選択した名前を設定します。
show crypto ca certificates, (354 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	変更箇所
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](#), (344 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](#), (344 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	実行

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 , (313 ページ)	CA からルータの証明書を取得します。
rsa keypair , (344 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	変更箇所
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**, (344 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**, (344 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	実行

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, (317 ページ)	信頼できるポイントを選択した名前を設定します。
rsaakeypair, (344 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](#), (317 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	変更箇所
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	実行

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, (317 ページ)	信頼できるポイントを選択した名前を設定します。
show crypto ca certificates, (354 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 **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

<i>ca-name</i>	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	変更箇所
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、選択した名前で作成された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) , (307 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](#) , (332 ページ) コマンド : ルータによって送信される、証明書要求のトライ回数 オプション

- [enrollment retry period](#), (334 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](#), (336 ページ) コマンド: ルータと認証局 (CA) 間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](#), (338 ページ) コマンド: (任意) CA の URL。
- [ip-address](#) (トラストポイント), (340 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](#), (342 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。「Idap://」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。
- [rsaakeypair](#), (344 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), (346 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), (348 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), (350 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), (352 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	実行

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)# rsaakeypair label-2
```

関連コマンド

コマンド	説明
crl optional (トラストポイント), (307 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 , (332 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 , (334 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 , (336 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 , (338 ページ)	CA の URL を指定します。
query url , (342 ページ)	CRL 分散ポイントの LDAP の URL を指定します。
rsa keypair , (344 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), (348 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), (350 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

変更箇所

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

実行

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, (326 ページ)	ルータから DSA キー ペアを削除します。
show crypto key mypubkey dsa, (358 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

<i>usage-keys</i>	(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。
<i>general-keys</i>	(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。
<i>keypair-label</i>	(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	変更箇所
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	実行

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, (328 ページ)	ルータ用の RSA キー ペアを削除します。
show crypto key mypubkey rsa, (360 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	変更箇所
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	実行

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

変更箇所

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

実行

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, (320 ページ)	DSA キー ペアを作成します。
show crypto key mypubkey dsa, (358 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	変更箇所
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**, ([313 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	実行

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, (303 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, (313 ページ)	CA からルータの証明書を取得します。
crypto key generate rsa, (322 ページ)	RSA キー ペアを生成します。
show crypto key mypubkey rsa, (360 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

<i>string</i>	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	変更箇所
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

<i>number</i>	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	変更箇所
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), (307 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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
enrollment retry period , (334 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 , (338 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	変更箇所
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), (307 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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
enrollment retry count , (332 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

変更箇所

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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。

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tring 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

変更箇所

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 21： 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 `ftp://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), (307 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 , (317 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), (340 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

<i>ip-address</i>	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	変更箇所
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), (307 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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
enrollment url , (338 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), (346 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), (352 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	変更箇所
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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。

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

変更箇所

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, (322 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	変更箇所
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), (307 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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
enrollment url , (338 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), (340 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), (352 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	変更箇所
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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
sftp-username (トラストポイント), (350 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	変更箇所
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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
sftp-password (トラストポイント), (348 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	変更箇所
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、ロ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), (307 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 , (317 ページ)	信頼できるポイントを選択した名前を設定します。
enrollment url , (338 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), (340 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), (346 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

変更箇所

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 , (309 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 , (313 ページ)	CA からルータの証明書を取得します。
crypto ca import , (315 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 , (317 ページ)	トラストポイントを選択した名前を設定します。

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

変更箇所

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, (305 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

変更箇所

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, (320 ページ)	DSA キー ペアを作成します。
crypto key zeroize dsa, (326 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

変更箇所

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, (322 ページ)	RSA キー ペアを生成します。
crypto key zeroize rsa, (328 ページ)	ルータからすべての RSA キーを削除します。

```
show crypto key mypubkey rsa
```



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, 364 ページ](#)
- [sam delete certificate, 367 ページ](#)
- [sam prompt-interval, 369 ページ](#)
- [sam verify, 371 ページ](#)
- [show sam certificate, 374 ページ](#)
- [show sam crl, 379 ページ](#)
- [show sam log, 382 ページ](#)
- [show sam package, 384 ページ](#)
- [show sam sysinfo, 388 ページ](#)

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

<i>filepath</i>	証明書のソース ロケーションへの絶対パス。
<i>location</i>	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	変更箇所
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ク 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、ネットワーク 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、ネットワーク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	実行

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 , (367 ページ)	証明書テーブルから証明書を削除します。
show sam certificate , (374 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	ネットワークデバイスのクロック情報を表示します。詳細については、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』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

<i>location</i>	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。
<i>certificate-index</i>	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	変更箇所
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ク 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、ネットワーク 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時、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	実行

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, (364 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, (374 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

<i>time-interval</i>	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	変更箇所
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 , (388 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

<i>location</i>	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。
<i>file-system</i>	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。
<i>digest</i>	(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	変更箇所
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、宛先ネットワーク 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	実行

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: /cr1_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 (<i>location</i> 引数および <i>certificate-index</i> 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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	変更箇所
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せん。

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:79:00:00:00:00:05
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 22 : 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:79:00:00:00:00:05
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 23 : 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 <i>crl-index</i> 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。
<i>crl-index</i>	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	変更箇所
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 24 : **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:83:00:00:00:00:44, revoked on Nov 03, 2002 00:59:02 GMT
    Serial #:21:2C:48:83:00:00:00:00:59, 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 25 : 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	変更箇所
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

ネットワーク 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	変更箇所
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:79:00:00:00:00:05
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 0f    [...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 26 : 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, (374 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

変更箇所

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 27 : *show sam sysinfo* フィールドの説明

フィールド	説明
Status	<p>running または not running のいずれか。</p> <p>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。</p>
Prompt Interval	<p>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。</p>
Prompt Default Response	<p>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。</p> <p>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」と表示されます。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。</p> <p>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。</p>

関連コマンド

コマンド	説明
sam prompt-interval, (369 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, 392 ページ](#)
- [sftp, 394 ページ](#)
- [sftp \(インタラクティブ モード\) , 398 ページ](#)
- [show ssh, 402 ページ](#)
- [show ssh session details, 404 ページ](#)
- [ssh, 406 ページ](#)
- [ssh client knownhost, 409 ページ](#)
- [ssh client source-interface, 411 ページ](#)
- [ssh client vrf, 413 ページ](#)
- [ssh server, 415 ページ](#)
- [ssh server logging, 417 ページ](#)
- [ssh server rate-limit, 419 ページ](#)
- [ssh server session-limit, 421 ページ](#)
- [ssh server v2, 423 ページ](#)
- [ssh timeout, 424 ページ](#)

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

<i>session-id</i>	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 <i>session-id</i>	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	変更箇所
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	実行

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。その後、**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 , (402 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-filename*] *source-filename dest-filename* [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

<i>username</i>	(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。
<i>hostname:remote-filename</i>	(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。
<i>source-filename</i>	SFTP の発信元 (パスを含む)
<i>dest-filename</i>	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。
<i>type</i>	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。
<i>interface-path-id</i>	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 (?) オンラインヘルプ機能を使用します。
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	変更箇所
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	実行
basic-services	実行

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 , (411 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 , (413 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

<i>username</i>	(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。
<i>hostname:remote-filename</i>	(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。
<i>type</i>	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。
<i>interface-path-id</i>	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 (?) オンラインヘルプ機能を使用します。
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	変更箇所
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 チャンネルを作成します。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 チャンネルが作成され、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	実行
basic-services	実行

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:/frmRouterdownload

/auto/tftp-server1-users5/admin/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownload againtoServer

/disk0:/frmRouterdownload
  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:/frmRouterdownload

/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownload againtoServer

/disk0:/frmRouterdownload
  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 , (411 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 , (413 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

変更箇所

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 28 : `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、アカウントिंग (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、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』を参照してください。
show ssh session details , (404 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

変更箇所

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 29 : 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, (402 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

<i>ipv4-address</i>	A:B:C:D 形式の IPv4 アドレス。
<i>ipv6-address</i>	X:X::X 形式の IPv6 アドレス。
<i>hostname</i>	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。
<i>type</i>	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。
<i>interface-path-id</i>	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 (?) オンラインヘルプ機能を使用します。
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	変更箇所
	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, \(411 ページ\)](#)) 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	実行
	basic-services	実行

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 , (402 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

変更箇所

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

<i>type</i>	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。
<i>interface-path-id</i>	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 (?) オンラインヘルプ機能を使用します。

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	変更箇所
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際の 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	変更箇所
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](#)、(409 ページ)、[ssh client source-interface](#)、(411 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 <i>vrf-name</i>	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。
<i>v2</i>	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	変更箇所
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ーに対してセキュア 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](#), (423 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、『 <i>Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference</i> 』を参照してください。
ssh server v2 , (423 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	変更箇所
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 番目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 サーバのログイン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 , (415 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	変更箇所
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	変更箇所
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	変更箇所
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	変更箇所
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、アカウントिंग（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	変更箇所
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, 428 ページ](#)

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	変更箇所
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 30 : **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。

 show ssl



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](#) , 432 ページ

storm-control

VPLS ブリッジ下の Access Circuit (AC ; 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。 <ul style="list-style-type: none"> 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。
pps 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	変更箇所
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

A

aaa accounting system default コマンド 7
aaa accounting update コマンド 9
aaa accounting コマンド 4
aaa authentication コマンド 11
aaa authorization command 14
aaa default-taskgroup コマンド 18
aaa group server radius コマンド 20
aaa group server tacacs+ コマンド 23
accept-lifetime コマンド 256
accept-tolerance コマンド 258
accounting (IKE) コマンド 145
accounting (回線) コマンド 25
address ipv4 (MPP) コマンド 276
address ipv6 (MPP) コマンド 279
address コマンド 147
allow コマンド 281
authentication (IKE ポリシー) コマンド 149
authorization コマンド 27

C

clear crypto ca certificates コマンド 303
clear crypto ca crt コマンド 305
clear crypto isakmp call admission statistics コマンド 154
clear crypto isakmp errors コマンド 156
clear crypto isakmp コマンド 152
clear crypto session コマンド 158
clear ssh コマンド 392
control-plane コマンド 284
crl optional (トラストポイント) コマンド 307
crypto ca authenticate コマンド 309
crypto ca cancel-enroll コマンド 311
crypto ca enroll コマンド 313
crypto ca import コマンド 315
crypto ca trustpoint コマンド 317

cryptographic-algorithm コマンド 260
crypto isakmp call admission limit コマンド 161
crypto isakmp identity コマンド 163
crypto isakmp keepalive コマンド 166
crypto isakmp peer コマンド 168
crypto isakmp policy-set コマンド 173
crypto isakmp policy コマンド 170
crypto isakmp profile コマンド 175
crypto isakmp コマンド 160
crypto key generate dsa コマンド 320
crypto key generate rsa コマンド 322
crypto key import authentication rsa コマンド 324
crypto keyring コマンド 177
crypto key zeroize dsa コマンド 326
crypto key zeroize rsa コマンド 328
crypto logging コマンド 179

D

deadtime (サーバグループコンフィギュレーション) コマンド 29
description (AAA) コマンド 31
description (IKE ポリシー) コマンド 180
description (ISAKMP ピア) コマンド 184
description (ISAKMP ポリシーセット) コマンド 182
description (キーリング) コマンド 186
description (トラストポイント) コマンド 330

E

encryption (IKE ポリシー) コマンド 188
enrollment retry count コマンド 332
enrollment retry period コマンド 334
enrollment terminal コマンド 336
enrollment url コマンド 338

G

group (AAA) コマンド [33](#)
group (IKE ポリシー) コマンド [190](#)

H

hash (IKE ポリシー) コマンド [192](#)

I

inband コマンド [286](#)
inherit taskgroup コマンド [35](#)
inherit usergroup コマンド [37](#)
interface (MPP) コマンド [288](#)
ip-address (トラストポイント) コマンド [340](#)

K

keepalive (ISAKMP プロファイル) コマンド [194](#)
key-string (IKE) コマンド [198](#)
key-string (キーチェーン) コマンド [266](#)
key chain (キーチェーン) コマンド [264](#)
key (key chain) コマンド [262](#)
key (RADIUS) コマンド [39](#)
keyring コマンド [196](#)
key (TACACS+) コマンド [41](#)

L

lawful-intercept disable コマンド [274](#)
lifetime (IKE ポリシー) コマンド [200](#)
local-address (キーリング) コマンド [202](#)
login authentication コマンド [43](#)

M

management-plane コマンド [291](#)
match identity (ISAKMP プロファイル) コマンド [206](#)
match identity (ISAKMP ポリシーセット) コマンド [204](#)

O

out-of-band コマンド [293](#)

P

password (AAA) コマンド [45](#)
policy (ISAKMP ポリシーセット) コマンド [209](#)
pre-shared-key コマンド [211](#)

Q

query url コマンド [342](#)

R

radius-server dead-criteria time コマンド [48](#)
radius-server dead-criteria tries コマンド [50](#)
radius-server deadtime コマンド [52](#)
radius-server host コマンド [54](#)
radius-server key コマンド [58](#)
radius-server retransmit コマンド [60](#)
radius-server timeout コマンド [62](#)
radius source-interface コマンド [64](#)
retransmit (RADIUS) コマンド [66](#)
rsa-pubkey コマンド [213](#)
rsakeypair コマンド [344](#)

S

sam add certificate コマンド [364](#)
sam delete certificate コマンド [367](#)
sam prompt-interval コマンド [369](#)
sam verify コマンド [371](#)
secret コマンド [68](#)
self-identity コマンド [215](#)
send-lifetime コマンド [268](#)
serial-number (トラストポイント) コマンド [346](#)
server-private (RADIUS) コマンド [76](#)
server-private (TACACS+) コマンド [80](#)
server (RADIUS) コマンド [71](#)
server (TACACS+) コマンド [74](#)
set interface tunnel-ipsec コマンド [217](#)
set ipsec-profile コマンド [219](#)
sftp-password (トラストポイント) コマンド [348](#)

sftp-username (トラストポイント) コマンド 350
 sftp (インタラクティブ モード) コマンド 398
 sftp コマンド 394
 show aaa コマンド 83
 show crypto ca certificates コマンド 354
 show crypto ca crls コマンド 356
 show crypto isakmp call admission statistics コマンド 221
 show crypto isakmp errors コマンド 224
 show crypto isakmp key コマンド 232
 show crypto isakmp peers コマンド 234
 show crypto isakmp policy コマンド 236
 show crypto isakmp profile コマンド 239
 show crypto isakmp sa コマンド 241
 show crypto isakmp stats コマンド 244
 show crypto key mypubkey dsa コマンド 358
 show crypto key mypubkey rsa コマンド 360
 show crypto key pubkey-chain rsa コマンド 248
 show crypto session コマンド 251
 show key chain コマンド 270
 show mgmt-plane コマンド 295
 show radius accounting コマンド 91
 show radius authentication コマンド 93
 show radius client コマンド 95
 show radius dead-criteria コマンド 97
 show radius server-groups コマンド 99
 show radius コマンド 89
 show sam certificate コマンド 374
 show sam crl コマンド 379
 show sam log コマンド 382
 show sam package コマンド 384
 show sam sysinfo コマンド 388
 show ssh session details コマンド 404
 show ssh コマンド 402
 show ssl コマンド 428
 show tacacs server-groups コマンド 104
 show tacacs コマンド 102
 show user コマンド 106
 single-connection コマンド 110
 ssh client knownhost コマンド 409

ssh client source-interface コマンド 411
 ssh client vrf コマンド 413
 ssh server logging コマンド 417
 ssh server rate-limit コマンド 419
 ssh server session-limit コマンド 421
 ssh server v2 コマンド 423
 ssh server コマンド 415
 ssh timeout コマンド 424
 ssh コマンド 406
 storm-control コマンド 432
 subject-name (トラストポイント) コマンド 352

T

tacacs-server host コマンド 112
 tacacs-server key コマンド 115
 tacacs-server timeout コマンド 117
 tacacs source-interface コマンド 119
 taskgroup コマンド 123
 task コマンド 121
 timeout login response コマンド 129
 timeout (RADIUS) コマンド 125
 timeout (TACACS+) コマンド 127

U

usergroup コマンド 131
 username コマンド 133
 users group コマンド 137

V

vrf (MPP) コマンド 298
 vrf (RADIUS) コマンド 139
 vrf (TACACS+) コマンド 141

