CHAPTER 4

その他のルータ機能の設定

この章では、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して基本的な設定を入力する方法について説明します。

目次

- 「ドメイン名とドメイン名サーバの設定」（P.4-1）
- 「Telnet サービスと XML ホスト サービスの設定」（P.4-4）
- 「コンフィギュレーション履歴の管理とロールバック」（P.4-6）
- 「ロギングとロギング相関の設定」（P.4-12）
- 「ユーザ アカウントとユーザ グループの作成と変更」（P.4-16）
- 「ソフトウェア エンタイトルメントの設定」（P.4-19）
- 「設定の制限」（P.4-19）

ドメイン名とドメイン名サーバの設定

ネットワーク上の他のデバイスに効率よく接続できるようにするために、ルータのドメイン名と Domain Name Server（DNS; ドメイン名サーバ）を設定します。次の注意事項に従ってください。

- Cisco IOS XR ソフトウェアが、修飾されていないホスト名（ドットで区切られた十進数のドメイン名）を完全なドメイン名にするために使用するデフォルト ドメイン名を定義するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。
- 名前/アドレス解決に使用する 1 つまたは複数のネーム サーバの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 **domain name-server** コマンドを使用します。ネーム サーバのアドレスが指定されていない場合は、DNS lookup をローカル ネットワーク セグメントにブロードキャストできるように、255.255.255.255 がデフォルトのネーム サーバとなります。ローカル ネットワーク上に DNS サーバがあれば、それが応答します。DNS サーバがなくても、DNS 要求を正しい DNS サーバに転送する方法を知っているサーバが置かれている場合もあります。
- EXEC モードで **show hosts** コマンドを使用すると、デフォルト ドメイン名、名前検索サービスのスタイル、ネーム サーバ ホストの一覧、およびキャッシュ内にあるホスト名とアドレスの一覧が表示されます。

DNS と DNS サーバを設定するには、次の手順を実行します。

手順概要

1. **configure**
2. **domain name** *domain-name-of-organization*
3. **domain name-server** *ipv4-address*
4. **commit**
   または
   end
5. **show hosts**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**domain name** *domain-name-of-organization* **例：** `RP/0/RSP0/CPU0:router(config)# domain name cisco.com`	修飾されていないホスト名を完全なホスト名にするために使用されるデフォルト ドメイン名を定義します。
ステップ 3	**domain name-server** *ipv4-address* **例：** `RP/0/RSP0/CPU0:router(config)# domain name-server 192.168.1.111`	名前/アドレス解決に使用するネーム サーバ（名前情報を提供するホスト）を指定します。 **（注）** 最大 6 つのアドレスを入力できますが、各コマンドでは 1 つずつしか指定できません。

	コマンドまたはアクション	目的

ステップ 4	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 5	**show hosts** **例：** `RP/0/RSP0/CPU0:router(config)# show hosts`	設定されているすべてのネーム サーバを表示します。

例

次の例では、ドメイン名と DNS を設定しています。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# domain name cisco.com
RP/0/RSP0/CPU0:router(config)# domain name-server 10.1.1.1
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# end
RP/0/RSP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers: 10.1.1.1
```

Telnet サービスと XML ホスト サービスの設定

セキュリティ上の理由から、一部のホスト サービスはデフォルトでは無効になっています。Telnet や Extensible Markup Language（XML; 拡張マークアップ言語）などのホスト サービスは、ここで説明するコマンドを使用して有効化できます。Telnet サーバを有効にすると、ユーザが IPv4 Telnet クライアントを使用してルータにログインできるようになります。

前提条件

Telnet サービスおよび XML ホスト サービスを設定する場合は、その前に次の前提条件が満たされていることを確認してください。

- XML ホスト サービスには、管理パッケージがルータにインストールされ、アクティブになっている必要があります。
- XML サービスの Secure Socket Layer（SSL; セキュア ソケット レイヤ）を有効にするには、セキュリティ パッケージがルータにインストールされ、アクティブになっている必要があります。

パッケージのインストールとアクティブ化については、『*Cisco ASR 9000 Series Aggregation Series Router System Management Configuration Guide*』を参照してください。

（注） このプロセスは、管理イーサネット インターフェイスでの Telnet サービスと XML ホスト サービスを有効にします。これらのサービスをその他のインバンド インターフェイスで使用可能にする方法については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』を参照してください。

手順概要

1. **configure**
2. **telnet ipv4 server max-servers** *limit*
3. **end** または **commit**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**telnet ipv4 server max-servers** *limit* **例：** `RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 5`	ルータ上の Telnet サービスを有効にし、使用可能な Telnet サーバの最大数を指定します。

ステップ 3	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

例

次の例では、ホスト サービスを有効化しています。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 5
RP/0/RSP0/CPU0:router(config)# http server
RP/0/RSP0/CPU0:router(config)# commit
```

関連資料

関連トピック	参照先
「管理パッケージおよびセキュリティ パッケージのインストールとアクティブ化」	『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』
「XML サーバ コマンドの説明」	『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』

コンフィギュレーション履歴の管理とロールバック

commit 処理を実行するたびに、コミットされた設定変更の記録がシステムに保存されます。この記録には、そのコンフィギュレーション セッション中に行われた変更だけが含まれます。完全な設定が含まれているわけではありません。各記録に一意の ID *commitID* が割り当てられます。commitID を使用すれば、次のことが行えます。

- 以前の設定に戻す場合に、どの設定に戻すかを指定できます。特定の commitID へと設定をロールバックする場合は、その前に次の点を考慮してください。
  - パッケージの互換性の問題が原因で削除された設定にロールバックできません。設定のロールバックが成功するのは、その設定がアクティブな Cisco IOS XR ソフトウェア リリースとのすべての互換性チェックに合格している場合だけです。
  - ロールバック中に互換性のない設定が見つかった場合は、操作が失敗し、エラーが表示されます。
- コンフィギュレーション セッション中に加えた設定変更をロードできます。
- 複数の commitID からの設定変更をロードできます。
- commitID を消去できます。

Cisco IOS XR は、最大 100 個の最新 commitID を自動的に保存します。

次の節で、設定変更を管理する方法と、以前にコミットされた設定までロールバックする方法を説明します。

- 「CommitID の表示」（P.4-7）
- 「1 つの CommitID に記録されている設定変更の表示」（P.4-7）
- 「ロールバックによる設定変更のプレビュー」（P.4-8）
- 「指定したロールバック ポイントまでの設定のロールバック」（P.4-9）
- 「指定したコミット数に渡る設定のロールバック」（P.4-9）
- 「ターゲット コンフィギュレーションに CommitID の設定変更をロードする」（P.4-10）
- 「ロールバックによる設定変更をターゲット コンフィギュレーションにロードする」（P.4-11）
- 「CommitID の削除」（P.4-12）

CommitID の表示

最大 100 個の最新 commitID を表示するには、EXEC モードまたは管理 EXEC モードで **show configuration commit list** コマンドを入力します。最大 100 個の最新 commitID が、システムによって保存されます。各 commitID エントリに、設定変更をコミットしたユーザ、コミットの実行に使用された接続、および commitID のタイム スタンプが表示されます。

commitID は、「Label/ID」カラムに表示されます。次の例では、EXEC モードおよび管理 EXEC モードでの **show configuration commit list** コマンドの表示を示します。

```
RP/0/RSP1/CPU0:router# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000219  cisco     vty0        CLI         12:27:50 UTC Wed Mar 22 2008
2    1000000218  cisco     vty1        CLI         11:43:31 UTC Mon Mar 20 2008
3    1000000217  cisco     con0_RSP0_C  CLI         17:44:29 UTC Wed Mar 15 2008

RP/0/RSP1/CPU0:router# admin
RP/0/RSP1/CPU0:router(admin)# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    2000000022  cisco     vty1        CLI         15:03:59 UTC Fri Mar 17 2008
2    2000000021  cisco     con0_RSP0_C  CLI         17:42:55 UTC Wed Mar 15 2008
3    2000000020  SYSTEM    con0_RSP0_C  Setup Dial  17:07:39 UTC Wed Mar 15 2008
```

1 つの CommitID に記録されている設定変更の表示

特定のコミット セッション（commitID）中に加えられた設定変更を表示するには、EXEC モードまたは管理 EXEC モードに入って **show configuration commit changes** コマンドを入力し、それに続けて commitID 番号を入力します。最も簡単に commitID を確認する方法は、**show configuration commit changes ?** コマンドを最初に入力することです。次の例では、コマンド ヘルプを使用して指定可能な commitID を表示してから、特定の commitID の変更内容を表示しています。

```
RP/0/RSP1/CPU0:router(admin)# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  2000000020  Commit ID
  2000000021  Commit ID
  2000000022  Commit ID

RP/0/RSP1/CPU0:router(admin)# show configuration commit changes 2000000020

Building configuration...
username cisco
 secret 5 $1$MgUH$xzUEW6jLfyAYLKJE.3p440
 group root-system
!
end
```

ロールバックによる設定変更のプレビュー

show configuration rollback changes コマンドを使用すると、指定した commitID までロールバックした場合に行われる設定変更をプレビューすることができます。たとえば、設定をある特定の時点までロールバックする場合、その時点より後に加えられたすべての設定変更を元に戻す必要があります。このロールバック プロセスは、多くの場合、元に戻す必要があるコマンドの **no** バージョンを実行することにより達成できます。

現在の設定から指定した commitID までに予想されるロールバックによる設定変更を表示するには、EXEC モードまたは管理 EXEC モードに入って、**show configuration rollback changes to** *commitId* コマンドを入力します。次の例では、指定できる commitID をコマンド ヘルプで表示してから、ロールバック変更を表示しています。

```
RP/0/RSP1/CPU0:router# show configuration rollback changes to ?

  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID

RP/0/RSP1/CPU0:router# show configuration rollback changes to 1000000218

Building configuration...
no interface Loopback100
interface Gi0/1/0/0
 no ipv4 nd dad attempts
!
!
no route-policy xx
end
```

現在の設定から最近の指定した回数分のセッションまでに予想されるロールバックによる設定変更を表示するには、次のように、EXEC モードまたは管理 EXEC モードに入って **show configuration rollback changes last** *commit-range* コマンドを入力します。

```
RP/0/RSP0/CPU0:router# show configuration rollback changes last 2

Building configuration...
interface Loopback3
no description
no ipv4 address 10.0.1.1 255.0.0.0
exit
interface Loopback4
no description
no ipv4 address 10.0.0.1 255.0.0.0
end
```

上の例では、最後の 2 つの commitID の予想されるロールバックによる設定変更が表示されています。

指定したロールバック ポイントまでの設定のロールバック

指定したロールバック ポイントまで設定をロールバックすると、そのロールバック ポイントの commitID で示されたセッションで行われたすべての設定変更が元に戻され、その時点以降に加えられたすべての設定変更も元に戻されます。ロールバック プロセスは、設定をロールバックし、ロールバックによる設定をコミットします。ロールバック プロセスは、ロールバック前の設定まで設定をロールバックできるように、新しいロールバック ポイントの生成も行います。

ヒント　ロールバックで元に戻される設定をプレビューするには、**show configuration rollback changes** コマンドを使用します。

ルータ設定を以前にコミットした設定までロールバックするには、次のように、EXEC モードまたは管理 EXEC モードに入って **rollback configuration to** *commitId* コマンド を入力します。

```
RP/0/RSP1/CPU0:router# rollback configuration to 1000000220
Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
2 items committed in 1 sec (1)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back to '1000000220'.
```

指定したコミット数に渡る設定のロールバック

指定したコミット数に渡って設定をロールバックする場合は、特定の commitID を入力する必要はありません。その代わりに回数 *x* を指定すれば、最近の *x* 回分のコミットされたコンフィギュレーション セッションで加えられた設定変更が元に戻されます。ロールバック プロセスは、設定をロールバックし、ロールバックされた設定をコミットし、ロールバック前の設定用に新しい commitID を生成します。

ヒント　ロールバックで元に戻される設定をプレビューするには、**show configuration rollback changes** コマンドを使用します。

最後の *x* 回分のコミットをロールバックするには、EXEC モードまたは管理 EXEC モードに移動し、**rollback configuration last** *x* コマンドを入力します。*x* には、1 からコミット データベースに保存されているコミットの数までの数字を指定できます。

次の例では、最近 2 回分のコミットで加えられた設定変更をロールバックするように要求しています。

```
RP/0/RSP0/CPU0:router# rollback configuration last 2

Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back 2 commits.
```

ターゲット コンフィギュレーションに CommitID の設定変更をロードする

特定の commitID に保存された変更内容がやりたいことに近いものの、ロールバックすることは適切でない場合は、その commitID の設定変更をターゲット コンフィギュレーションにロードし、ターゲット コンフィギュレーションに変更を加えてから、新しい設定をコミットできます。ロールバック プロセスとは異なり、ロードされた変更は、コミットされるまで適用されません。

（注） ロールバック プロセスと違って、commitID の設定変更をロードした場合は、そのコミット処理で行われた変更内容しかロードされません。ロード プロセスでは、その commitID から現在コミットされている設定までの間に加えられたすべての変更がロードされるわけではありません。

ターゲット コンフィギュレーションに commitID の変更をロードするには、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 モードに入って **load commit changes** コマンドを commitID 番号と共に入力します。次の例では、show コマンドを使用して 1 つの commitID の変更内容を表示し、その commitID の設定をターゲット コンフィギュレーションにロードし、ターゲット コンフィギュレーションを表示しています。

```
RP/0/RSP1/CPU0:router# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID
  1000000220  Commit ID
  1000000221  Commit ID

RP/0/RSP1/CPU0:router# show configuration commit changes 1000000219
Building configuration...
interface Loopback100
!
interface Gi0/1/0/0
 ipv4 nd dad attempts 50
!
end

RP/0/RSP1/CPU0:router# config

RP/0/RSP1/CPU0:router(config)# load commit changes 1000000219
Building configuration...
Loading.
77 bytes parsed in 1 sec (76)bytes/sec

RP/0/RSP1/CPU0:router(config)# show configuration

Building configuration...
interface Loopback100
!
interface Gi0/1/0/0
 ipv4 nd dad attempts 50
!
end
```

ロールバックによる設定変更をターゲット コンフィギュレーションにロードする

特定のロールバック ポイントへの変更内容がやりたいことに近いものの、ロールバックすることは適切でない場合は、そのロールバックによる設定変更をターゲット コンフィギュレーションにロードし、ターゲット コンフィギュレーションに変更を加えてから、新しい設定をコミットできます。ロールバック プロセスとは異なり、ロードされた変更は、コミットされるまで適用されません。

ヒント　ロールバック変更を表示するには、**show configuration rollback changes** コマンドを入力します。

現在の設定から指定したセッションまでのロールバックによる設定変更をロードするには、次のように、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 モードに入って **load rollback changes to** *commitId* コマンドを入力します。

```
RP/0/RSP0/CPU0:router(config)# load rollback changes to 1000000068

Building configuration...
Loading.
233 bytes parsed in 1 sec (231)bytes/sec
```

現在の設定から指定した回数分の以前のセッションまでのロールバックによる設定変更をロードするには、次のように、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 モードに入って **load rollback changes last** *commit-range* コマンドを入力します。

```
RP/0/RSP0/CPU0:router(config)# load rollback changes last 6

Building configuration...
Loading.
221 bytes parsed in 1 sec (220)bytes/sec
```

前の例では、入力したコマンドにより、最近 6 回分の commitID のロールバックによる設定変更がロードされます。

指定した commitID のロールバックによる設定変更をロードするには、次のように、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 モードに入って、**load rollback changes** *commitId* コマンドを入力します。

```
RP/0/RSP0/CPU0:router(config)# load rollback changes 1000000060

Building configuration...
Loading.
199 bytes parsed in 1 sec (198)bytes/sec
```

CommitID の削除

EXEC モードまたは管理 EXEC モードで **clear configuration commit** コマンドを入力することにより、最も古い設定の commitID を削除できます。**clear configuration commit** コマンドの後ろには、解放するディスク スペースの量または削除する commitID の数を指定する必要があります。最も古い一連の commitID を削除して指定したディスク スペースを空けるには、次のように、**clear configuration commit** コマンドの後ろにキーワード **diskspace** を続け、再要求するディスク スペース量を KB 単位で指定します。

```
RP/0/RSP0/CPU0:router# clear configuration commit diskspace 50

Deleting 4 rollback points '1000000001' to '1000000004'
64 KB of disk space will be freed. Continue with deletion?[confirm]
```

最も古い方からの指定した回数分の commitID を削除するには、次のように、**clear configuration commit** コマンドの後ろにキーワード **oldest** を続け、削除する commitID の数を指定します。

```
RP/0/RSP0/CPU0:router# clear configuration commit oldest 5

Deleting 5 rollback points '1000000005' to '1000000009'
80 KB of disk space will be freed. Continue with deletion?[confirm]
```

ロギングとロギング相関の設定

Cisco IOS XR ソフトウェア によって生成されたシステム メッセージは、メッセージの重大度に基づいてさまざまな場所にロギングできます。たとえば、情報メッセージはシステム コンソールに送り、デバッグ メッセージはネットワーク サーバにロギングするといったことができます。

さらに、関連のあるイベントをグループ化してまとめる相関規則を定義したり、複雑なクエリを生成してロギングされたイベントの一覧を作成したり、XML インターフェイスを通じてロギング イベントを取得したりすることもできます。

次の節で、Cisco IOS XR ソフトウェアでのロギング、およびメッセージのロギングに使用される基本コマンドについて説明します。

- 「ロギングの場所と重大度」（P.4-12）
- 「アラーム ロギング相関」（P.4-13）
- 「基本的なメッセージ ロギングの設定」（P.4-13）
- 「コンソール ロギングの無効化」（P.4-16）

ロギングの場所と重大度

エラー メッセージは、表 4-1 に示すように、さまざまな場所にロギングできます。

表 4-1　システム エラー メッセージのロギングの場所

ロギング先	コマンド（グローバル コンフィギュレーション モード）
コンソール	**logging console**
vty 端末	**logging monitor**
外部 syslog サーバ	**logging trap**
内部バッファ	**logging buffered**

メッセージは、メッセージの重大度に基づいてロギングできます。表 4-2 を参照してください。

表 4-2　システム エラー メッセージのロギング重大度

レベル	説明
レベル 0：緊急	システムが使用できなくなります。
レベル 1：アラート	システムの安定性を回復するため、ただちに対処する必要があります。
レベル 2：クリティカル	注意を要する可能性がある致命的な状態です。
レベル 3：エラー	問題の追跡に役立つ可能性のあるエラー状態です。
レベル 4：警告	さほど重大ではない警告状態です。
レベル 5：通知	通知される、正常なものの重大な状態です。
レベル 6：情報	処置を必要としない情報メッセージです。
レベル 7：デバッグ	システム トラブルシューティング専用のデバッグ メッセージです。

アラーム ロギング相関

アラーム ロギング相関は、よく似たメッセージをグループ化し、フィルタをかけて、冗長なログの量を減らし、メッセージの根本的な原因を分離するために使用されます。

たとえば、Online Insertion and Removal（OIR; 活性挿抜）と上下するシステム状態を表す元のメッセージを報告し、以降に続く同じイベントを含むメッセージはすべて相関させたりできます。相関規則を作成すると、その発生に続けて大量のエラー イベントを発生させる共通の根元イベントを分離し、相関バッファに送ることができます。オペレータは、後から必要に応じてすべての相関メッセージを取り出して確認できます。詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』を参照してください。

基本的なメッセージ ロギングの設定

Cisco IOS XR ソフトウェアでのシステム メッセージのロギングには、多数のオプションが使用できます。この節では、基本的な例を示します。

基本的なメッセージ ロギングを設定するには、次の手順を実行します。

手順概要

1. **configure**
2. **logging** {*ip-address* | *hostname*}
3. **logging trap** *severity*
4. **logging console** [*severity*]
5. **logging buffered** [*severity* | *buffer-size*]
6. **commit**
7. **end**
8. **show logging**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging** {*ip-address* | *hostname*} **例：** `RP/0/RSP0/CPU0:router(config)# logging 10.1.1.1`	システム ロギングに使用する syslog サーバ ホストを指定します。
ステップ 3	**logging trap** *severity* **例：** `RP/0/RSP0/CPU0:router(config)# logging trap debugging`	syslog サーバに送信されるメッセージのロギングを指定したレベルのメッセージのものだけに制限します。 • ロギングの重大度レベルの概要については、表 4-2 を参照してください。
ステップ 4	**logging console** [*severity*] **例：** `RP/0/RSP0/CPU0:router(config)# logging console emergencies`	メッセージをコンソールにロギングします。 • 重大度を指定した場合は、その重大度のメッセージだけがコンソールにロギングされます。 • ロギングの重大度レベルの概要については、表 4-2 を参照してください。
ステップ 5	**logging buffered** [*severity* | *buffer-size*] **例：** `RP/0/RSP0/CPU0:router(config)# logging buffered 1000000`	メッセージのロギングを内部バッファにコピーします。 • バッファがいっぱいになった後は、古いメッセージが新しいメッセージで上書きされます。 • 重大度を指定すると、その重大度のメッセージと、重大度の数字がそれより小さいメッセージが内部バッファにロギングされます。ロギングの重大度レベルの概要については、表 4-2 を参照してください。 • バッファ サイズは、4,096 ～ 4,294,967,295 バイトです。設定された制限値より上のメッセージは、コンソールにロギングされます。
ステップ 6	**commit** **例：** `RP/0/RSP0/CPU0:router(config)# commit`	ターゲット コンフィギュレーションを実行コンフィギュレーションにコミットします。
ステップ 7	**end** **例：** `RP/0/RSP0/CPU0:router(config)# end`	コンフィギュレーション セッションを終了し、EXEC モードに戻ります。
ステップ 8	**show logging** **例：** `RP/0/RSP0/CPU0:router# show logging`	バッファにロギングされたメッセージを表示します。

例

次の例では、基本的なメッセージ ロギングを設定しています。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# logging 10.1.1.1
RP/0/RSP0/CPU0:router(config)# logging trap debugging
RP/0/RSP0/CPU0:router(config)# logging console emergencies
RP/0/RSP0/CPU0:router(config)# logging buffered 1000000
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# end
RP/0/RSP0/CPU0:router# show logging

Syslog logging: enabled (162 messages dropped, 0 flushes, 0 overruns)
    Console logging: level emergencies, 593 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level debugging, 2 messages logged
    Logging to 10.1.1.1, 2 message lines logged
    Buffer logging: level debugging, 722 messages logged

Log Buffer (1000000 bytes):

RP/0/RSP0/CPU0:Apr  8 19:18:58.679 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RSP0/CPU0:Apr  8 19:19:01.287 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RSP0/CPU0:Apr  8 19:22:15.658 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
LC/0/1/CPU0:Apr  8 19:22:30.122 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
LC/0/6/CPU0:Apr  8 19:22:30.160 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
RP/0/RSP0/CPU0:Apr  8 19:22:30.745 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
RP/0/RSP1/CPU0:Apr  8 19:22:32.596 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
LC/0/1/CPU0:Apr  8 19:22:35.181 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
LC/0/6/CPU0:Apr  8 19:22:35.223 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
RP/0/RSP0/CPU0:Apr  8 19:22:36.122 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RSP1/CPU0:Apr  8 19:22:37.790 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RSP0/CPU0:Apr  8 19:22:41.015 : schema_server[332]: %MGBL-SCHEMA-6-VERSIONC
RP/0/RSP0/CPU0:Apr  8 19:22:59.844 : instdir[203]: %INSTALL-INSTMGR-4-ACTIVE_SOF
RP/0/RSP0/CPU0:Apr  8 19:22:59.851 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
 --More--
```

関連資料

関連トピック	参照先
「システム ロギングの設定」	『*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*』
「ロギングの設定に使用されるコマンド」	『*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*』
「アラーム相関の設定と複雑なクエリの生成」	『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』
「アラーム相関の設定に使用されるコマンド」	『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』
「XML インターフェイスを介したロギング イベントの取得」	『*Cisco ASR 9000 Series Aggregation Services Router XML API Guide*』

コンソール ロギングの無効化

コンソール ロギングを無効にするには、グローバル コンフィギュレーション モードで **logging console disable** コマンドを入力します。

ユーザ アカウントとユーザ グループの作成と変更

Cisco IOS XR ソフトウェアでは、ユーザには個別のユーザ名とパスワードが割り当てられます。各ユーザ名が 1 つまたは複数のユーザ グループに割り当てられ、そのそれぞれのユーザ グループで、所属するユーザに実行権限が与えられる表示コマンドとコンフィギュレーション コマンドが定義されます。この権限付与は Cisco IOS XR ソフトウェアのデフォルトで有効になっており、各ユーザが、固有のユーザ名とパスワードを使用してシステムにログインしなければなりません。

次の節で、ユーザおよびユーザ グループの設定に使用する基本的なコマンドについて説明します。

- 「ユーザ アカウント、ユーザ グループ、およびタスク ID に関する詳細情報の表示」（P.4-16）
- 「ユーザ アカウントの設定」（P.4-17）
- 「ユーザの作成とグループの割り当て」（P.4-17）

ユーザ アカウント、ユーザ グループ、およびタスク ID の概要については、「ユーザ グループ、タスク グループ、およびタスク ID」（P.3-7）を参照してください。

（注） ユーザ アカウント、ユーザ グループ、およびタスク ID の管理は、認証、認可、アカウンティング（AAA）機能の一部です。AAA は、Cisco IOS XR ソフトウェアでのセキュリティ機能のセットです。AAA の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』および『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』を参照してください。ソフトウェア パッケージをアクティブ化する操作手順については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』を参照してください。

ユーザ アカウント、ユーザ グループ、およびタスク ID に関する詳細情報の表示

表 4-3 に、ユーザ アカウント、ユーザ グループ、およびタスク ID の詳細情報の表示に使用する EXEC モード コマンドをまとめます。

表 4-3　ユーザおよびユーザ グループに関する詳細情報を表示するコマンド

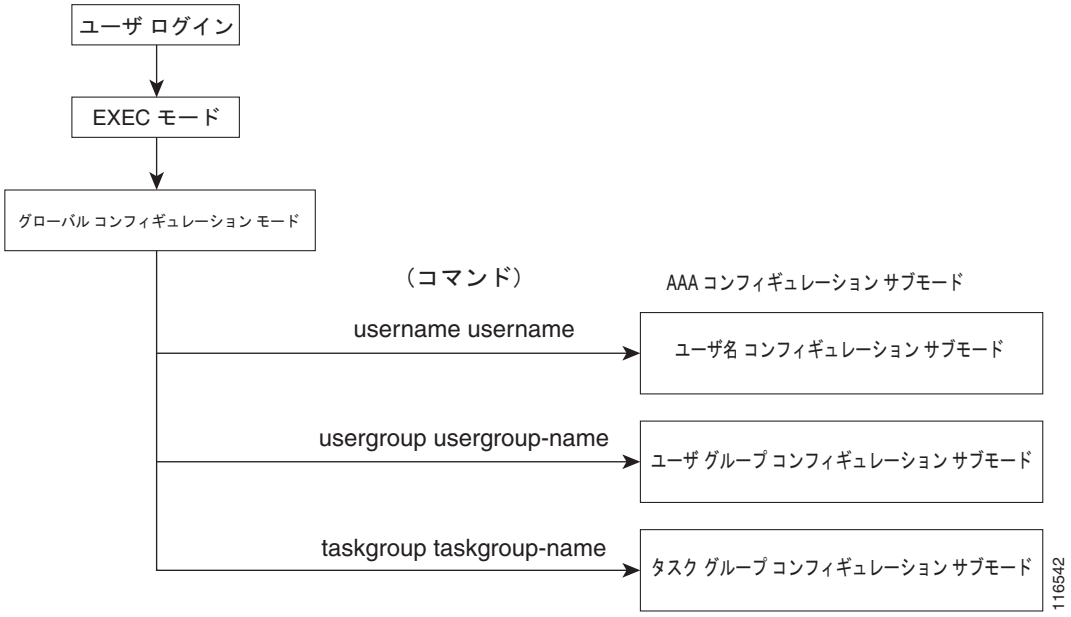
コマンド	説明
show aaa userdb *username*	指定されたユーザ名に割り当てられているタスク ID と特権を表示します。システム上のすべてのユーザを表示するには、ユーザ名を指定せずにコマンドを入力します。
show aaa usergroup *usergroup-name*	ユーザ グループに属するタスク ID と特権を表示します。システム上のすべてのグループを表示するには、グループ名を指定せずにコマンドを入力します。

ユーザ アカウントの設定

AAA コンフィギュレーション サブモードの 1 つで適切なコマンドを入力すると、図 4-1 に示すように、ユーザ アカウント、ユーザ グループ、およびタスク グループが作成されます。

この節では、ユーザ名を設定するプロセスについて説明します。ユーザ グループ、タスク グループ、およびその他の AAA セキュリティ機能を設定する操作手順については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』を参照してください。

図 4-1　　AAA コンフィギュレーション サブモード



ユーザの作成とグループの割り当て

ユーザを作成し、パスワードを割り当て、そのユーザをグループに割り当てるには、次の手順を実行します。

手順概要

1. **configure**
2. **username** *user-name*
3. **password** {**0** | **7**} *password*
   または
   secret {**0** | **5**} *password*
4. **group** *group-name*
5. ステップ 2 で指定されたユーザに関連付けられるユーザ グループごとに、ステップ 4 を繰り返します。
6. **commit**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *user-name* **例：** `RP/0/RSP0/CPU0:router(config)# username user1`	新しいユーザの名前を作成して（または現在のユーザを指定して）、ユーザ名コンフィギュレーション サブモードに入ります。 • *user-name* 引数に指定できるのは、1 つの単語だけです。スペースや引用符を入れることはできません。

ステップ 3	**password** {**0** | **7**} *password*
	または
	secret {**0** | **5**} *password*
	
	例：
	`RP/0/RSP0/CPU0:router(config-un)# password 0 pwd1`
	または
	`RP/0/RSP0/CPU0:router(config-un)# secret 5 pwd1`
		ステップ 2 で指定したユーザのパスワードを指定します。
		• **secret** コマンドを使用して、ステップ 2 で指定したユーザ名の安全なログイン パスワードを作成します。
		• **password** コマンドに続けて **0** を入力した場合は、暗号化されていない（クリアテキストの）パスワードを続けます。**password** コマンドに続けて **7** を入力した場合は、暗号化されたパスワードを続けます。
		• **secret** コマンドに続けて **0** を入力した場合は、暗号化されていない（クリアテキストの）安全なパスワードを続けます。**secret** コマンドに続けて **5** を入力した場合は、暗号化された安全なパスワードを続けます。
		• タイプ **0** が、**password** コマンドおよび **secret** コマンドのデフォルトです。

ステップ 4	**group** *group-name* **例：** `RP/0/RSP0/CPU0:router(config-un)# group sysadmin`	ステップ 2 で指定したユーザをユーザ グループに割り当てます。 • ユーザは、ユーザ グループのさまざまなタスク グループへの割り当てによって定義された内容に従って、ユーザ グループのすべての属性を受け取ります。 • どのユーザも、少なくとも 1 つのユーザ グループに割り当てられなければなりません。1 つのユーザが複数のユーザ グループに属することは可能です。
ステップ 5	ステップ 2 で指定されたユーザに関連付けられるユーザ グループごとに、ステップ 4 を繰り返します。	—
ステップ 6	**commit** **例：** `RP/0/RSP0/CPU0:router(config-un)# commit`	設定変更を保存し、実行コンフィギュレーションの一部としてアクティブ化します。

関連資料

関連トピック	参照先
「ユーザの作成、ユーザのユーザ グループへの割り当て、ユーザ グループの作成と変更、およびリモート AAA アクセスの設定」	『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』

ソフトウェア エンタイトルメントの設定

一部のソフトウェア機能およびハードウェア機能は、ソフトウェア エンタイトルメントを使用して有効化されます。ソフトウェア エンタイトルメントは、さまざまなソフトウェア機能とハードウェア機能のライセンスを管理する Cisco IOS XR デバイス上のライセンス マネージャで構成されるシステムです。ライセンス マネージャは、ライセンスを受け入れる前に、その解析と認証を行います。ルータ上のソフトウェア機能は、ライセンス マネージャ API を使用してライセンスのチェックアウトとリリースを行います。ライセンスは、ルータ上の固定ストレージに保存されます。

ルータの中心的な機能はすべて、ライセンスなしで使用できます。Cisco IOS XR ソフトウェア リリース 3.7 では、次の機能がライセンスによる有効化を必要とします。

- レイヤ 3 VPN
- モジュラ サービス カード帯域幅

ソフトウェア ラインセスの設定の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』を参照してください。

設定の制限

Cisco IOS XR ソフトウェア は、ルータの実行コンフィギュレーションに適用できる設定に対して、事前に制限を設けています。この制限により、ルータが正常に稼動するために十分なシステム リソース（メモリなど）が確保されます。ほとんどの状況では、この事前の制限で十分です。

特定の機能のために膨大な設定を必要とするなどの一部のケースでは、事前の制限を上書きすることが必要にある場合もあります。この上書きは、他の機能のための設定が少ないか、または未使用である場合にだけ行えます。

注意　デフォルトの設定制限を上書きすると、低メモリ状態が発生する場合があります。

次の節で、設定できる制限、デフォルト値と最大値、および設定制限の設定と表示のためのコマンドについて説明します。

- 「スタティック ルート設定の制限」（P.4-20）
- 「IS-IS 設定の制限」（P.4-20）
- 「OSPFv2 および v3 設定の制限」（P.4-21）
- 「ルーティング ポリシー言語の行数とポリシーの制限」（P.4-23）
- 「マルチキャスト設定の制限」（P.4-25）
- 「MPLS 設定の制限」（P.4-26）
- 「その他の設定の制限」（P.4-26）

スタティック ルート設定の制限

表 4-4 は、制限の表示と変更に使用するコマンドも含めて、スタティック ルートの最大制限値をまとめたものです。

表 4-4　スタティック ルート設定の制限とコマンド

機能制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド（スタティック ルータ コンフィギュレーション モード）	現在の設定を表示するコマンド（EXEC またはグローバル コンフィギュレーション モード）
最大スタティック IPv4 ルート	4,000	40,000	**maximum path ipv4** *n*	**show running-config router static**

例

次の例では、スタティック IPv4 ルートの最大数を 5000 に変更し、新しい設定を表示しています。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router static
RP/0/RSP1/CPU0:router(config-static)# maximum path ipv4 5000
RP/0/RSP1/CPU0:router(config-static)# commit
RP/0/RSP1/CPU0:router(config-static)# show running-config router static

router static
 maximum path ipv4 5000
 address-family ipv4 unicast
  0.0.0.0/0 172.29.52.1
 !
!
```

IS-IS 設定の制限

表 4-5 は、制限の表示と変更に使用するコマンドも含めて、Intermediate System to Intermediate System（IS-IS）ルーティング プロトコルの最大制限値をまとめたものです。

表 4-5　IS-IS 設定の制限とコマンド

機能制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド（アドレス ファミリ コンフィギュレーション モード）	現在の設定を表示するコマンド（EXEC モード）
IS-IS に再配布されるプレフィックスの最大数	10,000	28,000	**maximum-redistributed-prefixes** *n*	**show isis adjacency**
Cisco ASR 9000 シリーズ ルータ上の各ルートのアクティブなパラレル パスの数	8	32	**maximum-paths** *n*	**show isis route**

例

次の例では、各ルートのアクティブなパラレル パスの最大数を 10 に増やし、IS-IS に再配布されるプレフィックスの最大数を 12,000 に増やしています。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router isis 100 address-family ipv4
RP/0/RSP1/CPU0:router(config-isis-af)# maximum-paths 10
RP/0/RSP1/CPU0:router(config-isis-af)# maximum-redistributed-prefixes 12000
RP/0/RSP1/CPU0:router(config-isis-af)# commit
RP/0/RSP1/CPU0:Mar 30 14:11:07 : config[65739]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000535' to view
the changes.
RP/0/RSP1/CPU0:router(config-isis-af)#
```

OSPFv2 および v3 設定の制限

表 4-6 は、制限の表示と変更に使用するコマンドも含めて、Open Shortest Path First（OSPF）プロトコルの最大制限値をまとめたものです。

表 4-6　OSPFv2 設定の制限とコマンド

機能制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド（ルータ コンフィギュレーション モード）	現在の設定を表示するコマンド（EXEC モード）
OSPF インスタンスに設定できるインターフェイスの最大数	255	1,024	**maximum interfaces** *n*	**show ospf**
OSPF に再配布される最大ルート	10,000	4,294,967,295	**maximum redistributed-prefixes** *n*	**show ospf** **（注）** 再配布されたプレフィックスの最大数は、再配布が設定されている場合にだけ表示されます。
Cisco ASR 9000 シリーズ ルータ上のパラレルルートの最大数（最大パス）	32	32	**maximum paths** *n*	**show running-config router ospf** **（注）** このコマンドは、デフォルト値への変更だけを表示します。**maximum paths** コマンドが表示されない場合、ルータはデフォルト値に設定されています。

例

次の例で、OSPF 設定の制限を示します。

- 「各 OSPF インスタンスの最大インターフェイス数：例」（P.4-22）
- 「OSPF に再配布される最大ルート数：例」（P.4-23）
- 「パラレル リンクの数（max-paths）：例」（P.4-23）

各 OSPF インスタンスの最大インターフェイス数：例

次の例では、**show ospf** コマンドを使用して OSPF インターフェイスの最大数を表示しています。

```
RP/0/RSP1/CPU0:router# show ospf

 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 255
--More--
```

次の例では、ルータ上の最大インターフェイス制限を設定しています。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum interfaces 600
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP1/CPU0:Mar 30 16:12:39 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000540' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 16:12:39 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco

RP/0/RSP1/CPU0:router# show ospf

 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 600
--More--
```

OSPF に再配布される最大ルート数：例

次の例では、**maximum redistributed-prefixes** コマンドを使用して、OSPF に再配布される最大ルート数を設定しています。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum redistributed-prefixes 12000
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP1/CPU0:Mar 30 16:26:52 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000541' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 16:26:52 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco
RP/0/RSP1/CPU0:router#
```

パラレル リンクの数（max-paths）：例

次の例では、**maximum paths** コマンドを使用して、パラレル ルートの最大数を設定しています。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum paths 10
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP1/CPU0:Mar 30 18:05:13 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000542' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 18:05:13 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco
RP/0/RSP1/CPU0:router#
```

ルーティング ポリシー言語の行数とポリシーの制限

ルーティング ポリシー言語（RPL）の設定には次の 2 つの制限が存在します。

1. RPL 行の数：開始文と終了文も含めて、ユーザによって入力される設定行の数（つまり「route-policy」）。セットのための設定行の数も含まれます。
2. RPL ポリシーの数：ルータ上で設定できるポリシーの数。ポリシーは 1 度しかカウントされません。同じポリシーを複数回使用しても、制限 1 に向けて単一のポリシーとしてカウントされます。

RPL の行数とポリシーの制限について、表 4-7 にまとめます。デフォルト値を絶対最大値に変更できますが、数の値を現在設定されている項目の数より小さく変更することはできません。

表 4-7　RPL の最大行数：設定の制限とコメント

制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド（グローバル コンフィギュレーション モード）	現在の設定を表示する コマンド（EXEC モード）
RPL 行の最大数	65,536	131,072	**rpl maximum lines** *n*	**show rpl maximum lines**
RPL ポリシーの最大数	3,500	5,000	**rpl maximum policies** *n*	**show rpl maximum policies**

例

次の例では、EXEC モードで **show rpl maximum** コマンドを使用して、RPL 制限の現在の設定と、現在使用されている各制限の数を表示しています。制限値の下に、定義済みのすべてのポリシーによって使用されているメモリの概要も表示されます。

```
RP/0/RSP1/CPU0:router# show rpl maximum

                            Current    Current       Max
                             Total      Limit       Limit
-------------------------------------------------------------
Lines of configuration             0      65536     131072
Policies                           0       3500       5000
Compiled policies size (kB)        0
RP/0/RSP1/CPU0:router#
```

次の例では、**rpl maximum** コマンド で、現在設定されている行数とポリシーの制限を変更しています。**show rpl maximum** コマンドで、新しい設定値を表示します。

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# rpl maximum policies 4000
RP/0/RSP1/CPU0:router(config)# rpl maximum lines 80000
RP/0/RSP1/CPU0:router(config)# commit

RP/0/RSP1/CPU0:Apr  1 00:23:44.062 : config[65709]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'UNKNOWN'.   Use 'show configuration commit changes 1000000010' to view
the changes.
RP/0/RSP1/CPU0:router(config)# exit

RP/0/RSP1/CPU0:Apr  1 00:23:47.781 : config[65709]: %SYS-5-CONFIG_I : Configured from
console by console

RP/0/RSP1/CPU0:router# show rpl maximum

                            Current    Current       Max
                             Total      Limit       Limit
-------------------------------------------------------------
Lines of configuration             0      80000     131072
Policies                           0       4000       5000
Compiled policies size (kB)        0
RP/0/RSP1/CPU0:router#
```

マルチキャスト設定の制限

表 4-8 は、制限の表示と変更に使用するコマンドも含めて、マルチキャスト設定の最大制限値をまとめたものです。

表 4-8　マルチキャスト設定の制限とコマンド

機能制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド	現在の設定を表示するコマンド（EXEC モード）
Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）の制限				
IGMP に使用され、ルータに受け入れられるグループの最大数	50,000	75,000	**maximum groups** *n* （ルータ IGMP コンフィギュレーション モード）	**show igmp summary**
ルータに受け入れられる各インターフェイスのグループの最大数	25,000	40,000	**maximum groups-per-interface** *n* （ルータ IGMP インターフェイス コンフィギュレーション モード）	**show igmp summary**
Multicast Source Discovery Protocol（MSDP; マルチキャスト ソース検出プロトコル）の制限				
MSDP ソース アクティブ（SA）エントリの最大数	20,000	75,000	**maximum external-sa** *n* （ルータ MSDP コンフィギュレーション モード）	**show msdp summary**
MSDP ピアから学習できる MSDP SA エントリの最大数	20,000	75,000	**maximum peer-external-sa** *n* （ルータ MSDP コンフィギュレーション モード）	**show msdp summary**
Protocol Independent Multicast（PIM）の制限				
サポートされる最大 PIM ルート	100,000	200,000	**maximum routes** *n* （ルータ PIM コンフィギュレーション モード）	**show pim summary**
最大 PIM 出力状態	300,000	600,000	**maximum route-interfaces** *n* （ルータ PIM コンフィギュレーション モード）	**show pim summary**
最大 PIM レジスタ	20,000	75,000	**maximum register-states** *n* （ルータ PIM コンフィギュレーション モード）	**show pim summary**
自動 RP から学習される PIM グループ マップ範囲の最大数	500	5,000	**maximum group-mappings autorp** *n* （ルータ PIM コンフィギュレーション モード）	**show pim summary**

MPLS 設定の制限

表 4-9 は、制限の表示と変更に使用するコマンドも含めて、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）設定の最大制限値をまとめたものです。

表 4-9　MPLS 設定の制限とコマンド

制限の説明	デフォルト	絶対最大制限値	コンフィギュレーション コマンド（グローバル コンフィギュレーション モード）	現在の設定を表示する コマンド （EXEC モード）
最大トラフィック エンジニア（TE）トンネル ヘッド	2,500	65,536	**mpls traffic-eng maximum tunnels** *n*	**show mpls traffic-eng maximum tunnels**

その他の設定の制限

表 4-10 は、制限の表示と変更に使用するコマンドも含めて、その他の設定の制限の最大制限値をまとめたものです。

表 4-10　その他の設定の制限とコマンド

制限の説明	デフォルトの最大制限値	絶対最大制限値	コンフィギュレーション コマンド（グローバル コンフィギュレーション モード）	現在の設定を表示する コマンド （EXEC モード）
IPv4 ACL （アクセス リストおよびプレフィクス リスト）	5,000	16,000	**ipv4 access-list maximum acl threshold** *n*	**show access-lists ipv4 maximum**
IPv4 ACE （アクセス リストおよびプレフィクス リスト）	200,000	350,000	**ipv4 access-list maximum ace threshold** *n*	**show access-lists ipv4 maximum**