Cisco NCS 540 シリーズ ルータ（IOS XR リリース 6.3.x）システム セットアップおよびソフトウェア インストール ガイド

初版：2018 年 3 月 30 日

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

目 次

はじめに

この「はじめに」の内容は次のとおりです。

マニュアルの変更履歴

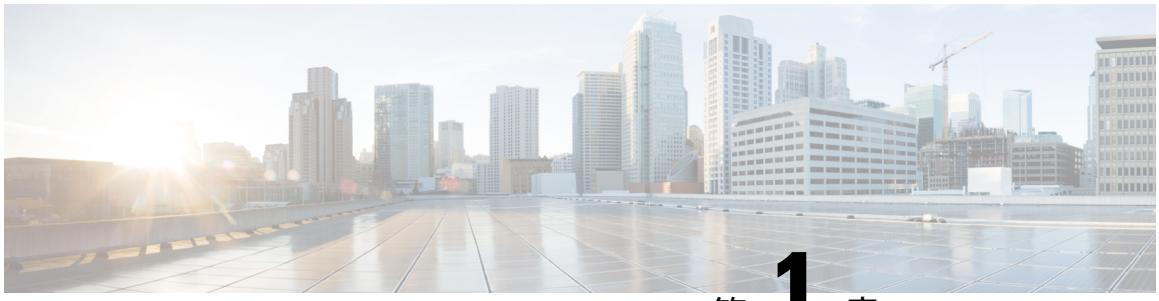
次の表に、このドキュメントで行われた技術的変更を示します。

日付	変更点
2018 年 3 月	このマニュアルの初回リリース

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、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html [英語] から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、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、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。



第 1 章

Cisco NCS 540 製品の概要

Cisco NCS 540 システムは、高い帯域幅と低遅延を備えた次世代のデータセンター スイッチング環境を実現する高耐障害性プラットフォームです。

Cisco NCS 540 システムは、次の機能を提供します。

- 高性能（300 Gbps 全二重スイッチング）
- フレキシブルなネットワーク インターフェイス（10GbE、25GbE、40GbE、50GbE、100GbE インターフェイス、および ILKN インターフェイス）
- トラフィック マネージャとインバンド管理
- フレキシブルでマイクロコードによるプログラムが可能なパケット プロセッサ
- VXLAN、NV-GRE、Geneve を含むデータセンター トンネリングのカプセル化
- ラベル スイッチド ルータ（LSR）およびライト ラベル スイッチド エッジ ルータ（LER）の機能およびハードウェアの規模とソフトウェアの機能に制限がある機能。

- コマンド モード （1 ページ）

コマンド モード

Cisco NCS 540 シリーズ システムは、仮想化された Cisco IOS XR ソフトウェアで動作します。したがって CLI コマンドは、仮想マシン上、つまり XR LXC およびシステム管理 LXC で実行する必要があります。次の表に、LXC のコマンド モードを示します。

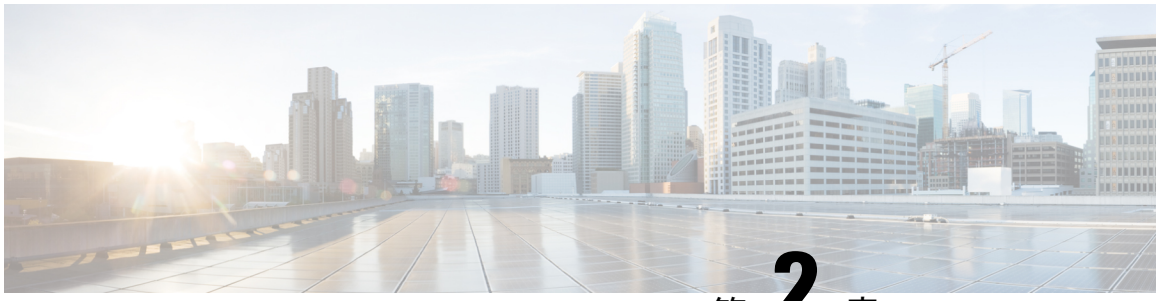
コマンド モード	説明
XR EXEC モード （XR LXC 実行モード）	XR LXC でコマンドを実行してルータの動作状態を表示します。 例： `RP/0/RP0/CPU0:router#`

コマンド モード	説明

XR コンフィギュレーション モード
（XR LXC コンフィギュレーション モード）
	XR LXC でセキュリティやルーティングなど、XR 機能の設定を行います。
	例：
	`RP/0/RP0/CPU0:router#configure`
	`RP/0/RP0/CPU0:router(config)#`

システム管理 EXEC モード
（システム管理 LXC 実行モード）
	システム管理 LXC でコマンドを実行して、ルータ ハードウェアの動作状態を表示およびモニタします。シャーシまたは個別のハードウェア モジュールは、このモードでリロードすることができます。
	例：
	`RP/0/RP0/CPU0:router#admin`
	`sysadmin-vm:0_RP0#`

システム管理コンフィギュレーション モード
（システム管理 LXC コンフィギュレーション モード）
	システム管理 LXC でコンフィギュレーション コマンドを実行して、シャーシ全体のハードウェア モジュールを管理および操作します。
	例：
	`RP/0/RP0/CPU0:router#admin`
	`sysadmin-vm:0_RP0#config`
	`sysadmin-vm:0_RP0(config)#`



第 2 章

ルータの起動

ハードウェアの設置後、ルータを起動します。XR コンソール ポートに接続し、ルータの電源をオンにします。ルータは、プリインストールされたオペレーティング システム（OS）イメージを使用してブート プロセスを実行します。ルータ内に使用できるイメージがない場合は、iPXE ブートまたは外部のブート可能な USB ドライブを使用してルータを起動できます。

起動が完了したら、root ユーザ名とパスワードを作成します。その組み合わせを使って XR コンソールにログインするとルータ プロンプトが表示されます。XR コンソールで作成された最初のユーザは、システム管理コンソールに同期されます。XR コンソールからシステム管理コンソールにアクセスして、システム管理設定を行います。

ルータの起動

新しいルータに接続するには、ルート プロセッサ（RP）のコンソール ポートを使用します。コンソール ポートはデフォルトで XR コンソールに接続されます。必要に応じて、設定済みの管理ポートを通じてさらに接続を確立できます。

手順

ステップ 1 RP のコンソール ポートに端末を接続します。

ステップ 2 ワークステーションで端末エミュレーション プログラムを起動します。

モジュラ型シャーシ RP の場合、コンソール設定はボー レートが 9600 bps、パリティなし、ストップ ビットが 2、データ ビットが 8 です。固定シャーシの場合、コンソール設定はボー レートが 115200 bps、パリティなし、ストップ ビットが 2、データ ビットが 8 です。

ステップ 3 ルータの電源を投入します。

電源コードを電源入力モジュール（PEM）に接続してルータを起動します。端末エミュレーション プログラムのコンソール画面に、ブート プロセスの詳細が表示されます。

ステップ 4 Enter を押します。

root-system ユーザ名の入力を求めるプロンプトが表示されたらブート プロセスは完了です。プロンプトが表示されない場合は、ルータの初期ブート手順が完了するまでしばらく待ってから Enter を押してください。

重要 ブート プロセスが失敗する原因として、ルータにプリインストールされているイメージが破損していることが考えられます。この場合は、外部のブート可能な USB ドライブを使用してルータを起動できます。

次のタスク

root ユーザ名およびパスワードを指定します。

root ユーザ クレデンシャルの設定

ルータの初回起動時に、root クレデンシャル（ユーザ名とパスワード）の設定を求めるプロンプトが表示されます。これらは、XR（root-lr）コンソールおよびシステム管理 LXC（root-system）の root ユーザ クレデンシャル、およびディザスタ リカバリのクレデンシャルとして設定されます。

始める前に

ブート プロセスを完了する必要があります。ブート プロセスの開始方法については、ルータの起動 （3 ページ） を参照してください。

手順

ステップ 1 **Enter root-system username:** *username*

root ユーザのユーザ名を入力します。文字数制限は 1023 文字です。この例では、root ユーザの名前は「root」です。

重要 指定したユーザ名は、XR コンソールの「root-lr」グループにマッピングされます。また、システム管理コンソールの「root-system」ユーザとしてもマッピングされます。

ルータの初回起動時またはイメージの再作成後は、ルータにユーザ設定がありません。この場合、ルータによって「root-system ユーザ名」を指定するように要求されます。ただしすでにルータが設定されている場合は、ステップ 4 で説明したように「ユーザ名」の入力を求めるプロンプトが表示されます。

ステップ 2 **Enter secret:** *password*

root ユーザのパスワードを入力します。文字数制限は 253 文字です。セキュリティ上の理由から、入力したパスワードは CLI に表示されません。

root ユーザにはスーパーユーザ権限があるため、root ユーザ名とパスワードは保護する必要があります。これはルータ設定全体へのアクセスに使用されます。

ステップ 3 **Enter secret again:** *password*

root ユーザのパスワードをもう一度入力します。パスワードは、前のステップで入力したパスワードと一致しないと拒否されます。セキュリティ上の理由から、入力したパスワードは CLI に表示されません。

ステップ 4 **Username:** *username*

XR LXC コンソールにログインするため、root-system ユーザ名を入力します。

ステップ 5 **Password:** *password*

root ユーザのパスワードを入力します。正しいパスワードを入力するとルータのプロンプトが表示されます。これで XR LXC コンソールにログインできました。

ステップ 6 （任意） **show run username**

ユーザの詳細を表示します。

```
username root
 group root-lr
 group cisco-support
 secret 5 $1$NBg7$fHs1inKPZVvzqxMv775UE/
!
```

例

（注） ルータの工場出荷時には、ルータを動作させる必要があるモードはあらかじめ定義されていません。したがって、ソフトウェアは、操作モードを決定する前に、使用状況、ポストラック マウント、および電源投入に基づいて、いくつかのイベントをスキャンします。ここでは、ソフトウェアがこの決定を行う時間帯があります。この間、スタンドアロンモードまたはZTPモードで動作することを目的としたルータが侵害され、nV サテライト モードになる可能性があります。その結果、ルータの特権的な制御が敵対的な外部エンティティに開放されます。

上記のように制御するには、外部エンティティが自動再生ポート（最高 10G および最低 100G のポート）と同じネットワークにアクセスできることを確認してください。一旦侵害されると、ルータは正当なユーザにアクセスできなくなる可能性がありますが、ネットワークへの物理的な切断や工場出荷時の初期状態へのリセットによって回復できます。

次のタスク

- XR コンソールからルーティング機能を設定します。
- システム管理プロンプトでシステム管理設定を行います。システム管理プロンプトは、システム管理コンソールへのアクセス時に表示されます。システム管理プロンプトを表示する方法については、システム管理コンソールへのアクセス （6 ページ）を参照してください。

システム管理コンソールへのアクセス

すべてのシステム管理とハードウェア管理の設定を行うには、XR コンソールからシステム管理コンソールにログインする必要があります。

手順

ステップ 1 root ユーザとして XR コンソールにログインします。

ステップ 2 **admin**

例：

次の例では、コマンド出力を示しています。

```
RP/0/RP0/CPU0:router#admin

Mon May 22 06:57:29.350 UTC

root connected from 127.0.0.1 using console on host
sysadmin-vm:0_RP0# exit
Mon May  22 06:57:32.360 UTC
```

ステップ 3 （任意） **exit**

システム管理モードから XR モードに戻ります。

管理ポートの設定

管理ポートをシステム管理およびリモート通信に使用するには、管理イーサネット インターフェイスの IP アドレスとサブネット マスクを設定する必要があります。他のネットワーク上のデバイス（リモート管理ステーションや TFTP サーバなど）と通信する場合は、ルータのデフォルト（スタティック）ルートを設定する必要があります。

始める前に

- ネットワーク管理者またはシステムの設計担当者に問い合わせて、管理インターフェイスの IP アドレスおよびサブネット マスクを入手します。

- RP の物理ポート イーサネット 0 とイーサネット 1 は管理ポートです。ポートが管理ネットワークに接続されていることを確認します。

（注） 管理性アプリケーションの設定中は、XR の物理ポート MgmtEth0/RP0/CPU0/1 をシャットダウンする必要があります。

手順

ステップ 1 **configure**

ステップ 2 **interfaceMgmtEth** *rack/slot/port*

例：

```
RP/0/RP0/CPU0:router(config)#interface mgmtEth 0/RP0/CPU0/0
```

プライマリ RP の管理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3 **ipv4address** *ipv4-address subnet-mask*

例：

```
RP/0/RP0/CPU0:router(config-if)#ipv4 address 10.1.1.1 255.0.0.0
```

IP アドレスとサブネット マスクをインターフェイスに割り当てます。

ステップ 4 **ipv4address** *ipv4 virtual address subnet-mask*

例：

```
RP/0/RP0/CPU0:router(config-if)#ipv4 address 1.70.31.160 255.255.0.0
```

仮想 IP アドレスとサブネット マスクをインターフェイスに割り当てます。

ステップ 5 **noshutdown**

例：

```
RP/0/RP0/CPU0:router(config-if)#no shutdown
```

インターフェイスを「アップ」状態にします。

ステップ 6 **exit**

例：

```
RP/0/RP0/CPU0:router(config-if)#exit
```

管理インターフェイス コンフィギュレーション モードを終了します。

ステップ 7 **routerstaticaddress-familyipv4unicast** *0.0.0.0/0default-gateway*

例：

```
RP/0/RP0/CPU0:router(config)#router static address-family ipv4 unicast 0.0.0.0/0 12.25.0.1
```

デフォルト ゲートウェイの IP アドレスを指定して、スタティック ルートを設定します。このルートは他のネットワーク上のデバイスと通信する際に使用します。

ステップ 8 **commit**

次のタスク

管理ポート経由でイーサネット ネットワークに接続します。端末エミュレーション プログラムで、管理インターフェイス ポートへの SSH または Telnet 接続をその IP アドレスを使って確立します。ルータに対して許可される Telnet セッションの数を設定するには、Telnet セッションを確立する前に、XR コンフィギュレーション モードで **telnet ipv4|ipv6 server max-servers** コマンドを使用します。SSH 接続の場合は、.rpm パッケージをルータにインストールする必要があります。パッケージ インストールの詳細については、次を参照してください。 パッケージのインストール （31 ページ）

NTP サーバとのクロック同期の実行

XR コンソールとシステム管理コンソールにはそれぞれのシステム クロックがあります。これらのクロックが実際の時間とずれないように、NTP サーバのクロックと同期する必要があります。このタスクでは、XR コンソール用に NTP サーバを設定します。XR コンソールのクロックを同期すると、システム管理コンソールのクロックは自動的に XR コンソールのクロックと同期されます。

始める前に

管理ポートを設定して接続します。

手順

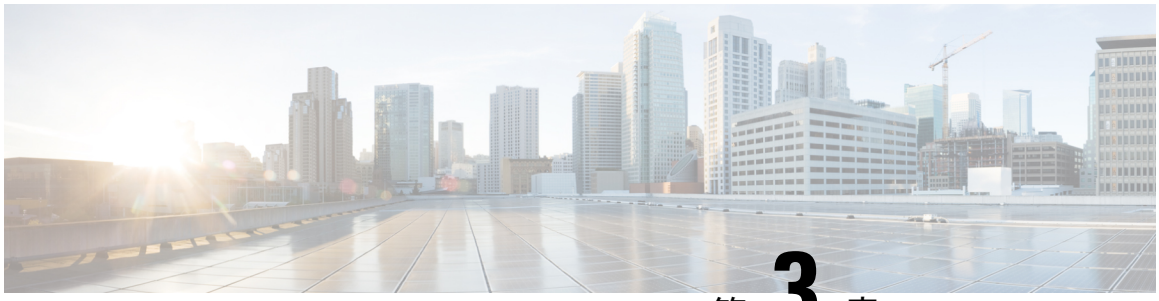
ステップ 1 **configure**

ステップ 2 **ntp server** *server_address*

例：

```
RP/0/RP0/CPU0:router#ntp server 64.90.182.55
```

指定したサーバと同期するように XR コンソールのクロックが設定されます。



第 3 章

予備チェックの実行

コンソールに正常にログインしたら、予備チェックを実行してデフォルト設定を確認する必要があります。チェックの実行時に設定の問題が検出された場合は、さらに設定を行う前に修正を行ってください。予備チェックの内容は次のとおりです。

ハードウェア モジュールのステータスの確認

ハードウェア モジュールにはRP、LC、ファン トレイなどがあります。ルータには複数のハードウェア モジュールが取り付けられています。すべてのハードウェア モジュールが正しく取り付けられて動作していることを確認するには、次のタスクを実行します。

始める前に

必要なハードウェア モジュールがすべてルータに取り付けられていることを確認します。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

システム管理 EXEC モードを開始します。

ステップ 2 **showplatform**

例：

```
sysadmin-vm:0_RP0#show platform
```

ルータで検出されたハードウェア モジュールのリストを表示します。

```
Location  Card Type                HW State      SW State      Config State
------------------------------------------------------------------------------
0/RP0     N540-24Z8Q2C-M   OPERATIONAL    OPERATIONAL   NSHUT
0/FT0     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT1     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT2     N540-FAN   OPERATIONAL    N/A     NSHUT
0/FT3     N540-FAN   OPERATIONAL    N/A     NSHUT
```

この結果で、シャーシに設置されたすべてのハードウェアモジュールが表示されていることを確認します。モジュールが表示されない場合、そのモジュールが正常に動作していないか、正しく設置されていないことを意味します。ハードウェアモジュールを取り外して、もう一度取り付けてください。

ステップ 3 **showhw-module fpd**

例：

```
RP/0/RP0/CPU0:router# show hw-module fpd
```

ルータで検出されたハードウェア モジュールのリストを表示します。

```
FPD Versions
=================
Location Card type      HWver FPD device ATR Status Running Programd
------------------------------------------------------------------------------
0/RP0    N540-24Z8Q2C-M 0.5   MB-MIFPGA      CURRENT 0.04    0.04
0/RP0    N540-24Z8Q2C-M 0.5   Bootloader     CURRENT 1.07    1.07
0/RP0    N540-24Z8Q2C-M 0.5   CPU-IOFPGA     CURRENT 0.03    0.03
0/RP0    N540-24Z8Q2C-M 0.5   MB-IOFPGA      CURRENT 0.16    0.16
RP/0/RP0/CPU0:ios#
```

ノード ステータスの確認

ルータ上の各カードはノードを表します。ノードの動作ステータスは、**show platform** コマンドを使用して確認します。このコマンドは、XR およびシステム管理モードの両方の CLI で個別に実行します。

手順

ステップ 1 **showplatform**

例：

```
RP/0/RP0/CPU0:router#show platform
```

XR EXEC モードで **show platform** コマンドを実行すると、さまざまな RP および LC で動作している XR コンソールのステータスが表示されます。

```
RP/0/RP0/CPU0:<router>#sh platform
Node   Type  State  Config state
------------------------------------------------------------------------------
```

```
0/RP0/CPU0 N540-X-24Z8Q2C-M(Active) IOS XR RUN NSHUT
0/RP0/NPU0 Slice UP
0/FT0  N540-FAN OPERATIONAL  NSHUT
0/FT1  N540-FAN OPERATIONAL  NSHUT
0/FT2  N540-FAN OPERATIONAL  NSHUT
0/FT3  N540-FAN OPERATIONAL  NSHUT
```

すべての RP が表示され、それぞれの状態が OPERATIONAL であることを確認します。これは、XR コンソールがカード上で動作していることを示します。

ステップ 2 admin

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 3 showplatform

例：

```
sysadmin-vm:0_RP0#show platform
```

システム管理 EXEC モードで **show platform** コマンドを実行すると、ルータ上のカード（RP、FC）、およびハードウェア モジュール（ファン トレイ）などのすべてのハードウェア ユニットのステータスが表示されます。

次に、単一シャーシ システムでの例を示します。

```
RP/0/RP0/CPU0:<router>#sh platform
Thu Mar 29 06:50:06.788 UTC
Location  Card Type  HW State  SW State  Config State
------------------------------------------------------------------------------
0/RP0  N540-X-24Z8Q2C-M OPERATIONAL  OPERATIONAL  NSHUT
0/FT0  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT1  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT2  N540-FAN   OPERATIONAL  N/A    NSHUT
0/FT3  N540-FAN   OPERATIONAL  N/A    NSHUT
```

ルータに取り付けられたすべてのカードが結果に表示されていることを確認します。LC および RP のソフトウェア ステータスと FC および FT のハードウェア ステータスは、「OPERATIONAL」である必要があります。ハードウェアおよびソフトウェアの各状態を次に示します。

ハードウェアの状態

- OPERATIONAL：カードは正常に動作しており、完全に機能します。
- POWERED_ON：電源がオンで、カードが起動しています。
- FAILED：カードは電源がオンになっていますが、内部障害が発生しています。
- PRESENT：カードはシャットダウン状態です。
- OFFLINE：ユーザによってカードの状態がオフラインに変更されています。診断のためにカードにアクセスできます。

ソフトウェアの状態

- OPERATIONAL：ソフトウェアは正常に動作しており、完全に機能します。
- SW_INACTIVE：ソフトウェアは完全には動作していません。
- FAILED：ソフトウェアは動作していますが、カードに内部障害が発生しています。

ソフトウェア バージョンの確認

ルータには、プリインストールされた Cisco IOS XR ソフトウェアが付属しています。ソフトウェアの最新バージョンがインストールされていることを確認します。新しいバージョンを使用できる場合は、システムアップグレードを実行してください。これにより新しいバージョンのソフトウェアがインストールされ、ルータに最新の機能セットが提供されます。

ルータで実行されている Cisco IOS XR ソフトウェアのバージョンを確認するには、次のタスクを実行します。

手順

showversion

例：

```
RP/0/RP0/CPU0:router# show version
```

ルータにインストールされている各種ソフトウェア コンポーネントのバージョンを表示します。結果には、Cisco IOS XR ソフトウェアとその各種コンポーネントのバージョンが含まれます。

例

```
Cisco IOS XR Software, Version 6.3.2
Copyright (c) 2013-2017 by Cisco Systems, Inc.

Build Information:
Built By : ahoang
Built On : Mon Mar 26 04:22:21 PDT 2018
Build Host : iox-ucs-030
Workspace : /auto/srcarchive17/prod/6.3.2/ncs540/ws
Version : 6.3.2
Location : /opt/cisco/XR/packages/

cisco NCS-540 () processor
System uptime is 1 day, 16 hours, 18 minutes
```

次のタスク

結果を確認して、システム アップグレードまたは追加のパッケージ インストールが必要かどうかを特定します。必要な場合は、「システム アップグレードの実行および機能パッケージのインストール （29 ページ）」の章のタスクを参照してください。

ファームウェア バージョンの確認

ルータのさまざまなハードウェア コンポーネントのファームウェアは、インストールされている Cisco IOS XR イメージと互換性がある必要があります。互換性がないと、ルータの誤動作を引き起こす可能性があります。ファームウェア バージョンを確認するには、次のタスクを実行します。

手順

showhw-module fpd

例：

ルータで検出されたハードウェア モジュールのリストを表示します。

（注）　このコマンドは、XR LXC とシステム管理 LXC の両方のモードで実行できます。

上記の出力で重要なフィールドは次のとおりです。

- FPD Device：FPD、CFP などのハードウェア コンポーネントの名前。
- ATR：ハードウェア コンポーネントの属性。次のような属性があります。
  - B：バックアップ イメージ
  - S：セキュア イメージ
  - P：保護されたイメージ
- Status：ファームウェアのアップグレード ステータス。それぞれの状態については次のとおりです。
  - CURRENT：ファームウェア バージョンは最新バージョンです。
  - READY：FPD のファームウェアはアップグレード可能な状態です。
  - NOT READY：FPD のファームウェアはアップグレード可能な状態ではありません。
  - NEED UPGD：インストール済みのイメージで新しいファームウェア バージョンを利用できます。アップグレードすることが推奨されます。
  - RLOAD REQ：アップグレードが完了しており、ISO イメージのリロードが必要です。
  - UPGD DONE：ファームウェア アップグレードが正常に行われました。

- UPGD FAIL：ファームウェア アップグレードが失敗しました。
- BACK IMG：ファームウェアが破損しています。ファームウェアを再インストールしてください。
- UPGD SKIP：インストール済みファームウェアのバージョンが、イメージで利用可能なバージョンよりも上位であるため、アップグレードがスキップされました。

- Running：FPD で現在実行中のファームウェアのバージョン。

次のタスク

- システム管理 EXEC モードで **upgrade hw-module location all fpd** コマンドを使用して、必要なファームウェアをアップグレードします。個々の FPD を選択して更新することも、すべてをまとめて更新することもできます。FPD アップグレードを有効にするには、ルータの電源を再投入する必要があります。
- 必要に応じて、自動 FPD アップグレード機能を有効にします。有効にするには、システム管理コンフィギュレーション モードで **fpdauto-upgradeenable** コマンドを使用します。有効にすると、ルータにインストールされているイメージに新しい FPD バイナリが存在する場合、システムのアップグレード処理中に FPD が自動的にアップグレードされます。

インターフェイス ステータスの確認

ルータが起動すると、使用可能なすべてのインターフェイスがシステムによって検出されます。インターフェイスが検出されない場合、ユニットの異常を示している可能性があります。検出されたインターフェイスの数を確認するには、次のタスクを実行します。

手順

showipv4interfacesummary

例：

```
RP/0/RP0/CPU0:router#show ipv4 interface summary
```

ルータの初回起動時には、すべてのインターフェイスが「未割り当て」の状態です。結果に表示されるインターフェイスの総数が、ルータに存在するインターフェイスの実際の数と一致することを確認してください。

上記の結果について説明します。

- Assigned：IP アドレスがインターフェイスに割り当てられています。
- Unnumbered：ルータの他のインターフェイスにすでに設定された IP アドレスを借用しているインターフェイスです。

• Unassigned：IP アドレスはインターフェイスに割り当てられていません。

XR EXEC モードで **show interfaces brief** および **show interfaces summary** コマンドを使用して、インターフェイス ステータスを確認することもできます。

SDR 情報の確認

セキュア ドメイン ルータ（SDR）は、単一の物理システムを論理的に独立した複数のルータに分割します。SDR は論理ルータ（LR）とも呼ばれます。ルータでは 1 つの SDR のみがサポートされます。この SDR をデフォルト SDR と呼びます。すべてのルータには、ルーティング システムにインストールされている RP をすべて所有するデフォルト SDR が付属しています。この SDR のインスタンスはすべてのノードで実行されます。SDR インスタンスの詳細を確認するには、次のタスクを実行します。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **showsdr**

例：

```
sysadmin-vm:0_RP0# show sdr
```

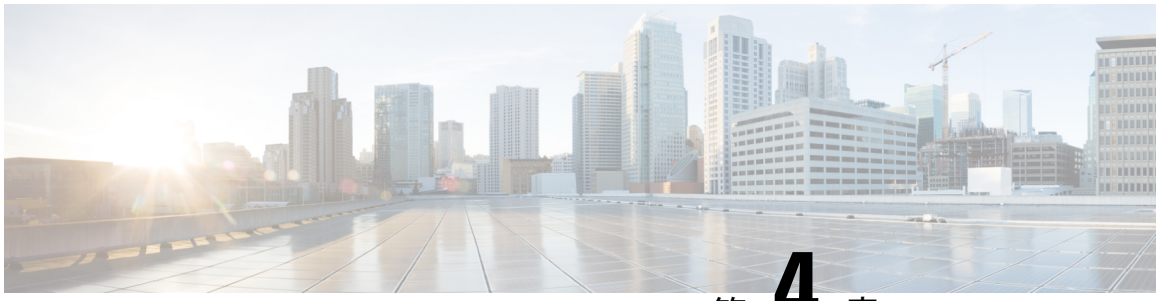
各ノードの SDR 情報が表示されます。

```
RP/0/RP0/CPU0:router#show  sdr
Type                 NodeName       NodeState      RedState       PartnerName
------------------------------------------------------------------------------
LC                   0/0/CPU0       IOS XR RUN     N/A            N/A
RP                   0/RP0/CPU0     IOS XR RUN     ACTIVE         NONE
Slice                0/RP0/NPU0     UP             N/A            N/A
N540-X-24Z8Q2C-M     0/RP0          OPERATIONAL                   N/A
N540-FAN             0/FT0          OPERATIONAL                   N/A
N540-FAN             0/FT1          OPERATIONAL                   N/A
N540-FAN             0/FT2          OPERATIONAL                   N/A
N540-FAN             0/FT3          OPERATIONAL                   N/A
```

機能 SDR では、VM の状態は「RUNNING」です。SDR がノードで動作していない場合、結果の該当箇所に出力が表示されません。ノードはコア ダンプを実行する場合があります。コア ダンプの実行中は、VM の状態が「Paused & Core Dump in Progress」になります。

次のタスク

SDR がノードで動作していない場合は、ノードのリロードを試してください。これを行うには、システム管理 EXEC モードで **hw-modulelocation** *node-id***reload** コマンドを使用します。



第 4 章

ユーザ プロファイルの作成および権限の割り当て

ルータ上のシステム管理設定へのアクセス権を管理するには、権限を割り当てたユーザ プロファイルを作成します。権限はコマンド ルールとデータ ルールを使用して指定します。ユーザ、グループ、コマンド ルール、およびデータ ルールを作成するには、認証、認可、およびアカウンティング（AAA）コマンドをシステム管理コンフィギュレーション モードで使用します。aaa コマンドはディザスタ リカバリ パスワードを変更する際にも使用します。

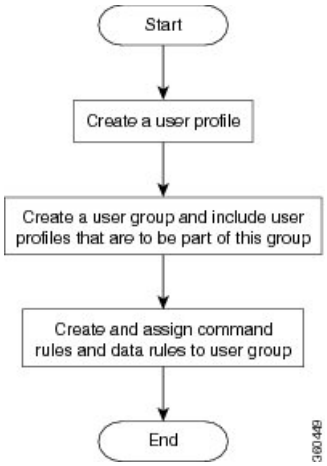
（注） システム管理LXCから外部AAAサーバおよびサービスを設定することはできません。その設定はXR LXC からのみ実行できます。

ユーザが制御されていないアクセスを行うのを制限するためにAAA認証を設定します。AAA認証が設定されていない場合、ユーザに割り当てられたグループに関連付けられたコマンドおよびデータ ルールはバイパスされます。IOS-XR ユーザは、ネットワーク設定プロトコル（NETCONF）、Google 定義のリモート プロシージャ コール（gRPC）または任意の YANG ベースのエージェントを介して、IOS-XR設定への完全な読み取り/書き込みアクセス権を持つことができます。制御されていないアクセスを許可しないようにするには、いずれかの設定を行う前に AAA 認証を有効にします。

ユーザの認証にはユーザ名とパスワードが使用されます。認証されたユーザは、ユーザ グループに対して作成および適用されているコマンド ルールとデータ ルールに基づいて、コマンドを実行しデータ要素にアクセスする権利が与えられます。ユーザ グループに属するすべてのユーザには、そのユーザ グループのコマンド ルールおよびデータ ルールで定義されているシステムへのアクセス権があります。

ユーザ プロファイルを作成するためのワークフローを次のフローチャートに示します。

図 *1:* ユーザ プロファイル作成のワークフロー



（注） ルータの初回起動時に作成された XR LXC の root-lr ユーザは、システム管理 LXC の root-system ユーザにマッピングされます。root-system ユーザにはシステム管理 LXC のスーパーユーザ権限があるため、アクセスは制限されません。

既存の AAA 設定を表示するには、システム管理コンフィギュレーション モードで **show run aaa** コマンドを使用します。

この章で説明する内容は次のとおりです。

ユーザ プロファイルの作成

システム管理 LXC の新しいユーザを作成します。ユーザはユーザ グループに含まれ、特定の権限が割り当てられます。ユーザは割り当てられた権限に基づいて、システム管理 LXC コンソールのコマンドと設定への制限付きアクセス権を持ちます。

ルータでは、最大で 1024 個のユーザ プロファイルがサポートされます。

（注） システム管理 LXC で作成したユーザは、XR LXC で作成したユーザとは異なります。したがって、システム管理 LXC ユーザのユーザ名とパスワードを使用して XR LXC にアクセスすることはできません。逆も同様です。

XR LXC の root-lr ユーザがシステム管理 LXC にアクセスするには、XR EXEC モードで **Admin** コマンドを入力します。ルータではユーザ名とパスワードの入力を求めるプロンプトは表示されません。XR LXC の root-lr ユーザには、システム管理 LXC へのフル アクセス権が提供されます。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション モードを開始します。

ステップ 3 **aaaauthenticationusersuser** *user_name*

例：

```
sysadmin-vm:0_RP0(config)#aaa authentication users user us1
```

新しいユーザを作成し、ユーザ コンフィギュレーション モードを開始します。例では、ユーザ「us1」が作成されます。

ステップ 4 **password** *password*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#password pwd1
```

システム管理 LXC へのログイン時にユーザ認証に使用するパスワードを入力します。

ステップ 5 **uid** *user_id_value*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#uid 100
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 6 **gid** *group_id_value*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#gid 50
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 7 **ssh_keydir** *ssh_keydir*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#ssh_keydir dir1
```

英数字の値を指定します。

ステップ 8 **homedir** *homedir*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#homedir dir2
```

英数字の値を指定します。

ステップ 9 **commit**

次のタスク

- このタスクで作成したユーザを含めるユーザ グループを作成します。ユーザ グループの作成 （20 ページ）を参照してください。
- ユーザ グループに適用するコマンド ルールを作成します。コマンド ルールの作成 （21 ページ）を参照してください。
- ユーザ グループに適用するデータ ルールを作成します。データ ルールの作成 （24 ページ）を参照してください。

ユーザ グループの作成

新しいユーザ グループを作成してコマンド ルールとデータ ルールを関連付けます。コマンド ルールおよびデータ ルールは、ユーザ グループに属するすべてのユーザに適用されます。

ルータでは、最大 32 のユーザ グループがサポートされます。

始める前に

ユーザ プロファイルを作成します。ユーザ プロファイルの作成および権限の割り当て （17 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション モードを開始します。

ステップ 3 **aaaauthenticationgroupsgroup** *group_name*

例：

```
sysadmin-vm:0_RP0(config)#aaa authentication groups group gr1
```

新しいユーザ グループ（まだ存在していない場合）を作成して、グループ コンフィギュレーション モードを開始します。この例では、ユーザ グループ「gr1」が作成されます。

（注） デフォルトで、root ユーザの作成時にユーザ グループ「root-system」がシステムによって作成されます。root ユーザはこのユーザ グループのメンバです。このグループに追加されたユーザは root ユーザ権限を取得します。

ステップ 4 **users** *user_name*

例：

```
sysadmin-vm:0_RP0(config-group-gr1)#users us1
```

ユーザ グループに含めるユーザの名前を指定します。

複数のユーザ名を二重引用符で囲んで指定することができますたとえば、**users** "*user1 user2 ...*" などです。

ステップ 5 **gid** *group_id_value*

例：

```
sysadmin-vm:0_RP0(config-group-gr1)#gid 50
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 6 **commit**

次のタスク

- コマンド ルールを作成します。コマンド ルールの作成 （21 ページ）を参照してください。
- データ ルールを作成します。データ ルールの作成 （24 ページ）を参照してください。

コマンド ルールの作成

コマンド ルールとは、ユーザ グループ内のどのユーザが特定のコマンドの使用を許可または拒否されるかに基づいたルールです。コマンド ルールはユーザ グループに関連付けられ、そのユーザ グループに属するすべてのユーザに適用されます。

コマンドでの動作を許可するか拒否するかを指定することで、コマンドルールを作成します。次の表に、有効な動作と権限の組み合わせを示します。

動作	承認権限	拒否権限
読み取り（R）	「?」を使用した場合にCLIにコマンドが表示されます。	「?」を使用した場合にCLIにコマンドが表示されません。
実行（X）	CLI からコマンドを実行できます。	CLI からコマンドを実行できません。
読み取りおよび実行（RX）	コマンドが CLI に表示され、実行可能です。	コマンドは CLI に表示されず、実行することもできません。

デフォルトでは、すべての権限が**Reject**に設定されています。

各コマンド ルールは、関連付けられている番号によって識別されます。ユーザ グループに複数のコマンド ルールを適用すると、より小さい番号のコマンド ルールが優先されます。たとえば cmdrule 5 は読み取りアクセスを許可しますが、cmdrule 10 は読み取りアクセスを拒否するとします。これら両方のコマンド ルールを同じユーザ グループに適用すると、cmdrule 5 が優先されるため、このグループのユーザは読み取りアクセス権を持ちます。

このタスクの例として、「show platform」コマンドの読み取りおよび実行権限を拒否するルールを作成します。

始める前に

ユーザ グループを作成します。ユーザ グループの作成 （20 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション モードを開始します。

ステップ 3 **aaaauthorizationcmdrulescmdrule** *command_rule_number*

例：

```
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 1100
```

コマンド ルール番号として数値を指定します。32 ビットの整数を入力できます。

重要　1 ～ 1000 の数字はシスコで予約済みのため使用しないでください。

このコマンドによって、新しいコマンドルール（まだ存在していない場合）が作成され、コマンドルールコンフィギュレーションモードが開始されます。例では、コマンドルール「1100」が作成されます。

（注） デフォルトでは、root-systemユーザの作成時に「cmdrule 1」がシステムによって作成されます。このコマンドルールは、すべてのコマンドの「読み取り」および「実行」動作に対する「承認」権限を提供します。したがって「cmdrule 1」が変更されない限り、root ユーザに課せられる制限はありません。

ステップ 4 **command** *command_name*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#command "show platform"
```

権限を制御するコマンドを指定します。

commandにアスタリスク「*」を入力した場合、そのコマンドルールがすべてのコマンドに適用されることを意味します。

ステップ 5 **ops{r | x|rx}**

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#ops rx
```

権限を指定する必要がある動作を指定します。

- **r** ：読み取り
- **x** ：実行
- **rx** ：読み取りおよび実行

ステップ 6 **action** {**accept** | **accept_log** | **reject**}

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#action reject
```

ユーザがその動作の使用を許可されるか拒否されるかを指定します。

- **accept** ：ユーザはその動作の実行を許可されます。
- **accept_log**：ユーザはその動作の実行を許可され、アクセスの試行がすべて記録されます。
- **reject**：ユーザはその動作の実行を制限されます。

ステップ 7 **group** *user_group_name*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#group gr1
```

コマンド ルールを適用するユーザ グループを指定します。

ステップ 8 **context** *connection_type*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#context *
```

このルールを適用する接続タイプを指定します。接続タイプは*netconf*（ネットワーク設定プロトコル）、*cli*（コマンドライン インターフェイス）、または*xml*（Extensible Markup Language）です。アスタリスク「*」の入力が推奨されます。これは、そのコマンド ルールがすべての接続タイプに適用されることを示します。

ステップ 9 **commit**

次のタスク

データ ルールを作成します。データ ルールの作成 （24 ページ）を参照してください。

データ ルールの作成

データ ルールとは、ユーザ グループ内のどのユーザが設定データ要素へのアクセスとその変更を許可または拒否されるかに基づいたルールです。データ ルールはユーザ グループに関連付けられます。データ ルールは、ユーザ グループに属するすべてのユーザに適用されます。

各データ ルールは、関連付けられている番号によって識別されます。ユーザ グループに複数のデータ ルールを適用すると、より小さい番号のデータ ルールが優先されます。

始める前に

ユーザ グループを作成します。ユーザ グループの作成 （20 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション モードを開始します。

ステップ 3 **aaaauthorizationdatarulesdatarule** *data_rule_number*

例：

```
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 1100
```

データ ルール番号として数値を指定します。32 ビットの整数を入力できます。

重要　1 ～ 1000 の数字はシスコで予約済みのため使用しないでください。

このコマンドによって、新しいデータ ルール（まだ存在していない場合）が作成され、データ ルール コンフィギュレーション モードが開始されます。例では、データ ルール「1100」が作成されます。

（注）　デフォルトで、root-system ユーザの作成時に「datarule 1」がシステムによって作成されます。このデータ ルールは、すべての設定データの「読み取り」、「書き込み」、および「実行」動作に対する「承認」権限を提供します。したがって「datarule 1」が変更されない限り、root ユーザに課せられる制限はありません。

ステップ 4　**keypath** *keypath*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#keypath  /aaa/disaster-recovery
```

データ要素のキーパスを指定します。キーパスはデータ要素の場所を定義する式です。**keypath** にアスタリスク「*」を入力した場合、そのコマンド ルールがすべての設定データに適用されることを意味します。

ステップ 5　**ops** 動作

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#ops rw
```

権限を指定する必要がある動作を指定します。各動作は次の文字で識別されます。

- c：作成
- d：削除
- u：更新
- w：書き込み（作成、更新、および削除の組み合わせ）
- r：読み込み
- x：実行

ステップ 6　**action** {**accept** | **accept_log** | **reject**}

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#action reject
```

ユーザがその動作を許可されるか拒否されるかを指定します。

- **accept** ：ユーザはその動作の実行を許可されます。
- **accept_log**：ユーザはその動作の実行を許可され、アクセスの試行がすべて記録されます。
- **reject**：ユーザはその動作の実行を制限されます。

ステップ 7　**group** *user_group_name*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#group gr1
```

データ ルールを適用するユーザ グループを指定します。複数のグループ名を指定することもできます。

ステップ 8 **context** 接続タイプ

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#context *
```

このルールを適用する接続タイプを指定します。接続タイプは*netconf*（ネットワーク設定プロトコル）、*cli*（コマンドライン インターフェイス）、または*xml*（Extensible Markup Language）です。アスタリスク「*」の入力が推奨されます。これは、そのコマンドがすべての接続タイプに適用されることを示します。

ステップ 9 **namespace** 名前空間

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#namespace *
```

アスタリスク「*」を入力して、データ ルールが名前空間の値すべてに適用されることを示します。

ステップ 10 **commit**

ディザスタ リカバリのユーザ名とパスワードの変更

ルータの起動後、最初にroot-systemユーザ名とパスワードを定義すると、同じユーザ名とパスワードがシステム管理コンソールのディザスタ リカバリ ユーザ名およびパスワードとしてマッピングされます。ただし、これらは変更可能です。

ディザスタ リカバリ ユーザ名およびパスワードは、次の状況で役立ちます。

- システム管理コンソールでの認証のデフォルト ソースである AAA データベースが破損した場合にシステムへアクセスする。
- 何らかの理由でシステム管理コンソールが機能しない場合に、管理ポートを通じてシステムにアクセスする。
- 通常のユーザ名およびパスワードを忘れた場合に、ディザスタ リカバリ ユーザ名とパスワードを使用してシステム管理コンソールにアクセスし、新しいユーザを作成する。

（注） ルータでは、ディザスタ リカバリ ユーザ名およびパスワードを一度に1つのみ設定できます。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/CPU0:router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション モードを開始します。

ステップ 3 **aaadisaster-recoveryusername** *username***password** *password*

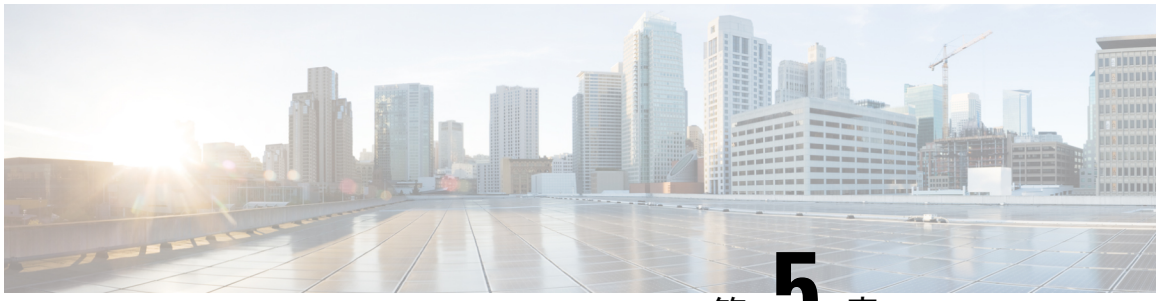
例：

```
sysadmin-vm:0_RP0(config)#aaa disaster-recovery username us1 password pwd1
```

ディザスタ リカバリ ユーザ名とパスワードを指定します。既存のユーザをディザスタ リカバリ ユーザとして選択する必要があります。この例では、ディザスタ リカバリ ユーザとして「us1」が選択され、パスワード「pwd1」が割り当てられます。パスワードは、プレーンテキストまたは MD5 ダイジェスト文字列として入力することができます。

ディザスタ リカバリ ユーザ名を使用する場合は、*username***@localhost** の形式で入力してください。

ステップ 4 **commit**



第 5 章

システム アップグレードの実行および機能パッケージのインストール

システム アップグレードおよびパッケージ インストール プロセスを実行するには、ルータで **install** コマンドを使用します。これらのプロセスでは、iso イメージ（*.iso*）、機能パッケージ（*.rpm*）、およびソフトウェア メンテナンス アップグレード ファイル（*.smu*）をルータ上で追加およびアクティブ化します。ネットワーク サーバからこれらのファイルにアクセスし、ルータ上でアクティブ化します。インストールしたパッケージまたは SMU が原因でルータに問題が発生した場合は、アンインストールすることができます。

この章で説明する内容は次のとおりです。

システムのアップグレード

システムのアップグレードとは、ルータに新しいバージョンの Cisco IOS XR オペレーティング システムをインストールするプロセスです。ルータには Cisco IOS XR イメージがプリインストールされています。ただし、ルータ機能を最新の状態に保つために新しいバージョンをインストールすることができます。システム アップグレードの操作は XR LXC から実行しますが、システム アップグレード時に、XR LXC とシステム管理 LXC の両方で動作しているオペレーティング システムがアップグレードされます。

（注） ルータ上のインターフェイスに設定が行われておらず、no-shut 操作を実行して起動した場合、ルータのリロード時にインターフェイスの状態が自動的に **admin-shutdown** に変更されます。

システム アップグレードは、基本パッケージ（Cisco IOS XR ユニキャスト ルーティング コア バンドル）のインストールによって行います。このバンドルのファイル名は *ncs540-mini-x.iso-6.3.2.36I* です。この ISO イメージは、**install** コマンドを使用してインストールします。インストール プロセスの詳細については、インストール プロセスのワークフロー（31 ページ）を参照してください。

注意 ルータのリロード時はインストール操作を実行しないでください。

システムのアップグレードおよび RPM の詳細については、『*Cisco IOS XR Flexible Packaging Configuration Guide*』を参照してください。

機能のアップグレード

機能のアップグレードとは、ルータに新機能とソフトウェア パッチを導入するプロセスです。機能アップグレードは、パッケージファイル（単にパッケージと呼ばれます）のインストールによって行います。ソフトウェア パッチのインストールはソフトウェア メンテナンス アップグレード（SMU）ファイルのインストールによって行います。

ルータにパッケージをインストールすると、そのパッケージに含まれる特定の機能がインストールされます。Cisco IOS XR ソフトウェアはさまざまなソフトウェア パッケージに分割されているため、ルータで実行する機能を選択することができます。各パッケージには、ルーティングやセキュリティなど、特定のルータ機能のセットを実行するコンポーネントが含まれています。

たとえばルーティング パッケージのコンポーネントは、BGP や OSPF など、個別の RPM に分かれています。BGP は必須 RPM であり、基本ソフトウェア バージョンに含まれているので削除できません。OSPF などの任意の RPM は、必要に応じて追加および削除できます。

パッケージの命名規則は `<platform>-<pkg>-<pkg version>-<release version>.<architecture>.rpm` です。標準パッケージは次のとおりです。

- ncs540-mpls-1.0.0.0-r63236I.x86_64.rpm
- ncs540-isis-1.0.0.0-r63236I.x86_64.rpm
- ncs540-mcast-1.0.0.0-r63236I.x86_64.rpm
- ncs540-mgbl-1.0.0.0-r63236I.x86_64.rpm
- ncs540-bgp-1.0.0.0-r63236I.x86_64.rpm
- ncs540-ospf-1.0.0.0-r63236I.x86_64.rpm
- ncs540-mpls-te-rsvp-1.0.0.0-r63236I.x86_64.rpm
- ncs540-li-1.0.0.0-r63236I.x86_64.rpm
- ncs540-eigrp-1.0.0.0-r63236I.x86_64.rpm
- ncs540-k9sec-1.0.0.0-r63236I.x86_64.rpm

パッケージおよびSMUのインストールは、**install**コマンドを使用して実行します。インストール プロセスの詳細については、パッケージのインストール （31 ページ）を参照してください。

XR LXC とシステム管理 LXC 用の個別のパッケージおよび SMU があります。それぞれをそのファイル名で識別できます。

システムのアップグレードおよび RPM の詳細については、『*Cisco IOS XR Flexible Packaging Configuration Guide*』を参照してください。

インストール プロセスのワークフロー

インストールおよびアンインストールプロセスのワークフローについては、次のフローチャートを参照してください。

パッケージのインストールについては、パッケージのインストール （31 ページ）を参照してください。パッケージのアンインストールについては、パッケージのアンインストール （39 ページ）を参照してください。

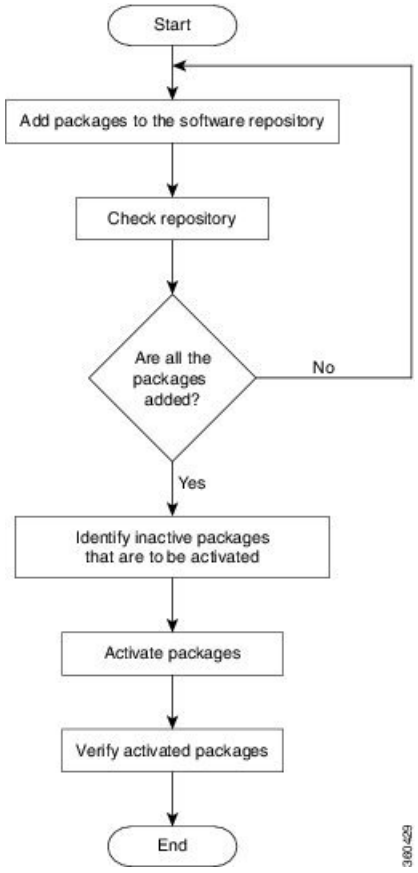
パッケージのインストール

システムをアップグレードするか、パッチをインストールするには、このタスクを完了します。システム アップグレードは ISO イメージ ファイルを使用して行いますが、パッチ インストールの場合はパッケージおよび SMU を使用します。*.rpm* ファイルをインストールする際もこのタスクを使用します。*.rpm* ファイルには、1 つのファイルに統合された複数のパッケージと SMU が含まれています。カード タイプにかかわらず、パッケージ形式によってコンポーネントごとに 1 つの RPM が定義されます。

（注） システム管理パッケージおよびXRパッケージは、システム管理EXECモードとXR EXECモードで**install**コマンドを使用して実行できます。すべての**install**コマンドは両方のモードで使用できます。

パッケージをインストールするためのワークフローを次のフローチャートに示します。

図 *2:* パッケージ インストールのワークフロー



始める前に

- 管理ポートを設定して接続します。インストール可能なファイルには管理ポートからアクセスできます。管理ポートの設定の詳細については、管理ポートの設定 （6 ページ） を参照してください。
- インストールするパッケージを、ルータのハードディスク、またはルータがアクセスできるネットワーク サーバにコピーします。

手順

ステップ 1 次のいずれかを実行します。

- **install add source** *<tftp transfer protocol>/package_path/ filename1 filename2 ...*
- **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path/ filename1 filename2 ...*

例：

```
RP/0/RP0/CPU0:router#install add source
/harddisk:/ncs540-mpls-te-rsvp-1.0.0.0-r63236I.x86_64.rpm
ncs540-mgbl-1.0.0.0-r63236I.x86_64.rpm
```

または

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
```

```
RP/0/RP0/CPU0:router#install add source
/harddisk:/ncs540-mpls-te-rsvp-1.0.0.0-r63236I.x86_64.rpm
ncs540-mgbl-1.0.0.0-r63236I.x86_64.rpm
```

または

```
RP/0/RP0/CPU0:router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
ncs540-mcast-1.0.0.0-r63236I.x86_64.rpm
 ncs540-mpls-1.0.0.0-r63236I.x86_64.rpm
```

（注） *package_path* と *filename* の間にはスペースが必要です。

パッケージからソフトウェア ファイルが展開され、ソフトウェア リポジトリに追加されます。追加するファイルのサイズによっては、この処理に時間がかかる場合があります。動作は非同期モードで実行されます。**install add** コマンドはバックグラウンドで実行され、EXEC プロンプトは最短で返されます。

（注） XR LXC とシステム管理 LXC のリポジトリは異なります。ルーティング パッケージは XR LXC リポジトリに、システム管理パッケージはシステム管理 LXC リポジトリに自動的に追加されます。

ステップ 2 show install request

例：

```
RP/0/RP0/CPU0:router#show install request
```

（任意）追加動作の動作 ID とステータスを表示します。動作 ID は、後で **activate** コマンドを実行する際に使用できます。

```
Install operation 8 is still in progress
```

システム管理パッケージの場合は、残りの手順をシステム管理 EXEC モードで実行する必要があります。システム管理 EXEC モードを開始するには、**admin** コマンドを使用します。

ステップ 3 show install repository

例：

```
RP/0/RP0/CPU0:router#show install repository
```

リポジトリに追加されるパッケージを表示します。パッケージは `install add` 動作の完了後にのみ表示されます。

ステップ 4 show install inactive

例：

```
RP/0/RP0/CPU0:router#show install inactive
```

リポジトリ内に存在する非アクティブなパッケージを表示します。アクティブ化できるのは非アクティブなパッケージだけです。

ステップ 5 次のいずれかを実行します。

- **install activate** *package_name*
- **install activate id** *operation_id*

例：

```
RP/0/RP0/CPU0:router#install activate ncs540-mcast-1.0.0.0-r63236I.x86_64.rpm
ncs540-mpls-1.0.0.0-r63236I.x86_64.rpm
```

operation_id は **install add** 動作の ID です。このコマンドは、システム管理モードでも実行できます。パッケージ設定がルータでアクティブになります。その結果、新機能とソフトウェア修正が有効になります。この動作は非同期モードで実行されます。**install activate** コマンドはバックグラウンドで実行され、EXEC プロンプトが返されます。

（注） 上位バージョンの RPM をアクティブ化した後で、下位バージョンの RPM のアクティブ化が必要になった場合は、force オプションを使用します。次に例を示します。

従来の方法を使用して下位バージョンの RPM をリポジトリに追加し、アクティベーションを強制します。

```
install add source repository ospf-1.0.0.0-r6006I.rpm
```

```
install activate ospf-1.0.0.0-r6006I.rpm force
```

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージがまとめてアクティブ化されます。たとえば 5 つのパッケージが動作 8 に追加されている場合、**install activate id 8** を実行すると、5 つのパッケージがすべてまとめてアクティブ化されます。パッケージを個別にアクティブ化する必要はありません。

アクティベーションは瞬時には完了せず、ある程度の時間がかかります。SMU によっては、アクティベーション時にルータの手動リロードが必要な場合があります。このような SMU をアクティブ化すると、リロードを実行するための警告メッセージが表示されます。SMU のコンポーネントは、リロードの完了後にのみアクティブ化されます。**install activate** コマンドの実行後すぐにルータをリロードします。SMU が XR LXC とシステム管理 LXC の両方と依存関係がある場合は、両方の LXC で SMU をアクティブ化した後でリロードを実行すると、両方で同時に反映されます。ルータをリロードするには、システム管理 EXEC モードで **hw-module location all reload** コマンドを使用します。

ステップ 6 **show install active**

例：

```
RP/0/RP0/CPU0:router#show install active
```

アクティブなパッケージを表示します。

この結果で、すべての RP と LC でイメージおよびパッケージの同じバージョンがアクティブになっていることを確認します。

ステップ 7 **install commit**

例：

```
RP/0/RP0/CPU0:router#install commit
```

XR の新たにアクティブ化されたソフトウェアをコミットします。XR とシステム管理の両方のソフトウェアをコミットするには、**install commit system** を使用します。

パッケージのインストール：関連コマンド

関連コマンド	目的
show install log	インストールプロセスのログ情報を表示します。これはインストールが失敗した場合のトラブルシューティングに使用できます。
show install package	リポジトリに追加されたパッケージの詳細を表示します。このコマンドは、パッケージの個々のコンポーネントを識別する際に使用します。
install prepare	アクティベーションの準備として、非アクティブなパッケージに対してアクティベーション前のチェックを実行します。
show install prepare	準備が完了してアクティベーション可能になったパッケージのリストを表示します。

次のタスク

- システムアップグレードを実行した後は、システム管理EXECモードで**upgrade hw-module location all fpd all** コマンドを使用して FPD をアップグレードします。FPD アップグレード プロセスの進行状況は、システム管理 EXEC モードで **show hw-module fpd** コマンドを使用してモニタできます。FPDアップグレードが完了したら、ルータをリロードします。
- **install verify packages** コマンドを使用してインストールを確認します。
- インストールによってルータに問題が発生した場合は、該当するパッケージまたは SMU をアンインストールしてください。パッケージのアンインストール （39 ページ）を参照してください。

（注） ISOイメージはアンインストールできません。ただし、旧バージョンのISOをインストールすることでシステムダウングレードを実行することができます。

準備済みパッケージのインストール

システムアップグレードまたは機能アップグレードは、ISOイメージファイル、パッケージ、およびSMUをアクティブ化することで実行します。アクティベーション前にこれらのインストール可能なファイルを準備することができます。準備フェーズでは、アクティベーション前のチェックが行われ、インストール可能なファイルのコンポーネントがルータ設定にロードされます。準備プロセスはバックグラウンドで実行されるため、その間もルータをフルに利用できます。準備フェーズが完了したら、すべての準備済みファイルを即座にアクティブ化できます。アクティベーション前の準備には、次の利点があります。

- インストール可能なファイルが破損していると、準備プロセスは失敗します。これによって問題が早期に警告されます。破損したファイルが直接アクティブ化されると、ルータの誤動作を招く可能性があります。
- システム アップグレード用のISOイメージを直接アクティブ化するには時間がかかり、その間にルータを使用できなくなります。ただし、アクティベーション前にイメージを準備すると、準備プロセスが非同期で実行されるだけでなく、準備済みのイメージを後でアクティブ化するときに、アクティベーション プロセスにかかる時間も著しく短縮されます。その結果、ルータのダウンタイムが大幅に削減されます。

システムのアップグレードおよびパッケージのインストールに準備動作を利用するには、次のタスクを実行します。

（注） システム管理パッケージまたはXRパッケージのどちらをインストールするかによって、それぞれシステム管理EXECモードまたはXR EXECモードで**install**コマンドを実行します。すべての**install**コマンドは両方のモードで使用できます。システム管理のインストール動作はXRモードで実行できます。

始める前に

- インストール可能なファイルが破損していると、準備プロセスは失敗します。これによって問題が早期に警告されます。破損したファイルが直接アクティブ化されると、ルータの誤動作を招く可能性があります。
- システム アップグレード用のISOイメージを直接アクティブ化するには時間がかかり、その間にルータを使用できなくなります。ただし、アクティベーション前にイメージを準備すると、準備プロセスが非同期で実行されるだけでなく、準備済みのイメージを後でアクティブ化するときに、アクティベーション プロセスにかかる時間も著しく短縮されます。その結果、ルータのダウンタイムが大幅に削減されます。

手順

ステップ1 必要なISOイメージおよびパッケージをリポジトリに追加します。

詳細については、パッケージのインストール （31 ページ）を参照してください。

ステップ 2 **show install repository**

例：

```
RP/0/RP0/CPU0:router#show install repository
```

必要なインストール可能ファイルがリポジトリ内にあることを確認するには、この手順を実行します。パッケージは「install add」動作の完了後にのみ表示されます。

ステップ 3 次のいずれかを実行します。

- **install prepare** *package_name*
- **install prepare id** *operation_id*

例：

準備プロセスが開始されます。この動作は非同期モードで実行されます。**install prepare** コマンドはバックグラウンドで実行され、EXEC プロンプトは最短で返されます。

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージの準備がまとめて行われます。たとえば 5 つのパッケージが動作 8 に追加されている場合、**install prepare id 8** を実行すると、5 つのパッケージの準備がすべてまとめて行われます。パッケージを個別に準備する必要はありません。

ステップ 4 **show install prepare**

例：

```
RP/0/RP0/CPU0:router#show install prepare
```

準備済みのパッケージを表示します。この結果で、必要なすべてのパッケージが準備されていることを確認します。

ステップ 5 **install activate**

例：

```
RP/0/RP0/CPU0:router#install activate
```

準備の完了したすべてのパッケージをまとめてアクティブ化し、ルータでパッケージ設定をアクティブにします。

（注） CLI でパッケージ名または動作 ID を指定しないでください。

SMU によっては、アクティベーション時にルータの手動リロードが必要な場合があります。このような SMU をアクティブ化すると、リロードを実行するための警告メッセージが表示されます。SMU のコンポーネントは、リロードの完了後にのみアクティブ化されます。**install activate** コマンドの完了後すぐにルータのリロードを実行します。

ステップ 6 **show install active**

例：

```
RP/0/RP0/CPU0:router#show install active
```

アクティブなパッケージを表示します。

この結果で、すべての RP と LC でイメージおよびパッケージの同じバージョンがアクティブになっていることを確認します。

ステップ 7 **install commit**

例：

```
RP/0/RP0/CPU0:router#install commit
```

パッケージのインストール：関連コマンド

関連コマンド	目的
show install log	インストールプロセスのログ情報を表示します。これはインストールが失敗した場合のトラブルシューティングに使用できます。
show install package	リポジトリに追加されたパッケージの詳細を表示します。このコマンドは、パッケージの個々のコンポーネントを識別する際に使用します。
install prepare clean	準備動作をクリアし、すべてのパッケージを準備済み状態から削除します。

次のタスク

- システムアップグレードを実行した後は、システム管理EXECモードで**upgrade hw-module location all fpd all** コマンドを使用して FPD をアップグレードします。FPD アップグレード プロセスの進行状況は、システム管理 EXEC モードで **show hw-module fpd** コマンドを使用してモニタできます。FPDアップグレードが完了したら、ルータをリロードします。
- **install verify packages** コマンドを使用してインストールを確認します。
- インストールによってルータに問題が発生した場合は、該当するパッケージまたは SMU をアンインストールしてください。パッケージのアンインストールを参照してください。

（注） ISOイメージはアンインストールできません。ただし、旧バージョンのISOをインストールすることでシステム ダウングレードを実行することができます。

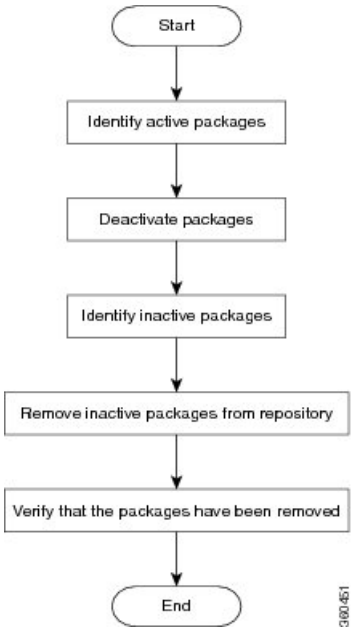
パッケージのアンインストール

パッケージをアンインストールするには、次のタスクを実行します。アンインストールしたパッケージに含まれるすべてのルータ機能は非アクティブ化されます。XR LXC で追加したパッケージをシステム管理LXCからアンインストールすることはできません。逆も同様です。

（注） インストール済みの ISO イメージはアンインストールできません。また、ホスト、XR LXC、およびシステム管理 LXC でサード パーティ製 SMU をインストールするカーネル SMU もアンインストールできません。ただし、ISO イメージまたはカーネル SMU を新たにインストールすると既存のインストールが上書きされます。

パッケージをアンインストールするためのワークフローを次のフローチャートに示します。

図 *3:* パッケージ アンインストールのワークフロー



このタスクでは、XR LXC パッケージをアンインストールします。システム管理パッケージをアンインストールする場合は、同じコマンドをシステム管理 EXEC モードで実行します。

手順

ステップ 1 **show install active**

例：

```
RP/0/RP0/CPU0:router#show install active
```

アクティブなパッケージを表示します。非アクティブ化できるのはアクティブなパッケージだけです。

ステップ 2 次のいずれかを実行します。

- **install deactivate** *package_name*
- **install deactivate id** *operation_id*

例：

operation_id は **install add** 動作の ID です。パッケージに関連するすべての機能およびソフトウェアパッチが非アクティブ化されます。複数のパッケージ名を指定して同時に非アクティブ化できます。

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージがまとめて非アクティブ化されます。パッケージを個別に非アクティブ化する必要はありません。**install add** 動作（非アクティブ化で使用した ID の動作）の一部として追加されたシステム管理パッケージがある場合、これらも非アクティブ化されます。

ステップ 3 **show install inactive**

例：

```
RP/0/RP0/CPU0:router#show install inactive
```

非アクティブ化済みのパッケージは、非アクティブなパッケージとして表示されるようになります。非アクティブなパッケージのみリポジトリから削除できます。

ステップ 4 **install remove** *package_name*

例：

非アクティブなパッケージがリポジトリから削除されます。

指定した動作 ID に追加されているすべてのパッケージを削除するには、**id** *operation-id* キーワードおよび引数を指定して **install remove** コマンドを使用します。

ステップ 5 **show install repository**

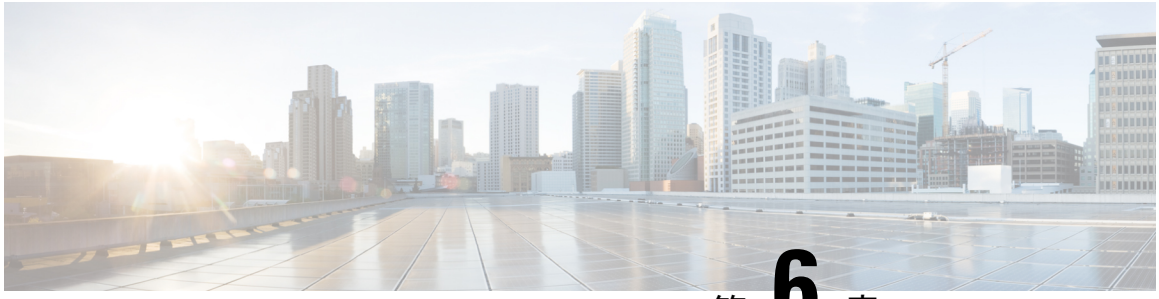
例：

```
RP/0/RP0/CPU0:router#show install repository
```

リポジトリ内の使用可能なパッケージを表示します。削除されたパッケージは結果に表示されなくなります。

次のタスク

必要なパッケージをインストールします。参照先 パッケージのインストール （31 ページ）

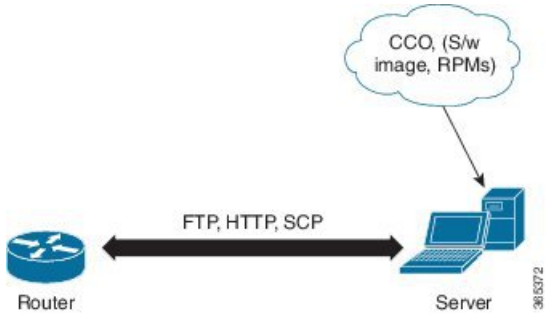


第 6 章

自動依存関係管理

フレキシブル パッケージでは、自動依存関係管理がサポートされます。RPM の更新中に、関連するすべての依存パッケージがシステムによって自動的に特定され、更新されます。

図 *4:* インストール フロー（基本ソフトウェア、*RPM*、および *SMU*）



このリリースまでは、ユーザはネットワーク サーバ（リポジトリ）上の CCO からソフトウェア イメージおよび必要な RPM をダウンロードしていました。また、**install add** コマンドおよび**install activate** コマンドを実行して、ダウンロードしたファイルを に追加し、それらでアクティブ化していました。さらに、関連する依存 RPM を手動で特定し、追加およびアクティブ化する必要がありました。

自動依存関係管理を使用すると、ユーザ側で依存 RPM を特定し、個別に追加およびアクティブ化する必要がありません。また、依存 RPM を自動的に特定し、インストールする新しいインストール コマンドを実行できます。

新しいコマンドは、**install update** コマンドおよび **install upgrade** コマンドです。**install update** コマンドは、依存パッケージを特定し、更新します。このコマンドは、基本パッケージを更新しません。 **install upgrade** コマンドは、基本パッケージをアップグレードします。

これ以降で説明する内容は、次のとおりです。

- RPM と SMU の更新 （42 ページ）
- 基本ソフトウェア バージョンのアップグレード （42 ページ）

RPM と SMU の更新

RPM には特定の不具合に対する修正が含まれており、その修正でシステムを更新する必要があります。RPM および SMU を新しいバージョンに更新するには、**install update** コマンドを使用します。特定の RPM に対して **install update** コマンドが発行されると、ルータによりリポジトリとの間で通信が行われ、RPM がダウンロードされてアクティブ化されます。依存関係にある RPM がリポジトリにある場合、ルータによってその RPM が特定され、インストールされます。

install update コマンドの構文は次のとおりです。

install update source *repository* **[rpm]**

install update コマンドは、次の 4 つの方法で実行できます。

- **パッケージ名を指定しない。**

  パッケージ名を指定しないと、すべてのインストール済みパッケージがコマンドによって最新の SMU で更新されます。

  ```
  install update source [repository]
  ```

- **パッケージ名を指定する。**

  パッケージ名を指定すると、そのパッケージがコマンドによってインストールされ、依存関係とともにそのパッケージの最新の SMU で更新されます。パッケージがすでにインストールされている場合、そのパッケージの SMU だけがインストールされます（すでにインストールされている SMU は、スキップされます）。

- **パッケージ名とバージョン番号を指定する。**

  パッケージの特定のバージョンをインストールする必要がある場合、完全なパッケージ名を指定します。このパッケージは、リポジトリにあるパッケージの最新の SMU とともにインストールされます。

- **SMU を指定する。**

  SMU を指定すると、その SMU は依存関係にある SMU とともにダウンロードおよびインストールされます。

基本ソフトウェア バージョンのアップグレード

基本ソフトウェアは、新しいバージョンが利用可能になった場合に、そのバージョンにアップグレードできます。基本ソフトウェアを最新バージョンにアップグレードするには、**install upgrade** コマンドを使用します。ベース バージョンをアップグレードすると、ルータで現在利用可能な RPM もアップグレードされます。

（注） SMU は、このプロセスの一部としてアップグレードされません。

install upgrade コマンドの構文は次のとおりです。

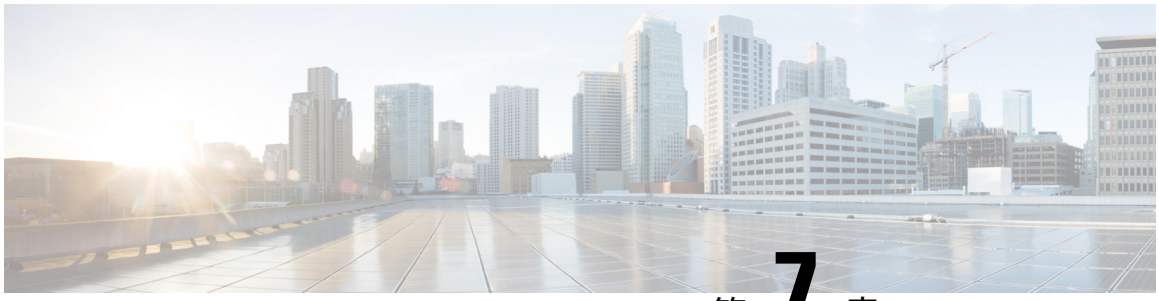
install upgrade source *repository* **version***version* **[rpm]**

次の場合は **install upgrade** コマンドを使用できます。

- **バージョン番号を指定する**

  基本ソフトウェア（.mini）は、特定のバージョンにアップグレードされます。すべてのインストール済み RPM も、同じリリース バージョンにアップグレードされます。

  ```
  install upgrade source [repository] version 6.2.2
  ```



第 7 章

ディザスタ リカバリ

この章で説明する内容は次のとおりです。

USB ドライブを使用した起動

ブート可能な USB ドライブを使用して、システム アップグレードの目的でルータのイメージを再適用したり、起動に失敗した場合にルータを起動したりします。ブート可能な USB ドライブは圧縮ブート ファイルを使用して作成できます。

圧縮ブート ファイルを使用したブート可能な USB ドライブの作成

圧縮ブート ファイルを USB ドライブにコピーすると、ブート可能な USB ドライブが作成されます。圧縮ファイルの内容が展開されると、USB ドライブがブート可能になります。

（注） USB ドライブからの読み込みまたはブートに失敗した場合は、ドライブが正しく挿入されていることを確認してください。ドライブが正しく挿入されていても USB ドライブから読み込めない場合は、別のシステムで USB の内容を確認してください。

このタスクは、ローカル マシンで利用できる Windows、Linux、または MAC オペレーティング システムを使用して実行できます。ここで説明する一般的な手順をそれぞれ実行するための操作は、使用中のオペレーティング システムによって異なります。

始める前に

- ストレージ容量が 8 GB（最小）~32 GB（最大）の USB ドライブにアクセスできるようにします。USB 2.0 および USB 3.0 がサポートされています。
- 圧縮ブート ファイルを cisco.com のソフトウェア ダウンロード ページからローカル マシンにコピーします。圧縮ブート ファイルのファイル名の形式は、 です（例： ）。

手順

ステップ 1 USB ドライブをローカル マシンに接続し、Windows オペレーティング システムまたは Apple MAC ディスク ユーティリティを使用して FAT32 または MS-DOS ファイル システムでフォーマットします。

ステップ 2 圧縮ブート ファイルを USB ドライブにコピーします。

ステップ 3 コピー処理が正常に行われたことを確認します。確認するには、コピー元とコピー先でファイル サイズを比較します。さらに、MD5 チェックサム値を確認します。

ステップ 4 圧縮ブート ファイルを USB ドライブ内で解凍して内容を展開します。これにより、USB ドライブがブート可能なドライブに変換されます。

（注） 圧縮ファイルの内容（「EFI」および「boot」ディレクトリ）は、USB ドライブのルートに直接展開する必要があります。解凍アプリケーションによって展開ファイルが新しいフォルダに配置された場合は、「EFI」および「boot」ディレクトリを USB ドライブのルートに移動してください。

ステップ 5 ローカル マシンから USB ドライブを取り出します。

次のタスク

ブート可能な USB ドライブを使用して、ルータの起動またはイメージのアップグレードを実行します。

iPXE を使用した起動

iPXE は、管理インターフェイスのネットワーク カードに含まれ、ルータのシステム ファームウェア（UEFI）レベルで動作するプリブート実行環境です。iPXE は、システムを再イメージするために使用され、ブートに失敗した場合や有効なブート可能なパーティションがない場合にルータを起動します。iPXE は ISO イメージをダウンロードして、イメージのインストールを進行させ、最後に新しいインストール内でブートストラップを行います。

iPXE はブート ローダとして機能し、システムを起動するイメージをプラットフォーム ID（PID）、シリアル番号、または管理 MAC アドレスに基づいて柔軟に選択できるようにします。iPXE は DHCP サーバのコンフィギュレーション ファイルで定義する必要があります。

ゼロタッチ プロビジョニング

ゼロタッチプロビジョニング（ZTP）は、iPXEを使用してルータでソフトウェアをインストールした後の自動プロビジョニングに役立ちます。

ZTP の自動プロビジョニングでは以下の手順を実行します。

- **設定**：コンフィギュレーション ファイルをダウンロードおよび実行します。ZTP でコンフィギュレーションとして処理されるように、ファイルの最初の行に `!! IOS XR` が含まれている必要があります。
- **スクリプト**：スクリプト ファイルをダウンロードおよび実行します。スクリプト ファイルには、タスクを完了するためのプログラムによるアプローチが含まれています。たとえば IOS XR コマンドを使用して作成されたスクリプトは、パッチ アップグレードを実行します。ZTP でスクリプトとして処理されるように、ファイルの最初の行に `#! /bin/bash` または `#! /bin/sh` が含まれている必要があります。

DHCP サーバの設定

DHCP サーバは、IPv4 か IPv6、またはその両方の通信プロトコルに対して設定する必要があります。次に、Linux システムで実行されている ISC-DHCP サーバの例を示します。

始める前に

- ネットワーク管理者またはシステムの設計担当者に問い合わせて、管理インターフェイスの IP アドレスおよびサブネット マスクを入手します。
- RP の物理ポート イーサネット 0 は管理ポートです。ポートが管理ネットワークに接続されていることを確認します。
- サーバが DHCP パケットを処理できるようにファイアウォールを有効にします。
- DHCPv6 の場合、IPv6 アドレスの取得方法を示すルーティング アドバタイズメント（RA）メッセージをネットワーク内のすべてのノードに送信する必要があります。クライアントが DHCP 要求を送信できるようにルータ アドバタイズ デーモン（radvd。yum install radvd を使用してインストールします）を設定します。次に例を示します。

```
interface eth3
{
        AdvSendAdvert on;
        MinRtrAdvInterval 60;
        MaxRtrAdvInterval 180;
        AdvManagedFlag on;
        AdvOtherConfigFlag on;
        prefix 2001:1851:c622:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };
};
```

- HTTP サーバは DHCP サーバと同じサーバにも、別のサーバにも設定できます。IP アドレスが DHCP サーバから割り当てられた後、ルータは HTTP サーバに接続してイメージをダウンロードします。

手順

ステップ 1 dhcpd.conf ファイル（IPv4、IPv6、または両方の通信プロトコル用）、dhcpv6.conf ファイル（IPv6 用）、またはその両方のファイルを /etc/ または /etc/dhcp ディレクトリに作成します。このコンフィギュレーション ファイルには、スクリプトへのパス、ISO インストール ファイルの場所、プロビジョニング設定ファイルの場所、ルータのシリアル番号、MAC アドレスなどのネットワーク情報が保存されます。

ステップ 2 DHCPサーバが稼働したら、サーバをテストします。たとえば、IPv4の場合は次のようになります。

- ルータの MAC アドレスを使用した場合：

  （注） host ステートメントを使用すると、DNS に使用される固定アドレスが提供されますが、要求内でオプション 77 が iPXE に設定されていることを確認します。このオプションは、必要に応じてブートファイルをシステムに提供するために使用されます。

  上記の設定が正常に行われていることを確認します。
- ルータのシリアル番号を使用した場合：ルータのシリアル番号はBIOSから取得され、IDとして使用されます。

ステップ 3 DHCP を再起動します。

```
killall dhcpd
/usr/sbin/dhcpd -f -q -4 -pf /run/dhcp-server/dhcpd.pid
-cf /etc/dhcp/dhcpd.conf ztp-mgmt &
```

例

次に、dhcpd.conf ファイルの例を示します。

```
allow bootp;
allow booting;
ddns-update-style interim;
option domain-name "cisco.com";
option time-offset -8;
ignore client-updates;
default-lease-time 21600;
max-lease-time 43200;
option domain-name-servers <ip-address-server1>, <ip-address-server2>;
log-facility local0;
 :
subnet <subnet> netmask <netmask> {
  option routers <ip-address>;
  option subnet-mask <subnet-mask>;
  next-server <server-addr>;
}
  :
host <hostname> {
  hardware ethernet e4:c7:22:be:10:ba;
  fixed-address <address>;
```

```
  filename "http://<address>/<path>/<image.bin>";
}
```

次に、dhcpd6.conf ファイルの例を示します。

```
option dhcp6.name-servers <ip-address-server>;
option dhcp6.domain-search "cisco.com";
dhcpv6-lease-file-name "/var/db/dhcpd6.leases";
option dhcp6.info-refresh-time 21600;
option dhcp6.bootfile-url code 59 = string;
subnet6 <subnet> netmask <netmask> {
       range6 2001:1851:c622:1::2 2001:1851:c622:1::9;
        option dhcp6.bootfile-url "http://<address>/<path>/<image.bin>";
```

次のタスク

ZTP を呼び出します。

ZTP の呼び出し

ZTP は XR 名前空間内と、管理インターフェイスおよびラインカードインターフェイスの場合はグローバル VPN ルーティング/転送（VRF）名前空間内で実行されます。

始める前に

DHCP サーバが設定されていることを確認します。詳細については、DHCP サーバの設定 （47 ページ）を参照してください。

手順

dhcpd.conf ファイルを編集して、ZTP の機能を利用します。

次に、iPXE と ZTP を含む DHCP サーバの設定例を示します。

```
host <host-name>
{
hardware ethernet <router-serial-number or mac-id>;
fixed-address <ip-address>;
  if exists user-class and option user-class = "iPXE" {
  # Image request, so provide ISO image
  filename "http://<ip-address>/<directory>/";
  } else
{
  # Auto-provision request, so provide ZTP script or configuration
  filename "http://<ip-address>/<script-directory-path>/";
  #filename "http://<ip-address>/<script-directory-path>/
  }
}
```

（注） 自動プロビジョニング用に一度に提供できるのは、ZTP .script ファイルまたは .cfg ファイルのいずれかのみです。

この設定では、インストール時に を使用してシステムを起動し、その後 XR LXC が起動した時点で をダウンロードして実行します。

手動による ZTP の呼び出し

ZTP は、変更されたワンタッチ プロビジョニング手法を使用して手動で呼び出すこともできます。このプロセスでは、次の手順を実行する必要があります。

始める前に

設定ファイルを使用して、XR で起動され、DHCP が呼び出されるインターフェイスのリストを指定することができます。/pkg/etc/ztp.config はプラットフォーム固有のファイルで、追加のインターフェイスを使用するかどうかをプラットフォームが指定できます。

```
#
# List all the interfaces that ZTP will consider running on. ZTP will attempt
# to bring these interfaces. At which point dhclient will be able to use them.
#
# Platforms may add dynamically to this list.
#
#ZTP_DHCLIENT_INTERFACES=" \
#    Gi0_0_0_0 \
#"
...
```

手順

ステップ 1 ルータを起動します。

ステップ 2 手動でログインします。

ステップ 3 インターフェイスを有効にします。

ステップ 4 **ztp initiate** コマンドを使用して新しい ZTP DHCP セッションを手動で呼び出します。

```
Router#ztp initiate
```

たとえば、GigabitEthernet インターフェイス 0/0/0/0 で DHCP 要求を送信するには、次のコマンドを実行します。

```
Router#ztp initiate debug verbose interface GigabitEthernet0/0/0/0
```

プラットフォームが別の方法で設定していない限り、ZTP はデフォルトで管理ポート上で実行されます。ログは `/disk0:/ztp/ztp/log` の場所に記録されます。

（注） 40G インターフェイスを 4 つの個別の 10G インターフェイスに設定するには、**ztp breakout nosignal-stay-in-breakout-mode** コマンドを使用します。

（注） データポートブレークアウトを有効にし、検出されたすべてのデータポートインターフェイスおよびラインカードインターフェイスでDHCPセッションを呼び出すには、**ztp breakout** コマンドを使用します。

```
Router#ztp breakout debug verbose
Router#ztp initiate dataport debug verbose
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:
```

プロンプトを上書きするには：

```
Router#ztp initiate noprompt
Invoke ZTP?(this may change your configuration) [confirm] [y/n]:

ZTP will now run in the background.
Please use "show logging" or look at /disk0:/ztp/ztp/log to check progress.
```

ZTP はデフォルトで起動している管理インターフェイス上で動作します。

ステップ 5 ZTP セッションを終了するには、**ztp terminate** コマンドを使用します。

次のタスク

iPXE を使用してルータを起動します。

iPXE を使用したルータの起動

iPXE ブートを使用する前に、次のことを確認してください。

- DHCP サーバが設定され、動作している。
- **admin** コマンドを使用してシステム管理コンソールにログインしている。

ルータのイメージを再作成するために、次のコマンドを実行して iPXE ブート プロセスを呼び出します。

```
hw-module location all bootmedia network reload
```

例：

```
sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
Wed Dec 23 15:29:57.376 UTC
Reload hardware module ? [no,yes]
```

次の例は、コマンドの出力を示しています。

```
iPXE 1.0.0+ (3e573) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
Trying net0...
net0: c4:72:95:a6:14:e1 using dh8900cc on PCI01:00.1 (open)
[Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 c4:72:95:a6:14:e1)..................... Ok << Talking to DHCP/PXE server
 to obtain network information
net0: 10.37.1.101/255.255.0.0 gw 10.37.1.0
net0: fe80::c672:95ff:fea6:14e1/64
net0: 2001:1800:5000:1:c672:95ff:fea6:14e1/64 gw fe80::20c:29ff:fefb:b9fe
```

```
net1: fe80::c672:95ff:fea6:14e3/64 (inaccessible)
Next server: 10.37.1.235
Filename: http://10.37.1.235/ncs5k/ncs5k-mini-x.iso
http://10.37.1.235/ ... 58% << Downloading file as indicated by DHCP/PXE server to boot
 install image
```