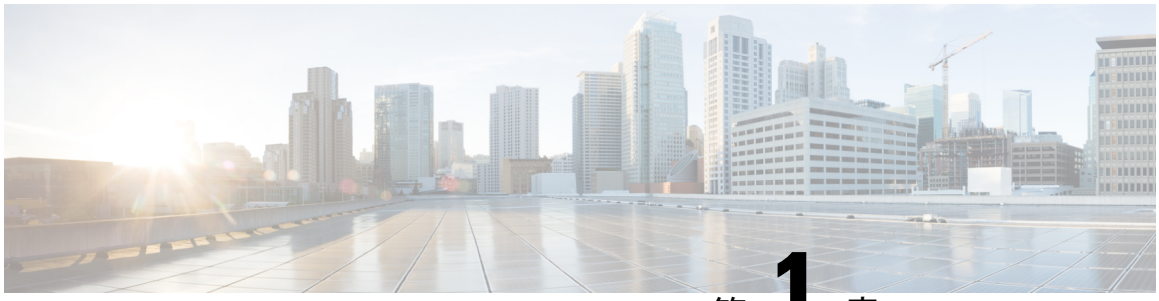
システム イメージのロードおよび管理のコンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

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



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

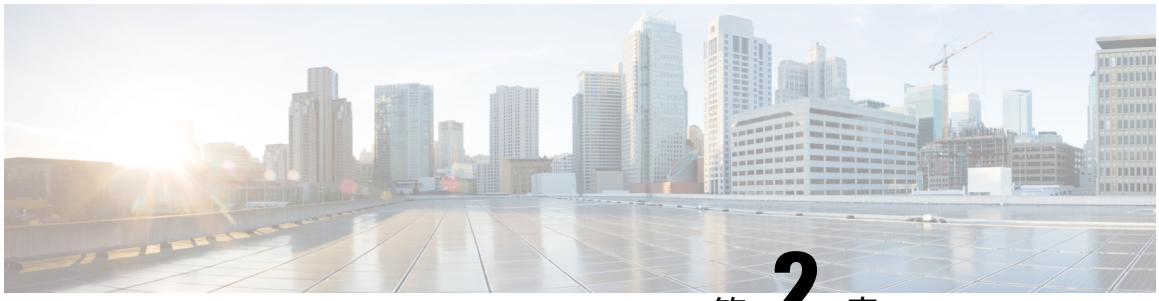
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- Cisco IOS コマンド リファレンス、すべてのリリース

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

デジタル署名付き Cisco ソフトウェア

デジタル署名付き Cisco ソフトウェア機能では、デジタル署名付き Cisco ソフトウェアの識別、デジタル署名付きイメージに関するソフトウェア認証情報の収集、およびキー失効の実行について説明します。デジタル署名付き Cisco ソフトウェアは、セキュアな非対称（公開キー）暗号化を使用してデジタル署名されたソフトウェアです。

デジタル署名付き Cisco ソフトウェアの目的は、自分のシステム内で動作しているソフトウェアが改ざんされていないセキュアなもので、信頼できる送信元のものであることを、お客様に確信していただくことです。

デジタル署名付き Cisco ソフトウェアに関するソフトウェア アップデートについてお客様が不安を抱えているかもしれませんが、向上した保護機能を有効にするのに特別な作業は必要ありません。システム操作の大部分は、現行方針に対する透明性が概ね確保されています。デジタル署名付き Cisco ソフトウェアの使用を反映して、システム表示に小さな変更が加えられています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

デジタル署名付き Cisco ソフトウェアに関する制限事項

Cisco IOS XE ソフトウェアを実行する Cisco Catalyst 4500 E+Series スイッチには、このドキュメントで説明する機能（デジタル署名付きソフトウェアのキーの失効と置換を除く）が含まれています。

デジタル署名付き Cisco ソフトウェアに関する情報

デジタル署名付き Cisco ソフトウェアの機能と利点

3 つの主な要因によって、デジタル署名付き Cisco ソフトウェアとソフトウェア整合性検証が推進されています。

- 米国政府は、連邦情報処理標準（FIPS）140 の改訂版を公表しています。FIPS-140-3 は最新の草稿であり、2010 年に批准し、2011 年に発効するようにスケジュールされています。この標準では、ソフトウェアをロードおよび実行する前に、そのソフトウェアで信頼性と整合性を証明し、デジタル署名することが求められています。
- 製品のセキュリティに焦点を合わせることにより、シスコ製品への攻撃や脅威からの保護を強化しています。デジタル署名付き Cisco ソフトウェアは、破損している、または変更されているソフトウェアのインストールおよびロードを防止する保護機能の強化を提供します。
- デジタル署名付き Cisco ソフトウェアは、お客様の購入した機器が主張どおりのものであることを保証する、偽造防止機能です。

デジタル署名付き Cisco ソフトウェアの識別

デジタル署名付き Cisco IOS ソフトウェアは、イメージ名に含まれる 3 文字の拡張子によって識別されます。Cisco IOS イメージ ファイルは、Cisco ソフトウェア ビルド プロセスによって作成されます。このファイルに含まれるファイル拡張子は、イメージを署名するために使用された署名キーに基づいています。これらのファイル拡張子は次のようになります。

- .SPA
- .SSA

ファイル拡張子の各文字の意味を以下の表に示します。

表 *1 :* デジタル署名付き *Cisco* ソフトウェア イメージのファイル拡張子における文字の意味

ファイル拡張子の文字	文字の意味
S（最初の文字）	デジタル署名付きソフトウェアであることを表します。
P または S（2 番目の文字）	P または S はそれぞれ、製品および特別（開発）イメージであることを表します。製品イメージは、一般リリースが承認された Cisco ソフトウェアを指します。特別イメージは、特別な条件下で限定的に使用される開発用ソフトウェアを指します。
A（3 番めの文字）	イメージのデジタル署名に使用されているキー バージョンを示します。キー バージョンは A、B、C のようなアルファベット文字で識別されます。

デジタル署名付き Cisco ソフトウェアのキー タイプとバージョン

デジタル署名付き Cisco ソフトウェアのキーは、キーのタイプとバージョンによって識別されます。キーのタイプには、特別キー、製品キー、ロールオーバー キーがあります。特別キーと製品キーは、失効させることができます。ロールオーバー キーは、特別キーまたは製品キーを失効させるために使用します。ファイル拡張子の 2 番目の文字は、キー タイプ（特別キーまたは製品キー）を示します。キー タイプが製品キーの場合は「P」となり、特別キーの場合は「S」となります。

製品キーおよび特別キーの各タイプには、それぞれキー バージョンが関連付けられています。ファイル拡張子の 3 番目の文字（A、B、C のようなアルファベット文字）によって、キー バージョンが定義されます。キーを置換すると、キー バージョンのアルファベットが 1 つ進みます。たとえば、キー バージョンが「A」で、キー タイプが「P」（製品キー）のキーが失効すると、新しいイメージはキー バージョン「B」で署名されます。キー タイプとキー バージョンは、デバイスのキー ストレージにキー レコードの一部として保存されます。

デジタル署名付き Cisco ソフトウェアのキーの失効と置換

（注） キーの失効と置換は、IOS XE ソフトウェアを実行している Catalyst 4500 E+Series スイッチではサポートされていません。

キー失効

キーの失効は、デジタル署名付き Cisco ソフトウェア内で動作中のキーを削除するプロセスです。

キーが侵害された場合、または使用されなくなった場合に、キー失効が発生します。キーの失効と置換は、特定の脆弱性またはシスコのセキュア キー インフラストラクチャに深刻な損失が発生した場合にのみ必要となります。そのような状況を修復する操作手順は、シスコによっ

て通知され、指示された場合にのみ必要になります。通知と指示は、www.cisco.com での勧告の掲載またはフィールド通知によって行われます。

失効されるキーのタイプによって異なる 2 つのキー失効プロセスが存在します。

- 無効化イメージと製品イメージを使用する製品キーの置換
- 製品イメージを使用する特別キーの置換

キーの置換

キーの置換は、侵害されたキーと置き換えるための新しいキーを作成するプロセスです。侵害されたキーを失効させる前に、新しいキーが追加されます。キーの置換は2段階のプロセスです。

1. 新しいキーがキー ストレージに追加され、失効したキーを置き換えます。
2. イメージが新しいキーで正しく動作することが確認されると、侵害されたキーはキー ストレージから失効されます。

キー失効イメージ

失効イメージは、新しい製品キーをキー ストレージ領域に追加する機能を持つ、通常イメージの基本バージョンとなります。失効イメージに他の機能はありません。キーを失効させ、置換する場合に、キーごとに 1 つの失効イメージが作成されます。

失効イメージには、その中でバンドルされている新しい製品キーが含まれます。

プラットフォームに保存されたロールオーバー キーは、失効イメージの署名を検証するために使用されます。有効な失効イメージは同じロールオーバー キーを使用して署名されます。

（注） 失効イメージが使用できるのは、製品キーの失効だけです。

失効イメージに関する重要なタスク

失効イメージに関して、2 つの重要な作業があります。

- 新しい製品キーのキー ストレージ領域への追加。
- 製品キーのアップグレードチェックの実行。詳細については、「製品キーの失効」の手順 2 を参照してください。

新しい製品キーのキー ストレージ領域への追加：

失効イメージは、バンドルされた製品キーをキー ストレージに追加します。追加されるキーはキー ストレージ内の既存のキー セットの一部ではないことが失効イメージによって確認された後、キーはプライマリおよびバックアップのキー ストレージ領域に書き込まれます。

キーのアップグレード チェックの実行：

新しいキーが追加され、お客様がソフトウェア（Cisco IOS および ROMmon）をアップグレードした後、show software authenticity upgrade-status コマンドを実行する必要があります。ユーザは、製品キーが正常にアップグレードされ、次回のブート時に選択できるようになっているか確認するため、コマンド出力を確認できます。

製品キーの失効

侵害された製品キーを使用して署名されたイメージは信頼できないため、ロールオーバー キーによって署名された失効イメージを使用して、製品キー（リリース キーとも呼ばれます）は失効および置換されます。ROMmon はロールオーバー キーを使用して署名されたイメージを起動することができます。製品キーの失効と置換のプロセスに、4 つの手順が関係しています。

1. 新しい製品キーをキー ストレージに追加する。新しい製品キーは、失効イメージ内でバンドルされます。
2. show software authenticity upgrade-status コマンドを使用してソフトウェア アップグレード チェックを実行し、以下を確認します。
   - 新しい製品キー バージョンがインストールされたこと。
   - 新しい製品キーがプライマリ キー ストレージに追加されたこと（されていない場合、既存の失効イメージで software authenticity key add production コマンドを再発行する）。
   - 新しい製品キーがバックアップ キー ストレージに追加されたこと（されていない場合、既存の失効イメージで software authenticity key add production コマンドを再発行する）。
   - イメージが新しい製品キーで署名され、オートブートするように（boot system コマンドを使用）設定されたこと（されていない場合、新しい製品イメージをボックスにコピーし、新しいイメージをポイントするように boot system コマンドが変更されていることを確認する）。
   - アップグレード可能な ROMmon が新しい製品キーによって署名されていること（されていない場合、新しい製品キーによって署名された ROMMON にアップグレードする）。
3. すべてを確認したら、reload コマンドを使用して、新しい製品キーで署名された製品イメージをロードします。
4. 新しい製品イメージをロードしたら、software authenticity key revoke production コマンドを使用して侵害されたキーを失効させることができます。

手順 1 と 2 は、特別失効イメージを使用して実行します。いずれかのソフトウェアが古いキーを使用している場合、リブートしても（手順 3）、古いキーは失効されないため、手順 2 でこれらを確認することは重要です。この作業によって、新しいキーのインストールが完了し、次のリブート（手順 3）では新しいリリースのソフトウェアと新しい ROMmon が使用されることを確認できます。古い製品キーの失効（手順 4）は、新しいキーと新しいソフトウェアがシステムにインストールされてからでなければ、実行できません。

特別キーの失効

特別キーの失効には製品キーで署名された製品イメージが使用されます。特別キーの失効に使用される各製品イメージには、バンドルされた特別キー（製品イメージの作成時の最新）があります。特別キーの失効と置換のプロセスには、3 つの手順が含まれます。

1. バンドルされた新しい特別キーのキー ストレージ領域への追加。
2. 侵害された特別キーを使用して署名された ROMmon の、新しい特別キーを使用して署名された新しい ROMmon へのアップグレード。
3. キー ストレージからの侵害されたキーの失効。

手順3ではリブートする必要はありません。製品イメージ自体を使用して実行されることに注意してください。これは、お客様がすでに製品イメージを実行していて、無効化自体が稼働中の製品イメージから発生することによります。どのようなキーについても、特別イメージに追加や無効化の機能はありません。

デジタル署名付き Cisco ソフトウェア イメージの作業方法

デジタル署名付き Cisco ソフトウェアの識別

以下のタスクを実行して、デジタル署名付き Cisco ソフトウェアを識別します。このタスクでは、show version コマンドのコマンド出力でイメージ ファイル名を調べ、「デジタル署名付き Cisco ソフトウェアの識別」セクションで説明されている条件に基づいて判断します。

（注） イメージファイルの名前がユーザによって変更された場合、デジタル署名されたイメージであることを示す条件をユーザが上書きしたために、イメージを識別できない可能性があります。

手順の概要

1. **enable**
2. **show version**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show version** 例： `Device# show version`	ルーティング デバイスで実行している Cisco IOS ソフトウェアのバージョン、ROM モニタとブートフラッシュ ソフトウェアのバージョン、およびシステム メモリの量を含むハードウェア構成についての情報が表示されます。

デジタル署名付き Cisco ソフトウェア署名情報の表示

以下のタスクを実行して、起動に使用する現在の ROMmon および Cisco IOS イメージ ファイルのソフトウェア認証に関する情報を表示します。この表示には、イメージのクレデンシャル情報、確認に使用されるキータイプ、署名情報、署名エンベロープのその他の属性が含まれます。

手順の概要

1. **enable**
2. **show software authenticity running**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show software authenticity running** 例： `Device# show software authenticity running`	起動に使用する現在の ROMmon および Cisco IOS イメージファイルのソフトウェア認証に関する情報を表示します。

特定のイメージ ファイルのデジタル署名情報の表示

以下のタスクを実行して、特定のイメージファイルのソフトウェア認証に関連したデジタル署名情報を表示します。

手順の概要

1. **enable**
2. **show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | flash0:filename | flash1:filename}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | flash0:filename | flash1:filename}** 例： `Device# show software authenticity file flash0:c3900-universalk9-mz.SPA`	特定のイメージ ファイルのデジタル署名とソフトウェア認証に関連した情報を表示します。

デジタル署名付き Cisco ソフトウェア キー情報の表示

以下のタスクを実行して、デジタル署名付き Cisco ソフトウェア キー情報を表示します。キータイプとともにストレージ内にあるソフトウェア公開キーの詳細情報を表示します。

手順の概要

1. **enable**
2. **show software authenticity keys**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show software authenticity keys** 例： `Device# show software authenticity keys`	デジタル署名付き Cisco ソフトウェアのキー タイプとともにストレージ内にあるソフトウェア公開キーを表示します。

デジタル署名付き Cisco ソフトウェア イメージのトラブルシューティング

以下のタスクを実行して、デジタル署名付き Cisco ソフトウェア イメージをトラブルシューティングします。

手順の概要

1. **enable**
2. **debug software- authenticity errors {envelope | errors | key | revocation | show | verbose}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug software- authenticity errors {envelope | errors | key | revocation | show | verbose}** 例： `Device# debug software-authenticity errors`	デジタル署名付き Cisco ソフトウェアでデバッグメッセージの表示をイネーブルにします。

デジタル署名付き Cisco ソフトウェアの設定例

デジタル署名付き Cisco ソフトウェアの識別例

次に、デジタル署名付き Cisco ソフトウェアのイメージ ファイル名を表示する例を示します。この方法によって、デジタル署名付き Cisco ソフトウェアの識別条件に基づいて識別することができます。

```
Device# show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M),
12.4(20090904:044027) [i12 577]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 04-Sep-09 09:22 by xxx
ROM: System Bootstrap, Version 12.4(20090303:092436)
C3900-2 uptime is 8 hours, 41 minutes
System returned to ROM by reload at 08:40:40 UTC Tue May 21 1901!
System image file is "xxx.SPA"
Last reload reason: Reload Command
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
```

```
Cisco xxx (revision 1.0) with CISCxxx with 987136K/61440K bytes of memory.
Processor board ID xxx
3 Gigabit Ethernet interfaces
1 terminal line
1 Virtual Private Network (VPN) Module
1 cisco Integrated Service Engine(s)
DRAM configuration is 72 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
1020584K bytes of USB Flash usbflash0 (Read/Write)
1020584K bytes of USB Flash usbflash1 (Read/Write)
500472K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
xx        xxx                   xxxx
Technology Package License Information for Module:'xxx'
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
Configuration register is 0x2102
```

デジタル署名付きイメージ ファイルは、以下の行で識別されます。

```
System image file is "xxx.SPA"
```

イメージの特性として、ファイル名にデジタル署名付き Cisco ソフトウェアの 3 文字の拡張子（.SPA）が付きます。「デジタル署名付き Cisco ソフトウェアの識別」セクションのガイドラインに基づいて、ファイル拡張子の先頭の文字「S」はイメージがデジタル署名付きソフトウェア イメージであること、2 番目の文字「P」はイメージが製品キーを使用してデジタル署名されたこと、3 番目の文字「A」はキー バージョンがバージョン A であることが示されています。

デジタル署名付き Cisco ソフトウェア署名情報の表示例

次に、起動に使用する現在の ROMmon および Cisco IOS イメージ ファイルのソフトウェア認証に関する情報を表示する例を示します。

```
Device# show software authenticity running
SYSTEM IMAGE
--------------------
Image type                    : Development
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : xxx
    Signature Algorithm       : 2048-bit RSA
    Key Version               : xxx

    Verifier Information
```

```
        Verifier Name         : ROMMON 2
        Verifier Version      :  System Bootstrap, Version 12.4(20090409:084310)
ROMMON 2
---------------
Image type                    : xxx
    Signer Information
        Common Name           : xxx
        Organization Unit     : xxx
        Organization Name     : xxx
    Certificate Serial Number : xxx
    Hash Algorithm            : xxx
    Signature Algorithm       : 2048-bit RSA
    Key Version               : xx

    Verifier Information
        Verifier Name         : ROMMON 2
        Verifier Version      :  System Bootstrap, Version 12.4(20090409:084310) [
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *2 : show software authenticity running* フィールドの説明

フィールド	説明
SYSTEM IMAGE	システム イメージ情報を表示する出力のセクション。
Image type	イメージのタイプを表示する。
Common Name	ソフトウェア製造業者の名前を表示する。
Organization Unit	ソフトウェア イメージが導入されているハードウェアを表示する。
Organization Name	ソフトウェア イメージの所有者を表示する。
Certificate Serial Number	デジタル署名の証明書シリアル番号を表示する。
Hash Algorithm	デジタル署名の確認に使用されるハッシュ アルゴリズムの種類を表示する。
Signature Algorithm	デジタル署名の確認に使用される署名アルゴリズムの種類を表示する。
Key Version	確認に使用されるキー バージョンを表示する。
Verifier Name	デジタル署名の確認を受け持つプログラムの名前を表示する。
Verifier Version	デジタル署名の確認を受け持つプログラムのバージョンを表示する。
ROMMON 2	現在の ROMmon 情報を表示する出力のセクション。

特定のイメージ ファイルのデジタル署名情報の表示例

次に、特定のイメージファイルのソフトウェア認証に関連したデジタル署名情報を表示する例を示します。

Device# **show software authenticity file flash0:**c3900-universalk9-mz.SSA

```
File Name                       : flash0:c3900-universalk9-mz.SSA
Image type                      : Development
    Signer Information
        Common Name             : xxx
        Organization Unit       : xxx
        Organization Name       : xxx
    Certificate Serial Number   : xxx
    Hash Algorithm              : SHA512
    Signature Algorithm         : 2048-bit RSA
    Key Version                 : A
```

The table below describes the significant fields shown in the display.

表 *3 : show software authenticity file* フィールドの説明

フィールド	説明
File Name	メモリのファイル名。たとえば、flash0:c3900-universalk9-mz.SSA は、フラッシュ メモリ（flash0:）内のファイル名 c3900-universalk9-mz.SSA を指します。
Image type	イメージのタイプを表示する。
Signer Information	署名情報。
Common Name	ソフトウェア製造業者の名前を表示する。
Organization Unit	ソフトウェア イメージが導入されているハードウェアを表示する。
Organization Name	ソフトウェア イメージの所有者を表示する。
Certificate Serial Number	デジタル署名の証明書シリアル番号を表示する。
Hash Algorithm	デジタル署名の確認に使用されるハッシュ アルゴリズムの種類を表示する。
Signature Algorithm	デジタル署名の確認に使用される署名アルゴリズムの種類を表示する。
Key Version	確認に使用されるキー バージョンを表示する。

デジタル署名付き Cisco ソフトウェア キー情報の表示例

次の例では、デジタル署名付き Cisco ソフトウェア キー情報を表示します。キー タイプを含むストレージ内にあるソフトウェア公開キーの詳細情報を表示します。

```
Device# show software authenticity keys
Public Key #1 Information
-------------------------
Key Type             : Release  (Primary)
Public Key Algorithm : RSA
```

```
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ...
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version          : A
Public Key #2 Information
-------------------------
Key Type             : Development  (Primary)
Public Key Algorithm : RSA
Modulus :
        CC:CA:40:55:8C:71:E2:4A:3A:B6:9D:5C:94:1D:02:BA:
       ....
        26:04:6B:33:EB:70:2B:18:24:C7:D9:31:3E:77:24:85
Exponent : xxx
Key Version          : A

The table below describes the significant fields shown in the display.
```

表 *4 : show software authenticity keys* フィールドの説明

フィールド	説明
Public Key #	公開キー番号。
Key Type	イメージの確認に使用されるキー タイプを表示する。
Public Key Algorithm	公開キーの暗号化に使用されるアルゴリズム名を表示します。
Modulus	公開キー アルゴリズムの係数。
Exponent	公開キー アルゴリズムの指数。
Key Version	確認に使用されるキー バージョンを表示する。

デジタル署名付き Cisco ソフトウェア イメージ キー情報のデバッグの有効化：例

次に、デジタル署名付き Cisco ソフトウェアのキー情報に関連するソフトウェア認証イベントのデバッグを有効にする例を示します。

```
Device# debug software authenticity key
```

その他の参考資料

ここでは、デジタル署名付き Cisco ソフトウェアの機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
『System Management Command Reference』	http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/system_manageme

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

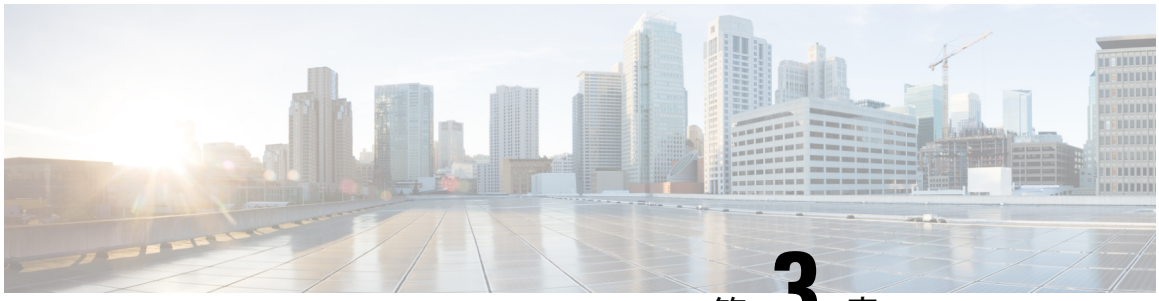
デジタル署名付き Cisco ソフトウェアの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5 :* デジタル署名付き *Cisco* ソフトウェアの機能情報

機能名	リリース	機能情報
デジタル署名付き Cisco ソフトウェア		デジタル署名付き Cisco ソフトウェア機能では、デジタル署名付き Cisco ソフトウェアの識別、デジタル署名付きイメージに関するソフトウェア認証情報の収集、およびキー失効の実行について説明します。デジタル署名付き Cisco ソフトウェアは、セキュアな非対称（公開キー）暗号化を使用してデジタル署名されたソフトウェアです。 次のコマンドが導入または変更されました。 **debug software authenticity, show software authenticity file, show software authenticity keys, show software authenticity running.**
キー失効機能のサポート		キー失効機能のサポートが追加されました。キー失効では、プラットフォームのキーストレージからキーを削除します。プラットフォームは製品イメージまたは特別イメージをホストでき、製品キー（製品イメージから）または特別キー（特別イメージから）はキー失効の過程で失効させられます。 この機能に関する詳細については、次の項を参照してください。 • デジタル署名付き Cisco ソフトウェアのキーの失効と置換 次のコマンドが導入または変更されました。 **debug software authenticity, show software authenticity upgrade-status, software authenticity key add, software authenticity key revoke, upgrade rom-monitor file.**



第 3 章

FTP を使用したシステム イメージの管理

このモジュールには、FTP を使用したシステム イメージの管理に関する情報が含まれています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

フラッシュ メモリから FTP サーバへのイメージのコピー

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用して、ルータからサーバにコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ipftpusername** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。

3. Anonymous

ルータは次のうち、最初に発見した有効なパスワードを送信します。

1. **copy** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ipftppassword** グローバル コンフィギュレーション コマンドで設定されたパスワード（コマンドが設定されている場合）。

ルータは、*username* @*routername* .*domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、ルータ上のユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーション ファイルまたはイメージは、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ipftpusername** および **ipftppassword** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

FTP サーバからフラッシュ メモリ ファイル システムへのイメージのコピー

FTP サーバからフラッシュ メモリ ファイル システムへシステム イメージをコピーできます。

FTP ユーザ名とパスワード

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用して、ルータからサーバにコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ipftpusername** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. Anonymous

ルータは次のうち、最初に発見した有効なパスワードを送信します。

1. **copy** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。

ルータは、*username* @*routername* .*domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合、ルータ上のユーザからの FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーションファイルまたはイメージは、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

フラッシュ メモリから FTP サーバにイメージをコピー

FTP ネットワーク サーバ上のシステム イメージをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ftp username** *username*
4. **ip ftp password** *password*
5. **end**
6. **show** *flash-filesystem* **:**
7. **copy** *flash-filesystem* **:** *filename* **ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 3	**ip ftp username** *username* 例： `Router(config)# ip ftp username user1`	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 4	**ip ftp password** *password* 例： `Router(config)# ip ftp password guessme`	（任意）デフォルトのパスワードを変更します。
ステップ 5	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 6	**show** *flash-filesystem* **:** 例： `Router# show flash:`	（任意）指定されたフラッシュ ディレクトリのシステム イメージ ファイルを表示します。フラッシュ メモリ内のシステム イメージ ファイル名を知らない場合は、このファイル名の正確なスペルをメモしておきます。
ステップ 7	**copy** *flash-filesystem* **:** *filename* **ftp:** [[[//[*username* [**:***password*]**@**]*location*]/*directory*]/*filename*] 例： `Router# copy slot0:1:your-ios ftp://myuser:mypass@172.23.1.129/dirt/sysadmin/your-ios`	このイメージを FTP サーバにコピーします。 （注） **copy** 特権 EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および**fileprompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

例

この例では、**showslot1:privileged**EXEC コマンドを使用して 2 番目の PCMCIA スロットにあるシステム イメージ ファイルの名前を表示し、ファイル（test）を FTP サーバにコピーします。

```
Router# show slot1:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. 1        46A11866 2036C   4    746      May 16 1995 16:24:37 test
Router# copy slot1:test ftp://thisuser:thatpass@172.16.13.110/test
```

```
writing test!!!!...
successful ftp write.
```

この例では、your-ios という名前のファイルを、スロット 0 にあるフラッシュ メモリ PC カードのパーティション 1 から、172.23.1.129 にある TFTP サーバにコピーします。このファイルは、リモート ユーザ名を持つディレクトリに対する dirt/sysadmin ディレクトリに your-ios という名前で保存されます。

```
Router# show slot0: partition 1
PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 your-ios
[1711152 bytes used, 2483152 available, 4194304 total]
Router# copy slot0:1:your-ios ftp://myuser:mypass@172.23.1.129/dirt/sysadmin/your-ios
Verifying checksum for 'your-ios' (file # 1)...  OK
Copy 'your-ios' from Flash to server
  as 'dirt/sysadmin/ios-2'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

FTP サーバからフラッシュ メモリへのコピー

FTP サーバからフラッシュ メモリ ファイル システムへシステム イメージをコピーするには、以下の手順を実行します。

手順の概要

1. **enable**
2. **show** *flash-filesystem* **:**
3. **copy** *flash-url* **tftp** :[[[*//location*]*/directory*]*/filename*]
4. **configure terminal**
5. **ip ftp username** *username*
6. **ip ftp password** *password*
7. **end**
8. **copy ftp:** [[[*//*[*username* [**:***password*]**@**]*location*] */directory*]*/filename*]*flash-filesystem***:**[*filename*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show** *flash-filesystem* **:** 例：	（任意）フラッシュ メモリ内のシステム イメージ ファイル名を表示します。このコマンドを使用して、この次のコマンドで使用するために、ファイル

	コマンドまたはアクション	目的
	`Router# show flash:`	の URL パスとシステム イメージ ファイル名の正確なスペルを確認します。
ステップ 3	**copy** *flash-url* **tftp** :[[[//*location*]/*directory*]/*filename*] 例： `Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios`	フラッシュ メモリから TFTP サーバにシステム イメージをコピーします。ファイルの場所とファイル名を *flash-url* 引数として指定します。 （注） **copy** 特権 EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **fileprompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。
ステップ 4	**configure terminal** 例： `Router# configure terminal`	（任意）端末からグローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 5	**ip ftp username** *username* 例： `Router(config)# ip ftp username netuser1`	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 6	**ip ftp password** *password* 例： `Router(config)# ip ftp password guessme`	（任意）デフォルトのパスワードを変更します。
ステップ 7	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 8	**copy ftp:** [[[//[*username* [**:***password*]**@**]*location*] /*directory*]/*filename*]*flash-filesystem***:**[*filename*] 例： `Router# copy`	コンフィギュレーション ファイルをネットワーク サーバから稼働中のメモリ、または rcp を使用してスタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	`ftp://myuser:mypass@theserver/tftpboot/sub3/c7200-js-mz slot1:c7200-js-mz`	（注） **copy** 特権 EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。表示されるプロンプトは、**copy** コマンドで入力した情報量および **fileprompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

例

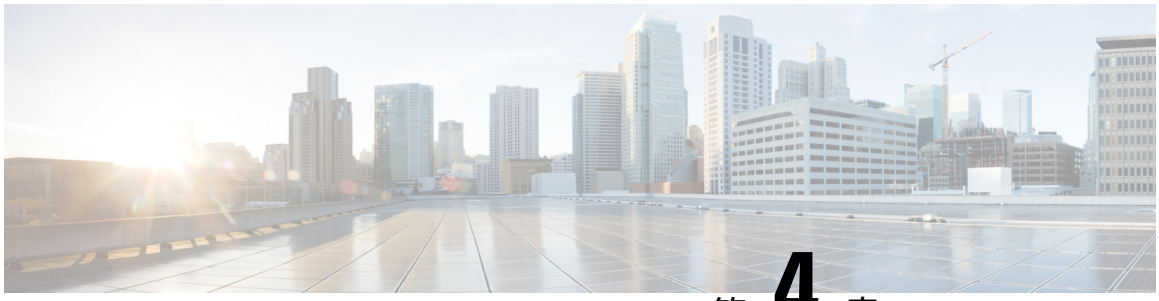
次に、**reload** コマンドを使用して、ルータでソフトウェアを現在の日の午後 7 時 30 分にリロードする例を示します。

```
Router# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

次に、**reload** コマンドを使用して、ルータでソフトウェアを将来リロードする例を示します。

```
Router# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

例



第 4 章

Cisco IOS Auto-Upgrade Manager の設定

Cisco IOS Auto-Upgrade Manager（AUM）機能を使用すると、新しい Cisco IOS イメージを指定、ダウンロード、アップグレードするための単純なインターフェイスが利用できるようになり、ソフトウェア イメージのアップグレード プロセスが単純化されます。

Auto-Upgrade Manager の指示に従ってプロセスを進めることにより、対話モードで新しい Cisco IOS イメージにアップグレードできます。また、単一の Cisco IOS コマンドまたは一連のコマンドを実行してアップグレードを行うこともできます。3 つの方法すべてで、ウォーム アップグレード機能を使用してアップグレードが行われ、ダウンタイムが最小化されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco IOS Auto-Upgrade Manager のための前提条件

- シスコからダウンロードするために、ルータ上で DNS サーバの IP アドレスを設定する必要があります。詳細については、「DNS サーバの IP アドレスの設定：例」セクションおよび「関連資料」セクションを参照してください。
- シスコからダウンロードするために、ルータ上でシスコの Web サイト（www.cisco.com）から取得した Secure Socket Layer（SSL）証明書を設定する必要があります。この設定は、シスコ以外のサーバからダウンロードする場合は不要です。詳細については、「シスコ ダウンロードの SSL 証明書の設定」セクションおよび「関連資料」セクションを参照してください。
- 暗号化 Cisco IOS ソフトウェア イメージをダウンロードする場合は、暗号化ソフトウェアのダウンロードのために、シスコに登録する必要があります。

Cisco IOS Auto-Upgrade Manager の制約事項

要求された Cisco IOS ソフトウェア イメージをロードおよび格納するための十分なメモリ リソースがルータにない場合、Cisco IOS Auto-Upgrade Manager は最後まで完了しません。Cisco IOS ソフトウェア イメージは、ルータで現在動作している Cisco IOS ソフトウェア イメージが暗号化イメージの場合にだけ www.cisco.com からダウンロードできます。

Cisco IOS Auto-Upgrade Manager について

Cisco IOS Auto-Upgrade Manager の概要

Cisco IOS Auto-Upgrade Manager は、新しい Cisco IOS ソフトウェア イメージのアップグレード プロセスを効率化します。Cisco IOS Auto-Upgrade Manager は、コマンドライン インターフェイス（CLI）を通じて実行できます。AUM では、ルータをシスコの Web サイト（www.cisco.com）に接続し、cisco.com のユーザ名とパスワードを認証のために送信できます。認証後、ルータは、ユーザが指定した Cisco IOS ソフトウェア イメージの名前をシスコのサーバに渡します。シスコのサーバは、Cisco IOS ソフトウェア イメージの完全な URL をルータに返します。

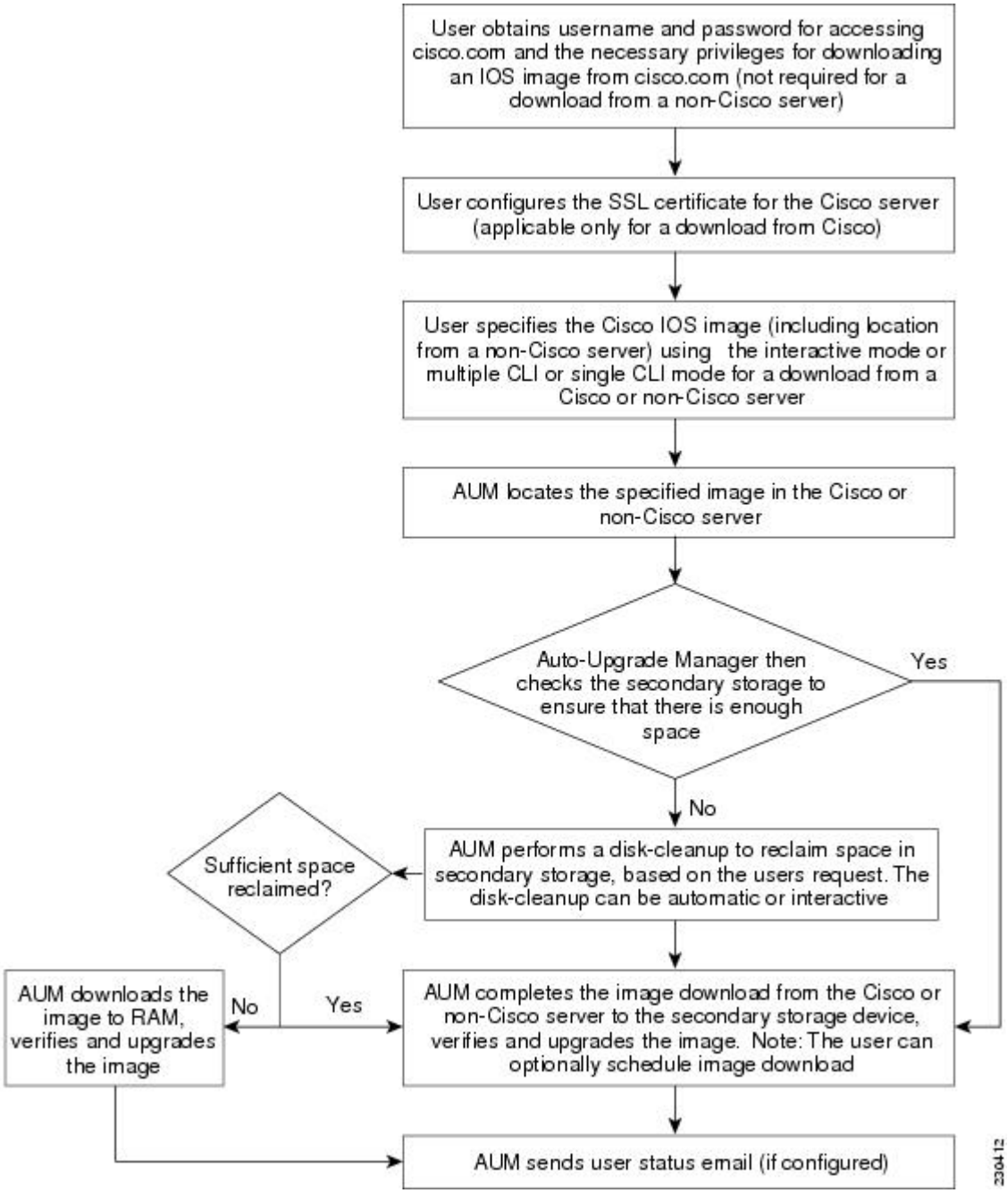
ルータで設定された Cisco IOS Auto-Upgrade Manager は、Cisco IOS ソフトウェア イメージへのアップグレード プロセス全体を管理します。AUM は、次の作業を実行することにより、ユーザによって指定された時刻に、ソフトウェア イメージを使用してルータをアップグレードします。

- Cisco IOS ソフトウェア イメージの検索とダウンロード
- すべての要件の確認

- 第 2 記憶域の管理
- Cisco IOS ソフトウェア イメージの検証
- ウォームアップグレードのスケジューリング

下の図に、Cisco IOS Auto-Upgrade Manager のワークフローを示します。

図 *1 : Cisco IOS Auto-Upgrade Manager* のワークフロー



（注） ルータが、ユーザが指定した Cisco IOS ソフトウェア イメージのロードに失敗すると、コンソール ウィンドウと syslog バッファに、エラーの理由を示すエラー メッセージが表示されます。ユーザが暗号化ソフトウェアをダウンロードする許可を持っていない場合、このサービスに登録するようユーザに求めるエラー メッセージが生成されます。同様に、いずれかの CLI 設定文がブート時にパーサーに理解されない場合、エラーメッセージが生成され、無効な設定行のログが nvram:invalid-config ファイルに格納されます。このエラー メッセージは、ユーザが指定した Cisco IOS ソフトウェア イメージが、以前の Cisco IOS ソフトウェア イメージと同じフィーチャ セットをサポートしていないことを示します。ルータに、両方のイメージをサポートするために十分な第 2 記憶域がなく、新しいイメージのアップグレードに成功した場合、再度シスコのサーバに接続して、第 2 記憶域に Cisco IOS ソフトウェア イメージをダウンロードします。このプロセスにより既存のイメージが消去されます。

シスコの Web サイトからの特定の Cisco IOS ソフトウェア イメージのダウンロード

www.cisco.com から特定の Cisco IOS ソフトウェア イメージをダウンロードできます。AUM は、セキュアな接続のために Secure Socket Layer（SSL）を使用するため、ユーザ側で証明書を設定する必要があります。ルータは、Cisco IOS ソフトウェア イメージの名前を、www.cisco.com サーバにログインするためのユーザ名およびパスワードとともに渡します。シスコのサーバは、特定の Cisco IOS ソフトウェア イメージの完全な URL をルータに返します。

Cisco IOS Auto-Upgrade Manager は、ユーザが指定した Cisco IOS ソフトウェア イメージを自動的に www.cisco.com からダウンロードして確認し、ダウンロードしたイメージでルータをアップグレードします。

（注） Intelligent Download Application（IDA）は、AUM に対するシスコのインターフェイスであり、AUM に関してはシスコのサーバと同じ意味で使用されます。

また、Cisco IOS Auto-Upgrade Manager では、次のオプション サービスが提供されます。

- ディスク クリーンアップ ユーティリティ
- アップグレードのスケジューリング

これらのサービスは、シスコのサーバとシスコ以外のサーバからのダウンロードに対して、対話モードとコマンド ラインモードの両方で使用できます。

シスコ以外のサーバからの特定の Cisco IOS ソフトウェア イメージのダウンロード

ローカルまたはシスコ以外の TFTP サーバまたは FTP サーバに存在する Cisco IOS ソフトウェア イメージをダウンロードできます。FTP ダウンロードのための FTP ユーザ名とパスワードは、**ipftpusername** および **ipftppassword** 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指定します。Cisco IOS Auto-Upgrade Manager では、特定の Cisco IOS ソフトウェア イメージのシスコ以外のサーバからのダウンロードとウォーム アップグレード サービスのプロセスが自動化されます。また、新しい Cisco IOS ソフトウェア イメージをダウンロードするために必要な領域が十分でない場合に使用する、ファイルを削除するためのディスク クリーンアップ ユーティリティも提供されています。

対話型およびシングル コマンド ライン モード

CLI を使用するか、次のユーザ インターフェイスを通じて、特定の Cisco IOS ソフトウェア イメージを www.cisco.com からダウンロードできます。

対話モード

Auto-Upgrade Manager に従って、対話モードで新しい Cisco IOS イメージにアップグレードできます。自動アップグレードを選択すると、対話モードでいくつかの問題に答えるだけでデバイスのアップグレードが完了します。対話モードを開始するには、オプションなしで **upgradeautomatic** コマンドを実行します。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

シングル コマンド ライン モード

対話型でないシングル ライン CLI は、上級ユーザ向けです。**upgradeautomaticgetversion** コマンドを使用し、必要なすべての引数を指定することで、シスコのサーバまたはシスコ以外のサーバから新しい Cisco IOS ソフトウェア イメージをダウンロードし、アップグレードできます。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

対話モードとシングル ライン CLI モードは、シスコのサーバとシスコ以外のサーバからのダウンロードに適用されます。

Cisco IOS Auto-Upgrade Manager を使用した Cisco IOS ソフトウェア イメージのアップグレード方法

シスコからのダウンロードのための SSL 証明書の設定

この作業では、シスコからダウンロードするための SSL 証明書を設定します。

始める前に

SSL 証明書を、cisco.com からダウンロードするように設定しておく必要があります。証明書は、セキュアな HTTP 通信のために必要です。SSL 証明書は、シスコの Web サイト（www.cisco.com）からダウンロードしてルータ上で設定します。

シスコの Web サイトから SSL 証明書を取得するには、次の作業を実行します。

1. Internet Explorer（IE）の [Tools] メニューから [Internet Options] を選択します。
2. [Advanced] タブで [Warn if changing between secure and not secure mode] を選択します。
3. IE に URL として https://www.cisco.com/ と入力します。セキュリティ警告のポップアップボックスが表示され、「You are about to leave a secure Internet connection. Do you want to continue?」というメッセージが表示されたら、[No] をクリックします。
4. IE のステータスバーにある鍵のアイコンをダブルクリックします。これにより、証明書の詳細を示すダイアログボックスが表示されます。
5. [Certification Path] タブをクリックします。タブには証明書チェーンが表示されます。
6. CA 証明書をそれぞれ選択して [View Certificate] をクリックします。これにより、証明書の詳細を示すウィンドウが表示されます。
7. 表示された証明書ウィンドウの [Details] タブを選択して、[Copy to File] をクリックします。これにより、証明書のエクスポート ウィザードが開きます。
8. 証明書を Base-64 符号化形式でファイル（cisco.cert など）に保存します。
9. cisco.cert ファイルをメモ帳で開き、ルータを設定するために必要な証明書データを取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal**
5. **revocation-check none**
6. **exit**
7. **crypto ca authenticate** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint cisco_ssl_cert`	認証局（CA）を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment terminal** 例： `Device(ca-trustpoint)# enrollment terminal`	コンソール端末上に証明書要求を表示し、発行された証明書データを端末上に入力できるようにします。
ステップ 5	**revocation-check none** 例： `Device(ca-trustpoint)# revocation-check none`	証明書の確認が必要ないことを指定します。
ステップ 6	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto ca authenticate** *name* 例： `Device(config)# crypto ca authenticate cisco_ssl_cert`	CA の自己署名証明書を取得することで、CA がルータに対して認証されます。

Cisco IOS Auto-Upgrade Manager の設定

Cisco IOS Auto-Upgrade Manager を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**}
4. **autoupgrade ida url** *url*
5. **autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**} 例： `Device(config)# autoupgrade disk-cleanup crashinfo`	Cisco IOS Auto-Upgrade Manager のディスク クリーンアップ ユーティリティを設定します。
ステップ 4	**autoupgrade ida url** *url* 例： `Device(config)# autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl`	Cisco IOS Auto-Upgrade Manager によってイメージ ダウンロード要求が送信される、www.cisco.com 上で動作しているシスコのサーバの URL を設定します。 （注） この手順は、デフォルトの URL が変更された場合にだけ必要です。
ステップ 5	**autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*} 例： `Device(config)# autoupgrade status email smtp-server smtpserver.abc.com`	ルータからのステータス電子メールの宛先となる電子メールアドレスと電子送信サーバを設定します。

Cisco IOS ソフトウェア イメージのダウンロード

Cisco IOS ソフトウェア イメージをシスコの Web サイト（www.cisco.com）またはシスコ以外のサーバからダウンロードするには、この作業を実行します。

手順の概要

1. **enable**
2. **upgrade automatic getversion** {**ciscousername***username***password***password***image***image* | *url*} [**at***hh***:***mm* | **now** | **in***hh***:***mm*] [**disk-management**{**auto** | **confirm** | **no**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**upgrade automatic getversion** {**ciscousername***username***password***password***image***image* | *url*} [**at***hh*:*mm* | **now** | **in***hh*:*mm*] [**disk-management** {**auto** | **confirm** | **no**}] 例： `Device# upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin at now disk-management auto`	www.cisco.com またはシスコ以外のサーバから、直接イメージをダウンロードします。

新しい Cisco IOS ソフトウェア イメージを使用したルータのリロード

新しい Cisco IOS ソフトウェア イメージを使用してルータをリロードするには、ここで説明する作業を実行します。

手順の概要

1. **enable**
2. **upgrade automatic runversion** [**at***hh*:*mm* | **now** | **in***hh*:*mm*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**upgrade automatic runversion** [**at***hh*:*mm* | **now** | **in***hh*:*mm*]	新しいイメージでルータをリロードします。

	コマンドまたはアクション	目的
	例： `Device# upgrade automatic runversion at 7:30`	（注） また、**upgradeautomaticgetversion** コマンドを使用して、新しい Cisco IOS ソフトウェア イメージでルータをリロードすることもできます。ただし、**upgradeautomaticgetversion** コマンドを使用してすでに Cisco IOS ソフトウェア イメージをダウンロードしてある場合は、**upgradeautomaticrunversion** コマンドを使用してルータをリロードする必要があります。

Cisco IOS ソフトウェア イメージのリロードの取り消し

特定の Cisco IOS ソフトウェア イメージのスケジューリングされたリロードを取り消すには、この作業を実行します。

次の状況でイメージのリロードを取り消すことができます。

- ルータをリロードするようスケジューリングされた時刻が十分でない場合。
- ルータを新しいイメージにアップグレードしない場合。

手順の概要

1. **enable**
2. **upgrade automatic abortversion**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**upgrade automatic abortversion** 例： `Device# upgrade automatic abortversion`	Cisco IOS ソフトウェア イメージのアップグレードを取り消します。

Cisco IOS Auto-Upgrade Manager の設定例

DNS サーバの IP アドレスの設定：例

Cisco IOS Auto-Upgrade Manager を設定する前に、ルータ上で DNS サーバの IP アドレスを設定する必要があります。これらの一連のイベントでは、ルータで **ping** コマンドを実行するときに、IP アドレスの代わりにホスト名を使用できます。ルータ上で DNS サーバの IP アドレスを設定した後、シスコの Web サイト（www.cisco.com）に正常に ping できるようになります。このアクションにより、ルータがインターネットに接続されていることも確認できます。

次に、ルータ上で DNS サーバの IP アドレスを設定する例を示します。DNS サーバの IP アドレスを設定した後、www.cisco.com に正常に ping できるようになります。

```
configure terminal
 ip domain name mycompany.com
 ip name-server 10.2.203.1
 end
  ping www.cisco.com
```

シスコからのダウンロードのための SSL 証明書の設定：例

Cisco IOS Auto-Upgrade Manager を使用してシスコの Web サイトからイメージをダウンロードする前に、ルータ上でシスコのサーバの SSL 証明書を設定する必要があります。

次に、SSL 証明書を設定する例を示します。

```
configure terminal
 crypto pki trustpoint cisco_ssl_cert
  enrollment terminal
  revocation-check none
  exit
 crypto ca authenticate cisco_ssl_cert
!Enter the base 64 encoded CA certificate and end this with a blank line or the word
quit
. !The console waits for the user input. Paste the SSL certificate text and press Return.


-----BEGIN CERTIFICATE-----


<The content of the certificate>

-----END CERTIFICATE-----


!Trustpoint 'cisco_ssl_cert' is a subordinate CA and holds a non self signed cert
!Trustpoint 'cisco_ssl_cert' is a subordinate CA.
!but certificate is not a CA certificate.
!Manual verification required
!Certificate has the following attributes:
      ! Fingerprint MD5: 49CE9018 C0CC41BA 1D2FBEA7 AD3011EF
      ! Fingerprint SHA1: A88EAA5D 73D63CB7 BF25197B 9C35ED97 023BB57B

% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Cisco IOS Auto-Upgrade Manager の設定：例

次に、ルータ上で Cisco IOS Auto-Upgrade Manager を設定する例を示します。

```
configure terminal
autoupgrade disk-cleanup crashinfo
autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl
autoupgrade status status email smtp-server
```

その他の参考資料

次の項では、Cisco IOS Auto-Upgrade Manager の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS Auto-Upgrade Manager コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト、使用ガイドライン、および例	『Cisco IOS Configuration Fundamentals Command Reference』
Cisco ルータでの DNS の設定	『Configuring DNS on Cisco Routers』テクニカル ノート
ウォーム アップグレード	機能モジュールのウォーム アップグレード

標準

標準	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
なし	--

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco IOS Auto-Upgrade Manager の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6 : Cisco IOS Auto-Upgrade Manager* の機能情報

機能名	リリース	機能情報
Cisco IOS Auto-Upgrade Manager	12.4(15)T Cisco IOS XE Release 3.9S	Cisco IOS Auto-Upgrade Manager を使用すると、新しい Cisco IOSイメージを指定し、ダウンロードして、アップグレードするための単純なインターフェイスが利用できるようになり、ソフトウェア イメージのアップグレード プロセスが単純化されます。 12.4(15)T で、この機能が Cisco 1800、Cisco 2800、および Cisco 3800 シリーズ ルータに追加されました。 この機能は、Cisco IOS XE Release 3.9S に統合されました。 この機能により、次のコマンドが導入または変更されました。**autoupgrade disk-cleanup**、**autoupgrade ida url**、**autoupgrade status email**、**debug autoupgrade**、**show autoupgrade configuration unknown**、**upgrade automatic abortversion**、**upgrade automatic getversion**、**upgrade automatic runversion**

用語集

CLI -- コマンドライン インターフェイス

IDA or Cisco server -- Intelligent Download Application

Cisco IOS -- Cisco Internetworking Operating System