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，1 ページ
- デジタル署名付き Cisco ソフトウェアに関する制限事項，2 ページ
- デジタル署名付き Cisco ソフトウェアに関する情報，2 ページ
- デジタル署名付き Cisco ソフトウェア イメージの作業方法，6 ページ
- デジタル署名付き Cisco ソフトウェアの設定例，14 ページ
- その他の参考資料，20 ページ
- デジタル署名付き Cisco ソフトウェアの機能情報，21 ページ

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。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 19xx シリーズ、29xx シリーズ、および 39xx シリーズのルータには、このドキュメントで説明する機能が含まれています。

IOS XE ソフトウェアを実行する Cisco Catalyst 4500 E+Series スイッチと Cisco ASR 1002-X ルータには、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、ルータのキー 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. イネーブル化
2. **showversion**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**showversion** 例： `Router# 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. イネーブル化
2. **showsoftwareauthenticityrunning**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**showsoftwareauthenticityrunning** 例： `Router# 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. イネーブル化
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	イネーブル化 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 software authenticity file {flash0:filename | flash1:filename | flash:filename | nvram:filename | flash0:filename | flash1:filename}** 例： `Router# show software authenticity file usbflash0: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. イネーブル化
2. **showsoftwareauthenticitykeys**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**showsoftwareauthenticitykeys** 例： `Router# 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 ソフトウェアの製品キーの失効の実行

以下のタスクを実行して、デジタル署名付き Cisco ソフトウェアの製品キーを失効させます。

はじめる前に

この作業は、専用の失効イメージで実行する必要があります。

手順の概要

1. イネーブル化
2. **softwareauthenticitykeyaddproduction**
3. **showsoftwareauthenticityupgrade-status**
4. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
5. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
6. **upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path]
7. reload [/verify | /noverify] [line | in [hhh:mm | mmm [text]] | at hh:mm [text] | reason [reason string] | cancel]
8. **softwareauthenticitykeyrevokeproduction**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**softwareauthenticitykeyaddproduction** 例： `Router# software authenticity key add production`	失効イメージから実行した場合は、バンドルされた製品キーをデジタル署名付き Cisco ソフトウェアが稼働中のルータのキー ストレージに追加します。 • 特別イメージまたは製品イメージでこのコマンドを使用した場合、エラー メッセージが表示されます。
ステップ 3	**showsoftwareauthenticityupgrade-status** 例： `Router# show software authenticity upgrade-status`	Cisco IOS デジタル署名付きイメージ ファイルおよび ROMMON ファイルに関するソフトウェア認証アップグレード ステータス情報を表示します。
ステップ 4	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* 例： `Router# copy tftp: usbflash0:`	TFTP サーバから選択したルータ ストレージ領域にイメージをコピーします。 • このコマンドで、新しい製品キーで署名された新しい製品 ROMmon イメージが、選択されたルータ ストレージにコピーされます。
ステップ 5	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* 例： `Router# copy /verify tftp: usbflash0:`	TFTP サーバから選択したルータ ストレージ領域にイメージをコピーします。 • このコマンドで、新しい製品キーで署名された新しい製品イメージが、選択されたルータ ストレージにコピーされます。 • コピー プロセス中に新しいイメージの署名を検証するために /verify オプションを使用することを推奨します。
ステップ 6	**upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path] 例： `Router# upgrade rom-monitor file flash0:C3900_ROMMON_RM2.srec.SPB`	ROM モニタ（ROMMON）イメージをアップグレードします。

	コマンドまたはアクション	目的
ステップ 7	reload [/verify | /noverify] [line | in [hhh:mm | mmm [text]] | at hh:mm [text] | reason [reason string] | cancel] 例： `Router# reload`	ルータ上でソフトウェアをリロードします。 （注） ウォーム アップグレード機能は、キー失効をサポートしていません。
ステップ 8	**softwareauthenticitykeyrevokeproduction** 例： `Router# software authenticity key revoke production`	製品イメージから実行するときに、キー ストレージの古い製品キーを失効させるか、無効にします。 • 特別イメージでこのコマンドを使用した場合、エラーメッセージが表示されます。 （注） この手順は、リロード完了後に実行する必要があります。 スケジューリングされたリロード時に、この点を認識していることは重要です。

デジタル署名付き Cisco ソフトウェアの特別キーの失効の実行

以下のタスクを実行して、デジタル署名付き Cisco ソフトウェアの特別キーを失効させます。

はじめる前に

以下のタスクは、製品イメージで実行する必要があります。

手順の概要

1. イネーブル化
2. **softwareauthenticitykeyaddspecial**
3. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
4. **copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url*
5. **upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path]
6. **softwareauthenticitykeyrevokespecial**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**softwareauthenticitykeyaddspecial** 例： `Router# software authenticity key add production`	デジタル署名付き Cisco ソフトウェアでロードしたルータのキー ストレージに新しい特別キーを追加します。 • 失効イメージまたは特別イメージでこのコマンドを使用した場合、エラー メッセージが表示されます。
ステップ 3	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* 例： `Router# copy tftp: usbflash0:`	TFTP サーバから選択したルータ ストレージ領域にイメージをコピーします。 • この行で、新しい特別キーで署名された新しい特別 ROMmon イメージが、選択されたルータ ストレージ領域にコピーされます。
ステップ 4	**copy** [**/erase**] [**/verify** | **/noverify**] *source-urldestination-url* 例： 例： 例： 例： `Router# copy /verify tftp: usbflash0:`	TFTP サーバから選択したルータ ストレージ領域にイメージをコピーします。 • この行で、新しい特別キーで署名された新しい特別イメージが、選択されたルータ ストレージ領域にコピーされます。 • コピープロセス中に新しいイメージの署名を検証するために /verify オプションを使用することを推奨します。
ステップ 5	**upgrade rom-monitor file {archive: | cns: | flash0: | flash1: | flash: | ftp: | http: | https: | null: | nvram: | rcp: | scp: | system: | tar: | tftp: | tmpsys: | usbflash0: | xmodem: | ymodem:}** [file-path] 例： `Router# upgrade rom-monitor file flash0:C3900_ROMMON_RM2.srec.SSB`	特権 EXEC モードで、ROM モニタ（ROMmon）イメージをアップグレードします。

	コマンドまたはアクション	目的
ステップ 6	**softwareauthenticitykeyrevokespecial** 例： `Router# software authenticity key revoke special`	製品イメージから実行するときに、キー ストレージの古い特別キーを失効させるか、無効にします。 • 特別イメージまたは失効イメージで実行した場合、エラー メッセージが表示されます。

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. イネーブル化
2. **debugsoftwareauthenticity{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	イネーブル化 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	**debugsoftwareauthenticity{envelope|errors|key|revocation|show|verbose}** 例： `Router# 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。

```
Router# 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。

```
Router# 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。
組織単位	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。

フィールド	説明
組織名	ソフトウェア イメージの所有者を表示する。
証明書シリアル番号	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。

Router# **showsoftwareauthenticityfileflash0:**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。
組織単位	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。
組織名	ソフトウェア イメージの所有者を表示する。
証明書シリアル番号	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。

```
Router# 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 ソフトウェアの特別キーの失効の実行例

次の例では、特別キー失効プロセスを表示します。

```
Router# software authenticity key add special
Validating running image...
Validating new special key...
Adding the key to Primary
Checking for duplicate keys
Writing the key...e.Success
Adding the key to Backup
Checking for duplicate keys
Writing the key...e.Success
Done!
```

software authenticity key add special コマンドは、新しい特別キーをルータのプライマリとバックアップのストレージ領域に追加し、重複するキーが存在しないことを確認します。

```
Router# copy tftp: usbflash0:
Address or name of remote host []? 209.165.200.226
Source filename []? rommon_image_location/ C3900_rom-monitor.srec.SSB
```

新しい特別キーを持つ新しい ROMmon 特別イメージ ファイルは、ROMmon ストレージ領域（usbflash0:）にコピーされます。

```
Router# copy /verify tftp: usbflash0:
```

```
Address or name of remote host []? 209.165.200.225
Source filename []? image_location/c3900-universalk9-mz.SSB
Destination filename [c3900-universalk9-mz.SSB]?
Accessing tftp:// 209.165.200.225/image_location/c3900-universalk9-mz.SSB...
Loading image_location/c3900-universalk9-mz.SSB from 209.165.200.225 (via GigabitEthernet0/0):

!!!
```

```
Scanning the keys in Primary
Revoking the key with version A...e.Success
Scanning the keys in Backup
Revoking the key with version A...e.Success
Done!

Router#
*Mar  8 10:29:17.219 PST: %DIGISIGN-4-DEV_IMAGE: Upgradable rommon software signed using
special key version B
```

古い特別キー（Rev A）は、プライマリおよびバックアップ キーストレージ領域で失効されます。

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の例

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。

```
Router# 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 ソフトウェア アクティベーションの概要	『Cisco IOS Software Activation Conceptual Overview』
Cisco IOS ソフトウェア アクティベーションに関連するコマンド	『Cisco IOS Software Activation Tasks and Commands』

標準

規格	タイトル
なし	--

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

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
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	15.0(1)M、15.0(1)M2、15.1(1)T、Cisco IOS XE_3.1.0SG	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。 Cisco IOS リリース 15.0(1)M では、この機能が Cisco 1941、2900、3900 ルータで導入されました。 この機能は、Cisco IOS リリース 15.1(1)T に統合されました。 この機能は、Catalyst 4500 E+Series スイッチの Cisco IOS XE リリース 3.1.0.SG に統合されました。 コマンド **debugsoftwareauthenticity**、**showsoftwareauthenticityfile**、**showsoftwareauthenticitykeys**、**showsoftwareauthenticityrunning** の導入または変更が行われました。

機能名	リリース	機能情報
キー失効機能のサポート	15.0(1)M2、15.1(1)T	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 この機能は、Cisco IOS リリース 15.1(1)T に統合されました。 コマンド **debugsoftwareauthenticity**、**showsoftwareauthenticityupgrade-status**、**softwareauthenticitykeyadd**、**softwareauthenticitykeyrevoke**、**upgraderom-monitorfile** の導入または変更が行われました。