



ソフトウェアのインストール

この章は、次の項で構成されています。

- [ソフトウェアのインストール](#) (1 ページ)
- [IOS XE ダウングレードの警告](#) (5 ページ)
- [セキュアデータワイプ機能の有効化](#) (5 ページ)
- [ROMMON イメージ](#) (6 ページ)
- [ファイル システム](#) (6 ページ)
- [USB アクセスを有効または無効にするためのオプション](#) (7 ページ)
- [自動生成されるファイル ディレクトリおよびファイル](#) (9 ページ)
- [フラッシュ ストレージ](#) (10 ページ)
- [LED インジケータ](#) (10 ページ)
- [初期ブートアップセキュリティの改善点](#) (11 ページ)
- [関連資料](#) (11 ページ)

ソフトウェアのインストール

ルータにソフトウェアをインストールする際には、統合パッケージ（ブート可能イメージ）をインストールします。これはサブパッケージ（モジュール型ソフトウェアユニット）のバンドルで構成されており、各サブパッケージはそれぞれ異なる機能セットを制御します。

ソフトウェアをインストールする主要な方法として、次の 2 つの方法があります。

- 統合パッケージを使用して実行されるルータの管理および設定：この方法では、サブパッケージを個別にアップグレードでき、次に説明する方法と比較して、通常はブート時間が短くなります。モジュールのソフトウェアを個別にアップグレードする場合は、この方法を使用します。
- 個別のパッケージを使用して実行されるルータの管理および設定：これは、Cisco ルータ全般でサポートされている標準的な Cisco ルータ イメージインストールおよび管理に類似した、シンプルな方法です。

サービスの中断が可能な、予定されている保守期間内にソフトウェアのアップグレードを実行することをお勧めします。ソフトウェアアップグレードを有効にするには、ルータをリブートする必要があります。

ライセンス

この項の内容は、次のとおりです。

シスコソフトウェアのライセンス

シスコソフトウェアライセンスは、シスコソフトウェアライセンスを入手して検証することで Cisco IOS ソフトウェアのセットをアクティブ化するためのプロセスとコンポーネントで構成されています。

ライセンス付き機能を有効にし、ルータのブートフラッシュにライセンスファイルを格納することができます。ライセンスは、統合パッケージ、テクノロジーパッケージ、または個別の機能を対象とします。

IR1101 はスマートライセンスを使用します。これについては、次の章で詳しく説明します。

IR1101 は使用権ライセンスをサポートせず、Specific License Reservation (SLR) のみをサポートしています。

統合パッケージ

ルータのソフトウェアイメージを取得するには、次にアクセスしてください。
<https://software.cisco.com/download/home/286319772/type>



(注) IR1101 にすべての IOS XE 機能セットが適用されない場合があります。一部の機能はまだ実装されていないか、このプラットフォームに適していない可能性があります。

あるライセンスに対応するすべてのサブシステムを起動させるために、イメージベースのライセンスが使用されます。このライセンスは、ブート時にのみ適用されます。

IR1101 ルータには、次のイメージベースライセンスのいずれかを事前にインストールできます。

- Network-Essentials
- Network-Advantage



(注) Network-Essentials および Network-Advantage の内容の詳細については、次の製品データシートを参照してください。

<https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html>

Network-Essentials

Network-Essentials テクノロジー パッケージには、ベースライン機能が含まれています。また、セキュリティ機能もサポートしています。

Network-Essentials_npe パッケージ (npe=ペイロード暗号化なし) には、ペイロード暗号化機能を除く **Network-Essentials** テクノロジー パッケージのすべての機能が含まれています。これは、輸出規制要件への準拠に伴うものです。**Network-Essentials_npe** は、**Network-Essentials_npe** イメージでのみ使用できます。したがって**Network-Essentials** パッケージと**Network-Essentials_npe** パッケージの機能の相違点は、ペイロード暗号化機能 (IPsec や Secure VPN など) のセットです。

Network-Advantage

Network-Advantage テクノロジー パッケージには、すべての暗号化機能が含まれています。

Network-Advantage_npe パッケージ (npe=ペイロード暗号化なし) には、ペイロード暗号化機能を除く **Network-Advantage** テクノロジー パッケージのすべての機能が含まれています。これは、輸出規制要件への準拠に伴うものです。**Network-Advantage_npe** パッケージは、**Network-Advantage_npe** イメージでのみ使用できます。したがって**Network-Advantage** パッケージと**Network-Advantage_npe** パッケージの機能の相違点は、ペイロード暗号化対応機能 (IPsec や Secure VPN など) のセットです。

関連資料

ソフトウェア ライセンスの詳細については、「スマートライセンス」の章を参照してください。

Cisco IOS XE 用ソフトウェアのインストール方法

ソフトウェアをインストールするには、「[ソフトウェアのインストール \(1 ページ\)](#)」の章に記載されている次のいずれかの方法を使用します。

Cisco IOS XE リリースのインストール

デバイスは Cisco IOS XE イメージを使って初めて起動するとき、インストールされている ROMMON のバージョンをチェックし、システムが古いバージョンを実行している場合はアップグレードします。アップグレードプロセス中はデバイスの電源を再投入しないでください。新しいバージョンの ROMMON がインストールされると、システムは自動的にデバイスを再起動します。インストール後、システムは Cisco IOS XE イメージを通常どおりに起動します。



- (注) デバイスを初めて起動したときにアップグレードが必要な場合、起動プロセス全体に数分かかることがあります。このプロセスでは、ROMMON をアップグレードするため、通常の起動よりも長くなります。

次の例は、統合パッケージの起動プロセスを示しています。

```

Router# configure terminal
Router(config)#boot sys bootflash:ir1101-universalk9.16.10.01.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router#
*Nov 7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#show run | inc license
license udi pid IR1101-K9 sn FCW2150TH0F
license boot level network-advantage
Router#
Router#reload ?
  /noverify Don't verify file signature before reload.
  /verify   Verify file signature before reload.
  at        Reload at a specific time/date
  cancel    Cancel pending reload
  in        Reload after a time interval
  pause     Pause during reload
  reason    Reload reason
  <cr>     <cr>

Router#reload /verify

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
*Nov 7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Verifying file integrity of bootflash:/ir1101-universalk9.16.10.01.SPA.bin.....
.....

Embedded Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Computed Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Starting image verification
Hash Computation: 100%Done!
Computed Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                5b343e6f7aecdd70e50e5203909aec8f
                3d276529d2a6af6859d4c77237f812d5
                0da93678edc942c8874edca2d5224101

Embedded Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                5b343e6f7aecdd70e50e5203909aec8f
                3d276529d2a6af6859d4c77237f812d5
                0da93678edc942c8874edca2d5224101

Digital signature successfully verified in file
bootflash:/ir1101-universalk9.16.10.01.SPA.bin
Signature Verified

Proceed with reload? [confirm] <Enter>

*Jul 9 06:43:37.910: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command. Jul 9 14:43:59.134: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
process exit with reload chassis code

watchdog watchdog0: watchdog did not stop!
reboot: Restarting system

Press RETURN to get started!

```

IOS XE ダウングレードの警告

この機能は、**boot system flash** コマンドに続けて、実行中のイメージのいずれかよりバージョン番号が小さいイメージのファイル名を発行すると、警告を表示します。ユーザーに表示される警告メッセージを無視することで、ダウングレード操作は引き続き可能です。実行中のイメージと同じまたはそれ以上のバージョンでのイメージの起動は、警告なしで許可されます。この機能は、ルータのブートフラッシュにすでにロードされているイメージのみ、つまり、**boot system flash <file_name> CLI** のみを対象としています (ftp、mop、rpc、tftp、rom などのその他のソース/デバイスを除く)。

システムがバージョンを比較する方法の例を次に示します。

次のように 2 つのバージョン番号を比較する場合：

- 17.7.1
- 17.7.1c

文字の付いたバージョン (17.7.1c) が、最新のバージョンとみなされます。

次のように 2 つのバージョン番号を比較する場合：

- 17.7.3a
- 17.7.3f

比較は、アルファベット順を考慮して行われます。上記の場合、17.7.3f が最新のバージョンとみなされます。

セキュアデータワイプ機能の有効化

セキュアデータワイプは、すべての IOS XE ベースのプラットフォーム上のストレージデバイスが NIST SP 800-88r1 準拠の安全に消去するコマンドを使用して適切に消去されるようにするためのシスコ全体のイニシアチブです。可能な限り常に、IoT プラットフォームは、対応する ENG の設計とこれまでのプラットフォームで利用可能な実装を活用します。

この機能は、次の IoT プラットフォームでサポートされます。

- IR1101
- IR1800
- IR8140
- ESR6300

セキュアデータワイプの有効化が実行されると、以下が消去されます。

- IR1101、IR1800、IR8140 : NVRAM、rommon 変数、およびブートフラッシュ
- ESR6300 : NVARM、rommon 変数、ブートフラッシュ

コマンドの実行後、ルータは工場出荷時のデフォルト設定（ボーレート9600）でrommonプロンプトになります。TFTPダウンロード（プラットフォームでサポートされている場合）またはusbflashを介してIOSイメージで起動するまで、ブートフラッシュはフォーマットされません。

セキュアデータワイプの実行

この機能を有効にするには、次を実行します。

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure?
[confirm]Y
```



重要 この操作には数時間かかる場合があります。電源を入れ直さないでください。
コマンドの実行後にログを確認し、IOS XE を起動するには、次の手順を実行します。

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

ROMMON イメージ

ROMMON イメージは、ルータのROM モニタ（ROMMON）ソフトウェアで使用されるソフトウェアパッケージです。このソフトウェアパッケージは、ルータの起動に通常使用される統合パッケージとは別のものです。

独立したROMMON イメージ（ソフトウェアパッケージ）がリリースされることがあります。新しいROMMON ソフトウェアを使ってルータをアップグレードできます。詳細な手順については、ROMMON イメージに付属のマニュアルを参照してください。



(注) ROMMON イメージの新しいバージョンは、常にルータの統合パッケージと同時にリリースされるとは限りません。

ファイル システム

次の表に、シスコ IR1101 シリーズ ルータで表示可能なファイル システムのリストを示します。

表 1: ルータのファイル システム

ファイルシステム	説明
bootflash:	ブートフラッシュ メモリのファイル システム。
flash:	上記のブートフラッシュ メモリのファイル システムのエイリアス。
cns:	Cisco Networking Service のファイル ディレクトリ。
nvrn:	ルータの NVRAM。NVRAM 間で startup-config をコピーできます。
obfl:	オンボード障害ロギング (OBFL) ファイル用のファイル システム。
system:	実行コンフィギュレーションを含む、システムメモリ用のファイル システム。
tar:	アーカイブ ファイル システム。
tmsys:	一時システム ファイルのファイル システム。
usbflash0:	Universal Serial Bus (USB) フラッシュ ドライブのファイル システム。 (注) USB フラッシュ ドライブのファイル システムは、USB ドライブ USB ポートに装着されている場合にのみ表示されます。

上の表に記載されていないファイルシステムがある場合は、?ヘルプオプションを使用します。

USB アクセスを有効または無効にするためのオプション

USB フラッシュドライブは、イメージ、コンフィギュレーション ファイル、その他のファイルを保存するための安価で簡単に使えるストレージを提供します。



- (注) IR1101 は、USB フラッシュドライブの ext2 および vfat ファイルシステムをサポートしていません。

IR1101 は、USB フラッシュドライブのホットプラグ/アンプラグをサポートしています。USB フラッシュドライブにアクセスするには、デバイスをルータの USB インターフェイスに挿入します。USB が認識されると、コンソールにアラートメッセージが表示されます。

```
Aug 1 11:08:53.198 PDT: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
```

このメッセージが表示されたら、USB フラッシュドライブにアクセスできます。ユーザは、**dir usbflash0:** コマンドを使用して USB コンテンツにアクセスできます。

```
Device#dir usbflash0:
Directory of usbflash0:/
 5  drwx                    512  Aug 23 2019 10:42:18 -07:00  System Volume Information
```

USB アクセスを有効または無効にするためのオプション

```

    6  -rwx                35  Aug 27 2019 17:40:38 -07:00  test.txt
206472192 bytes total (206470144 bytes free)
Device#

```

copy コマンドを使用して、USB フラッシュドライブとの間でファイルをコピーできます。コピーが完了すると、コピーされたバイト数を示すログメッセージが表示されます。

```

Device#copy flash:test.txt usbflash0:
Destination filename [test.txt]? <Enter>
Copy in progress...C
35 bytes copied in 0.020 secs (1750 bytes/sec)
Device#

```

USB フラッシュドライブのホットプラグ/アンプラグはサポートされていますが、この機能にはセキュリティの脆弱性が伴います。ユーザが機密情報を USB フラッシュドライブにコピーできないようにするために、USB の有効化/無効化機能が追加されました。

デフォルトでは、USB フラッシュドライブは有効になっています。ユーザが USB を無効にする場合は、**disable** コマンドを使用します。

```

Device# config terminal
Device(config)#platform usb disable

Device(config)#end

```

USB フラッシュドライブを無効にするとファイルシステムはデバイスに表示されず、USB を挿入しても syslog メッセージは表示されません。ユーザは USB の内容にアクセスできません。

次に例を示します。

```

Device#dir usbflash0:
dir usbflash0:
^
% Invalid input detected at '^' marker.
Device#

```

disable コマンドで「**no**」を発行すると、USB が有効になります。

```

Device#config terminal

Device(config)#no platform usb disable
Device(config)#end

```

USB のステータスは、次のコマンドで表示できます。

```

Device#show platform usb status
USB enabled
Device#

```

USB ポートは潜在的なセキュリティリスクと見なされる可能性があります。USB ポートを無効にするには、次の手順を実行します。

```

Configure terminal
platform usb disable
exit

```


自動生成されるファイル ディレクトリおよびファイル

ここでは、作成可能な自動生成ファイルとディレクトリについて、およびこれらのディレクトリ内のファイルを管理する方法について説明します。

表 2: 自動生成されるファイル

ファイルまたはディレクトリ	説明
crashinfo ファイル	<p>crashinfo ファイルが bootflash: ファイルシステムに保存されることがあります。</p> <p>これらのファイルにはクラッシュに関する説明情報が含まれており、調整やトラブルシューティングに役立ちます。ただし、これらのファイルはルータ動作には使用されないため、消去してもルータの機能には影響がありません。</p>
core ディレクトリ	<p>.core ファイルのストレージ領域</p> <p>このディレクトリは消去されると、ブートアップ時に自動的に再生成されます。このディレクトリ内の .core ファイルは、ルータ機能に影響を及ぼさずに消去することはできますが、ディレクトリ自体は消去しないでください。</p>
managed ディレクトリ	<p>システムチェックが実行されると、ブートアップ時にこのディレクトリが作成されます。このディレクトリが表示されることは完全に正常な状態であり、ルータに問題が発生したわけではありません。</p>
tracelogs ディレクトリ	<p>trace ファイルのストレージ領域</p> <p>trace ファイルはトラブルシューティングに役立ちます。たとえば Cisco IOS プロセスに障害が発生した場合、ユーザやトラブルシューティング担当者は診断モードを使って trace ファイルにアクセスし、Cisco IOS 障害に関連する情報を収集できます。</p> <p>ただし、trace ファイルはルータ動作には使用されないため、消去してもルータのパフォーマンスには影響がありません。</p>

自動生成されるディレクトリに関する重要事項

自動生成されるディレクトリに関する重要な情報は次のとおりです。

- Cisco カスタマーサポートからの指示がない限り、bootflash: ディレクトリに自動生成されたファイルの削除、名前変更、移動、またはその他の変更を行わないでください。



(注) **bootflash:** に自動生成されたファイルを変更すると、システムパフォーマンスに予期せぬ結果をもたらす場合があります。

- **core** および **tracelogs** ディレクトリ内の **Crashinfo** ファイルとファイルは削除できます。

フラッシュストレージ

サブパッケージは、フラッシュなどのローカルメディアストレージにインストールされます。フラッシュストレージの場合は **dir bootflash:** コマンドを使用するとファイル名がリストされます。



(注) ルータが正常に動作するためにはフラッシュストレージが必要です。

LED インジケータ

ルータの LED の詳細については、『[Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide](#)』の「Product Overview」の項の「LED Indicators」を参照してください。

システムの LED ステータス、アラームおよびインターフェイスポートを監視するため、IOS モードでは **show LED** コマンドラインがサポートされています。

```
Router# show LED
SYSTEM LED : Green

Custom LED : Off

VPN LED : Off

ALARM LED : Off

GigabitEthernet0/0/0 LED : Off
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off
GigabitEthernet0/0/5 LED : On

EM Module digital I/O 1 LED : Off
EM Module digital I/O 2 LED : Off
EM Module digital I/O 3 LED : Off
EM Module digital I/O 4 LED : Off

*System LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
```

```
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On

*EM Module LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On
Router#
```

カスタム制御 LED

IR-1101 には点滅しない3色のカスタム LED があり、次のエグゼクティブ権限 CLI で制御できます。

```
router# set platform hardware custom-led <0-7>
```

0～7の番号は次のとおりです。

- 0 : 消灯
- 1 : 青
- 2 : 緑
- 3 : 赤
- 4 : 青/緑
- 5 : 青/赤
- 6 : 緑/赤
- 7 : 青/緑/赤

初期ブートアップセキュリティの改善点

この項の内容は、次のとおりです。

関連資料

ソフトウェア ライセンスの詳細については、「スマートライセンス」の章を参照してください。

機能ライセンスの取得とインストールの詳細については、「[Configuring the Cisco IOS Software Activation Feature](#)」を参照してください。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。