2.3.2.x から 2.3.3.x または 2.3.4.x

Catalyst Center ISO イメージからの新規インストール

オフライン インストール ワークフロー

オフラインの Catalyst Center のインストールには、次の手順が含まれます。

1. イメージをダウンロードします。
2. ダウンロードしたファイルを確認します。
3. ブート可能な USB ドライブを作成します。
4. Catalyst Center ISO イメージをインストールします。
5. Catalyst Center アプライアンスを設定します。
6. 初期設定を完了します。
7. デバイス EULA に同意します。
8. アプリケーションをインストールします。

イメージのダウンロード

お客様またはシスコのアカウント担当者が TAC リクエストを行う必要があります。その後、TAC の担当者が、シスコのファイルサーバーからバイナリイメージをダウンロードするためのアクセス権と手順を提供します。

ステップ 1 インターネット経由でアクセス可能なシスコのファイルサーバーにログインします。

ステップ 2 指定された場所から Catalyst Center バイナリイメージ（.bin）をダウンロードします。

ステップ 3 署名検証用のシスコ公開キー（cisco_image_verification_key.pub）をダウンロードします。

ステップ 4 イメージのセキュア ハッシュ アルゴリズム（SHA512）チェックサムファイルをダウンロードします。

ステップ 5 バイナリイメージの署名ファイル（.sig）をダウンロードします。

ダウンロードしたファイルの確認

ポータルで提供されるシスコの署名検証と SHA512 チェックサムを使用して、ダウンロードしたイメージの完全性を確認します。

ステップ 1 （オプション）SHA 検証を実行して、不完全なダウンロードによってバイナリイメージが破損していないかを確認します。

OS に応じて、次のコマンドのいずれかを入力します。

- Linux：

  ```
  sha512sum Catalyst-Center-image-filename
  ```

- Mac：

  ```
  shasum -a 512 Catalyst-Center-image-filename
  ```

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256 | md5
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windowsでは、Windows PowerShell を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

実行したコマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、バイナリイメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 2 署名を確認し、バイナリイメージが正規のものでシスコ製であることを確認します。

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

このコマンドは Mac と Linux の両方の環境で動作します。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります。

バイナリイメージが正規であれば、このコマンドを入力すると、「Verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、バイナリイメージをインストールせず、シスコサポートにお問い合わせください。

ブート可能な USB ドライブの作成

Cisco ISO イメージをダウンロードしたことを確認してから、Catalyst Center ISO イメージを含むブート可能 USB ドライブを作成します。詳細については、『Cisco Catalyst Center Second-Generation Appliance Installation Guide』の「Prepare the Appliance for Configuration」の章の「Create a Bootable USB Flash Drive」のトピックを参照してください。

Catalyst Center ISO イメージのインストール

ステップ 1 Catalyst Center ISO イメージを含むブート可能 USB ドライブをアプライアンスに接続します。

ステップ 2 Cisco IMC にログインし、KVM セッションを開始します。

ステップ 3 アプライアンスの電源を投入または再投入します。

- アプライアンスが現在実行されていない場合には、**[Power]** > **[Power On System]** を選択します。
- アプライアンスがすでに実行されている場合には、**[Power]** > **[Power Cycle System (cold boot)]** を選択します。

ステップ 4 表示されたポップアップウィンドウで **[Yes]** をクリックして、サーバ制御アクションを実行しようとしていることを確認します。

ステップ 5 シスコのロゴが表示されたら、**F6** キーを押すか、[KVM] メニューから **[Macros]** > **[User Defined Macros]** > **[F6]** を選択します。ブートデバイス選択メニューが表示されます。

ステップ 6 USB ドライブを選択してから、**Enter** を押します。

ステップ 7 [GNU GRUB] ブートローダーウィンドウで、[Cisco DNA Center Installer] を選択し、**Enter** を押します。

（注） 30 秒以内に選択しなかった場合、ブートローダーが自動的に Maglev インストーラを起動します。

Catalyst Center アプライアンスの設定

Catalyst Center ISO イメージのインストールが完了すると、インストーラがリブートし、Maglev 設定ウィザードの初期画面が開きます。ネットワークで日常使用するアプライアンスを設定するには、次のいずれかの項で説明されている手順を実行します。

- Maglev 構成ウィザードを使用する場合は、『Cisco Catalyst Center Second-Generation Appliance Installation Guide』の「Configure the Appliance Using the Maglev Wizard」を参照してください。

- 44 または 56 コアアプライアンスを設定するためにブラウザベースの構成ウィザードを使用する場合は、『Cisco Catalyst Center Second-Generation Appliance Installation Guide』の「Configure the 44/56-Core Appliance Using the Browser-Based Wizard」を参照してください。
- 112 コアアプライアンスを設定するためにブラウザベースの構成ウィザードを使用する場合は、『Cisco Catalyst Center Second-Generation Appliance Installation Guide』の「Configure the 112-Core Appliance Using the Browser-Based Wizard」を参照してください。

初期設定の完了

ステップ 1 Catalyst Center アプライアンスのリブートが完了したら、ブラウザを起動します。

ステップ 2 HTTPS:// と設定プロセスの最後に表示された Catalyst Center GUI の IP アドレスを使用して、Catalyst Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（ブラウザによって異なります）。

- Google Chrome：接続のプライバシーは保護されません
- Mozilla Firefox：警告：今後セキュリティリスクが見つかる潜在的可能性があります

ステップ 3 メッセージを無視して **[詳細設定（Advanced）]** をクリックします。次のメッセージが表示されます。

- Google Chrome：`This server could not prove that it is GUI-IP-address; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.`
- Mozilla Firefox：`Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.`

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Catalyst Center での証明書の使用方法については、『Cisco Catalyst Center Administrator Guide』の「Certificate and Private Key Support」の項を参照してください。

ステップ 4 メッセージを無視し、次のいずれかを実行します。

- Google Chrome：[Proceed to <*GUI-IP-address*> (unsafe)] リンクをクリックします。
- Mozilla Firefox：**[リスクを理解して続行する（Accept the Risk and Continue）]** をクリックします。

[ログイン（Login）]Catalyst Center ウィンドウが表示されます。

ステップ 5 [Login] ウィンドウで Catalyst Center の設定時に設定した管理ユーザー名（admin）とパスワードを入力し、[Log In] をクリックします。
[ログインのリセット（Reset Login）] ウィンドウが表示されます。

ステップ 6 古いパスワードを入力してから、スーパーユーザ権限を持つ管理者の新しいパスワードを入力して確認し、**[保存（Save）]** をクリックします。

[Cisco.com ID の入力（Enter Cisco.com ID）] ウィンドウが表示されます。

ステップ 7 （この手順はスキップ）Cisco.com ユーザーのユーザー名とパスワードを入力してから [Next] をクリックします。Cisco.com ユーザログインが既知の Cisco スマート アカウント ユーザログインと一致しない場合には、**[スマートアカウント（Smart Account）]** ウィンドウが表示されます。

ステップ 8 （この手順はスキップ）[Smart Account] ウィンドウが表示された場合には、組織のスマートアカウントのユーザー名とパスワードを入力するか、対応するリンクをクリックして新しいスマートアカウントを開きます。完了したら **[次へ（Next）]** をクリックします。
[IP アドレスマネージャ（IP Address Manager）] ウィンドウが表示されます。

ステップ 9 組織が外部 IP アドレスマネージャ（IPAM）を使用している場合には、次の手順を実行してから **[次へ（Next）]** をクリックします。

- IPAM サーバの名前と URL を入力します。
- サーバへのアクセスに必要なユーザ名とパスワードを入力します。
- 使用中の IPAM プロバイダー（Infoblox など）を選択します。
- Catalyst Center で使用する利用可能な IP アドレスの特定のビューを IPAM サーバデータベースで選択します。

[プロキシサーバの入力（Enter Proxy Server）] ウィンドウが表示されます。

ステップ 10 [Next] をクリックします。
ソフトウェアの **[EULA]** ウィンドウが表示されます。

ステップ 11 **[次へ（Next）]** をクリックして、ソフトウェアのエンドユーザライセンス契約書に同意します。
[準備完了（Ready to go!）] ウィンドウが表示されます。

ステップ 12 シスコでは、[User Management] リンクをクリックして、[User Management] ウィンドウを表示することを推奨しています。**[追加（Add）]** をクリックして、新しい Catalyst Center ユーザの追加を開始します。新しいユーザの名前とパスワードを入力し、ユーザのロールを選択したら、**[保存（Save）]** をクリックして新しいユーザを作成します。初期展開の新しいユーザすべてが追加されるまで、必要に応じてこの手順を繰り返します。ネットワーク管理者ロール（NETWORK-ADMIN-ROLE）を持つユーザを少なくとも 1 人作成してください。

デバイス EULA への同意

ステップ 1 Catalyst Center クラスタにログインし、ディレクトリを目的の場所に変更します。次に例を示します。

```
$ cd /mnt/install-artifacts/eula
$ ls
finalize_offline_installation-1.3.0.147.bin
```

ステップ 2 権限を変更します。

```
$ sudo chmod 755 finalize_offline_installation-1.3.0.147.bin
[sudo] password for maglev:
```

ステップ 3 次のコマンドを入力します。

```
$ sudo ./finalize_offline_installation-1.3.0.147.bin -Y
```

-Y 引数は、Catalyst Center ソフトウェアライセンス EULA に同意することを示します。

（注） Catalyst Center **GUI の[Design]** > **[Image Repository]** では、イメージの EULA は引き続き同意されていないと表示されますが、これは予期されることであり、機能的な影響はありません。

アプリケーションのインストール

前述のタスクを完了すると、uber ISO に多数のアプリケーションがロードされているので、インストールする必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Software Management]** の順に選択します。

（注） この時点で、Catalyst Center によって接続性チェックが実行されます。接続に問題がある場合、[Software Management] ウィンドウに、現在利用可能なアプリケーション更新は表示されません。

ステップ 2 アプリケーション更新が利用可能な場合は、ウィンドウの下部に表示されます。次のいずれかを実行します。

- 利用可能なすべてのアプリケーション更新をインストールするには、[Select All] リンクをクリックします。
- 個々のアプリケーション更新をインストールするには、該当するチェックボックスをオンにします。

（注） 更新のファイルサイズおよび対応するアプリケーションの簡単な説明を示すスライドインペインを開くには、その [More details] リンクをクリックします。

ステップ 3 [Install] をクリックします。

ステップ 4 Catalyst Center による依存関係のチェックが完了したら、[Continue] をクリックします。
更新中の各アプリケーションの進行状況バーがウィンドウに表示されます。すべての更新がインストールされると、[Software Management] ウィンドウが更新されます。

ステップ 5 [Currently Installed Applications] リンクをクリックし、選択したアプリケーションが更新されていることを確認します。

Catalyst Center バイナリイメージからの更新

前提条件

インストール済みの Catalyst Center のインスタンスをアップグレードする前に、次の前提条件を確認します。

- Catalyst Center にインターネット接続がないことを確認します。
- SUPER-ADMIN-ROLE 権限を持つユーザーのみが Catalyst Center のソフトウェア更新を実行することができます。
- Catalyst Center データベースのバックアップを作成します。バックアップの作成手順については、『Cisco Catalyst Center Administrator Guide』の「Backup and Restore」の章を参照してください。
- ダウンロードに使用可能な cisco.com ユーザーアカウントのユーザー名とパスワードがあること。有効な cisco.com ユーザーアカウントを使用できます。
- アップグレードプロセスには十分な時間を割り当てます。完了までに 6 時間以上かかる可能性があります。
- アップグレードプロセス中は、Catalyst Center またはそのアプリケーションやツールの使用はできるだけ避けてください。
- ディスクについて次の最小要件が満たされていることを確認します。
  - /パーティションに空き領域が 2 GB 以上あること。
  - /data パーティションに空き領域が 35 GB 以上あり、使用率が 70% 以下であること。
- **df -h** コマンドを使用して、ディスク容量を確認します。

```
$ df -h
Filesystem        Size  Used Avail Use% Mounted on
udev                                126G     0  126G   0% /dev
tmpfs                               26G   14M   26G   1% /run
/dev/sdb2                           29G   23G  4.5G  84% /
tmpfs                               126G     0  126G   0% /dev/shm
tmpfs                               5.0M     0  5.0M   0% /run/lock
tmpfs                               126G     0  126G   0% /sys/fs/cgroup
/dev/sdb3                           29G   44M   27G   1% /install2
/dev/sdb5                           374G   99G  256G  28% /data
/dev/sdb4                           9.3G  601M  8.2G   7% /var
/dev/sdc1                           420G  1.4G  397G   1%
/data/maglev/srv/fusion
/dev/sdc2                           1.4T   41G  1.3T   4%
/data/maglev/srv/maglev-system
/dev/sdd1                           3.5T  243M  3.3T   1% /data/maglev/srv/ndp
glusterfs-server.maglev-…ault_vol   1.4T   54G  1.3T   5%
/mnt/glusterfs/default_vol
[Fri Jan 10 18:59:27 UTC] maglev@10.82.128.100 (maglev-master-10-82-128-100) /
$
```

storage validation failed エラーが発生した場合は、Cisco TAC にお問い合わせください。

Catalyst Center のダウンロード、更新、またはインストール手順が何らかの理由で失敗した場合は、手順を必ず再試行してください。

オフライン更新ワークフロー

オフラインの Catalyst Center の更新には、次の手順が含まれます。

1. エアギャップ/オフライン更新用のイメージにアクセスするための TAC リクエストを行います。
2. シスコのファイルサーバーから Catalyst Center バイナリイメージをダウンロードします（インターネットへのアクセスが必要です）。
3. ダウンロードしたイメージの完全性を確認します。
4. ダウンロードしたイメージを、セキュアなエアギャップ環境の Catalyst Center クラスタに転送します。
5. Catalyst Center クラスタに SSH 接続し、バイナリを実行します。
6. Catalyst Center GUI にログインし、システムの更新とアプリケーションの更新を実行します。

イメージのダウンロード

お客様またはシスコのアカウント担当者が TAC リクエストを行う必要があります。その後、TAC の担当者が、シスコのファイルサーバーからバイナリイメージをダウンロードするためのアクセス権と手順を提供します。

ステップ 1 インターネット経由でアクセス可能なシスコのファイルサーバーにログインします。
ステップ 2 指定された場所から Catalyst Center バイナリイメージ（.bin）をダウンロードします。
ステップ 3 署名検証用のシスコ公開キー（cisco_image_verification_key.pub）をダウンロードします。
ステップ 4 イメージのセキュア ハッシュ アルゴリズム（SHA512）チェックサムファイルをダウンロードします。
ステップ 5 バイナリイメージの署名ファイル（.sig）をダウンロードします。

ダウンロードしたファイルの確認

ポータルで提供されるシスコの署名検証と SHA512 チェックサムを使用して、ダウンロードしたイメージの完全性を確認します。

ステップ 1 （オプション）SHA 検証を実行して、不完全なダウンロードによってバイナリイメージが破損していないかを確認します。

OS に応じて、次のコマンドのいずれかを入力します。

- Linux：

```
sha512sum Catalyst-Center-image-filename
```

- Mac：

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256 | md5
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windowsでは、Windows PowerShell を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

実行したコマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、バイナリイメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 2 署名を確認し、バイナリイメージが正規のものでシスコ製であることを確認します。

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

このコマンドは Mac と Linux の両方の環境で動作します。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります。

バイナリイメージが正規であれば、このコマンドを入力すると、「Verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、バイナリイメージをインストールせず、シスコサポートにお問い合わせください。

Catalyst Center へのファイルの転送

ステップ 1 サポートされているファイル転送メカニズム（SCP または SFTP）を使用して、ダウンロードしたイメージを Catalyst Center クラスタと /data/tmp パーティションに転送します。USB を使用する場合は、エアギャップネットワーク内の端末にイメージを転送してから、Catalyst Center クラスタと /data/tmp パーティションにイメージを転送します（SCP または SFTP 経由）。

ステップ 2 Catalyst Center クラスタにイメージを転送した後は、SHA 検証を再度実行して、プロセスでファイルが破損していないかどうかを確認します。

3 ノードクラスタに関する考慮事項

ステップ 1 3 ノード Catalyst Center クラスタの場合は、catalogserver ポッドが実行されているノードに bin ファイルをコピーします。

ステップ 2 カタログサーバーが実行されているノードの IP アドレスを確認するには、次のように入力します。

```
magctl service status catalogserver | grep Node:
```

たとえば、出力は次のようになります。

```
$ magctl service status catalogserver | grep Node:
Node: 192.192.192.72/192.192.192.72

[Thu Mar 19 22:59:48 UTC]maglev@192.192.192.68(maglev-master-192-192-192-68) ~
$
```

この例では、bin ファイルを **192.192.192.72** の /data/tmp パーティションにコピーします。

バイナリファイルの実行

ステップ 1 SSH を使用して Catalyst Center クラスタにログインします。

ステップ 2 次のコマンドを入力して、実行権限を追加します。

```
chmod +x <uber-bin-file>
```

ステップ 3 次のコマンドを入力して、バイナリファイルを実行します。

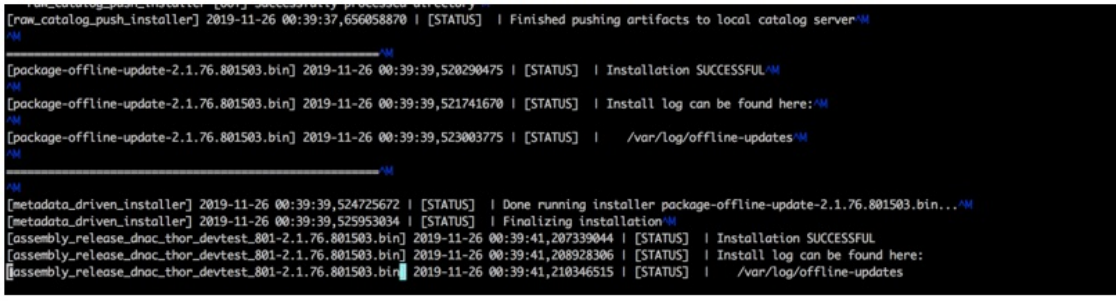
```
sudo ./<uber-bin-file>
```

このコマンドの出力は次のとおりです。

```
$ sudo ./<bin-filename>.bin
[sudo] password for maglev:
==============================
Welcome to DNAC offline update
==============================
Please provide your credentials to get started
[administration] username: admin <Catalyst Center login/password combo>
[administration] password for admin: <Catalyst Center password>
```

ステップ 4 バイナリファイルを実行すると、システムおよびアプリケーションパッケージのローカルカタログが更新されます。bin ファイルが正常に実行されたことを示す [Installation SUCCESSFUL] ステータスメッセージを見つけます。

ログファイル <*bin-filename*>-install.log を追跡することで、プロセスの現在のステータスを追跡できます。必要に応じて、/var/log/offlineupdates/ からログを確認することもできます。



オフライン更新の実行

Cisco DNA Center 2.3.2.x または 2.3.3.x から 2.3.4.x にアップグレードするには、以下の手順を実行します。

ステップ 1 バイナリファイルが正常に実行されたら、必要なパッチをインストールします。

重要 ステップ 1 は、2.3.2.0 または 2.3.2.1 からアップグレードする場合にのみ有効です。2.3.2.3 からアップグレードする場合は、この手順のステップ 2 から始めてください。

a) 次の URL から **CSCwb00526.sh.zip** のローカルコピーをダウンロードします。https://software.cisco.com/download/specialrelease/46a2ecbbe1219e5184d0094771637b2a

b) zip ファイルを解凍します。

c) **ssh maglev@***cluster's-IP-address***:/data/tmp** コマンドを実行して、ファイル **CSCwb00526.sh** を Cisco DNA Center クラスタにコピーします。

d) 次のコマンドを実行します。

sudo chmod 777 CSCwb00526.sh

sudo bash CSCwb00526.sh

e) **magctl appstack status | grep catalogs** コマンドを実行して、カタログサービスが実行されていることを確認します。

f) 出力を参照します。次の例のようになります。

```
$ magctl appstack status | grep catalogs
maglev-system catalogserver 1/1 Running
```

ステップ 2 Cisco DNA Center GUI にログインします。

ステップ 3 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Software Management]** の順に選択します。

ステップ 4 [Software Management] ウィンドウに、Catalyst Center <*version*> が使用可能であることが表示されることを確認します。

ステップ 5 [Install now] をクリックします。

ステップ 6 Cisco DNA Center の事前チェック完了後、[Install] をクリックします。

ステップ 7 アップグレードの完了後、[Currently Installed Applications] リンクをクリックし、各アプリケーションが更新されたことを確認します。

PSIRT スキャンのナレッジパックの更新

ナレッジパックのオフライン更新

オフラインナレッジパックの更新には、次の手順が含まれます。

1. ナレッジパックファイルをダウンロードします。
2. USB またはその他の転送可能なメディアにファイルをエクスポートします。
3. エアギャップデバイスの Catalyst Center にファイルをインポートします。

ファイルのダウンロード

ステップ 1 推奨される検索エンジン（Chrome または Firefox）のいずれかを使用していることを確認します。

ステップ 2 次のリンクを選択してダウンロードを開始します。

https://tools.cisco.com/cscrdr/security/center/files/mre/mre_workflow_signed.tar.gz

USB またはその他の転送可能なメディアへのエクスポート

ステップ 1 ファイルが .tar.gz 形式であることを確認します。

ステップ 2 ダウンロードしたファイルを USB（またはその他のメディア）に転送します。

ダウンロードしたファイルの確認

ポータルで提供されるシスコの署名検証と SHA512 チェックサムを使用して、ダウンロードしたイメージの完全性を確認します。

ステップ 1 （オプション）SHA 検証を実行して、不完全なダウンロードによってバイナリイメージが破損していないかを確認します。

OS に応じて、次のコマンドのいずれかを入力します。

- Linux：

```
sha512sum Catalyst-Center-image-filename
```

- Mac：

```
shasum -a 512 Catalyst-Center-image-filename
```

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256 | md5
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windowsでは、Windows PowerShell を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

実行したコマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、バイナリイメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 2 署名を確認し、バイナリイメージが正規のものでシスコ製であることを確認します。

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
signature-filename Catalyst-Center-image-filename
```

このコマンドは Mac と Linux の両方の環境で動作します。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります。

バイナリイメージが正規であれば、このコマンドを入力すると、「Verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、バイナリイメージをインストールせず、シスコサポートにお問い合わせください。

完全性検証用の最新の KGV ファイルのダウンロード

完全性の検証に使用する KGV ファイルをダウンロードするには、次の手順を実行します。

ステップ 1 インターネットにアクセスできるデバイスを使用して、次の URL から **Cisco_KnownGoodValues.tar** KGV ファイルをダウンロードします。https://tools.cisco.com/cscrdr/security/center/files/trust/Cisco_KnownGoodValues.tar。

ステップ 2 このファイルを、エアギャップ環境のストレージメディアまたはデバイスに転送します。

ステップ 3 エアギャップ Catalyst Center クラスタにブラウザでアクセスできるデバイスを使用して、ファイルをインポートします。

a) Catalyst Center クラスタで、次の URL をブラウザで開きます。/dna/systemSettings/settings?settings-item=IntegrityVerficationSettings。
b) [Import New from Local] を選択します。
c) ステップ 1 でダウンロードした KGV ファイルをインポートします。

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。