PowerOn Auto Provisioning の使用方法

この章は、次の項で構成されています。

PowerOn Auto Provisioning について

PowerOn Auto Provisioning（POAP）は、ネットワークに初めて導入された Cisco Nexus スイッチに対して、ソフトウェアイメージのアップグレードと構成ファイルのインストールのプロセスを自動化します。

POAP 機能を備えたデバイスが起動し、スタートアップ設定が見つからない場合、デバイスは POAP モードに入り、DHCP サーバーを検索、インターフェイス IP アドレス、ゲートウェイ、および DNS サーバーの IP アドレスを使用して自身をブートストラップします。また、TFTP サーバーの IP アドレスを取得し、ダウンロードするためのスイッチを有効化し、適切なソフトウェアイメージと構成ファイルをダウンロードしてインストールする構成スクリプトをダウンロードします。

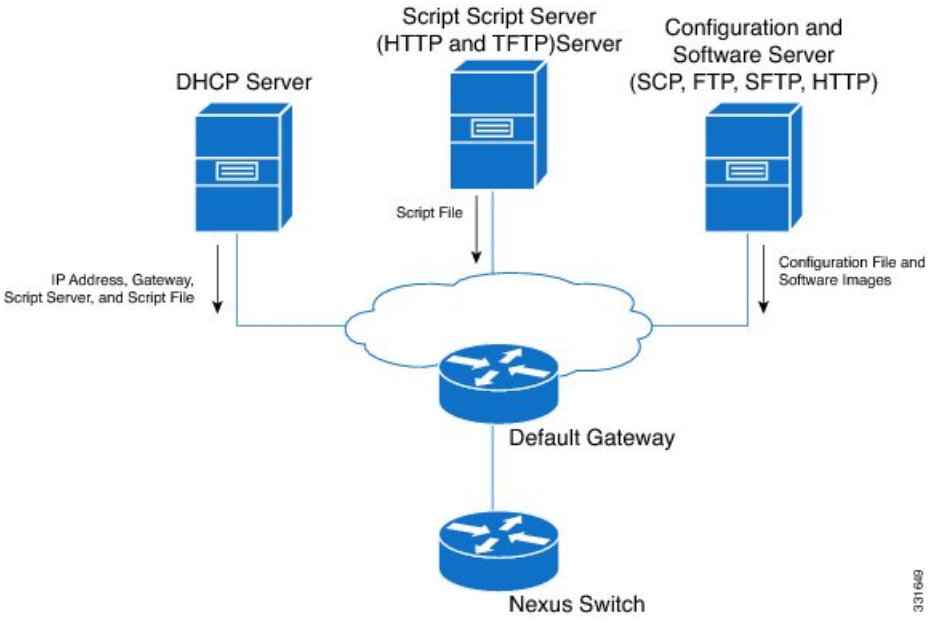
（注） DHCP 情報は、POAP 処理中にだけ使用されます。

POAP のためのネットワーク要件

POAP には、次のネットワーク インフラが必要です。

- インターフェイス IP アドレス、ゲートウェイ アドレス、およびドメイン ネーム システム（DNS）サーバーをブートストラップする DHCP サーバー。
- ソフトウェア イメージのインストールと構成のプロセスを自動化する構成スクリプトが保管されている TFTP または HTTP サーバー。
- 必要なソフトウェア イメージと構成ファイルが保管されている 1 台以上のサーバー。
- USB を使用する場合、POAP に DHCP サーバーまたは TFTP サーバーは必要ありません。

図 *1: POAP* ネットワーク インフラ



POAP スクリプトの安全なダウンロード

Cisco NX-OS リリース 10.2(3)F 以降、POAP スクリプトを安全にダウンロードするオプションがあります。POAP 機能を備えたデバイスが起動し、スタートアップ設定が見つからない場合、デバイスは POAP モードに入り、DHCP サーバーを検索、インターフェイス IP アドレス、ゲートウェイ、および DNS サーバーの IP アドレスを使用して自身をブートストラップします。また、デバイスは HTTPS サーバーの IP アドレスを取得し、POAP スクリプトを安全にダウンロードします。このスクリプトにより、スイッチは適切なソフトウェア イメージと構成ファイルをダウンロードしてインストールできます。

POAP スクリプトを安全にダウンロードするには、特定の POAP オプションを選択する必要があります。Cisco NX-OS リリース 10.2(3)F までは、POAP は IPv4 の場合はオプション 66 と 67、IPv6 の場合はオプション 77 と 15 を使用して、ブート スクリプト情報を抽出していました。ただし、スクリプトの転送は http を使用するため、あまり安全ではありません。Cisco NX-OS リリース 10.2(3)F 以降、オプション 43 は IPv4 のセキュア POAP 関連のプロビジョニング スクリプト情報を指定し、オプション 17 は IPv6 の同じことを指定します。さらに、これらのオプションにより、POAP は安全な方法でファイル サーバーに到達できます。POAP オプション

66、67、77、および 15 は、Cisco NX-OS Release10.2(3)F で引き続きサポートされます。さらに、オプション43または17を使用している場合は、必要に応じて、以前のオプションをフォールバック オプションとして使用できます。Cisco NX-OS リリース 10.4(1)F 以降では、セキュア POAP 用の単一の .pem 証明書の代わりにルート CA バンドルを使用できます。

（注） オプション 43 とオプション 17 の両方の最大文字長は 512 バイトです。

オプション 43 およびオプション 17 で使用できるサブオプションについては、次のセクションで説明します。

- オプション 43 - IPv4 IPv4 （3 ページ）
- オプション 17 - IPv6 IPv6 （4 ページ）

IPv4

オプション 43 には、IPv4 の次のサブオプションがあります。

- option space poap length width 2;
- option poap.version code 1 = unsigned integer 8;

（注） このサブオプションは必須です。

- option poap.ca_list code 50 = text;
- option poap.url code 2 = text;

（注） このサブオプションは必須です。

- option poap.version code 1 = unsigned integer 8;
- option poap.ntp code 3 = ip-address;

（注） このサブオプションは、IPv4（オプション43）でのみサポートされます。

- option poap.version code 1 = unsigned integer 8;

（注） フラグは、クライアントでのサーバー証明書の検証をスキップするために使用されます。

IPv4 の構成例は次のとおりです。

```
host dhclient-n9kv {
hardware ethernet 00:50:56:85:c5:30;
fixed-address 3.3.3.1;
default-lease-time 3600;
option broadcast-address 192.168.1.255;
#option log-servers 1.1.1.1;
max-lease-time 3600;
option subnet-mask 255.255.255.0;
option routers 10.77.143.1;
#option domain-name-servers 1.1.1.1;
          vendor-option-space poap;
option poap.version 1;
option poap.ca_list "https://<ip>/poap/ca_file1.pem, https://<ip>/poap/ca_file2.pem";
option poap.url "https://<url>/poap.py";
option poap.debug 1;
option poap.ntp 10.1.1.39;
option poap.flag 0;
  }
```

IPv6

オプション 17 には、IPv6 の次のサブオプションがあります。

- option space poap_v6 length width 2;
- option poap_v6.version code 1 = unsigned integer 8;

（注） このサブオプションは必須です。

- option poap_v6.ca_list code 50 = text;
- option poap.url code 2 = text;

（注） このサブオプションは必須です。

- option poap_v6.debug code 51 = unsigned integer 8;
- option vsio.poap_v6 code 9 = encapsulate poap_v6;

IPv6 の設定例は次のとおりです。

```
 option dhcp6.next-hop-rt-prefix code 242 = { ip6-address, unsigned integer 16,
unsigned integer 16, unsigned integer 32, unsigned integer 8, unsigned integer 8,
ip6-address };
 option dhcp6.bootfile-url code 59 = string;

 default-lease-time 3600;
 max-lease-time 3600;
 log-facility local7;
 subnet6 2003::/64 {
```

```
  # This statement configures actual values to be sent
# RTPREFIX option code = 243, RTPREFIX length = 22
# Ignore value 22. It is something related to option-size RT_PREFIX option length.
# lifetime = 9000 seconds
# route ETH1_IPV6_GW/64
# metric 1
option dhcp6.next-hop-rt-prefix 2003::2222 243 22 9000 0 1 ::;
#ipv6 ::/0 2003::2222
#Another example - support not there in NXOS - CSCvs05271:
#option dhcp6.next-hop-rt-prefix 2003::2222 243 22 9000 112 1 2003::1:2:3:4:5:0;
#ipv6 2003::1:2:3:4:5:0/112 2003::2222

  # Additional options
#option dhcp6.name-servers fec0:0:0:1::1;
#option dhcp6.domain-search "domain.example";


range6 2003::b:1111 2003::b:9999;
option dhcp6.bootfile-url "tftp://2003::1111/poap_github_v6.py";
vendor-option-space poap_v6;
option poap_v6.version 1;
option poap_v6.ca_list "https://<ip>/new_ca.pem,https://<ip>/another_ca.pem";
option poap_v6.url "https://<ip>/poap_github_v4.py";
option poap_v6.debug 1;
  }
```

安全な POAP のネットワーク要件

POAP には、次のネットワーク インフラが必要です。

- インターフェイス IP アドレス、ゲートウェイ アドレス、およびドメイン ネーム システム（DNS）サーバーをブートストラップする DHCP サーバー。
- ソフトウェア イメージのインストールと構成のプロセスに使用される POAP スクリプトを含む HTTP サーバー。

（注）
- POAP スクリプトの安全なダウンロードの場合、TFTP サーバーは HTTPS サーバーに置き換えられます。したがって、この章の TFTP サーバーに関連する内容を読むときは、TFTP サーバーを HTTPS サーバーとして読むことを忘れないでください。

- 必要なソフトウェア イメージと構成ファイルが保管されている 1 台以上のサーバー。

導入シナリオ

Cisco デバイスには、Secure Unique Device Identifier (SUDI) と呼ばれる一意の識別子があります。ハードウェア SUDI は、暗号化、暗号解読、署名、操作対象のデータの通過を許可する検証などの非対称キー操作に使用できます。シスコ以外のすべてのデバイスは、非 SUDI デバイスとして分類されます。非SUDIデバイスの場合、ファイル サーバーを認証するためにルート

CA バンドルが必要です。ただし、ファイル サーバーは、SUDI または非 SUDI デバイスのいずれかでホストできます。

これらすべての機能に基づいて、次の展開シナリオのいずれかを使用して、POAP スクリプトを安全な方法でダウンロードできます。

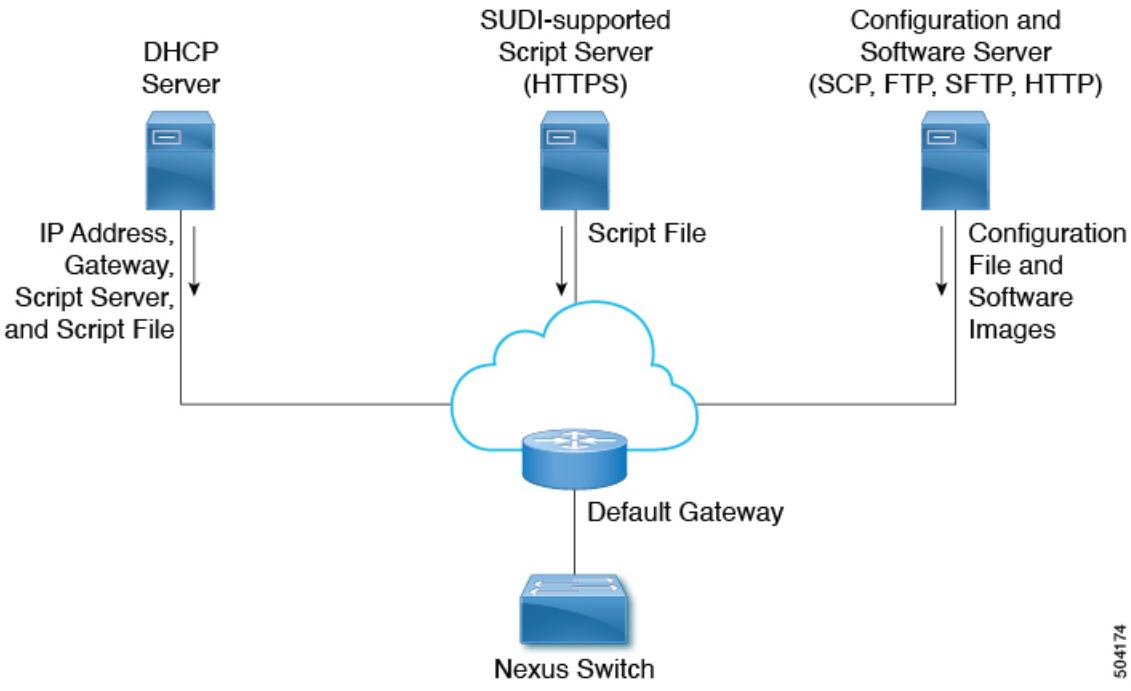
- ファイル サーバーとしての SUDI 対応デバイス
- ファイル サーバーとしての非 SUDI 対応デバイス

ファイル サーバーとしての SUDI 対応デバイス

SUDI がサポートするデバイスは Cisco デバイスです。以前の実装とは異なり、DHCP サーバーは http/tftp ではなく https の場所を提供するようになりました。このシナリオでは、必要なソフトウェア イメージと構成ファイルを含む 1 つ以上のサーバーを除き、DHCP サーバーと SUDI がサポートするスクリプト サーバー（HTTPS サーバー）のみが必要です。

（注） SUDI は TLSv1.2 以下のみをサポートします。また、SUDI ソリューションは https を使用した安全なダウンロードのみを考慮し、sftp は考慮しません。

図 *2:* ファイル サーバー インフラストラクチャとしての *SUDI* 対応デバイス



SUDI 対応デバイスのワークフローは次のとおりです。

- 起動デバイスは SUDI 対応であり、SUDI 証明書を検証するために必要なトラスト ストアがあります。

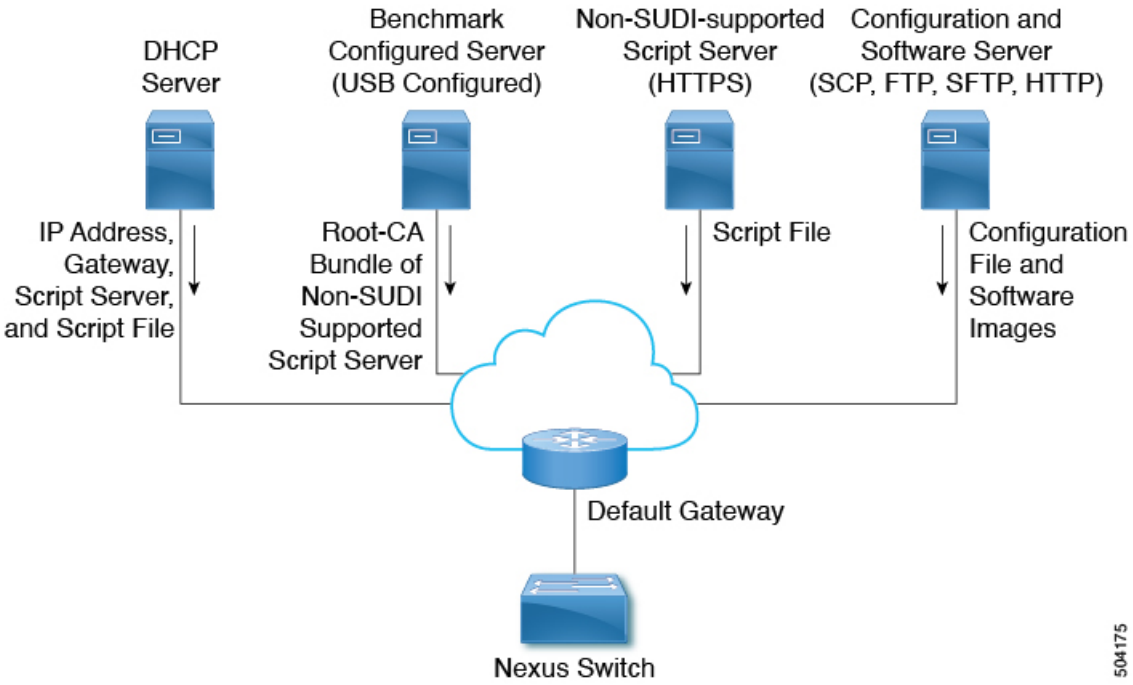
- 起動デバイスは DHCP 検出を送信します
- DHCP サーバーは、https サーバーの詳細で起動デバイスに応答します
- デバイスは、標準の SSL API を使用して安全なチャネルを確立します
- 認証は両側でSUDIを検証することで行われます
- **poap.py** のダウンロード

ファイル サーバーとしての SUDI 対応デバイス

このシナリオでは、ルート CA バンドルをブート デバイスにインストールする必要があります。認証にはルートCAバンドルが必要です。ここでは、必要なソフトウェア イメージと構成ファイルを含む 1 つ以上のサーバー以外に、DHCP サーバー、中間デバイス、および非 SUDI サポート スクリプト サーバー（HTTPS サーバー）が必要です。

DHCP オファーには、ルート CA バンドルが利用可能な中間サーバーの詳細が含まれています。中間デバイスはSUDIをサポートする必要があります。ブートデバイスは中間デバイスを使用してルートCAバンドルをダウンロードしてインストールし、ファイルサーバーと通信します。中間デバイスを最初にプロビジョニングする必要があります。

図 *3:* ファイル サーバー インフラストラクチャとしての非 *SUDI* 対応デバイス



非対応 SUDI デバイスのワークフローは次のとおりです。

- 起動デバイスは SUDI 対応であり、SUDI 証明書を検証するために必要なトラスト ストアがあります。
- ルート CA バンドルを使用してサーバーをホストする中間デバイスも SUDI 対応です

- 起動デバイスは DHCP 検出を送信します
- DHCP サーバーは、https サーバーの詳細とルート CA サーバーの詳細で起動デバイスに応答します
- ブートデバイスが中間デバイスに到達し、CA バンドルを取得して、それをトラストストアに追加します
- 起動デバイスがファイル サーバーに到達し、**poap.py** をダウンロードします。

ベンチマーク構成されたデバイス

非 SUDI サポート スクリプト サーバのルート CA 証明書チェーン ファイルは、ベンチマーク構成済みサーバの `/bootflash/poap/sudi_fs` に配置する必要があります。

（注） ベンチ構成済みデバイスのポートを変更するには、**file-server** <*port-number*> コマンドを使用します。ポート 80（http）やポート 443（https）などの標準ポートの使用は避けてください。

file-server <*port-number*> コマンドは、管理インターフェイスを介してコンテンツを提供するだけです。

古いイメージで出荷されたデバイスの安全な POAP

セキュア POAP のサポートは、安全な POAP 機能を備えたイメージとともに出荷されるデバイスでのみ利用できます。

デバイスに安全な POAP 機能がない場合は、レガシー DHCP オプションを使用して、デバイスをセキュア POAP をサポートする新しいバージョンのイメージに移動します。次に、これらのデバイスをリロードして、安全な POAP 機能を使用できます。

安全な POAP のトラブルシューティング

安全な POAP に関するデバッグ情報を収集するには、次の手順を実行します。

1. オプション 43 の IPv4 のデバッグ オプションを 1 に設定し、オプション 17 の IPv6 のデバッグ オプションを設定します。

   デバッグ オプションは、追加のログを有効にします。

2. スイッチが POAP の 1 サイクルを実行できるようにします。
3. POAP を中止します。
4. システムが起動したら、**show tech-support poap** コマンドを実行します。

   このコマンドは、POAP のステータスまたは構成を表示します。

POAP の無効化

POAP は、システムに構成がない場合に有効になります。ブートアップの一部として実行されます。ただし、初期設定時に POAP の有効化をバイパスできます。POAP を永続的に無効にする場合 (システムに構成がない場合でも)、「system no poap」コマンドを使用できます。このコマンドは、(構成がない場合でも) 次の起動時に POAP が開始されないようにします。POAP を有効にするには、「system poap」コマンドまたは「write erase poap」コマンドを使用します。「write erase poap」コマンドは、POAP フラグを消去し、POAP を有効にします。

- 例：POAP の無効化

```
switch# system no poap
switch# sh boot
Current Boot Variables:
 sup-1
NXOS variable = bootflash:/nxos.9.2.1.125.bin
Boot POAP Disabled

POAP permanently disabled using 'system no poap'


Boot Variables on next reload:

sup-1
NXOS variable = bootflash:/nxos.9.2.1.125.bin
Boot POAP Disabled

POAP permanently disabled using 'system no poap'


switch# sh system poap
System-wide POAP is disabled  using exec command 'system no poap'
POAP will be bypassed on write-erase reload.
(Perpetual POAP cannot be enabled when system-wide POAP is disabled)
```

- 例：POAP の有効化

```
switch# system poap

switch# sh system poap

System-wide POAP is enabled
```

- 例：POAP の消去

```
switch# write erase poap
This command will erase the system wide POAP disable flag only if it is set.
Do you wish to proceed anyway? (y/n)  [n] y
System wide POAP disable flag erased.

switch# sh system poap
System-wide POAP is enabled
```

POAP コンフィギュレーション スクリプト

シスコから提供される参照スクリプトでは、次の機能がサポートされています。

- スイッチ固有の識別子（シリアル番号など）を取得します。
- スイッチ上に nx-os ソフトウェア イメージがまだ存在しない場合は、それををダウンロードします。nx-os イメージがスイッチ上にインストールされ、次回のリブート時に使用されます。
- ダウンロードされた設定がスイッチの次回のリブート時に適用されるようにスケジュールします。
- スタートアップ構成として構成を保存します。

Python プログラミング言語と Tool Command Language（Tcl）を使用して開発された構成スクリプトのサンプルが用意されています。これらのスクリプトのいずれかを、自分のネットワーク環境に合わせてカスタマイズできます。次のリンクでPython スクリプトにアクセスして、Cisco Nexus 9000 シリーズ スイッチ上の POAP を実行できます。https://github.com/datacenter/nexus9000/tree/master/nx-os/poap。

Python プログラミング言語は CLI Commands を実行できる 2 つの API を使用します。これらの API については、次の表で説明します。これらの API の引数は CLI コマンドの文字列です。

API	説明
cli()	制御文字/特殊文字を含む CLI コマンドの未処理の出力を返します。
clid()	XML をサポートする CLI コマンドの場合、この API はコマンド出力を Python ディクショナリとして返します。 この API は、**show** コマンドの出力の検索に役立ちます。

POAP コンフィギュレーション スクリプト

Python プログラミング言語を使用して開発された構成スクリプトのサンプルが用意されています。提供されているスクリプトを使用し、ネットワーク環境の要件を満たすように変更することをお勧めします。

POAP スクリプトは https://github.com/datacenter/nexus9000/blob/master/nx-os/poap/poap.py にあります。

Python を使用してスクリプトを変更するには、ご使用のプラットフォームの『*Cisco NX-OS Python API* リファレンス ガイド』を参照してください。

POAP スクリプトおよび POAP スクリプト オプションの使用

POAP スクリプトを使用する前に、次の操作を実行します。

1. スクリプトの上部にあるオプションディクショナリを編集して、セットアップに関連するすべてのオプションがスクリプトに含まれるようにします。デフォルトを（デフォルトのオプション機能で）直接変更しないでください。
2. シェル コマンドを使用して、表示されているように POAP スクリプトの MD5 チェックサムを更新します。

```
f=poap_nexus_script.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i
"s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f
```

3. デバイスにスタートアップ構成がある場合は、書き込み消去を実行してデバイスをリロードします。

次の POAP スクリプト オプションを指定して、POAP スクリプトの動作を変更できます。サーバーからファイルをダウンロードするときは、ホスト名、ユーザー名、およびパスワードのオプションが必要です。パーソナリティを除くすべてのモードでは、target_system_image も必要です。必須パラメータはスクリプトによって強制され、必須パラメータが存在しない場合、スクリプトは中止されます。ホスト名、ユーザー名、およびパスワードを除くすべてのオプションには、デフォルトのオプションがあります。オプションディクショナリでオプションを指定しない場合、デフォルトが使用されます。

- **username**

  サーバーからファイルをダウンロードするときに使用するユーザー名。

- **password**

  サーバーからファイルをダウンロードするときに使用するパスワード。

- **hostname**

  ファイルのダウンロード元のサーバーの名前またはアドレス。

- モード（**Certificate verification mode**）

  デフォルトは **serial_number** です。

  次のいずれかのオプションを使用します。

  - パーソナリティ

    tarball からスイッチを復元する方法。

  - **SERIAL_NUMBER**

    構成ファイル名を決定するスイッチのシリアル番号。構成ファイルのシリアル番号の形式は conf.*serialnumber* です。例: conf.FOC123456

  - **hostname**

構成ファイル名を決定するためにDHCPオプションで受け取ったホスト名。構成ファイルのホスト名の形式は、conf_*hostname.cfg* です。例：conf_3164-RS.cfg

- **mac**

  構成ファイル名を決定するインターフェイスの MAC アドレス。構成ファイルのホスト名の形式は、conf_*macaddress*.cfg です。例：conf_7426CC5C9180.cfg

- **raw**

  構成ファイル名は、オプションで指定されたとおりに使用されます。ファイル名は変更されません。

- **location**

  CDP ネイバーは、構成ファイル名を決定するために使用されます。構成ファイル内の場所の形式は conf_*host_intf*.cfg です。ここで、*host* は POAP インターフェースを介してデバイスに接続されているホストであり、*intf* は POAP インターフェースが接続されているリモート インターフェースです。例：conf_remote-switch_Eth1_8.cfg

- **必要なスペース**

  POAP の特定の反復に必要な KB 単位のスペース。デフォルト値は 100,000 です。複数ステップのアップグレードの場合、ターゲット イメージのアップグレード パスにある最後のイメージのサイズを指定します。

- **transfer_protocol**

  VSH でサポートされている http、https、ftp、scp、sftp、tftp などの転送プロトコル。デフォルトは scp です。

- **config_path**

  サーバー上の構成ファイルのパス。例：/tftpboot。デフォルトは /var/lib/tftpboot です。

- **target_system_image**

  リモート サーバーからダウンロードするイメージの名前。これは、POAPが完了した後に取得するイメージです。このオプションは、パーソナリティを除くすべてのモードで必須のパラメータです。デフォルトは「」です。

- **target_image_path**

  サーバー上のイメージへのパス。例：/tftpboot。デフォルトは /var/lib/tftpboot です。

- **destination-path**

  イメージと MD5 サムをダウンロードするパス。デフォルトは /bootflash です。

- **destination_system_image**

  指定宛先イメージ ファイル名。指定しない場合、デフォルトはtarget_system_image名になります。

- **user_app_path**

ユーザー スクリプト、エージェント、およびユーザー データが配置されているサーバー上のパス。デフォルトは /var/lib/tftpboot です。

- **disable_md5**

  これは、MD5 チェックを無効にする必要がある場合は True です。デフォルトは [いいえ（False）] です。

- **midway_system_image**

  途中のシステムアップグレードに使用するイメージの名前。デフォルトでは、POAP スクリプトはアップグレードパスで必要な中間イメージの名前を見つけて使用します。2 段階アップグレードで別の中間イメージを選択する場合は、このオプションを設定します。デフォルトは「」です。

- **source_config_file**

  raw モードを使用する場合の構成ファイルの名前。デフォルトは poap.cfg です。

- **vrf**

  ダウンロードなどに使用する VRF。VRF は POAP プロセスによって自動的に設定されます。デフォルトは POAP_VRF 環境変数です。

- **destination_config**

  ダウンロードした構成に使用する名前。デフォルトは poap_replay.cfg です。

- **split_config_first**

  構成を分割する必要がある場合に、最初の構成部分に使用する名前。構成を有効にするためにリロードするときにのみ適用されます。デフォルトは poap_1.cfg です。

- **split_config_second**

  構成が分割されている場合に 2 番目の構成部分に使用する名前。デフォルトは poap_2.cfg です。

- **timeout_config**

  構成ファイルのコピーのタイムアウト（秒単位）。デフォルトは 120 です。レガシー イメージ以外の場合、このオプションは使用されず、POAP プロセスがタイムアウトします。レガシー イメージの場合、FTP はこのタイムアウトをコピー プロセスではなくログイン プロセスに使用しますが、scp および他のプロトコルはこのタイムアウトをコピー プロセスに使用します。

- **timeout_copy_system**

  システム イメージのコピーのタイムアウト (秒単位)。デフォルトは 2100 です。レガシー イメージ以外の場合、このオプションは使用されず、POAP プロセスがタイムアウトします。レガシー イメージの場合、FTP はこのタイムアウトをコピー プロセスではなくログイン プロセスに使用しますが、scp および他のプロトコルはこのタイムアウトをコピー プロセスに使用します。

- **timeout_copy_personality**

パーソナリティ tarball のコピーのタイムアウト (秒単位)。デフォルトは 900 です。レガシーイメージ以外の場合、このオプションは使用されず、POAPプロセスがタイムアウトします。レガシー イメージの場合、FTP はこのタイムアウトをコピー プロセスではなくログイン プロセスに使用しますが、scp および他のプロトコルはこのタイムアウトをコピー プロセスに使用します。

- **timeout_copy_user**

  ユーザー スクリプトとエージェントをコピーする際のタイムアウト (秒単位)。デフォルトは 900 です。レガシー イメージ以外の場合、このオプションは使用されず、POAP プロセスがタイムアウトします。レガシー イメージの場合、FTP はこのタイムアウトをコピー プロセスではなくログイン プロセスに使用しますが、scp および他のプロトコルはこのタイムアウトをコピー プロセスに使用します。

- **personality_path**

  パーソナリティ tarball のダウンロード元のリモート パス。tarball がダウンロードされ、パーソナリティ プロセスが開始されると、パーソナリティは、tarball 設定内で指定された場所から将来的にすべてのファイルをダウンロードします。デフォルトは /var/lib/tftpboot です。

- **source_tarball**

  ダウンロードするパーソナリティ tarball の名前。デフォルトは、personality.tar です。

- **destination_tarball**

  ダウンロード後のパーソナリティ tarball の名前。デフォルトは、personality.tar です。

POAP の DNS なしでの DHCP サーバーのセットアップ

Cisco NX-OS リリース 7.0(3)I6(1) 以降、tftp-server-name は DNS オプションなしで使用できます。以前のリリースで DNS なしで POAP 機能を有効にするには、150 のカスタム オプションを使用して tftp-server-address を指定する必要があります。

tftp-server-address オプションを使用するには、dhcpd.conf ファイルの先頭で次を指定します。

```
option tftp-server-address code 150 = ip-address;
```

例：

```
host MyDevice {
    option dhcp-client-identifier "\000SAL12345678";
    fixed-address 2.1.1.10;
    option routers 2.1.1.1;
    option host-name "MyDevice";
    option bootfile-name "poap_nexus_script.py";
    option tftp-server-address 2.1.1.1;
}
```

次の例は、IPv6 を介した POAP の DHCPv6 の設定を示しています。

```
default-lease-time 3600;
max-lease-time 3600;
log-facility local7;
```

```
subnet6 2003::/64 {

        # This statement configures actual values to be sent
        # RTPREFIX option code = 243, RTPREFIX length = 22
      # Ignore value 22. It is something related to option-size RT_PREFIX option length.

        # lifetime = 9000 seconds
        # route ETH1_IPV6_GW/64
        # metric 1
        option dhcp6.next-hop-rt-prefix 2003::2222 243 22 9000 0 1 ::;
        #ipv6 ::/0 2003::2222
        #Another example - support not there in NXOS - CSCvs05271:
       #option dhcp6.next-hop-rt-prefix 2003::2222 243 22 9000 112 1 2003::1:2:3:4:5:0;

        #ipv6 2003::1:2:3:4:5:0/112 2003::2222

        # Additional options
        #option dhcp6.name-servers fec0:0:0:1::1;
        #option dhcp6.domain-search "domain.example";

        range6 2003::b:1111 2003::b:9999;
        #range6 2003::c:2222 2003::c:2222;
        option dhcp6.bootfile-url "tftp://2003::1111/poap_github_v6.py";
```

POAP の一部としてのユーザー データ、エージェント、およびスクリプトのダウンロードと使用

オプション ディクショナリの下に、**download_scripts_and_agents** 関数があります。ユーザー スクリプトとデータをダウンロードする場合は、最初の **poap_log** 行のコメントを外し、一連の **download_user_app** 関数呼び出しを使用して各アプリケーションをダウンロードします。古い Cisco NX-OS バージョンはディレクトリの再帰的コピーをサポートしていないため、そのようなディレクトリは tarball (TAR アーカイブ) に入れてから、スイッチで一度解凍する必要があります。**download_scripts_and_agents** 関数のパラメータは次のとおりです。

- **source_path** - ファイルまたは tarball がある場所へのパス。このパラメータは必須です。例：/var/lib/tftpboot
- **source_file** - ダウンロードするファイルの名前。このパラメータは必須です。例：agents.tar、script.py など。
- **dest_path** - スイッチ上のファイルをダウンロードする場所。以前に存在しなかったディレクトリが作成されます。これは省略可能なパラメータです。デフォルトは /bootflash です。
- **dest_file** - ダウンロードしたファイルに付ける名前。これは省略可能なパラメータです。デフォルトは変更されていない source_file です。
- **unpack** - アンパック用の tarball が存在するかどうかを示します。解凍は **tar -xf** *tarfile* **-C /bootflash** で行います。これは省略可能なパラメータです。デフォルトは [いいえ（False）] です。
- **delete_after_unpack** - アンパックが成功した後にダウンロードした tarball を削除するかどうかを示します。unpack が False の場合、効果はありません。デフォルトは [いいえ（False）] です。

ダウンロード機能を使用すると、POAP の実行に必要なすべてのエージェントとファイルをダウンロードできます。エージェントを開始するには、POAP によってダウンロードされた実行構成に構成が存在する必要があります。次に、エージェント、スケジューラ、および cron エントリを EEM とともに使用できます。

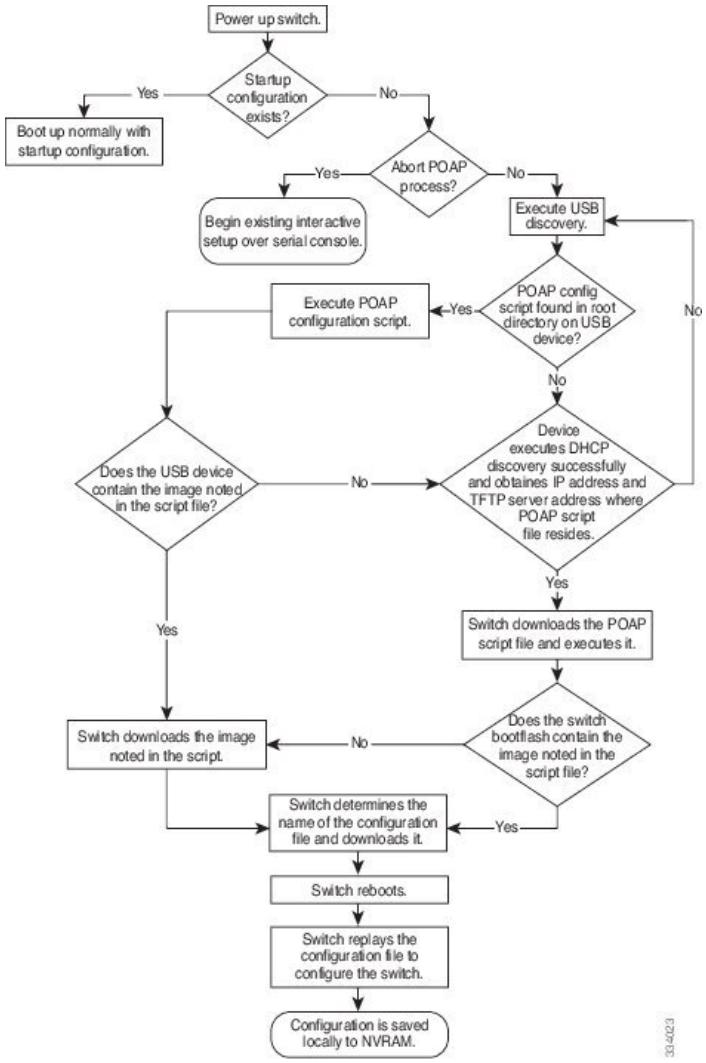
POAP 処理

POAP プロセスには次のフェーズがあります。

1. 電源投入
2. USB の検出
3. DHCP の検出
4. スクリプトの実行
5. インストール後のリロード

これらのフェーズ内では、他の処理や分岐点が発生します。次に、POAP 処理のフロー図を示します。

図 *4 : POAP* 処理



電源投入フェーズ

デバイスの電源を初めて投入すると、デバイスは製造時にインストールされたソフトウェアイメージをロードし、起動に使用する構成ファイルを探します。構成ファイルが見つからなかった場合、POAP モードが開始されます。

起動中、POAP を中止して通常のセットアップに進むかどうかを確認するプロンプトが表示されます。POAP を終了することも、続行することもできます。

（注） POAP を続行する場合、ユーザの操作は必要ありません。POAP を中止するかどうかを確認するプロンプトは、POAP 処理が完了するまで表示され続けます。

POAPモードを終了すると、通常のインタラクティブなセットアップスクリプトが開始されます。POAP モードを続行すると、すべての前面パネルのインターフェイスはデフォルト設定で構成されます。

USB 検出フェーズ

POAP が開始すると、プロセスはアクセス可能なすべての USB デバイスのルート ディレクトリから POAP スクリプト ファイル（Python スクリプト ファイル、poap_script.py）、構成ファイル、およびシステムとキックスタート イメージを検索します。

スクリプト ファイルが USB デバイスで見つかった場合、POAP はスクリプトの実行を開始します。スクリプト ファイルが USB デバイスに存在しない場合は、POAP は DHCP の検出を実行します（障害が発生した場合は、POAP が成功または手動で POAP プロセスを停止するまで、POAP プロセスは USB 検出と DHCP 検出を交互に実行します）。

構成スクリプトで指定されたソフトウェアイメージおよびスイッチ構成ファイルが存在する場合、POAP は、それらのファイルを使用して、ソフトウェアをインストールし、スイッチを構成します。ソフトウェア イメージおよびスイッチ構成ファイルが USB デバイスに存在しない場合、POAP はクリーン アップをして DHCP フェーズを最初から開始します。

DHCP 検出フェーズ

スイッチは、前面パネルのインターフェイスまたは MGMT インターフェイスで、DHCP サーバーからの DHCP オファーを要請する DHCP 検出メッセージを送信します。（次の図を参照してください）。Cisco Nexus スイッチ上の DHCP クライアントは、クライアント ID オプションにスイッチ シリアル番号を使用して、それ自体を DHCP サーバーに識別させます。DHCP サーバーはこの ID を使用して、IP アドレスやスクリプト ファイル名などの情報を DHCP クライアントに返すことができます。

POAP には、最低 3600 秒（1 時間）の DHCP リース期間が必要です。POAP は、DHCP リース期間を確認します。DHCP リース期間が 3600 秒（1 時間）に満たない場合、POAP は DHCP ネゴシエーションを実行しません。

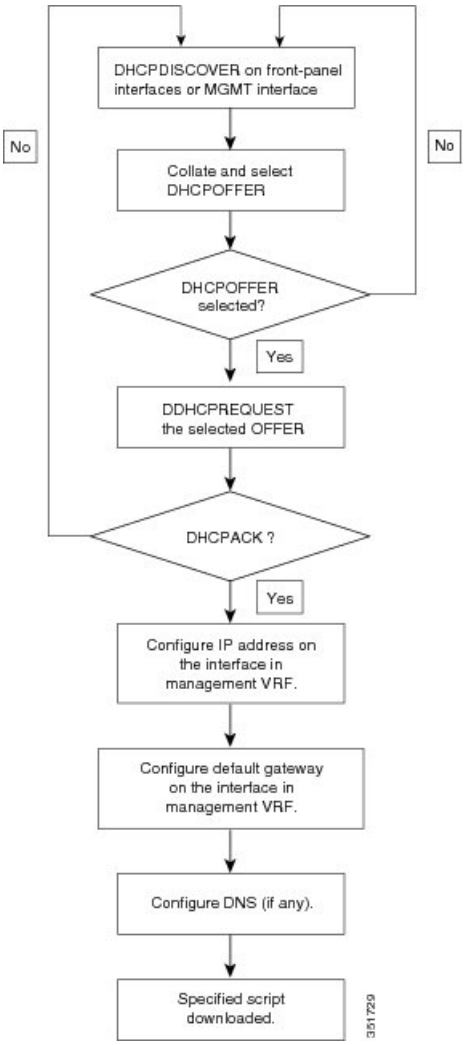
また、DHCP 検出メッセージでは、DHCP サーバーからの次のオプションを要請します。

- TFTP サーバ名または TFTP サーバ アドレス：DHCP サーバは TFTP サーバ名または TFTP サーバ アドレスを DHCP クライアントに中継します。DHCP クライアントはこの情報を使用して TFTP サーバーに接続し、スクリプト ファイルを取得します。
- ブートファイル名：DHCP サーバは DHCP クライアントにブートファイル名を中継します。ブートファイル名には、TFTP サーバ上のブートファイルへの完全パスが含まれます。DHCP クライアントは、この情報を使用してスクリプト ファイルをダウンロードします。

要件を満たす複数の DHCP オファーが受信されると、最初に到着したものが受け入れられ、POAP プロセスは次の段階に進みます。デバイスは、選択された DHCP サーバとの DHCP ネゴシエーション（要求と確認応答）を実行し、DHCP サーバはスイッチに IP アドレスを割り当てます。POAP 処理の後続のステップでエラーが発生すると、IP アドレスは DHCP に戻されます。

要件を満たす DHCP オファーが存在しない場合、スイッチは DHCP ネゴシエーション（要求と確認応答）を実行せず、IP アドレスは割り当てられません。

図 *5 : DHCP* 検出プロセス



POAP ダイナミック ブレークアウト

Cisco NX-OS リリース 7.0(3)I4(1) 以降、POAP は、破損したポートの 1 つの背後にある DHCP サーバーを検出しようとして、ポートを動的に分割します。以前は、ブレークアウトケーブルがサポートされていなかったため、POAP に使用される DHCP サーバーは通常のケーブルに直接接続する必要がありました。

POAP は、どのブレイクアウト マップ (たとえば、10gx4、50gx2、25gx4、または 10gx2) が DHCP サーバーに接続されたリンクを起動するかを決定します。どのポートでもブレイクアウトがサポートされていない場合、POAP はダイナミック ブレイクアウト プロセスをスキップします。ブレークアウトループが完了すると、POAP は通常どおり DHCP 検出フェーズを続行します。

（注） ダイナミックブレイクアウトの詳細については、デバイスのインターフェイス構成ガイドを参照してください。

スクリプトの実行フェーズ

デバイスがDHCP確認応答の情報を使用してデバイス自体をブートストラップした後で、スクリプト ファイルが TFTP サーバーからダウンロードされます。

スイッチは、コンフィギュレーション スクリプトを実行します。これにより、ソフトウェアイメージのダウンロードとインストール、およびスイッチ固有のコンフィギュレーションファイルのダウンロードが行われます。

ただし、この時点では、構成ファイルはスイッチに適用されません。スイッチ上で現在実行中のソフトウェアイメージが構成ファイル内の一部のコマンドをサポートしていない可能性があるためです。新しいソフトウェアイメージがインストールされた場合、スイッチのリブート後にそのソフトウェアイメージの実行が開始されます。その時点でスイッチにコンフィギュレーションが適用されます。

（注） スイッチの接続が切断されると、スクリプトは停止し、スイッチはオリジナルのソフトウェアイメージとブートアップ変数をリロードします。

インストール後のリロード フェーズ

スイッチが再起動し、アップグレードされたソフトウェアイメージ上でコンフィギュレーションが適用（リプレイ）されます。その後、スイッチは、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

POAPv3

PowerOn 自動プロビジョニング バージョン 3（POAPv3）は、Cisco NX-OS リリース 9.3(5) で導入されました。この機能を使用すると、POAPを介してライセンス、RPM、および証明書をインストールできます。

POAPを介してライセンス、RPM、または証明書をインストールするには、次の手順を実行します。

1. ボックスのシリアル番号を名前にして、POAP サーバーにフォルダを作成します。
2. インストールするファイルを含む .yaml または .yml ファイルを作成します。ファイル名が <serial-number>.yaml または .yml 形式 に含まれていることを確認してください。
3. .yaml または .yml ファイルの MD5 チェックサムを作成します。
4. .yaml ファイルの形式が次の形式に似ていることを確認してください。

```
Version : 1

Target-image : nxos.9.3.4.bin

Description : Yaml for box XYZ12345 poap provisioning. N9k Leaf mode box

License : [license1.lic, XYZ12345/license2.lic, folder1/license3.lic]

RPM :

  - rpm1.rpm

  - patches/reload/rpm2-reload.rpm

  - rpm3.rpm

Certificate : [ssh1.pub, XYZ12345/ssh2key.pub]

Trustpoint :

    CA1 :

        cert_1.p12 : password1 (priv_key_passphrase)

        XYZ12345/CA1/cert_2.pfx : password2

    CA2 :

        CA2/XYZ12345/cert_3.p12 : password3
```

5. yaml キーワードは、上記の例に示されている形式と一致する必要があることに注意してください。
6. すべてのファイルを適切なパスに配置します。
7. install_path 変数を名前としてシリアル番号を持つフォルダが配置されるパスとして POAP スクリプトを更新します。

次のリストに、POAPv3 に関連するガイドラインと制限事項を示します。

- YAML は、あらゆるプログラミング言語のための、人が読んで理解できるデータ シリアル化標準規格です。YAML は YAML Ain't Markup Language の略で、このファイル形式テクノロジはドキュメントで使用されます。これらのドキュメントはプレーンテキスト形式で保存され、. yml 拡張子が追加されます。YAML はファイル形式で、.yml はファイル拡張子です。
- YAML は JSON のスーパーセットであり、YAML パーサーは JSON を認識します。YAML ファイル形式は、読みやすく、コメントが役立つため、構成管理に使用されます。
- yaml で言及されている Target_image は、POAP スクリプト内で言及されている target_system_image パスにのみ保持する必要があります。yaml ファイルの Target_image では、相対パスはサポートされていません。
- .yaml と .yml の両方の拡張機能がサポートされています。これらの拡張機能のいずれかを使用することを選択するオプションがあります。オプションを選択しない場合、<serial> .yaml 拡張子が最初に試行され、失敗した場合は、 .yml が考慮されます。

- 構成ファイルと同様に、yaml/yml の MD5 ファイルが必要です。ただし、disable_md5 が「True」の場合、yaml/yml の MD5 ファイルは必要ありません。
- デバイスの yaml ファイルが見つからない場合、「install_path」が POAP スクリプト ファイルに設定されていますが、POAP ワークフローは従来のパスで続行されます。つまり、RPM、ライセンス、および証明書のインストールは行われません。
- インストール リセットは、RPM インストールを使用した PoAP が Day-0 以外のシナリオで実行される場合、書き込み消去よりも優先されます。
- ISSU は、PoAP 経由で新しいイメージに移動するための新しいデフォルトです。「use_nxos_boot」を使用する必要があることに注意してください。レガシー ブート nxos <> が必要な場合は True です。
- Filetype は、トラストポイントの .pfx、.p12、ライセンスの .lic、. rpms の and.rpm で、チェック/ファイル形式が尊重されない場合、現在の POAP を中止します。
- .rpm の場合、yaml ファイルに元のファイル名を指定する必要があります。

  例：customCliGoApp-1.0-1.7.5.x86_64.rpm から custom.rpm に名前を変更した場合、PoAP は名前の不一致を示して解決します。

  rpm の元の名前を取得するには：

```
bash-4.3$ rpm -qp --qf '%{NAME}-%{VERSION}-%{RELEASE}.%{ARCH}.rpm' custom.rpm
customCliGoApp-1.0-1.7.5.x86_64.rpm
bash-4.3$
```

- POAP 経由の ISSU が開始されると、PoAP の中止がブロックされます。何らかの理由で ISSU が失敗すると、中止機能が再び有効になります。

POAP の注意事項および制約事項

POAP 構成時の注意事項および制約事項は次のとおりです。

- bootflash:poap_retry_debugs.log は、内部目的でのみ POAP-PNP によって入力されるファイルです。このファイルは、POAP 障害が発生した場合には関係ありません。
- Syslog の制限により、securePOAP pem ファイル名の文字長は 230 文字に制限されていますが、セキュア POAP は pem ファイル名に 256 文字の長さをサポートしています。
- この機能が動作するには、スイッチ ソフトウェア イメージで POAP をサポートしている必要があります。
- POAP では、スイッチが設定されて動作可能になった後のスイッチのプロビジョニングをサポートしません。スタートアップ コンフィギュレーションのないスイッチの自動プロビジョニングだけがサポートされます。
- POAP の https プロトコルで **ignore-certificate** キーワードを使用するには、**https_ignore_certificate** オプションをオンにする必要があります。これにより、POAP スク

リプトで HTTPS 転送を正常に実行でき、プロトコルは POAP で機能しないため、このオプション https なしで実行できます。

- Day 0 プロビジョニングに HTTP/HTTPS サーバーを使用する場合は、HTTP ヘッダー内の MAC 情報およびその他の関連詳細に基づいてプロビジョニング手順が提供されます。POAP は、HTTP GET ヘッダーからのこれらの詳細を使用して、正しいプロビジョニングスクリプトが識別されて使用されるようにします。これは、他のベンダー (および他の Cisco OS) で利用可能でした。これらの追加情報は、Cisco Nexus 9000 の Cisco NX-OS リリース 10.2(1) からの HTTP get ヘッダーで利用できます。この機能は、POAP および非 POAP HTTP 取得操作でデフォルトで使用できます。
- copy http/https GET コマンドを使用すると、次のフィールドが HTTP ヘッダーの一部として共有されます。

```
Host: IP address
User-Agent: cisco-nxos
X-Vendor-SystemMAC: System MAC
X-Vendor-ModelName: Switch-Model
X-Vendor-Serial: Serial_Num
X-Vendor-HardwareVersion: Hardwareversion
X-Vendor-SoftwareVersion: sw_version
X-Vendor-Architecture: Architecture
```

- 仮想ポート チャネル（vPC）ペアの一部である Cisco Nexus デバイスをブートストラップするために POAP を使用する場合、Cisco Nexus デバイスは POAP の起動時にそのすべてのリンクをアクティブにします。vPC のリンクの端に二重接続されているデバイスは、Cisco Nexus デバイスに接続されているポート チャネル メンバ リンクにそのトラフィックの一部またはすべての送信を開始する場合があり、トラフィックが失われることがあります。

  この問題を回避するには、リンクが POAP を使用してブートストラップされている Cisco Nexus デバイスへのトラフィックの転送を誤って開始しないように、vPC リンクにリンク集約制御プロトコル（LACP）を設定します。

- POAP を使用して、LACP ポート チャネル経由で Cisco Nexus 9000 シリーズ スイッチのダウンストリームに接続されている Cisco Nexus デバイスをブートストラップした場合、メンバー ポートをポート チャネルの一部としてバンドルできないと、Cisco Nexus 9000 シリーズ スイッチはデフォルトでそのメンバー ポートを一時停止します。この問題を回避するには、インターフェイス コンフィギュレーション モードから **no lacp suspend-individual** コマンドを使用して、そのメンバー ポートを一時停止しないように Cisco Nexus 9000 シリーズ スイッチを構成します。
- 重要な POAP の更新は syslog に記録され、シリアル コンソールから使用可能になります。
- 重大な POAP エラーは、ブートフラッシュに記録されます。ファイル名のフォーマットは *date-time*_poap_*PID*_[init,1,2].log です。ここで、 *date-time* のフォーマットは YYYYMMDD_hhmmss で、*PID* はプロセス ID になります。
- POAP プロンプトで **skip** オプションを使用すると、パスワードと基本的な POAP 設定をバイパスできます。この **skip** オプションを使用すると、管理者ユーザーのパスワードは構成されません。admin ユーザーに有効なパスワードが設定されるまで、コマンドはブロックされます。**copy running-config startup-config**

- **boot poap enable** コマンド（永続的な POAP）がスイッチで有効になっている場合、リロード時に、スタートアップ コンフィギュレーションが存在していても、POAP ブートがトリガーされます。このシナリオで POAP を使用しない場合は、**no boot poap enable** コマンドを使用して boot poap enable 構成を削除します。
- スクリプト ログは、ブートフラッシュ ディレクトリに保存されます。ファイル名のフォーマットは *date-time*_poap_*PID*_script.log です。ここで、 *date-time* のフォーマットは YYYYMMDD_hhmmss で、*PID* はプロセス ID になります。

  スクリプトのログ ファイルの形式を構成できます。スクリプト ファイルのログ形式は、スクリプトで指定されます。スクリプトのログ ファイルのテンプレートにはデフォルトの形式があります。ただし、スクリプト実行ログ ファイルに別の形式を選択できます。
- POAP 機能にライセンスは必要ありません。デフォルトでイネーブルになっています。ただし、POAP 機能が正しく動作するためには、ネットワークの導入前に適切なライセンスがネットワーク内のデバイスにインストールされている必要があります。
- POAP の USB サポートにより、構成スクリプト ファイルを含む USB デバイスを POAP モードでチェックできます。この機能は、Nexus 9300-EX、-FX、-FX2、-FX3、および Nexus 9200-X、-FX2 スイッチでサポートされています。
- デバイスが高いトラフィック レートを受信すると、POAP DHCP トランザクションが失敗することがあります。この問題は、POAP がフロントパネルを使用している場合に発生します。この問題を回避するには、POAP が管理ポートを使用していることを確認してください。
- NX-OS 7.0(3)I7(4) 以降、RFC 3004（DHCP のユーザー クラス オプション）がサポートされています。これにより、POAP は DHCPv4 のユーザー クラス オプション 77 と DHCPv6 のユーザー クラス オプション 15 をサポートできます。DHCPv4 と DHCPv6 の両方のユーザー クラス オプションに表示されるテキストは「Cisco-POAP」です。
  - RFC 3004（DHCP のユーザー クラス オプション）のサポートにより、Nexus 9000 スイッチで IPv6 上の POAP がサポートされます。
    - NX-OS 9.2(2) 以降、IPv6 を介した POAP は、–R ラインカードを備えた Nexus 9504 および Nexus 9508 スイッチでサポートされます。

  IPv6 上の POAP 機能により、IPv4 で障害が発生したときに POAP プロセスが IPv6 を使用できるようになります。この機能は、接続障害が発生したときに IPv4 プロトコルと IPv6 プロトコルの間を循環するように設計されています。
- 安全な POAP の場合は、DHCP スヌーピングが有効になっていることを確認してください。
- POAP をサポートするには、ファイアウォール ルールを設定して、意図しないまたは悪意のある DHCP サーバーをブロックします。
- システムのセキュリティを維持し、POAP をより安全にするには、次のように構成します。
  - DHCP スヌーピングをイネーブルにします。

- ファイアウォールルールを設定して、意図しない、または悪意のある DHCP サーバーをブロックします。

- POAP は、MGMT ポートとインバンド ポートの両方でサポートされます。
- Cisco NX-OS リリース 10.2(3)F 以降、POAP/HTTPS 機能のハードウェア SUDI には、POAP スクリプトを安全にダウンロードするオプションが用意されています。
- POAP のデバッグ情報を収集するには、POAP のポスト アボートである **show tech-support poap** コマンドを使用します。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチの Cisco Nexus X9836DM-A ライン カードで POAP がサポートされています。
  - Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9808 スイッチの Cisco Nexus X98900CD-A ライン カードで POAP がサポートされています。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 プラットフォーム スイッチ、および Cisco Nexus X98900CD-A と X9836DM-A ライン カードで POAP がサポートされています。
- Cisco NX-OS リリース 10.4(3)F 以降では、セキュリティ強化のために、スキップ オプションが無効になっています。POAP プロセスが停止しているかどうかに関係なく、ボックスにアクセスするには有効なパスワードを入力する必要があります。
- Cisco NX-OS リリース 10.5(3)F 以降、Cisco 9364E-SG2 ToR スイッチでは POAP がサポートされています。

POAP を使用するためのネットワーク環境の設定

手順

ステップ 1 シスコが提供する基本設定スクリプトを変更するか、独自のスクリプトを作成します。詳細については、『*Python Scripting and API Configuration Guide*』を参照してください。

ステップ 2 構成スクリプトに変更を加えるたびに、bash シェルを使用して、**# f=poap_nexus_script.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f** を実行することにより、必ずMD5チェックサムを再計算することを確認してください。詳細については、『*Python API Reference Guide*（*Python API* リファレンス ガイド）』を参照してください。

ステップ 3 （オプション）POAP の構成スクリプトおよびその他の必要なソフトウェア イメージおよびスイッチの構成 ファイルを、スイッチからアクセスできる USB デバイスに配置します。

ステップ 4 DHCP サーバを配置し、このサーバにインターフェイス、ゲートウェイ、および TFTP サーバの IP アドレスと、コンフィギュレーション スクリプト ファイルのパスと名前が指定されたブートファイルを設定します。（この情報は、最初の起動時にスイッチに提供されます）。すべてのソフトウェア イメージおよびスイッチ構成ファイルが USB デバイスにある場合は、DHCP サーバーを配置する必要はありません。

ステップ 5 構成スクリプトをホストするための TFTP または HTTP サーバを展開します。サーバーへの HTTP 要求をトリガーするには、TFTP サーバー名の前に HTTP:// を付けます。HTTPS はサポートされていません。

ステップ 6 URL 部分を TFTP スクリプト名に追加して、ファイル名への正しいパスを表示します。

ステップ 7 ソフトウェア イメージおよびコンフィギュレーション ファイルをホストするための 1 つまたは複数のサーバを配置します。

POAP を使用するスイッチの設定

始める前に

POAP を使用するためにネットワーク環境がセットアップされていることを確認します。

手順

ステップ 1 ネットワークにスイッチを設置します。

ステップ 2 スイッチの電源を投入します。

構成ファイルが見つからない場合は、スイッチは POAP モードで起動して、POAP を中止して通常のセットアップで続行するかどうかを尋ねるプロンプトが表示されます。

POAP モードで起動を続行するためのエントリは必要ありません。

ステップ 3 （オプション）POAP モードを終了して、通常のインタラクティブ セットアップ スクリプトを開始する場合は、**y**（yes）を入力します。

スイッチが起動して、POAP 処理が開始されます。

次のタスク

設定を確認します。

md5 ファイルの作成

構成スクリプトに変更を加えるたびに、bash シェルを使用して、# f=poap_fabric.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=\"$(md5sum $f.md5 | sed 's/ .*//')\"/" $f を実行することにより、必ず MD5 チェックサムを再計算します。

このプロシージャは、`poap_fabric.py` の md5sum を新しい値に置き換えます（そのファイルに変更があった場合）。

（注） 手順 1 ～ 4 および 7 ～ 8 は、BASH シェルを使用している場合にのみ必要です。他の Linux サーバーにアクセスできる場合、これらの手順は必要ありません。

始める前に

bash シェルにアクセスします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**feature bash-shell** 例： `switch(config)# feature bash-shell`	BASH シェル機能を有効にします。
ステップ 3	**exit** 例： `switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	**run bash** 例： `switch# run bash`	Linux BASH を開きます。
ステップ 5	**md5sum /bootflash/nxos.***release_number***.bin > /bootflash/nxos.***release_number***.bin.md5** 例： `bash-4.2$ md5sum /bootflash/nxos.7.0.3.I6.1.bin > /bootflash/nxos.7.0.3.I6.1.bin.md5`	`.bin` ファイルの md5sum を作成します。
ステップ 6	**md5sum /bootflash/poap.cfg > /bootflash/poap.cfg.md5** 例： `bash-4.2$ md5sum /bootflash/poap.cfg > /bootflash/poap.cfg.md5`	`.cfg` ファイルの md5sum を作成します。
ステップ 7	**exit** 例： `switch(config)# exit`	BASH シェルを終了します。

	コマンドまたはアクション	目的

ステップ 8	**dir | i .md5**
	例：
	`switch# dir | i .md5`
	`65 Jun 09 12:38:48 2017 nxos.7.0.3.I6.1.bin.md5`
	`54 Jun 09 12:39:36 2017 poap.cfg.md5`
	`67299 Jun 09 12:48:58 2017 poap.py.md5`
		.md5 ファイルを表示します。

ステップ 9	**copy bootflash:poap.cfg.md5 scp://***ip_address***/**
	例：
	`copy bootflash:poap.cfg.md5 scp://10.1.100.3/`
	`Enter vrf (If no input, current vrf 'default' is considered): management`
	`Enter username: root`
	`root@10.1.100.3's password:`
	`poap.cfg.md5 100%`
	`54 0.1KB/s 00:00`
	`Copy complete.`
		ファイルを構成およびソフトウェア サーバーにアップロードします。

デバイス コンフィギュレーションの確認

構成を確認するためには、次のいずれかのコマンドを使用します。

コマンド	目的
show running-config [**[exclude]** *command*] **[sanitized]**	現在の実行コンフィギュレーションまたはそのコンフィギュレーションのサブセットの内容を表示するには、該当するモードで **show running-config** コマンドを使用します。。 • **exclude**：（任意）特定のコンフィギュレーションを表示から除外します。 **exclude** キーワードのあとに *command* 引数を指定し、表示から特定のコンフィギュレーションを除外します。 • コマンド：（任意）1 つのコマンドのみを、または指定のコマンド ノード下で使用可能なコマンドのサブセットを表示します。 • **sanitized**：（任意）安全な配布と分析のためにサニタイズされたコンフィギュレーションを表示します。 Cisco NX-OS リリース 10.3(2)F 以降、**sanitized** キーワードが Cisco Nexus 9000 シリーズ スイッチでサポートされています。

コマンド	目的
show startup-config	スタートアップ コンフィギュレーションを表示します。 **Note** レイヤ 3 ベースの機能構成が running-config で無効になっている場合、**show startup-config** コマンドはそれらを表示しません。ただし、**copy running startup** コマンドが実行されるまで、構成はスタートアップ PSS にそのまま残ります。
show time-stamp running-config last-changed	実行構成が最後に変更されたときのタイムスタンプを表示します。

次に、**show running-config**コマンドで **sanitized** キーワードを指定した場合の出力例を示します。サニタイズされた構成は、構成の一部の詳細を公開せずに、構成を共有するために使用できます。

このオプションは、実行構成出力の機密ワードを<removed>キーワードによりマスクします。

```
switch# show running-config sanitized

!Command: show running-config sanitized
!Running configuration last done at: Wed Oct 12 09:14:54 2022
!Time: Wed Oct 12 13:52:55 2022

version 10.3(2) Bios:version 07.69

username admin password 5 <removed> role network-admin

copp profile strict
snmp-server user admin network-admin auth md5 <removed> priv aes-128 <removed>
localizedV2key
rmon event 1 log trap <removed> description FATAL(1) owner PMON@FATAL
rmon event 2 log trap <removed> description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap <removed> description ERROR(3) owner PMON@ERROR
rmon event 4 log trap <removed> description WARNING(4) owner PMON@WARNING
rmon event 5 log trap <removed> description INFORMATION(5) owner PMON@INFO
--More--
```

POAP のトラブルシューティング

以下は、POAP を使用する際の既知の問題と提案のリストです。

- 問題：POAP スクリプトの実行がすぐに失敗し、「スクリプトの実行に失敗しました」というステートメントを除いて、syslog または出力が表示されません。

  提案：サーバーで **python** *script-name* コマンドを使用し、構文エラーがないことを確認します。options ディクショナリは Python ディクショナリであるため、各エントリはコンマで区切って、キーまたはオプションと値をコロンで区切る必要があります。

- 問題：正しく使用されていないオプションに応じて、さまざまな場所で TypeError 例外が発生します。

提案：一部のオプションでは整数を使用します(たとえば、タイムアウトやその他の数値)。引用符で囲まれた数値については、optionsディクショナリを確認してください。正しい使用法については、オプション リストを参照してください。

- 問題：POAP over USB が存在するファイルを見つけられません。

  提案：一部のデバイスには 2 つの USB スロットがあります。USB スロット 2 を使用している場合は、オプションで指定する必要があります。

- 問題：POAP に関する問題。

  提案：POAP を中止し、システムが起動したら、**show tech-support poap** コマンドを実行します。これにより、POAP のステータスと構成が表示されます。

POAP パーソナリティの管理

POAP パーソナリティ

Cisco NX-OS リリース 7.0(3)I4(1) で導入された POAP パーソナリティ機能により、ユーザー データ、Cisco NX-OS とサードパーティのパッチ、および構成ファイルをバックアップおよび復元できます。以前のリリースでは、POAP は構成のみを復元できました。

POAP のパーソナリティは、スイッチ上で追跡されたファイルによって定義されます。パーソナリティ ファイルの構成およびパッケージ リストは ASCII ファイルです。

バイナリ バージョンはパーソナリティ ファイルに記録されますが、実際のバイナリ ファイルは含まれません。バイナリ ファイルは通常大きいため、指定されたリポジトリからアクセスします。

パーソナリティ ファイルは .tar ファイルで、通常は一時フォルダに抽出されます。次に例を示します。

```
switch# dir bootflash: 042516182843personality # timestamp name
46985 Dec 06 23:12:56 2015 running-config  Same as "show running-configuration" command.
20512 Dec 06 23:12:56 2015 host-package-list  Package/Patches list
58056 Dec 06 23:12:56 2015 data.tar  User Data
25    Dec 06 23:12:56 2015 IMAGEFILE  Tracked image metadata
```

POAP パーソナリティのバックアップ

スイッチ上でローカルに、またはサーバー上でリモートにPOAPパーソナリティのバックアップを作成できます。スイッチから取得したパーソナリティ バックアップは、同じモデルのスイッチでのみ復元する必要があります。

（注） バックアップに Cisco スケジューラ機能を使用している場合は、次の例に示すように、POAP パーソナリティもバックアップするように設定できます。スケジューラの詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

```
switch(config)# scheduler schedule name weeklybkup
switch(config-schedule)# time weekly mon:07:00
switch(config-schedule)# job name personalitybkup
switch(config-schedule)# exit
switch(config)# scheduler job name personalitybkup
switch(config-job)# personality backup bootflash:/personality-file ; copy
bootflash:/personality-file tftp://10.1.1.1/ vrf management
```

手順の概要

1. **personality backup** [**bootflash:***uri* | **scp:***uri*]

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	必須: **personality backup** [**bootflash:***uri* | **scp:***uri*]
	例：
	`switch# personality backup bootflash:personality1.tar`
	例：
	`switch# personality backup scp://root@2.1.1.1/var/lib/tftpboot/backup.tar`
		POAPパーソナリティのバックアップを作成します。

POAP パーソナリティの構成

POAP パーソナリティをシステムの実行状態またはコミット（起動）状態のどちらから取得するかを指定できます。

手順の概要

1. **configure terminal**
2. **personality**
3. **track** [**running-state** | **startup-state** | **data** *local-directories-or-files*]
4. **binary-location** *source-uri-folder*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	必須: **configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	必須: **personality**
	例：
	`switch# personality`
	`switch(config-personality)#`
		パーソナリティ構成モードに入ります。

ステップ 3	必須: **track** [**running-state** | **startup-state** | **data** *local-directories-or-files*]
	例：
	`switch(config-personality)# track data bootflash:myfile1`
	例：
	`switch(config-personality)# track data bootflash:user_scripts/*.py`
	例：
	`switch(config-personality)# track data bootflash:basedir/*/backup_data`
		POAP パーソナリティの派生方法を指定します。次のオプションを使用できます。
		• **running-state** ：次の情報を取得します。実行構成（**show running-config** コマンドで表示）、ホスト システムのアクティブな Cisco NX-OS パッチとサードパーティ パッケージ、およびイメージ名（**show version** コマンドで表示）。これがデフォルトのオプションです。
		• **startup-state** ：次の情報をキャプチャします。スタートアップ コンフィギュレーション（**show startup-config** コマンドで表示）、ホスト システムでコミットされた Cisco NX-OS パッチおよびサードパーティ パッケージ、およびイメージ名（**show version** コマンドで表示）。
		• **data** *local-directories-or-files* ：バックアップするディレクトリまたはファイルを指定します。このコマンドを複数回入力して、複数のディレクトリおよびファイルをバックアップできます。UNIX 形式のワイルドカード文字がサポートされています。この例では、1 つのフォルダと 2 つのディレクトリが指定されています。
		（注）
		このコマンドを使用してブートフラッシュ内のバイナリ ファイルをバックアップしたり、ブートフラッシュ全体をポイントしたりしないでください。
		（注）

	コマンドまたはアクション	目的
		ゲスト シェル パッケージは追跡されません。 （注） 署名付き RPM（キーが必要）はサポートされていません。POAP パーソナリティ機能は、署名された RPM では機能しません。
ステップ 4	必須: **binary-location** *source-uri-folder* 例： `switch(config-personality)# binary-location scp://remote-dir1/nxos_patches/`	POAP パーソナリティの復元時にバイナリ ファイルを取得するローカル ディレクトリまたはリモート ディレクトリを指定します。このコマンドを複数回（優先順位に従って）入力して、複数の場所を指定できます。

POAP パーソナリティの復元

POAP スクリプトの実行フェーズ中に、現在起動されているスイッチ イメージが Cisco NX-OS リリース 7.0(3)I4(1) 以降である場合、スクリプト内のパーソナリティ モジュールは POAP パーソナリティを復元します。必要に応じて、スイッチを正しいソフトウェア イメージにアップグレードします。

（注） パーソナリティの復元は、パーソナリティのバックアップに使用されたのと同じソフトウェア イメージを使用して実行されます。新しいイメージへのアップグレードは、POAP パーソナリティ機能ではサポートされていません。新しいイメージにアップグレードするには、通常の POAP スクリプトを使用します。

（注） パーソナリティ スクリプトが何らかの理由（ブートフラッシュに十分なスペースがない、スクリプトの実行に失敗するなど）で失敗した場合、POAP プロセスは DHCP 検出フェーズに戻ります。

復元プロセスは、次のアクションを実行します。

1. ブートフラッシュ内のパーソナリティ ファイルを解凍します。
2. パーソナリティ ファイルを検証します。
3. パーソナリティ ファイルから構成ファイルとパッケージ リスト ファイルを読み取り、ダウンロードするバイナリのリストを作成します。
4. 現在のイメージまたはパッチがパーソナリティ ファイルで指定されたものと異なる場合、バイナリをブートフラッシュ（存在しない場合）にダウンロードし、正しいイメージで再起動してから、パッケージまたはパッチを適用します。

5. 「/」を基準にしてユーザー データ ファイルを解凍します。
6. POAP パーソナリティの構成ファイルをスタートアップ構成にコピーします。
7. スイッチをリブートします。

POAP パーソナリティ サンプル スクリプト

次のサンプル POAP スクリプト（poap.py）には、パーソナリティ機能が含まれています。

```
#md5sum="b00a7fffb305d13a1e02cd0d342afca3"
# The above is the (embedded) md5sum of this file taken without this line, # can be #
created this way:
# f=poap.py ; cat $f | sed '/^#md5sum/d' > $f.md5 ; sed -i "s/^#md5sum=.*/#md5sum=$(md5sum
 $f.md5 | sed 's/ .*//')/" $f # This way this script's integrity can be checked in case
 you do not trust # tftp's ip checksum. This integrity check is done by
/isan/bin/poap.bin).
# The integrity of the files downloaded later (images, config) is checked # by downloading
 the corresponding file with the .md5 extension and is # done by this script itself.

from poap.personality import POAPPersonality import os

# Location to download system image files, checksums, etc.
download_path = "/var/lib/tftpboot"
# The path to the personality tarball used for restoration personality_tarball =
"/var/lib/tftpboot/foo.tar"
# The protocol to use to download images/config protocol = "scp"
# The username to download images, the personality tarball, and the # patches and RPMs
during restoration username = "root"
# The password for the above username
password = "passwd754"
# The hostname or IP address of the file server server = "2.1.1.1"

# The VRF to use for downloading and restoration vrf = "default"
if os.environ.has_key('POAP_VRF'):
    vrf = os.environ['POAP_VRF']

# Initialize housekeeping stuff (logs, temp dirs, etc.) p = POAPPersonality(download_path,
 personality_tarball, protocol, username, password, server, vrf)

p.get_personality()
p.apply_personality()

sys.exit(0)
```

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。