

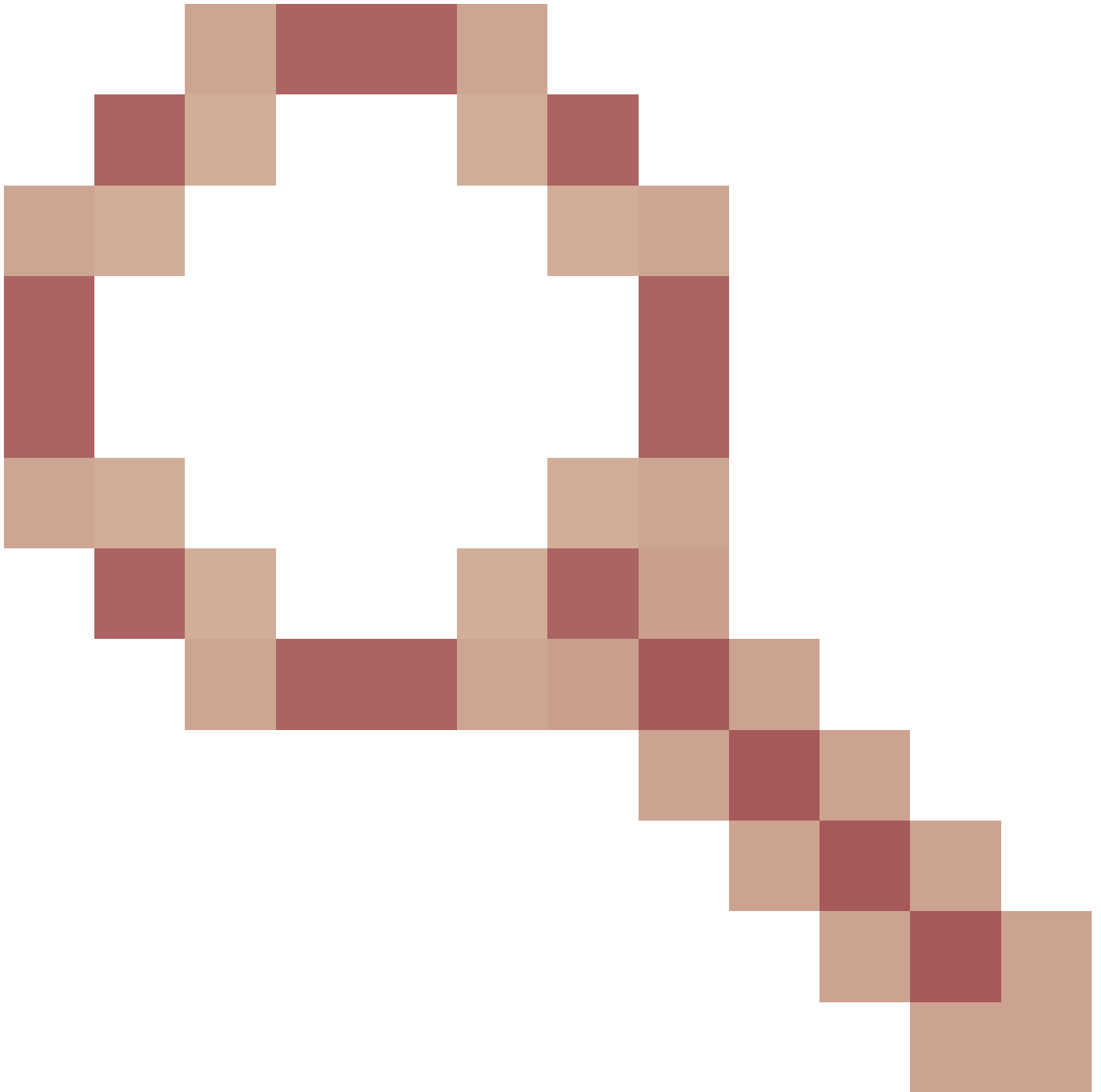
ブートループを引き起こすイメージ破損を回避しながら、アクセスポイントを安全にアップグレードする

内容

はじめに

シスコの一部のアクセスポイント(AP)では、9800シリーズコントローラからCAPWAPを介して破損したイメージをダウンロードする場合があります。 APのソフトウェアバージョンによっては、APが破損したイメージのブートを試行する場合があります、その結果、ブートループが発生します。 この記事では、イメージ破損の影響を受けやすいAPモデルとネットワークパス、および安全にアップグレードする方法について説明します。

この問題が原因でAPがブートループになる場合は、「[Wave 2および11axアクセスポイント\(CSCvx32806\)](#)



[\)でのイメージ破損によるブートループからの回復](#)」で回復手順のガイダンスを参照してください。

アップグレードがイメージ破損の影響を受けるかどうかを判断する方法

展開に次の条件が当てはまる場合、APでは破損したソフトウェアがダウンロードされ、そのソフトウェアをブートしようとする可能性があります。

該当しない製品

- ワイヤレスLANコントローラ(WLC):AireOSワイヤレスLANコントローラからダウンロード

するAPは該当しません

- Mobility Express、組み込みワイヤレスコントローラ
- AP - Aironet 1800/1540/1100ACシリーズWave 2 11ac APおよびWave1 11acアクセスポイント(1700/2700/3700/1570/IW3700)は影響を受けません (これらのAPが9800 WLCに登録されている場合でも、影響はありません)。
- 2023年から導入されたWi-Fi 6E AP:IW9167、IW9165、C9163

該当製品

- WLC: Cisco Catalyst 9800シリーズワイヤレスLANコントローラからのAPのダウンロードが影響を受ける可能性
- AP: Cisco Catalyst 9800シリーズWireless LAN Controllerに登録する次のAPモデルが影響を受けます。
 - Aironet Wave2 11acアクセスポイント(2800/3800/4800/1560/IW6330/ESW6300)
 - Catalyst 9100シリーズWi-Fi6アクセスポイント(9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
 - Catalyst 9100シリーズWi-Fi6Eアクセスポイント(9136/9162/9164/9166)

該当バージョン : Boot a Bad Image症候群

APが破損していることを認識してイメージのブートを試行する場合のこの問題は、Cisco Bug ID [CSCvx32806](#)、[CSCwc72021](#)、[CSCwd90081](#)で対処されており、次のリリースで修正されています。

- 8.10.185.0以降
- 17.3.7以降
- 17.6.6以降
- 17.9.3以降
- 17.11.1以降

アクセスポイントは、上記の修正を適用したソフトウェアにアップグレードされた後も、破損したイメージをダウンロードする可能性があります。ただし、そのイメージをブートするのではなく、成功するまでダウンロードを再試行し続けます。

影響を受けるネットワークパス

APイメージの破損の問題は、9800とAPの間のLANパス (つまり、フル1500バイトのIP MTUを持ち、低遅延でパケット損失の非常に低いパス) では発生していません。この問題は、WAN上のCAPWAPトンネルで発生する可能性が高く、次のようなパス特性があります。

- 高いパケット損失
- 低いCAPWAP MTU (1485バイト未満) : MTUが低いほど、リスクが高くなります
 - capwap MTUが低い場合は、パケット損失の症状である可能性があります

ネットワークパスが危険にさらされているかどうかを判断する方法

- 9800では、次のコマンドを使用してCAPWAPパスMTUを確認します

```
<#root>
```

```
9800-L#show capwap detailed
```

```
Name          APMAC          SourceIP          SrcPort DestIP          DestPort
```

```
MTU
```

```
Mode          McastIf
```

```
-----
```

Name	APMAC	SourceIP	SrcPort	DestIP	DestPort
Capwap1	D4AD.BDA2.8240	192.168.203.203	5247	192.168.6.100	5248
1485					
multicast Mc1					
Capwap2	084F.F983.4A40	192.168.203.203	5247	192.168.6.103	5253
1005					
multicast Mc1					

```
1485
```

```
multicast Mc1
```


```
Capwap2          084F.F983.4A40 192.168.203.203 5247          192.168.6.103  5253
```

```
1005
```

```
multicast Mc1
```

- 特定のAPのMTUが変動している場合、これはリスクの強いインジケータです
- またはshow ap config general | include CAPWAP Path MTU(show tech-support wireless内)
 - 9800の「show tech-support wireless」の出力で[Wireless Config Analyzer Express\(WCAE\)](#)を使用して、「Access Points」>「Configuration」の下でAPのMTUを確認します
- 9800では、「show ap uptime」を使用して、「AP Up Time」が長く、「Association Up Time」が短いAPを探します
 - APのアソシエーションアップタイムが短い(つまり、再設定がない)理由がない場合、これはネットワークパスが危険にさらされていることを示している可能性があります

未修正のAPソフトウェアバージョンから安全にアップグレードする方法

 注：展開がイメージ破損の影響を受ける場合(例：該当するAPモデル、ブートa不良イメージ症候群の修正プログラムなしで実行されているソフトウェア、危険なWAN特性)は、9800ソフトウェアをアップグレードし、APを再加入させて新しいソフトウェアをダウンロードするだけでは、アップグレードしないでください。APはイメージ破損の可能性があります、ブートループが発生します。代わりに、次のいずれかの方法を使用します。

WLCを使用したAPへのローカルなアップグレード

可能であれば、APのLANにステージングコントローラを配置します。これは、9800-CL、または(Wave 2/Wi-Fi 6 APの場合)EWCモードのAPに配置し、APをターゲットバージョンにアップグレードします。これで、実稼働コントローラに安全に参加できるようになります。

AireOSコントローラ経由のアップグレード

8.10.190.0以降を実行しているAireOSコントローラがあり、APモデルがAireOSでサポートされている場合は、APをそのコントローラに加入させます。これにより、APは修正済みソフトウェアに安全にアップグレードされ、実稼働コントローラに安全に加入できるようになります。

archive download-swを使用したアップグレード

アップグレードするAPにアクセス可能なTFTP/SFTPサーバでターゲットAPイメージをステージングします。TFTPまたはSFTP経由でのAPイメージのアップグレードでは、イメージ破損の問題は発生しません。APは、AP CLIから、または (APがコントローラに加入している場合は) コントローラCLIからイメージのダウンロード要求を開始できます。

1. APからアクセス可能な場所にTFTPまたはSFTPサーバをセットアップします。TFTPのパフォーマンスは遅延によってゲートされるため、TFTPサーバがAPから離れている場合はダウンロードが遅くなります。SFTPはTCPを使用するため、高遅延パスを使用する場合はスループットが大幅に向上します。ただし、SFTPはWLCからトリガーできません。ユーザ名とパスワードを入力するためにインタラクティブなダイアログが必要になるためです。
2. TFTPまたはSFTPサーバで目的のAPイメージをステージングします。適切なIOS-XEバージョンにマッピングする15.3(3)J* APバージョンの互換性マトリクスの表4を参照し、該当するAPモデルに適したLightweight APソフトウェアイメージをsoftware.cisco.comからダウンロードしてください。

1. たとえば、CW9162 [isap1g6b-k9w8-tar.153-3.JPN4.tar](#)用の17.9.5 APイメージです。

3. APのCLIからアップグレードするには：コンソールまたはSSHを使用してAPのCLIにアクセスできる場合：

1. TFTPまたはSFTPコマンドを入力します。

```
archive download-sw /no-reload tftp://<ip-address>/<apimage>  
または
```

```
archive download-sw /no-reload sftp://<ip-address>/<apimage>
```

ユーザ名：USER

パスワード：XXX

これにより、破損したイメージが有効なイメージで上書きされます。

2. イメージのダウンロードが完了したら、次のコマンドを発行します。

capwap再起動のテスト

これにより、CAPWAPプロセスが再起動し、APが新しくインストールされたイメージを認識します。

3. 「archive download-sw」を使用して多数のAPをアップグレードする場合、各APで個別にコマンドを入力するのではなく、スクリプト方式を使用できます。次の「WLANポーターによるAPのアップグレード」を参照してください。

4. APがコントローラに加入している場合は、コントローラCLI (TFTPのみ) からAPをアップグレードできます。

1. IOS-XEの場合：

```
ap nameAPNAMEtftp-downgradeip.addr.of.server  
imasename.tar
```

2. AireOSの場合：

```
config ap tftp-downgradeip.addr.of.server  
imasename.tarAPNAME
```

1. AireOSからのCAPWAPダウンロードはイメージ破損の影響を受けることはありませんが、APをAireOSから9800に移行することを計画している場合は、APを9800に加入させる前に、まずAlt-bootおよびBoot a Bad Image症候群 (8.10.190.0以

上)の修正を含むAPイメージをダウンロードするする必要があります。

3. TFTPまたはSFTPサーバのログを監視して、各APがイメージを正常にダウンロードしたことを確認します。ダウンロードが完了すると、各APがリロードされ、新しくダウンロードしたイメージが実行されます。

プレダウンロード、エラーのモニタリングによるAPのアップグレード

9800でターゲットイメージをロードし、APプリダウンロードを使用して新しいイメージをAPにプッシュし、APイメージ破損のインスタンスを監視します。

ステップ 1 : C9800 WLCのAP加入プロファイルでSSHが有効になっていることを確認します。ネットワークにsyslogサーバをセットアップします。AP Join Profile for でsyslogサーバのIPアドレスを設定し、ログトラップ値をDebugに設定します。syslogサーバがAPからsyslogを受信していることを確認します。

Edit AP Join Profile

- General
- Client
- CAPWAP
- AP
- Management**
- Security
- ICap
- QoS

- Device**
- User
- Credentials
- CDP Interface

TFTP Downgrade		Telnet/SSH Configuration	
IPv4/IPv6 Address	<input type="text" value="0.0.0.0"/>	Telnet	<input type="checkbox"/>
Image File Name	<input type="text" value="Enter File Name"/>	SSH	<input checked="" type="checkbox"/>
System Log		Serial Console ⓘ	<input checked="" type="checkbox"/>
Facility Value	<input type="text" value="KERN"/>	AP Core Dump	
Host IPv4/IPv6 Address	<input type="text" value="192.168.1.10"/>	Enable Core Dump	<input type="checkbox"/>
Log Trap Value	<input type="text" value="Debug"/>		
Secured ⓘ	<input type="checkbox"/>		

ステップ 2 : CLIを使用してソフトウェアイメージをC9800 WLCにダウンロードし、プレダウンロードの準備を行います。

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:  
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

ステップ 3 : 次のように、Cisco C9800 WLCでAPイメージのプレダウンロードを実行します。

```
C9800# ap image predownload
```

注 : 導入の規模とタイプによっては、数分から数時間かかる場合があります。 イメージが有効であることを確認するまで、コントローラまたはAPをリブートしないでください。

ステップ 4 : すべてのAPのプレダウンロードが完了したら、syslogサーバで次の2つのログメッセージのいずれかを確認します。

- イメージ署名の検証に成功しました。
- イメージ署名検証エラー : -3

また、`show ap image summary`コマンドの出力を確認し、Failed to Downloadのインスタスがないかを調べます。 カウンタがゼロ以外の場合は、`show ap image`を使用して失敗したAPを見つけます。 | include Failedを発行します。

注意 : いずれかのAPでイメージ署名検証の失敗が記録された場合、またはいずれかのAPでのダウンロードが失敗した場合は、アップグレードプロセスを先に進めないでください。すべてのAPで「Image signing verify success」メッセージが表示された場合、すべてのAPでイメージが正しくダウンロードされているので、9800のアップグレードを安全に進めることができます。

ステップ5 : いずれかのAPで検証エラーが発生したり、ダウンロードに失敗した場合は、ブートループを回避するために、次の手順に従って、APのバックアップパーティション内のイメージを別のAPイメージのアーカイブダウンロードで上書きする必要があります。

障害が発生したAPの数が少ない場合は、単に各APにSSHで接続し、次の手順を開始します。

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

注 : 「test capwap restart」は、バックアップパーティションのイメージが更新されたことをAPのCAPWAPプロセスが認識するために必要です。 これにより、9800とのCAPWAP接続が再開されるため、短時間のサービス中断が発生します。 これが運用上の問題である場合は、この手順をメンテナンス時間帯に延期できます。

WLANポーラーを使用したAPのアップグレード

`archive download-sw`を使用してアップグレードするAPの数が多い場合は、[WLAN Poller](#)を使用して自動プロセスを使用できます。

ステップ1a:Macまたは[Windowsマシン](#)にWLANポーターをインストールします。

ステップ1b:Aplist csvファイルに、関連する障害が発生したAPを入力します。

ステップ1c:次のコマンドを使用してcmdlistファイルにデータを入力します (必要に応じて、いつでも追加できます)。

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

ステップ1d:WLANポーターを実行します。

ステップ1e:実行が完了したら、各APのログファイルを確認して、正常に完了したことを検証します。

ステップ 2 : C9800 WLCでイメージをただちにアクティブ化し、リロードします。

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

手順3:C9800 WLC上でイメージをコミットします。この手順をスキップすると、WLCは以前のソフトウェアイメージにロールバックします

```
C9800#install commit
```

よく寄せられる質問 (FAQ)

Q.数日前にプレダウンロードを実行しましたが、まだCisco C9800 WLCとAPをリブートしていません。イメージが破損しているかどうかを確認するためのsyslogがありません。イメージが破損しているかどうかを確認するにはどうすればよいですか。

A. APまたはsyslogでshow loggingをチェックします。show loggingの出力に成功または失敗のメッセージが表示されない場合は、「show flash syslog」コマンドを使用して、プレダウンロードを実行したときからのsyslog出力をファイルできます。「Image signing verify success」メッセージが表示された場合、このAPがイメージを正常にダウンロードしたことを意味します。

Q : ローカルモードのAPを使用して集中型の導入を行っています。「回避策とソリューション」セクションに記載されている手順を実行する必要がありますか。

A：この問題が報告されているのは、WAN接続経由でAPをアップグレードする場合だけです。ローカルモードやローカルネットワーク上のAPでこの問題が発生する可能性はほとんどないため、コントローラとAPの間のパケット損失がごくわずかであると確信できる場合は、アップグレードのためにこの手順に従う必要はありません。

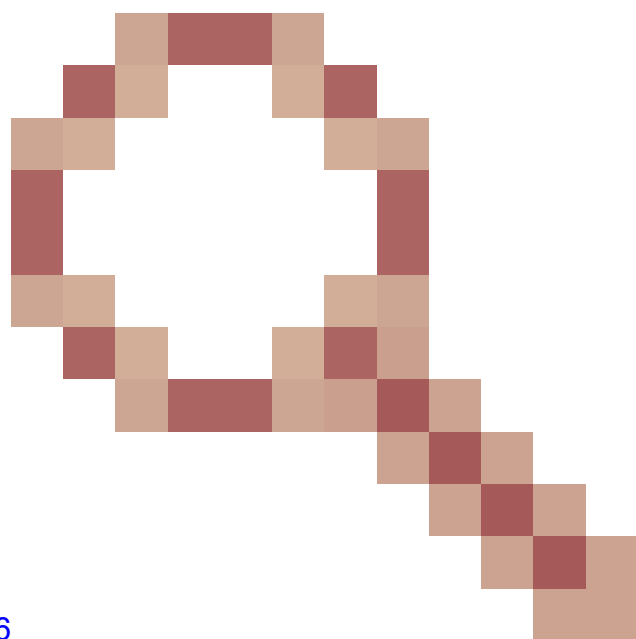
Q：新しいアウトオブボックスAPがあります。この問題が発生せずに導入するには、どうすればよいですか。

A:WAN経由でコードをダウンロードする新しいアウトオブボックスのAPも、2023年12月以降に製造されたものを除き、この問題が発生する可能性があります。

Q: 9800からダウンロードしたCAPWAPイメージが破損するこの問題に対処するために、シスコは長期的にはどのような対策を講じていますか。

A:APで17.11以降がすでに実行されている場合は、アウトオブバンドイメージダウンロード機能を使用して、HTTPSを使用してコントローラからイメージを取得できます。TCPはスライディングウィンドウを使用して信頼性の高い方法でデータを送信するため、WAN上でもCAPWAP (またはTFTP) よりもはるかに高速です

Q.現在ブートループにあるAPがあります。 どうすれば回復できますか。



A: [Wave 2および11axアクセスポイント\(CSCvx32806\)](#)でのイメージ破損が原因で発生するブートループからの復旧に関する記事を参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。