



# 自律アクセスポイントの Lightweight モード への変換

- 機能情報の確認, 1 ページ
- Lightweight モードに自律アクセスポイントを変換するための前提条件, 2 ページ
- Lightweight モードに変換される Autonomous アクセスポイントについて, 2 ページ
- Lightweight アクセスポイントの Autonomous アクセスポイントへの再変換方法, 4 ページ
- アクセスポイントの認可 (CLI) , 5 ページ
- アクセスポイントの認可 (GUI) , 7 ページ
- 変換したアクセスポイントでの Reset ボタンのディセーブル化 (CLI) , 7 ページ
- AP クラッシュログ情報のモニタリング, 8 ページ
- アクセスポイントでの固定 IP アドレスの設定方法, 9 ページ
- TFTP リカバリ手順を使用したアクセスポイントのリカバリ, 11 ページ
- Autonomous アクセスポイントを Lightweight モードに変換する場合の設定例, 12 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノート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 には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

## Lightweight モードに自律アクセス ポイントを変換するための前提条件

- Lightweight モードに変換したアクセス ポイントは、無線ドメインサービス (WDS) をサポートしません。変換したアクセス ポイントは、Cisco ワイヤレス LAN スイッチとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、スイッチが WDS に相当する機能を提供します。
- すべての Cisco Lightweight アクセス ポイントでは、無線ごとに 16 の Basic Service Set Identifier (BSSID) およびアクセス ポイントごとに合計 16 のワイヤレス LAN をサポートします。変換されたアクセス ポイントがスイッチにアソシエートすると、アクセス ポイントがアクセス ポイント グループのメンバーでない限り、ID 1~16 のワイヤレス LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネットブロードキャストを使用して IP アドレスを取得し、スイッチを検出する必要があります。

## Lightweight モードに変換される Autonomous アクセス ポイントについて

Autonomous Cisco Aironet アクセス ポイントを Lightweight モードに変換できます。アクセス ポイントを Lightweight モードにアップグレードしようとする、アクセス ポイントはスイッチと通信し、スイッチから構成およびソフトウェア イメージを受信します。

## Lightweight モードから Autonomous モードへの復帰

Autonomous アクセス ポイントを Lightweight モードに変換してから、Autonomous モードをサポートする Cisco IOS リリース (Cisco IOS リリース 12.3(7)JA 以前のリリース) をロードして、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがスイッチに関連付けられている場合、スイッチを使用して Cisco IOS リリースをロードします。アクセス ポイントがスイッチに関連付けられていない場合、TFTP を使用して Cisco IOS リリースをロードします。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセス ポイントがアクセスできる必要があります。

## DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value (TLV) 形式を使用します。DHCP サーバは、アクセス ポイントの DHCP ベンダー クラス ID (VCI) 文字列に基づいてオプションを返すよう、プログラムする必要があります (DHCP オプション 60)。

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセスポイントが、サービスプロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセスポイントの VCI 文字列は、前の表にある VCI 文字列と異なります。VCI 文字列の末尾には「ServiceProvider」が付きます。たとえば、このオプションが付いた 1260 は、VCI 文字列「Cisco AP c1260-ServiceProvider」を返します。



(注) DHCP サーバから取得するスイッチの IP アドレスは、ユニキャスト IP アドレスになります。DHCP オプション 43 を設定する場合は、スイッチの IP アドレスをマルチキャストアドレスとして設定しないでください。

## 変換したアクセスポイントがクラッシュ情報をスイッチに送信する方法

変換したアクセスポイントが予期せずリブートした場合、アクセスポイントではクラッシュ発生時にローカルフラッシュメモリ上にクラッシュファイルが保存されます。装置がリブートしたら、アクセスポイントはリブートの理由をスイッチに送信します。クラッシュにより装置がリブートした場合、スイッチは既存の CAPWAP メッセージを使用してクラッシュファイルを取得し、スイッチのフラッシュメモリに保存します。クラッシュ情報のコピーは、スイッチがアクセスポイントから取得した時点で、アクセスポイントのフラッシュメモリから削除されます。

## 変換したアクセスポイントからのメモリコアダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセスポイントは、スイッチにメモリコアダンプを送信しません。このセクションでは、スイッチ GUI または CLI を使用してアクセスポイントコアダンプをアップロードする手順について説明します。

## 変換されたアクセスポイントの MAC アドレスの表示

コントローラが変換されたアクセスポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ページには、コントローラにより変換されたアクセスポイントのイーサネット MAC アドレスのリストが表示されます。
- [AP Detail] ページには、変換されたアクセスポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセスポイントのリストがスイッチにより無線 MAC アドレス順に表示されます。

## Lightweight アクセス ポイントの静的 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。静的 IP アドレスは、通常、AP 数の限られた導入でのみ使用されます。

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメインネームシステム (DNS) 解決を使用してスイッチを検出できません。これらのパラメータは、スイッチ CLI または GUI のいずれかを使用して設定できます。



- (注) アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォールバックします。アクセス ポイントが DHCP アドレスにフォールバックした場合は、`show ap config general Cisco_AP CLI` コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバックアドレスであるとは識別しません。

## Lightweight アクセス ポイントの Autonomous アクセス ポイントへの再変換方法

### Lightweight アクセス ポイントを Autonomous モードに戻す方法 (CLI)

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Device# enable	特権 EXEC モードを開始します。
ステップ 2	<b>ap name Cisco_AP tftp-downgrade tftp_server_ip_address tftp_server_image_filename</b>  例 : Device# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname	Lightweight アクセス ポイントを Autonomous モードに戻します。  (注) このコマンドを入力したら、アクセス ポイントが再起動するまで待機し、CLI または GUI を使用してアクセス ポイントを再設定します。

## モード ボタンと TFTP サーバを使用して Lightweight アクセス ポイントを Autonomous モードに戻す方法

### 手順

- ステップ 1 TFTP サーバソフトウェアを実行している PC に、10.0.0.2 ~ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。
- ステップ 2 コンピュータの TFTP サーバフォルダにアクセスポイントのイメージファイル（たとえば、1140 シリーズ アクセスポイントの場合は *c1140-k9w7-tar.123-7.JA.tar*）が存在すること、およびその TFTP サーバがアクティブであることを確認します。
- ステップ 3 TFTP サーバフォルダ内の 1140 シリーズ アクセスポイントのイメージファイルの名前を **c1140-k9w7-tar.default**に変更します。
- ステップ 4 Category 5 (CAT 5; カテゴリ 5) のイーサネット ケーブルを使用して、PC をアクセスポイントに接続します。
- ステップ 5 アクセスポイントの電源を切ります。
- ステップ 6 MODE ボタンを押しながら、アクセスポイントに電源を再接続します。  
(注) アクセスポイントの **MODE** ボタンがイネーブルになります。
- ステップ 7 MODE ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ~ 30 秒かかります）、MODE ボタンを放します。
- ステップ 8 アクセスポイントがリブートしてすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。
- ステップ 9 アクセスポイントがリブートしたら、GUI または CLI を使用してアクセスポイントを再設定します。

## アクセスポイントの認可 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device# <b>enable</b>	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b>  例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>ap auth-list ap-policy authorize-ap</b>  例： Device(config)# ap auth-list ap-policy authorize-ap	アクセス ポイントの許可ポリシーを設定します。
ステップ 4	<b>username user_name mac aaa attribute list list_name</b>  例： Device(config)# username aaa.bbb.ccc mac aaa attribute list attrlist	アクセス ポイントの MAC アドレスをローカルで設定します。
ステップ 5	<b>aaa new-model</b>  例： Device(config)# aaa new-model	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 6	<b>aaa authorization credential-download auth_list local</b>  例： Device(config)# aaa authorization credential-download auth_download local	ローカル サーバから EAP 資格情報をダウンロードします。
ステップ 7	<b>aaa attribute list</b> リスト  例： Device(config)# aaa attribute list alist	AAA 属性リストの定義を設定します。
ステップ 8	<b>aaa session-id common</b>  例： Device(config)# aaa session-id common	AAA の共通セッション ID を設定します。
ステップ 9	<b>aaa local authentication default authorization default</b>  例： Device(config)# aaa local authentication default authorization default	ローカル 認証方式 リストを設定します。
ステップ 10	<b>show ap name Cisco_AP config general</b>  例： Device(config)# show ap name AP01 config general	特定のアクセス ポイントに対応する設定情報を表示します。

## アクセスポイントの認可 (GUI)

### 手順

- 
- ステップ 1** [Configuration] > [Security] > [AAA] > [AP Policy] の順に選択します。  
[AP Policy] ページが表示されます。
- ステップ 2** [Policy Configuration] 領域で、次のパラメータをイネーブルまたはディセーブルにします。
- Authorize LSC APs against Auth-List
  - AP with Self-Signed Certificate
  - Authorize MIC APs against AAA
  - AP with Manufacturing Installed Certificate
- ステップ 3** [Apply] をクリックします。
- ステップ 4** [Save Configuration] をクリックします。
- 

## 変換したアクセスポイントでの Reset ボタンのディセーブル化 (CLI)

Lightweight モードに変換したアクセスポイントの Reset ボタンをイネーブルまたはディセーブルにできます。Reset ボタンには、アクセスポイントの外面に MODE と書かれたラベルが付けられています。



(注) コントローラ GUI を使用してこのタスクを実行する手順は現在利用できません。

---

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Device# enable	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b>  例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>no ap reset-button</b>  例： Device(config)# no ap reset-button	スイッチに関連付けられ、変換したすべてのアクセスポイントの Reset ボタンをディセーブルにします。  (注) スイッチに関連付けられ、変換したすべてのアクセスポイントの Reset ボタンをイネーブルにするには、 <b>ap reset-button</b> コマンドを入力します。
ステップ 4	<b>end</b>  例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。
ステップ 5	<b>ap name Cisco_AP reset-button</b>  例： Device# ap name AP02 reset-button	指定した変換済みアクセスポイントの Reset ボタンをイネーブルにします。

## AP クラッシュ ログ情報のモニタリング



(注) スイッチ GUI を使用してこのタスクを実行する手順は現在利用できません。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device# <b>enable</b>	特権 EXEC モードを開始します。
ステップ 2	<b>show ap crash-file</b>  例： Device# <b>show ap crash-file</b>	クラッシュ ファイルがスイッチにダウンロードされているかどうかを確認します。



# アクセスポイントでの固定 IP アドレスの設定方法

## アクセスポイントでの固定 IP アドレスの設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例： Device# enable</p>	特権 EXEC モードを開始します。
ステップ 2	<p><b>ap name Cisco_AP static-ip ip-address static_ap_address netmask static_ip_netmask gateway static_ip_gateway</b></p> <p>例： Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2</p>	<p>アクセスポイントの固定 IP アドレスを設定します。このコマンドには、次のキーワードと引数が含まれます。</p> <ul style="list-style-type: none"> <li>• <b>ip-address</b> : Cisco アクセスポイントの固定 IP アドレスを指定します。</li> <li>• <b>ip-address</b> : Cisco アクセスポイントの固定 IP アドレス。</li> <li>• <b>netmask</b> : Cisco アクセスポイントの固定 IP ネットマスクを指定します。</li> <li>• <b>netmask</b> : Cisco アクセスポイントの固定 IP ネットマスク。</li> <li>• <b>gateway</b> : Cisco アクセスポイントゲートウェイを指定します。</li> <li>• <b>gateway</b> : Cisco アクセスポイントゲートウェイの IP アドレス。</li> </ul> <p>アクセスポイントがリブートしてスイッチに再 join し、指定した固定 IP アドレスがアクセスポイントにプッシュされます。固定 IP アドレスがアクセスポイントに送信された後、DNS サーバの IP アドレスおよびドメイン名を設定できます。アクセスポイントのリブート後にステップ 3 と 4 を実行します。</p>
ステップ 3	<p><b>enable</b></p> <p>例： Device# enable</p>	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<b>configure terminal</b>  例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 5	<b>ap static-ip name-server</b> <i>nameserver_ip_address</i>  例： Device(config)# ap static-ip name-server 10.10.10.205	特定のアクセスポイントまたはすべてのアクセスポイントが DNS 解決を使用してスイッチを検出できるよう DNS サーバを設定します。  (注) DNS サーバ設定を元に戻すには、 <b>no ap static-ip name-server nameserver_ip_address</b> コマンドを入力します。
ステップ 6	<b>ap static-ip domain</b> <i>static_ip_domain</i>  例： Device(config)# ap static-ip domain domain1	特定のアクセスポイントまたはすべてのアクセスポイントが属するドメインを設定します。  (注) ドメイン名の設定を元に戻すには、 <b>no ap static-ip domain static_ip_domain</b> コマンドを入力します。
ステップ 7	<b>end</b>  例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	<b>show ap name</b> <i>Cisco_AP</i> <b>config</b> <b>general</b>  例： Device# show ap name AP03 config general	アクセスポイントの IP アドレス設定を表示します。

## アクセスポイントでの固定 IP アドレスの設定 (GUI)

### 手順

- ステップ 1 [設定 (Configuration) ]>[ワイヤレス (Wireless) ]>[アクセスポイント (Access Points) ]>[すべての AP (All Aps) ]の順に選択します。  
[All APs] ページが表示されます。
- ステップ 2 アクセスポイントの名前をクリックします。

[AP] > [編集 (Edit)] ページが表示されます。

- ステップ 3** [一般 (General)] タブの [IP 設定 (IP Config)] 領域で、アクセスポイントに固定 IP アドレスを割り当てる場合は、[固定 IP (Static IP)] チェックボックスをオンにします。
- ステップ 4** 次の詳細を入力します。
- Static IP
  - ネットマスク
  - Gateway
- ステップ 5** [Apply] をクリックします。  
アクセスポイントがリブートしてスイッチを再 join し、指定した固定 IP アドレスがアクセスポイントに送信されます。
- ステップ 6** 固定 IP アドレスがアクセスポイントに送信された後、[DNS IP アドレス (DNS IP Address)] と [ドメイン名 (Domain Name)] を設定します。
- ステップ 7** [Apply] をクリックします。
- ステップ 8** [Save Configuration] をクリックします。
- 

## TFTP リカバリ手順を使用したアクセスポイントのリカバリ

### 手順

---

- ステップ 1** 必要なリカバリイメージを Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) からダウンロードし、ご利用の TFTP サーバのルートディレクトリにインストールします。
- ステップ 2** TFTP サーバをターゲットのアクセスポイントと同じサブネットに接続して、アクセスポイントをパワーサイクリングします。アクセスポイントは TFTP イメージから起動し、スイッチに接続してサイズの大きなアクセスポイントのイメージをダウンロードし、アップグレード手順を完了します。
- ステップ 3** アクセスポイントが回復したら、TFTP サーバを削除できます。
-

# Autonomous アクセスポイントを Lightweight モードに変換する場合の設定例

## アクセスポイントの IP アドレス設定の表示：例

次に、アクセスポイントの IP アドレス設定を表示する例を示します。

```
Device# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier..... 4
Cisco AP Name..... AP6
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.10.118
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.10.1
Domain..... Domain1
Name Server..... 10.10.10.205
....
```

## アクセスポイントのクラッシュ ファイル情報の表示：例

次の例は、アクセスポイントのクラッシュファイル情報を表示する方法を示しています。このコマンドを使用して、ファイルがスイッチにダウンロードされたかどうかを確認できます。

```
Device# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)
```

The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.