



## Cisco Aironet Wave 2 アクセス ポイント リリース 8.7 コマンド リファレンス

初版 : 2018 年 4 月 10 日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 : シスコ コンタクトセンター  
0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間 : 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークボロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



## 目次

---

はじめに :

はじめに ix

対象読者 ix

表記法 ix

関連資料 xii

マニュアルの入手方法およびテクニカル サポート xii

---

第 1 章

コマンドライン インターフェイスの使用 1

コマンド モードについて 2

コマンドの省略形 3

コマンドの no 形式について 4

CLI のエラー メッセージについて 5

ターミナルの設定 6

コマンドの呼び出し 7

CLI のアクセス 8

---

第 2 章

capwap コマンド 9

capwap ap 10

capwap ap auth-token 11

capwap ap erase 12

capwap ap ethernet 13

capwap ap hostname 14

capwap ap ip 15

capwap ap lag 16

capwap ap mode 17

capwap ap restart 18

---

第 3 章**clear コマンド 19**

clear avc nbar 20

clear counters 21

clear cts 22

clear datapath 23

clear dot11 24

clear logging 25

---

第 4 章**config コマンド 27**

config ap client-trace 28

config ap client-trace filter 30

config ap client-trace output 31

config boot baudrate 32

config boot break 33

config boot crashkernel 34

config boot debug-memory 35

config boot manual 36

config boot path 37

config cts debug enforcement host\_ip 38

config cts debug enforcement rate 39

config cts debug enforcement permissions 40

config cts debug enforcement protocol 41

---

第 5 章**debug コマンド 43**

debug arp 45

debug ble 46

debug capwap client 47

debug capwap client avc 48

debug cdp 49

debug cleanair 50

debug dhcp 51

debug dot11 52

debug dot11 client datapath	53
debug dot11 client level	54
debug dot11 driver slot	55
debug dot11 sensor	56
debug dtls client	57
debug ethernet	58
debug flexconnect	59
debug lldp	60
debug memory	61
debug memory pool	62
debug memory pool alloc	63
debug memory pool free	64
debug mesh	65
debug mesh adjacency	66
debug mesh path-control	67
debug rrm neighbor	68
debug rrm reports	69
debug sip	70
debug wips	71
debug authentication interface	72
debug process memory	73
debug traffic	74
debug tunnel	75
debug client trace	76
no	77
traceroute	78
undebug	79

---

**第 6 章**

<b>show コマンド</b>	<b>81</b>
show ap client-trace status	83
show arp	84
show avc cft	85
show avc nbar	86
show avc netflow flows	87

show avc status	88
show boot	89
show capwap	90
show capwap client	91
show capwap client trace	92
show capwap ids sig	93
show cdp	94
show class-map	95
show cleanair debug	96
show client statistics	97
show clock	98
show configuration	99
show controller ble	100
show controllers dot11Radio	102
show controllers nss status	103
show controllers wired	104
show crypto	105
show debug	106
show dhcp	107
show dot11 qos	108
show filesystems	109
show flash	110
show flexconnect	111
show flexconnect ocap firewall	112
show flexconnect wlan	113
show interfaces dot11Radio	114
show interfaces network	115
show interfaces wired	116
show inventory	117
show ip	118
show lacp	119
show logging	120
show memory	121
show policy-map	123

show processes	124
show processes memory	125
show rrm	127
show rrm rogue containment	128
show rrm rogue detection	129
show running-config	131
show security data-corruption	133
show security system state	134
show spectrum	136
show tech-support	137
show version	138
show trace dot11_chn	139
show trace	140
show wips	141

---

**第 7 章****システム管理コマンド 143**

ap-type	144
archive	145
copy	146
delete	147
disable	148
enable	149
exec-timeout	150
logging	151
more	152
reload	153
terminal	154







## はじめに

ここでは、『Cisco Aironet Wave 2 アクセス ポイント コマンド リファレンス』の対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

- [対象読者 \(ix ページ\)](#)
- [表記法 \(ix ページ\)](#)
- [関連資料 \(xii ページ\)](#)
- [マニュアルの入手方法およびテクニカル サポート \(xii ページ\)](#)

## 対象読者

このマニュアルは、Cisco Aironet Wave 2 アクセス ポイントの設定および保守に携わる、十分な経験を持つネットワーク管理者を対象としています。



(注) **test** コマンドを使用すると、Cisco AP の予期しない再起動など、システムが中断することがあります。このため、デバッグ目的で **test** コマンドを Cisco AP で使用する際は Cisco Technical Assistance Center (TAC) 担当者の支援を受けることをお勧めします。

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは太字で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。

表記法	説明
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



ヒント 「問題解決に役立つ情報」です。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



警告 This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (このマニュアルに記載されている警告の翻訳を参照するには、付録の「翻訳版の安全上の警告」を参照してください)。

警告タイトル	説明
Waarschuwing	Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").

警告タイトル	説明
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

## 関連資料

- Cisco アクセス ポイント : <https://www.cisco.com/c/en/us/products/wireless/access-points/index.html>
- Cisco ワイヤレス コントローラ ソフトウェア マニュアル : <https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html>

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



# コマンドラインインターフェイスの使用

---

この章では、Cisco Aironet Wave 2 AP コマンドラインインターフェイス (CLI) について説明し、CLI を使用して AP を設定する方法について説明します。

- [コマンドモードについて \(2 ページ\)](#)
- [コマンドの省略形 \(3 ページ\)](#)
- [コマンドの no 形式について \(4 ページ\)](#)
- [CLI のエラーメッセージについて \(5 ページ\)](#)
- [ターミナルの設定 \(6 ページ\)](#)
- [コマンドの呼び出し \(7 ページ\)](#)
- [CLI のアクセス \(8 ページ\)](#)

## コマンドモードについて

Cisco Aironet Wave 2 AP のコマンドラインインターフェイスは、次の 2 つの異なるモードに分けられます。

- ユーザ EXEC モード：AP でセッションを開始すると、ユーザ EXEC モードで開始します。このモードでは、一部のコマンドしか使用できません。また、ユーザ EXEC モードで利用できる **show** コマンドは、特権 EXEC モードで利用できる **show** コマンドのサブセットです。  
ユーザ EXEC コマンドは、AP を再起動するときに保存されません。
- 特権 EXEC モード：このモードでは、すべてのコマンドを利用できます。特権 EXEC モードを開始するには、パスワードを入力する必要があります。

利用できるコマンドは、現在実行しているモードによって異なります。現在のコマンドモードで利用できるコマンドのリストを取得するには、システムプロンプトで疑問符 (?) を入力します。たとえば、以下ではユーザ EXEC モードで利用可能なコマンドのリストが表示されています。

```
cisco-wave2-ap>?
Exec mode commands
  enable Turn on privileged commands
  logout Logout out from CLI
  ping Send echo messages
  show Show running system information
```

表 1: コマンドモードの概要

モード	アクセス方式	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	cisco-wave2-ap>	<b>logout</b> または <b>quit</b> を入力します。	このモードを使用して次の作業を行います。 <ul style="list-style-type: none"> <li>• 端末の設定変更</li> <li>• 基本テストの実行</li> <li>• システム情報の表示</li> </ul>
特権 EXEC	ユーザ EXEC モードを実行している場合は、 <b>enable</b> コマンドを入力し、プロンプトが表示されたらパスワードを入力します。	cisco-wave2-ap#	<b>disable</b> を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。

## コマンドの省略形

AP でコマンドが一意に認識される長さまでコマンドを入力します。

**show configuration** 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
cisco-wave2-ap# show conf
```

## コマンドの **no** 形式について

多くの機能でデバッグを有効にするには **debug** コマンドを使用する必要がありますが、プレフィックス **no** を使用するとそれらの各機能でデバッグが無効になります。次に例を示します。

デバッグを有効にするコマンド：

```
cisco-wave2-ap# debug client ...
```

デバッグを無効にするコマンド：

```
cisco-wave2-ap# no debug client ...
```



## CLIのエラーメッセージについて

次の表に、CLIを使用してAPを設定するときに表示される可能性のあるエラーメッセージの一部を紹介します。

表 2: CLIの代表的なエラーメッセージ

エラーメッセージ	意味	ヘルプの表示方法
% Ambiguous command: "show con"	APがコマンドを認識できるだけの文字数が入力されていません。	最後に疑問符 (?) を付けて、コマンドを再度入力します。コマンドと疑問符の間にはスペースを1つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	最後に疑問符 (?) を付けて、コマンドを再度入力します。コマンドと疑問符の間にはスペースを1つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Invalid input detected at '^' marker.	コマンドの入力ミスです。間違っている箇所をキャレット (^) 記号で示しています。	疑問符 (?) を入力すると、そのコマンドモードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

# ターミナルの設定

## 始める前に

特権 EXEC モードを開始します。

## 手順

- 次のコマンドを入力して、画面上の行数を設定します。

**terminal length** *number-of-lines*

有効な範囲は 0 ～ 512 です。0 を入力すると、一時停止しなくなります。

例：

```
cisco-wave2-ap# terminal length 20
```

- 次のコマンドを入力して、現在のターミナル回線にデバッグ出力をコピーします。

**terminal monitor**

- 次のコマンドを入力して、現在のターミナル回線へのロギングを無効にします。

**terminal monitor disable**

- 次のコマンドを入力して、ターミナルのタイプを指定します。

**terminal type** *type-name*

- 次のコマンドを入力して、画面の行に表示する文字数を設定します。

**terminal width** *number-of-characters*

有効な範囲は 0 ～ 132 です。

例：

```
cisco-wave2-ap# terminal width 30
```

## コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 3: コマンドの呼び出し

アクション	結果
上矢印キーを押す	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
下矢印キーを押す	上矢印キーでコマンドを呼び出してから、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。

## CLI のアクセス

CLIにはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。1つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。



## capwap コマンド

---

- [capwap ap](#) (10 ページ)
- [capwap ap auth-token](#) (11 ページ)
- [capwap ap erase](#) (12 ページ)
- [capwap ap ethernet](#) (13 ページ)
- [capwap ap hostname](#) (14 ページ)
- [capwap ap ip](#) (15 ページ)
- [capwap ap lag](#) (16 ページ)
- [capwap ap mode](#) (17 ページ)
- [capwap ap restart](#) (18 ページ)

## capwap ap

AP にプライマリ、セカンダリ、ターシャリ コントローラを設定するには、**capwap ap** コマンドを使用します。

**capwap ap {primary-base | secondary-base | tertiary-base}**  
*controller-name controller-ip-address*

構文の説明	<b>primary-base</b>	AP のプライマリ コントローラを設定する
	<b>secondary-base</b>	AP のセカンダリ コントローラを設定する
	<b>tertiary-base</b>	AP のターシャリ コントローラを設定する
	<i>controller-name</i>	コントローラの名前
	<i>controller-ip-address</i>	コントローラの IP アドレス。

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
 ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、AP にプライマリ コントローラを設定する例を示します。

```
cisco-wave2-ap# capwap ap primary-base wlc-5520 209.165.200.224
```

## capwap ap auth-token

認証トークンを設定するには、**capwap ap auth-token** コマンドを使用します。

**capwap ap auth-token** *ssc-token*

構文の説明	<i>ssc-token</i> SSC トークン。有効な範囲は 8 ～ 32 文字
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 ス 8.1.111.0 このコマンドが導入されました。

### 例

次に、認証トークンを設定する例を示します。

```
cisco-wave2-ap# capwap ap auth-token myauthtoken
```

## capwap ap erase

CAPWAP 設定を消去するには、**capwap ap erase** コマンドを使用します。

**capwap ap erase** {**all** | **static-ip**}

### 構文の説明

**all** すべての CAPWAP 設定を消去します。

(注) AP がブリッジモードの場合、初期設定にリセットした後の AP は同じブリッジモードのままになります。AP が FlexConnect、Local、Sniffer、またはその他のモードの場合は、初期設定にリセットした後、AP モードは Local モードに設定されます。AP でリセットボタンを押し、正しい初期設定へのリセットを実行すると、AP は cookie 設定モードに移行します。

**static-ip** スタティック IP または DNS 設定を消去します。

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、AP 上のすべての CAPWAP 設定を消去する例を示します。

```
cisco-wave2-ap# capwap ap erase all
```



## capwap ap ethernet

AP イーサネット パラメータを設定するには、**capwap ap ethernet** コマンドを使用します。

**capwap ap ethernet tag** *ethernet-vlan-id*

---

### 構文の説明

*ethernet-vlan-id* イーサネット VLAN ID。有効な範囲は 0 ～ 4094 です。VLAN ID の値に 0 を入力すると、VLAN タギングは無効になります。

---

---

### コマンド モード

Privileged EXEC (#)

---

### コマンド履歴

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、AP でイーサネット VLAN タギングを設定する例を示します。

```
cisco-wave2-ap# capwap ap ethernet tag 2
```

## capwap ap hostname

AP のホスト名を設定するには、**capwap ap hostname** コマンドを使用します。

**capwap ap hostname** *ap-name*

---

### 構文の説明

---

*ap-name* AP  
名

---

---

### コマンドモード

Privileged EXEC (#)

---

### 使用上のガイドライン

AP がすでに Cisco WLC に関連付けられている場合、新しいホスト名が Cisco WLC で反映されるには、AP と Cisco WLC の関連付けをいったん解除して再度関連付ける必要があります。

---

### コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、AP にホスト名を設定する例を示します。

```
cisco-wave2-ap# capwap ap hostname cisco-wave2-ap-2802
```

## capwap ap ip

CAPWAP AP にスタティック IP アドレスと DNS を設定するには、**capwap ap ip** コマンドを使用します。

```
capwap ap ip static-ip-addr static-netmask ip-addr-default-gateway [ip-addr-dns1 | ip-addr-dns2]
[domain-name]
```

構文の説明	
<i>static-ip-addr</i>	AP のスタティック IP アドレス
<i>static-netmask</i>	スタティック ネットマスク
<i>ip-addr-default-gateway</i>	デフォルトゲートウェイの IP アドレス。
[ <i>ip-addr-dns1</i>   <i>ip-addr-dns2</i> ]	(任意のパラメータ) DNS の IP アドレス
[ <i>domain-name</i> ]	(任意のパラメータ) ドメイン名

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、CAPWAP AP にスタティック IP アドレスと DNS を設定する例を示します。

```
cisco-wave2-ap# capwap ap ip 209.165.200.225 255.255.255.224 209.165.200.227
209.165.200.226 example.org
```

## capwap ap lag

CAPWAP LAG を設定するには、**capwap ap lag** コマンドを使用します。

**capwap ap lag** {enable | disable}

---

### 構文の説明

---

**enable** LAG を有効にする

---

**disable** LAG を無効にする

---

---

### コマンドモード

Privileged EXEC (#)

---

### コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、AP で LAG を有効にする例を示します。

```
cisco-wave2-ap# capwap ap lag enable
```

## capwap ap mode

AP モードを設定するには、**capwap ap mode** コマンドを使用します。

**capwap ap mode {bridge | local}**

---

### 構文の説明

---

**bridge** ブリッジモードを有効にする

---

**local** ローカルモードを有効にする

---

---

### コマンドモード

Privileged EXEC (#)

---

---

### コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、AP をローカルモードで動作するように設定する例を示します。

```
cisco-wave2-ap# capwap ap mode local
```

## capwap ap restart

CAPWAP プロトコルを再起動するには、**capwap ap restart** コマンドを使用します。

### capwap ap restart

構文の説明	<b>restart</b> CAPWAP プロトコルを再起動する
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

### 例

次に、CAPWAP プロトコルを再起動する例を示します。

```
cisco-wave2-ap# capwap ap restart
```



## clear コマンド

---

- [clear avc nbar](#) (20 ページ)
- [clear counters](#) (21 ページ)
- [clear cts](#) (22 ページ)
- [clear datapath](#) (23 ページ)
- [clear dot11](#) (24 ページ)
- [clear logging](#) (25 ページ)

## clear avc nbar

AVC NBAR 統計情報をクリアするには、**clear avc nbar** コマンドを使用します。

### clear avc nbar statistics

構文の説明	<b>statistics</b> AVC NBAR 統計情報をクリアする
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

### 例

次に、AVC NBAR 統計情報をクリアする例を示します。

```
cisco-wave2-ap# clear avc nbar statistics
```



## clear counters

802.11 無線の統計情報をクリアするには、**clear counters** コマンドを使用します。

**clear counters** [**Dot11Radio** *interface-number*]

---

### 構文の説明

**Dot11Radio** (任意) Dot11 インターフェイスの統計情報をクリアする

*interface-number* Dot11Radio インターフェイス番号。有効な値は 0 または 1

---

---

### コマンドモード

Privileged EXEC (#)

---

### コマンド履歴

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、指定したインターフェイス番号の 802.11 インターフェイスの統計情報をクリアする例を示します。

```
cisco-wave2-ap# clear counters Dot11Radio 1
```

## clear cts

Cisco TrustSec Security の統計情報をクリアするには、**clear cts** コマンドを使用します。

**clear cts role-based counters** [**all** | **client** *mac-addr* | **from** *sgt* **to** *dgt*]

### 構文の説明

<b>counters</b>	Cisco TrustSec の要約カウンタをクリアする
<b>all</b>	すべての Cisco TrustSec カウンタをクリアする
<b>client</b> <i>mac-addr</i>	xx:xx:xx:xx:xx:xx フォーマットで指定されたクライアントの MAC アドレスに関する Cisco TrustSec カウンタをクリアする
<b>from</b>	フィルタリングされるトラフィックの送信元グループ タグを指定する
<i>sgt</i>	セキュリティ グループ タグ (SGT)。有効な値は 0 ~ 65535
<b>to</b>	フィルタリングされるトラフィックの宛先グループ タグを指定する
<i>dgt</i>	宛先グループ タグ (DGT)。有効な値は 0 ~ 65535

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、Cisco TrustSec Security カウンタのすべての統計情報をクリアする例を示します。

```
cisco-wave2-ap# clear cts role-based counters all
```

# clear datapath

データパス カウンタ、またはドロップをクリアするには、**clear datapath** コマンドを使用します。

**clear datapath {drops | statistics}**

構文の説明	<b>drops</b> データパス ドロップ カウンタをクリアする
	<b>statistics</b> データパス カウンタをクリアする
コマンド モード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

次に、データパス ドロップ カウンタをクリアする例を示します。

```
cisco-wave2-ap# clear datapath drops
```

# clear dot11

802.11 の設定をクリアするには、**clear dot11** コマンドを使用します。

## clear dot11 sensor

構文の説明	<b>sensor</b> センサーの設定をクリアして再起動する
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

次に、802.11 の設定をクリアする例を示します。

```
cisco-wave2-ap# clear dot11 sensor
```

# clear logging

ロギングの詳細をクリアするには、**clear logging** コマンドを使用します。

**clear logging** [**capwap** | **message** | **warning**]

構文の説明	<b>capwap</b> (任意) CAPWAP ロギングの詳細をクリアする
	<b>message</b> (任意) メッセージ ロギングの詳細をクリアする
	<b>warning</b> (任意) 警告ロギングの詳細をクリアする

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、CAPWAP ロギングの詳細をクリアする例を示します。

```
cisco-wave2-ap# clear logging capwap
```





## config コマンド

---

- [config ap client-trace](#) (28 ページ)
- [config ap client-trace filter](#) (30 ページ)
- [config ap client-trace output](#) (31 ページ)
- [config boot baudrate](#) (32 ページ)
- [config boot break](#) (33 ページ)
- [config boot crashkernel](#) (34 ページ)
- [config boot debug-memory](#) (35 ページ)
- [config boot manual](#) (36 ページ)
- [config boot path](#) (37 ページ)
- [config cts debug enforcement host\\_ip](#) (38 ページ)
- [config cts debug enforcement rate](#) (39 ページ)
- [config cts debug enforcement permissions](#) (40 ページ)
- [config cts debug enforcement protocol](#) (41 ページ)

## config ap client-trace

アクセスポイントにクライアントトレースを設定するには、**configapclient-trace** コマンドを使用します。

```
config ap client-trace {address {add|clear-all|delete}|all-clients {enable|disable}|filter {all
{enable|disable}|arp {enable|disable}|assoc {enable|disable}|auth {enable|disable}|dhcp
{enable|disable}|eap {enable|disable}|icmp {enable|disable}|ndp {enable|disable}|probe
{enable|disable}}|inline-mon {enable|disable}|output console-log|start|stop}
```

### 構文の説明

<b>addresses</b>	トレースするクライアントを設定する。クライアントのMACアドレスを指定する
<b>add</b>	トレースするクライアントを指定する
<b>clear-all</b>	このアクセスポイント上のすべてのクライアントトレースを削除する
<b>delete</b>	トレースするように設定されているクライアントのアドレスを削除する。クライアントのMACアドレスを使う
<b>all-clients</b>	すべてのクライアントをトレースする
<b>enable</b>	すべてのクライアントのトレースを有効にする
<b>disable</b>	すべてのクライアントのトレースを無効にする
<b>filter</b>	クライアントトレースのためのフィルタを設定する
<b>all</b>	すべてのフィルタをトレースする
<b>arp</b>	ARP パケットをトレースする このフィルタを有効、または無効にするには、 <b>enable</b> または <b>disable</b> キーワードを使用する。
<b>assoc</b>	ASSOC パケットをトレースする
<b>auth</b>	auth パケットをトレースする
<b>dhcp</b>	DHCP パケットをトレースする
<b>eap</b>	EAP パケットをトレースする
<b>icmp</b>	ICMP パケットをトレースする
<b>ndp</b>	NDP パケットをトレースする
<b>probe</b>	プローブ パケットをトレースする
<b>inline-mon</b>	インライン モニタリングを有効または無効にする



---

**output** コンソールまたはログファイルへのロギングを有効または無効にする

---

*console-log* コンソール ログのキーワードを指定する

---

**start** クライアントのトレースを開始する

---

**stop** クライアント トラッキングを停止する

---

---

コマンドモード Privileged EXEC (#)

---

コマンド履歴 リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、AP でクライアント トレースを開始する例を示します。

```
cisco-wave2-ap# config ap client-trace start
```

## config ap client-trace filter

クライアントトレースのフィルタを設定するには、**configapclient-tracefilter** コマンドを使用します。

```
config ap client-trace filter {all[disable | enable] | arp[disable | enable] | assoc[disable | enable] | auth[disable | enable] | dhcp[disable | enable] | eap[disable | enable] | icmp[disable | enable] | ndp[disable | enable] | probe[disable | enable]}
```

### 構文の説明

**all** すべてのフィルタをトレースする

**arp** ARP パケットをトレースする

**assoc** ASSOC パケットをトレースする

**auth** auth パケットをトレースする

**dhcp** DHCP パケットをトレースする

**eap** EAP パケットをトレースする

**icmp** ICMP パケットをトレースする

**ndp** NDP パケットをトレースする

**probe** プロブ パケットをトレースする

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

クライアントトレースのフィルタを設定するには、次のコマンドを使用します。

```
cisco-wave2-ap# config ap client-trace filter
```

## config ap client-trace output

トレースの出力を設定するには、**configapclient-traceoutput** コマンドを使用します。

```
config ap client-trace output console-log {disable | enable}
```

### 構文の説明

**console-log** トレースの出力をコンソールとログに表示する

**disable** コンソールとログへのトレースの出力を無効にする

**enable** コンソールとログへのトレースの出力を有効にする

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、トレースの出力を設定する例を示します。

```
cisco-wave2-ap# config ap client-trace output
```

## config boot baudrate

ボー レートを設定するには、**config boot baudrate** コマンドを使用します。

**config boot baudrate** {115200 | 9600}

構文の説明	<p><i>115200</i> ボー レートを 115200 に設定する</p> <p><i>9600</i> ボー レートを 9600 に設定する</p>
コマンドモード	Privileged EXEC (#)
コマンド履歴	<p>リリー 変更内容</p> <p>ス</p> <p>8.1.111.0 このコマンドが導入されました。</p>

### 例

次に、ボー レートを 9600 に設定する例を示します。

```
cisco-wave2-ap# config boot baudrate 9600
```

## config boot break

ブレイクを有効にするには、**config boot break** コマンドを使用します。

**config boot break** {**enable** | **disable**}

---

### 構文の説明

---

**enable** ブートブレイクを有効にする

---

**disable** ブートブレイクを無効にする

---

---

### コマンドモード

Privileged EXEC (#)

---

### コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、ブートブレイクを有効にする例を示します。

```
cisco-wave2-ap# config boot break enable
```

# config boot crashkernel

カーネルクラッシュを有効または無効にするには、**config boot crashkernel** コマンドを使用します。

**config boot crashkernel** {enable | disable}

構文の説明	<p><b>enable</b> カーネルクラッシュを有効にする</p> <p><b>disable</b> カーネルクラッシュを無効にする</p>
コマンドモード	Privileged EXEC (#)
コマンド履歴	<p>リリース 変更内容</p> <p>8.1.111.0 このコマンドが導入されました。</p>

## 例

次に、カーネルクラッシュを有効にする例を示します。

```
cisco-wave2-ap# config boot crashkernel enable
```

## config boot debug-memory

メモリ デバッグを有効にするには、**config boot debug-memory** コマンドを使用します。

**config boot debug-memory** {enable |disable}

構文の説明	<b>enable</b> メモリ デバッグを有効にする
	<b>disable</b> メモリ デバッグを無効にする
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 ス 8.1.111.0 このコマンドが導入されました。

次に、メモリ デバッグを有効にする例を示します。

```
cisco-wave2-ap# config boot debug-memory enable
```

# config boot manual

AP のマニュアルブートを有効にするには、**config boot manual** コマンドを使用します。

**config boot manual** {**enable** | **disable**}

## 構文の説明

**enable** マニュアルブートを有効にする

**disable** マニュアルブートを無効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、マニュアルブートを有効にする例を示します。

```
cisco-wave2-ap# config boot manual enable
```



## config boot path

ブートパスを設定するには、**config boot path** コマンドを使用します。

**config boot path** {1 | 2}

構文の説明	{1 2} パート1またはパート2として指定するパス
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 ス 8.1.111.0 このコマンドが導入されました。

### 例

次に、ブートパスを1に設定する例を示します。

```
cisco-wave2-ap# config boot path 1
```

## config cts debug enforcement host\_ip

ホスト IP に基づいて SGACL 強制デバッグをフィルタリングするには、**config cts debug enforcement host\_ip** コマンドを使用します。

**config cts debug enforcement host\_ip** {**ipv4** *dst-ip* [*src-ip*] | **ipv6** *dst-ip* [*src-ip*] }

構文の説明	<b>ipv4</b> <i>dst-ip</i> [ <i>src-ip</i> ]	宛先 IP アドレス、またはオプションで送信元 IP アドレスに基づいた、IPv4 SGACL 強制デバッグのみを表示する
	<b>ipv6</b> <i>dst-ip</i> [ <i>src-ip</i> ]	宛先 IP アドレス、またはオプションで送信元 IP アドレスに基づいた、IPv6 SGACL 強制デバッグのみを表示する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、ホスト IP に基づいて IPv4 SGACL 強制デバッグをフィルタリングする例を示します。

```
cisco-wave2-ap# config cts debug enforcement host_ip ipv4 209.165.200.224 209.165.200.227
```

## config cts debug enforcement rate

デバッグ ログの出力レートを設定するには、**config cts debug enforcement rate** コマンドを使用します。

**config cts debug enforcement rate** {*X Y*}

コマンドモード	Privileged EXEC (#)
構文の説明	<p><b>rate</b> デバッグ ログの出力レートを設定する</p> <p><i>X</i> 処理した <i>Y</i> 個の пакеттごとにデバッグを表示する пакеттの数。有効な範囲は 0 ~ 10000</p> <p><i>Y</i> 処理する пакеттの数。有効な範囲は 0 ~ 10000</p>
コマンド履歴	<p>リリース 変更内容</p> <p>8.1.111.0 このコマンドが導入されました。</p>

### 例

次に、処理される 500 パケットごとに 100 パケットのデバッグを表示するなど、デバッグ ログの出力レートの設定例を示します。

```
cisco-wave2-ap# config cts debug enforcement rate 100 500
```

## config cts debug enforcement permissions

送信元グループタグ (SGT) および宛先グループタグ (DGT) に基づいて SGACL 強制デバッグをフィルタリングするには、**configctsdebugenforcementpermissions** コマンドを使用します。

```
config cts debug enforcement permissions {dgt | sgt} tag-id
```

### 構文の説明

**dgt** 宛先グループ タグ

**sgt** 送信元グループ タグ

*tag-id* タグ識別子。有効な値は0～65535

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、ID が 600 の宛先グループ タグに基づいて、SGACL 強制デバッグをフィルタリングする例を示します。

```
cisco-wave2-ap# config cts debug enforcement permissions dgt 600
```

# config cts debug enforcement protocol

プロトコルに基づいて SGACL 強制デバッグをフィルタリングするには、**configctsdebugenforcementprotocol** コマンドを使用します。

```
config cts debug enforcement protocol {protocol-id | icmp | tcp | udp}
```

## 構文の説明

*protocol-id* プロトコル ID。有効な値は 0 ～ 65535

**icmp** ICMP トラフィックで SGACL 強制デバッグをフィルタリングする

**tcp** TCP トラフィックで SGACL 強制デバッグをフィルタリングする

**udp** UDP トラフィックで SGACL 強制デバッグをフィルタリングする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、UDP トラフィックのプロトコルに基づいて SGACL 強制デバッグをフィルタリングする例を示します。

```
cisco-wave2-ap# config cts debug enforcement protocol udp
```





## debug コマンド

---

- [debug arp \(45 ページ\)](#)
- [debug ble \(46 ページ\)](#)
- [debug capwap client \(47 ページ\)](#)
- [debug capwap client avc \(48 ページ\)](#)
- [debug cdp \(49 ページ\)](#)
- [debug cleanair \(50 ページ\)](#)
- [debug dhcp \(51 ページ\)](#)
- [debug dot11 \(52 ページ\)](#)
- [debug dot11 client datapath \(53 ページ\)](#)
- [debug dot11 client level \(54 ページ\)](#)
- [debug dot11 driver slot \(55 ページ\)](#)
- [debug dot11 sensor \(56 ページ\)](#)
- [debug dtls client \(57 ページ\)](#)
- [debug ethernet \(58 ページ\)](#)
- [debug flexconnect \(59 ページ\)](#)
- [debug lldp \(60 ページ\)](#)
- [debug memory \(61 ページ\)](#)
- [debug memory pool \(62 ページ\)](#)
- [debug memory pool alloc \(63 ページ\)](#)
- [debug memory pool free \(64 ページ\)](#)
- [debug mesh \(65 ページ\)](#)
- [debug mesh adjacency \(66 ページ\)](#)
- [debug mesh path-control \(67 ページ\)](#)
- [debug rrm neighbor \(68 ページ\)](#)
- [debug rrm reports \(69 ページ\)](#)
- [debug sip \(70 ページ\)](#)
- [debug wips \(71 ページ\)](#)
- [debug authentication interface \(72 ページ\)](#)
- [debug process memory \(73 ページ\)](#)

- [debug traffic](#) (74 ページ)
- [debug tunnel](#) (75 ページ)
- [debug client trace](#) (76 ページ)
- [no](#) (77 ページ)
- [traceroute](#) (78 ページ)
- [undebug](#) (79 ページ)



# debug arp

ARP のデバッグを有効にするには、**debug arp** コマンドを使用します。

**debug arp** {**errors** | **events** | **packets**}

## 構文の説明

**errors** ARP エラーのデバッグを有効にする

**events** ARP イベントのデバッグを有効にする

**packets** ARP Tx および Rx パケットのデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、ARP エラーのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug arp errors
```

# debug ble

Bluetooth Low Energy (BLE) のデバッグを有効にするには、**debug ble** コマンドを使用します。

**debug ble** {critical |error |events |fastpath {rssi |scan |sync} |receive |transmit}

## 構文の説明

<b>critical</b>	BLE クリティカル イベントのデバッグを有効にする
<b>error</b>	BLE エラー イベントのデバッグを有効にする
<b>events</b>	BLE イベントのデバッグを有効にする
<b>fastpath</b> {rssi   scan   sync}	CMX にエクスポートされたデータを表示する。次のオプションを使用できます。 <ul style="list-style-type: none"> <li>• RSSI データ</li> <li>• スキャンデータ</li> <li>• 同期データ</li> </ul>
<b>receive</b>	BLE 無線から受信した BLE パケットのデバッグを有効にする
<b>transmit</b>	BLE 無線に送信された BLE パケットのデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー ス	変更内容
8.7	このコマンドが導入されました。

## 例

次に、BLE クリティカル イベントのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug ble critical
```

## debug capwap client

CAPWAP クライアントのデバッグを有効にするには、**debug capwap client** コマンドを使用します。

**debug capwap client** { **ble** | **detail** | **efficient-upgrade** | **error** | **events** | **flexconnect** | **info** | **keepalive** | **payload** | **pmtu** | **qos** | **reassembly** | **security** }

構文の説明	
<b>ble</b>	CAPWAP BLE 詳細のデバッグを有効する
<b>detail</b>	CAPWAP 詳細のデバッグを有効する
<b>efficient-upgrade</b>	イメージのプレダウロードのデバッグを有効にする
<b>error</b>	CAPWAP エラーのデバッグを有効にする
<b>events</b>	CAPWAP のイベントのデバッグを有効にする
<b>flexconnect</b>	CAPWAP FlexConnect モードのイベントのデバッグを有効にする
<b>info</b>	CAPWAP の情報のデバッグを有効にする
<b>keepalive</b>	CAPWAP のキープアライブのデバッグを有効にする
<b>payload</b>	CAPWAP ペイロードのデバッグを有効にする
<b>pmtu</b>	CAPWAP パス MTU のデバッグを有効にする
<b>qos</b>	CAPWAP QoS のデバッグを有効にする
<b>reassembly</b>	CAPWAP リアセンブルのデバッグを有効にする
<b>security</b>	CAPWAP セキュリティのデバッグを有効にする

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容

8.1.111.0 このコマンドが導入されました。

### 例

次に、CAPWAP クライアントの詳細のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug capwap client detail
```

## debug capwap client avc

CAPWAP クライアント AVC のデバッグを有効にするには、**debug capwap client avc** コマンドを使用します。

**debug capwap client avc** {all | detail | error | event | info | netflow {all | detail | error | event | packet} | numflows}

構文の説明	all	すべての CAPWAP クライアントの AVC のデバッグを有効にする
	<b>detail</b>	CAPWAP AVC 詳細のデバッグを有効にする
	<b>error</b>	CAPWAP AVC エラーのデバッグを有効にする
	<b>event</b>	CAPWAP AVC のイベントのデバッグを有効にする
	<b>info</b>	CAPWAP AVC の情報のデバッグを有効にする
	<b>netflow</b>	CAPWAP クライアントの AVC NetFlow のデバッグを有効にする
	<b>netflow all</b>	すべての CAPWAP クライアントの AVC NetFlow のデバッグを有効にする
	<b>netflow detail</b>	CAPWAP クライアントの AVC NetFlow 詳細のデバッグを有効にする
	<b>netflow error</b>	CAPWAP クライアントの AVC NetFlow エラーのデバッグを有効にする
	<b>netflow event</b>	CAPWAP クライアントの AVC NetFlow イベントのデバッグを有効にする
	<b>netflow packet</b>	CAPWAP クライアントの AVC NetFlow パケットのデバッグを有効にする
	<b>numflows</b>	CAPWAP クライアント AVC numflows のデバッグを有効にする

コマンドモード Privileged EXEC (#)

コマンド履歴 リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、すべての CAPWAP クライアント AVC のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug capwap client avc all
```

## debug cdp

Controller Discovery Protocol (CDP) のデバッグを有効にするには、**debug cdp** コマンドを使用します。

**debug cdp** {**adjacency** | **events** | **ilp** | **packets**}

### 構文の説明

**adjacency** CDP ネイバーのデバッグを有効にする

**events** CDP イベントのデバッグを有効にする

**ilp** インラインパワーのデバッグを有効にする

**packets** CDP パケットのデバッグを有効にする

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、CDP イベントのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug cdp events
```

# debug cleanair

CleanAir のデバッグを設定するには、**debug cleanair** コマンドを使用します。

```
debug cleanair {bringup | event | logdebuglow | major | nsi | offchan {0 | 1}}
```

## 構文の説明

<b>bringup</b>	CleanAir ポートまたは起動のデバッグを有効にする
<b>events</b>	通常の CleanAir イベントのデバッグを有効にする
<b>logdebug</b>	CleanAir のデバッグ出力をログファイルに記録する
<b>low</b>	一部のメッセージの 16 進ダンプのデバッグを有効にする
<b>major</b>	主要な CleanAir イベントのデバッグを有効にする
<b>nsi</b>	NSI メッセージのデバッグを有効にする
<b>offchan 0   1</b>	CleanAir MSMT 要求のデバッグを有効にする。無線スロットを 0 または 1 で指定する必要がある

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、主要な CleanAir イベントのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug cleanair major
```

# debug dhcp

DHCP のデバッグを設定するには、**debug dhcp** コマンドを使用します。

**debug dhcp {errors | events | packets}**

## 構文の説明

**errors** DHCP エラーのデバッグを有効にする

**events** DHCP イベントのデバッグを有効にする

**packets** DHCP パケットのデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、DHCP エラーのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dhcp errors
```

# debug dot11

802.11 のデバッグを有効にするには、**debug dot11** コマンドを使用します。

**debug dot11** {**critical** | **errors** | **events** | **info**}

## 構文の説明

**critical** 802.11 のクリティカル レベルのデバッグを有効にする

**errors** 802.11 のエラー レベルのデバッグを有効にする

**events** 802.11 のイベント レベルのデバッグを有効にする

**info** 802.11 の情報レベルのデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、802.11 のエラー レベルのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 errors
```



## debug dot11 client datapath

802.11 クライアント データパスのデバッグを有効にするには、**debug dot11 client datapath** コマンドを使用します。

```
debug dot11 client datapath {{arp | dhcp | eapol} {addr {mac-addr1 | mac-addr2 | mac-addr3 | mac-addr4} | all}} | dns-acl}
```

構文の説明	<b>arp</b>	クライアント データパスの ARP デバッグを有効にする
	<b>dhcp</b>	クライアント データパスの DHCP デバッグを有効にする
	<b>eapol</b>	クライアント データパスの EAPOL デバッグを有効にする
	{ <b>addr</b>   <b>all</b> }	特定のクライアントまたはすべてのクライアントの MAC アドレスを指定するオプション
	{ <i>mac-addr1</i>   <i>mac-addr2</i>   <i>mac-addr3</i>   <i>mac-addr4</i> }	入力する必要があるクライアントの MAC アドレス
	<b>dns-acl</b>	クライアント データパスの DNS-ACL デバッグを有効にする
コマンドモード	Privileged EXEC (#)	
コマンド履歴	リリー	変更内容
	ス	
	8.1.111.0	このコマンドが導入されました。

### 例

次に、クライアント データパスの ARP のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 client datapath arp
```

## debug dot11 client level

802.11 クライアント デバッグ レベルを有効にするには、**debug dot11 client level** コマンドを使用します。

```
debug dot11 client level {critical | errors | events | info} {addr {mac-addr1 | mac-addr2
| mac-addr3 | mac-addr4} | all}
```

構文の説明	<b>critical</b>	クライアントのクリティカル レベルのデバッグを有効にする
	<b>errors</b>	クライアントのエラー レベルのデバッグを有効にする
	<b>events</b>	クライアントのイベント レベルのデバッグを有効にする
	<b>info</b>	クライアントの情報レベルのデバッグを有効にする
	<b>{addr   all}</b>	特定のクライアントまたはすべてのクライアントの MAC アドレスを指定するオプション
	<b>{mac-addr1   mac-addr2   mac-addr3   mac-addr4}</b>	入力する必要があるクライアントの MAC アドレス

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、イベント レベルですべてのクライアントのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 client level events all
```

# debug dot11 driver slot

802.11 ドライバのデバッグを有効にするには、**debug dot11 driver slot** コマンドを使用します。

```
debug dot11 driver slot {0 | 1} {all | {cac {info | metrics}} | chd | save-acnt-data
| save-on-failure [extended] | stop-on-failure | tsm | vim}
```

構文の説明	slot {0   1}	無線ごとの 802.11 ドライバのデバッグを有効にする
	all	すべての 802.11 ドライバのデバッグを有効にする
	cac	802.11 CAC デバッグを有効にする
	cac info	802.11 CAC の情報レベルのデバッグを有効にする
	cac metrics	802.11 CAC メトリックのデバッグを有効にする
	chd	802.11 CHD デバッグを有効にする
	save-acnt-data	無線アカウントリング データを保存する
	save-on-failure	無線の障害発生時に無線クラッシュ情報を保存する
	save-on-failure extended	無線障害に関する詳細情報を保存する
	stop-on-failure	無線障害時に AP の再起動を停止する
	tsm	802.11 トラフィック ストリーム メトリックのデバッグを有効にする
	vim	802.11 ビデオ メトリックのデバッグを有効にする

コマンドモード Privileged EXEC (#)

コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、情報レベルで CAC のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 driver slot cac info
```

## debug dot11 sensor

802.11 センサーのデバッグを有効にするには、**debug dot11 sensor** コマンドを使用します。

```
debug dot11 sensor {dns | file-transfer | mail-server | ping | radius | ssh | telnet | web-server}
```

### 構文の説明

<b>dns</b>	802.11 センサーの DNS のデバッグを有効にする
<b>file-transfer</b>	802.11 センサーのファイル転送のデバッグを有効にする
<b>mail-server</b>	802.11 センサーのメール サーバのデバッグを有効にする
<b>ping</b>	802.11 センサーの ping のデバッグを有効にする
<b>radius</b>	802.11 センサーの radius のデバッグを有効にする
<b>ssh</b>	802.11 センサーの SSH のデバッグを有効にする
<b>telnet</b>	802.11 センサーの Telnet のデバッグを有効にする
<b>web-server</b>	802.11 センサーの Web サーバのデバッグを有効にする

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース	変更内容
8.1.111.0	このコマンドが導入されました。

### 例

次に、802.11 センサー のファイル転送のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 sensor file-transfer
```

## debug dtls client

DTLS クライアントエラーとイベントのデバッグを設定するには、**debug dtls client** コマンドを使用します。

**debug dtls client** {**error** | **event** [**detail**] }

構文の説明	<b>error</b>	DTLS クライアント エラーのデバッグを設定する
	<b>event</b> [ <b>detail</b> ]	DTLS クライアント イベントのデバッグを設定する
コマンド モード	Privileged EXEC (#)	
コマンド履歴	リリー	変更内容
	8.1.111.0	このコマンドが導入されました。

### 例

次に、DTLS クライアント イベントのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dtls client event
```

# debug ethernet

イーサネットのデバッグを設定するには、**debug ethernet** コマンドを使用します。

**debug ethernet** *interface-number* {**both** | **rcv** | **xmt**}

## 構文の説明

*interface-number* インターフェイス番号で 0 または 1 を入力する必要があります

**both** 送信と受信の両方のデバッグを有効にする

**rcv** 受信のデバッグを有効にする

**xmt** 送信のデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、インターフェイス 0 の送信のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug ethernet 0 xmt
```

## debug flexconnect

FlexConnect 機能をデバッグするには、**debug flexconnect** コマンドを使用します。

```
debug flexconnect {acl | cckm | dot11r | event | multicast {igmp | traffic} | pmk | proxy-arp | vsa | wlan-vlan | wsastats}
```

### 構文の説明

<b>acl</b>	FlexConnect ACL のデバッグを設定する
<b>cckm</b>	CCKM のデバッグを設定する
<b>dot11r</b>	802.11r のデバッグを設定する
<b>event</b>	Wireless Control Protocol (WCP) イベントのデバッグを設定する
<b>multicast igmp</b>	マルチキャスト IGMP のデバッグを設定する
<b>multicast traffic</b>	マルチキャスト トラフィックのデバッグを設定する
<b>pmk</b>	Opportunistic Key Caching (OKC) またはペアワイズ マスター キー キャッシングのデバッグを設定する
<b>vsa</b>	AAA ベンダー固有属性 (VSA) のデバッグを設定する
<b>wlan-vlan</b>	WLAN-VLAN マッピングのデバッグを設定する
<b>wsastats</b>	RADIUS または DHCP ワイヤレス サービス保証の統計情報のデバッグを設定する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、FlexConnect ACL のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug flexconnect acl
```

# debug lldp

LLDP をデバッグするには、**debug lldp** コマンドを使用します。

**debug lldp** {**errors** | **events** | **packet**}

## 構文の説明

**errors** LLDP エラーをデバッグする

**events** LLDP イベントをデバッグする

**packet** LLDP パケットをデバッグする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、LLDP エラーのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug lldp errors
```



## debug memory

メモリをデバッグするには、**debug memory** コマンドを使用します。

**debug memory** {**clear** | **save**}

### 構文の説明

**clear** ブートアップ時にメモリのデバッグを削除する

**save** 現在のデバッグ レベルを保存し、次のブート時に適用する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、ブートアップ時にメモリ デバッグを削除する例を示します。

```
cisco-wave2-ap# debug memory clear
```

# debug memory pool

メモリ プールをデバッグするには、**debug memory pool** コマンドを使用します。

**debug memory pool** {**diff** | **realtime interval** *1-1000000-seconds* | **start**}

構文の説明	<b>diff</b>	メモリ プールのデバッグの差分を詳細に示す
	<b>realtime interval</b> <i>1 ~ 1000000</i>	メモリ プールのリアルタイムの間隔を設定する。 秒
	<b>start</b>	メモリ プールのデバッグを開始する

コマンドモード Privileged EXEC (#)

コマンド履歴	リリース 変更内容
	8.1.111.0 このコマンドが導入されました。

## 例

次に、メモリ プールにリアルタイムの間隔として 180 秒を設定する例を示します。

```
cisco-wave2-ap# debug memory pool realtime interval 180
```

## debug memory pool alloc

メモリ プールの割り当てコールをデバッグするには、**debug memory pool alloc** コマンドを使用します。

```
debug memory pool alloc {all | name pool-name} {diff | realtime interval 1-1000000-seconds | start}
```

構文の説明	all	すべてのメモリ プールの割り当てコールにデバッグを設定する
	<b>name</b> <i>pool-name</i>	特定のメモリ プールの割り当てコールにデバッグを設定する
	<b>diff</b>	メモリ プールのデバッグの割り当てコールの差分を詳細に示す
	<b>realtime interval</b> <i>1</i> ~ <i>1000000</i> 秒	メモリ プールの割り当てコールにリアルタイムの間隔を設定する
	<b>start</b>	メモリ プールの割り当てコールのデバッグを開始する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、すべてのメモリ プールの割り当てコールにデバッグの開始を設定する例を示します。

```
cisco-wave2-ap# debug memory pool alloc all start
```

## debug memory pool free

メモリ プールの解放コールをデバッグするには、**debug memory pool free** コマンドを使用します。

```
debug memory pool free {all | name pool-name} {diff | realtime interval 1-1000000-seconds | start}
```

構文の説明	all	すべてのメモリ プールの解放コールにデバッグを設定する
	<b>name</b> <i>pool-name</i>	特定のメモリ プールの解放コールにデバッグを設定する
	<b>diff</b>	メモリ プールのデバッグの解放コールの差分を詳細に示す
	<b>realtime interval</b> <i>1 ~ 1000000</i> 秒	メモリ プールの解放コールにリアルタイムの間隔を設定する
	<b>start</b>	メモリ プールの解放コールのデバッグを開始する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、すべてのメモリ プールの解放コールにデバッグの開始を設定する例を示します。

```
cisco-wave2-ap# debug memory pool free all start
```

## debug mesh

メッシュ ネットワークのデバッグを設定するには、**debug mesh** コマンドを使用します。

**debug mesh** {**channel** |**clear** |**convergence** |**events** |**forward-mcast** |**forward-packet** |**forward-table** |**linktest** |**path-control** |**port-control** |**security** |**trace**}

### 構文の説明

<b>channel</b>	メッシュ チャネルのデバッグを設定する
<b>clear</b>	すべてのメッシュ デバッグをリセットする
<b>convergence</b>	メッシュ コンバージェンスのデバッグを設定する
<b>events</b>	メッシュ イベントのデバッグを設定する
<b>forward-mcast</b>	メッシュ 転送マルチキャストのデバッグを設定する
<b>forward-packet</b>	メッシュ 転送パケットのデバッグを設定する
<b>forward-table</b>	メッシュ 転送テーブルのデバッグを設定する
<b>linktest</b>	メッシュ リンクテストのデバッグを設定する
<b>port-control</b>	メッシュ ポート制御のデバッグを設定する
<b>security</b>	メッシュ セキュリティのデバッグを設定する
<b>trace</b>	メッシュ トレースのデバッグを設定する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
 8.1.111.0 このコマンドが導入されました。

### 例

次に、メッシュ チャネルのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug mesh channel
```

# debug mesh adjacency

メッシュ隣接関係をデバッグするには、**debug mesh adjacency** コマンドを使用します。

**debug mesh adjacency** {**child** |**clear** |**dfs** |**message** |**packet** |**parent** }

## 構文の説明

<b>adjacency</b>	メッシュ隣接関係をデバッグする
<b>child</b>	メッシュ隣接関係の子をデバッグする
<b>clear</b>	メッシュ隣接関係のクリアをデバッグする
<b>dfs</b>	メッシュ DFS をデバッグする
<b>message</b>	メッシュ隣接関係のメッセージをデバッグする
<b>packet</b>	メッシュ隣接関係のパケットをデバッグする
<b>parent</b>	メッシュ隣接関係の親をデバッグする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、メッシュ隣接関係の親のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug mesh adjacency parent
```

## debug mesh path-control

メッシュパス制御のデバッグを設定するには、**debug mesh path-control** コマンドを使用します。

**debug mesh path-control** {**error** |**events** |**packets** }

### 構文の説明

**error** メッシュパス制御エラーのデバッグを設定する

**events** メッシュパス制御イベントのデバッグを設定する

**packets** メッシュパス制御パケットのデバッグを設定する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、メッシュパス制御エラーのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug mesh path-control error
```

## debug rrm neighbor

RRM ネイバーのデバッグを有効にするには、**debug rrm neighbor** コマンドを使用します。

```
debug rrm neighbor {tx | rx | detail }
```

### 構文の説明

**tx** RRM ネイバー Tx のデバッグを有効にする

**rx** RRM ネイバー Rx のデバッグを有効にする

**detail** RRM ネイバーの詳細のデバッグを有効にする

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、RRM ネイバーの送信のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug rrm neighbor tx
```



## debug rrm reports

RRM レポートのデバッグを有効にするには、**debug rrm reports** コマンドを使用します。

### debug rrm reports

構文の説明	<b>reports</b> RRM レポートのデバッグを有効にする
コマンド モード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

### 例

次に、RRM レポートのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug rrm reports
```

# debug sip

Session Initiation Protocol (SIP) のデバッグを有効にするには、**debug sip** コマンドを使用します。

**debug sip** {all | tx | rx}

## 構文の説明

**al** SIP の送信と受信のデバッグを有効にする

**tx** SIP の送信のデバッグを有効にする

**rx** SIP の受信のデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、SIP の送信と受信のデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug sip all
```

## debug wips

wIPS デバッグを有効にするには、**debug wips** コマンドを使用します。

**debug wips {errors | events | critical}**

---

### 構文の説明

---

**errors** wIPS エラー レベルのデバッグを有効にする

---

**events** wIPS イベント レベルのデバッグを有効にする

---

**critical** wIPS クリティカル レベルのデバッグを有効にする

---

---

### コマンドモード

Privileged EXEC (#)

---

### コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

### 例

次に、wIPS エラー レベルのデバッグ を有効にする例を示します。

```
cisco-wave2-ap# debug wips errors
```

# debug authentication interface

FlexConnect 無線インターフェイスのデバッグを有効にするには、**debug authentication interface** コマンドを使用します。

**debug authentication interface** *interface-name* { **all** | **dot11** | **dot1x** | **driver** | **others** | **radius** | **wpa** }

## 構文の説明

<i>interface-name</i>	デバッグするインターフェイスの名前
<b>all</b>	すべてのパーツのデバッグを有効にする
<b>dot11</b>	802.11 モジュールのデバッグを有効にする
<b>dot1x</b>	802.1x モジュールのデバッグを有効にする
<b>driver</b>	ドライバ モジュールのデバッグを有効にする
<b>others</b>	その他の非モジュール パーツのデバッグを有効にする
<b>radius</b>	RADIUS モジュールのデバッグを有効にする
<b>wpa</b>	WPA モジュールのデバッグを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー	変更内容
8.1.111.0	このコマンドが導入されました。

## 例

次に、WPA モジュールのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug authentication interface management wpa
```

## debug process memory

プロセス メモリをデバッグするには、**debug process memory** コマンドを使用します。

```
debug process memory {diff | realtime [interval interval-in-seconds] |start}
```

### 構文の説明

**diff** プロセス メモリのデバッグで差分を表示する

**realtime** プロセス メモリをリアルタイムにデバッグする

**interval** 更新間隔。有効な範囲は 1 ~ 1000000 秒

**start** プロセス メモリのデバッグを開始する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、プロセス メモリのデバッグの開始を有効にする例を示します。

```
cisco-wave2-ap# debug process memory start
```

# debug traffic

トラフィックのデバッグを有効にするには、**debug traffic** コマンドを使用します。

```
debug traffic {host {icmpv6 | ip | ipv6 | tcp | udp { verbose}} | wired {ip | tcp | udp {verbose}}}
```

## 構文の説明

**host** ホスト トラフィックのデバッグを有効にする

**wired** 有線トラフィックのデバッグを有効にする

**verbose** 詳細な出力を表示する

**icmpv6** ホスト ICMPv6 トラフィック ダンプを有効にする

**ip** ホスト IP トラフィック ダンプを有効にする

**ipv6** ホスト IPv6 トラフィック ダンプを有効にする

**tcp** TCP トラフィック ダンプを有効にする

**udp** UDP トラフィック ダンプを有効にする

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、ホスト IP トラフィック ダンプのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug traffic host ip
```

# debug tunnel

トンネルのデバッグを設定するには、**debug tunnel** コマンドを使用します。

## debug tunnel eogre

構文の説明	<b>eogre</b> EoGRE トンネルのデバッグを設定する
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

## 例

次に、EoGRE トンネルのデバッグを有効にする例を示します。

```
cisco-wave2-ap# debug tunnel eogre
```

## debug client trace

クライアント トレースのデバッグを有効にするには、**debug client trace** コマンドを使用します。

```
debug client trace {all |address mac-address |enable |filter {assoc | auth | dhcp | eap | icmp | mgmt
| probe | proto}}
```

構文の説明	
<b>all</b>	すべてのクライアント トレースを設定する
<b>address</b>	トレースするアドレスを設定する
<i>mac-address</i>	トレースする MAC アドレス
<b>enable</b>	トレースを有効にする
<b>filter</b>	トレース フィルタを設定する
<b>assoc</b>	関連付けパケットをトレースする
<b>auth</b>	認証パケットをトレースする
<b>dhcp</b>	DHCP パケットをトレースする
<b>eap</b>	EAP パケットをトレースする
<b>icmp</b>	ICMP パケットをトレースする
<b>mgmt</b>	probe、assoc、auth、EAP パケットをトレースする
<b>probe</b>	プローブ パケットをトレースする
<b>proto</b>	DHCP、ICMP パケットをトレースする

コマンド モード Privileged EXEC (#)

コマンド履歴

```
リリー 変更内容
ス
8.1.111.0 このコマンドが導入されました。
```

### 例

次に、すべてのクライアントのトレースを有効にする例を示します。

```
cisco-wave2-ap# debug client trace all
```



## no

コマンドを無効にするか、デフォルトに設定するには、**no** コマンドを使用します。

**no**

---

コマンドモード

Privileged EXEC (#)

---

コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

コマンドを無効にするか、デフォルトに設定するには、次のコマンドを使用します。

```
cisco-wave2-ap# no debug
```

## tracert

ネットワーク内を移動するパケットのルートを表示するには、**tracert** コマンドを使用します。

**tracert** *destination-address*

構文の説明	<i>destination-address</i> パケットの宛先の IP アドレス
-------	---

コマンドモード	Privileged EXEC (#)
---------	---------------------

コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。
--------	---------------------------------------

### 例

次に、ネットワーク内を移動する、指定した宛先 IP アドレスを持つパケットのルートを表示する例を示します。

```
cisco-wave2-ap# tracert 209.165.200.224
```

# undebug

アクセス ポイントでデバッグを無効にするには、**undebug** コマンドを使用します。

## undebug [all]

構文の説明	■ すべてのデバッグ メッセージを無効にする
コマンド モード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 8.1.111.0 このコマンドが導入されました。

## 例

次に、すべてのデバッグ メッセージを無効にする例を示します。

```
cisco-wave2-ap# undebug all
```





## show コマンド

---

- [show ap client-trace status](#) (83 ページ)
- [show arp](#) (84 ページ)
- [show avc cft](#) (85 ページ)
- [show avc nbar](#) (86 ページ)
- [show avc netflow flows](#) (87 ページ)
- [show avc status](#) (88 ページ)
- [show boot](#) (89 ページ)
- [show capwap](#) (90 ページ)
- [show capwap client](#) (91 ページ)
- [show capwap client trace](#) (92 ページ)
- [show capwap ids sig](#) (93 ページ)
- [show cdp](#) (94 ページ)
- [show class-map](#) (95 ページ)
- [show cleanair debug](#) (96 ページ)
- [show client statistics](#) (97 ページ)
- [show clock](#) (98 ページ)
- [show configuration](#) (99 ページ)
- [show controller ble](#) (100 ページ)
- [show controllers dot11Radio](#) (102 ページ)
- [show controllers nss status](#) (103 ページ)
- [show controllers wired](#) (104 ページ)
- [show crypto](#) (105 ページ)
- [show debug](#) (106 ページ)
- [show dhcp](#) (107 ページ)
- [show dot11 qos](#) (108 ページ)
- [show filesystems](#) (109 ページ)
- [show flash](#) (110 ページ)
- [show flexconnect](#) (111 ページ)
- [show flexconnect ocap firewall](#) (112 ページ)

- [show flexconnect wlan](#) (113 ページ)
- [show interfaces dot11Radio](#) (114 ページ)
- [show interfaces network](#) (115 ページ)
- [show interfaces wired](#) (116 ページ)
- [show inventory](#) (117 ページ)
- [show ip](#) (118 ページ)
- [show lacp](#) (119 ページ)
- [show logging](#) (120 ページ)
- [show memory](#) (121 ページ)
- [show policy-map](#) (123 ページ)
- [show processes](#) (124 ページ)
- [show processes memory](#) (125 ページ)
- [show rrm](#) (127 ページ)
- [show rrm rogue containment](#) (128 ページ)
- [show rrm rogue detection](#) (129 ページ)
- [show running-config](#) (131 ページ)
- [show security data-corruption](#) (133 ページ)
- [show security system state](#) (134 ページ)
- [show spectrum](#) (136 ページ)
- [show tech-support](#) (137 ページ)
- [show version](#) (138 ページ)
- [show trace dot11\\_chn](#) (139 ページ)
- [show trace](#) (140 ページ)
- [show wips](#) (141 ページ)

## show ap client-trace status

AP クライアント トレースの詳細を表示するには、**showapclient-tracestatus** コマンドを使用します。

```
show ap client-trace { events { all | mac word | system } | skb { drop-list | stats } | status }
```

### 構文の説明

<b>events</b>	クライアント トレース イベント情報を表示する
<b>all</b>	すべてのクライアント トレース イベントを表示する
<b>system</b>	すべてのシステム イベントを表示する
<b>mac</b>	特定の MAC アドレスのクライアント トレース イベントを表示する
<b>word</b>	特定のクライアントの MAC アドレス
<b>skb</b>	クライアント トレース SKB 情報を表示する
<b>drop-list</b>	クライアント トレース SKB ドロップ リスト情報を表示する
<b>stats</b>	クライアント トレース SKB 統計情報を表示する
<b>status</b>	クライアント トレース設定を表示する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、AP クライアント トレースのステータスを表示する例を示します。

```
cisco-wave2-ap# show ap client-trace status
```

# show arp

ARP テーブルを表示するには、**show arp** コマンドを使用します。

## show arp

### 構文の説明

**arp** ARP テーブルを表示する

### コマンドモード

User EXEC (>)  
Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、このコマンドの出力例を示します。

```
cisco-wave2-ap# show arp
Address Age (min)      Hardware Addr
 9.11.8.1           0 84:80:2D:A0:D2:E6
9.11.32.111        0 3C:77:E6:02:33:3F
```



## show avc cft

AVC クライアントフロー テーブル情報を表示するには、**show avc cft** コマンドを使用します。

**show avc cft** *word*

---

**構文の説明**

---

*word* Client MAC  
address

---

---

**コマンドモード**

---

User EXEC (>)  
Privileged EXEC (#)

---

---

**コマンド履歴**

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、AVC クライアントフロー テーブルを表示する例を示します。

```
cisco-wave2-ap# show avc cft 02:35:2E:03:E0:F2
```

## show avc nbar

AVC NBAR 情報を表示するには、**show avc nbar** コマンドを使用します。

**show avc nbar** {**statistics** |**build** |**version**}

### 構文の説明

**statistics** NBAR のビルドの詳細を表示する

**build** NBAR の統計情報を表示する

**version** NBAR および PP のバージョンを表示する

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、AVC NBAR のビルド情報を表示する例を示します。

```
cisco-wave2-ap# show avc nbar build
```

## show avc netflow flows

現在キャッシュされており、Cisco WLCに送られるすべてのフローのリストを表示するには、**show avc netflow flows** コマンドを使用します。

**show avc netflow flows {download |upload}**

### 構文の説明

**download** 現在キャッシュされているダウンロードフローのリストを表示する

**upload** 現在キャッシュされているアップロードフローのリストを表示する

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、現在キャッシュされているすべてのフローを表示する例を示します。

```
cisco-wave2-ap# show avc netflow flows
```

## show avc status

WLAN/VAP ごとの AVC プロビジョニング ステータスのリストを表示するには、**show avc status** コマンドを使用します。

### show avc status

コマンド モード

User EXEC (>)

Privileged EXEC (#)

コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、WLAN/VAP ごとの AVC プロビジョニング ステータスを表示する例を示します。

```
cisco-wave2-ap# show avc status
```

```
VAP FNF-STATUS AVC-QOS-STATUS
 0 Disabled Disabled
 1 Disabled Disabled
 2 Disabled Disabled
 3 Disabled Disabled
 4 Disabled Disabled
 5 Disabled Disabled
 6 Disabled Disabled
 7 Disabled Disabled
 8 Disabled Disabled
 9 Disabled Disabled
10 Disabled Disabled
11 Disabled Disabled
12 Disabled Disabled
13 Disabled Disabled
14 Disabled Disabled
15 Disabled Disabled
```

# show boot

ブート属性を表示するには、**show boot** コマンドを使用します。

## show boot

---

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

### コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、ブート属性を表示する例を示します。

```
cisco-wave2-ap# show boot

BOOT path-list:      part2
Console Baudrate:   9600
Enable Break:       yes
Manual Boot:        no
Memory Debug:       no
Crashkernel:
```

## show capwap

CAPWAP オプションを表示するには、**show capwap** コマンドを使用します。

```
show capwap [{ip |mcast |traffic}]
```

構文の説明	<b>client</b> CAPWAP クライアント情報
	<b>ids</b> CAPWAP ID 情報
	<b>ip</b> CAPWAP IP 設定
	<b>location</b> CAPWAP ロケーション情報
	<b>mcast</b> CAPWAP マルチキャスト情報
	<b>pnp</b> PNP 情報
	<b>traffic</b> CAPWAP トラフィック情報

コマンドモード	User EXEC (>) Privileged EXEC (#)
---------	--------------------------------------

コマンド履歴	リリー 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、CAPWAP マルチキャスト情報を表示する例を示します。

```
cisco-wave2-ap# show capwap mcast
```

## show capwap client

CAPWAP クライアント情報を表示するには、**show capwap client** コマンドを使用します。

```
show capwap client {callinfo info |detailrcb |rcb |config |ha |msginfo |timers |traffic}
```

### 構文の説明

<b>callinfo</b> <i>info</i>	CAPWAP クライアントのコール情報
<b>detailrcb</b>	CAPWAP クライアントの詳細な RCB 情報
<b>rcb</b>	CAPWAP クライアントの RCB 情報
<b>config</b>	CAPWAP クライアントの設定情報
<b>ha</b>	CAPWAP クライアントの HA パラメータ
<b>msginfo</b>	CAPWAP クライアントのメッセージ情報
<b>timers</b>	CAPWAP クライアントのタイマー
<b>traffic</b>	CAPWAP クライアントの 802.11 トラフィック情報

### コマンドモード

User EXEC (>)  
Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、CAPWAP クライアント トラフィック情報を表示する例を示します。

```
cisco-wave2-ap# show capwap client traffic
```

# show capwap client trace

CAPWAP トレースを表示するには、**show capwap client trace** コマンドを使用します。

**show capwap client trace** {clear |delete |disable |save |start |stop}

## 構文の説明

<b>clear</b>	トレースをクリアする
<b>delete</b>	トレースを削除する
<b>disable</b>	起動時にトレースを無効にする
<b>enable</b>	起動時にトレースを有効にする
<b>save</b>	トレースを保存する
<b>start</b>	トレースを開始する
<b>stop</b>	トレースを停止する

## コマンドモード

User EXEC (>)  
Privileged EXEC (#)

## コマンド履歴

リリー	変更内容
8.1.111.0	このコマンドが導入されました。

次に、CAPWAP クライアント トレースを表示する例を示します。

```
cisco-wave2-ap# show capwap client trace
```



## show capwap ids sig

CAPWAP ID シグネチャを表示するには、**show capwap ids sig** コマンドを使用します。

```
show capwap ids sig [{list |stats}]
```

### 構文の説明

**list** シグネチャ リストのエントリ

**stats** シグネチャ攻撃の統計情報

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、CAPWAP ID シグネチャの統計情報を表示する例を示します。

```
cisco-wave2-ap# show capwap ids sig stats
```

# show cdp

CDP オプションを表示するには、**show cdp** コマンドを使用します。

**show cdp** {**entry device** *device-name* |**inline\_power** |**interface** |**neighbors** |**traffic**}

構文の説明		
	<b>entry device</b> <i>device-name</i>	名前を入力する必要がある特定のネイバー エントリに関する情報
	<b>inline_power</b>	インライン電力ネゴシエーション情報
	<b>interface</b>	CDP インターフェイスのステータスと設定
	<b>neighbors</b>	CDP ネイバー エントリ
	<b>traffic</b>	CDP 統計情報

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、特定のネイバー エントリに関する情報を表示する例を示します。

```
cisco-wave2-ap# show cdp entry device mydevice
```

## show class-map

CPL クラス マップを表示するには、**show class-map** コマンドを使用します。

### show class-map

---

#### コマンド モード

User EXEC (>)

Privileged EXEC (#)

---

#### コマンド履歴

---

リリース	変更内容
------	------

---

8.1.111.0	このコマンドが導入されました。
-----------	-----------------

---

次に、CPL クラス マップを表示する例を示します。

```
cisco-wave2-ap# show class-map
```

## show cleanair debug

CleanAir のデバッグ設定を表示するには、**show cleanair debug** コマンドを使用します。

### show cleanair debug

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

次に、CleanAir のデバッグ設定を表示する例を示します。

```
cisco-wave2-ap# show cleanair debug
```

## show client statistics

クライアントの統計情報を表示するには、**show client statistics** コマンドを使用します。

**show client statistics** *client-mac-address*

---

構文の説明

---

*client-mac-address* クライアントの MAC アドレス

---

---

コマンドモード

---

Privileged EXEC (#)

---

コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、クライアントの統計情報を表示する例を示します。

```
cisco-wave2-ap# show client statistics 70:DB:98:66:34:FA
```

# show clock

システムクロックを表示するには、**show clock** コマンドを使用します。

## show clock

---

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

### コマンド履歴

---

リリース	変更内容
------	------

---

8.1.111.0	このコマンドが導入されました。
-----------	-----------------

---

次に、システムクロックを表示する例を示します。

```
cisco-wave2-ap# show clock
```

# show configuration

不揮発性メモリの内容を表示するには、**show configuration** コマンドを使用します。

## show configuration

---

コマンドモード	Privileged EXEC (#)
---------	---------------------

---

コマンド履歴	リリー 変更内容 ス
--------	---------------

---

8.1.111.0 このコマンドが導入されました。

---

次に、不揮発性メモリの内容を表示する例を示します。

```
cisco-wave2-ap# show configuration
```

## show controller ble

Bluetooth Low Energy 無線インターフェイス パラメータ情報を表示するには、**show controller ble** コマンドを使用します。

```
show controller ble ble-interface-number { {broadcast |counters |floor-tag floor-beacon-mac-addr
|interface |local |scan { brief |detail floor-beacon-mac-addr } |timers }
```

構文の説明		
	<i>ble-interface-number</i>	入力する必要がある BLE インターフェイス番号。有効な値は 0
	<b>broadcast</b>	BLE ブロードキャスト サマリー情報を表示する
	<b>counters</b>	BLE トランSPORT カウンタ情報を表示する
	<b>floor-tag</b> <i>floor-beacon-mac-addr</i>	指定する必要がある MAC アドレスを持つフロアビーコンの同期データを表示する
	<b>interface</b>	BLE インターフェイス サマリー情報を表示する
	<b>local</b>	ホスト BLE 無線の同期情報を表示する
	<b>scan brief</b>	簡単な BLE スキャン サマリー情報を表示する
	<b>scan detail</b> <i>floor-beacon-mac-addr</i>	詳細な BLE スキャン サマリー情報を表示する。フロアビーコンの MAC アドレスを指定する必要がある
	<b>timers</b>	BLE タイマー情報を表示する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.7 このコマンドが導入されました。

### 例

BLE タイマー情報を表示するには、次のコマンドを使用します。

```
cisco-wave2-ap# show controller ble 0 timers
```

```
Timers
-----
Scan timer status      : Running
Scan timer interval    : 10 secs
Scan started at       : 0D:00H:04M:28S ago
Last scan done at     : 0D:00H:00M:06S ago
```



スキャンが想定通りに行われている場合、「Last scan done at」の時間は必ず、設定されているスキャン間隔より短いか、同じです。

## show controllers dot11Radio

dot11 インターフェイス情報を表示するには、**show controllers dot11Radio** コマンドを使用します。

**show controllers dot11Radio** *dot11-interface-no* {**antenna** | **client** *client-mac-addr* | **frequency** | **powercfg** | **powerreg** | **radiostats** | **rate** | **vlan** | **wlan** *wlan-id*}

構文の説明	
<i>dot11-interface-no</i>	Dot11Radio インターフェイス番号
<b>antenna</b>	アンテナ設定を表示する
<b>client</b> <i>client-mac-addr</i>	MAC アドレスが指定されているクライアントの詳細を表示する
<b>frequency</b>	周波数情報を表示する
<b>powercfg</b>	設定されている電力情報を表示する
<b>powerreg</b>	送信電力情報を表示する
<b>radio-stats</b>	無線統計情報を表示する
<b>rate</b>	レート情報を表示する
<b>vlan</b>	VLAN サマリーを表示する
<b>wlan</b> <i>wlan-id</i>	指定された WLAN ID の VLAN/WLAN の詳細を表示する

コマンドモード  
User EXEC (>)  
Privileged EXEC (#)

コマンド履歴  
リリー 変更内容  
ス  
8.1.111.0 このコマンドが導入されました。

次に、インターフェイス番号 1 の 802.11 インターフェイス情報を表示する例を示します。

```
cisco-wave2-ap# show controllers dot11Radio 1
```

## show controllers nss status

NSS 情報を表示するには、**show controllers nss status** コマンドを使用します。

### show controllers nss status

---

#### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

#### コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、NSS 情報を表示する例を示します。

```
cisco-wave2-ap# show controllers nss status
```

# show controllers wired

有線インターフェイスを表示するには、**show controllers wired** コマンドを使用します。

**show controllers wired** *wired-interface-number*

構文の説明	<i>wired-interface-number</i> 有線インターフェイス番号 (0~3)
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 ス 8.1.111.0 このコマンドが導入されました。

次に、コントローラの有線インターフェイス (ID が 1) に関する情報を表示する例を示します。

```
cisco-wave2-ap# show controllers wired 1

wired1    Link encap:Ethernet  HWaddr C8:8B:6A:33:59  eMac Status: DOWN
          inet addr:9.11.8.104  Bcast:9.255.255.255  Mask:255.255.255.255
          DOWN BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          RX packets:38600 errors:0 dropped:1 overruns:0 frame:0
          TX packets:179018 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:80
          RX bytes:3812643 (3.6 MiB)  TX bytes:54721869 (52.1 MiB)

Gig Emacl Counters
-----
0 Good octets rx, 0 Bad octets rx, 0 Unicast frames rx,
0 Broadcast frames rx, 0 Multicast frames rx, 0 64 byte frames rx,
0 65_TO_127 byte frames, 0 128_TO_255 byte frames, 0 256_TO_511 byte frames,
0 512_TO_1023 byte frames, 0 1024_TO_MAX byte frames, 0 Good octets tx,
0 Unicast frames tx, 0 Multicast frames tx, 0 Broadcast frames tx,
0 Crc errors sent, 0 Flow control rx, 0 Flow control tx,
0 Rx fifo overrun, 0 Undersized rx, 0 Fragments rx,
0 Oversize rx, 0 Jabber rx, 0 Mac rx error,
0 Bad crc event, 0 Collision, 0 Late collision,
```

## show crypto

暗号化属性を表示するには、**show crypto** コマンドを使用します。

### show crypto

---

#### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

#### コマンド履歴

---

リリース	変更内容
------	------

---

8.1.111.0	このコマンドが導入されました。
-----------	-----------------

---

次に、暗号化属性を表示する例を示します。

```
cisco-wave2-ap# show crypto
```

## show debug

有効なデバッグを表示するには、**show debug** コマンドを使用します。

### show debug

---

#### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

#### コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、有効な状態のデバッグを表示する例を示します。

```
cisco-wave2-ap# show debug
```

# show dhcp

Dynamic Host Configuration Protocol (DHCP) のステータスを表示するには、**show dhcp** コマンドを使用します。

**show dhcp {lease | servers}**

---

## 構文の説明

---

**lease** サーバからリースされている DHCP アドレスを表示する

---

**servers** 既知の DHCP サーバを表示する

---

---

## コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

---

## コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、サーバからリースされている DHCP アドレスのステータスを表示する例を示します。

```
cisco-wave2-ap# show dhcp lease
```

## show dot11 qos

802.11 ネットワークの Quality of Service (QoS) パラメータを表示するには、**showdot11qos** コマンドを使用します。

### show dot11 qos

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、802.11 ネットワークの Quality of Service (QoS) パラメータを表示する例を示します。

```
cisco-wave2-ap# show dot11 qos
```



# show filesystems

ファイルシステム情報を表示するには、**show filesystems** コマンドを使用します。

## show filesystems

---

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

### コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、ファイルシステム情報を表示する例を示します。

```
cisco-wave2-ap# show filesystems
```

```
Filesystem      Size      Used Available Use% Mounted on  
/dev/ubivol/storage  57.5M    1.9M    52.6M    4% /storage
```

## show flash

フラッシュの内容を表示するには、**show flash** コマンドを使用します。

```
show flash [{cores [detail core-file-name ]|crash |syslogs}]
```

### 構文の説明

<b>cores</b>	フラッシュにあるコア ファイルを表示する
<b>detail</b>	コア ファイルの内容を表示する
<i>core-file-name</i>	コア ファイル名
<b>crash</b>	フラッシュにあるクラッシュ ファイルを表示する
<b>syslogs</b>	フラッシュにある syslog ファイルを表示する

### コマンドモード

User EXEC (>)  
Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、フラッシュにあるコア ファイルの詳細を表示する例を示します。

```
cisco-wave2-ap# show flash cores detail filename1
```

## show flexconnect

アクセス ポイントの FlexConnect 情報を表示するには、**show flexconnect** コマンドを使用します。

```
show flexconnect { calea | cckm | client [aaa-override | counter | priority] | dot11r
| mcast | oeap | pmk | status | vlan-acl | wlan }
```

構文の説明	
<b>calea</b>	CALEA 情報を表示する
<b>cckm</b>	CCKM キャッシュ エントリ情報を表示する
<b>client</b>	クライアント情報を表示する
<b>aaa-override</b>	AAA オーバーライドパラメータを指定する
<b>counter</b>	すべてのクライアントにカウンタを指定する
<b>priority</b>	クライアントの優先順位を指定する
<b>dot11r</b>	802.11r キャッシュ エントリ情報を表示する
<b>mcast</b>	マルチキャスト情報を表示する
<b>oeap</b>	FlexConnect OEAP 情報を表示する
<b>pmk</b>	OKC または PMK キャッシュ エントリ情報を表示する
<b>status</b>	スタンドアロン ステータスを表示する
<b>vlan-acl</b>	VLAN ACL マッピングを表示する
<b>wlan</b>	WLAN の設定を表示する

コマンドモード  
User EXEC (>)  
Privileged EXEC (#)

コマンド履歴  
リリー 変更内容  
ス  
8.1.111.0 このコマンドが導入されました。

次に、FlexConnect AP のクライアントに関する情報を表示する例を示します。

```
cisco-wave2-ap# show flexconnect client
```

# show flexconnect oep firewall

OEAP ファイアウォール情報を表示するには、**show flexconnect oep firewall** コマンドを使用します。

**show flexconnect oep firewall** [{dmz |filtering |forwarding}]

## 構文の説明

**dmz** OEAP ファイアウォールの DMZ 情報を表示する

**filtering** OEAP ファイアウォールのフィルタリング情報を表示する

**forwarding** OEAP ファイアウォールのポート フォワーディング情報を表示する

## コマンドモード

User EXEC (>)

Privileged EXEC (#)

## コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、OEAP ファイアウォールの DMZ 情報を表示する例を示します。

```
cisco-wave2-ap# show flexconnect oep firewall dmz
```

## show flexconnect wlan

FlexConnect AP モードの WLAN 設定を表示するには、**show flexconnect wlan** コマンドを使用します。

**show flexconnect wlan** [{**l2acl** | **qos** | **vlan**}]

### 構文の説明

**l2acl** WLAN のレイヤ 2 ACL マッピングを指定する

**qos** WLAN の QoS パラメータを指定する

**vlan** WLAN の VLAN マッピングを指定する

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、FlexConnect AP の WLAN レイヤ 2 ACL マッピングを表示する例を示します。

```
cisco-wave2-ap# show flexconnect wlan l2acl
```

## show interfaces dot11Radio

802.11 無線のインターフェイス ステータスと設定を表示するには、**show interfaces dot11Radio** コマンドを使用します。

```
show interfaces dot11Radio radio-interface-number { dfs | memory [memory-address length
| firmware] | mumimo wlan-number | sniffer | statistics | wlan wlan-id statistics}
```

### 構文の説明

*radio-interface-number* 802.11 無線のインターフェイス番号を指定する。有効な範囲は 0 ～ 1

**dfs** DFS 統計情報を表示する

**memory** ダンプ無線メモリを表示する

*memory-address* メモリ アドレスを指定する。有効な範囲は 0 ～ ffffffff

*length* 長さを指定する。有効な範囲は 0 ～ 64

**firmware** ファームウェアのログをダンプする

**mumimo** マルチユーザの MIMO 統計情報を表示する

*wlan-number* 有効な範囲が 0 ～ 15 の 802.11 固有の値

**sniffer** スニファ モードの統計情報を表示する

**statistics** 802.11 無線の統計情報を表示する

**wlan** *wlan-id* 指定した VLAN 情報を表示する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、802.11 インターフェイス（番号 1）の DFS 統計情報を表示する例を示します。

```
cisco-wave2-ap# show interfaces dot11Radio 1 dfs
```

```
DFS Data:
Radar Detected:          0
Inactive Radar Detected: 0
```

## show interfaces network

Linux ネットワーク インターフェイスを表示するには、**show interfaces network** コマンドを使用します。

### show interfaces network

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、Linux ネットワーク インターフェイスを表示する例を示します。

```
cisco-wave2-ap# show interfaces network
```

## show interfaces wired

有線インターフェイスを表示するには、**show interfaces wired** コマンドを使用します。

**show interfaces wired** *wired-interface-number*

構文の説明	<i>wired-interface-number</i> 有線インターフェイスの番号。有効な範囲は 0 ~ 3
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

次に、有線インターフェイス（番号 1）を表示する例を示します。

```
cisco-wave2-ap# show interfaces wired 1
```



# show inventory

物理インベントリを表示するには、**show inventory** コマンドを使用します。

## show inventory

---

### コマンドモード

User EXEC (>)

Privileged EXEC (#)

---

### コマンド履歴

---

リリース	変更内容
------	------

---

8.1.111.0	このコマンドが導入されました。
-----------	-----------------

---

次に、物理インベントリを表示する例を示します。

```
cisco-wave2-ap# show inventory
```

```
NAME: AP2800, DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point  
PID: AIR-AP2802I-D-K9 , VID: V01, SN: XXXXXXXXXXXX
```

# show ip

IP 情報を表示するには、**show ip** コマンドを使用します。

```
show ip {access-lists | interface brief | route | tunnel [eogre {domain | forwarding-table
| gateway} | fabric | summary]}
```

## 構文の説明

<b>access-lists</b>	IP アクセス リストを表示する
<b>interface</b>	IP インターフェイスのステータスおよび設定を表示する
<b>brief</b>	IP ステータスおよび設定の概要を表示する
<b>route</b>	IP ルーティング テーブルを表示する
<b>tunnel</b>	IP トンネル情報を表示する
<b>eogre</b>	EoGRE トンネル情報を表示する
<b>domain</b>	EoGRE トンネル ドメイン情報を表示する
<b>forwarding-table</b>	EoGRE トンネルのカプセル化およびカプセル化解除の情報を表示する
<b>gateway</b>	EoGRE トンネルのゲートウェイ情報を表示する
<b>fabric</b>	IP ファブリック トンネルの情報を表示する
<b>summary</b>	すべてのトンネルの情報を表示する

## コマンドモード

User EXEC (>)  
Privileged EXEC (#)

## コマンド履歴

```
リリー 変更内容
ス
8.1.111.0 このコマンドが導入されました。
```

次に、IP アクセス リストについての情報を表示する例を示します。

```
cisco-wave2-ap# show ip access-lists
```

# show lacp

Link Aggregation Control Protocol (LACP) オプションを表示するには、**show lacp** コマンドを使用します。

**show lacp {counters [internal |neighbors]}**

---

## 構文の説明

---

**counters** トラフィック情報を表示する

---

**internal** 内部情報を表示する

---

**neighbors** LACP ネイバー エントリを表示する

---

---

## コマンドモード

Privileged EXEC (#)

---

## コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、LACP トラフィック情報を表示する例を示します。

```
cisco-wave2-ap# show lacp counters
```

# show logging

ロギング バッファの内容を表示するには、**show logging** コマンドを使用します。

## show logging

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、ロギング バッファの内容を表示する例を示します。

```
cisco-wave2-ap# show logging
```

# show memory

アクセスポイントのメモリ使用量を表示するには、**show memory** コマンドを使用します。

**show memory** [{detail |pool |summary}]

構文の説明	<b>detail</b> 詳細なシステムのメモリ使用量を表示する
	<b>pool</b> システムのメモリ プールを表示する
	<b>summary</b> システムのメモリ使用量の統計情報を表示する
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス 8.1.111.0 このコマンドが導入されました。

次に、システムのメモリ使用量の統計情報を表示する例を示します。

```
cisco-wave2-ap# show memory
Memory summary:
MemTotal:      1030608 kB
MemFree:       713832 kB
MemAvailable:  710492 kB
Buffers:       0 kB
Cached:        88224 kB
SwapCached:    0 kB
Active:        28932 kB
Inactive:      82872 kB
Active(anon):  28900 kB
Inactive(anon): 82812 kB
Active(file):  32 kB
Inactive(file): 60 kB
Unevictable:   0 kB
Mlocked:      0 kB
SwapTotal:     0 kB
SwapFree:      0 kB
Dirty:         0 kB
Writeback:     0 kB
AnonPages:    23580 kB
Mapped:       11380 kB
Shmem:        88132 kB
Slab:         132140 kB
SReclaimable: 3368 kB
SUnreclaim:   128772 kB
KernelStack:  864 kB
PageTables:   748 kB
NFS_Unstable: 0 kB
Bounce:       0 kB
WritebackTmp: 0 kB
CommitLimit:  515304 kB
Committed_AS: 193960 kB
```

## show memory

```
VmallocTotal: 1024000 kB
VmallocUsed: 69808 kB
VmallocChunk: 915324 kB
```

## System Memory:

	total	used	free	shared	buffers
Mem:	1030608	316848	713760	0	0
-/+ buffers:		316848	713760		
Swap:	0	0	0		

# show policy-map

アクセス ポイント上のポリシー マップを表示するには、**show policy-map** コマンドを使用します。

## show policy-map

コマンド モード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

次に、アクセス ポイント上のポリシー マップを表示する例を示します。

```
cisco-wave2-apshow policy-map
```

# show processes

プロセス使用率の詳細を表示するには、**show processes** コマンドを使用します。

**showprocesses** {*cpu* *cpu-number* | **dmalloc** {*capwap* | *wcp*} | **status**}

構文の説明	<b>cpu</b> <i>cpu-number</i>	プロセスの指定された CPU の使用率を表示する。CPU 番号の値の有効な範囲は 0 ~ 3
	<b>dmalloc</b>	dmalloc プロセスのプロセス使用率を表示する
	<b>capwap</b>	CAPWAP の dmalloc 統計情報を表示する
	<b>wcp</b>	WCP の dmalloc 統計情報を表示する
	<b>status</b>	watchdog プロセスのステータスを表示する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、**watchdog** プロセスのステータスを表示する例を示します。

```
cisco-wave2-ap# show processes status
      Process           Alive           Monitored
      capwapd           True            True
      switchdrvr       True            False
      wcpd              True            True
      kclick            True            True
      cleanaird         True            True
      mrvlfwd           True            True
```



## show processes memory

アクセスポイント上のプロセスを表示するには、**show processes memory** コマンドを使用します。

**show processes memory** {maps|smaps} pid pid-number

構文の説明	<b>maps</b>	プロセスのマップを表示する
	<b>smaps</b>	プロセスの smaps を表示する
	<b>pid</b> <i>pid-number</i>	指定する必要があるプロセス ID

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、アクセスポイント上のメモリを利用するプロセスのリストを表示する例を示します。

```
cisco-wave2-ap# show processes memory

Mem total:1030608 anon:23876 map:11424 free:712728
slab:132748 buf:0 cache:88284 dirty:0 write:0
Swap total:0 free:0
  PID  VSZ^VSZRW  RSS (SHR)  DIRTY (SHR)  STACK  COMMAND
  6227 56500 53464 1168 732 1144 732 132 /usr/sbin/mrvlfd
  6283 27536 20668 13032 2400 13032 2400 132 /usr/sbin/capwapd
  6297 24880 10612 14536 1376 14536 1376 132 wcpd
  6255 9612 6600 1508 1052 1508 1052 132 /usr/sbin/cleanaird
  5122 9556 4144 2664 2012 2664 2012 132 /usr/bin/capwap_brain
29097 7148 1536 3560 2392 3556 2388 132 /usr/sbin/cisco_shell
 3142 6828 1216 2992 2264 2992 2264 132 /usr/sbin/cisco_shell
 5106 4588 404 1912 1644 1912 1644 132 /usr/bin/fastcgi -s /tmp/fcgi_sock
 5108 4588 404 1912 1644 1912 1644 132 /usr/bin/slowcgi -s /tmp/slow_fcgi_sock

 6084 4544 452 928 360 928 360 132 /usr/sbin/lighttpd -f /etc/lighttpd.conf

 6214 3692 344 1420 960 1420 960 132 tamd_proc ap-tam 1 0 -debug err
 6213 3556 340 1460 1104 1460 1104 132 tams_proc -debug err
 6133 3396 400 1196 976 1196 976 132 /usr/bin/poder_agent
 4689 3176 336 1012 812 1012 812 132 /usr/bin/sync_log /storage/syslogs/13
 6143 3140 304 1428 1204 1428 1204 132 /usr/bin/failover
 4716 3136 284 616 436 616 436 132 watchdogd
 6121 3116 280 988 820 988 820 132 bigacl_d
 5084 3112 272 952 804 952 804 132 /usr/bin/led_core
 6181 1884 320 1044 260 1044 260 132 perl /usr/bin/drt.pl
 1 1596 196 492 412 492 412 132 init
30914 1596 196 428 344 428 344 132 top -m -b -n 1
 6145 1596 196 248 176 248 176 132 {S80cisco} /bin/sh /etc/init.d/S80cisco
```

## show processes memory

```
start
30912 1592 192 424 356 424 356 132 {show_process_me} /bin/ash
/usr/bin/cli_scripts/show_process_memory.sh 0 0 0 0 0 0 0 0 0
30911 1592 192 400 336 400 336 132 /bin/sh -c
/usr/bin/cli_scripts/show_process_memory.sh 0 0 0 0 0 0 0 0 0 | more
4684 1592 192 368 304 368 304 132 syslogd -S -s 100 -b 1 -L -R
255.255.255.255
30913 1592 192 332 264 332 264 132 more
4688 1584 184 344 284 344 284 132 klogd
4686 1584 184 320 264 320 264 132 printkd
30906 1584 184 284 228 284 228 132 sleep 10
29085 1452 332 640 416 640 416 132 /usr/sbin/dropbear -E -j -k -d
/storage/dropbear/dropbear_dss_host_key -r /storage/dropbear/dropbear_rsa_host_key
6209 1384 264 416 364 416 364 132 /usr/sbin/dropbear -E -j -k -d
/storage/dropbear/dropbear_dss_host_key -r /storage/dropbear/dropbear_rsa_host_key
8411 1096 212 444 336 444 336 132 dnsmasq -C /etc/dnsmasq.host.conf
6115 1096 212 436 340 436 340 132 dnsmasq -C /etc/dnsmasq.vaperr.conf
```

## show rrm

Radio Resource Management (RRM) プロパティを表示するには、**showrrm** コマンドを使用します。

```
show rrm {hyperlocation [level1-list] | neighbor-list [details] | receive {configuration | statistics}}
```

### 構文の説明

<b>hyperlocation</b> <i>level1-list</i>	AP の Cisco Hyperlocation のステータスを表示する
<b>neighbor-list</b>	neighbor-list の統計情報を表示する
<b>receive</b>	AP の Receive Signal Strength Indicator (RSSI)
<b>rogue</b>	不正関連情報を表示する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 使用上のガイドライン

次に、HyperLocation のレベル 1 チャンネル スキャン リストを表示する例を示します。

```
cisco-wave2-ap# show rrm hyperlocation level1-list
Level-1 List for 2.4GHz Band
=====
Channel   Width           Serving MAC      Max Clients
-----
Level-1 List for 5GHz Band
=====
Channel   Width           Serving MAC      Max Clients
-----
```

# show rrm rogue containment

アクセスポイントでの不正の阻止情報を表示するには、**show rrm rogue containment** コマンドを使用します。

**show rrm rogue containment {ignore|info} Dot11Radio radio-interface-number**

構文の説明	<b>ignore</b>	無視するよう設定されている不正 AP のリストを表示する
	<b>info</b>	AP の不正の阻止の設定および統計情報を表示する
	<b>Dot11Radio</b>	<b>Dot11Radio</b> インターフェイス キーワードを指定する
	<b>radio-interface-number</b>	無線インターフェイスのロット。有効な値は 0 および 1

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、802.11 インターフェイス（番号 1）の不正の阻止および統計情報を表示する例を示します。

```
cisco-wave2-ap# show rrm rogue containment info Dot11Radio 1
Rogue Containment Info and Stats for slot 1:
ssid client-addr contain-type channels

Request Status count
Submit 0
Success 0
Timeout 0
Error 0
Tuned 0
Flushed 0
Bad Channel 0
Tail Dropped 0
Cancelled 0
NDP DFS Tx Cancelled 0
Tx Failed 0
Created 0
```

## show rrm rogue detection

RRM 不正検出の設定パラメータを表示するには、**showrrmroguedetection** コマンドを使用します。

**show rrm rogue detection {adhoc|ap|clients|config|rx-stats} Dot11Radio radio-interface-number**

構文の説明	パラメータ	説明
	<b>adhoc</b>	802.11 無線スロットのマスターアドホック不正 AP リストを表示する。有効な値は 0 および 1
	<b>ap</b>	802.11 無線スロットの AP の不正検出パラメータを表示する。有効な値は 0 および 1
	<b>clients</b>	不正なクライアントのマスター リストを表示する
	<b>config</b>	AP 上の不正検出の設定を表示する
	<b>rx-stats</b>	AP の 802.11 インターフェイスでの不正検出受信の統計情報を表示する
	<b>Dot11Radio</b>	802.11 無線インターフェイスを指定する
	<b>radio-interface-number</b>	802.11 無線インターフェイス番号。有効な値は 0 および 1

コマンドモード Privileged EXEC (#)

コマンド履歴 リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

次に、RRM 不正検出の設定の詳細情報を表示する例を示します。

```
cisco-wave2-ap# show rrm rogue detection config
```

```
Rogue Detection Configuration for Slot 0:
Rogue Detection Mode : Enabled
Rogue Detection Report Interval : 10
Rogue Detection Minimum Rssi : -90
Rogue Detection Transient Interval : 0
Rogue Detection Flex Contain : Disabled
Rogue Detection Flex Contain Adhoc : Disabled
Rogue Detection Flex Contain SSID : Disabled
Rogue Containment Autorate : Disabled
Scan Duration : 180000
Channel Count : 11
Transient Threshold : 0
```

```
Rogue Detection Configuration for Slot 1:
Rogue Detection Mode : Enabled
Rogue Detection Report Interval : 10
Rogue Detection Minimum Rssi : -90
Rogue Detection Transient Interval : 0
```

```
Rogue Detection Flex Contain : Disabled  
Rogue Detection Flex Contain Adhoc : Disabled  
Rogue Detection Flex Contain SSID : Disabled  
Rogue Containment Autorate : Disabled  
Scan Duration : 180000  
Channel Count : 25  
Transient Threshold : 0
```

## show running-config

アクセスポイントの現在の実行コンフィギュレーションの内容を表示するには、**show running-config** コマンドを使用します。

### show running-config

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリー 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、アクセスポイントの現在の実行コンフィギュレーションの内容を表示する例を示します。

```
cisco-wave2-ap# show running-config

AP Name                : ap1540
Admin State            : Enabled
AP Mode                : Local
AP Submode             : None
Location               : default location
Reboot Reason         : Config Mwar
Primary controller name : cisco_3504
Primary controller IP  : <controller-ip-address>
Secondary controller name :
Secondary controller IP :
Tertiary controller name :
Tertiary controller IP  :
Controller from DHCP offer : <controller-dhcp-server-address>
Controller from DNS server : <controller-dns-server-address>
AP join priority       : 1
IP Prefer-mode        : IPv4
CAPWAP UDP-Lite       : Unconfigured
Last Joined Controller name: wlc3504
DTLS Encryption State  : Disabled
Discovery Timer        : 10
Heartbeat Timer        : 30
CDP State              : Enabled
Watchdog monitoring    : Enabled
IOX                    : Disabled
RRM State              : Enabled
LSC State              : Disabled
SSH State              : Enabled
AP Username            : admin
Session Timeout        : 0
Extlog Host            : 0.0.0.0
Extlog Flags           : 0
Extlog Status Interval : 0
Syslog Host            : <syslog-host-ip-address>
Syslog Facility        : 0
Syslog Level           : errors
Core Dump TFTP IP Addr :
Core Dump File Compression : Disabled
Core Dump Filename     :
```

```
Client Trace Status      : Enabled(All)
Client Trace All Clients : Enabled
Client Trace Filter     : 0x0000000E
Client Trace Out ConsoleLog: Disabled
WLC Link LAG status     : Disabled
AP Link LAG status      : Disabled
AP WSA Mode              : Disabled
```



## show security data-corruption

データ不整合エラーを表示するには、**show security data-corruption** コマンドを使用します。

### show security data-corruption

---

**構文の説明**

このコマンドには引数またはキーワードはありません。

---

**コマンドモード**

Privileged EXEC (#)

---

**コマンド履歴**

---

リリース 変更内容  
ス

---

8.7 このコマンドが導入されました。

---

### 例

次に、データ不整合エラーを表示する例を示します。

```
cisco-wave2-ap# show security data-corruption
```

## show security system state

システムレベルのセキュリティの現在の状態を表示するには、**show security system state** コマンドを使用します。

### show security system state

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドモード

Privileged EXEC (#)

#### コマンド履歴

リリース 変更内容  
ス

8.7 このコマンドが導入されました。

#### 例

システムレベルのセキュリティの現在の状態を表示するには、次のコマンドを使用します。

```
cisco-wave2-ap# show security system state
```

```
XSPACE:
          Non-Executable stack:    Yes
          Non-Executable heap:     Yes
          Non-Writable text:        Yes

OSC:
          Version:                  1.1.0

SafeC:
          Version:                  3.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4: show security system state のフィールドの説明

フィールド	説明
Non-Executable stack	システムがスタックからの実行を防止するかどうかを示す
Non-Executable heap	システムがヒープからの実行を防止するかどうかを示す
Non-Writable text	システムがテキストセクションへの書き込みを防止するかどうかを示す
OSC version	アプリケーションで使用されている OSC ライブラリのバージョンを示す

フィールド	説明
SafeC version	アプリケーションで使用されている SafeC ライブラリのバージョンを示す

# show spectrum

Spectrum ファームウェアの show コマンドを表示するには、**show spectrum** コマンドを使用します。

**show spectrum {list |recover |status }**

構文の説明	<p><b>list</b> Spectrum FW データ ファイルのリストを表示する</p> <p><b>recover</b> Spectrum FW の回復カウントを表示する</p> <p><b>status</b> Spectrum FW のステータスを表示する</p>
コマンドモード	Privileged EXEC (#)
コマンド履歴	<p>リリー 変更内容</p> <p>8.1.111.0 このコマンドが導入されました。</p>

次に、Spectrum ファームウェアのステータスを表示する例を示します。

```
cisco-wave2-ap# show spectrum status

Spectrum FW status slot 0:
  version: 1.15.4
  status:  up, crashes 0, resets 0, radio reloads 0
  load:    37.00  34.75  33.50  33.25
  NSI Key: 26c1bd25893a4b6dd3a00fe71735d067
  NSI:     not configured
  reg_wdog: 255 26309 0
  dfs_wdog: 0
  dfs_freq: 0
Spectrum FW status slot 1:
  version: 1.15.4
  status:  up, crashes 0, resets 0, radio reloads 0
  load:    37.25  38.00  38.75  39.00
  NSI Key: 26c1bd25893a4b6dd3a00fe71735d067
  NSI:     not configured
  reg_wdog: 255 26309 0
  dfs_wdog: 0
  dfs_freq: 0
```

# show tech-support

システム情報を表示する show コマンドを自動的に実行するには、**showtech-support** コマンドを使用します。

## show tech-support

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス
	8.1.111.0 このコマンドが導入されました。

次に、システム情報を表示する show コマンドを自動的に実行する例を示します。

```
cisco-wave2-ap# show tech-support
```

# show version

AP のソフトウェアのバージョン情報を表示するには、**show version** コマンドを使用します。

## show version

---

コマンドモード

Privileged EXEC (#)

---

コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、AP のソフトウェアのバージョン情報を表示する例を示します。

```
cisco-wave2-ap# show version
```

## show trace dot11\_chn

AP の 802.11 チャンネルの off-channel イベントを表示するには、**show tracedot11\_chn** コマンドを使用します。

**show trace dot11\_chn {enable |disable |statistics}**

### 構文の説明

**enable** 802.11 無線 0 および 1 の off-channel イベントの表示を有効にする

**disable** 802.11 無線 0 および 1 の off-channel イベントの表示を無効にする

**statistics** 802.11 無線 0 および 1 の off-channel イベントの統計情報を表示する

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、802.11 無線の off-channel イベントの統計情報を表示する例を示します。

```
cisco-wave2-ap# show trace dot11_chn statistics

Dot11Radio0 Off-Channel Statistics:
total_count in_prog_count last-chan last-type last-dur
           0             0         0         0         0

Dot11Radio1 Off-Channel Statistics:
total_count in_prog_count last-chan last-type last-dur
           0             0         0         0         0
```

## show trace

AP のトレース ログを表示するには、**showtrace** コマンドを使用します。

```
show trace
```

---

コマンドモード

Privileged EXEC (#)

---

コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

次に、AP のトレース ログを表示する例を示します。

```
cisco-wave2-ap# show trace
```



# show wips

wIPS モードに設定されている AP の詳細を表示するには、**showwips** コマンドを使用します。

```
show wips {alarm alarm-id|analyzer|buffer|channel channelno|infrastructure-device|neighbors
|node mac mac-address|node number number|object policy policy-id|policy ssid|session
mac-address|stats|violation node mac-address|violation channel channel-number}
```

## 構文の説明

<b>alarm</b>	AP が wIPS モードに設定されている場合に、設定されているアラームの統計情報を表示する。有効な値は 0 ～ 255
<i>alarm-id</i>	アラーム ID。有効な値は 0 ～ 255
<b>analyzer</b>	アナライザ関連の統計情報を表示する
<b>buffer</b>	バッファの統計情報を表示する
<b>channel</b>	チャンネル関連の統計情報を表示する
<i>channelno</i>	チャンネル番号。有効な値は 0 ～ 255
<b>infrastructure-device</b>	AP のインフラストラクチャ情報を表示する
<b>neighbors</b>	ネイバーの統計情報を表示する
<b>node</b>	AP のノード情報を表示する
<b>mac</b> <i>mac-address</i>	ノードの MAC アドレス
<b>node</b>	ノード
<b>number</b> <i>number</i>	ノード番号。有効な値は 1 ～ 500
<b>object</b>	AP オブジェクトストア
<b>policy</b> { <i>policy-id</i>   <i>ssid</i> }	AP ポリシー。ポリシー ID またはポリシー SSID のいずれかを指定する必要がある
<b>session</b> <i>mac-address</i>	ノードセッションの詳細を表示する。ノードの MAC アドレスを入力する必要がある
<b>stats</b>	AP の統計情報を表示する
<b>violation</b>	AP 違反をトラッキングする
<b>node</b> <i>mac-address</i>	ノードベースの違反をトラッキングする
<b>channel</b> <i>channel-number</i> <i>alarm-id</i>	チャンネルベースの違反をトラッキングする。チャンネル番号とアラーム ID を入力する必要がある

---

コマンドモード	Privileged EXEC (#)
---------	---------------------

---

コマンド履歴	リリース 変更内容 ス
--------	----------------

---

8.1.111.0 このコマンドが導入されました。

---

次に、AP の wIPS 統計情報を表示する例を示します。

```
cisco-wave2-ap# show wips stats
```



## システム管理コマンド

---

- [ap-type](#) (144 ページ)
- [archive](#) (145 ページ)
- [copy](#) (146 ページ)
- [delete](#) (147 ページ)
- [disable](#) (148 ページ)
- [enable](#) (149 ページ)
- [exec-timeout](#) (150 ページ)
- [logging](#) (151 ページ)
- [more](#) (152 ページ)
- [reload](#) (153 ページ)
- [terminal](#) (154 ページ)

## ap-type

AP に AP タイプを設定するには、**ap-type** コマンドを使用します。

```
ap-type {capwap |mobility-express word}
```

構文の説明	<p><b>capwap</b> AP を CAPWAP AP タイプとして有効にします。</p> <p><b>mobility-express</b> AP を Mobility Express AP タイプとして有効にします。</p> <p><i>word</i> TFTP 転送コマンドの詳細を次の形式で入力します。 tftp://&lt;tftp-server-ip-address&gt;/&lt;filename with path from root&gt;</p>
コマンドモード	Privileged EXEC (#)
コマンド履歴	<p>リリース 変更内容</p> <p>8.1.111.0 このコマンドが導入されました。</p>

### 例

次に、AP タイプを CAPWAP に設定する例を示します。

```
cisco-wave2-ap# ap-type capwap
```

# archive

AP イメージをダウンロードするには、**archive** コマンドを使用します。

```
archive download-sw {/no-reload |/reload [capwap word}
```

構文の説明	<b>download-sw</b> ソフトウェア ダウンロード コマンド
	<b>/no-reload</b> イメージのロード後にリロードしない
	<b>/reload</b> イメージのロード後にリロードする
	<b>capwap</b> イメージを Cisco WLC からダウンロードする
	<i>word</i> <b>ap image type ap3g3/ap1g4</b> フォーマットでイメージの詳細を入力します。
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 ス 8.1.111.0 このコマンドが導入されました。

# copy

ファイルをコピーするには、**copy** コマンドを使用します。

```
copy {cores filename [scp: scp-url | tftp: tftp-url] | flash filename [scp: scp-url | tftp: tftp-url] | support-bundle [scp: scp-url | tftp: tftp-url] | syslogs [filename {scp: scp-url | tftp: tftp-url} | scp: scp-url | tftp: tftp-url] }
```

構文の説明	
<b>cores</b>	コア ファイルにアクションを適用する
<i>filename</i>	ファイルの名前
<b>scp:</b>	SCP プロトコルを使用する
<i>scp-url</i>	SCP URL は、次の形式で入力する： username@A.B.C.D:[dir]/filename
<b>tftp:</b>	TFTP プロトコルを使用する
<i>tftp-url</i>	TFTP URL は、次の形式で入力する： A.B.C.D[/dir]/filename
<b>flash</b>	フラッシュ ファイルにアクションを適用する
<b>support-bundle</b>	サポート バンドルをサーバにコピーする
<b>syslogs</b>	syslog ファイルにアクションを適用する

コマンドモード Privileged EXEC (#)

コマンド履歴 リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

# delete

ファイルを削除するには、**delete** コマンドを使用します。

```
delete{/force | /recursive | /rf } cores filename
```

## 構文の説明

**/force** 強制削除

**/recursive** 再帰的削除

**/rf** 再帰的な強制削除

**cores** コア ファイルにアクションを適用する

*filename* 削除するファイル名

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、ファイルを削除する例を示します。

```
cisco-wave2-ap# delete /rf cores file-name
```

# disable

特権コマンドをオフにするには、**disable** コマンドを使用します。

## **disable**

コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

## 例

次に、特権コマンドをオフにする例を示します。

```
cisco-wave2-ap# disable
```



# enable

特権コマンドをオンにするには、**enable** コマンドを使用します。

## enable

---

### コマンドモード

User EXEC (>)

---

### コマンド履歴

---

リリース 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

## 例

次に、特権コマンドをオンにする例を示します。

```
cisco-wave2-ap> enable
```

# exec-timeout

exec-timeout を設定するには、**exec-timeout** コマンドを使用します。

**exec-timeout** *timeout-value*

構文の説明	<i>timeout-value</i> タイムアウト値。有効な値は0～2147483647
コマンドモード	Privileged EXEC (#)
コマンド履歴	リリース 変更内容 8.1.111.0 このコマンドが導入されました。

## 例

次に、exec-timeout を 20 秒に設定する例を示します。

```
cisco-wave2-ap# exec-timeout 20
```

# logging

コマンドのログを作成するには、**logging** コマンドを使用します。

```
logging {console [disable] | host {clear | disable | enable}}
```

## 構文の説明

---

**console** コンソール ロギング

---

**host** syslog サーバを設定する

---

**disable** syslog ホストのロギングを無効にする

---

**enable** syslog サーバを有効にする

---

**clear** syslog サーバ IP をクリアする

---

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

---

リリー 変更内容  
ス

---

8.1.111.0 このコマンドが導入されました。

---

## 例

次に、コンソール ロギングを有効にする例を示します。

```
cisco-wave2-ap# logging console
```

## more

ファイルを表示するには、**more** コマンドを使用します。

**more** {**flash** | **syslog**} *file-name*

### 構文の説明

**flash** フラッシュ ファイルにアクションを適用する

**syslog** syslog ファイルにアクションを適用する

*name* ファイル名

### コマンドモード

Privileged EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

### 例

次に、**test-log** という名前の **syslog** ファイルを表示する例を示します。

```
cisco-wave2-ap# more syslog test-log
```

# reload

アクセスポイントを停止するには、または再起動を実行するには、**reload** コマンドを使用します。

**reload** [{**at** *hours minutes day-of-month year* | **cancel** | **in** *minutes* | **reason** *reason-string*}]

## 構文の説明

**at** 特定の日に AP をリロードする

このキーワードは、時間、分、日付、月、年をパラメータとして取る。有効な値は次のとおり：

- *hour* : 0 ~ 23
- *minutes* : 0 ~ 59
- *day-of-the-month* : 1 ~ 31
- *month* : 1 ~ 12
- *year* : 2015 ~ 2099

**cancel** 中断しているリロードをキャンセルする

**in** 一定の間隔後にリロードする。この時間は分で指定する。有効な値は 1 ~ 1440 分

**reason** リロードの理由を指定する文字列

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、10 分後に AP をリロードする例を示します。

```
cisco-wave2-ap# reload in 10
```

# terminal

ターミナルパラメータを設定するには、**terminal** コマンドを使用します。

**terminal** {**length** |**monitor** [**disable** ]|**type** *word* |**width** *no-of-characters*}

## 構文の説明

**length** 画面上の行数を指定する。有効な値は 0 ～ 512。出力を一時停止しない場合は 0 を入力する

**monitor** デバッグの出力先を現在のターミナル回線に指定する。モニタリングを有効にするには Enter キーを押す。モニタリングを無効にするには、キーワード **disable** を入力する

**type** ターミナルのタイプを指定する

**width** ディスプレイ ターミナルの幅を指定する。有効な値は 0 ～ 132

## コマンドモード

Privileged EXEC (#)

## コマンド履歴

リリー 変更内容  
ス

8.1.111.0 このコマンドが導入されました。

## 例

次に、ターミナルの行数を 50 に設定する例を示します。

```
cisco-wave2-ap# terminal length 50
```