Cisco Catalyst 9100 シリーズ Wi-Fi6/6E アクセスポイント（IOS-XE リリース）コマンドリファレンス

初版：2023 年 8 月 15 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/**）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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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/c/en/us/about/legal/trademarks.html. 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)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

ここでは、『Cisco Catalyst 9100 アクセス ポイント コマンド リファレンス』の対象者、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

このマニュアルは、Cisco Catalyst 9100 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、以下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、およびユーザー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、およびユーザーが値を指定する関数は、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 この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。（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 fisicos. 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

通信、サービス、およびその他の情報

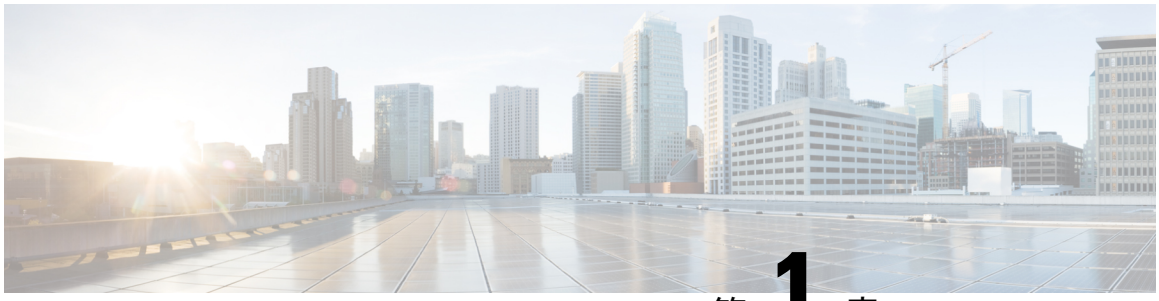
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Ciscoシスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

コマンドライン インターフェイスの使用

この章では、Cisco Catalyst 9100 アクセスポイントのコマンドライン 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

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、ユーザー 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-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	アクセス方法	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-ap>`	**logout** または **quit** 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。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザー EXEC モードを実行している場合は、**enable** 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-ap#`	終了するには、**disable** と入力します。	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-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-ap# debug client ...
```

デバッグを無効にするコマンド：

```
cisco-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-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-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。

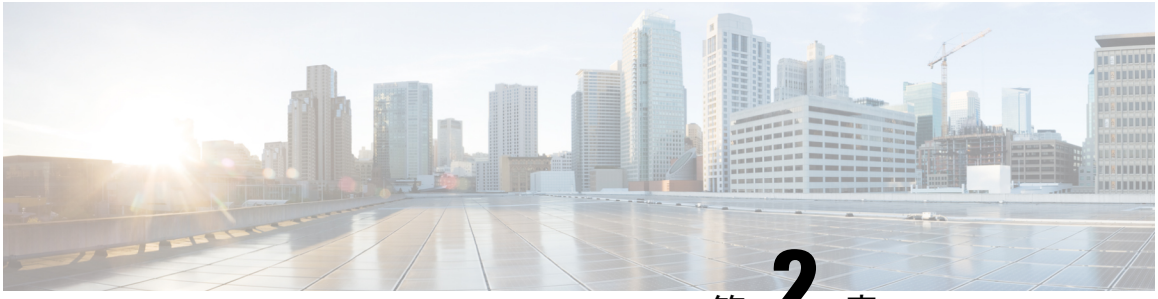
（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

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

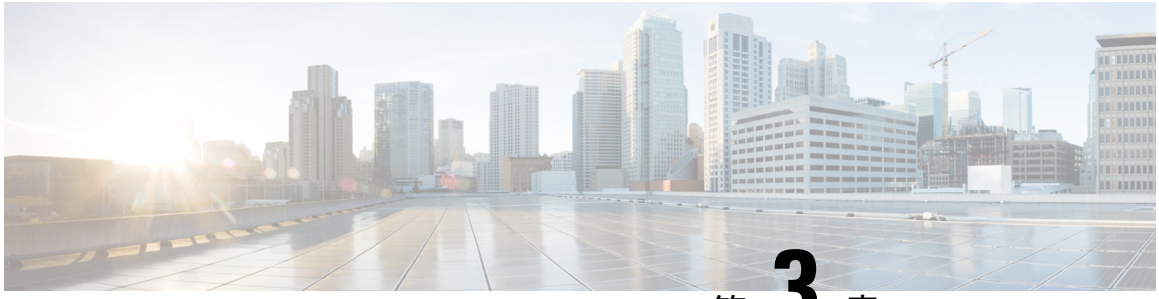
CLI にはコンソール接続、Telnet、またはブラウザを使用することによってアクセスできます。1 つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。



第 2 章

サポートされているシスコのアクセス ポイント

このマニュアルでは、Cisco Catalyst 9100 Wi-Fi 6/6E ファミリのアクセスポイントでサポートされているコマンドについて説明します。



第 3 章

capwap コマンド

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

primary-base	AP のプライマリ コントローラを設定する
secondary-base	AP のセカンダリ コントローラを設定する
tertiary-base	AP のターシャリ コントローラを設定する
controller-name	コントローラの名前
controller-ip-address	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、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-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		
	ssc-token	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、認証トークンを設定する例を示します。

```
cisco-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
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-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、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-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、AP にホスト名を設定する例を示します。

```
cisco-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

static-ip-addr	AP のスタティック IP アドレス
static-netmask	スタティック ネットマスク
ip-addr-default-gateway	デフォルト ゲートウェイの IP アドレス。
[*ip-addr-dns1* | *ip-addr-dns2*]	（任意のパラメータ）DNS の IP アドレス
[*domain-name*]	（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
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-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、AP で LAG を有効にする例を示します。

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

capwap ap mesh strict-wired-uplink

有線アップリンクが失われた場合でも、ルートアクセスポイント（RAP）を永続的な RAP として維持するように設定するには、**capwap ap mesh strict-wired-uplink** コマンドを使用します。

capwap ap mesh strict-wired-uplink {**enable** | **disable**}

構文の説明		
	enable	Cisco AP で厳密な有線アップリンクを有効にする。
	disable	Cisco AP で厳密な有線アップリンクを無効にする。

コマンド モード	Privileged EXEC (#)

コマンド履歴	リリース	変更内容
	8.9 Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、有線アップリンクが失われた場合でも、ルートアクセスポイント（RAP）を永続的な RAP として維持する例を示します。

```
cisco-ap# capwap ap mesh strict-wired-uplink 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、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-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		
	restart	CAPWAP プロトコルを再起動する

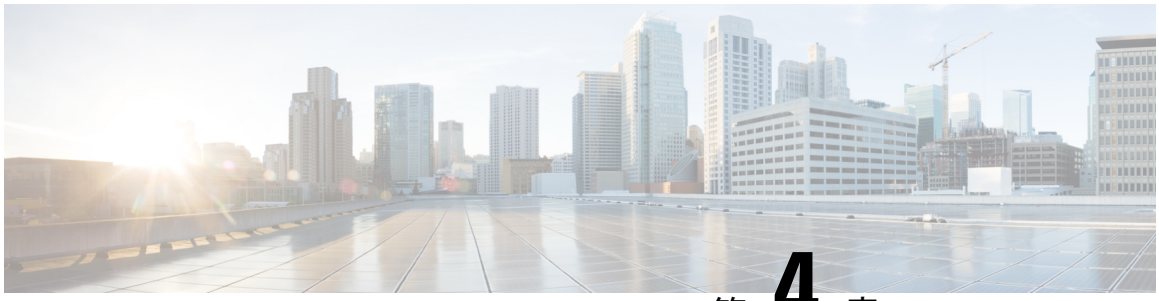
コマンド モード	
	Privileged EXEC (#)

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 プロトコルを再起動する例を示します。

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



第 4 章

clear コマンド

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		
	statistics	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、AVC NBAR 統計情報をクリアする例を示します。

```
cisco-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 countersDot11Radio *interface-number* | **client** | **fast-path profinet** | **wired** *interface-number* **MIB-stats**

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 インターフェイスの番号。有効な値は 0 または 1。
client	クライアントの統計情報をクリアする。
fast-path	コントローラの高速パスの統計情報をクリアする。
profinet	Profinet の統計情報をクリアする。
wired	有線インターフェイスの統計情報をクリアする。
interface-number	有線インターフェイスの番号。有効な値は 0 ～ 3。
MIB-stats	AP 内部スイッチ MIB 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

リリース	変更内容
8.1.111.0	このコマンドが導入されました。
8.7	**client, fast-path, profinet, wired** パラメータを追加することで、このコマンドが拡張されました。

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-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

counters	Cisco TrustSec の要約カウンタをクリアする
all	すべての Cisco TrustSec カウンタをクリアする
client *mac-addr*	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
from	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
sgt	セキュリティ グループ タグ（SGT）。有効な値は 0 ～ 65535
to	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
dgt	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、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-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

drops	データパス ドロップ カウンタをクリアする
statistics	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、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-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

sensor	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、802.11 の設定をクリアする例を示します。

```
cisco-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

capwap	（任意）CAPWAP ロギングの詳細をクリアする
message	（任意）メッセージ ロギングの詳細をクリアする
warning	（任意）警告ロギングの詳細をクリアする

コマンド モード

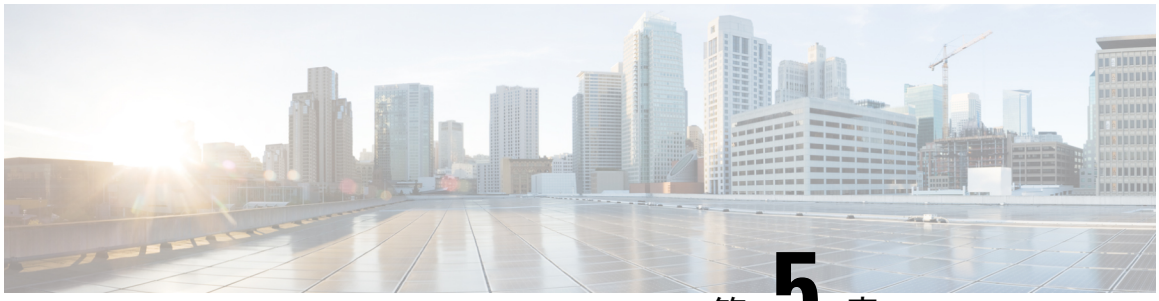
Privileged EXEC (#)

コマンド履歴

リリース	変更内容
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-ap# clear logging capwap
```



第 5 章

config コマンド

config ap address

AP IPv4 または IPv6 アドレスを設定するには、**config ap address** コマンドを使用します。

config ap address ipv4 { **dhcp** | **static** { *static-ip-addr static-netmask default-gateway-ip-addr* | **ipv6** { **auto-config** {**enable** | **disable**} | **dhcp** | **disable** | **link-local** *ipv6-addr* | **static** *ipv6-addr ipv6-prefix gateway-ipv6-addr*

構文の説明

ipv4	IPv4 アドレスを設定する
ipv6	IPv6 アドレスを設定する
auto-config	IPv6 アドレスを自動設定する
dhcp	IPv6 DHCP を設定する

auto-config
auto-config

コマンド デフォルト　なし。

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

使用上のガイドライン

例

関連コマンド

コマンド	説明

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、**config ap client-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

addresses	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
add	トレースするクライアントを指定する
clear-all	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
delete	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
all-clients	すべてのクライアントをトレースする
enable	すべてのクライアントのトレースを有効にする
disable	すべてのクライアントのトレースを無効にする
filter	クライアント トレースのためのフィルタを設定する
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 このフィルタを有効または無効にするには、**enable** または **disable** キーワードを使用します。
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	プローブ パケットをトレースする
inline-mon	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
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-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、**config ap client-trace filter** 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**] }

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

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。

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-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、**config ap client-trace output** 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、トレースの出力を設定する例を示します。

```
cisco-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		
	115200	ボー レートを 115200 に設定する
	9600	ボー レートを 9600 に設定する

コマンド デフォルト	デフォルトの config boot baudrate は 9600 です。
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、ボー レートを 9600 に設定する例を示します。

```
cisco-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、ブート ブレイクを有効にする例を示します。

```
cisco-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

enable	カーネル クラッシュを有効にする
disable	カーネル クラッシュを無効にする

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、カーネル クラッシュを有効にする例を示します。

```
cisco-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

enable	メモリ デバッグを有効にする
disable	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、メモリ デバッグを有効にする例を示します。

```
cisco-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、マニュアル ブートを有効にする例を示します。

```
cisco-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、ブートパスを 1 に設定する例を示します。

```
cisco-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	
ipv4 *dst-ip* [*src-ip*]	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
ipv6 *dst-ip* [*src-ip*]	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
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-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

rate	デバッグ ログの出力レートを設定する
X	処理した *Y* 個のパケットごとにデバッグを表示するパケットの数。有効な範囲は 0 ～ 10000
Y	処理するパケットの数。有効な範囲は 0 ～ 10000

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、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-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、 **config cts debug enforcement permissions** 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、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-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、 **config cts debug enforcement protocol** コマンドを使用します。

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

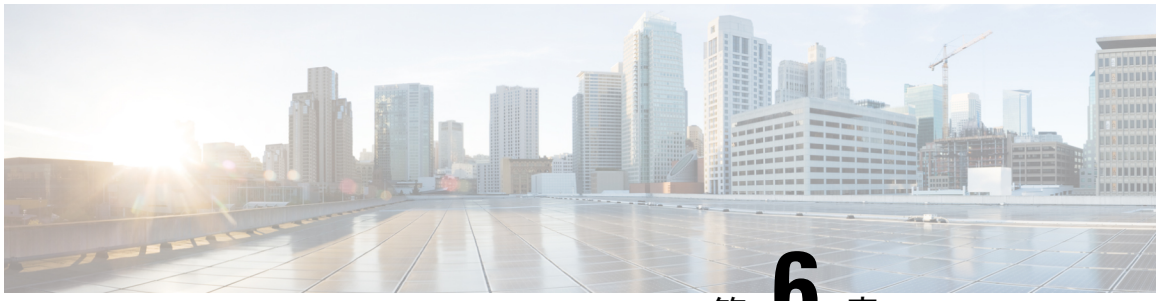
構文の説明		
	protocol-id	プロトコル ID。有効な値は 0 ～ 65535
	icmp	ICMP トラフィックで SGACL 強制デバッグをフィルタリングする
	tcp	TCP トラフィックで SGACL 強制デバッグをフィルタリングする
	udp	UDP トラフィックで SGACL 強制デバッグをフィルタリングする

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、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-ap# config cts debug enforcement protocol udp
```



第 6 章

debug コマンド

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、ARP エラーのデバッグを有効にする例を示します。

```
cisco-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

critical	BLE クリティカル イベントのデバッグを有効にする
error	BLE エラー イベントのデバッグを有効にする

events	BLE イベントのデバッグを有効にする
fastpath {**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。 • RSSI データ • スキャン データ • 同期データ
receive	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
transmit	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-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

ble	CAPWAP BLE 詳細のデバッグを有効する
detail	CAPWAP 詳細のデバッグを有効する
efficient-upgrade	イメージのプレダウンロードのデバッグを有効にする
error	CAPWAP エラーのデバッグを有効にする
events	CAPWAP のイベントのデバッグを有効にする
flexconnect	CAPWAP FlexConnect モードのイベントのデバッグを有効にする

info	CAPWAP の情報のデバッグを有効にする
keepalive	CAPWAP のキープアライブのデバッグを有効にする
payload	CAPWAP ペイロードのデバッグを有効にする
pmtu	CAPWAP パス MTU のデバッグを有効にする
qos	CAPWAP QoS のデバッグを有効にする
reassembly	CAPWAP リアセンブルのデバッグを有効にする
security	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-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
detail	CAPWAP AVC 詳細のデバッグを有効にする
error	CAPWAP AVC エラーのデバッグを有効にする
event	CAPWAP AVC のイベントのデバッグを有効にする
info	CAPWAP AVC の情報のデバッグを有効にする
netflow	CAPWAP クライアントの AVC NetFlow のデバッグを有効にする

netflow all	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
netflow detail	CAPWAP クライアントの AVC NetFlow 詳細のデバッグを有効にする
netflow error	CAPWAP クライアントの AVC NetFlow エラーのデバッグを有効にする
netflow event	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
netflow packet	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
numflows	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、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-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、CDP イベントのデバッグを有効にする例を示します。

```
cisco-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

bringup	CleanAir ポートまたは起動のデバッグを有効にする
events	通常の CleanAir イベントのデバッグを有効にする
logdebug	CleanAir のデバッグ出力をログファイルに記録する
low	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
major	主要な CleanAir イベントのデバッグを有効にする
nsi	NSI メッセージのデバッグを有効にする
offchan *0* | *1*	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、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-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、DHCP エラーのデバッグを有効にする例を示します。

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

debug dot11 driver level

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 driver level { **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 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-ap# debug dot11 errors
```

debug dot11 client data-path

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 data-path** コマンドを使用します。

debug dot11 client data-path { { **all-types** | **arp** | **dhcp** | **eapol** | **ipv6-ra** | **opendns** | **dns-acl** } { **addr** { *mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4* } } }

構文の説明

arp	クライアント データパスの ARP デバッグを有効にする
dhcp	クライアント データパスの DHCP デバッグを有効にする
eapol	クライアント データパスの EAPOL デバッグを有効にする
dns-acl	クライアント データパスの DNS-ACL デバッグを有効にする
ipv6-ra	クライアントデータパスの IPv6 RA-MC2UC デバッグを有効にする
opendns	クライアントデータパスの openDNS デバッグを有効にする
{**addr** | **all-types**}	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
{*mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4*}	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
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-ap# debug dot11 client data-path arp
```

debug dot11 client management

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 management** コマンドを使用します。

debug dot11 client management { **critical** | **errors** | **events** | **info** } { **addr** { *mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4* } }

構文の説明

critical	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
errors	クライアントのエラー レベルのデバッグを有効にする
events	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
info	クライアントの情報レベルのデバッグを有効にする
{*mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4*}	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
8.1.111.0	このコマンドが導入されました。

例

次に、イベントレベルでクライアントのデバッグを有効にする例を示します。

```
cisco-ap# debug dot11 client management events e1:90:6f:7e:e6:29
```

debug dot11 client probe

802.11 クライアントのデバッグプローブを有効にするには、**debug dot11 client probe** コマンドを使用します。

debug dot11 client probe { { **address** *mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4* } | **all** }

構文の説明

address	MAC アドレスを使用して特定のクライアントをプローブする。
mac-addr	クライアントの MAC アドレス。最大 4 つの MAC アドレスを入力できる。
all	AP に関連付けられているすべてのクライアントをプローブする。

コマンド モード

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
8.10	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デバッグを有効にする例を示します。

```
cisco-wave2-ap# debug dot11 client probe 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-types** | { **cac** { **info** | **metrics** } } | **chd** | **save-accounting-data** | **save-on-failure** [**extended**] | **stop-on-failure** | **metrics traffic** | **metrics video** | **type** { **all** | **association** | **authentication** | **dhcp** | **eap** | **icmp** | **probe** } *mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4*

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-types	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-accounting-data	無線アカウンティング 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
metrics traffic	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
metrics video	802.11 ビデオ メトリックのデバッグを有効にする
type	デバッグタイプを有効にする。
all	all タイプのデバッグを有効にする。
association	関連付けのデバッグを有効にする。
authentication	認証のデバッグを有効にする。
dhcp	dhcp のデバッグを有効にする。
eap	eap のデバッグを有効にする。
icmp	icmp のデバッグを有効にする。
probe	プローブのデバッグを有効にする。
mac-addr	クライアントの MAC アドレス。最大 4 つの MAC アドレスを入力できる。

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。
8.5.140.0 および 8.8	**type** パラメータを追加することで、このコマンドが拡張されました。

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

debug dot11 firmware

802.11 ファームウェアをデバッグするには、**debug dot11 firmware** コマンドを使用します。

debug dot11 firmware slot *slot_ID* **level** { **all-level** | **critical** | **emergency** | **error** | **info** } **address** { *mac-addr1* | *mac-addr2* | *mac-addr3* | *mac-addr4* }

構文の説明

slot_ID	無線ごとの 802.11 ドライバのデバッグを有効にする

all-level	すべてのデバッグレベルを有効にする。
critical	クリティカルレベルのデバッグを有効にする。
emergency	緊急レベルのデバッグを有効にする。
error	エラーレベルのデバッグを有効にする。
info	情報レベルのデバッグを有効にする。
address	ドライバ/ファームウェアのデバッグ用のクライアントアドレスを追加する。
mac-addr	クライアントの MAC アドレス。最大 4 つの MAC アドレスを入力できる。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
8.5.140.0 および 8.8	このコマンドが導入されました。

例

次に、802.11 の緊急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 firmware slot 1 emergency address 92:FB:D6:B3:7A:6C
```

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

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

web-server	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-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

error	DTLS クライアント エラーのデバッグを設定する
event [**detail**]	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、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-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る
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
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-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

acl	FlexConnect ACL のデバッグを設定する
cckm	CCKM のデバッグを設定する
dot11r	802.11r のデバッグを設定する
event	Wireless Control Protocol（WCP）イベントのデバッグを設定する
multicast igmp	マルチキャスト IGMP のデバッグを設定する
multicast traffic	マルチキャスト トラフィックのデバッグを設定する
pmk	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
vsa	AAA ベンダー固有属性（VSA）のデバッグを設定する

wlan-vlan	WLAN-VLAN マッピングのデバッグを設定する
wsastats	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
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-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、LLDP エラーのデバッグを有効にする例を示します。

```
cisco-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、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-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

diff	メモリ プールのデバッグの差分を詳細に示す
realtime interval *1-1000000-seconds*	メモリ プールのリアルタイムの間隔を設定する。
start	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-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
name *pool-name*	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
diff	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
realtime interval *1-1000000-seconds*	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
start	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
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-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
name *pool-name*	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
diff	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
realtime interval *1-1000000-seconds*	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
start	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
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-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

channel	メッシュ チャネルのデバッグを設定する
clear	すべてのメッシュ デバッグをリセットする
convergence	メッシュ コンバージェンスのデバッグを設定する
events	メッシュ イベントのデバッグを設定する
forward-mcast	メッシュ転送マルチキャストのデバッグを設定する
forward-packet	メッシュ転送パケットのデバッグを設定する

forward-table	メッシュ転送テーブルのデバッグを設定する
linktest	メッシュ リンクテストのデバッグを設定する
port-control	メッシュ ポート制御のデバッグを設定する
security	メッシュ セキュリティのデバッグを設定する
trace	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-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

adjacency	メッシュ隣接関係をデバッグする
child	メッシュ隣接関係の子をデバッグする
clear	メッシュ隣接関係のクリアをデバッグする
dfs	メッシュ DFS をデバッグする
message	メッシュ隣接関係のメッセージをデバッグする
packet	メッシュ隣接関係のパケットをデバッグする
parent	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、メッシュ隣接関係の親のデバッグを有効にする例を示します。

```
cisco-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
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-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
	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-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		
	reports	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-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

all	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、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-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、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-ap# debug wips errors
```

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、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-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、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-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		
	eogre	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、EoGRE トンネルのデバッグを有効にする例を示します。

```
cisco-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

all	すべてのクライアント トレースを設定する
address	トレースするアドレスを設定する
mac-address	トレースする MAC アドレス
enable	トレースを有効にする
filter	トレース フィルタを設定する
assoc	関連付けパケットをトレースする
auth	認証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
mgmt	probe、assoc、auth、EAP パケットをトレースする
probe	プローブ パケットをトレースする
proto	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、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-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
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-ap# no debug
```

traceroute

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、**traceroute** コマンドを使用します。

traceroute *destination-address*

構文の説明

destination-address	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、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-ap# traceroute 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	
al	すべてのデバッグ メッセージを無効にする

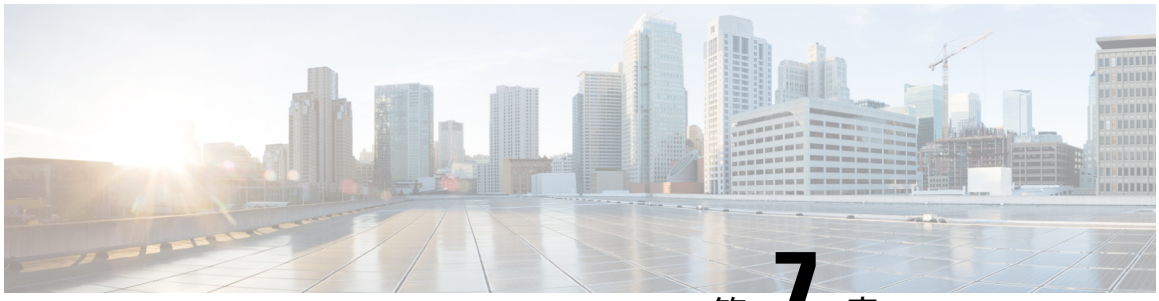
コマンド モード	
Privileged EXEC (#)	

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、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-ap# undebug all
```



第 7 章

show コマンド

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、**show ap client-trace status** 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

events	クライアント トレース イベント情報を表示する
all	すべてのクライアント トレース イベントを表示する
system	すべてのシステム イベントを表示する
mac	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

word	特定のクライアントの MAC アドレス
skb	クライアント トレース SKB 情報を表示する
drop-list	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
stats	クライアント トレース SKB 統計情報を表示する
status	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
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-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
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-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	クライアントの MAC アドレス

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、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-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
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-ap# show avc nbar build
```

show avc netflow flows

現在キャッシュされていて、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、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-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
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-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
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-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

client	CAPWAP クライアント情報
ids	CAPWAP ID 情報
ip	CAPWAP IP 設定
location	CAPWAP ロケーション情報
mcast	CAPWAP マルチキャスト情報
pnp	PNP 情報
traffic	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、CAPWAP マルチキャスト情報を表示する例を示します。

```
cisco-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

callinfo *info*	CAPWAP クライアントのコール情報
detailrcb	CAPWAP クライアントの詳細な RCB 情報
rcb	CAPWAP クライアントの RCB 情報
config	CAPWAP クライアントの設定情報
ha	CAPWAP クライアントの HA パラメータ
msginfo	CAPWAP クライアントのメッセージ情報
timers	CAPWAP クライアントのタイマー

traffic	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、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-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

clear	トレースをクリアする
delete	トレースを削除する
disable	起動時にトレースを無効にする
enable	起動時にトレースを有効にする
save	トレースを保存する
start	トレースを開始する
stop	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、CAPWAP クライアント トレースを表示する例を示します。

```
cisco-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、CAPWAP ID シグネチャの統計情報を表示する例を示します。

```
cisco-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

entry device *device-name*	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
inline_power	インライン電力ネゴシエーション情報
interface	CDP インターフェイスのステータスと設定
neighbors	CDP ネイバー エントリ
traffic	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
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-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-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-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
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-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-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 configurationrlan

コマンド モード	Privileged EXEC (#)

構文の説明

rlan	RLAN設定を表示する。

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。
8.9	**rlan** パラメータを追加することで、このコマンドが拡張されました。
8.10.112.0	破損アンテナの検出のステータスが表示されるように、このコマンドの出力が拡張されました。

次に、AP 設定の詳細を表示する例を示します。

```
cisco-ap# show configuration

AP Name                     : AP58AC.78DC.C2F0
Admin State                 : Enabled
AP Mode                     : FlexConnect
AP Submode                  : Not Configured
Location                    : default location
Reboot Reason               : Reload command
.
.
AP Link LAG status          : Disabled
AP WSA Mode                 : Enabled
Vlan Interface              : Disabled

Broken antenna detection    : Enabled (Global)
RSSI Failure Threshold      : 40
Weak RSSI                   : 60
Detection Time              : 12
If any broken antenna?      : ALL
AP58AC.78DC.C2F0#
```

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

ble-interface-number	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
broadcast	BLE ブロードキャスト サマリー情報を表示する
counters	BLE トランスポート カウンタ情報を表示する

floor-tag *floor-beacon-mac-addr*	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
interface	BLE インターフェイス サマリー情報を表示する
local	ホスト BLE 無線の同期情報を表示する
scan brief	簡単な BLE スキャン サマリー情報を表示する
scan detail *floor-beacon-mac-addr*	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
timers	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
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-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** | { **atfconfiguration** | **statistics**} | **bandselect** | **client** { *client-mac-addr* | **all detail** } | **frequency** | **powercfg** | **powerreg** | **radiostats** | **rate** | **vlan** | **wlan** { *wlan-id* | **all detail** } }

構文の説明

dot11-interface-no	Dot11Radio インターフェイスの番号。
atf configuration	AirTime Fairness の設定を表示する。

atf statistics	AirTime Fairness の統計情報を表示する。
bandselect	BandSelect の統計情報を表示する。
antenna	アンテナの設定を表示する
client *client-mac-addr*	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。
detail	すべてのクライアントの TID 統計情報を表示する。
frequency	周波数情報を表示する。
powercfg	設定されている電力情報を表示する。
powerreg	送信電力情報を表示する。
radio-stats	無線統計情報を表示する。
rate	レート情報を表示する。
vlan	VLAN の概要を表示する。
wlan *wlan-id*	指定された WLAN ID の VLAN/WLAN の詳細を表示する。
detail	すべてのクライアントの TID 統計情報を表示する。

コマンド モード

User 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。
8.9	**bandselect** 、**client all detail** 、**wlan** パラメータを追加することで、このコマンドが拡張されました。

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-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
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-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

wired-interface-number	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、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-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 Emac1 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-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
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-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
	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-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、**show dot11 qos** 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
	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-ap# show dot11 qos
```

show dot11 wlan wpa3

802.11 ネットワークでの WPA3 設定を表示するには、**show dot11 wlan wpa3** コマンドを使用します。

show dot11 wlan wpa3 ［**transition**］

構文の説明		
	transition	WPA3 移行モードの詳細を表示する。

コマンド モード	
	Privileged EXEC (#)

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

次に、802.11 ネットワークでの WPA3 設定を表示する例を示します。

```
cisco-ap# show dot11 wlan wpa3
```

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
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-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		
	cores	フラッシュにあるコア ファイルを表示する
	detail	コア ファイルの内容を表示する
	core-file-name	コア ファイル名

crash	フラッシュにあるクラッシュ ファイルを表示する
syslogs	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、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-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

calea	CALEA 情報を表示する
cckm	CCKM キャッシュ エントリ情報を表示する
client	クライアント情報を表示する
aaa-override	AAA オーバーライド パラメータを指定する
counter	すべてのクライアントにカウンタを指定する
priority	クライアントの優先順位を指定する
dot11r	802.11r キャッシュ エントリ情報を表示する
mcast	マルチキャスト情報を表示する
oeap	FlexConnect OEAP 情報を表示する
pmk	OKC または PMK キャッシュ エントリ情報を表示する
status	スタンドアロン ステータスを表示する

vlan-acl	VLAN ACL マッピングを表示する
wlan	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、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-ap# show flexconnect client
```

show flexconnect oeap firewall

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

show flexconnect oeap 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
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-ap# show flexconnect oeap 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
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-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* **datapathcounters** | **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 （注） Cisco 1852、9117、9130 AP では、802.11 tx 統計情報カウンタの下にビーコン tx 統計情報が含まれていません。
wlan *wlan-id*	指定した VLAN 情報を表示する
datapath	データパスカウンタを表示する。
counters	データパスカウンタおよびドロップを表示する。

コマンド モード

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
8.1.111.0	このコマンドが導入されました。
8.9	**datapath** パラメータを追加することで、このコマンドが拡張されました。

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-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
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-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* {**MIB-stats** | **datapath counters**}

構文の説明

wired-interface-number	有線インターフェイスの番号。有効な範囲は 0 ～ 3
MIB-stats	AP 内部スイッチ MIB カウンタを表示する。
datapath	データパスカウンタを表示する。
counters	データパスカウンタおよびドロップを表示する。

コマンド モード

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
8.1.111.0	このコマンドが導入されました。
8.9	**datapath** パラメータを追加することで、このコマンドが拡張されました。

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-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-ap# show inventory

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

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**| **sip-snooping**{ **stats**| **status**}]}

構文の説明

access-lists	IP アクセス リストを表示する
interface	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
brief	IP ステータスおよび設定の概要を表示する
route	IP ルーティング テーブルを表示する
tunnel	IP トンネル情報を表示する
eogre	EoGRE トンネル情報を表示する
domain	EoGRE トンネル ドメイン情報を表示する
forwarding-table	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
gateway	EoGRE トンネルのゲートウェイ情報を表示する
fabric	IP ファブリック トンネルの情報を表示する
summary	すべてのトンネルの情報を表示する
sip-snooping	SIP スヌーピングのオプションを表示する。
stats	送受信された SIP スヌーピングの統計情報を表示する。
status	SIP スヌーピングのステータスを表示する。

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
8.1.111.0	このコマンドが導入されました。
8.9	**sip-snooping** パラメータを追加することで、このコマンドが拡張されました。

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-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、LACP トラフィック情報を表示する例を示します。

```
cisco-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
	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-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		
	detail	詳細なシステムのメモリ使用量を表示する
	pool	システムのメモリ プールを表示する
	summary	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
	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-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
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-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

cpu *cpu-number*	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
dmalloc	dmalloc プロセスのプロセス使用率を表示する

capwap	CAPWAP の dmalloc 統計情報を表示する
wcp	WCP の dmalloc 統計情報を表示する
status	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
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-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

maps	プロセスのマップを表示する
smaps	プロセスの smaps を表示する
pid *pid-number*	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
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-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/mrvlfwd
 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/slowfcgi -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
 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 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 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、**show rrm** 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

hyperlocation *level1-list*	AP の Cisco Hyperlocation のステータスを表示する

neighbor-list	neighbor-list の統計情報を表示する
receive	AP の Receive Signal Strength Indicator（RSSI）
rogue	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

リリース	変更内容
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 チャネル スキャン リストを表示する例を示します。

```
cisco-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

ignore	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
info	AP の不正の阻止の設定および統計情報を表示する
Dot11Radio	**Dot11Radio** インターフェイスキーワードを指定する。
radio-interface-number	無線インターフェイスのスロット。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
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-ap# show rrm rogue containment info Dot11Radio 1
Rogue Containment Info and Stats for slot 1:
bssid 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、**show rrm rogue detection** 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

adhoc	802.11 無線スロットのプライマリアドホック不正 AP リストを表示する。有効な値は 0 および 1
ap	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
clients	不正なクライアントのプライマリリストを表示する
config	AP 上の不正検出の設定を表示する
rx-stats	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
Dot11Radio	802.11 無線インターフェイスを指定する
radio-interface-number	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、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-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-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
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-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
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-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
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

list	Spectrum FW データ ファイルのリストを表示する
recover	Spectrum FW の回復カウントを表示する
status	Spectrum FW 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
8.1.111.0	このコマンドが導入されました。

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-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、**show tech-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
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-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
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-ap# show version
```

show trace dot11_chn

AP の 802.11 チャネルの off-channel イベントを表示するには、**show trace dot11_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 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-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、**show trace** 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
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-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、**show wips** 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

alarm	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
alarm-id	アラーム ID。有効な値は 0 ～ 255
analyzer	アナライザ関連の統計情報を表示する
buffer	バッファの統計情報を表示する
channel	チャネル関連の統計情報を表示する
channelno	チャネル番号。有効な値は 0 ～ 255
infrastructure-device	AP のインフラストラクチャ情報を表示する
neighbors	ネイバーの統計情報を表示する
node	AP のノード情報を表示する
mac *mac-address*	ノードの MAC アドレス
node	ノード
number *number*	ノード番号。有効な値は 1 ～ 500
object	AP オブジェクト ストア
policy {*policy-id* |**ssid**	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
session *mac-address*	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
stats	AP の統計情報を表示する
violation	AP 違反をトラッキングする

node *mac-address*	ノードベースの違反をトラッキングする
channel *channel-number alarm-id*	チャネルベースの違反をトラッキングする。チャ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

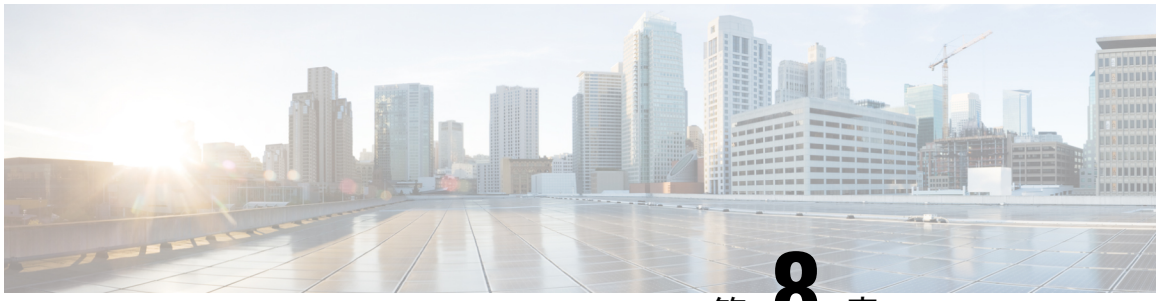
Privileged EXEC (#)

コマンド履歴

リリース	変更内容
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-ap# show wips stats
```



第 8 章

システム管理コマンド

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* | **workgroup-bridge**}

構文の説明

capwap	AP を CAPWAP AP タイプとして有効にします。
mobility-express	AP を Mobility Express AP タイプとして有効にします。
word	TFTP 転送コマンドの詳細を次の形式で入力します。 tftp://<tftp-server-ip-address>/<filename with path from root>
workgroup-bridge	ワークグループブリッジ（WGB）APタイプを有効にします。

コマンド モード

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
8.1.111.0	このコマンドが導入されました。
8.8.120.0	**workgroup-bridge** パラメータを追加することで、このコマンドが拡張されました。

例

次に、AP タイプを CAPWAP に設定する例を示します。

```
cisco-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

download-sw	ソフトウェア ダウンロード コマンド
/no-reload	イメージのロード後にリロードしない
/reload	イメージのロード後にリロードする
capwap	イメージを Cisco WLC からダウンロードする
word	**ap image type ap3g3/ap1g4** 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
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

cores	コア ファイルにアクションを適用する

filename	ファイルの名前
scp:	SCP プロトコルを使用する
scp-url	SCP URL は、次の形式で入力する： username@A.B.C.D:[/dir]/filename
tftp:	TFTP プロトコルを使用する
tftp-url	TFTP URL は、次の形式で入力する： A.B.C.D[/dir]/filename
flash	フラッシュ ファイルにアクションを適用する
support-bundle	サポート バンドルをサーバにコピーする
syslogs	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
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、ファイルを削除する例を示します。

```
cisco-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-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
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-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

timeout-value	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-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、コンソール ロギングを有効にする例を示します。

```
cisco-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
	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-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** 分 | **reason** *reason-string*}]

構文の説明

at	特定の日時に 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、10 分後に AP をリロードする例を示します。

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

terminal

端末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、ターミナルの行数を 50 に設定する例を示します。

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。