CHAPTER 13

Cisco CleanAir の設定

この章の内容は、次のとおりです。

CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題に予防的に対応するスペクトラム インテリジェンス ソリューションです。この機能を使用すると、共有スペクトラムの全ユーザを確認できます（ネイティブ デバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルを変更して干渉を受けないようにすることができます。

Cisco CleanAir システムは、CleanAir 対応のアクセス ポイント、コントローラ、WCS で構成されます。アクセス ポイントでは工業、科学、医療用（ISM）帯域で動作しているすべてのデバイスの情報を収集し、これらの情報を潜在的な干渉源として特定および評価し、コントローラに転送します。コントローラはアクセス ポイントを制御し、スペクトラム データを収集し、これらの情報を要求に応じて WCS またはシスコ モビリティ サービス エンジン（MSE）に転送します。コントローラにはローカルなユーザ インターフェイスがあり、CleanAir の基本的な機能を設定することや、基本的なスペクトラム情報を表示することができます。WCS には高度なユーザ インターフェイスがあり、Cisco CleanAir の機能の設定、情報の表示、記録の保持などを行えます。MSE は基本的な機能セットに対するオプションですが、非 Wi-Fi 干渉デバイスの位置の追跡など、高度な機能を使用するためには必須です。

Cisco CleanAir では、ライセンス不要の帯域で動作している各デバイスについて、その種類、場所、ワイヤレス ネットワークに与える影響の程度、取るべき対策を提示します。これによって RF がシンプルになり、管理者が RF のエキスパートである必要がなくなります。

ワイヤレス LAN システムは、ライセンスが不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。この無線周波数（RF）の干渉に関する問題は、Cisco Unified Wireless Network に Cisco CleanAir 機能を組み込むことによって解決できます。

Cisco CleanAir システムにおけるコントローラの役割

Cisco CleanAir システムにおいて、コントローラは次のような処理を実行します。

- アクセス ポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイスを提供する（GUI、CLI、SNMP）。
- スペクトラム データを表示する。
- アクセス ポイントから電波品質レポートを収集して処理し、電波品質データベースに保存する。電波品質レポート（AQR）には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が記載されます。また CleanAir システムでは、干渉の種類ごとのレポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセス ポイントから干渉デバイス レポート（IDR）を収集して処理し、干渉デバイス データベースに保存する。
- スペクトラム データを WCS および MSE に転送する。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir では、干渉を検出し、その干渉の発生箇所や重大度をレポートし、さまざまな緩和方法を推奨することができます。これらの緩和方法には、Persistent Device Avoidance（PDA）と Event Driven RRM（EDRRM）という 2 つの方法があります。

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャネル計画の割り当てに使用するノイズの測定値は、一部のクライアント デバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。
- 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、その場所や WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。CleanAir では、次の 2 種類の干渉イベントが一般的です。

- 永続的干渉
- 突発的干渉

永続的干渉イベントは、本質的に固定型のデバイスから発生し、断続的ではあるものの、干渉が大規模に反復して繰り返されるものを指します。たとえば、休憩室に設置してある電子レンジの場合を考えます。このような装置が動作するのは、1 回に付き 1 ～ 2 分程度です。しかし一旦動作すると、ワイヤレス ネットワークと、関係するクライアントのパフォーマンスに非常に大きな影響が生じます。Cisco

CleanAir を使用すると、電子レンジなどの装置を無秩序なノイズとしてではなく明確に識別できるようになります。また、その装置によって影響を受ける帯域の部分を正確に特定できます。そして、その設置場所も特定できるため、最も大きな影響を受けるアクセス ポイントを判別することができます。そして、この情報を使用して RRM に指示し、範囲内にあるアクセス ポイントに対してこの干渉源を避けるようなチャネル計画を選択させることができます。この干渉は 1 日の大部分にわたって発生するものではないため、既存の RF 管理アプリケーションによって、影響を受けるアクセス ポイントのチャネルの再変更が試みられている場合もあります。しかし、永続的デバイスの回避は、干渉源が周期的に検出されて永続的な状態が新たに発生する限り影響があり続けるという点で独特です。Cisco CleanAir システムでは、電子レンジが存在することを認識し、それを将来のすべての計画に取り込みます。電子レンジまたはその近くのアクセス ポイントを移動させた場合は、このアルゴリズムによって RRM が自動的に更新されます。

（注）　Event Driven RRM（EDRRM）は、Cisco CleanAir 対応でローカル モードにあるアクセス ポイントによってのみ動作します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir の Event Driven RRM（EDRRM）機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Bluetooth デバイスの場合、Cisco CleanAir 対応のアクセス ポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetooth デバイスには、さまざまなパワー セーブ モードがあります。たとえば、接続されたデバイス間でデータまたは音声がストリーム化されている最中に干渉が検出されます。

永続的デバイス

屋外型ブリッジや電子レンジなどの一部の干渉デバイスは、必要な場合にのみ送信を行います。通常の RF 管理基準では短時間の定期的な動作はたいていは検出されないままになるため、このようなデバイスによってローカルの WLAN に対する大規模な干渉が引き起こされる可能性があります。CleanAir を使用すると、RRM DCA アルゴリズムによって、この影響が検出、測定、登録、記録され、DCA アルゴリズムが調整されます。このため、その干渉源と同じ場所にあるチャネル計画によって、その永続的デバイスによって影響を受けるチャネルの使用が最小限に留められます。Cisco CleanAir では、永続的デバイスの情報を検出してコントローラに保存し、チャネルの干渉の緩和に利用します。

永続的デバイスの検出

CleanAir 対応でモニタ モードのアクセス ポイントでは、設定されているすべてのチャネルで永続的デバイスに関する情報を収集して、この情報をコントローラに保存します。ローカル/ブリッジ モードの AP は、稼働チャネルでのみ干渉デバイスを検出します。

永続的デバイスの伝搬

ローカル モードまたはモニタ モードのアクセス ポイントによって検出された永続的デバイス情報は、同じコントローラに接続されている隣接アクセス ポイントに伝搬されます。この機能により、永続的デバイスの制御や回避がより適切に行えるようになります。CleanAir 対応アクセス ポイントによって検出された永続的デバイスは、CleanAir 非対応の隣接アクセス ポイントにも伝搬されるため、チャネル選択の品質が向上します。

ガイドラインと制限事項

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- Local：このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャネルだけに関する電波品質と干渉検出のレポートが作成されます。
- FlexConnect：FlexConnect アクセス ポイントがコントローラに接続されているとき、その Cisco CleanAir 機能はローカル モードと同じになります。
- Monitor：Cisco CleanAir がモニタ モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャネルに関する電波品質と干渉検出のレポートが作成されます。

  次のオプションを使用できます。

  - All：すべてのチャネル
  - DCA：DCA リストによって管理されるチャネル選択
  - Country：規制区域内で合法なすべてのチャネル

（注） AP が 2 台あり、一方が FlexConnect モード、もう一方がモニタ モードであると仮定します。また、802.1x 認証に対する EAP 攻撃を有効にしたプロファイルを作成済みと仮定します。Airmagnet（AM）ツールは、さまざまな種類の攻撃を発生させることのできるツールですが、有効な AP MAC アドレスおよび STA MAC アドレスを指定していても、攻撃の発生に失敗します。しかし、AM ツールで AP MAC アドレスと STA MAC アドレスを交換すると（つまり、AP MAC アドレスを STA MAC フィールドに指定し、STA MAC アドレスを AP MAC フィールドに指定すると）、攻撃を発生させることができ、モニタ モードの AP でこれを検出できるようになります。

（注） アクセス ポイントは WCS では AQ HeatMap に参加しません。

- **SE-Connect**：このモードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラム データを表示および分析できるようになります。Spectrum Expert アプリケーションは、コントローラをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラム データがコントローラに提供されません。これに加えてスペクトラム インテリジェンスを実行すると、アクセス ポイントから他にデータが提供されるようになります。Spectrum Expert のコンソール接続を確立する手順については、「Spectrum Expert の接続の設定」（P.13-25）を参照してください。
- Cisco 2100 シリーズのコントローラとコントローラ ネットワーク モジュールでは、最大 75 のデバイス クラスタ（1 つまたは複数の無線によって検出された一意の干渉デバイス）と、最大 300 のデバイス レコード（1 つの無線によって検出された干渉デバイスについての情報）をサポートしてい

ます。Cisco 4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G ワイヤレス LAN コントローラ スイッチでは、最大 750 のデバイス クラスタと、最大 3,000 のデバイス レコードをサポートしています。Cisco 5500 シリーズのコントローラでは、最大 2,500 のデバイス クラスタと、最大 10,000 のデバイス レコードをサポートしています。

- スペクトラム データの処理に必要な電力量によって、Cisco CleanAir のモニタリングに使用できるモニタ モードのアクセス ポイントの数が制限されます。Cisco CleanAir システムでは、Cisco 2100 シリーズのコントローラとコントローラ ネットワーク モジュールで、最大 6 台のモニタ モードのアクセス ポイントをサポートします。また、Cisco 4400 シリーズのコントローラ、Catalyst 3750G ワイヤレス LAN コントローラ スイッチ、およびそれぞれの Cisco WiSM コントローラでは、最大 25 台のモニタ モードのアクセス ポイントをサポートします。サポートできるモニタ モードのアクセス ポイントの数は、Cisco 5500 および Flex 7500 シリーズのコントローラでサポートされているアクセス ポイントの最大数と同じです。この制限は、Cisco CleanAir の機能だけに影響します。
- モニタ モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは Radio Resource Management（RRM）計画から除外され、隣接アクセス ポイントのリストに含まれません。IDR クラスタリングは、コントローラがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセス ポイントから関係する干渉デバイスを検出する機能を使用できるのは、モニタ モードのアクセス ポイント間に限られます。
- Spectrum Expert（SE）の接続機能は、ローカル、FlexConnect、ブリッジ、および監視の各モードでサポートされています。アクセス ポイントは、Spectrum Expert に現在のチャネルに関するスペクトラム情報だけを提供します。ローカル、FlexConnect、およびブリッジの各モードでは、スペクトラム データは現在アクティブなチャネル（複数可）に対して有効です。またモニタ モードでは、共通の監視対象チャネル リストを使用できます。アクセス ポイントは AQ（電波品質）レポートと IDR（干渉デバイス レポート）をコントローラに送り続け、現在のモードに応じて通常の処理を実行します。スニファおよび不正検出のアクセス ポイント モードは、CleanAir のスペクトラム モニタリングのすべてのタイプと互換性がありません。
- コントローラでは、サポートできるモニタ モードの AP の数に制限があります。これは、モニタ モードの AP によってすべてのチャネルのデータが保存されるためです。
- SE Connect モードでは、Cisco 2100 または 2500 シリーズ コントローラの物理ポートにアクセス ポイントを直接接続しないでください。
- Spectrum Expert（Windows XP ラップトップ クライアント）と AP 間では ping が可能である必要があります。不可能な場合は正しく動作しません。

Cisco CleanAir の設定

この項では、次のトピックを扱います。

- 「コントローラでの Cisco CleanAir の設定」（P.13-5）
- 「アクセス ポイントに対する Cisco CleanAir の設定」（P.13-12）

コントローラでの Cisco CleanAir の設定

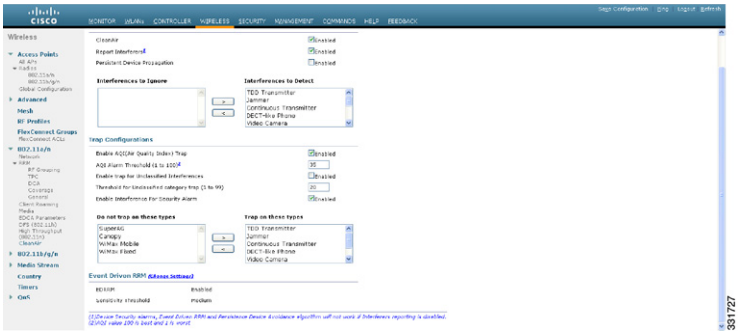
この項では、次のトピックを扱います。

- 「コントローラでの Cisco CleanAir の設定（GUI）」（P.13-6）
- 「コントローラでの Cisco CleanAir の設定（CLI）」（P.13-8）

コントローラでの Cisco CleanAir の設定（GUI）

ステップ 1　[Wireless] > [802.11a/n] または [802.11b/g/n] > [CleanAir] の順に選択して、[802.11a（または 802.11b）> CleanAir] ページを開きます。

図 13-1　[802.11a（または 802.11b）> CleanAir]



ステップ 2　[CleanAir] チェックボックスを選択して、802.11a/n または 802.11b/g/n ネットワークで Cisco CleanAir の機能を有効にします。コントローラがスペクトラム干渉を検出しないようにするには、これを選択解除します。デフォルトでは、この値は選択されていません。

ステップ 3　[Report Interferers] チェックボックスを選択して、Cisco CleanAir システムで検出した干渉源をレポートできるようにします。コントローラが干渉源をレポートしないようにするには、これを選択解除します。デフォルト値ではオンになっています。

（注）　[Report Interferers] が無効の場合は、デバイス セキュリティ アラーム、イベント駆動型アラーム、および Persistent Device Avoidance（PDA）アルゴリズムは機能しません。

ステップ 4　[Persistent Device Propagation] チェックボックスを選択して、CleanAir によって検出された永続的デバイスの情報の伝搬を有効にします。永続的デバイスの伝搬を有効にすると、同じコントローラに接続されている隣接アクセス ポイントに永続的デバイスの情報を伝播させることができます。永続型の干渉源は、検出されない場合でも、常にいずれかに存在し、WLAN の動作に干渉しています。

ステップ 5　Cisco CleanAir システムによって検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源は [Interferences to Ignore] ボックスに表示されるようにします。[>] ボタンと [<] ボタンを使用して、2 つのボックス間で干渉源を移動させます。デフォルトでは、すべての干渉源が検出されます。選択できる干渉源の候補には、次のものがあります。

- [Bluetooth Paging Inquiry]：Bluetooth の検出（802.11b/g/n のみ）
- [Bluetooth Sco Acl]：Bluetooth リンク（802.11b/g/n のみ）
- [Generic DECT]：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話
- [Generic TDD]：時分割複信（TDD）トランスミッタ
- [Generic Waveform]：連続トランスミッタ

- [Jammer]：電波妨害デバイス
- [Microwave]：電子レンジ（802.11b/g/n のみ）
- [Canopy]：Canopy ブリッジ デバイス
- [Spectrum 802.11 FH]：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
- [Spectrum 802.11 inverted]：スペクトラム反転 Wi-Fi 信号を使用するデバイス
- [Spectrum 802.11 non std channel]：非標準の Wi-Fi チャネルを使用するデバイス
- [Spectrum 802.11 SuperG]：802.11 SuperAG デバイス
- [Spectrum 802.15.4]：802.15.4 デバイス（802.11b/g/n のみ）
- [Video Camera]：アナログ ビデオ カメラ
- [WiMAX Fixed]：WiMAX 固定デバイス（802.11a/n のみ）
- [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ）
- [XBox]：Microsoft Xbox（802.11b/g/n のみ）

（注）　コントローラにアソシエートされているアクセス ポイントは、[Interferences to Detect] ボックスに表示されている干渉源に関する干渉レポートだけを送信します。この機能によって、対象としたくない干渉源のほか、ネットワークにフラッディングを発生させたり、コントローラや WCS にパフォーマンスの問題を引き起こす可能性のある干渉源をフィルタで除去することができます。フィルタリングによって、システムが通常のパフォーマンス レベルに戻ることができます。

ステップ 6　Cisco CleanAir のアラームを次のように設定します。

a. [Enable AQI (Air Quality Index) Trap] チェックボックスを選択して、電波品質アラームのトリガーを有効にします。この機能を無効にするには、このボックスを選択解除します。デフォルト値ではオンになっています。

b. ステップ a で [Enable AQI Trap] チェックボックスを選択した場合は、電波品質アラームをトリガーするしきい値を指定するために、1 ～ 100 の範囲の値を [AQI Alarm Threshold] テキスト ボックスに入力します。電波品質がこのしきい値のレベルを下回ると、アラームがトリガーされます。1 という値は最低の電波品質を、100 は最高の電波品質を表します。デフォルト値は 35 です。

- [AQI Alarm Threshold (1 to 100)] に任意の値を設定します。電波品質がここに設定した値を下回ると、アラームが発生します。デフォルトは 35 です。有効な範囲は 1 ～ 100 です。
- [Enable trap for Unclassified Interferences] チェックボックスを選択して、[AQI Alarm Threshold] で指定した重大度しきい値を超える未分類の干渉が検出されたときに AQI アラームが発生するようにします。未分類の干渉とは、検出されたものの、識別可能な干渉のタイプに該当しないものです。
- [Threshold for Unclassified category trap (1 to 99)] に値を入力します。有効な範囲は 1 ～ 99 です。デフォルトは 20 です。これは未分類の干渉のカテゴリに対する重大度の指標となるしきい値です。

c. [Enable Interference Type Trap] チェックボックスを選択して、指定したデバイス タイプがコントローラによって検出されたときに干渉源アラームをトリガーするようにします。この機能を無効にするには、このボックスを選択解除します。デフォルト値ではオンになっています。

d. 干渉アラームをトリガーする必要のある干渉源が [Trap on These Types] ボックスに表示され、干渉アラームをトリガーする必要のない干渉源は [Do Not Trap on These Types] ボックスに表示されるようにします。[>] ボタンと [<] ボタンを使用して、2 つのボックス間で干渉源を移動させます。デフォルトでは、すべての干渉源で干渉アラームがトリガーされます。

たとえば、コントローラが電波妨害デバイスを検出したときにアラームを送信するようにするには、[Enable Interference Type Trap] チェックボックスを選択して、電波妨害デバイスを [Trap on These Types] ボックスに移動させます。

ステップ 7　[Apply] をクリックして、変更を確定します。

ステップ 8　Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、Event Driven Radio Resource Management（RRM）の実行をトリガーするよう設定します。

a. [EDRRM] フィールドを見て、Event Driven RRM（EDRRM）の現在の状態を確認します。これが有効である場合は、[Sensitivity Threshold] フィールドを見て、イベント駆動型 RRM が起動されるしきい値レベルを確認します。

b. イベント駆動型 RRM の現在の状態や感度のレベルを変更する場合は、[Change Settings] をクリックします。[802.11a（または 802.11b）> RRM > Dynamic Channel Assignment (DCA)] ページが表示されます。

c. [EDRRM] チェックボックスを選択して、アクセス ポイントがあるレベルの干渉を検出した場合に RRM の実行がトリガーされるようにします。この機能を無効にするには選択解除します。デフォルト値ではオンになっています。

d. ステップ c で [EDRRM] チェックボックスを選択した場合は、[Sensitivity Threshold] ドロップダウン リストから [Low]、[Medium]、[High]、または [Custom] を選択して、RRM をトリガーするしきい値を指定します。アクセス ポイントに対する干渉が発生し、対応する AQ の指標がこのしきい値レベルを下回ると、RRM によってローカル チャネルの割り当てが開始されます。また、可能であればネットワークのパフォーマンスが向上するように、影響を受けているアクセス ポイント無線のチャネルが変更されます。[Low] は、この環境内で変更が行われる感度を下げることを表し、[High] はこの感度を上げることを表します。

EDRRM の感度のしきい値に [Custom] を選択した場合は、[Custom Sensitivity Threshold] フィールドにしきい値を設定する必要があります。デフォルトの感度は 35 です。

EDRRM AQ のしきい値は、感度が [Low] の場合は 35、[Medium] の場合は 50、[High] の場合は 60 です。

デフォルトでは [Medium] です。

e. [Apply] をクリックして、変更を確定します。

ステップ 9　[Save Configuration] をクリックして、変更を保存します。

コントローラでの Cisco CleanAir の設定（CLI）

ステップ 1　次のコマンドを入力して、802.11a/n または 802.11b/g/n ネットワークで Cisco CleanAir の機能を設定します。

config {802.11a | 802.11b} cleanair {enable | disable} *all*

この機能を無効にすると、コントローラはスペクトラム データをまったく受信しなくなります。デフォルト値は enable です。

ステップ 2　次のコマンドを入力して、干渉検出を設定し、Cisco CleanAir システムで検出する必要がある干渉源を指定します。

config {802.11a | 802.11b} cleanair device {enable | disable} *type*

ここで、*type* には次のいずれかを選択します。

- **802.11-fh**：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
- **802.11-inv**：スペクトラム反転 Wi-Fi 信号を使用するデバイス

- **802.11-nonstd**：非標準の Wi-Fi チャネルを使用するデバイス
- **802.15.4**：802.15.4 デバイス（802.11b/g/n のみ）
- **all**：すべての干渉デバイス タイプ（これがデフォルト値です）
- **bt-discovery**：Bluetooth の検出（802.11b/g/n のみ）
- **bt-link**：Bluetooth リンク（802.11b/g/n のみ）
- **canopy**：Canopy デバイス
- **cont-tx**：連続トランスミッタ
- **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話
- **jammer**：電波妨害デバイス
- **mw-oven**：電子レンジ（802.11b/g/n のみ）
- **superag**：802.11 SuperAG デバイス
- **tdd-tx**：時分割複信（TDD）トランスミッタ
- **video camera**：アナログ ビデオ カメラ
- **wimax-fixed**：WiMAX 固定デバイス
- **wimax-mobile**：WiMAX モバイル デバイス
- **xbox**：Microsoft Xbox（802.11b/g/n のみ）

（注） コントローラにアソシエートされているアクセス ポイントは、このコマンドで指定された干渉の種類に対してのみ干渉レポートを送信します。この機能によって、ネットワークにフラッディングを発生させたり、コントローラや WCS にパフォーマンスの問題を引き起こす可能性のある干渉源をフィルタで除去することができます。フィルタリングによって、システムが通常のパフォーマンス レベルに戻ることができます。

ステップ 3　次のコマンドを入力して、電波品質アラームのトリガーを設定します。

config {802.11a | 802.11b} cleanair alarm air-quality {enable | disable}

デフォルト値は有効（enable）です。

ステップ 4　次のコマンドを入力して、電波品質アラームをトリガーするしきい値を指定します。

config {802.11a | 802.11b} cleanair alarm air-quality threshold *threshold*

threshold の値は、1 ～ 100（両端の値を含む）です。電波品質がこのしきい値のレベルを下回ると、アラームがトリガーされます。1 という値は最低の電波品質を、100 は最高の電波品質を表します。デフォルト値は 35 です。

ステップ 5　次のコマンドを入力して、干渉源アラームのトリガーを有効にします。

config {802.11a | 802.11b} cleanair alarm device {enable | disable}

デフォルト値は enable です。

ステップ 6　次のコマンドを入力して、アラームをトリガーする干渉源を指定します。

config {**802.11a** | **802.11b**} **cleanair alarm device** *type* {**enable** | **disable**}

ここで、*type* には次のいずれかを選択します。

- **802.11-fh**：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
- **802.11-inv**：スペクトラム反転 Wi-Fi 信号を使用するデバイス
- **802.11-nonstd**：非標準の Wi-Fi チャネルを使用するデバイス

- **802.15.4**：802.15.4 デバイス（802.11b/g/n のみ）
- **all**：すべての干渉デバイス タイプ（これがデフォルト値です）
- **bt-discovery**：Bluetooth の検出（802.11b/g/n のみ）
- **bt-link**：Bluetooth リンク（802.11b/g/n のみ）
- **canopy**：Canopy デバイス
- **cont-tx**：連続トランスミッタ
- **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話
- **jammer**：電波妨害デバイス
- **mw-oven**：電子レンジ（802.11b/g/n のみ）
- **superag**：802.11 SuperAG デバイス
- **tdd-tx**：時分割複信（TDD）トランスミッタ
- **video camera**：アナログ ビデオ カメラ
- **wimax-fixed**：WiMAX 固定デバイス
- **wimax-mobile**：WiMAX モバイル デバイス
- **xbox**：Microsoft Xbox（802.11b/g/n のみ）

ステップ 7　次のコマンドを入力して、未分類のデバイスに対する電波品質アラームのトリガーを設定します。

config {802.11a | 802.11b} cleanair alarm unclassified {*enable* **|** *disable***}**

ステップ 8　次のコマンドを入力して、未分類のデバイスに対して電波品質アラームをトリガーするしきい値を指定します。

config {802.11a | 802.11b} cleanair alarm unclassified threshold *threshold*

threshold の値は、1 ～ 99 バイト（両端の値を含む）です。電波品質がこのしきい値のレベルを下回ると、アラームがトリガーされます。1 という値は最低の電波品質を、100 は最高の電波品質を表します。デフォルト値は 35 です。

ステップ 9　次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、Event Driven Radio Resource Management（RRM）の実行がトリガーされるよう設定します。

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}：Event Driven RRM（EDRRM）を有効または無効にします。デフォルト値では無効になっています。
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event sensitivity {low** | **medium | high | custom**}：RRM をトリガーするしきい値を指定します。アクセス ポイントに対してしきい値レベルを上回るレベルの干渉が発生すると、RRM によってローカルの動的チャネル割り当て（DCA）の実行が開始され、可能であればネットワークのパフォーマンスが向上するように、影響を受けているアクセス ポイント無線のチャネルが変更されます。low は、この環境内で変更が行われる感度を下げることを表し、high はこの感度を上げることを表します。感度の値に custom を設定して、任意のレベルを選択することもできます。デフォルトは medium です。
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event sensitivity threshold** *thresholdvalue*：感度のしきい値を custom に設定した場合は、しきい値を設定する必要があります。デフォルトは 35 です。

ステップ 10　次のコマンドを入力して、永続的デバイスの伝搬を有効にします。

config advanced {**802.11a | 802.11b**} **channel pda-prop** {*enable* | *disable*}

ステップ 11　次のコマンドを入力して、変更を保存します。

save config

ステップ 12　次のコマンドを入力して、802.11a/n または 802.11b/g/n ネットワークに対する Cisco CleanAir の設定を確認します。

show {802.11a | 802.11b} cleanair config

以下に類似した情報が表示されます。

```
(Cisco Controller) >show 802.11a cleanair config

Clean Air Solution..............................  Disabled
Air Quality Settings:
    Air Quality Reporting.......................  Enabled
    Air Quality Reporting Period (min)..........  15
    Air Quality Alarms..........................  Enabled
      Air Quality Alarm Threshold...............  35
      Unclassified Interference.................  Disabled
      Unclassified Severity Threshold...........  20
Interference Device Settings:
    Interference Device Reporting...............  Enabled
    Interference Device Types:
        TDD Transmitter.........................  Enabled
        Jammer..................................  Enabled
        Continuous Transmitter..................  Enabled
        DECT-like Phone.........................  Enabled
        Video Camera............................  Enabled
        WiFi Inverted...........................  Enabled
        WiFi Invalid Channel....................  Enabled
        SuperAG.................................  Enabled
        Canopy..................................  Enabled
        WiMax Mobile............................  Enabled
       WiMax Fixed.............................. Enabled
Interference Device Alarms.................... Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.........................  Disabled
        Jammer..................................  Enabled
        Continuous Transmitter..................  Disabled
        DECT-like Phone.........................  Disabled
        Video Camera............................  Disabled
        WiFi Inverted...........................  Enabled
        WiFi Invalid Channel....................  Enabled
        SuperAG.................................  Disabled
        Canopy..................................  Disabled
        WiMax Mobile............................  Disabled
        WiMax Fixed.............................  Disabled
Additional Clean Air Settings:
    CleanAir ED-RRM State.......................  Disabled
    CleanAir ED-RRM Sensitivity.................  Medium
    CleanAir ED-RRM Custom Threshold............  50
    CleanAir Persistent Devices state...........  Disabled
    CleanAir Persistent Device Propagation.......  Enabled
```

ステップ 13　次のコマンドを入力して、802.11a/n または 802.11b/g/n ネットワークに対する Event Driven RRM（EDRRM）の設定を確認します。

show advanced {802.11a | 802.11b} *channel*

以下に類似した情報が表示されます。

```
Automatic Channel Assignment
  Channel Assignment Mode.....................  AUTO
  Channel Update Interval.....................  600 seconds [startup]
  Anchor time (Hour of the day)...............  0
  Channel Update Contribution.................  SNI
  CleanAir Event-driven RRM option............  Enabled
```

```
CleanAir Event-driven RRM sensitivity...... Medium
```

アクセス ポイントに対する Cisco CleanAir の設定

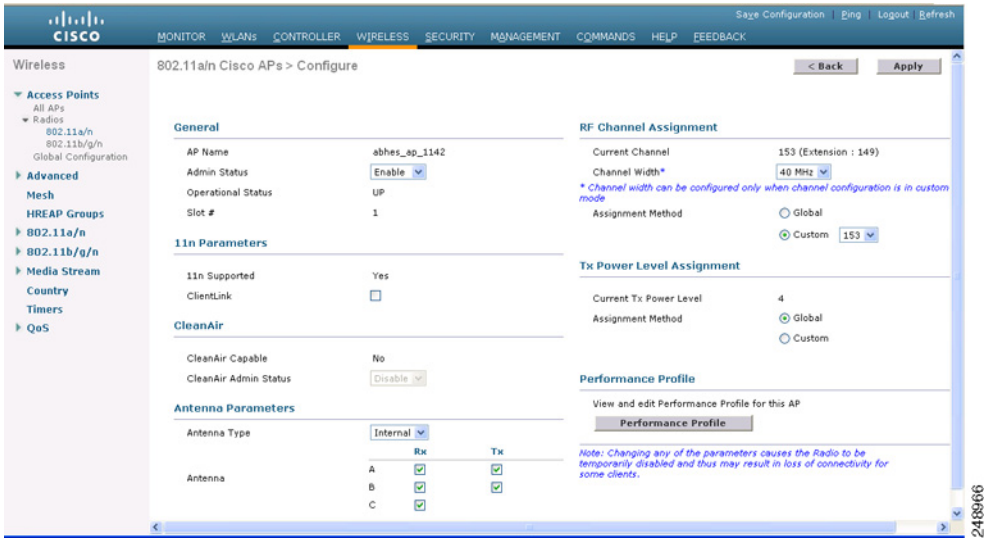
この項では、次のトピックを扱います。

アクセス ポイントに対する Cisco CleanAir の設定（GUI）

コントローラの GUI を使用して、特定のアクセスポイントに Cisco CleanAir の機能を設定するには、次の手順を実行してください。

ステップ 1　[Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。

図 13-2　[802.11a/n Cisco APs > Configure] ページ



ステップ 2　カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて [Configure] をクリックします。[802.11a/n（または 802.11b/g/n）Cisco APs > Configure] ページが表示されます。

[CleanAir Capable] フィールドには、このアクセス ポイントが CleanAir の機能に対応しているかどうかが表示されます。対応している場合は、次の手順に進み、このアクセス ポイントに対して CleanAir を有効または無効にします。アクセス ポイントが CleanAir の機能に対応していない場合は、このアクセス ポイントに対して CleanAir を有効にすることはできません。

（注）　デフォルトでは、Cisco CleanAir の機能は無線に対して有効になっています。

ステップ 3　[CleanAir Status] ドロップダウン リストから [Enable] を選択して、このアクセス ポイントに対して Cisco CleanAir の機能をイネーブルにします。このアクセス ポイントで CleanAir の機能を無効にするには、[Disable] を選択します。デフォルト値は [Enable] です。この設定は、このアクセス ポイントに対するグローバルな CleanAir の設定より優先します。

[Number of Spectrum Expert Connections] テキスト ボックスには、このアクセス ポイント無線に現在接続している Spectrum Expert アプリケーションの数が表示されます。アクティブな接続は最大で 3 つまで可能です。

ステップ 4　[Apply] をクリックして、変更を確定します。

ステップ 5　[Save Configuration] をクリックして、変更を保存します。

ステップ 6　[Back] をクリックして、[802.11a/n（または 802.11b/g/n）Radios] ページに戻ります。

ステップ 7　[802.11a/n（または 802.11b/g/n）Radios] ページの [CleanAir Status] テキスト ボックスを見て、各アクセス ポイント無線の Cisco CleanAir のステータスを確認します。

Cisco CleanAir のステータスは次のいずれかになります。

- [UP] : アクセス ポイント無線に対するスペクトラム センサーが現在正常に動作中です（エラー コード 0）。
- [DOWN] : アクセス ポイント無線に対するスペクトラム センサーは、エラーが発生したために現在動作していません。最も可能性の高いエラーの原因は、アクセス ポイント無線が無効になっていることです（エラー コード 8）。このエラーを修正するには、無線を有効にしてください。
- [ERROR] : アクセス ポイント無線に対するスペクトラム センサーがクラッシュしており（エラー コード 128）、この無線に対する CleanAir のモニタリングが機能していません。このエラーが発生した場合は、アクセス ポイントをリブートしてください。エラーが引き続き発生する場合は、この無線に対して Cisco CleanAir の機能を無効にすることもできます。
- [N/A] : このアクセス ポイント無線は Cisco CleanAir の機能に対応していません。

（注）　フィルタを作成して、Cisco CleanAir の特定のステータス（UP、DOWN、ERROR、N/A など）を持つアクセス ポイント無線だけを表示する [802.11a/n Radios] ページや [802.11b/g/n Radios] ページを作成することもできます。この機能は、アクセス ポイント無線のリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。フィルタを作成するには、[Change Filter] をクリックして [Search AP] ダイアログボックスを開き、[CleanAir Status] チェックボックスを 1 つ以上選択して、[Find] をクリックします。検索基準に一致するアクセス ポイント無線のみが [802.11a/n Radios] ページまたは [802.11b/g/n Radios] ページに表示されます。また、ページ上部の [Current Filter] パラメータには、リストの作成に使用したフィルタが表示されます（たとえば、CleanAir Status: UP）。

アクセス ポイントに対する Cisco CleanAir の設定（CLI）

ステップ 1　次のコマンドを入力して、特定のアクセスポイントに Cisco CleanAir の機能を設定します。

config {**802.11a** | **802.11b**} **cleanair** {**enable** | **disable**} *Cisco_AP*

ステップ 2　次のコマンドを入力して、変更を保存します。

save config

ステップ 3　次のコマンドを入力して、802.11a/n または 802.11b/g/n ネットワークにあるアクセス ポイントの Cisco CleanAir の設定を確認します。

show ap config {802.11a | 802.11b} *Cisco_AP*

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Disabled
       Spectrum Sensor State.................. Configured (Error code = 0)
```

（注）　スペクトラム管理機能の状態とスペクトラム センサーの状態についての説明は、「アクセス ポイントに対する Cisco CleanAir の設定（GUI）」の「*ステップ 7*」を参照してください。

干渉デバイスのモニタリング

この項では、次のトピックを扱います。

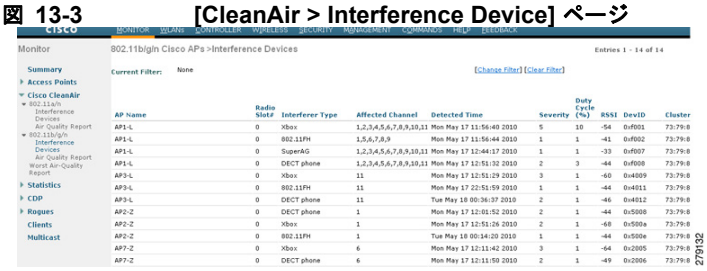
干渉デバイスをモニタリングするための前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

干渉デバイスのモニタリング（GUI）

ステップ 1　[Monitor] > [Cisco CleanAir] > [802.11a/n] または [802.11b/g] > [Interference Devices] を選択して、[CleanAir > Interference Devices] ページを開きます。

図 13-3　[CleanAir > Interference Device] ページ



このページには、次の情報が表示されます。

- [AP Name]：干渉デバイスが検出されたアクセス ポイントの名前
- [Radio Slot #]：無線が取り付けられているスロット。
- [Interferer Type]：干渉源のタイプ。
- [Affected Channel]：デバイスから影響を受けているチャネル。
- [Detected Time]：干渉が検出された時刻。
- [Severity]：干渉デバイスの重大度の指標。
- [Duty Cycle (%)]：干渉デバイスが動作している間の時間の割合。
- [RSSI]：アクセス ポイントの受信信号強度表示（RSSI）。
- [DevID]：一意に識別できる干渉デバイスのデバイス識別番号。
- [ClusterID]：デバイスのタイプを一意に識別できるクラスタ識別番号。

  CleanAir 対応のアクセス ポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラム センサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラム データベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタ ID を長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

  たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされるようにします。この処理によってユーザ レコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

ステップ 2　ある基準に基づいて干渉デバイスに関する情報を表示するには、[Change Filter] をクリックします。

ステップ 3　フィルタを削除して、アクセス ポイントのリスト全体を表示するには、[Clear Filter] をクリックします。

次に示すパラメータに基づいて干渉デバイスのリストを表示するフィルタを作成することができます。

- [Cluster ID]：クラスタ ID に基づいてフィルタリングを行うには、このチェックボックスをクリックして、このフィールドの隣にあるテキスト ボックスにクラスタ ID を入力します。
- [AP Name]：アクセス ポイントの名前に基づいてフィルタリングを行うには、このチェックボックスをクリックして、このフィールドの隣にあるテキスト ボックスにアクセス ポイントの名前を入力します。
- [Interferer Type]：干渉デバイスのタイプに基づいてフィルタリングを行うには、このチェックボックスをクリックして、オプションから干渉デバイスを選択します。

  次のいずれかの干渉デバイスを選択してください。
  - BT Link
  - MW Oven
  - 802.11 FH
  - BT Discovery
  - TDD Transmit
  - Jammer
  - Continuous TX
  - DECT Phone
  - Video Camera
  - 802.15.4
  - WiFi Inverted
  - WiFi Inv.Ch
  - SuperAG
  - Canopy
  - XBox
  - WiMax Mobile
  - WiMax Fixed
  - WiFi ACI
  - Unclassified
- Activity Channels
- Severity
- Duty Cycle (%)
- RSSI

ステップ 4　[Find] をクリックして、変更を適用します。

現在選択されているフィルタ パラメータは、[Current Filter] フィールドに表示されます。

干渉デバイスのモニタリング（CLI）

この項では、802.11a/n または 802.11b/g/n の無線帯域に対する干渉デバイスのモニタリングに使用するコマンドについて説明します。

アクセス ポイントによる干渉源の検出

802.11a/n または 802.11b/g/n 無線帯域について、特定のアクセス ポイントによって検出されたすべての干渉源について情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair device ap *Cisco_AP*

以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No  ClusterID          DevID  Type       AP Name      ISI  RSSI  DC   Channel
--- ------------------ ------ ---------- ------------- ---- ----- ---- -------------
1   c2:f7:40:00:00:03  0x8001 DECT phone CISCO_AP3500 1    -43   3   149,153,157,161
3   c2:f7:40:00:00:03  0x8005 Canopy     CISCO_AP3500 2    -62   2   153,157,161,165
```

CleanAir 対応のアクセス ポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラム センサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラム データベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタ ID を長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされるようにします。この処理によってユーザ レコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

デバイスのタイプによる干渉源の検出

802.11a/n または 802.11b/g/n 無線帯域について、特定のデバイス タイプのすべての干渉源の情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair device type *type*

以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
  * indicates cluster center device

No  ClusterID          DevID  Type        AP Name      ISI  RSSI DC   Channel
--- ------------------ ------ ------------ ------------ ---- ----- --- --------------
1   b4:f7:40:00:00:03 0x4185 DECT-like (26) CISCO_AP35001  -58   3  153,157,161,165
```

永続的干渉源の検出

802.11a/n または 802.11b/g/n 無線帯域について、特定のアクセス ポイントに対する永続的干渉源の一覧を表示するには、次のコマンドを入力します。

show ap auto-rf {802.11a | 802.11b} *Cisco_AP*

```
Information similar to the following appears:
Number Of Slots.................................. 2
AP Name.......................................... AP1-L
MAC Address...................................... c4:7d:4f:3a:07:1e
  Slot ID........................................ 1
  Radio Type..................................... RADIO_TYPE_80211a
  Sub-band Type.................................. All
  Noise Information
    Noise Profile................................ PASSED
    Channel 34..................................  -97 dBm
    Channel 36..................................  -90 dBm
    Channel 38..................................  -97 dBm
Interference Information
    Interference Profile......................... PASSED
    Channel 34................................... -128 dBm @  0 % busy
    Channel 36................................... -128 dBm @  0 % busy
    Channel 38................................... -128 dBm @  0 % busy
    Channel 40................................... -128 dBm @  0 % busy
Load Information
    Load Profile................................. PASSED
    Receive Utilization.......................... 0 %
    Transmit Utilization......................... 0 %
    Channel Utilization.......................... 0 %
    Attached Clients............................. 0 clients
  Coverage Information
    Coverage Profile............................. PASSED
    Failed Clients............................... 0 clients
  Client Signal Strengths
    RSSI -100 dbm................................ 0 clients
    RSSI  -92 dbm................................ 0 clients
    RSSI  -84 dbm................................ 0 clients
Client Signal To Noise Ratios
    SNR    0 dB.................................. 0 clients
    SNR    5 dB.................................. 0 clients
    SNR   10 dB.................................. 0 clients
    SNR   15 dB.................................. 0 clients
Nearby APs
    AP c4:7d:4f:52:cf:a0 slot 1..................  -36 dBm on 149 (10.10.10.27)
    AP c4:7d:4f:53:1b:50 slot 1..................  -10 dBm on 149 (10.10.10.27)
Radar Information
  Channel Assignment Information
    Current Channel Average Energy............... unknown
    Previous Channel Average Energy.............. unknown
    Channel Change Count......................... 0
Last Channel Change Time..................... Mon May 17 11:56:32 2010
    Recommended Best Channel..................... 149
  RF Parameter Recommendations
    Power Level.................................. 7
    RTS/CTS Threshold............................ 2347
    Fragmentation Tnreshold...................... 2346
    Antenna Pattern.............................. 0

  Persistent Interference Devices
  Classtype Channel DC (%) RSSI (dBM) Last Update Time
---------------  -------  ------  ----------  ------------------------
  Canopy    149       4    -63           Tue May 18 03:21:16 2010
  All third party trademarks are the property of their respective owners.
```

永続的デバイスのモニタリング（GUI）

コントローラの GUI を使用して特定のアクセス ポイントに対する永続的デバイスをモニタリングするには、次の手順を実行します。

[Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて [Detail] をクリックします。[802.11a/n（または 802.11b/g/n）AP Interfaces > Detail] ページが表示されます。

このページには、アクセス ポイントの詳細と、このアクセス ポイントによって検出された永続的デバイスのリストが表示されます。永続的デバイスの詳細は、[Persistent Devices] セクションの下に表示されます。

それぞれの永続的デバイスについて、次の情報が表示されます。

[Class Type]：永続的デバイスの分類タイプ。

[Channel]：このデバイスが影響を与えているチャネル。

[DC(%)]：永続的デバイスのデューティ サイクル（パーセンテージ）。

[RSSI(dBm)]：永続的デバイスの RSSI インジケータ。

[Last Seen Time]：このデバイスが最後にアクティブになったときのタイムスタンプ。

永続的デバイスのモニタリング（CLI）

CLI を使用して永続的デバイスの一覧を表示するには、次のコマンドを入力します。

show ap auto-rf {**802.11a** | **802.11b**} *ap_name*

```
Number Of Slots.................................. 2
AP Name.......................................... AP_1142_MAP
MAC Address...................................... c4:7d:4f:3a:35:38
  Slot ID........................................ 1
  Radio Type..................................... RADIO_TYPE_80211a
  Sub-band Type.................................. All
  Noise Information
. . ..
. . . .
Power Level.................................. 1
    RTS/CTS Threshold.......................... 2347
    Fragmentation Threshold.................... 2346
    Antenna Pattern............................ 0

Persistent Interference Devices
  Class Type                Channel  DC (%%)  RSSI (dBm)  Last Update Time
  ------------------------  -------  ------  ----------  ------------------------
  Video Camera              149      100     -34         Tue Nov  8 10:06:25 2011
```

それぞれの永続的デバイスについて、次の情報が表示されます。

- [Class Type]：永続的デバイスの分類タイプ。
- [Channel]：このデバイスが影響を与えているチャネル。
- [DC(%)]：永続的デバイスのデューティ サイクル（パーセンテージ）。
- [RSSI(dBm)]：永続的デバイスの RSSI インジケータ。
- [Last Updated Time]：このデバイスが最後にアクティブになったときのタイムスタンプ。

無線帯域の電波品質のモニタリング

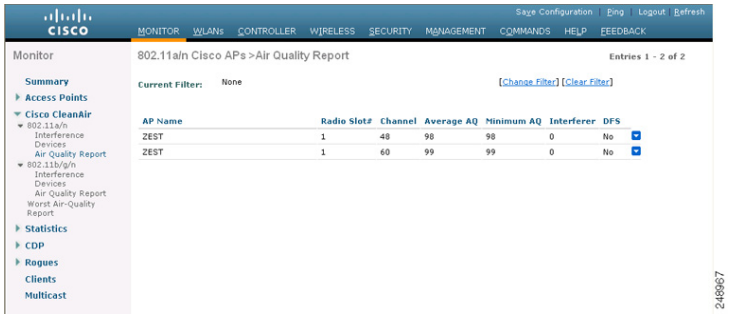
この項では、次のトピックを扱います。

無線帯域の電波品質のモニタリング（GUI）

コントローラの GUI を使用して無線帯域の電波品質をモニタリングするには、次の手順を実行します。

[Monitor] > [**Cisco** CleanAir] > [802.11a/n] または [802.11b/g] > [Air Quality Report] を選択して、[CleanAir > Air Quality Report] ページを開きます。

図 13-4　[CleanAir > Air Quality Report] ページ



このページには、802.11a/n と 802.11b/g/n の両方の無線帯域の電波品質が表示されます。特に、次の情報が表示されます。

- [AP Name]：802.11a/n または 802.11b/g/n 無線帯域において、電波品質が最悪と報告されているアクセス ポイントの名前。
- [Radio Slot]：無線が取り付けられているスロットの番号。
- [Channel]：電波品質をモニタしている無線チャネル。
- [Minimum AQ]：この無線チャネルの最低電波品質。
- [Average AQ]：この無線チャネルの平均電波品質。
- [Interferer]：802.11a/n または 802.11b/g/n 無線帯域で無線によって検出された干渉源の数。
- [DFS]：動的周波数選択。DFS が有効かどうかを表します。

無線帯域の電波品質のモニタリング（CLI）

この項では、802.11a/n または 802.11b/g/n の無線帯域の電波品質のモニタリングに使用するコマンドについて説明します。

電波品質のサマリーの表示

802.11a/n または 802.11b/g/n 無線帯域の電波品質のサマリーを表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality summary

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel  Avg AQ  Min AQ  Interferers DFS
--------------- -------- ------- ------- ------------ ----
CISCO_AP3500     36         95      70       0
CISCO_AP3500     40         93      75       0
CISCO_AP3500     44         95      80       0
CISCO_AP3500     48         97      75       0
CISCO_AP3500     52         98      80       0
...
```

ある無線帯域のすべてのアクセス ポイントの電波品質の表示

802.11a/n または 802.11b/g/n のアクセス ポイントとその電波品質の情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel  Avg AQ    Min AQ  Interferers  DFS
--------------- --------- -------- --------- ------------ ------
CISCO_AP3500       1       83       57          3          5
```

ある無線帯域のアクセス ポイントの電波品質の表示

802.11a/n または 802.11b/g/n 無線帯域にある特定のアクセス ポイントの電波品質に関する情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality *Cisco_AP*

以下に類似した情報が表示されます。

```
Slot Channel Avg AQ  Min AQ  Total Power (dBm) Total Duty Cycle (%)
---- ------- ------- ------  ----------------- --------------------
1    140       100     100        -89               0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
---------------------- ------------------------- ------------ ---
-128                      0                         0
```

無線帯域の電波品質（ワースト ケース）のモニタリング（GUI）

ステップ 1　[Monitor] > [Cisco CleanAir] > [802.11b/g] > [Worst Air-Quality] を選択して、[CleanAir > Worst Air Quality Report] ページを開きます。

図 13-5　[CleanAir > Worst Air Quality Report] ページ

このページには、802.11a/n と 802.11b/g/n の両方の無線帯域の電波品質が表示されます。特に、次の情報が表示されます。

- [AP Name]：802.11a/n または 802.11b/g/n 無線帯域において、電波品質が最悪と報告されているアクセス ポイントの名前。
- [Channel Number]：電波品質が最悪と報告された無線チャネル。
- [Minimum Air Quality Index(1 to 100)]：この無線チャネルの最低電波品質。電波品質の指標（AQI）の値は、100 が最高で、1 が最悪です。
- [Average Air Quality Index(1 to 100)]：この無線チャネルの平均電波品質。電波品質の指標（AQI）の値は、100 が最高で、1 が最悪です。
- [Interference Device Count]：802.11a/n または 802.11b/g/n 無線帯域で無線によって検出された干渉源の数。

ステップ 2　特定のアクセス ポイント無線に対する永続的干渉源の一覧を表示するには、次の手順を実行します。

a.　[Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。

b.　カーソルを目的のアクセス ポイント無線の青いドロップダウン矢印の上に置いて [CleanAir-RRM] をクリックします。[802.11a/n（または 802.11b/g/n）Cisco APs > *Access Point Name* > Persistent Devices] ページが表示されます。このページには、このアクセス ポイント無線によって検出された干渉源のデバイス タイプが一覧されます。また、干渉が検出されたチャネル、干渉がアクティブだった時間のパーセンテージ（デューティ サイクル）、干渉源の受信信号強度（RSSI）、および干渉が最後に検出された日付と時刻も表示されます。

無線帯域の電波品質（ワースト ケース）のモニタリング（CLI）

この項では、802.11a/n または 802.11b/g/n の無線帯域の電波品質のモニタリングに使用するコマンドについて説明します。

電波品質のサマリーの表示（CLI）

802.11a/n または 802.11b/g/n 無線帯域の電波品質のサマリーを表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality summary

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel  Avg AQ  Min AQ  Interferers DFS
--------------- -------- ------- ------- ------------ ----
CISCO_AP3500     36         95      70       0
CISCO_AP3500     40         93      75       0
CISCO_AP3500     44         95      80       0
CISCO_AP3500     48         97      75       0
CISCO_AP3500     52         98      80       0
...
```

ある無線帯域におけるすべてのアクセス ポイントの中で最も悪い電波品質に関する情報の表示（CLI）

802.11a/n または 802.11b/g/n のアクセス ポイントとその電波品質（ワースト ケース）についての情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality worst

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel  Avg AQ    Min AQ  Interferers  DFS
--------------- --------- -------- --------- ------------ ------
CISCO_AP3500       1       83       57          3          5
```

ある無線帯域のアクセス ポイントの電波品質の表示（CLI）

802.11a/n または 802.11b/g/n 無線帯域にある特定のアクセス ポイントの電波品質に関する情報を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b} cleanair air-quality *Cisco_AP*

以下に類似した情報が表示されます。

```
Slot Channel Avg AQ  Min AQ  Total Power (dBm) Total Duty Cycle (%)
---- ------- ------- ------  ----------------- --------------------
1    140       100     100        -89               0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
---------------------- ------------------------- ------------ ---
```

```
-128                    0                       0
```

デバイス タイプごとのアクセス ポイントの電波品質の表示（CLI）

- 802.11a/n または 802.11b/g/n 無線帯域について、特定のアクセス ポイントによって検出されたすべての干渉源について情報を表示するには、次のコマンドを入力します。

  show {802.11a | 802.11b} cleanair device ap *Cisco_AP*

  以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No  ClusterID          DevID  Type       AP Name      ISI  RSSI  DC   Channel
--- ------------------ ------ ---------- ---------------- ---- ----- ---- -------------
1   c2:f7:40:00:00:03  0x8001 DECT phone CISCO_AP3500 1    -43   3   149,153,157,161
3   c2:f7:40:00:00:03  0x8005 Canopy     CISCO_AP3500 2    -62   2   153,157,161,165
```

- 802.11a/n または 802.11b/g/n 無線帯域について、特定のデバイス タイプのすべての干渉源の情報を表示するには、次のコマンドを入力します。

  show {802.11a | 802.11b} cleanair device type *type*

  ここで、*type* には次のいずれかを選択します。

  - **802.11-fh**：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
  - **802.11-inv**：スペクトラム反転 Wi-Fi 信号を使用するデバイス
  - **802.11-nonstd**：非標準の Wi-Fi チャネルを使用するデバイス
  - **802.15.4**：802.15.4 デバイス（802.11b/g/n のみ）
  - **all**：すべての干渉デバイス タイプ（これがデフォルト値です）
  - **bt-discovery**：Bluetooth の検出（802.11b/g/n のみ）
  - **bt-link**：Bluetooth リンク（802.11b/g/n のみ）
  - **canopy**：Canopy ブリッジ デバイス
  - **cont-tx**：連続トランスミッタ
  - **dect-like**：Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話
  - **jammer**：電波妨害デバイス
  - **mw-oven**：電子レンジ（802.11b/g/n のみ）
  - **superag**：802.11 SuperAG デバイス
  - **tdd-tx**：時分割複信（TDD）トランスミッタ
  - **video camera**：アナログ ビデオ カメラ
  - **wimax-fixed**：WiMAX 固定デバイス
  - **wimax-mobile**：WiMAX モバイル デバイス
  - **xbox**：Microsoft Xbox（802.11b/g/n のみ）

  以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
```

```
  * indicates cluster center device

No  ClusterID          DevID  Type        AP Name     ISI  RSSI DC   Channel
--- ----------------- ------ ----------- ---------- ---- ----- --- --------------
1   b4:f7:40:00:00:03 0x4185 DECT-like (26) CISCO_AP35001  -58   3  153,157,161,165
```

永続的干渉源の検出（CLI）

802.11a/n または 802.11b/g/n 無線帯域にある特定のアクセス ポイントに対する永続的干渉源の一覧を表示するには、次のコマンドを入力します。

show ap auto-rf {802.11a | 802.11b} *Cisco_AP*

以下に類似した情報が表示されます。

```
Number Of Slots.................................. 2
AP Name.......................................... CISCO_AP3500
...
Persistent Interferers
  Classtype                  Channel  DC (%)  RSSI (dBm)  Last Update Time
  -------------------------  -------  ------  ----------  -------------------------
    802.11FH                  149     3       -58         Thu Jan 1 00:20:34 2009
    Radar                     153     2       -81         Thu Jan 1 00:20:35 2009
    Continuous Transmitter    157     2       -62         Thu Jan 1 00:20:36 2009
    ...
    All third party trademarks are the property of their respective owners.
```

Spectrum Expert の接続の設定

スペクトラム アナライザから提供されるような RF 分析プロットの作成に使用できる詳細なスペクトラム データを入手するには、Cisco CleanAir 対応のアクセス ポイントを、Spectrum Expert アプリケーションを実行している Microsoft Windows XP または Vista の PC（*Spectrum Expert コンソール*と呼ばれる）に直接接続するよう設定します。Spectrum Expert との接続は、WCS から半自動的に開始することも、コントローラから手動で開始することもできます。この項では、後者の方法について説明します。

Spectrum Expert を設定するには、次の手順に従ってください。

ステップ 1　Spectrum Expert コンソールとアクセス ポイントとの間に接続を確立する前に、IP アドレスのルーティングが正しく設定され、途中にあるすべてのファイアウォールでネットワーク スペクトラム インターフェイス（NSI）ポートが開かれていることを確認します。

ステップ 2　Spectrum Expert コンソールに接続するアクセス ポイントで、Cisco CleanAir 機能が有効になっていることを確認します。

ステップ 3　コントローラの GUI または CLI を使用して、アクセス ポイントを SE-Connect モードに設定します。

（注）　SE-Connect モードは、1 つの無線だけでなく、そのアクセス ポイント全体に対して設定されます。しかし、Spectrum Expert コンソールが接続するのは一度に 1 つの無線です。

- コントローラの GUI を使用している場合は、次の手順に従ってください。
  a. [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b. 対象のアクセス ポイントの名前を選択して、[All APs > Details for] ページを開きます。

c. [AP Mode] ドロップダウン リストから [SE-Connect] を選択します。このモードは、Cisco CleanAir 機能にをサポートできるアクセス ポイントでのみ使用できます。SE-Connect モードが使用可能なオプションとして表示されるには、アクセス ポイントに有効状態のスペクトラム対応無線が少なくとも 1 つ以上あることが必要です。

d. [Apply] をクリックして、変更を確定します。

e. アクセス ポイントをリブートするように求められたら、[OK] をクリックします。

- コントローラの CLI を使用している場合は、次の手順に従ってください。

a. 次のコマンドを入力して、アクセス ポイントに SE-Connect モードを設定します。

config ap mode se-connect *Cisco_AP*

b. アクセス ポイントをリブートするように求められたら、「**Y**」と入力します。

c. 次のコマンドを入力して、アクセス ポイントの SE-Connect の設定状況を確認します。

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Enabled
       Spectrum Sensor State.................. Configured (Error code = 0)
```

ステップ 4　Windows PC で、次の URL から Cisco Software Center にアクセスします。

http://www.cisco.com/cisco/software/navigator.html

ステップ 5　[Product] > [Wireless] > [Cisco Spectrum Intelligence] > [Cisco Spectrum Expert] > [Cisco Spectrum Expert Wi-Fi] の順にクリックし、Spectrum Expert 4.0 の実行可能ファイル（*.exe）をダウンロードします。

ステップ 6　PC で Spectrum Expert アプリケーションを実行します。

ステップ 7　[Connect to Sensor] ダイアログボックスが表示されたら、アクセス ポイントの IP アドレスを入力し、アクセス ポイントの無線を選択し、認証のために 16 バイトのネットワーク スペクトラム インターフェイス（NSI）キーを入力します。Spectrum Expert アプリケーションによって、NSI プロトコルを使用して、アクセス ポイントへの TCP/IP による直接接続が開かれます。

（注）　アクセス ポイントは、2.4 GHz の周波数をポート 37540 で、5 GHz の周波数をポート 37550 でリスニングする TCP サーバである必要があります。これらのポートは、Spectrum Expert アプリケーションが NSI プロトコルを使用してアクセス ポイントに接続するために、開かれている必要があります。

（注）　コントローラの CLI から NSI キーを確認するには、**show** {**802.11a** | **802.11b**} **spectrum se-connect** *Cisco_AP command* と入力します。

SE-Connect モードのアクセス ポイントがコントローラに join すると、アクセス ポイントから Spectrum Capabilities 通知メッセージが送信され、これにコントローラは Spectrum Configuration Request で応答します。この要求には 16 バイトのランダム NSI キーが含まれます。このキーは NSI 認証で使用するためにコントローラで作成されたものです。コントローラはアクセス ポイントごとにキーを 1 つ作成し、アクセス ポイントはこのキーをリブートするまで保存します。

（注）　Spectrum Expert コンソール接続は、アクセス ポイントの無線ごとに最大 3 つまで確立できます。コントローラの GUI の [802.11a/n（または 802.11b/g/n）Cisco APs > Configure] ページにある [Number of Spectrum Expert Connections] テキスト ボックスには、現在アクセス ポイント無線に接続されている Spectrum Expert アプリケーションの数が表示されます。

ステップ 8　Spectrum Expert アプリケーションの右下隅にある [Slave Remote Sensor] テキスト ボックスを選択して、Spectrum Expert コンソールがアクセス ポイントに接続されていることを確認します。デバイスが 2 台接続されている場合は、このテキスト ボックスにアクセス ポイントの IP アドレスが表示されます。

ステップ 9　Spectrum Expert アプリケーションを使用して、アクセス ポイントからのスペクトラム データを表示および分析します。

その他の参考資料

CleanAir の設定の詳細については、次の各項を参照してください。

関連資料

関連項目	ドキュメント名
CleanAir に関する Cisco WCS レポート	『Cisco Wireless Control System Configuration Guide』 URL： http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html
WCS を使用して Spectrum Expert の接続を開始する方法	『Cisco Wireless Control System Configuration Guide』
Spectrum Expert の使用方法	『Cisco Spectrum Expert Users Guide, Release 4.0』 URL： http://www.cisco.com/en/US/products/ps9393/products_user_guide_list.html

CleanAir の設定の機能履歴

表 13-1 に、この機能のリリース履歴を示します。

表 13-1　CleanAir の設定の機能履歴

機能名	リリース	機能情報
クラスタ ID	7.0.116.0	デバイスのタイプを一意に識別できるクラスタ識別番号。
CleanAir	7.0.98.0	CleanAir を使用すると、Wi-Fi 以外の干渉源を識別および追跡し、最適なパフォーマンスが得られるようネットワーク設定を調整し、悪意のあるデバイスからの脅威を識別し、WLAN と他のワイヤレス デバイスを共存させられるようになります。