不正なデバイスの管理

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正なデバイスについて

不正なアクセスポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセスポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセスポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホック クライアントをより効果的に阻止することができます。
- ローカル モード アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 または 60 秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。
- クライアントカードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセスポイントの封じ込めを無線チャンネルごとに 3 台（監視モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセス ポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。ただし RLDP は、管理対象のアクセス ポイントが DFS チャネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[**Validate Rogue Clients Against AAA**] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることによって、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。
- オープン認証を使用する不正アクセス ポイントはネットワーク上で検出できます。NAT 有線または不正有線検出は、WLC（RLDP と不正検出 AP の両方）ではサポートされません。非隣接 MAC アドレスは、RLDP ではなく AP の不正検出モードでサポートされます。
- ハイ アベイラビリティのシナリオでは、不正検出セキュリティ レベルを高か重要に設定すると、スタンバイ Cisco WLC の不正タイマーは、不正検出保留の安定時間の 300 秒が過ぎないと開始しません。したがって、スタンバイ Cisco WLC のアクティブ設定が反映されるのは、300 秒が過ぎてからです。

（注） 不正AP、不正クライアント、または一時的な封じ込めの設定は、リロード時に破棄されます。リロード後にすべての不正を再設定する必要があります。

（注） 不正クライアントのトラップを制御するための独立したコマンドはありません。ただし、不正クライアントのトラップは、不正 AP でも使用する **config trapflags rogueap {enable | disable}** コマンドで有効、無効を切り替えることができます。GUI 設定でも、[Management] -> [SNMP] -> [TrapControl] -> [Security] -> [Rogue AP] で AP フラグを使用して、不正クライアントを制御してください。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

（注） Lightweight AP が不正 AP とアソシエートして DHCP アドレスを受信するかどうかを確認するには、**debug dot11 rldp enable** コマンドを使用します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*.....0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x.....0040 00 00 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

ここで、RLDP の動作手順を示します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。

3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。
5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が重大度が critical の on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカルモード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDPは、シスコのAtonomous不正アクセス ポイントではサポートされていません。これらのアクセス ポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセス ポイント チャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。自動 RLDP 試行で不正（ノイズの多い RF 環境などが原因）が検出されなかった場合は、コントローラが再試行しません。ただし、不正デバイス上でRLDPを手動で開始できます。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセス ポイントを継続的に監視し、不正なアクセス ポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセス ポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDPのサイクルが終了すると、クライアントはアクセスポイン

トに再接続します。不正なアクセスポイントが検出された時点で（自動設定）、RLDPのプロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドで設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。RLDP を開始するための同等の GUI オプションはサポートされていません。

   config rogue ap rldp initiate *mac-address*

2. コントローラの CLI から RLDP をスケジュールします。RLDP をスケジュールするための同等の GUI オプションはサポートされていません。

   config rogue ap rldp schedule

3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。

   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントが Friendly 状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

不正検出の設定方法

不正検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wpsroguedetectionmin-rssi** *rssi in dBm* 例： `Device(config)# wireless wps rogue detection min-rssi 100`	不正に必要な最小 RSSI 値を指定します。これは、AP が不正を検出し、デバイスで不正エントリが作成されるために必要な値です。 rssi in dBm パラメータの有効範囲は –128 ～ –70 dBm で、デフォルト値は –128 dBm です。

	コマンドまたはアクション	目的
		（注） この機能は、すべてのAPモードに適用できます。RSSI値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、APが不正を検出する最小RSSI値を指定することで、このオプションを使用して不正をフィルタリングすることができます。
ステップ3	**wireless wpsroguedetectionmin-transient-time** *time in seconds* 例： `Device(config)# wireless wps rogue detection min-transient-time`	不正が初めてスキャンされた後、APで不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。 （注） この機能は、モニタ モードのAP のみに適用されます。 一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • APからコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる
ステップ4	**wireless wpsrogueclient** {**aaa** | **mse**} 例： `Device(config)# wireless wps rogue client aaa`	不正なクライアントが有効なクライアントかどうかを検証するために、AAAサーバまたはローカル データベース、またはMSEを設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless wps rogue client mse`	
ステップ 5	**wireless wpsrogue apvalid-clientauto-contain** 例： `Device(config)# wireless wps rogue ap valid-client auto-contain`	信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止するように指定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正検出のモニタリング

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、上で不正検出をモニタするために使用できます。

表 *1*:不正検出モニタリングのコマンド

コマンド	目的
show wireless wps rogue ap summary	によって検出されたすべての不正アクセス ポイントのリストを表示します。
show wireless wps rogue client detailed *client-mac*	特定の不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	で検出されたすべての不正なクライアントのリストを表示します。
show nmsp capability	NMSP 機能を表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、で作成されたエントリを持つように設定する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、不正なクライアントが有効なクライアントかどうかを検証するために MSE を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue client mse
Device(config)# end
Device# show wireless wps rogue client summary
```

次に、信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue ap valid-client auto-contain
Device(config)# end
Device# show wireless wps rogue ap summary
Device# show nmsp capability
```

不正検出に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

不正検出設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	MSE に対する不正な検証。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

不正なデバイスについて

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のク

ライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセスポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホック クライアントをより効果的に阻止することができます。
- ローカル モード アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 または 60 秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。
- クライアントカードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセスポイントの封じ込めを無線チャンネルごとに 3 台（監視モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。
- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセスポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。

- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。ただし RLDP は、管理対象のアクセス ポイントが DFS チャネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[**Validate Rogue Clients Against AAA**] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることによって、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。
- オープン認証を使用する不正アクセス ポイントはネットワーク上で検出できます。NAT 有線または不正有線検出は、WLC（RLDP と不正検出 AP の両方）ではサポートされません。非隣接 MAC アドレスは、RLDP ではなく AP の不正検出モードでサポートされます。
- ハイ アベイラビリティのシナリオでは、不正検出セキュリティ レベルを高か重要に設定すると、スタンバイ Cisco WLC の不正タイマーは、不正検出保留の安定時間の 300 秒が過ぎないと開始しません。したがって、スタンバイ Cisco WLC のアクティブ設定が反映されるのは、300 秒が過ぎてからです。

（注） 不正 AP、不正クライアント、または一時的な封じ込めの設定は、リロード時に破棄されます。リロード後にすべての不正を再設定する必要があります。

（注） 不正クライアントのトラップを制御するための独立したコマンドはありません。ただし、不正クライアントのトラップは、不正 AP でも使用する **config trapflags rogueap {enable | disable}** コマンドで有効、無効を切り替えることができます。GUI 設定でも、[Management] -> [SNMP] -> [TrapControl] -> [Security] -> [Rogue AP] で AP フラグを使用して、不正クライアントを制御してください。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

RLDP の不正 AP の検出精度は 100% です。オープン AP と NAT AP を検出します。

（注） Lightweight AP が不正 AP とアソシエートして DHCP アドレスを受信するかどうかを確認するには、**debug dot11 rldp enable** コマンドを使用します。このコマンドは、Lightweight AP からコントローラに送信された UDP パケットも表示します。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*.....0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 .....x.....0040 00 00 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

ここで、RLDP の動作手順を示します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。
3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。

5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が重大度が critical の on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。
- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカルモード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDPは、シスコのAtonomous不正アクセス ポイントではサポートされていません。これらのアクセス ポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセス ポイント チャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。自動 RLDP 試行で不正（ノイズの多い RF 環境などが原因）が検出されなかった場合は、コントローラが再試行しません。ただし、不正デバイス上でRLDPを手動で開始できます。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセス ポイントを継続的に監視し、不正なアクセス ポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセス ポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDPのサイクルが終了すると、クライアントはアクセス ポイントに再接続します。不正なアクセス ポイントが検出された時点で（自動設定）、RLDPのプロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混

雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドで設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。RLDP を開始するための同等の GUI オプションはサポートされていません。

   config rogue ap rldp initiate *mac-address*

2. コントローラの CLI から RLDP をスケジュールします。RLDP をスケジュールするための同等の GUI オプションはサポートされていません。

   config rogue ap rldp schedule

3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。

   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントがFriendly状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

不正検出の設定方法

不正検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wpsroguedetectionmin-rssi** *rssi in dBm* 例： `Device(config)# wireless wps rogue detection min-rssi 100`	不正に必要な最小 RSSI 値を指定します。これは、AP が不正を検出し、デバイスで不正エントリが作成されるために必要な値です。 rssi in dBm パラメータの有効範囲は –128 ～ –70 dBm で、デフォルト値は –128 dBm です。 （注） この機能は、すべてのAPモードに適用できます。RSSI値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、APが不正を検出する最小RSSI値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

	コマンドまたはアクション	目的
ステップ 3	**wireless wpsroguedetectionmin-transient-time** *time in seconds* 例： `Device(config)# wireless wps rogue detection min-transient-time`	不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。 （注） この機能は、モニタ モードの AP のみに適用されます。 一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • APからコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる

ステップ 4	**wireless wpsrogueclient** {**aaa** | **mse**}
	例：
	`Device(config)# wireless wps rogue client aaa`
	`Device(config)# wireless wps rogue client mse`
		不正なクライアントが有効なクライアントかどうかを検証するために、AAAサーバまたはローカル データベース、または MSE を設定します。

ステップ 5	**wireless wpsrogue apvalid-clientauto-contain** 例： `Device(config)# wireless wps rogue ap valid-client auto-contain`	信頼できるクライアントが関連付けられる不正なアクセス ポイントを自動的に阻止するように指定します。
ステップ 6	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

不正検出のモニタリング

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、上で不正検出をモニタするために使用できます。

表 *2:* 不正検出モニタリングのコマンド

コマンド	目的
show wireless wps rogue ap summary	によって検出されたすべての不正アクセスポイントのリストを表示します。
show wireless wps rogue client detailed *client-mac*	特定の不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	で検出されたすべての不正なクライアントのリストを表示します。
show nmsp capability	NMSP 機能を表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、で作成されたエントリを持つように設定する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

次に、不正なクライアントが有効なクライアントかどうかを検証するために MSE を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue client mse
```

```
Device(config)# end
Device# show wireless wps rogue client summary
```

次に、信頼できるクライアントが関連付けられる不正なアクセスポイントを自動的に阻止する例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue ap valid-client auto-contain
Device(config)# end
Device# show wireless wps rogue ap summary
Device# show nmsp capability
```

不正検出に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	『*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

不正検出設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。
Cisco IOS XE 3E	MSE に対する不正な検証。