不正なデバイスの管理

Rogue Detection

不正なデバイス

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、権限のないユーザー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。ワイヤレス ユーザーがエンタープライズ ネットワーク内のアクセス ポイントに接続する場合、エンタープライズ セキュリティ違反が発生する可能性が高くなります。

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。

- アクセスポイントは、関連付けられたクライアントにサービスを提供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）。大量の不正 AP とクライアントを高感度で検出する場合、モニター モード 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 秒や 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 ポイントは引き続き各チャネル上で約 50 ミリ秒を費やします。
- 家庭環境で展開されるアクセス ポイントは多数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がデフォルトで無効になっています。
- クライアントカードの実装により、封じ込めの効果が低下することがあります。これは通常、「関連付け解除/認証解除」フレームを受信後、クライアントがネットワークにすぐに再接続する可能性がある場合に発生し、一部のトラフィックが引き続き通過できる可能性があります。ただし、不正なクライアントが封じ込められると、そのブラウジングエクスペリエンスに悪影響を及ぼす可能性があります。
- 不正の状態と、状態の自動的な移行を可能にするユーザー定義の分類規則を使って、不正なアクセス ポイントを分類および報告できます。
- 各コントローラは、モニターモードでの不正アクセスポイントの封じ込めを無線ごとに 3 および 6 台に制限します。
- 設定を使用して手動の阻止を実行すると、不正エントリは有効期限が切れた後でも保持されます。
- 不正エントリの有効期限が切れると、管理対象のアクセス ポイントはすべてのアクティブな封じ込めを停止するように指示されます。
- [Validate Rogue Clients Against AAA] が有効になっている場合、コントローラは一度だけ不正なクライアントの検証を AAA サーバーに要求します。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、認証サーバーに有効なクライアント エントリを追加します。

不正検出の制約事項

- 不正な封じ込めは DFS チャネルではサポートされていません。

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、モニター 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。

不正な封じ込めに関する情報（保護された管理フレーム（PMF）が有効）

Cisco IOS XE Amsterdam 17.3.1 以降では、802.11w 保護された管理フレーム（PMF）が有効になっている不正デバイスは含まれていません。代わりに、不正デバイスは [Contained Pending] としてマークされ、WSA アラームが発生して Contained Pending イベントに関する通知がされます。デバイスの抑制は実行されないため、アクセスポイント（AP）リソースが不必要に消費されることはありません。

（注） この機能は Wave 2 AP でのみサポートされています。

不正デバイスで PMF が有効になっているときに、show wireless wps rogue ap detailed コマンドを実行して、デバイスの抑制を確認します。

AP 偽装検出

AP 偽装の検出方法は次のとおりです。

- 管理対象 AP が AP 自体を不正であると報告した場合の AP 偽装検出。この方法は常に有効であり、設定は不要です。
- MFP に基づく AP 偽装検出。
- AP 認証に基づく AP 偽装検出。

インフラストラクチャ MFP は、クライアントではなく、AP によって送信され、ネットワーク内の他の AP によって検証される管理フレームにメッセージ整合性チェック（MIC）情報要素を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP が有効になっている場合、管理対象 AP によって、MIC 情報要素の存在の有無、MIC 情報要素が期待どおりの内容であるかがチェックされます。いずれかの条件が満たされていない場合、管理対象 AP は、更新された AP 認証失敗カウンタを含む不正 AP レポートを送信します。

AP認証機能を使用すると、AP偽装を検出できます。この機能を有効にすると、コントローラで AP ドメインの秘密が作成され、同じネットワーク内の他の AP と共有されます。これにより、AP が相互に認証できるようになります。

AP認証情報要素は、ビーコンおよびプローブ応答フレームに添付されます。AP認証情報要素に不正な [Signature] フィールドがある場合、タイムスタンプがオフの場合、または AP 認証情報要素が欠落している場合、そのような状態を検出した AP により [AP authentication failure count] フィールドが増分されます。[AP authentication failure count] フィールドがしきい値を超えると、偽装アラームが発生します。不正 AP は、状態が [Threat] である [Malicious] として分類されます。

show wireless wps rogue ap detail コマンドを実行して、認証エラーが原因で偽装が検出された時刻を確認します。

不正検出の設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] を選択します。
ステップ 2 [AP Join Profile Name] をクリックして、AP 接続プロファイルのプロパティを編集します。
ステップ 3 [Edit AP Join Profile] ウィンドウで [Rogue AP] タブをクリックします。
ステップ 4 [Rogue Detection] チェックボックスをオンにして、不正 AP 検知を有効にします。
ステップ 5 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。
ステップ 6 [Rogue Detection Transient Interval] フィールドに、間隔を秒単位で入力します。
ステップ 7 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を秒単位で入力します。
ステップ 8 [Rogue Detection Client Number Threshold] フィールドに、不正なクライアント検出のしきい値を入力します。
ステップ 9 [Auto Containment on FlexConnect Standalone] チェックボックスをオンにして、自動封じ込めを有効にします。
ステップ 10 [Update & Apply to Device] をクリックします。

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	**ap profile** *profile-name* **rogue detection min-transient-time** *time in seconds*
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection min-transient-time 120`
		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。

	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。 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。 この機能には次のような利点があります。 • 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3	**ap profile** *profile-name* **rogue detection containment** {**auto-rate** | **flex-rate**}
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection containment flex-rate`
		不正な封じ込めオプションを指定します。auto-rateオプションを指定すると、不正を封じ込めるための自動レートが有効になります。flex-rateオプションを指定すると、スタンドアロンFlexConnect APの不正な封じ込めが有効になります。

ステップ4	**ap profile** *profile-name* **rogue detection enable** 例： `Device(config)# ap profile profile1`	すべてのAPで不正AP検知を有効にします。

ステップ5	**ap profile** *profile-name* **rogue detection report-interval** *time in seconds*
	例：
	`Device(config)# ap profile profile1`
	`Device(config)# rogue detection report-interval 120`
		モニターモードのCisco APに対する不正レポートの間隔を設定します。
		報告する間隔の有効な範囲（秒単位）は、10 ～ 300秒です。

管理フレーム保護の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] を選択します。

ステップ 2 [Rogue Policy] タブの [MFP Configuration] セクションで、[Global MFP State] チェックボックスと [AP Impersonation Detection] チェックボックスをオンにして、グローバル MFP 状態と AP 偽装検出をそれぞれ有効にします。

ステップ 3 [MFP Key Refresh Interval] フィールドで、更新間隔を時間単位で指定します。

ステップ 4 [Apply] をクリックします。

管理フレーム保護の設定（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 wps mfp** 例： `Device(config)# wireless wps mfp`	管理フレーム保護を設定します。

ステップ 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	例：
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		AP の偽装検出（または）MFP キーの更新間隔を時間単位で設定します。
		key-refresh-interval：MFP キーの更新間隔を時単位で設定します。有効な範囲は 1 ～ 24 です。デフォルト値は 24 です。

ステップ 4	**end** 例： `Device(config)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 **EXEC** モードに戻ります。

アクセスポイント認証の有効化

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 wps ap-authentication** 例： `Device(config)# wireless wps ap-authentication`	ワイヤレス WPS AP 認証を設定します。
ステップ 3	**wireless wps ap-authentication threshold** *threshold* 例： `Device(config)# wireless wps ap-authentication threshold 100`	AP ネイバー認証を設定し、AP 認証エラーのしきい値を設定します。
ステップ 4	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN を設定します。
ステップ 5	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet 情報要素のサポートを有効にします。
ステップ 6	**end** 例： `Device# end`	特権 EXEC モードに戻ります。

管理フレーム保護の確認

管理フレーム保護（MFP）機能が有効かどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
```

```
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

MFP の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

不正検出の検証

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。

次のコマンドを使用して、デバイスでの不正 AP 検知を確認できます。

表 *1:* アドホック不正情報の確認

コマンド	目的
show wireless wps rogue adhoc detailed *mac_address*	アドホック不正の詳細情報を表示します。
show wireless wps rogue adhoc summary	すべてのアドホック不正のリストを表示します。

表 *2:* 不正 *AP* 情報の確認

コマンド	目的
show wireless wps rogue ap clients *mac_address*	不正に関連付けられているすべての不正クライアントのリストを表示します。
show wireless wps rogue ap custom summary	カスタム不正 AP の情報を表示します。
show wireless wps rogue ap detailed *mac_address*	不正 AP の詳細情報を表示します。
show wireless wps rogue ap friendly summary	危険性のない不正 AP の情報を表示します。
show wireless wps rogue ap list *mac_address*	特定の AP によって検出された不正 AP のリストを表示します。
show wireless wps rogue ap malicious summary	悪意のある不正 AP の情報を表示します。
show wireless wps rogue ap summary	すべての不正 AP のリストを表示します。
show wireless wps rogue ap unclassified summary	未分類の不正 AP の情報を表示します。

表 *3:* 不正の自動封じ込めに関する情報の確認

コマンド	目的
show wireless wps rogue auto-contain	不正の自動封じ込めに関する情報を表示します。

表 *4:* 分類ルールの情報の確認

コマンド	目的
show wireless wps rogue rule detailed *rule_name*	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	すべての不正ルールのリストを表示します。

表 *5:* 不正統計情報の確認

コマンド	目的
show wireless wps rogue stats	不正統計情報を表示します。

表 *6:* 不正クライアントの情報の確認

コマンド	目的
show wireless wps rogue client detailed *mac_address*	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	すべての不正クライアントのリストを表示します。

表 *7:* 不正無視リストの確認

コマンド	目的
show wireless wps rogue ignore-list	不正無視リストを表示します。

例：不正検出の設定

次に、検出された不正 AP が存在する必要がある最小 RSSI を、デバイスで作成されたエントリを持つように設定する例を示します。

```
Device# wireless wps rogue ap notify-min-rssi 100
```

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)#
Device(config)#
```

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

不正ポリシーの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [Rogue Policies] タブで、[Rogue Detection Security Level] ドロップダウンを使用してセキュリティレベルを選択します。

ステップ 3 [Expiration timeout for Rogue APs (seconds)] フィールドに、タイムアウト値を入力します。

ステップ 4 [Validate Rogue Clients against AAA] チェック ボックスをオンにして、AAA サーバーに対して不正クライアントを検証します。

ステップ 5 [Validate Rogue APs against AAA] チェック ボックスをオンにして、AAA サーバーに対して不正アクセス ポイントを検証します。

ステップ 6 [Rogue Polling Interval (seconds)] フィールドに、不正情報について AAA サーバーにポーリングする間隔を入力します。

ステップ 7 不正アドホックネットワークの検出を有効にするには、[Detect and Report Adhoc Networks] チェックボックスをオンにします。

ステップ 8 [Rogue Detection Client Number Threshold] フィールドに、SNMP トラップを生成するしきい値を入力します。

ステップ 9 [Auto Contain] セクションで、次の詳細情報を入力します。

ステップ 10 [Auto Containment Level] ドロップダウンを使用してレベルを選択します。

ステップ 11 自動封じ込めをモニター モードの AP のみに制限するには、[Auto Containment only for Monitor Mode APs] チェック ボックスをオンにします。

ステップ 12 自動封じ込めを有線の不正 AP のみに制限するには、[Rogue on Wire] チェック ボックスをオンにします。

ステップ 13 コントローラに設定されているいずれかの SSID を使用している不正 AP のみに自動封じ込めを制限するには、[Using our SSID] チェックボックスをオンにします。

ステップ 14 自動封じ込めをアドホック不正 AP のみに制限するには、[Adhoc Rogue AP] チェック ボックスをオンにします。

ステップ 15 [Apply] をクリックします。

不正ポリシーの設定（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 wps rogue ap timeout** *number of seconds* 例： `Device(config)# wireless wps rogue ap timeout 250`	不正なエントリの有効期限を秒単位で設定します。秒単位の時間の有効な範囲は 240 ～ 3600 秒です。
ステップ 3	**wireless wps rogue client notify-min-rssi** *RSSI threshold* 例： `Device(config)# wireless wps rogue client notify-min-rssi -128`	不正なクライアントの最小 RSSI 通知しきい値を設定します。RSSI しきい値（dB 単位）の有効な範囲は -128 ～ -70 dB です。
ステップ 4	**wireless wps rogue client notify-min-deviation** *RSSI threshold* 例： `Device(config)# wireless wps rogue client notify-min-deviation 4`	不正なクライアントの RSSI 偏差通知しきい値を設定します。RSSI しきい値（dB 単位）の有効な範囲は 0 ～ 10 dB です。
ステップ 5	**wireless wps rogue ap aaa polling-interval** *AP AAA Interval* 例： `Device(config)# wireless wps rogue ap aaa polling-interval 120`	不正 AP AAA 検証間隔を設定します。AP AAA 間隔の有効な範囲（秒単位）は 60 ～ 86400 秒です。
ステップ 6	**wireless wps rogue adhoc** 例： `Device(config)# wireless wps rogue adhoc`	アドホック不正（IBSS）の検出とレポートを有効にします。
ステップ 7	**wireless wps rogue client client-threshold** *threshold* 例： `Device(config)# wireless wps rogue client client-threshold 100`	不正 AP SNMP トラップしきい値ごとに不正なクライアントを設定します。しきい値の有効な範囲は 0 ～ 256 です。

Rogue Location Discovery Protocol（RLDP）

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。

RLDP を管理するためのガイドラインの一部を次に示します。

- 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組み込みワイヤレスコントローラへの 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。
- 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組み込みワイヤレス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 がモニター 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。

次の手順では、RLDP の機能について説明します。

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ると、AP（WLAN クライアントとして機能している）は、 組み込みワイヤレスコントローラのそれぞれの IP アドレスに UDP パケットを送信します。
5. 組み込みワイヤレスコントローラがクライアントから RLDP パケットを 1 つでも受信すると、その不正が on-wire としてマークされます。

（注） 組み込みワイヤレス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パケットが組み込みワイヤレスコントローラに到達できません。

組み込みワイヤレスコントローラは、すべての近隣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およびクライアントに関する情報を自動的に検出して収集します。組み込みワイヤレスコントローラは、不正アクセスポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、その不正アクセスポイントがネットワークに接続されているかどうかを判断します。

組み込みワイヤレスコントローラは、オープンの不正デバイスで 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。不正アクセスポイントが検出された時点で、RLDPプロセスが開始されます。

すべてのアクセスポイントで、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、組み込みワイヤレス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ー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 組み込みワイヤレスコントローラを設定していて、モニター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場合、 組み込みワイヤレスコントローラは常に RLDP 動作に対してモニター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。再試行回数は、 を使用して設定できます。

3 つの方法で 組み込みワイヤレスコントローラから RLDP を開始またはトリガーできます。

1. 組み込みワイヤレスコントローラの CLI から RLDP 開始コマンドを手動で入力します。
2. 組み込みワイヤレスコントローラ CLI から RLDP をスケジュールします。
3. 自動 RLDP。 組み込みワイヤレスコントローラの CLI または GUI のどちらからでも 組み込みワイヤレスコントローラの自動 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。

RLDP の制約事項

- 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 はモニター 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。
- RLDP は、Cisco IOS AP でのみサポートされています。

アラームを生成する RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンリストを使用して、次のいずれかのオプションを選択します。

a) [Disable]：すべてのアクセスポイントで RLDP を無効にします。[Disable] がデフォルトオプションです。

b) [All APs]：すべての AP で RLDP を有効にします。

c) [Monitor Mode APs]：モニターモードの AP でのみ RLDP を有効にします。

（注） [Schedule RLDP] チェックボックスは、[Disable] オプションが選択されている場合にのみ有効になります。[All APs] オプションまたは [Monitor Mode APs] オプションを選択すると、[Schedule RLDP] チェックボックスは無効のままになります。

ステップ 3 [Retry Count] フィールドで、試行する再試行の回数を指定します。許可される範囲は 1 ～ 5 です。

ステップ 4 [Apply] をクリックします。

アラームを生成する RLDP 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 wps rogue ap rldp alarm-only <monitor-ap-only>**
	例：
	`Device(config)# wireless wps rogue ap rldp alarm-only`
	`Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only`
		RLDP でアラームを生成できるようにします。この方法では、RLDP は常に有効になります。
		monitor-ap-only キーワードはオプションです。
		alarm-only キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。
		alarm-only <monitor-ap-only> キーワードを指定してコマンドを実行すると、モニター モードのアクセス ポイントでのみ RLDP が有効になります。

ステップ 3	**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。

RLDP のスケジュールの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンリストから次のオプションを選択します。

- [Disable]（デフォルト）：すべてのアクセスポイントで RLDP を無効にします。

ステップ 3 [Retry Count] フィールドで、試行する再試行の回数を指定します。有効な範囲（1 ～ 5）を指定してください、

ステップ 4 [Schedule RLDP] チェックボックスをオンにして、プロセスを実行する曜日、開始時刻、終了時刻を指定します。

ステップ 5 [Apply] をクリックします。

RLDP のスケジュールの設定（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 wps rogue ap rldp schedule day** *day* **start** *start-time* **end** *end-time* 例： `Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00`	スケジュール設定された曜日、開始時刻、終了時刻に基づいてRLDPを有効にします。 ここで、各変数は次のように定義されます。 *day* は、RLDP のスケジューリングを実行できる曜日です。値は Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday です。 *start-time* は、RLDP のスケジューリングの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end time* は、RLDP のスケジューリングの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 3	**wireless wps rogue ap rldp schedule** 例： `Device(config)# wireless wps rogue ap rldp schedule`	スケジュールを有効にします。
ステップ 4	**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。

自動封じ込め用の RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [Rogue Policies] タブの [Auto Contain] セクションで、[Rogue on Wire] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。

自動封じ込め用の RLDP 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 wps rogue ap rldp auto-contain** [**monitor-ap-only**]
	例：
	`デバイス(config)# wireless wps rogue ap rldp auto-contain`
	`デバイス(config)# wireless wps rogue ap rldp auto-contain monitor-ap-only`
		RLDP で自動封じ込めを実行できるようにします。この方法では、RLDPは常に有効になります。
		monitor-ap-only キーワードはオプションです。
		auto-contain キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。
		auto-contain <monitor-ap-only> キーワードを指定してコマンドを実行すると、モニター モードのアクセス ポイントでのみ RLDP が有効になります。

ステップ 3	**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。

不正アクセス ポイントでの RLDP 再試行回数の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** を選択します。

ステップ 2 [Wireless Protection Policies] ページで [RLDP] タブをクリックします。

ステップ 3 [Retry Count] フィールドに、不正アクセス ポイントの RLDP 再試行の値を入力します。

有効な範囲は 1 ～ 5 です。

ステップ 4 設定を保存します。

不正アクセス ポイントでの RLDP 再試行回数の設定（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 wps rogue ap rldp retries** *num-entries* 例： `Device(config)# wireless wps rogue ap rldp retries 2`	不正アクセス ポイントでの RLDP 再試行回数を有効にします。 *num-entries* は、不正アクセス ポイントごとの RLDP 再試行回数です。 有効な範囲は 1 ～ 5 です。
ステップ 3	**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 AP RLDP の確認

次のコマンドを使用して、不正 AP RLDP を確認できます。

表 *8:* 不正 *AP* 情報の確認

コマンド	目的

show wireless wps rogue ap rldp detailed *mac_address*	不正 AP の RLDP の詳細を表示します。
show wireless wps rogue ap rldp in progress	進行中の RLDP のリストを表示します。
show wireless wps rogue ap rldp summary	RLDP スケジューリング情報の要約を表示します。

不正検出セキュリティ レベル

不正検出セキュリティ レベルの設定を使用して、不正検出パラメータを設定できます。

使用可能なセキュリティ レベルは次のとおりです。

- Critical：機密性の高い展開向けの基本不正検出。
- High：中規模な展開向けの基本不正検出。
- Low：小規模な展開向けの基本不正検出。
- Custom：デフォルトのセキュリティレベル（すべての検出パラメータが設定可能）。

（注） Critical、High、または Low の場合、一部の不正パラメータは固定されており、設定できません。

次の表に、事前に定義された 3 つのレベルについてパラメータの詳細を示します。

表 *9:* 不正検出：事前に定義されたレベル

パラメータ	Critical	High	Low
クリーンアップ タイマー	3600	1200	240
AAA 検証クライアント	ディセーブル	ディセーブル	ディセーブル
アドホック レポート	イネーブル	イネーブル	イネーブル
モニターモードレポート間隔	10 秒	30 秒	60 秒
最小 RSSI	-128 dBm	-80 dBm	-80 dBm
一時間隔	600 秒	300 秒	120 秒

パラメータ	Critical	High	Low
自動封じ込め モニター モードの AP でのみ動作します。	ディセーブル	ディセーブル	ディセーブル
自動封じ込めレベル	1	1	1
同じ SSID の自動封じ込め	ディセーブル	ディセーブル	ディセーブル
不正 AP 上の有効なクライアントの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
アドホックの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
封じ込め自動レート	イネーブル	イネーブル	イネーブル
CMX によるクライアントの検証	イネーブル	イネーブル	イネーブル
封じ込め FlexConnect	イネーブル	イネーブル	イネーブル
RLDP	RLDP スケジューリングが無効になっている場合は、モニター AP。	RLDP スケジューリングが無効になっている場合は、モニター AP。	ディセーブル
RLDP の自動封じ込め	ディセーブル	ディセーブル	ディセーブル

不正検出セキュリティレベルの設定

不正検出セキュリティレベルを設定するには、次の手順に従います。

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 wps rogue security-level custom** **例：**	不正検出セキュリティ レベルを「カスタム」に設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless wps rogue security-level custom`	
ステップ 3	**wireless wps rogue security-level low** 例： `Device(config)# wireless wps rogue security-level low`	小規模展開向けの基本不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 4	**wireless wps rogue security-level high** 例： `Device(config)# wireless wps rogue security-level high`	中規模展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 5	**wireless wps rogue security-level critical** 例： `Device(config)# wireless wps rogue security-level critical`	機密性の高い展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。

Wireless Service Assurance 不正イベント

リリース 16.12.x 以降のリリースでサポートされている Wireless Service Assurance（WSA）不正イベントは、SNMP トラップのサブセットに対応したテレメトリ通知で構成されています。WSA 不正イベントは、対応する SNMP トラップの一部となっている同じ情報を複製します。

エクスポートされたすべてのイベントについて、次の詳細が Wireless Service Assurance（WSA）インフラストラクチャに提供されます。

- 不正 AP の MAC アドレス
- 最も強力な RSSI で不正 AP を検出した管理対象 AP と無線の詳細
- イベント固有のデータ（SSID、潜在的なハニーポットイベントのチャネル、偽装イベント用偽装 AP の MAC アドレスなど）

WSA 不正イベント機能は、サポートされる AP の最大数の 4 倍まで、およびサポートされるクライアントの最大数の半分まで拡張できます。

WSA 不正イベント機能は、Cisco DNA Center およびその他のサードパーティ インフラストラクチャでサポートされています。

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。

	コマンドまたはアクション	目的
ステップ 2	**network-assurance enable** 例： `Device# network-assurance enable`	Wireless Service Assurance を有効にします。
ステップ 3	**wireless wps rogue network-assurance enable** 例： `Device# wireless wps rogue network-assurance enable`	不正デバイスに対する Wireless Service Assurance を有効にします。これにより、WSA 不正イベントがイベント キューに送信されます。

Wireless Service Assurance 不正イベントのモニターリング

手順

- **show wireless wps rogue stats**

  例：

```
Device# show wireless wps rogue stats

WSA Events
  Total WSA Events Triggered            : 9
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 2
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 3
    ROGUE_AP_IMPERSONATION_DETECTED     : 4
  Total WSA Events Enqueued             : 6
    ROGUE_POTENTIAL_HONEYPOT_DETECTED   : 1
    ROGUE_POTENTIAL_HONEYPOT_CLEARED    : 2
    ROGUE_AP_IMPERSONATION_DETECTED     : 3
```

  この例では、9 つのイベントがトリガーされていますが、そのうちの 6 つだけがキューに入れられています。これは、WSA 不正機能が有効になる前に 3 つのイベントがトリガーされたためです。

- **show wireless wps rogue stats internal**

  show wireless wps rogue ap detailed *rogue-ap-mac-addr*

  これらのコマンドは、WSA イベントに関連する情報をイベント履歴に表示します。