不正なアクセス ポイントの分類

- 不正なアクセス ポイントの分類について （1 ページ）
- 不正アクセスポイントの分類に関する注意事項と制約事項 （3 ページ）
- 不正なアクセス ポイントの分類方法 （4 ページ）
- 不正分類ルールのモニターリング （10 ページ）
- 例：不正なアクセス ポイントの分類 （10 ページ）

不正なアクセス ポイントの分類について

組み込みワイヤレスコントローラソフトウェアでは、不正なアクセスポイントを Friendly、Malicious、または Unclassified に分類して表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも使用されません。ルールを有効にする必要があります。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成または変更し、条件を設定して有効にすると、すべての不正アクセス ポイントが再分類されます。ルールを変更するたびに、すべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にルールが適用されます。

（注）

- ルールベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。
- 組み込みワイヤレスコントローラごとに最大 64 個の不正分類ルールを設定できます。

組み込みワイヤレスコントローラは、管理対象のアクセスポイントの 1 つから不正レポートを受信すると、次のように応答します。

- 不明なアクセスポイントが危険性のない MAC アドレスのリストに含まれている場合、組み込みワイヤレスコントローラはそのアクセスポイントを Friendly に分類します。
- 不明なアクセスポイントが危険性のない MAC アドレスのリストに含まれていない場合、組み込みワイヤレスコントローラはそのアクセスポイントに対して不正分類ルールの適用を開始します。

-
- 設定されているルールの条件に不正アクセスポイントが一致すると、組み込みワイヤレスコントローラはそのルールに設定された分類タイプに基づいて不正を分類します。
- 設定されたルールのいずれにも不正アクセスポイントが一致しない場合、不正はUnclassifiedのままになります。

  組み込みワイヤレスコントローラは、すべての不正アクセスポイントに対して上記の手順を繰り返します。
- 不正アクセスポイントが同じ有線ネットワーク上で検出されると、ルールが設定されていなくても、 組み込みワイヤレスコントローラは不正の状態を Threat とマークし、そのアクセスポイントを自動的に Malicious に分類します。その後は、不正を手動で封じ込めて不正の状態を Contained に変更できます。不正アクセスポイントがネットワーク上で使用不可能な場合、 組み込みワイヤレスコントローラは不正の状態を Alert としてマークします。その後は、不正を手動で封じ込めることができます。
- 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

表 *1:* 分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセス ポイントが WLAN のセキュリティに脅威を与えない場合は、手動で Friendly、Internal に設定できます。たとえば、ラボ ネットワーク内のアクセス ポイントがこれに該当します。 • External：ネットワーク内に存在する不明なアクセスポイントがWLANのセキュリティに脅威を与えない場合は、手動でFriendly、Externalに設定できます。たとえば、隣接するコーヒー ショップのアクセス ポイントがこれに該当します。 • Alert：
Malicious	• Alert： • Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
Unclassified	• Alert： • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。

前述したように、ユーザー定義のルールに基づいて、未知のアクセスポイントの分類タイプと不正の状態を組み込みワイヤレスコントローラで自動的に変更できます。または、手動で未知のアクセス ポイントを別の分類タイプや不正の状態に移行させることも可能です。

不正アクセスポイントの分類に関する注意事項と制約事項

- カスタムタイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で Custom として分類することはできません。カスタム クラスの変更は、不正ルールが使用されている場合にのみ行われます。
- 一部の は、不正分類の変更に対して、ルールによって 30 分ごとに封じ込めのために送信されます。
- 不正ルールは、優先順位に従って、組み込みワイヤレスコントローラ内のすべての新しい着信不正レポートに適用されます。
- 不正がのルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 不正 AP が Friendly に分類される
- コントローラが AP からのネイバーレポートを介してすべての AP を検出するまで、不正 AP は検出後から 3 分間、未設定状態に維持されます。3 分後、不正ポリシーが不正 AP に適用され、AP は、Unclassified、Friendly、Malicious、またはカスタムクラスに移動されます。未設定状態のままになっている不正 AP は、不正ポリシーがまだ適用されていないことを意味します。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの封じ込めのために不正な BSSID が送信された場合、コントローラに十分なリソースがある場合は封じ込められます。特定の封じ込まれた不正 AP を検出した AP は、DEAUTH パケットのブロードキャストを開始します。

  封じ込まれた不正な BSSID に接続されているワイヤレスクライアントは、DEAUTH パケットを受信すると切断されます。ただし、クライアントが接続状態にあると想定すると、再接続が繰り返し試行され、ワイヤレスクライアントのユーザー ブラウジング エクスペリエンスが悪影響を受けます。

  また、スタジアムのような高 RF 環境では、DEAUTH パケットがブロードキャストされますが、クライアントは RF 妨害のためにすべてのパケットを受信できません。このシナリオでは、クライアントが完全に切断されていない可能性がありますが、深刻な影響を受けます。

不正なアクセス ポイントの分類方法

不正アクセス ポイントおよびクライアントの手動による分類（GUI）

手順

ステップ 1 [Monitoring] > [Wireless] > [Rogues] の順に選択します。
ステップ 2 [Unclassified] タブで AP を選択し、下部のペインに詳細を表示します。
ステップ 3 [Class Type] ドロップダウンを使用して、ステータスを設定します。
ステップ 4 [Apply] をクリックします。

不正アクセス ポイントおよびクライアントの手動による分類（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 adhoc** { **alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} 例： `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	アドホック不正を検出して報告します。 **adhoc** キーワードの後に、次のいずれかのオプションを入力します。 • **alert**：アドホック不正アクセス ポイントをアラート モードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **auto-contain**：アドホック不正の自動的な封じ込めを自動封じ込めモードに設定します。 • **contain**：アドホック不正アクセス ポイントの封じ込めを封じ込めモードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力し、

	コマンドまたはアクション	目的
		containment-level パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。 • **external**：アドホック不正アクセス ポイントを **external** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **internal**：アドホック不正アクセス ポイントを **internal** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。
ステップ 3	**wireless wps rogue ap** { **friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} 例： `Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	不正アクセス ポイントを設定します。 **ap** キーワードの後に、次のいずれかのオプションを入力します。 • **friendly**：危険性のない不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **internal** または **external** のいずれかのオプションを入力します。**internal** オプションを選択した場合は、外部アクセス ポイントを信頼していることを示します。**external** オプションを選択した場合は、不正アクセス ポイントの存在を認識していることを示します。 • **malicious**：悪意のある不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **alert** または **contain** のいずれかのオプションを入力します。

	コマンドまたはアクション	目的
		• **alert**：悪意のある不正アクセス ポイントを**アラート** モードに設定します。 • **contain**：悪意のある不正アクセス ポイントを**封じ込め**モードに設定します。このオプションを選択した場合は、*containment-level* パラメータに封じ込めレベルを入力します。有効な範囲は 1 ～ 4 です。
ステップ 4	**wireless wps rogue client** { **contain** *mac-addr containment-level*} 例： `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	不正クライアントを設定します。 **client** キーワードの後に次のオプションを入力します。 **contain**：不正クライアントを封じ込めます。このオプションを選択した後は、*mac-addr* パラメータに MAC アドレスを入力し、*containment-level* パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。
ステップ 5	**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。

不正分類ルールの設定（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 [Rogue AP Rules] タブを選択します。

ステップ 3 [Rogue AP Rules] ページで、**ルール**の名前をクリックするか、[Add] をクリックして新しいルールを作成します。

ステップ 4 表示される [Add/Edit Rogue AP Rule] ウィンドウで、[Rule Name] フィールドにルールの名前を入力します。

ステップ 5 次の [Rule Type] ドロップダウンリストのオプションからルール タイプを選択します。

- Friendly

- Malicious
- Unclassified
- Custom

不正分類ルールの設定（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 rule** *rule-name* **priority** *priority* 例： `Device(config)# wireless wps rogue rule rule_3 priority 3`	ルールを作成またはイネーブルにします。ルールの作成時にルールのプライオリティを入力する必要があります。 （注） ルールの作成後に編集およびプライオリティの変更が可能なのは、無効になっている不正ルールのみです。有効になっている不正ルールのプライオリティは変更できません。編集時の不正ルールのプライオリティ変更は任意です。

ステップ 3	**classify** {**friendly state** {**alert** | **external** | **internal**} | **malicious state** {**alert** | **contained** }}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# classify friendly`
		• **friendly**：危険性のない不正アクセス ポイントを設定します。その後、**state** キーワードに続けて、**alert**、**internal**、または **external** のいずれかのオプションを入力します。**internal** オプションを選択した場合は、外部アクセスポイントを信頼していることを示します。**external** オプションを選択した場合は、不正アクセスポイントの存在を認識していることを示します。
		• **malicious**：悪意のある不正アクセス ポイントを設定します。その

	コマンドまたはアクション	目的
		後、state キーワードに続けて alert または contained のいずれかのオプションを入力します。 • alert：悪意のある不正アクセスポイントをアラートモードに設定します。 • contained：悪意のある不正アクセスポイントを封じ込めモードに設定します。

ステップ 4	**condition** {**client-count** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# condition client-count 5`
		不正アクセスポイントが満たす必要がある次の条件をルールに追加します。
		• **client-count**：不正アクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正アクセスポイントに関連付けられているクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、不正アクセスポイントに関連付けられるクライアントの最小数をパラメータに入力します。有効な範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
		• **duration**：不正アクセス ポイントが最小期間で検出される必要があります。このオプションを選択する場合は、パラメータに最小検出期間の値を入力します。有効な範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
		• **encryption**：アドバタイズされた WLAN で暗号化が無効になっている必要があります。任意のタイプの暗号化には any、暗号化なしの場合は off、WPA 暗号化の場合は wpa1、WPA2 暗号化の場合は wpa2、WPA3 OWE 暗号化の場合

	コマンドまたはアクション	目的
		はwpa3-owe、WPA3 SAE暗号化の場合はwpa3-saeを選択できます。 • **infrastructure**：SSIDがコントローラで認識される必要があります。 • **rssi**：有効な範囲は -95 ～ -50 dBm（両端の値を含む）です。 • **ssid**：不正アクセスポイントには、特定の SSID が必要です。最大 25 個の異なるSSIDを指定できます。コントローラによって管理されていない SSID を指定する必要があります。このオプションを選択する場合は、パラメータに SSID を入力します。 • **wildcard-ssid**：SSID 文字列に一致する可能性のある表現を指定できます。SSID は最大 25 個指定できます。

ステップ 5	**match** {**all** | **any**}
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# match all`
		検出された不正アクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。

ステップ 6	**default**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# default`
		コマンドをデフォルトに設定します。

ステップ 7	**exit**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# exit`
	`Device(config)#`
		サブモードを終了します。

	コマンドまたはアクション	目的

ステップ 8	**shutdown**
	例：
	`Device(config)# wireless wps rogue rule rule_3 priority 3`
	`Device(config-rule)# shutdown`
		特定の不正ルールを無効にします。この例では、ルール **rule_3** が無効になります。

ステップ 9	**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。
ステップ 10	**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 11	**wireless wps rogue rule shutdown** 例： `Device(config)# wireless wps rogue rule shutdown`	すべての不正ルールを無効にします。
ステップ 12	**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。

不正分類ルールのモニターリング

次のコマンドを使用して、不正分類ルールをモニタリングできます。

表 *2:* 不正分類ルールのモニターリング用コマンド

コマンド	目的
show wireless wps rogue rule detailed	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	分類ルールの概要を表示します。

例：不正なアクセス ポイントの分類

次に、MAC アドレスが 00:11:22:33:44:55 の不正 AP を Malicious として分類し、2 つの管理対象 AP に含まれているとマークする例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue ap malicious 0011.2233.4455 state contain 2
```

次に、SSID my-friendly-ssid を使用している不正 AP を分類できるルールを作成する方法、および少なくとも 1000 秒間、Friendly Internal として表示される例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition ssid my-friendly-ssid
Device(config-rule)# condition duration 1000
Device(config-rule)# match all
Device(config-rule)# classify friendly state internal
```

この例は、不正アクセス ポイントが満たす必要がある条件を適用する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# end
```

例：不正なアクセス ポイントの分類