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
- 不正なアクセス ポイントの分類の制限，4 ページ
- 不正分類ルールの設定（GUI），5 ページ
- 不正なデバイスの表示および分類（GUI），9 ページ
- 不正分類ルールの設定（CLI），12 ページ
- 不正なデバイスの表示および分類（CLI），15 ページ

不正なアクセス ポイントの分類について

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、Custom または Unclassified に分類して表示するルールを作成できます。 カスタム タイプの場合、重大度スコアと分類の名前を指定する必要があります。

（注） 手動分類と、auto-containment または rogue-on-wire の結果行われた分類は、不正ルールをオーバーライドします。 不正な AP のクラスおよび/または状態を手動で変更し、不正ルールを AP に適用する場合、それを Unclassified および Alert 状態に変更する必要があります。

デフォルトでは、いずれの分類ルールも有効になっていません。 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。 ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセスポイントは分類し直されます。 ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、Custom および Unclassified）にそのルールが適用されます。

1 台のコントローラにつき最大 64 の不正分類ルールを設定できます。

また、クライアントカウント状態を除くアドホック不正に、不正ルールを適用できます。

不正アクセス ポイントのデータベース テーブルに格納できる不正クライアントの最大数は 256 です。

RSSI 不正ルール状態によって不正な AP またはアドホック不正が分類される場合、トリガーを生じた RSSI 値がコントローラの GUI/CLI に表示されます。 コントローラには、トラップにある分類された RSSI、分類された AP MAC アドレス、およびルール名が含まれます。 新しいトラップは、新しい分類が作成されるか、不正ルールによって状態が変更するたびに生成されますが、そのレートは不正な AP またはアドホック不正に対して 30 分ごとに制限されています。 ただし、不正ルールによる阻止で状態が変更した場合、トラップは即座に送信されます。 デフォルト以外の分類タイプ（Friendly、Malicious、および Custom 分類）に有効な値は、「classified by」、「classified at」、および「classified by rule name」です。 未分類のタイプの場合、これらのフィールドは表示されません。

（注） 不正ルールの RSSI 状態の場合、再分類は RSSI の変動が設定された RSSI 値の 2 dBm よりも多い場合にのみ行われます。

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。

1. コントローラは未知（管理対象外）のアクセス 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か確認します。 そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス 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、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。 不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。 不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、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、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。 不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。
8. 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：未知（管理対象外）のアクセス ポイントがネットワーク内に存在し、WLANのセキュリティに脅威を与えない場合、手動でFriendly、Internalに設定します。 たとえば、ラボ ネットワーク内のアクセス ポイントなどです。 • External：未知（管理対象外）のアクセス ポイントがネットワーク外に存在し、WLANのセキュリティに脅威を与えない場合、手動でFriendly、External に設定します。 たとえば、近隣のコーヒー ショップに属するアクセス ポイントなどです。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。
Malicious	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • 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。
カスタム	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • 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。

ルールベースの分類タイプ	不正の状態
未分類	• Pending：最初の検出で、未知（管理対象外）のアクセス ポイントは 3 分間 Pending 状態に置かれます。 この間に、管理対象のアクセス ポイントでは、未知（管理対象外）のアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • 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。 • Contained Pending：未知（管理対象外）のアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

分類および不正アクセス ポイントのステータスは以下のように設定されています。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。 不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正なアクセス ポイントの分類の制限

いくつかの不正なルールがあります。 その内容は次のとおりです。

- 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を使用する場合にのみ行えます。
- 不正分類の変更に対して、ルールによって 30 分ごとに阻止用のトラップが送信されます。 カスタム分類の場合、最初のトラップはカスタム分類よりも前に存在していたため、そのトラップに重大度スコアは含まれません。 不正が分類されると、30 分後に生成される後続のトラップから重大度スコアが取得されます。
- 不正ルールは、優先順位に従って、コントローラ内の新しい着信不正レポートごとに適用されます。

- 不正がより高い優先度ルールを満たし、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。
- 以前に分類された不正は、次の制限に従って、新しい不正レポートが作成されるたびに、再分類されます。
  - ルールによって Friendly に分類され、状態が ALERT に設定されている不正は、新しい不正レポートを受け取ると再分類が開始されます。
  - 不正が管理者によって Friendly に手動で分類されると、状態は INTERNAL になり、次に続く不正レポートで再分類されません。
  - 不正が Malicious に分類されると、その状態に関係なく、後続の不正レポートで再分類されません。
- 一部の属性が新しい不正レポートで欠落している場合、複数の不正ルールによって、Friendly から Malicious に不正の状態が遷移する可能性があります。
- どの不正ルールによっても、Malicious から他の分類に不正の状態が遷移することはありません。
- 不正なデバイスを異なるクラス タイプ間で移動した場合、不正なデバイスの contain または alert へのステータス変更は、不正なクラス タイプを unclassified に移動するまで機能しません。

不正分類ルールの設定（GUI）

ステップ 1 [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] を選択して、[Rogue Rules] ページを開きます。
すでに作成されているすべてのルールが優先順位に従って一覧表示されます。 各ルールの名前、タイプ、およびステータスが表示されます。

（注） ルールを削除するには、そのルールの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

ステップ 2 次の手順を実行して、新しいルールを作成します。

a) [Add Rule] をクリックします。 [Add Rule] セクションがページ上部に表示されます。
b) [Rule Name] テキスト ボックスに、新しいルールの名前を入力します。 名前にはスペースを含めないでください。
c) [Rule Type] ドロップダウン リストで、以下のオプションから選択してこのルールと一致する不正アクセス ポイントを [Friendly] または [Malicious] として分類します。
   - Friendly
   - Malicious
   - カスタム

d) [Notify] ドロップダウン リストから、ルールがマッチする場合の通知を [All]、[Global]、[Local]、または [None] に設定します。

（注） [Rogue Rule Notification] のオプション [All]、[Global]、[Local]、および [None] は、次の不正トラップだけを制御できます。

- Rogue AP Detected (Rogue AP: XX:XX:XX:XX:XX:XX detected on Base Radio MAC: XX:XX:XX:XX:XX:XX Interface no: 0(1) Channel: 6 RSSI: 45 SNR: 10 Classification: unclassified, State: alert, RuleClassified : unclassified, Severity Score: 100, RuleName: rule1, Classified AP MAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue Adhoc Detected (Adhoc Rogue : XX:XX:XX:XX:XX:XX detected on Base Radio MAC : XX:XX:XX:XX:XX:XX Interface no: 0(1) on Channel 6 with RSSI: 45 and SNR: 10 Classification: unclassified, State: alert, RuleClassified: unclassified, Severity Score: 100, RuleName: rule1,Classified APMAC: XX:XX:XX:XX:XX:XX, Classified RSSI: 45)
- Rogue AP contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX has been contained due to rule with containment Level : 1)
- Rogue AP clear contained (Rogue AP: Rogue with MAC Address: XX:XX:XX:XX:XX:XX is no longer contained due to rule

e) [State] ドロップダウン リストから、ルールがマッチする場合の不正な AP の状態を構成します。

f) [Rule Type] を [Custom] に選択する場合、[Severity Score] と [Classification Name] に入力します。

g) [Add] をクリックして既存のルール リストにこのルールを追加するか、[Cancel] をクリックしてこの新しいルールを破棄します。

ステップ 3 次の手順を実行して、ルールを編集します。

a) 編集するルールの名前をクリックします。 [Rogue Rule > Edit] ページが表示されます。

b) [Type] ドロップダウン リストで、以下のオプションから選択してこのルールと一致する不正アクセス ポイントを分類します。

- Friendly
- Malicious
- カスタム

c) [Notify] ドロップダウン リストから、ルールがマッチする場合の通知を [All]、[Global]、[Local]、または [None] に設定します。

d) [State] ドロップダウン リストから、ルールがマッチする場合の不正な AP の状態を構成します。

e) [Match Operation] テキスト ボックスから、次のいずれかを選択します。

[Match All]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定されたすべての条件を満たしている場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。

[Match Any]：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定された条件のいずれかを満たす場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。 これはデフォルト値です。

f) このルールを有効にするには、[Enable Rule] チェックボックスをオンにします。 デフォルト値はオフです。

g) [Rule Type] を [Custom] に選択する場合、[Severity Score] と [Classification Name] に入力します。

h) [Add Condition] ドロップダウン リストで、不正なアクセス ポイントが満たす必要がある次の条件から 1 つまたは複数を選択し、[Add Condition] をクリックします。

- [SSID]：不正なアクセス ポイントには、特定のユーザ設定 SSID が必要です。 このオプションを選択する場合は、[User Configured SSID] テキスト ボックスに SSID を入力し、[Add SSID] をクリックします。

  （注） SSID を削除するには、SSID を強調表示して [Remove] をクリックします。

- [RSSI]：不正なアクセスポイントには、最小の受信信号強度インジケータ（RSSI）値が必要です。 たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス 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、[Minimum RSSI] テキスト ボックスに最小 RSSI 値を入力します。 有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。

- [Duration]：不正なアクセス ポイントが最小期間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、[Time Duration] テキスト ボックスに最小検出期間の値を入力します。 有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。

- [Client Count]：不正なアクセス 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、不正なアクセスポイントにアソシエートされた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、[Minimum Number of Rogue Clients] テキスト ボックスに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。 有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。

- [No Encryption]：不正なアクセス ポイントの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。 不正なアクセスポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセスポイントに対してアソシエートを試行します。 このオプションに関して、これ以外の設定を行う必要はありません。

  （注） Cisco Prime Infrastructure は、このオプションを「Open Authentication（オープンな認証）」と呼んでいます。

- [Managed SSID]：不正なアクセス ポイントの管理対象 SSID（WLAN に設定された SSID）がコントローラで認識される必要があります。 このオプションに関して、これ以外の設定を行う必要はありません。

  （注） SSID および管理対象 SSID の 2 つのリストは相互に排他的であるため、[SSID] および [Managed SSID] の条件を [Match All] 操作で使用することはできません。 [Match All] を使用してルールを定義し、これら 2 つの条件を設定した場合は、いずれかの条件が満たされないので、不正なアクセス ポイントが Friendly または Malicious に分類されることはありません。

  1 つのルールにつき最大 6 つの条件を追加できます。 条件を追加すると、[Conditions] セクションにその条件が表示されます。

（注） 条件を削除するには、その条件の青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

- [SSID Wildcard]：不正なアクセス ポイントに特定のユーザ設定 SSID のサブストリングが存在する必要があります。 コントローラは同じ発生パターン内でサブ文字列を検索し、サブ文字列が SSID の文字列全体で見つかった場合はその一致を返します。

i) [Apply] をクリックします。

ステップ 4 [Save Configuration] をクリックします。

ステップ 5 不正分類ルールを適用する順序を変更する場合の手順は、次のとおりです。

1. [Back] をクリックして、[Rogue Rules] ページに戻ります。
2. [Change Priority] をクリックして、[Rogue Rules > Priority] ページにアクセスします。

   不正ルールが優先順位に従って [Change Rules Priority] テキスト ボックスに表示されます。
3. 優先順位を変更するルールを強調表示し、[Up] をクリックしてリスト内の順位を上げるか、[Down] をクリックしてリスト内の順位を下げます。
4. 目的の順位になるまで、ルールを上または下に移動します。
5. [Apply] をクリックします。

ステップ 6 次の手順を実行して、任意の不正なアクセス ポイントを Friendly に分類し、危険性のない MAC アドレス リストに追加します。

- [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Friendly Rogue] の順に選択して、[Friendly Rogue > Create] ページにアクセスします。
- [MAC Address] テキスト ボックスに、危険性のない不正なアクセス ポイントの MAC アドレスを入力します。
- [Apply] をクリックします。
- [Save Configuration] をクリックします。 このアクセス ポイントは、コントローラの、危険性のないアクセス ポイントのリストに追加され、[Friendly Rogue APs] ページに表示されます。

不正なデバイスの表示および分類（GUI）

はじめる前に

⚠

注意 **不正なデバイスを封じ込める**ことを選択すると、「There may be legal issues following this containment. Are you sure you want to continue?」という警告メッセージが表示されます。工業、科学、医療用（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。 したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

ステップ 1 [Monitor] > [Rogues] の順に選択します。

ステップ 2 次のオプションを選択すると、コントローラで検出された各タイプの不正なアクセス ポイントを表示できます。

- Friendly APs
- Malicious APs
- Unclassified APs
- Custom APs

不正な AP の各ページには、不正アクセス ポイントの MAC アドレスと SSID、チャネル番号、不正なアクセス ポイントが検出された無線の数、不正アクセス ポイントに接続しているクライアントの数、および不正アクセス ポイントの現在のステータスの情報が含まれます。

（注） データベースから認識済みの不正を削除するには、不正状態を Alert に変更します。 不正が存在しなくなれば、不正データが 20 分以内にデータベースから削除されます。

（注） これらのいずれかのページから不正なアクセス ポイントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。 複数の不正なアクセスポイントを削除するには、削除対象の行に該当するチェックボックスをオンにし、[Remove] をクリックします。

（注） それぞれのページで [Move to Alert] ボタンをクリックして、阻止されているまたは阻止された悪意のある未分類の不正 AP を Alert 状態に戻すことができます。

ステップ 3 不正なアクセス ポイントの詳細を取得するには、アクセスポイントの MAC アドレスをクリックします。[Rogue AP Detail] ページが表示されます。
このページには、不正なデバイスの MAC アドレス、不正なデバイスのタイプ（アクセスポイントなど）、不正なデバイスが有線ネットワーク上にあるかどうか、不正なデバイスが最初および最後に報告された日時、デバイスの現在のステータスといった情報が表示されます。

[Class Type] テキスト ボックスには、この不正なアクセス ポイントの現在の分類が表示されます。

- [Friendly]：ユーザ定義の Friendly ルールと一致した不明なアクセス ポイント、または既知の不正なアクセス ポイント。 危険性のないアクセス ポイントは阻止することができません。

- [Malicious]：ユーザ定義の Malicious ルールと一致した不明なアクセス ポイント、またはユーザが Friendly または Unclassified 分類タイプから手動で移動した不明なアクセス ポイント。

  （注） アクセス ポイントが Malicious に分類されると、その後でそのアクセス ポイントにルールを適用することはできなくなります。また、別の分類タイプに移動することもできません。危険性のあるアクセス ポイントを Unclassified 分類タイプに移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

- [Unclassified]：ユーザ定義の Friendly または Malicious ルールと一致しない不明なアクセス ポイント。未分類のアクセス ポイントは阻止することができます。 また、このアクセス ポイントは、ユーザ定義のルールに従って自動的に、またはユーザが手動で、Friendly または Malicious 分類タイプに移動できます。

- [Custom]：不正ルールに関連付けられている、ユーザ定義の分類タイプ。 手動で不正を Custom に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を使用する場合にのみ行えます。

ステップ 4 このデバイスの分類を変更するには、[Class Type] ドロップダウン リストから別の分類を選択します。

（注） 不正なアクセス ポイントの現在の状態が [Contain] である場合、そのアクセス ポイントは移動できません。

ステップ 5 [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、この不正なアクセス ポイントに対するコントローラの応答方法を指定します。

- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。 このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。 このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。 このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。

ページの下部には、この不正なアクセス ポイントが検出されたアクセス ポイントと、不正なアクセス ポイントにアソシエートされたすべてのクライアントの両方に関する情報が提供されます。 クライアントの詳細を表示するには、[Edit] をクリックして [Rogue Client Detail] ページを開きます。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

ステップ 8 コントローラに接続された不正なクライアントを表示するには、[Rogue Clients] を選択します。 [Rogue Clients] ページが表示されます。 このページには、不正なクライアントの MAC アドレス、不正なクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID、不

正なクライアントが検出された無線の数、不正なクライアントが最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

ステップ 9 不正なクライアントの詳細情報を取得するには、そのクライアントの MAC アドレスをクリックします。[Rogue Client Detail] ページが表示されます。
このページには、不正なクライアントの MAC アドレス、このクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID および IP アドレス、不正なクライアントが最初および最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

ステップ 10 [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、この不正なクライアントに対するコントローラの応答方法を指定します。

- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。

ページの下部には、この不正なクライアントが検出されたアクセス ポイントに関する情報が提供されます。

ステップ 11 [Apply] をクリックします。

ステップ 12 必要に応じて [Ping] をクリックすると、このクライアントへのコントローラの接続をテストできます。

ステップ 13 [Save Configuration] をクリックします。

ステップ 14 コントローラで検出されたアドホック不正を確認するには、[Adhoc Rogues] を選択します。 [Adhoc Rogues] ページが表示されます。
このページには、MAC アドレス、BSSID、アドホック不正の SSID、アドホック不正が検出された無線の数、アドホック不正の現在のステータスといった情報が表示されます。

ステップ 15 アドホック不正の詳細情報を取得するには、その不正の MAC アドレスをクリックします。 [Adhoc Rogue Detail] ページが表示されます。
このページには、アドホック不正の MAC アドレスおよび BSSID、不正が最初および最後に報告された日時、不正の現在のステータスといった情報が表示されます。

ステップ 16 [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、このアドホック不正に対するコントローラの応答方法を指定します。

- [Contain]：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert]：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
- [Internal]：コントローラはこの不正なアクセス ポイントを信頼します。
- [External]：コントローラはこの不正なアクセス ポイントの存在を認識します。

ステップ 17 [Maximum number of APs to contain the rogue] ドロップダウン リストから、[1]、[2]、[3]、[4] のオプションのいずれかを選択して、このアドホック不正を阻止するために使用するアクセス ポイントの最大数を指定します。

ページの下部には、このアドホック不正が検出されたアクセス ポイントに関する情報が提供されます。

- 1：対象の不正なアクセス ポイントが 1 つのアクセス ポイントで阻止されることを指定します。 これは最も低い阻止レベルです。
- 2：対象の不正なアクセス ポイントが 2 つのアクセス ポイントで阻止されることを指定します。
- 3：対象の不正なアクセス ポイントが 3 つのアクセス ポイントで阻止されることを指定します。
- 4：対象の不正なアクセス ポイントが 4 つのアクセス ポイントで阻止されることを指定します。 これは最も高い阻止レベルです。

ステップ 18 [Apply] をクリックします。

ステップ 19 [Save Configuration] をクリックします。

ステップ 20 無視するように設定されている任意のアクセス ポイントを表示するには、[Rogue AP Ignore-List] を選択します。 [Rogue AP Ignore-List] ページが表示されます。
このページには、無視するように設定されている任意のアクセス ポイントの MAC アドレスが表示されます。 不正無視リストには、ユーザが Cisco Prime Infrastructure マップに手動で追加した任意の自律アクセス ポイントのリストが含まれています。 コントローラでは、これらの自律アクセス ポイントが、Prime Infrastructure によって管理されていても不正と見なされます。 不正無視リストを使用すると、コントローラでこれらのアクセス ポイントを無視できます。 このリストは次のように更新されます。

- コントローラは、不正レポートを受信すると、不明なアクセス ポイントが不正無視アクセス ポイント リストに存在するかどうかを確認します。
- 不明なアクセス ポイントが不正無視リストに存在する場合、コントローラはこのアクセス ポイントを無視して他の不正なアクセス ポイントの処理を続けます。
- 不明なアクセス ポイントが不正無視リストにない場合、コントローラは Prime Infrastructure にトラップを送信します。 Prime Infrastructure が自律アクセス ポイントにこのアクセス ポイントを検出した場合、Prime Infrastructure はこのアクセス ポイントを不正無視リストに追加するためのコマンドをコントローラに送信します。 このアクセス ポイントは、今後の不正レポートで無視されるようになります。
- ユーザが Prime Infrastructure から自律アクセス ポイントを削除した場合、Prime Infrastructure はこのアクセス ポイントを不正無視リストから削除するコマンドをコントローラに送信します。

不正分類ルールの設定（CLI）

ステップ 1 次のコマンドを入力して、ルールを作成します。
config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule-name*

後でこのルールの優先順位を変更し、それに従ってリスト内の他の順番も変更する場合は、**config rogue rule priority** *priority rule-name* コマンドを入力します。

後でこのルールの分類を変更する場合は、**config rogue rule classify** {**friendly** | **malicious**} *rule-name* コマンドを入力します。

すべての不正分類ルールまたは特定のルールを削除するには、{**config rogue rule delete** {**all** | *rule-name*} コマンドを入力します。

ステップ 2 次のコマンドを入力して、ルールを作成します。

- 次のコマンドを入力して、Friendly 不正のルールを設定します。
  config rogue rule add ap priority *priority* **classify friendly notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **internal** | **external** | **delete**} *rule-name*
- 次のコマンドを入力して、Malicious 不正のルールを設定します。
  config rogue rule add ap priority *priority* **classify malicious notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*
- 次のコマンドを入力して、Custom 不正のルールを設定します。
  config rogue rule add ap priority *priority* **classify custom** *severity-score classification-name* **notify** {**all** | **global** | **local** | **none**} **state** {**alert** | **contain**} *rule-name*

後でこのルールの優先順位を変更し、それに従ってリスト内の他の順番も変更する場合は、**config rogue rule priority** *priority rule-name* コマンドを入力します。

後でこのルールの分類を変更する場合は、**config rogue rule classify** {**friendly** | **malicious** | **custom** *severity-score classification-name*} *rule-name* コマンドを入力します。

すべての不正分類ルールまたは特定のルールを削除するには、{**config rogue rule delete** {**all** | *rule-name*} コマンドを入力します。

ステップ 3 次のコマンドを入力して、ルールに基づき、不正 AP の状態を設定します。
config rogue rule state {**alert** | **contain** | **internal** | **external**} *rule-name*

ステップ 4 次のコマンドを入力して、ルール マッチの通知を設定します。
config rogue rule notify {**all** | **global** | **local** | **none**} *rule-name*

ステップ 5 次のコマンドを入力して、すべてのルールまたは特定のルールを無効にします。
config rogue rule disable {*all* | *rule_name*}

（注） ルールの属性を変更する前にルールを無効にする必要があります。

ステップ 6 次のコマンドを入力して、不正なアクセス ポイントが満たす必要があるルールに条件を追加します。
config rogue rule condition ap set *condition_type condition_value rule_name*

利用可能な状態の種類は、次のとおりです。

- **ssid**：不正なアクセス ポイントには、特定の SSID が必要です。 コントローラによって管理されない SSID を追加する必要があります。 このオプションを選択する場合は、*condition_value* パラメータに SSID を入力します。 SSID はユーザ設定の SSID リストに追加されます。

（注） ユーザ設定の SSID リストからすべての SSID または特定の SSID を削除するには、**config rogue rule condition ap delete ssid** {**all** | **ssid**} *rule_name* コマンドを入力します。

- **rssi**：不正なアクセス ポイントには、最小の RSSI 値が必要です。 たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス 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、*condition_value* パラメータに最小 RSSI 値を入力します。 有効な値の範囲は -95 ～ -50 dBm（両端の値を含む）で、デフォルト値は 0 dBm です。
- **duration**：不正なアクセス ポイントが最小期間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、*condition_value* パラメータに最小検出期間の値を入力します。 有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
- **client-count**：不正なアクセス 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、不正なアクセス ポイントにアソシエートされた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、*condition_value* パラメータに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。 有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
- **managed-ssid**：不正なアクセス ポイントの SSID がコントローラで認識される必要があります。 このオプションには *condition_value* パラメータは必要ありません。

  （注） 1 つのルールにつき最大 6 つの条件を追加できます。 ルールからすべての条件または特定の条件を削除するには、**config rogue rule condition ap delete all** *condition_type condition_value rule_name* コマンドを入力します。

- **wildcard-ssid**：不正なアクセス ポイントに特定のユーザ設定 SSID のワイルドカードが存在する必要があります。 サブストリングが SSID の全文字列内で検出されると、コントローラは同じ発生パターンのワイルドカードを検索して一致を返します。

ステップ 7 検出された不正なアクセス ポイントがルールに一致しているとみなされ、そのルールの分類タイプが適用されるためには、ルールで指定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。
config rogue rule match {**all** | **any**} *rule_name*

ステップ 8 次のコマンドを入力して、すべてのルールまたは特定のルールを有効にします。
config rogue rule enable {**all** | **rule_name**}
（注） 変更を有効にするには、ルールを有効にする必要があります。

ステップ 9 次のコマンドを入力して、新しい危険性のないアクセス ポイント エントリを危険性のない MAC アドレスのリストに追加したり、リストから既存の危険性のないアクセス ポイント エントリを削除したりします。
config rogue ap friendly {**add** | **delete**} *ap_mac_address*

ステップ 10 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 11 次のコマンドを入力して、コントローラ上に設定されている不正分類ルールを表示します。
show rogue rule summary

ステップ 12 次のコマンドを入力して、特定の不正分類ルールの詳細情報を表示します。
show rogue rule detailed *rule_name*

不正なデバイスの表示および分類（CLI）

- 次のコマンドを入力して、コントローラによって検出されたすべての不正なアクセスポイントのリストを表示します。
  show rogue ap summary
- 次のコマンドを入力して、コントローラによって検出された危険性のない不正なアクセスポイントのリストを表示します。

  show rogue ap friendly summary
- 次のコマンドを入力して、コントローラによって検出された危険性のある不正なアクセスポイントのリストを表示します。

  show rogue ap malicious summary
- 次のコマンドを入力して、コントローラによって検出された未分類の不正なアクセスポイントのリストを表示します。
  show rogue ap unclassified summary
- 次のコマンドを入力して、特定の不正なアクセスポイントに関する詳細情報を表示します。
  show rogue ap detailed *ap_mac_address*
- 次のコマンドを入力して、特定の 802.11a/n/ac 無線に関する不正レポート（各種チャネル幅で検出された不正なデバイスの数を示す）を表示します。
  show ap auto-rf 802.11a *Cisco_AP*
- 次のコマンドを入力して、不正なアクセスポイントにアソシエートされているすべての不正なクライアントのリストを表示します。
  show rogue ap clients *ap_mac_address*
- 次のコマンドを入力して、コントローラによって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 rogue client summary
- 次のコマンドを入力して、特定の不正なクライアントに関する詳細情報を表示します。
  show rogue client detailed *client_mac_address*
- 次のコマンドを入力して、コントローラによって検出されたすべてのアドホック不正のリストを表示します。
  show rogue adhoc summary
- 次のコマンドを入力して、特定のアドホック不正に関する詳細情報を表示します。
  show rogue adhoc detailed *rogue_mac_address*
- 次のコマンドを入力して、分類に基づいてアドホック不正の要約を表示します。
  show rogue adhoc {friendly | malicious | unclassified} summary
- 次のコマンドを入力して、無視するように設定されている不正なアクセスポイントのリストを表示します。

show rogue ignore-list

（注） 不正無視アクセス ポイント リストの詳細については、「不正なデバイスの表示および分類（GUI）」を参照してください。

- 次のコマンドを入力して、不正なアクセス ポイントを Friendly に分類します。
  config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

  値は次のとおりです。

  internal は、コントローラがこの不正なアクセス ポイントを信頼することを表しています。

  external は、コントローラがこの不正なアクセス ポイントの存在を認識することを表しています。

（注） 不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Friendly クラスに移動することはできません。

- 次のコマンドを入力して、不正なアクセス ポイントに Malicious のマークを付けます。
  config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

  値は次のとおりです。

  alert は、コントローラからシステム管理者に、更なる処理を行うよう即時に警告が転送されることを表しています。

  contain は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。

（注） 不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Malicious クラスに移動することはできません。

- 次のコマンドを入力して、不正なアクセス ポイントに Unclassified のマークを付けます。
  config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

（注） 現在の状態が Contain の場合、不正なアクセス ポイントは Unclassified クラスに移動できません。

alert は、コントローラからシステム管理者に、更なる処理を行うよう即時に警告が転送されることを表しています。

contain は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。

- 次のコマンドを入力して、アドホック不正の阻止に使用するアクセス ポイントの最大数を選択します。
  config rogue ap classify unclassified state contain *rogue_ap_mac_address 1, 2, 3, or 4*
  - 1：対象の不正なアクセス ポイントが 1 つのアクセス ポイントで阻止されることを指定します。 これは最も低い阻止レベルです。
  - 2：対象の不正なアクセス ポイントが 2 つのアクセス ポイントで阻止されることを指定します。
  - 3：対象の不正なアクセス ポイントが 3 つのアクセス ポイントで阻止されることを指定します。
  - 4：対象の不正なアクセス ポイントが 4 つのアクセス ポイントで阻止されることを指定します。 これは最も高い阻止レベルです。
- 次のコマンドのいずれかを入力して、不正なクライアントに対するコントローラの応答方法を指定します。
  config rogue client alert *client_mac_address*：コントローラからシステム管理者に対し、さらなる処理を行うよう即時に警告が転送されます。

  config rogue client contain *client_mac_address*：コントローラによって危険性のあるデバイスが阻止されます。これにより、そのデバイスの信号は、認証されたクライアントに干渉しなくなります。
- 次のコマンドのいずれかを入力して、アドホック不正に対するコントローラの応答方法を指定ます。
  config rogue adhoc alert *rogue_mac_address*：コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。

  config rogue adhoc contain *rogue_mac_address*：コントローラによって危険性のあるデバイスが阻止されます。これにより、そのデバイスの信号は、認証されたクライアントに干渉しなくなります

  config rogue adhoc external *rogue_mac_address*：コントローラによって、このアドホック不正の存在が認識されます。
- これらのコマンドのいずれかを入力して、アドホック不正の分類を設定します。
  - [Friendly] 状態：**config rogue adhoc classify friendly state** {**internal** | **external**} *mac-addr*
  - [Malicious] 状態：**config rogue adhoc classify malicious state** {**alert** | **contain**} *mac-addr*
  - [Unclassified] 状態：**config rogue adhoc classify unclassified state** {**alert** | **contain**} *mac-addr*
- 次のコマンドを入力して、カスタム不正 AP 情報の要約を表示します。
  show rogue ap custom summary
- 次のコマンドを入力して、カスタム アドホック不正情報を表示します。
  show rogue adhoc custom summary
- 次のコマンドを入力して、不正な AP を削除します。
  config rogue ap delete {**class** | **all** | *mac-addr*}

- 次のコマンドを入力して、不正なクライアントを削除します。
  config rogue client delete {**state** | **all** | *mac-addr*}
- 次のコマンドを入力して、アドホック不正を削除します。
  config rogue adhoc delete {**class** | **all** | *mac-addr*}
- 次のコマンドを入力して、変更を保存します。
  save config