



ASパス長違反（AS Path Length Violation）

• [ASパス長違反（AS Path Length Violation）](#)（1 ページ）

ASパス長違反（AS Path Length Violation）

設定されたプレフィックスの AS パス長が上限しきい値または下限しきい値を超えた場合に検出します。このアラームは、観察された AS パスが、AS パス長の下限しきい値を下回るか、上限しきい値を超えた場合に検出します。

BGP AS パスは、プレフィックスの遅延に影響しますが、BGP ベストパス選択（ベストパス選択で使用される最も高い設定不可能な属性）の重要なタイブレークステップでもあります。より短い AS パスが優先されるため、このプロパティはハイジャッカーによって悪用される可能性があります。モニタ対象プレフィックスの AS パス長に予想範囲を設定する必要があります。アドバタイズされたこの範囲外の AS パス長は、違反アドバタイズメントです



- (注) 問題にすぐに対処できるように、問題（ルート情報の漏えい、または何らかのタイプの設定不備）を起こしている可能性があるピアを知っておくと役立ちます。[マイピア（My Peers）]ルールは、特定の Crosswork Cloud サブスクリプションでこのアラームに使用できます。[c_subscription-plan-options.xml](#)[マイピア（My Peers）]オプションは、ピアからの BGP 更新のみに従いますが、[すべてのピア（All Peers）]はピアおよびグローバルピアからの BGP 更新に従います。[ピアの追加](#)このオプションを設定するには、[Crosswork Cloud Network Insights](#)ポリシーの追加、

考えられる検出される問題

このアラームは、ルートルークまたはハイジャックの特定に役立ちます。また、モニタ対象プレフィックスの遅延のモニタにも役立ちます。

関連するアラームルールの設定

このアラームルールをプレフィックスポリシー設定に追加する場合は、次のオプションを設定する必要があります（[外部ルーティング分析（External Routing Analysis）]>[設定（Configure）]

> [ポリシー (Policies)] > [ポリシーの追加 (Add Policy)] > [プレフィックスポリシー (Prefix Policy)] > [ルールの追加 (Add Rule)] > [ASパス長違反 (AS Path Length Violation)] 。

- [しきい値](#)
- [許可されたASパス長の範囲 (Allowed AS path length range)]

例

[ASパス長違反 (AS Path Length Violation)] アラームルールを使用してプレフィックスポリシーを作成し、プレフィックス 8.8.0.0/24 および 9.9.0.0/24 にリンクします。プレフィックス 8.8.0.0/24 は、異なるピアリングポイントを介してユーザによってリークされることにより、AS パスが短くなり、アラームがトリガーされます。アラームは、プレフィックス 8.8.0.0/24 が正当なアドバタイズメント (許可された範囲内のパス長) によってアドバタイズされるとクリアされます。後で、プレフィックス発信元 9.9.0.0/24 からのアップストリームパスでピアリング関係が変更されると (正当または MITM 攻撃により)、より長い AS パスでアドバタイズされます。これらのアップストリーム関係をほとんど制御できない可能性があり、設定された AS パス範囲をアラームがクリアされるように変更する必要があります。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。