



Cisco Crosswork Cloud ユーザーガイド

初版：2020年1月23日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

Short Description

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目次

Short Description ii

第 I 部 :	Crosswork Cloud について 17
第 1 章	Crosswork Cloud 外部ルーティング分析について 1 Crosswork Cloud Network Insights について 1
第 2 章	Crosswork Cloud Traffic Analysis について 3 トラフィック分析について 3
第 3 章	Crosswork Cloud Trust Insights について 5 Trust Insights について 5 Trust Insights で使用されるデータ 6 デバイスからの信頼情報の収集方法 6 Trust Insights による信頼性の測定方法 6 Trust Insights で確認できる内容 7
第 II 部 :	Crosswork Cloud の使用開始 9
第 4 章	ログイン 11 サポートされるブラウザ 11 ログイン 11 メイン ウィンドウ コントロール 12 ホームページの設定 14

第 5 章	セットアップツールの使用	15
	外部ルーティングの Express Setup の使用	15
	トラフィック分析のセットアップチェックリストの使用	16

第 6 章	Crosswork Data Gateway のインストール	17
	Crosswork Data Gateway のインストール	17
	Crosswork Data Gateway の情報の追加	17

第 III 部 :	ネットワークのモニタ	19
-----------	-------------------	-----------

第 7 章	モニタの概要	21
	モニタリングの概要	21

第 8 章	アラームのモニタ	23
	アラームの説明	23
	予期しないASプレフィックス (Unexpected AS Prefix)	23
	AS発信元違反 (AS Origin Violation)	24
	新しいASパスのエッジ (New AS Path Edge)	25
	ASパス長違反 (AS Path Length Violation)	26
	親集約の変更 (Parent Aggregate Change)	27
	プレフィックスアドバタイズメント (Prefix Advertisement)	28
	プレフィックスの取り消し (Prefix Withdrawal)	28
	ROAの有効期限 (ROA Expiry)	29
	ROA障害 (ROA Failure)	30
	ROAが見つからない (ROA Not Found)	30
	DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)	31
	サブプレフィックスアドバタイズメント (SubPrefix Advertisement)	32
	アップストリームASの変更 (Upstream AS Change)	33
	有効なASパス違反 (Valid AS Path Violation)	34
	ピアの停止 (Peer Down)	35

アドバタイズされたプレフィックスの数 (Advertised Prefix Count)	35
禁止されたIPプレフィックス (Prohibited IP Prefix)	36
ゲートウェイ接続	36
デバイスの接続性	37
インターフェイス TX の使用率	38
インターフェイス RX の使用率	39
プレフィックス使用率	39
すべてのアラームの表示	40
アラームの詳細の表示	41
アラームの概要の詳細	42
アラーム検索グラスの詳細	43
アラームプレフィックスの詳細	43
アラームに関連する BGP 更新の詳細	44
アラームサブプレフィックスの詳細	45
アラーム履歴の表示	45

 第 9 章

ASN のモニタ 47

すべての ASN の表示	47
ASN の詳細の表示	48
ASN の概要の詳細	48
ASN アラームの詳細	49
ASN BGP 更新の詳細	50
ASN 検索グラスの詳細	51
ASN ROA の詳細	51
ASN RPSL カバレッジ	52
ASN トラフィックの詳細の表示	54
日次 ASN 変更の表示 (ASN ルーティングレポート)	55
AS ピアレポート	56
IPv4 および IPv6 プレフィックスレポート	57

 第 10 章

プレフィックスのモニタ 59

プレフィックスの概要	59
プレフィックスの追加	59
すべてのプレフィックスの表示	60
プレフィックスの詳細の表示	61
プレフィックスの概要の詳細	61
プレフィックスアラームの詳細	62
プレフィックス BGP 更新の詳細	63
プレフィックス検索グラスの詳細	64
プレフィックス ROA の詳細	64
プレフィックス RPSL の詳細	65
プレフィックストラフィックの詳細の表示	67

第 11 章 **BGP 更新のモニタ** 69

BGP 更新の表示	69
-----------	----

第 12 章 **デバイスのモニタリング** 71

デバイス ステータスの表示	71
デバイス分析の詳細の表示	72
Trust Insights の詳細の表示	72
デバイス インベントリの表示	76
デバイスの変更の表示	76
デバイスソフトウェアの変更の表示	77
デバイスパッケージの一致しないファイルの表示	79
ファイル異常の表示	80
デバイスの機能の表示	80

第 13 章 **インターフェイスのモニタ** 83

インターフェイストラフィックの詳細の表示	83
----------------------	----

第 IV 部 : **Crosswork Cloud の設定** 85

第 14 章	プレフィックスの設定 87
	プレフィックスの追加 87
	プレフィックスの編集およびリンク解除 88
	プレフィックスの削除および登録解除 88
	プレフィックス通知の一時的な抑制 89

第 15 章	ASN の設定 91
	監視する ASN を追加する 91

第 16 章	ピアの設定 93
	ピアのインポート 93
	ピアの追加 94
	ピアの詳細の表示 94
	ピアデバイスの設定 97
	ピアの編集 98
	ピアの無効化 99
	ピアの削除 100

第 17 章	ポリシーの設定 101
	ポリシーの概要 101
	Crosswork Cloud Network Insights ポリシー 101
	Crosswork Cloud Network Insights ポリシーの追加 101
	Crosswork Cloud Network Insights ポリシーの管理 104
	Crosswork Cloud Traffic Analysis ポリシー 106
	Crosswork Cloud Traffic Analysis ポリシーの追加 106
	Crosswork Cloud Traffic Analysis ポリシーの管理 107

第 18 章	通知エンドポイントの設定 109
	通知エンドポイントについて 109
	通知エンドポイントの設定 110

Google ストレージエンドポイントの設定	111
Webex エンドポイントの設定	112
エンドポイントの確認コードの再送信	113
通知メッセージの例	113
電子メールのエンドポイント通知の例	114
スラックのエンドポイント通知の例	114
Microsoft Teams のエンドポイント通知の例	115
Cisco Webex のエンドポイント通知の例	115
アラームタイプ別 Amazon S3 と Google ストレージのエンドポイント通知の例	115
AS 発信元違反の例	115
AS パス長違反の例	118
DNS ルートサーバーの取り消しの例	123
新しい AS パスのエッジの例	124
親集約の変更例	139
ピアでアドバタイズされたプレフィックス数の例	143
ピアの停止の例	144
プレフィックス アドバタイズメントの例	144
プレフィックス取り消しの例	147
禁止された IP プレフィックスの例	149
ROA の有効期限の例	151
ROA が見つからない例	154
ROA 障害の例	157
サブプレフィックス アドバタイズメントの例	160
予期しない AS プレフィックスの例	162
アップストリーム AS の変更例	164
有効な AS パスの例	167

第 19 章

デバイスの設定 173

デバイスの追加	173
トラフィック分析用のデバイスを追加するための前提条件	176
SNMP の構成例	176

Cisco IOS デバイス用 BGP の構成例	177
Cisco IOS XR デバイス用 Netflow の構成例	179
Cisco IOS XR デバイス用 IPFIX の構成例	180
トラフィック分析で使用される SNMP の識別子	181
Crosswork Traffic Analysis 用の外部インターフェースの指定	182
Crosswork Trust Insights にデバイスを追加するための前提条件	182
Crosswork Trust Insights のルータ構成の確認	183
Crosswork Trust Insights の制限付き権限のユーザの設定	186
Trust Insights の信頼ドシエ情報	187
Trust Insights のデバイスドシエのデータ収集	188
デバイスドシエ収集頻度の変更	188
Trust Insights 用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング	189
デバイスの無効化	189
デバイスの削除	190
削除されたデバイスの復元	190

第 20 章

Crosswork Data Gateways の設定 193

Crosswork Data Gateway のインストール	193
Crosswork Data Gateway の情報の追加	194
Data Gateway の正常性の表示	195
トラフィックデバイスと Crosswork Data Gateway とのリンク	195
トラフィックデバイスと Crosswork Data Gateway とのリンクの削除	196
トラフィック分析用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング	196
Crosswork Data Gateway へのデバイスのリンク	198
Crosswork Data Gateway へのデバイスリンクの削除	198
Crosswork Data Gateways の非アクティブ化	199
Crosswork Data Gateways の削除	199

第 21 章

複数の宛先への NetFlow トラフィックの送信 201

複数の宛先への NetFlow トラフィックの送信 201

第 22 章

クレデンシャルの設定 203

クレデンシャルの作成 203

クレデンシャルの編集 203

デバイスとクレデンシャルとのリンク 204

第 23 章

デバイスグループの設定 205

デバイスグループの作成 205

第 24 章

既知の適正なファイルの設定 207

既知の適正なファイルについて 207

既知の適正なファイルの追加 207

既知の適正なファイルの無効化 208

既知の適正なファイルの削除 208

第 25 章

レポートの設定 211

ASN ルーティングレポートの設定 211

オンデマンドでのレポートの生成 213

第 V 部 :

Crosswork 外部分析ツールを使用する 215

第 26 章

プレフィックスパストポロジの表示 217

プレフィックスパストポロジの表示 217

パストポロジの変更を比較 220

第 VI 部 :

Crosswork トラフィック分析ツールを使用する 223

第 27 章

インターフェイス使用率の最適化 225

インターフェイス使用率の最適化 225

第 28 章	トラフィックのドリルダウン 227
	トラフィックのドリルダウン 227

第 29 章	ピア探査 229
	ピア探査の概要 229
	推奨されるピアの検索 229
	ピアの最適化 230
	推奨されるピアの無視 231

第 30 章	トラフィックの比較 233
	トラフィックの比較 233

第 VII 部 :	Crosswork Trust Insights ツールを使用する 235
-----------	---------------------------------------

第 31 章	デバイスの比較 237
	デバイスの比較について 237
	デバイスの比較 237

第 32 章	パッケージの検索 239
	パッケージの検索 239

第 33 章	ハードウェアの検索 241
	ハードウェアの検索 241
	ハードウェアの変更の表示 241
	ハードウェアインベントリの表示 242

第 VIII 部 :	管理タスク 243
------------	-----------

第 34 章	ユーザーの管理 245
	ユーザの追加 245

ユーザの役割	246
ユーザ権限の変更	246
ユーザプロフィールの表示	247

第 35 章	ライセンスの管理	249
	サブスクリプションまたはトライアルをアクティブ化する	249
	組織名の変更	250

第 36 章	構成ファイルのインポートとエクスポート	251
	構成ファイルのアップロード	251
	構成ファイルのダウンロード	252

第 37 章	実行されたアクションのリストの表示	253
	実行されたアクションのリストの表示	253

第 38 章	製品のヘルプとサポートの取得	255
	サポート ケースのオープン	255
	製品フィードバックの送信	255
	シスコ コミュニティ フォーラムへのアクセス	255

第 39 章	Crosswork Cloud API	257
	Crosswork Cloud API の概要	257
	API ヘルプおよびドキュメント	257
	API の使用開始	258
	API キーの定義	258
	Crosswork Cloud Network Insights クライアントスクリプト	259
	クライアントスクリプトのオプション	259
	Crosswork Cloud Network Insights クライアントスクリプト例	260
	クライアントスクリプトの使用方法	263
	Crosswork トラフィック分析クライアントスクリプトの例	266

第 IX 部 :	サブスクリプションの購入および管理 271
第 40 章	サブスクリプションプランのオプションの表示 273 サブスクリプションプランのオプションの表示 273 無料のサブスクリプションプランの要件 273
第 41 章	Crosswork Cloud を購入する 275 Amazon Web Services (AWS) マーケットプレイスでの購入 275 AWS Marketplace から直接購入 278 シスコパートナーまたはリセラーを通じた購入 281 購入に関する問題のトラブルシューティング 281
第 42 章	サブスクリプションまたはトライアルをアクティブ化する 283 サブスクリプションまたはトライアルをアクティブ化する 283
第 43 章	サブスクリプションとライセンスの表示 285 サブスクリプションとトライアルの詳細の表示 285
第 44 章	サブスクリプションの変更 287 サブスクリプションの更新 287
第 45 章	サブスクリプションを別の組織に転送 289 サブスクリプションを別の組織に転送 289
第 46 章	組織名の変更 291 組織名の変更 291
第 X 部 :	ユーザ設定の変更 293
第 47 章	ユーザ設定の変更 295

ユーザインターフェイスのテーマの変更 295

タイムゾーンの変更 295

第 XI 部 : **アラームの説明 297**

第 48 章 **アラームの説明 299**

アラームの説明 299

第 49 章 **予期しないASプレフィックス (Unexpected AS Prefix) 301**

予期しないASプレフィックス (Unexpected AS Prefix) 301

第 50 章 **AS発信元違反 (AS Origin Violation) 303**

AS発信元違反 (AS Origin Violation) 303

第 51 章 **新しいASパスのエッジ (New AS Path Edge) 305**

新しいASパスのエッジ (New AS Path Edge) 305

第 52 章 **ASパス長違反 (AS Path Length Violation) 307**

ASパス長違反 (AS Path Length Violation) 307

第 53 章 **親集約の変更 (Parent Aggregate Change) 309**

親集約の変更 (Parent Aggregate Change) 309

第 54 章 **プレフィックスアドバタイズメント (Prefix Advertisement) 311**

プレフィックスアドバタイズメント (Prefix Advertisement) 311

第 55 章 **プレフィックスの取り消し (Prefix Withdrawal) 313**

プレフィックスの取り消し (Prefix Withdrawal) 313

第 56 章 **ROAの有効期限 (ROA Expiry) 315**

ROAの有効期限 (ROA Expiry) 315

第 57 章	ROA障害 (ROA Failure)	317
	ROA障害 (ROA Failure)	317

第 58 章	ROAが見つからない (ROA Not Found)	319
	ROAが見つからない (ROA Not Found)	319

第 59 章	DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)	321
	DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)	321

第 60 章	サブプレフィックスアドバタイズメント (SubPrefix Advertisement)	323
	サブプレフィックスアドバタイズメント (SubPrefix Advertisement)	323

第 61 章	アップストリームASの変更 (Upstream AS Change)	325
	アップストリームASの変更 (Upstream AS Change)	325

第 62 章	有効なASパス違反 (Valid AS Path Violation)	327
	有効なASパス違反 (Valid AS Path Violation)	327

第 63 章	ピアの停止 (Peer Down)	329
	ピアの停止 (Peer Down)	329

第 64 章	禁止されたIPプレフィックス (Prohibited IP Prefix)	331
	禁止されたIPプレフィックス (Prohibited IP Prefix)	331

第 65 章	ゲートウェイ接続	333
	ゲートウェイ接続	333

第 66 章	デバイスの接続性	335
	デバイスの接続性	335

第 67 章	インターフェイス TX の使用率 337
	インターフェイス TX の使用率 337

第 68 章	インターフェイス RX の使用率 339
	インターフェイス RX の使用率 339

第 69 章	プレフィックス使用率 341
	プレフィックス使用率 341

付録 A :	アラームについて 343
	アラームライフサイクル 343
	アラームの状態 344
	アラーム通知 345
	アラームタイプ 346
	アラームのしきい値 347

?



第 1 部

Crosswork Cloud について

- [Crosswork Cloud 外部ルーティング分析について \(1 ページ\)](#)
- [Crosswork Cloud Traffic Analysis について \(3 ページ\)](#)
- [Crosswork Cloud Trust Insights について \(5 ページ\)](#)



第 1 章

Crosswork Cloud 外部ルーティング分析について

- [Crosswork Cloud Network Insights について \(1 ページ\)](#)

Crosswork Cloud Network Insights について

ネットワークは複雑になりがちで、予測不能な出来事も多く発生します。自動化されたシステム、悪意のある攻撃、または単純な運用エラーによって発生するルーティングイベントが、ネットワークサービスに対して予測不能な影響を及ぼす場合もあります。ルーティングプロトコルのイベント情報は、論理的に整理、分析、表示されない限り、把握するのが困難です。

Crosswork Cloud Network Insights は、実用的なネットワークイベントに関する豊富な分析、可視化、およびアラートを提供する SaaS アプリケーションです。Crosswork Cloud Network Insights はホステッドサービスとして動作し、ネットワークのルーティングの正常性を評価するのに役立ちます。Crosswork Cloud Network Insights は、ネットワークの安定性と IP ルーティング資産に対する潜在的なリスクを判断するために必要な情報を提供します。Crosswork Cloud Network Insights は、グローバルおよびローカルのルーティング情報を集約し、ルーティングデータベースのコンセンサスに基づいて異常の送信元を特定します。独自のグローバル BGP および IP 情報のライブおよび履歴アクティビティを追跡できます。また、プラットフォームによって提供される情報に基づいて、問題の原因である可能性がある他のエンティティを迅速かつ簡単に調査できます。

安全かつ低リスクな方法により、世界規模でルーティング情報を収集します。



第 2 章

Crosswork Cloud Traffic Analysis について

- [トラフィック分析について \(3 ページ\)](#)

トラフィック分析について

Crosswork Cloud Traffic Analysis は、トラフィックがネットワークにどのように影響しているかに関する有用な情報を提供します。Crosswork Cloud Traffic Analysis では、ネットワークの ASN、プレフィックス、およびインターフェイスのトラフィック統計情報を提供することにより、デバイスのパフォーマンスに関するリアルタイム情報を得ることができます。

Crosswork Cloud Traffic Analysis を使用すると、ネットワークエッジの輻輳の防止と対処に役立つだけでなく、次の質問に答えることができます。

- ネットワークエッジで輻輳を迅速に管理できますか。
- ネットワークエッジの輻輳をプロアクティブに特定できますか。ネットワークエッジの輻輳に役立つ小さな変更は何ですか。
- IP ルーティングテーブルは、輻輳したデバイスのトラフィックフローにどのように関連しますか。
- ピ어링トラフィックのロードバランスを実現するには、誰とピアリングし、どのような変更を行う必要がありますか。
- エッジデバイス間でトラフィックを移動すると、どのような影響がありますか。

Crosswork Cloud Traffic Analysis は、複数のデバイスのトラフィックフローデータを集約し、ネットワーク全体のトラフィックマトリックスのビューをオペレータに提供します。Crosswork Cloud Network Insights サービスからの外部ルーティングデータの既存の豊富なデータセットに基づいて、確認されたトラフィックフローに重要なコンテキストが追加されるため、オペレータは、ネットワーク上のトラフィックフローの発信元と、外部ルーティング状態とポリシーの変更による影響をより深く理解できます。オペレータは、大量のデータを効果的に抽出して管理することで、イベントの中断や差し迫ったセキュリティ脅威に迅速に対処し、プロアクティブに回避することもできます。

Cisco Crosswork Cloud Traffic Analysis は、輻輳したネットワークエッジでトラフィックを最適化するための実用的な推奨事項も提供します。今日の分散型ネットワークでは、ピアリングポイントの数が増えるにつれて、このエンドツーエンドのトラフィックの可視性を大規模に提供することが、効果的なネットワーク最適化の重要な要件になります。この可視性により、ネットワークオペレータは、定義されたポリシーに基づいて、ネットワーク全体で明確かつ簡単に実装できる手動または自動の変更を推進できます。



第 3 章

Crosswork Cloud Trust Insights について

- [Trust Insights について](#) (5 ページ)
- [Trust Insights で使用されるデータ](#) (6 ページ)
- [デバイスからの信頼情報の収集方法](#) (6 ページ)
- [Trust Insights による信頼性の測定方法](#) (6 ページ)
- [Trust Insights で確認できる内容](#) (7 ページ)

Trust Insights について

Crosswork Cloud Trust Insights は、ネットワーク上の Cisco IOS XR デバイスの完全性を保護およびテストする方法を提供します。Crosswork Cloud Trust Insights は、安全な測定値を収集し、データが特定の時間に収集されたことを証明します。これにより、ネットワークの完全性を測定、確認、および監査できます。Crosswork Cloud Trust Insights は、IOS XR ルータからの既知の適正な値 (KGV) の測定の完全性を自動的に解釈して確認します。これにより、環境内の実稼働ルータのハードウェアおよびソフトウェアの完全性と信頼できるステータスを独自に可視化できます。

Crosswork Cloud Trust Insights は、ネットワークの現在の状況と過去の状況を把握するのに役立ちます。また、次のことがわかります。

- 実行したいソフトウェアをルータが実行していることを確認するにはどうすればよいか。
- 変更されたハードウェアとソフトウェアを追跡するにはどうすればよいか。
- ネットワークで実行されているハードウェアまたはソフトウェアが変更されたかどうかを確認するにはどうすればよいか。
- 重要なセキュリティ更新が適用され、現在アクティブになっている場所とタイミングを証明するにはどうすればよいか。
- 実行中のソフトウェアがシスコによって作成されたことを確認するにはどうすればよいか。
- 過去の特定の日付に実行されていたハードウェアとソフトウェアを確認するにはどうすればよいか。

- 準拠したハードウェアとソフトウェアをシステムが実行していることを証明するにはどうすればよいか。

Trust Insights で使用されるデータ

Crosswork Cloud Trust Insights は、ネットワーク内のハードウェアとソフトウェアの完全性を確認および証明するために、次のデータを使用します。

- 既知の適正な値 (KGV) : シスコは、ハードウェア製品およびソフトウェア製品の KGV を製造および公開しています。KGV.json ファイルはシスコによって署名されており、ブート整合性の可視性、boot0 イメージの測定値、起動 OS イメージの測定値、実行イメージファイルの測定値などのさまざまなコンポーネントの測定値が含まれています。KGV は、有効性をテストする既知の適正な値の標準を提供します。
- IOS XR デバイスからの署名付き証拠ドシエ : IOS XR の新機能を使用すると、動作ステータス、発明者、ハードウェア、起動、ランタイムの完全性など、実行中のハードウェアおよびソフトウェアに関する信頼情報を含むドシエを生成できます。Crosswork Data Gateway はドシエを収集し、Trust Insights に転送します。

デバイスからの信頼情報の収集方法

次の手順では、Crosswork Cloud Trust Insights がデバイスから信頼ドシエを取得するプロセスについて説明します。

1. Crosswork Data Gateway は Crosswork Cloud (HTTPS) に接続します。
2. 管理者が Crosswork Data Gateway の情報とデバイスを Crosswork Cloud Trust Insights に追加します。
3. Trust Insights は、クエリするデバイスのリストを Crosswork Data Gateway に送信します。
4. Crosswork Data Gateway はデバイスにログインし、信頼ドシエを収集します。
5. Crosswork Data Gateway は、信頼ドシエを Crosswork Cloud Trust Insights に転送します。
6. Crosswork Cloud Trust Insights は、確認と分析を実行します。

Trust Insights による信頼性の測定方法

ネットワークデバイスの信頼性をテストおよび測定するために、Crosswork Trust Insights は次の手順を実行します。

- Trust Insights は、Cisco Crosswork データゲートウェイ (Cisco Crosswork Data Gateway) を使用して、IOS XR デバイスから署名付き証拠ドシエを安全に要求し、収集します。

- ドシエの証拠が確認され、実行中のハードウェアとソフトウェアのタイムラインに追加されます。
- Crosswork Trust Insights は、ハードウェアおよびソフトウェアについて、ドシエに含まれるデータをシスコの KGV と比較します。
- Crosswork Trust Insights は、デバイスの履歴と信頼の可視性を備えたアシュアランス インベントリ レポートを表示します。

Trust Insights で確認できる内容

Crosswork Cloud Trust Insights は、ソフトウェアおよびハードウェアの変更の証拠を収集し、レポートします。たとえば、デバイスのセキュリティの脆弱性に対処するために SMU を適用する必要がある場合、Trust Insights は適切な SMU を実行していることと、インストールしたコードによって脆弱性が修正されたことを示す証拠を提示できます。

Trust Insights は次のことを実行できません。

- ルータがアップ状態かダウン状態かを判別する。Trust Insights は運用ツールではありません。
- シスコが作成しなかったコードの完全性を確認する。オペレーティングシステムまたは SMU からのデータを認識した場合、デバイスが実行していると思われるソフトウェアを実行しているかどうかを確認できます。ただし、認識できないデータが見つかった場合、Trust Insights はその有効性または完全性を判断できません。



第 II 部

Crosswork Cloud の使用開始

- [ログイン \(11 ページ\)](#)
- [セットアップツールの使用 \(15 ページ\)](#)
- [Crosswork Data Gateway のインストール \(17 ページ\)](#)



第 4 章

ログイン

- サポートされるブラウザ (11 ページ)
- ログイン (11 ページ)
- メインウィンドウ コントロール (12 ページ)
- ホームページの設定 (14 ページ)

サポートされるブラウザ

Crosswork Cloud 製品は次のブラウザでサポートされています。

- Google Chrome 70 以降
- Mozilla Firefox 62 以降

ログイン



(注) 次のブラウザが Cisco Crosswork でサポートされています。

- Google Chrome 70 以降
 - Mozilla Firefox 62 以降
-

Cisco Crosswork Cloud にログインするには、次の手順を実行します。

ステップ 1 ブラウザで、<https://crosswork.cisco.com> に移動します。

ステップ 2 Crosswork Cloud ページから、[ログイン (Login)] をクリックします。

ステップ 3 Cisco.com アカウントの電子メールアドレス (Cisco.com のユーザー ID ではない) を入力し、[ログイン (Login)] をクリックします。

ステップ 4 ログアウトするには、右上隅にあるユーザのイニシャルをクリックしてから、[サインアウト (Sign Out)] をクリックします。

非アクティブな時間が長すぎると自動的にログアウトされ、再度ログインする必要があります。

メインウィンドウコントロール

Crosswork Cloud のウィンドウの主なナビゲーションコントロールについては、以下で説明します。

The screenshot shows the Crosswork Cloud main dashboard. The interface includes a left-hand navigation menu, a top header with user information, and a main content area with several sections:

- 1**: Monitor icon in the navigation menu.
- 2**: Overview icon in the navigation menu.
- 3**: Alarms icon in the navigation menu.
- 4**: Prefixes icon in the navigation menu.
- 5**: Policies icon in the navigation menu.
- 6**: Notification Endpoints icon in the navigation menu.
- 7**: A vertical bar in the navigation menu.
- 8**: User profile icon (Elizabeth Baker) in the top right corner.

The main content area displays:

- Active Alarms**: A table showing policy violations occurring now.
- Active Alarms By Rule**: A donut chart showing 3 AS Origin Violation and 3 SubPrefix Advertisement.
- Prefix Usage**: A donut chart showing 364 Available and 136 Used.
- Violation Peers**: A world map and a table showing peer counts by country.
- Quick Jump**: A search box for ASN, Prefix, or IP.
- Application Shortcuts**: Links to Configure Notification Endpoints, Express Setup, and Manage Users.

以下の表に、Crosswork Cloud のホームページで上図の引き出し線を説明します。



(注) 表示されるアイコンは、サブスクリプションの対象となる Crosswork Cloud 製品によって異なります。

表 1: Crosswork Cloud のホームページナビゲーションに関する説明

引き出し線番号	説明
1	Crosswork Cloud Network Insights の機能にアクセスするには、このアイコンをクリックします。
2	Crosswork Cloud Traffic Analysis の機能にアクセスするには、このアイコンをクリックします。詳細については、 トラフィック分析について (3 ページ) を参照してください。
3	Crosswork Cloud Trust Insights の機能にアクセスするには、このアイコンをクリックします。詳細については、 Trust Insights について (5 ページ) を参照してください。
4	アクティビティログ。詳細については、 実行されたアクションのリストの表示 (253 ページ) を参照してください。
5	ヘルプとサポート。詳細については、 製品のヘルプとサポートの取得 (255 ページ) を参照してください。
6	[設定 (Settings)] をクリックして、次のタスクを実行します。 <ul style="list-style-type: none"> • ユーザーの管理 (245 ページ) • 構成ファイルのインポートとエクスポート (251 ページ) • Crosswork Cloud を購入する • サブスクリプションとライセンスの表示
7	この列に表示されるメニュー項目は、選択した製品アイコンによって異なります。この列には通常、次のカテゴリで構成された機能が含まれています。 <ul style="list-style-type: none"> • モニタ (Monitor) • Tools • 設定 (Configure)

引き出し線番号	説明
8	<p>ユーザのイニシャルをクリックすると、次のオプションが表示されます。</p> <ul style="list-style-type: none"> • [全画面表示 (View in Fullscreen)] : Crosswork Cloud を全画面モードで展開できます。 • [設定 (My settings)] : ロールとプロバイダーを表示できます。タイムゾーンを変更したり、ユーザインターフェイスのテーマを変更したりすることもできます。詳細については、ユーザ設定の変更 (293 ページ) を参照してください。 • [APIキー (My API Keys)] : 新しい API キーを生成するか、既存の API キーを表示できます。詳細については、Crosswork Cloud API (257 ページ) を参照してください。 • ユーザ名が属する組織。複数の組織に属している場合は、切り替える組織の横にあるチェックボックスをオンにして、組織を切り替えることができます。 • [サインアウト (Sign Out)] : Crosswork Cloud からログアウトします。

ホームページの設定

特定の Cisco Crosswork Cloud のページをデフォルトのホームページに設定できます。ホームページを指定すると、Cisco Crosswork Cloud にログイン後にそのページが表示されます。

-
- ステップ 1** Cisco Crosswork Cloud にログインします。詳細については、[ログイン \(11 ページ\)](#) を参照してください。
- ステップ 2** Cisco Crosswork Cloud ウィンドウの左側のナビゲーションウィンドウで、ホームページを作成するメニュー項目の上にカーソルを合わせます。
- ステップ 3** 表示されるピンアイコンをクリックします。
- ログアウトしてから再度ログインすると、ピン留めしたページが表示されます。
-



第 5 章

セットアップツールの使用

- [外部ルーティングの Express Setup の使用 \(15 ページ\)](#)
- [トラフィック分析のセットアップチェックリストの使用 \(16 ページ\)](#)

外部ルーティングの Express Setup の使用



(注) この機能は、Crosswork Network Insights 専用です。

環境をセットアップして使用する準備を整えるために、Express Setup 機能を使用できます。
Express Setup を使用して、以前に追加した ASN を変更することはできません。

- ステップ 1** メインウィンドウで、ページの左下にある [Express Setup] をクリックします。[ヘルプとサポート (Help & Support)] をクリックしてから、[Express Setup] をクリックして、Express Setup ツールにアクセスすることもできます。
- ステップ 2** 次のプロンプトに従い、必要な情報を入力します。
- 以前に追加した ASN を入力すると、既存の関連付けられたプレフィックスまたはポリシーを示すエラーメッセージが表示されます。エラーメッセージで説明されているように、まず既存のポリシーを削除してリンクを解除する必要があります。
- ステップ 3** Express Setup が正常に終了すると、Crosswork Cloud Network Insights では入力した情報に基づいて変更が表示されます。
- 作成するポリシー。自動生成されたポリシー名、ポリシータイプ (ASN またはプレフィックス)、およびそのポリシーに含まれるルールを表示できます。
 - 登録する ASN (ASN ポリシーを指定した場合)。
 - 登録するプレフィックス (プレフィックスポリシーを指定した場合)。
 - リンクするエンドポイント (指定されている場合)。エンドポイントに関連付けられているエンドポイント名、タイプ、およびポリシーを表示できます。

ステップ4 変更内容を確認してから、[送信 (Submit)] をクリックして変更を保存します。

ポリシーに含まれるルールで指定されたしきい値を超えると、Crosswork Cloud Network Insights はアラームを生成し、ポリシーに関連付けられたエンドポイントにアラーム通知を送信します。

トラフィック分析のセットアップチェックリストの使用



(注) この機能は、Crosswork Traffic Analysis 専用です。

環境をセットアップして使用する準備を整えるために、Crosswork Cloud Traffic Analysis のセットアップチェックリスト機能を使用できます。

ステップ1 メインウィンドウで、ページの左下にある [セットアップチェックリスト (Setup Checklist)] をクリックします。[ヘルプとサポート (Help & Support)] をクリックしてから、[セットアップチェックリスト (Setup Checklist)] をクリックして、セットアップチェックリストツールにアクセスすることもできます。

ステップ2 チェックリストの各ステップに緑色のチェックマークが含まれていることを確認します。

ステップ3 緑色のチェックマークが付いていないステップの横にある青色の変更リンクをクリックします。これにより、対応するページが表示され、エラーを修正するための編集を行うことができます。



第 6 章

Crosswork Data Gateway のインストール

- [Crosswork Data Gateway のインストール](#) (17 ページ)
- [Crosswork Data Gateway の情報の追加](#) (17 ページ)

Crosswork Data Gateway のインストール



(注) Crosswork Data Gateway は Crosswork Cloud Traffic Analysis と Crosswork Cloud Trust Insights にも必要です。Crosswork Cloud Network Insights には必要ありません。

Crosswork Cloud はそのデータに依存しているため、最初に Crosswork Data Gateway をインストールする必要があります。Crosswork Cloud でサポートされている Crosswork Data Gateway のバージョンについては、[Cisco Crosswork Data Gateway Release Notes](#) を参照してください。

ステップ 1 [Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications](#) の説明に従って Crosswork Data Gateway をインストールします。

ステップ 2 [Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications](#) の説明に従って Crosswork Data Gateway から [登録パッケージの取得とエクスポート](#) します。



Crosswork Data Gateway の登録データを取得したら、Crosswork Cloud にログインできます。

Crosswork Data Gateway の情報の追加

クラウドデータゲートウェイの展開プロセスの一環として、新しい仮想マシンを展開した後に一意の登録ファイルが作成されます。json 登録ファイルには、Crosswork Data Gateway を Crosswork Cloud に登録する際に使用される一意のデジタル証明書が含まれています。Crosswork Data Gateway をインストールして登録データをダウンロードしたら、次に説明するようにその情報を追加する必要があります。



- (注) Crosswork Data Gateway の出力トラフィックでファイアウォールを使用する場合は、ファイアウォールの構成で `cdg.crosswork.cisco.com` および `crosswork.cisco.com` が許可されていることを確認します。

- ステップ 1** メインウィンドウから、次のいずれかを実行します。
- Crosswork Cloud Traffic Analysisについては、 > [設定 (Configure)] > [データゲートウェイ (Data Gateways)] の順に選択してから、[データゲートウェイの追加 (Add Data Gateway)] をクリックします。
 - Crosswork Cloud Trust Insightsについては、 > [設定 (Configure)] > [データゲートウェイ (Data Gateways)] の順に選択してから、[データゲートウェイの追加 (Add Data Gateway)] をクリックします。
- ステップ 2** [登録 (Registration File)] をクリックして、Crosswork Data Gateway からダウンロードした登録データファイルをアップロードし、.json ファイルの場所に移動してから、[次へ (Next)] をクリックします。
- ステップ 3** Crosswork Data Gateway の名前を入力します。
- ステップ 4** [アプリケーション (Application)] フィールドで、この Crosswork Data Gateway インスタンスを使用している該当 Crosswork Cloud アプリケーションが正しいものかどうか確認します。各 Crosswork Data Gateway は、1 つの Crosswork Cloud アプリケーションにのみ適用できます。
- ステップ 5** 残りの必須フィールドに入力してから、[次へ (Next)] をクリックします。
- ステップ 6** (オプション) タグ名を入力し、[新しい項目 (New Item)] をクリックします (または既存のタグ名から選択します)。これにより、同じタグを持つ Crosswork Data Gateway をグループ化できます。その後、[次へ (Next)] をクリックします。
- ステップ 7** 複数の NIC があり、そのうちの 1 つをサウスバウンドトラフィックと通信するようにする場合は、このウィンドウで設定します。
- ステップ 8** 入力した Crosswork Data Gateway の情報を確認してから、[次へ (Next)] をクリックします。
- ステップ 9** [承認 (Accept)] をクリックして、セキュリティ証明書を受け入れます。
- Crosswork Data Gateway の追加に成功したことを示すメッセージが表示されます。
- ステップ 10** 数分後、Crosswork Data Gateway が正常に接続されていることを確認します。[データゲートウェイ (Data Gateways)] をクリックし、続けて Crosswork Data Gateway の名前をクリックして、追加した Crosswork Data Gateway について次の値を確認します。
- [接続 (Connectivity)] : [セッションアップ (Session Up)]
 - 管理状態 : 有効
 - コンテナイメージ : 一致
- 変更を表示するには、更新が必要な場合があります。



第 III 部

ネットワークのモニタ

- [モニタの概要 \(21 ページ\)](#)
- [アラームのモニタ \(23 ページ\)](#)
- [ASN のモニタ \(47 ページ\)](#)
- [プレフィックスのモニタ \(59 ページ\)](#)
- [BGP 更新のモニタ \(69 ページ\)](#)
- [デバイスのモニタリング \(71 ページ\)](#)
- [インターフェイスのモニタ \(83 ページ\)](#)



第 7 章

モニタの概要

- [モニタリングの概要 \(21 ページ\)](#)

モニタリングの概要

[モニタ (Monitor)]>[概要 (Overview)]を選択したときに表示される情報は Crosswork Cloud 製品ごとに異なりますが、すべての概要のモニタリングでは、システムの正常性を全体的に確認できます。

[時間範囲 (Time Range)] ドロップダウンリストから、特定の期間中の概要情報を表示する値を選択します。



第 8 章

アラームのモニタ

問題を迅速に解決するために、[アラーム (Alarms)] ページ ([外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)]) でポリシー違反を簡単に表示できます。[アラーム (Alarms)] ページでは、アクティブなアラーム、確認済みアラーム、またはアラーム履歴を表示できます。アラームの詳細については、次を参照してください。

- [アラームの説明 \(23 ページ\)](#)
- [すべてのアラームの表示 \(40 ページ\)](#)
- [アラームの詳細の表示 \(41 ページ\)](#)
- [アラーム履歴の表示 \(45 ページ\)](#)

アラームの説明

このセクションには、アラームと説明のリストが含まれています。アラームは、ポリシー内で構成されたときにトリガーされます。ポリシーの設定方法の詳細については、次のいずれかのトピックを参照してください。

- [Crosswork Cloud Network Insightsポリシーの追加 \(101 ページ\)](#)
- [Crosswork Cloud Traffic Analysisポリシーの追加 \(106 ページ\)](#)

予期しないASプレフィックス (Unexpected AS Prefix)

このアラームは、新しいプレフィックスが以前になかった AS の予期しない変更を検出します。モニタ対象の BGP AS から発信されるプレフィックスは、ピアしきい値の対象となる組織によって登録されていない場合、違反プレフィックスです。

考えられる検出される問題

このアラームは、新しいプレフィックスが以前に観察されなかった AS の予期しない変更またはルートリークのシナリオを特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールを ASN 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)] > [ASNポリシー (ASN Policy)] > [ルールの追加 (Add Rule)] > [予期しないASプレフィックス (Unexpected AS Prefix)])。

- [アラームのしきい値](#) (アドバタイズされたプレフィックスごと)
- [プレフィックスの設定](#)

例

[予期しないASプレフィックス (Unexpected AS Prefix)] アラームルールを使用して ASN ポリシーを作成し、モニタ対象の AS 15169 にリンクします。また、AS 15169 から発信されると予想されるすべてのプレフィックスにも登録されます。設定不備により、プレフィックス 8.8.0.0/24 が AS からリークされます。同時に、プレフィックス 9.9.0.0/24 は正しくアドバタイズされませんが、登録されません。ピアのしきい値に応じて、これらのイベントは両方ともアラームをトリガーします。その後、プレフィックス 8.8.0.0/24 を取り消すように設定を修正し、アラームをクリアするプレフィックス 9.9.0.0/24 に登録できます。

AS発信元違反 (AS Origin Violation)

このアラームは、発信元 AS を持つモニタ対象プレフィックスのアドバタイズメントが [AS発信元リスト (AS Origin List)] にない場合に検出します。これは違反アドバタイズメントであり、特にアドバタイズメントの AS パス長が正規のアドバタイズメントよりも短い場合に、プレフィックスハイジャックの試みを表す可能性があります。



- (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 \(94 ページ\)](#) 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 \(101 ページ\)](#) 、

考えられる検出される問題

このアラームは、ルートリークまたはプレフィックスハイジャックの特定に役立ちます。

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 of 追加 (Add Rule)] > [AS発信元違反 (AS Origin Violation)]。

- アラームのしきい値
- 許可された発信元 ASN

例

プレフィックス 8.8.8.0/24 の [AS発信元違反 (AS Origin Violation)] アラームルールでプレフィックスポリシーを作成し、[AS発信元リスト (AS Origin List)] フィールド値が 15169 で設定されています。しかし、確認された BGP 更新が 8.8.8.0/24 および 109 の発信元 AS で受信されます。AS 109 が [AS発信元リスト (AS Origin List)] に含まれていないために、このアラームがトリガーされます。

新しいASパスのエッジ (New AS Path Edge)

このアラームは、以前に確認されていない新しい AS ピアリングを検出します。

中間者 (MITM) 攻撃では、攻撃者が自身の AS をプレフィックスの AS パスに挿入し、AS を介してプレフィックスのトラフィックを誘導します。攻撃の検出を回避するために、MITM 攻撃は通常短命で、少数のプレフィックスをターゲットとします。

一時的な AS ピアリングの別の原因として、すぐに修正されるオペレータエラーが考えられます。



- (注) AS ピアリング関係は、多くのピアによってアドバタイズされた多数のプレフィックスの AS パスに存在するか、または長期間存続しますが、正当なネットワーク設定の変更である可能性が高く、Crosswork Cloud Network Insights ではこれらのアラートは表示されません。

考えられる検出される問題

このアラームは、潜在的な MITM 攻撃またはオペレータエラーの特定に役立ちます。

例

[新しいASパスのエッジ (New AS Path Edge)] 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 にリンクします。アラームは、Crosswork Cloud Network Insights が、疑わしい AS ピアリング (すべてのプレフィックスのすべてのパスで以前に確認されていないピアリング、または新しいピアリング) を含む AS パスでプレフィックス 8.8.0.0/24 がアドバタイズされたことを検出したときにトリガーされます。一定の時間が経過すると、Crosswork Cloud Network Insights は、これらの AS ピアリング関係が長期間存続していると判断します。ピアリング関係が長期間存続していると判断されると、アラームはクリアされます。

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 \(94 ページ\)](#) 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 \(101 ページ\)](#) 、

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)])。

- [アラームのしきい値](#)
- [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。

親集約の変更 (Parent Aggregate Change)

このアラームは、予期しないスーパーネットまたはしきい値違反を検出します。

ネットワークオペレータは通常、アドバタイズされたプレフィックスの直接のスーパーネットプレフィックス (集約またはサマリー)、およびその他の集約された上位スーパーネット、およびそれらの発信元 AS を認識しています。ユーザは、Classless inter-domain routing (CIDR) プレフィックス長を指定して、予想される IPv4 および IPv4 スーパーネットのセットを少なくとも 1 つ設定する必要があります。ユーザは、許可された送信元 AS のリストから、観測された集約が発信されるように強制することもできます。



- (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 \(94 ページ\)](#) 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 \(101 ページ\)](#)、

考えられる検出される問題

このアラームは、サマリープレフィックスの誤った取り消しやルートリークを特定するのに役立ちます。

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)] > [親集約の変更 (Parent Aggregate Change)])。

- **アラームのしきい値** (アドバタイズされた集約ごと)
- [許可された発信元 ASN (Allowed Origin ASNs)] (オプション)
- [許可される IPv4/IPv6 スーパーネット (Allowed IPv4/IPv6 supernets)]

例

[親集約の変更 (Parent Aggregate Change)] 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 にリンクします。ポリシーは、許可された IPv4 集約プレフィックス長 [22, 9] および許可された発信元 AS 3356 で設定されます。次のイベントがアラームをトリガーします。

- 予想されるスーパーネット 8.8.0.0/22 がハイジャックされます (プレフィックスは予期しない発信元 AS から発信されます)。
- 集約、プレフィックス 8.8.0.0/20 がアドバタイズされ、潜在的なリークとして識別されず。

リークまたはハイジャックが解決されるか、ユーザがアラーム設定を変更して、これらの集約アドバタイズメントが正当であることを示すと、アラームはクリアされます。

プレフィックスアドバタイズメント (Prefix Advertisement)

このアラームは、モニタ対象プレフィックスの優先 BGP パスでの予期しない変更を検出します。したがって、プレフィックスのアドバタイズされたパスの BGP 属性に対する予期しない変更をモニタし、潜在的なルートリークの広がりを確認できます。



- (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 \(94 ページ\)](#) 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 \(101 ページ\)](#)、

考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスの優先 BGP パスの変更を特定するのに役立ちます。

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)] > [プレフィックスアドバタイズメント (Prefix Advertisement)])。

- [アラームのしきい値](#)

プレフィックスの取り消し (Prefix Withdrawal)

このアラームは、ピアがプレフィックスを取り消した場合に検出します。

少数の BGP ピアからのプレフィックスの取り消しは、プレフィックスに到達する複数のパスがあるため、必ずしもプレフィックスが到達不能であることを意味しません。ただし、多数のピアが地理的エリアのプレフィックスを取り消すと、プレフィックスの到達可能性が低下する

可能性があります。ルータのフラップによるノイズを抑制するために、このアラームのしきい値を他のアラームよりも高く設定することをお勧めします。



- (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 \(94 ページ\)](#) 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 \(101 ページ\)](#)、

考えられる検出される問題

このアラームは、プレフィックスの取り消しにつながる設定不備を特定するのに役立ちます。

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)] > [プレフィックスの取り消し (Prefix Withdrawal)])。

- [アラームのしきい値](#)

ROAの有効期限 (ROA Expiry)

このアラームは、Route Origin Authorization (ROA) レコードの有効期限が切れる前に警告します。ROA レコードは、リソース (アドバタイズされたプレフィックス) の所有権を主張するオペレータによって作成され、地域インターネットレジストリ (RIR) またはルーティング資産データベース (RADB) などの他のサービスによって暗号化されて配布されます。詳細については、[ripe.net](#) を参照してください。

ROA レコードの有効期限切れの何日前にアラートを送信するかを指定できます。これは、情報提供を目的とするアラームです。新しいレコードを作成するアクションを実行して、ルータによるプレフィックスの考えられるフィルタリングを回避できます。このアラームは、プレフィックスが ROA レコードでカバーされていて、現在と設定したトリガー間隔の間 (現在 + [有効期限が切れる前にトリガーする日数 (Days to Trigger Before Expiration)]) のどの時点でも、プレフィックスに有効な ROA レコードがない場合にアクティブになります。特に、期限切れのレコードと期限が切れていないレコードが混在している場合、設定された間隔内のいずれかの時点で期限が切れていないカバーしているレコードが存在する限り、アラームはアクティブになりません。

考えられる検出される問題

このアラームは、保留中の ROA カバレッジの欠如を検出します。

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)] > [ROAの有効期限 (ROA Expiry)])。

- ROA レコードの期限が切れる前にトリガーする日数。

例

[ROAの有効期限 (ROA Expiry)] 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、[有効期限が切れる前にトリガーする日数 (Days to Trigger Before Expiration)] に 30 を指定して、プレフィックス 8.8.0.0/24 にリンクします。このアラームは、プレフィックス 8.8.0.0/24 が複数の ROA レコードでカバーされている場合にトリガーされ、Crosswork Cloud Network Insights はこれらすべてのレコードがすでに期限切れになっているか、または 30 日未満で期限切れになることを検出します。アラームをクリアするには、トリガー時間間隔をカバーする 8.8.0.0/24 に対して少なくとも 1 つの ROA レコードを作成する必要があります。

ROA障害 (ROA Failure)

このアラームは、モニタ対象プレフィックスの **ROA 有効性状態** が無効かどうかを示します。発信元 AS がプレフィックスをカバーする ROA レコードにない、モニタ対象プレフィックスのアドバタイズメントは、違反アドバタイズメントです。アラームは、プレフィックスの観測されたすべての送信元 ASN を含む ROA レコードの追加、またはすべてのレコードの期限切れのいずれかによりクリアされます。具体的には、このアラームは、ROA レコードがない (存在しない、またはすべてが期限切れになっている) 場合はアクティブになりません。

ROA の詳細については、ripe.net を参照してください。

考えられる検出される問題

このアラームは、プレフィックスハイジャックの試行を特定するのに役立ちます。

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)] > [ROA障害 (ROA Failure)])。

- [アラームのしきい値](#)

ROAが見つからない (ROA Not Found)

プレフィックスは、それをカバーする複数の ROA レコードを持つことができます。このアラームは、モニタ対象のプレフィックスに ROA レコードがない (存在しない、または期限切れに

なっている) 場合にトリガーされます。これにより、RTR プロトコルを実装するルータによってプレフィックスがドロップされることを回避できます。

ROA の詳細については、ripe.net を参照してください。

考えられる検出される問題

これは、モニタ対象のプレフィックスに ROA レコードがないことをユーザに警告する情報アラームです。

DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)

IANA によって割り当てられ、OpenDNS と Google によって提供されるサーバーを含むパブリック DNS ルートサーバーは、通常のルータ操作がパブリック インターネットルーティングに参加するために必要です。このアラームは、DNS サーバアドレスが属する一連のプレフィックス (ネットブロック) をモニタします。セット内のいずれかのプレフィックスが取り消されると、ユーザに警告します。



- (注) このアラームは [プレフィックスの取り消し (Prefix Withdrawal)] アラームとは異なります。これらのプレフィックスは、ユーザがサブスクリプションで消費するプレフィックスの合計量に追加されず、アラームルールにリンクされたピアからの取り消しだからです。

考えられる検出される問題

このアラームは、既知のルート DNS サーバプレフィックスがモニタ対象ピアのルーティングテーブルから削除されたかどうかを検出します。このアラームは、DNS ルートサーバーの撤回につながるインターネットルータの不良構成を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールをピア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)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)])。

- 監視対象の DNS ルートサーバー

例

[DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)] アラームルールを使用してピアポリシーを作成し、ピア RTR1 にリンクします。プレフィックス 198.41.0.0/24 (A ルートサーバ) および 2001:7fd::/48 (K ルートサーバ) に対するアラートを受け取ることを選択します。アラームは、これらのプレフィックスのいずれかが RTR1 によって取り消されるとアクティブになり、両方がアドバタイズされるとクリアされます。

サブプレフィックスアドバタイズメント (SubPrefix Advertisement)

ハイジャッカーは、ルータが新しいサブプレフィックスをインストールすることで、モニタ対象プレフィックスによってカバーされる IP スペースの一部のトラフィックをリダイレクトできます。これは、ルータが具体的ではないルートよりも具体的なルートを優先するためです。ハイジャッカーは、既存のサブプレフィックスの新しいルートをインストールすることもできます。これらのハイジャックの試行を検出するために、サブプレフィックスの許可された発信元 ASN のリストを設定できます。このアラームの場合、違反アドバタイズメントは、アドバタイズされたサブプレフィックスとそのピアのしきい値のいずれかが違反している場合です。

考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスのサブプレフィックスのハイジャックを特定するのに役立ちます。

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)] > [サブプレフィックスアドバタイズメント (SubPrefix Advertisement)])。

- [プレフィックスの設定](#)
- アドバタイズされたサブプレフィックスごとのしきい値 (Peers to Resolve および Peers to Trigger) [アラームのしきい値 \(347 ページ\)](#)
- 許可された発信元 ASN



(注) 発信元 ASN リストを無視するには、[発信元ASNリストを使用 (Use Origin ASNs)] オプションを [いいえ (No)] に切り替えます。発信元 ASN リストが無視されると、すべての ASN に対してアラームがトリガーされます。

- IPv4/IPv6 の最大長：設定された IPv4/IPv6 の最大長よりも長いサブプレフィックスマスクを無視するオプションを使用できます。IPv4 の最大長は 8 より大きく、IPv6 の最大長は 16 より大きい必要があります。

例

[サブプレフィックスアドバタイズメント (Subprefix Advertisement)] 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 にリンクします。次のサブプレフィックスアドバタイズメントが発生し、アラームがトリガーされます。

- 予期しないサブプレフィックス 8.8.0.5/30 がアドバタイズされます。この場合、このプレフィックスは新しい管理組織に割り当てられ、新しい発信元 AS から初めてアドバタイズされます。このアラームをクリアするには、サブプレフィックス 8.8.0.5/30 を登録するように Crosswork Cloud Network Insights を設定するか、または新しい発信元 AS を許可された発信元 ASN のリストに追加します。
- 予期しないサブプレフィックス 8.8.0.4/30 がアドバタイズされます。これは、ルートリークまたはハイジャックのいずれかを示している可能性があります。このアラームをクリアするには、8.8.0.4/30 を取り消す必要があります。

アップストリームASの変更 (Upstream AS Change)

BGP オペレータは、アウトバウンドポリシー（たとえば、どのアップストリーム AS がプレフィックスを伝播できるか）によってピアリング関係を制御できます。このアラームは、プレフィックスを伝播しない既存のピアへのルートリークを検出します。ユーザは、許可されたアップストリーム ASN のリストを設定する必要があります。リストにないアップストリーム AS パスに 1 ホップが残っている ASN を持つモニタ対象プレフィックスのアドバタイズメントは、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 \(94 ページ\)](#) 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 (101 ページ) 、

考えられる検出される問題

このアラームは、モニタ対象プレフィックスのルートリークを特定するのに役立ちます。

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)] > [アップストリームASの変更 (Upstream AS Change)])。

- [アラームのしきい値](#)
- [許可されるアップストリームASN (Allowed upstream ASNs)]

例

[アップストリームASの変更 (Upstream AS Change)] アラームルールで許可されたアップストリームASN [293,1221] 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 にリンクします。プレフィックス 8.8.0.0/24 は、AS パス [2711, 1299, 3356] を持つピアによってアドバタイズされます。AS1299は許可されたアップストリームASNではないため、しきい値が適用されて、アラームがトリガーされます。違反しているASパスを持つルートが取り消されるか、許可されたアップストリームASNのリストにAS1229が追加されると、アラームはクリアされます。

有効なASパス違反 (Valid AS Path Violation)

このアラームは、プレフィックスアドバタイズメントASパスが指定されたASNパターンと一致しない場合に検出します。

Crosswork Network Insights は、設定された**有効なASパスパターン**を、アドバタイズされたプレフィックスのASパスと比較します。ASNパターンは、スペースで区切ったAS番号を順に並べた予測されるシーケンスであり、107 3462 109のように発信元ASで終わります。演算子を使用して複雑なパターンを表現できます。パターンが一致しない場合は、Crosswork Network Insights はアラームをトリガーしてアクティブにします。



- (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 \(94 ページ\)](#) 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 (101 ページ) 、

パターンの例 : [0-]* 806 * 200

- 有効な AS パス : 1900 1731 806 100 200
- 違反 AS パス : 1900 1731 807 100 200
- 違反 AS パス : 1900 1731 806 150 100 200

考えられる検出される問題

このアラームは、潜在的なMITM攻撃または遅延の低下を示す予期しないBGP ASパスの変更を検出します。

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)] > [有効なASパス違反 (Valid AS Path Violation)])。

- [アラームのしきい値](#)

ピアの停止 (Peer Down)

このアラームは、Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションの状態をモニタします。Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションが、予測されていた確立状態でない場合に、問題が発生する可能性があります。ピアリングセッションが確立状態になると、アラームはクリアされます。

考えられる検出される問題

このアラームは、モニタ対象ピアでの BGP プロセスの問題、またはピアリングに影響を与えるハードウェアやソフトウェアの問題を特定するのに役立ちます。

アドバタイズされたプレフィックスの数 (Advertised Prefix Count)

このアラームは、モニタ対象ピアの RIB のサイズをモニタします。Crosswork Cloud Network Insights は、すべてのモニタ対象ピアに関連する統計情報 (各ピアが Crosswork Cloud Network Insights にアドバタイズするプレフィックスの数を含む) を定期的に収集します。モニタ対象ピアから Crosswork Cloud Network Insights にアドバタイズされると予想されるプレフィックスの数に対して、少なくとも1つのIPv4/IPv6アドレスファミリー範囲を設定する必要があります。アドバタイズされたプレフィックスの数が予想される最小数を下回った場合は、モニタ対象ピアと Crosswork Cloud Network Insights またはその他のピアとの間のピアリングセッションに問題があることを示しています。また、ピアに適用されている、モニタ対象ピアに設定されたインバウンドポリシーの制限が Crosswork Cloud Network Insights よりも厳しい場合や、Crosswork Cloud Network Insights ピアに適用されているアウトバウンドポリシーの制限が厳しい場合にも発生します。逆に、アドバタイズされたプレフィックスの数が予想される最大数を超過している場合は、制限の緩いポリシーが設定されているか、またはプレフィックスアドバタイズメントでピアに大きな負担をかける悪意のある試みを示している可能性があります。

考えられる検出される問題

このアラームは、ピアリングの問題 (ソフトウェア、ハードウェア、または設定不備の問題による) またはピアでの DoS 攻撃を特定するのに役立ちます。

関連するアラームルールの設定

このアラームルールを ASN 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)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [アドバタイズされたプレフィックスの数 (Advertised Prefix Count)])。

- 予期されるプレフィックスの数の範囲 (IPv4/IPv6 アドレスファミリーごと)

例

ピア RTR1 にリンクされている、[アドバタイズされたプレフィックスの数 (Advertised Prefix Count)] アラームルールで、予期される IPv4 プレフィックス範囲 [1000, 800000] を使用して、ピアポリシーを作成します。RTR1 から Crosswork Cloud Network Insights にアドバタイズされた IPv4 プレフィックスの数がこの範囲外で、以前に記録されたものと異なる場合、アラームはデータ収集イベントごとにアクティブになります。

禁止されたIPプレフィックス (Prohibited IP Prefix)

このアラームは、監視対象ピアの Routing Information Base (RIB) にインストールされているパブリック IP ルーティングスペースに禁止されたプレフィックスがあるか、または監視対象ピアがそれを転送している場合に検出します。

Bogon は、予約されているか、地域インターネットレジストリ (RIR) に割り当てられていないため、パブリックではない IP アドレスブロックです。[フルBogon (Full bogons)] には、RIR に割り当てられているが、RIR によって特定のネットワークに割り当てられていないアドレスブロックも含まれます。禁止されたプレフィックスのアドバタイズメントをルータでフィルタリングすることをお勧めします。ユーザーは、このアラームを使用して、Bogon アドバタイズメントについてのみアラートを受け取るように選択できます。

考えられる検出される問題

このアラームは、ルータに対する DoS 攻撃の特定に役立ちます。

関連するアラームルールの設定

このアラームルールをピアポリシー設定に追加する場合は、[Bogon (Bogons)] または [フル Bogon (Full bogons)] を選択します ([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)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [禁止されたIPプレフィックス (Prohibited IP Prefix)])。

例

[禁止されたIPプレフィックス (Prohibited IP Prefix)] アラームルールでオプション [Bogons] を使用してピアポリシーを作成し、ピア RTR1 にリンクします。RTR1 が 10.0.0.0/24 (RFC1918 による BOGON) を Crosswork Cloud Network Insights にアドバタイズすると、アラームはアクティブになりますが、2001:221::/32 (フル Bogons) がアドバタイズされるとアクティブになりません。

ゲートウェイ接続

Crosswork Data Gateway が Crosswork Cloud Traffic Analysis 用にインストールされると、Crosswork Data Gateway と Crosswork Cloud の間の接続をモニターするポリシーが自動的に作成されます。Crosswork Data Gateway が Crosswork Cloud への接続を失った場合 (レポート間隔内で Crosswork

Cloudとの通信に失敗した場合)、アラームが生成され、Crosswork Cloud Traffic Analysis[アラーム (Alarms)]ページに表示されます (🔍)>[モニター (Monitor)]>[アラーム (Alarms)]。ゲートウェイ接続の詳細を表示したり、アラーム重大度レベル、モニター対象ゲートウェイのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。

ステップ 1 🔍 > [構成 (Configure)] > [ポリシー (Policies)] の順に選択します。

[ゲートウェイ接続 (Gateway Connectivity)] で、アクティブなアラームの数、モニター対象のゲートウェイの数、および最新のアクティブなアラームを持つゲートウェイを表示できます。

ステップ 2 [ゲートウェイ接続 (Gateway Connectivity)] で、[詳細 (Details)] をクリックします。

ステップ 3 デフォルトでは、[概要 (Overview)] タブに現在のゲートウェイ接続ポリシーの設定が表示されます。

ステップ 4 アラームの詳細を表示するには、[アラーム (Alarms)] タブをクリックします。このページから、[ゲートウェイ接続の喪失 (Lost Gateway Connection)] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active)]、[確認 (Acknowledge)]、または [履歴 (History)] のタブ間を移動したりできます。

ステップ 5 アラームの重大度やモニター対象ゲートウェイのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit)] をクリックします。

- [トリガー (Triggers)] > [ゲートウェイルール (Gateway Rules)] > [重大度 (Severity)] ドロップダウンメニューで、重大度を選択します。
- [データ (Data)] で、[変更 (Modify)] をクリックして、モニターまたは無視するゲートウェイを更新します。
- [アクション (Actions)] で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて \(109 ページ\)](#) を参照してください。
- [保存 (Save)] をクリックします。

デバイスの接続性

デバイスが Crosswork Data Gateway にリンクされて Crosswork Cloud Traffic Analysis に追加されると、Crosswork Data Gateway とそのデバイス間の接続をモニターするためのポリシーが自動的に作成されます。Crosswork Data Gateway がデバイスとの接続を失うと、アラームが生成され、Crosswork Cloud Traffic Analysis [アラーム (Alarms)] ページに表示されます (🔍)>[モニター (Monitor)]>[アラーム (Alarms)]。

デバイス接続の詳細を表示したり、重大度レベル、モニター対象デバイスのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。


ステップ 1 🔍 > [構成 (Configure)] > [ポリシー (Policies)] の順に選択します。

[デバイス接続 (Device Connectivity)] で、アクティブなアラームの数、モニタ対象のデバイスの数、および最新のアクティブなアラームを持つデバイスを表示できます。

- ステップ 2** [デバイス接続 (Device Connectivity)] で、[詳細 (Details)] をクリックします。
- ステップ 3** デフォルトでは、[概要 (Overview)] タブに現在のデバイス接続のポリシー設定が表示されます。
- ステップ 4** アラームの詳細を表示するには、[アラーム (Alarms)] タブをクリックします。このページから、[デバイス接続の喪失 (Lost Device Connection)] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active)]、[確認 (Acknowledge)]、または[履歴 (History)] のタブ間を移動したりできます。
- ステップ 5** アラームの重大度やモニター対象デバイスのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit)] をクリックします。
- [トリガー (Triggers)] > [デバイスルール (Device Rules)] > [重大度 (Severity)] ドロップダウンメニューで、重大度を選択します。
 - [データ (Data)] で、[変更 (Modify)] をクリックして、モニターまたは無視するデバイスを更新します。
 - [アクション (Actions)] で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて \(109 ページ\)](#) を参照してください。
 - [保存 (Save)] をクリックします。


インターフェイス TX の使用率

このアラームは、送信トラフィック情報をモニターし、インターフェイスの TX 使用率が指定した範囲外の場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1** メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4** [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5** [インターフェイス TX の使用率 (Interface TX Utilization)] をクリックします。
- ステップ 6** [Next] をクリックします。
- ステップ 7** デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8** このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9** [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10** その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。


インターフェイス RX の使用率

このアラームは、受信トラフィック情報をモニターし、インターフェイスの RX 使用率が指定した範囲外になった場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5 [インターフェイス RX の使用率 (Interface RX Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。

プレフィックス使用率

このアラームは、プレフィックスのキャパシティをモニターするもので、モニター対象インターフェイスのプレフィックスの1つが合計キャパシティのうち最大となるパーセンテージを超えた場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5 [プレフィックス使用率 (Prefix Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。

ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。

すべてのアラームの表示

アクティブなアラームは、ポリシーのいずれかの条件が満たされると生成されます。[アラーム (Alarms)] ページで発生する可能性のあるアラームの説明を表示するには、[アラームの説明 \(23 ページ\)](#) を参照してください。アラームの詳細を表示するには、[アラームの詳細の表示 \(41 ページ\)](#) を参照してください。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックします。

ステップ 2 [アラーム (Alarms)] ページの上部にある次のいずれかのタブをクリックします。

- [アクティブ (Active)] : すべてのアクティブなアラームのリストが表示され、優先順位でソートされます。
- [確認済み (Acknowledged)] : 優先順位でソートされたすべての確認済みアラームのリストが表示されます。
- [履歴 (History)] : [タイムフレーム (Timeframe)] ドロップダウンリストから時間範囲を指定できる履歴アラームが表示されます。詳細については、[アラーム履歴の表示 \(45 ページ\)](#) を参照してください。

次の表で、アラームフィールドについて説明します。

表 2: アラームのフィールドに関する説明

カラム	説明
アラームの詳細 (Alarm Details)	違反してアラームをトリガーしたルール。詳細については、 アラームの詳細の表示 (41 ページ) を参照してください。
トリガー (Trigger)	アラームが発生したプレフィックスまたは ASN。プレフィックスまたは ASN の詳細については、このリンクをクリックしてください。
ポリシー (Policy)	アラームをトリガーしたポリシーの名前。このリンクをクリックすると、ポリシーに関する詳細が表示されます。
# ピア (# Peers)	アラームをレポートしたピアの数。
シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。

カラム	説明
注記 (Notes)	ユーザが入力したアラームに関するメモ。アイコンをクリックしてメモを表示します。

- ステップ 3** 昇順または降順で列をソートできます。いずれかの列の見出しにカーソルを合わせ、表示される下矢印をクリックして、ソート順を変更するか、フィルタリングするテキストを入力します。
- ステップ 4** 一時的にアラームのアラートを停止するには、アラームの横にあるボックスをクリックしてから、[スヌーズ (Snooze)] をクリックします。
- ステップ 5** アラームをスヌーズする時間範囲を選択し、[スヌーズ (Snooze)] をクリックします。Crosswork Cloud Network Insights では、選択した期間、このアラームの通知は送信されません。
- ステップ 6** アラームを確認済みの状態にするには、アラームの横にあるボックスをクリックしてから、[確認 (Acknowledge)] をクリックします。

アラームの詳細の表示

特定のアラームに関する詳細情報を表示できます。

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックします。
- ステップ 2** 詳細を表示する特定のアラームをクリックします。[アラーム詳細 (Alarm Details)] ページが表示されます。
- ステップ 3** 右上隅にあるボタンを使用して、このアラームに関連する次の操作のいずれかを実行できます。
- [プレフィックス/ASNをポリシーから削除 (Remove Prefix/ASN from Policy)] をクリックして、ポリシーからアラームをトリガーしたプレフィックスまたは ASN とルールを削除します。
 - [スヌーズ (Snooze)] をクリックして一時的にアラームのアラートを停止し、アラームをスヌーズする時間範囲を選択してから、[スヌーズ (Snooze)] をクリックします。Crosswork Cloud Network Insights は、選択した期間、このアラームの通知は送信しません。
- アラームをスヌーズすると、アラームは [アクティブ (Active)] アラームページから [確認済みアラーム (Acknowledged Alarm)] ページに移動します。[アラーム (Alarms)] > [履歴 (History)] タブでは、アラームの状態が [スヌーズ済み (Snoozed)] に設定されており、その状態のままになる時間が示されています。スヌーズしたアラームをキャンセルするには、[アラームの詳細 (Alarm details)] ページに戻り、[未確認 (Unacknowledge)] をクリックします。
- [確認 (Acknowledge)] をクリックして、アラームを確認済みの状態にします。これは、アラームが認識され、確認されることを意味します。
- アラームを確認すると、アラームは [アクティブ (Active)] アラームページから [確認済み (Acknowledged)] ページに移動します。

ステップ 4 アラームに関する追加情報を表示するには、次のいずれかのタブをクリックします。

(注) 以下に説明するすべてのタブが、すべてのアラームタイプに表示されるわけではありません。指定したアラームタイプに関連するタブのみを使用できます。

- [概要 (Overview)] : このページはデフォルトで表示されます。アラームが発生したポリシーに含まれるアラームおよびルールに関する詳細が含まれています。詳細については、[アラームの概要の詳細 \(42 ページ\)](#) を参照してください。
- [関連するBGP更新 (Relevant BGP Updates)] : このアラームをトリガーしたピアによってレポートされたBGP更新に関する詳細が含まれています。詳細については、[アラームに関連するBGP更新の詳細 \(44 ページ\)](#) を参照してください。
- [プレフィックス (Prefixes)] : アラームのプレフィックス情報が含まれます。[アラームプレフィックスの詳細 \(43 ページ\)](#) を参照してください。
- [履歴 (History)] : アラームに関する履歴の詳細が含まれています。詳細については、[アラーム履歴の表示 \(45 ページ\)](#) を参照してください。

アラームの概要の詳細

アラームの概要の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[概要 (Overview)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームの概要の詳細が表示されます。

表 3: アラームの概要のフィールドに関する説明

フィールド	説明
重大度	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。
非アクティブ化 (Deactivated)	アラームが以前に非アクティブ化された日時。
最後のユーザアクション (Last User Action)	ユーザがこのアラームに対して実行した直近のアクション。
想定される結果 (Expected)	Crosswork Cloud Network Insights がアラームをレポートすることを想定する値。
観察 (Observed)	Crosswork Cloud Network Insights によって観察された実際の値。
違反ピア	違反を観察したピア。

フィールド	説明
地理的マップ (Geographical map)	アラームが発生した場所。
注記 (Notes)	アラームに関するメモを入力します。

アラーム検索グラスの詳細

アラームの検索グラスの詳細を表示するには、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示するアラームの [表示 (View)] をクリックしてから、[検索グラス (Looking Glass)] タブをクリックします。



(注) このタブは、使用可能で、指定したアラームタイプに関連する場合にのみ表示されます。

Crosswork Cloud Network Insights では、次の表に示すように、アラームの検索グラスの詳細が表示されます。

表 4: アラーム検索グラスのフィールドに関する説明

フィールド	説明
ピア AS (Peer AS)	ピア AS。
ピア (Peer)	ピアを識別するために使用されるが、その ID は非公開のままに維持するピア識別子。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
最終変更日 (Last Modified)	プレフィックスが最後に変更された日時。

アラームプレフィックスの詳細

アラームのプレフィックスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[プレフィックス (Prefixes)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームのプレフィックスの詳細が表示されます。

表 5: アラームプレフィックスのフィールドに関する説明

フィールド	説明
違反 (Violating)	予期しないプレフィックスを表示するには、[違反 (Violating)] をクリックします。
登録 (Subscribed)	[登録 (Subscribed)] をクリックすると、自分が登録しているプレフィックスのみが表示されます。
すべて (All)	[すべて (All)] をクリックすると、すべての違反プレフィックスおよび登録済みプレフィックスが表示されます。
プレフィックス (Prefix)	違反が発生したプレフィックス。
レポートピア (Reporting Peers)	違反をレポートしたピアの数。
登録 (Subscribed)	プレフィックスに登録されているかどうかを示します。

アラームに関連する BGP 更新の詳細

アラームに関連する BGP 更新の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[関連する BGP 更新 (Relevant BGP Updates)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームに関連する BGP 更新の詳細が表示されます。

表 6: アラーム関連の BGP 更新のフィールドに関する説明

フィールド	説明
非表示 (Not displayed)	更新が 6 ヶ月より古い違反ピアが表示されない場合は、メモが表示されます。
ピア (Peer)	BGP 更新を受信したピア。
ピア AS (Peer AS)	BGP 更新を受信したピア AS。
プレフィックス (Prefix)	BGP 更新を受信したプレフィックス。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
更新のタイプ (Update Type)	BGP 更新のタイプ。
最終更新日 (Last Updated)	前回の BGP 更新の日時。

アラームサブプレフィックスの詳細

アラームのサブプレフィックスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [アラーム (Alarms)] の順にクリックし、詳細を表示する特定のアラームをクリックしてから、[サブプレフィックス (Subprefixes)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、アラームのサブプレフィックスの詳細が表示されます。



表 7: アラームサブプレフィックスのフィールドに関する説明

フィールド	説明
プレフィックス (Prefix)	サブプレフィックスがアドバタイズされたプレフィックス。
登録 (Subscribed)	プレフィックスに登録されているかどうかを示します。
ピア AS (Peer AS)	サブプレフィックス アドバタイズメントのピア AS。
ピア (Peer)	サブプレフィックス アドバタイズメントのピア。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
最終変更日 (Last Modified)	最後に行った変更の日時。



アラーム履歴の表示

[アラーム履歴 (Alarm history)] ページには、時間範囲を指定できる履歴アラームが表示されます。デフォルトでは、アラームは最新の [イベント (EVENTAt)] の日付でソートされます。アラームの履歴には、そのライフサイクル中に発生したすべての状態遷移が含まれます。アラーム履歴レコードは変更されません。

ステップ 1 このページには次のようにしてアクセスできます。


- Crosswork Cloud Network Insights の場合 :
 -  > [モニター (Monitor)] > [アラーム (Alarms)] から、詳細を表示する特定のアラームをクリックし、[履歴 (History)] タブをクリックします。
 -  > [設定 (Configure)] > [ポリシー (Policies)] <ポリシー名> > [アラーム (Alarms)] タブ > [履歴 (History)] タブをクリックします。

- Crosswork Cloud Traffic Analysis の場合 :

-  > [モニター (Monitor)] > [アラーム (Alarms)] から、詳細を表示する特定のアラームをクリックし、[履歴 (History)] タブをクリックします。
-  > [設定 (Configure)] > [ポリシー (Policies)] <ポリシー名> > [アラーム (Alarms)] タブ > [履歴 (History)] タブをクリックします。

ステップ 2 [タイムフレーム (Timeframe)] ドロップダウンリストから、目的の期間を選択します。ウィンドウが更新され、選択した時間範囲のアラート情報が表示されます。

ステップ 3 [フィルタの追加 (Add Filter)] テキストを表示する任意の列をフィルタリングできます。[フィルタの追加 (Add Filter)] をクリックし、フィルタリングするテキストを入力します。

ステップ 4 [タイムフレーム (Timeframe)] ドロップダウンリストで、次のタスクのいずれかをクリック  して実行します。

- [列のカスタマイズ (Customize Columns)] : デフォルトでは、使用可能なすべての列が表示されるわけではありません。列を追加、削除、または並べ替えるには、このオプションを選択します。
- [CSVのエクスポート (Export CSV)] : 現在ロードされているすべての行をエクスポートするには、このオプションを選択します。
 - (注) ロードされた行は、現在表示されている行であり、合計の全体の一部にすぎない可能性があります。下にスクロールすると、さらに多くの行をロードできます。
- [テーブル設定の保存 (Save Table Settings)] : カスタマイズしたテーブル設定を保存するには、このオプションを選択します。これには、列幅のサイズ変更、列の追加または削除、および適用されたフィルタが含まれます。最初にテーブル設定を保存した後、[テーブル設定の削除 (Remove Table Settings)] または [テーブル設定の更新 (Update Table Settings)] を選択できます。

(注) トリガー値の上にマウスを合わせると、Whois 情報が表示されます (使用可能な場合)。



第 9 章

ASN のモニタ

- [すべての ASN の表示](#) (47 ページ)
- [ASN の詳細の表示](#) (48 ページ)
- [ASN の概要の詳細](#) (48 ページ)
- [ASN アラームの詳細](#) (49 ページ)
- [ASN BGP 更新の詳細](#) (50 ページ)
- [ASN 検索グラスの詳細](#) (51 ページ)
- [ASN ROA の詳細](#) (51 ページ)
- [ASN RPSL カバレッジ](#) (52 ページ)
- [ASN トラフィックの詳細の表示](#) (54 ページ)
- [日次 ASN 変更の表示 \(ASN ルーティングレポート\)](#) (55 ページ)

すべての ASN の表示

次の手順に従って、すべての ASN を表示できます。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックします。

Crosswork Cloud Network Insights では、次の列に情報が表示されます。

- [ASN] : ASN。
- [ポリシー (Policy)] : ASN に関連付けられたポリシー。
- [タグ (Tags)] : ASN に関連付けられたタグのリスト。
- [アクティブなアラーム (Active Alarms)] : ASN に関連付けられたアクティブなアラームの数。
- [シビラティ (重大度) (Severity)] : ASN に関連付けられた最上位のアラームレベル ([高 (High)]、[中 (Medium)]、または [低 (Low)])。
- [最後のアクティブなアラーム (Last Active Alarm)] : ASN に関連付けられた最後のアクティブなアラームのアラームタイプ、日、時刻。

ステップ2 特定のプレフィックスに関する詳細を表示するには、ASN をクリックします。[ASN の詳細の表示 \(48 ページ\)](#) を参照してください。

ステップ3 新しいASNを追加するには、[ASNのモニタ (Monitor ASNs)] をクリックします。詳細については、[監視するASNを追加する \(91 ページ\)](#) を参照してください。

ASN の詳細の表示

ステップ1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックします。

ステップ2 特定のASNに関する詳細を表示するには、ASN名をクリックします。

ステップ3 ASNに関する詳細を表示するには、次のいずれかのタブをクリックします。

- [概要 (Overview)] : ASNに関する概要情報が含まれています。詳細については、[ASNの概要の詳細 \(48 ページ\)](#) を参照してください。
- [アラーム (Alarms)] : ASNに関連付けられたアラームの詳細を提供します。詳細については、[ASNアラームの詳細 \(49 ページ\)](#) を参照してください。
- [トラフィック (Traffic)] : ASNで実行されているトラフィックに関する詳細を提供します。
- [BGP更新 (BGP Updates)] : アラームをトリガーしたBGP更新に関する詳細が含まれています。詳細については、[ASN BGP更新の詳細 \(50 ページ\)](#) を参照してください。
- [検索グラス (Looking Glass)] : ASNの検索グラスの情報が含まれています。詳細については、[ASN検索グラスの詳細 \(51 ページ\)](#) を参照してください。
- [ROA] : ASNに関連付けられたすべての既知のROAに関する詳細が含まれています。詳細については、[ASN ROAの詳細 \(51 ページ\)](#) を参照してください。
- [RPSL] : ASNに関連付けられたRPSLデータが含まれています。詳細については、[ASN RPSLカバレッジ \(52 ページ\)](#) を参照してください。
- [レポート (Reports)] : このASNで使用可能なレポートを一覧表示します。レポートを設定するには、[設定 (Configure)] をクリックします。詳細については、[ASNルーティングレポートの設定 \(211 ページ\)](#) を参照してください。

ASN の概要の詳細

ASNの概要の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [ASN] の順にクリックし、ASNの名前をクリックしてから、[概要 (Overview)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、ASN の概要の詳細が表示されます。

表 8: ASN 概要の詳細のフィールドに関する説明

フィールド	説明
リンクされたポリシー (Linked Policy)	ASN に関連付けられたポリシー。
タグ (Tags)	ASN に適用されるユーザ指定のタグ。
最後のアクティブなアラーム (Last Active Alarm)	ASN に関連付けられた最後のアクティブなアラームのリスト。
発信プレフィックス (Originating Prefixes)	ASN の発信プレフィックスの数。
要約 (Summary)	ピアの地理的な位置と数を示すマップを含む要約データ。
IRR/RPSL データ (IRR/RPSL data)	<p>ASN の RPSL 情報を提供します。Crosswork Cloud Network Insights では、ASN の情報を検出した RPSL データベースが表示されます。</p> <p>Crosswork Cloud Network Insights は、ASN から発信される観察対象プレフィックスのリストを取得し、これを RPSL レコードの情報と比較して、発信元 ASN が一致するかどうかを判断します。[有効な RPSL プレフィックスカバレッジ (Valid RPSL Prefix Coverage)] は、プレフィックスが RPSL データベースで指定されたものと同じ ASN から発信されたことを Crosswork Cloud Network Insights が検証したプレフィックスの数を示します。RPSL の詳細を表示するには、番号をクリックします。詳細については、ASN RPSL カバレッジ (52 ページ) を参照してください。</p>
ピア (Peers)	ピアの数と、ピアの場所を示すマップ。ピアの表形式のビューを表示するには、[テーブル (Table)] をクリックします。
注記 (Notes)	ASN に関連付けられたユーザ設定のメモ。

ASN アラームの詳細

ASN アラームの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [ASN] の順にクリックし、ASN の名前をクリックしてから、[アラーム (Alarms)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、ASN のアラームの詳細が表示されます。

表 9: ASN アラームの詳細のフィールドに関する説明

フィールド	説明
アラームの状態 (Alarm state)	次のアラームの状態のいずれかをクリックします。 <ul style="list-style-type: none"> [アクティブ (Active)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべてのアクティブなアラームのリストが表示されます。 [確認済み (Acknowledged)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべての確認済みアラームのリストが表示されます。
アラームの詳細 (Alarm Details)	アラームの詳細。
# ピア (# Peers)	違反をレポートしたピアの数。
シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。
注記 (Notes)	ユーザが入力したアラームに関するメモ。

ASN BGP 更新の詳細

ASN BGP 更新の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニター (Monitor)] > [ASN] の順にクリックし、ASN の名前をクリックしてから、[BGP更新 (BGP Updates)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、ASN BGP 更新の詳細が表示されます。

表 10: ASN BGP 更新の詳細のフィールドに関する説明

フィールド	説明
タイムフレーム	[タイムフレーム (Timeframe)] ドロップダウンリストから値を選択して、タイムフレームを指定します。
ピア AS (Peer AS)	BGP 更新を受信したピア AS。
プレフィックス (Prefix)	BGP 更新の受信元になっているプレフィックス IP アドレス。

フィールド	説明
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
更新のタイプ (Update Type)	BGP 更新のタイプ。
最終更新日 (Last Updated)	前回の BGP 更新の日時。

ASN 検索グラスの詳細

ASN 検索グラスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックし、ASN の名前をクリックしてから、[検索グラス (Looking Glass)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、ASN の検索グラスの詳細が表示されます。

表 11: ASN 検索グラスのフィールドに関する説明

フィールド	説明
プレフィックス (Prefix)	BGP 更新の受信元になっているプレフィックス IP アドレス。
レポートピア (Reporting Peers)	レポートピアの数。
有効 (Valid)	プレフィックスが有効かどうかを示します。
登録 (Subscribed)	特定のプレフィックスに登録済みかどうかを示します。
有効なRPSL (Valid RPSL)	プレフィックスが RPSL データベースで指定されたものと同じ ASN から発信されたことを Crosswork Cloud Network Insights が検証済みかどうかを示します。

ASN ROA の詳細

ASN ROA の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックし、ASN の名前をクリックしてから、[ROA] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、ASN ROA の詳細が表示されます。

表 12: ASN ROA の詳細のフィールドに関する説明

フィールド	説明
ROA ステータス別 AS プレフィックス (AS Prefixes by ROA Status)	各ステータスの ROA を持つ ASN のプレフィックスの総数。
観察対象プレフィックス (Observed Prefix)	ASN によって発信されたプレフィックスに対する観察対象プレフィックス。
ROA プレフィックス (ROA prefix)	ROA が AS のアドバタイズを許可するベース IP プレフィックス。ROA は、最大長によって決定されるベースプレフィックスのサブネットの範囲をカバーできます。
最大長 (Max Length)	ROA が AS のアドバタイズを許可する最も具体的な IP プレフィックスの最大プレフィックス長。
送信元 (Source)	ROA を公開した組織。
発信元ASN (Origin ASN)	プレフィックスの発信が ROA によって許可される AS 番号。
ROAステータス (ROA Status)	ROA のステータスは次のいずれかになります。 <ul style="list-style-type: none"> • [有効 (Valid)] : ROA 証明書は有効です。 • [期限切れ (Expired)] : 現在の時刻が ROA の <i>not-after</i> または <i>end</i> の時刻を過ぎています。 • [不明 (Unknown)] : このプレフィックスには一致する ROA がありません。
開始 (Start)	この ROA が有効と見なされる開始日時。
終了 (End)	この ROA が有効と見なされる終了日時。

ASN RPSL カバレッジ

ASN RPSL の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)]>[モニタ (Monitor)]>[ASN (ASNs)]の順にクリックし、ASN の名前をクリックしてから、[RPSL] タブをクリックします。

Crosswork Cloud Network Insights では、ASN から発信される観察対象のすべてのプレフィックスの RPSL レコードを収集し、次の表に示すように、RPSL レコードが表示されます。



- (注) テーブルには、特定のプレフィックスに対して複数の行が存在する場合があります。これは、Crosswork Cloud Network Insights で特定のプレフィックスのすべてのレコードが表示されるためです。データベースに2つのRPSLレコードがあり、それぞれがプレフィックスに異なる発信元ASNを指定している場合、Crosswork Cloud Network Insights で両方のレコードが表示されます。

表 13: ASN RPSL の詳細のフィールドに関する説明

フィールド	説明
ビューオプション (View options)	<p>表示する RPSL レコードを選択します。</p> <ul style="list-style-type: none"> • [すべて (All)] : すべての RPSL レコードを表示します。 • [有効 (Valid)] : プレフィックスが RPSL データベースで指定されたものと同じ ASN から発信されたことを Crosswork Cloud Network Insights が検証した、有効な RPSL レコードと部分一致の RPSL レコードを表示します。 • [不一致 (Mismatch)] : プレフィックスが RPSL データベースで指定されているものとは異なる ASN から発信された RPSL レコードを表示します。 • [RPSLなし (No RPSL)] : RPSL レコードがないプレフィックスを表示します。
最後のスキャン (Last Scan)	<p>Crosswork Cloud Network Insights が RPSL データベースを最後にスキャンした日時。Crosswork Cloud Network Insights は、RPSL データベースを 1 日に 1 回スキャンします。</p> <p>Crosswork Cloud Network Insights が各 RPSL データベースをスキャンした特定の日時を表示するには、日付をクリックします。これにより、Crosswork Cloud Network Insights が最後に RPSL データベースからデータを取得したのはどの時点かを判断できます。</p>
プレフィックス (Prefix)	Crosswork Cloud Network Insights によって観察された、この ASN から発信されたプレフィックス。
送信元 (Source)	Crosswork Cloud Network Insights がこのレコードを取得した RPSL データベースソース。プレフィックスは複数の RPSL データベースにレコードを持つことができるため、Crosswork Cloud Network Insights で、各データベースソースが新しい行に表示されます。
発信元ASN (Origin ASN)	RPSL レコードの <i>origin</i> 属性で指定された ASN。
説明 (Description)	RPSL route / route6 レコード内の <i>descr</i> 属性。通常、ルートレコードに関する説明が含まれています。

フィールド	説明
Member Of	PSL route/route6 レコードの <i>member-of</i> 属性。これは、route/route6 レコードが関連付けられているルートセットを示します。
分類 (Classification)	<p>プレフィックスの RPSL レコードの分類。Crosswork Cloud Network Insights は、プレフィックスと完全に一致する RPSL レコードを検出できない場合、親の RPSL レコードを調べて分類を決定します。分類値は次のいずれかになります。</p> <ul style="list-style-type: none"> • [不一致 (Mismatch)] : プレフィックスの発信元 ASN が RPSL データベースで指定されたものとは異なることを、Crosswork Cloud Network Insights が判断したことを示します。 • [有効 (Valid)] : プレフィックスがそのプレフィックスの RPSL レコードで指定された発信元 ASN から発信されたことを、Crosswork Cloud Network Insights が検証したことを示します。 • [部分一致 (Partial Match)] : プレフィックスはそのプレフィックスの親の RPSL レコードの発信元 ASN として指定された ASN から発信されていることを、Crosswork Cloud Network Insights が検証したことを示します。部分一致の分類には、この分類に一致する親プレフィックスも含まれます。 • [RPSLなし (No RPSL)] : RPSL データベースでプレフィックスまたはその親の RPSL レコードを、Crosswork Cloud Network Insights が検出しなかったことを示します。
最終更新日 (Last Updated)	プレフィックスまたはその親の RPSL レコード内で最後に変更された属性の日時。

ASN トラフィックの詳細の表示



(注) この機能は、Crosswork Traffic Analysis 専用です。

1 つまたは複数の ASN のトラフィックの詳細を表示できます。

ステップ 1 メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックします。

Crosswork Cloud Traffic Analysis では、すべての ASN のトラフィック情報が表示されます。

- ステップ2** 特定の ASN のトラフィックの詳細を表示するには、最初の列の ASN 名または番号をクリックします。
- ステップ3** 2つ以上の ASN のトラフィックの詳細を比較するには、ASN の横にあるチェックボックスをクリックしてから、テーブルの上部にある [トラフィックの比較 (Traffic Comparison)] をクリックします。
- Crosswork Cloud Traffic Analysis では、選択したすべての ASN のトラフィック情報が表示されます。

日次 ASN 変更の表示 (ASN ルーティングレポート)

各 ASN ルーティングレポート インスタンスは、ASN のレポートが最後に生成されてからの AS ピアリング (新規、変更済み、非アクティブ) と発信されたプレフィックス (新規、変更済み、削除) の違いを要約して識別します。この日次レポートは、ASN および関連するプレフィックスに対処する必要がある RIR/RPSL/ROA 設定の潜在的な問題またはギャップに焦点を当て、役に立ちます。各レポートインスタンスは、設定したエンドポイントに送信され、Crosswork Cloud のレポート UI への直接リンクが含まれています。この手順では、UI を使用してレポートインスタンスの内容を表示する方法について説明します。

始める前に

日次レポートを表示する前に、ASN ルーティングレポートを設定する必要があります。詳細については、[ASN ルーティングレポートの設定 \(211 ページ\)](#) を参照してください。

- ステップ1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [ASN (ASNs)] の順にクリックします。
- ステップ2** ASN の名前をクリックし、[レポート (Reports)] をクリックします。
この ASN に対して生成されたすべてのレポートが、このページに概要とともに表示されます。
- ステップ3** レポートインスタンス名をクリックします。
デフォルトでは、[概要 (Summary)] ページに AS ピアリングとプレフィックス変更の高レベルの数が表示されます。
- ステップ4** 次の [AS ピアリング変更 (AS Peering Changes)] 値のいずれかをクリックします。
- [新規 (New)] : [AS ピア (AS Peers)] ページには、最後のレポートインスタンス以降の新しい AS ピアリングが表示されます。
 - [変更済み (Changed)] : [AS ピア (AS Peers)] ページには、最後のレポートインスタンス以降に変更された AS ピアリングのリストが表示されます。
 - [非アクティブ (Inactive)] : [AS ピア (AS Peers)] ページには、最後のレポートインスタンス以降に [非アクティブ (Inactive)] としてマークされた AS ピアリングが表示されます。選択した ASN で少なくとも 30 日間、この ASN ピアリングを含むプレフィックス通知がない (ASN がどの AS パスにも表示されない) 場合、AS ピアリングは非アクティブとしてマークされます。[前回の検出 (Last Seen)] 列には、AS ピアが最後にアクティブだった時間が表示されます。
- (注) 詳細については、[AS ピアレポート \(56 ページ\)](#) を参照してください。

ステップ 5 [IPv4/IPv6プレフィックスの変更 (IPv4/IPv6 Prefix Changes)] 値をクリックします。

- [新規 (New)] : [IPv4/IPv6プレフィックス (IPv4/IPv6 Prefix)] ページには、最後のレポートインスタンス以降にこの ASN から発信されて検出された新しいプレフィックスが表示されます。
- [変更済み (Changed)] : [IPv4/IPv6プレフィックス (IPv4/IPv6 Prefix)] ページには、この ASN から発信されて検出された、最後のレポートインスタンス以降に変更されたプレフィックスのリストが表示されます。
- [削除済み (Deleted)] : [IPv4/IPv6プレフィックス (IPv4/IPv6 Prefix)] ページには、最後のレポートインスタンス以降に取り消されたプレフィックスのリストが表示されます。

(注) 詳細については、[IPv4 および IPv6 プレフィックスレポート \(57 ページ\)](#) を参照してください。

AS ピアレポート

[ASピア (AS Peers)] ページには、選択した ASN がピアリングしている ASN と、最後に生成されたレポートインスタンス以降に変更された詳細が表示されます。



(注) デフォルトでは、[新規 (New)]、[アクティブで変更済み (Active Changed)]、または [非アクティブ (Inactive)] 状態の AS ピアリングのみがページに表示されます。すべての AS ピアリングと状態を表示するには、フィルタに [アクティブ (Active)] を含めるか、またはフィルタをリセットして、[アクティブ (Active)] (ただし変更されていない) AS ピアリングも含む AS ピアリングの完全なセットを表示します。

- [ピアASN (Peer ASN)] : 対象の ASN との AS ピアリング。
- [ピアリングタイプ (Peering Type)] : ピア ASN が対象の ASN のすぐ上流または下流であるかどうかを示します。
- [ピアリング状態 (Peering State)] : レポートインスタンスが生成された時点の AS ピアリング状態を表示します。次のリストに、ASN ピアリングで考えられる状態を示します。
 - [アクティブ (Active)] : 2つの ASN 間のピアリングが確認されました。これは、最初に生成されたレポートインスタンスであるか、最後のレポートインスタンス以降、このピアリングについて何も変更されていません。
 - [アクティブで変更済み (Active Changed)] : ピアリングはアクティブでしたが、最後のレポートインスタンス以降に変更されました。
 - [新規 (New)] : これは新しい AS ピアリングです。このピアリングは、以前のレポートインスタンスにはありませんでした。
 - [非アクティブ (Inactive)] : 非アクティブ状態は、2つの ASN 間のピアリングが少なくとも 30 日間どの AS パスにも存在しないことを意味します。

- [プレフィックス数 (Prefix Count)] : アドバタイズメントに AS パスの AS ピアリングが含まれるプレフィックスの数を示します。
- [新しいプレフィックス数 (New Prefix Count)] : アドバタイズされる新しいプレフィックスの数を示します。
- [最初の確認日時/最新の確認日時 (First Seen/Last Seen)] : プレフィックス通知の AS パスに ASN ピアリングが最初に表示された時刻または最後に表示された時刻を表示します。

IPv4 および IPv6 プレフィックスレポート

IPv4 および IPv6 プレフィックスページには、レポートインスタンスが生成された時点のプレフィックスステータスと詳細が表示されます。



- (注) デフォルトでは、[新規 (New)]、[アクティブで変更済み (Active Changed)]、または [非アクティブ (Inactive)] 状態のプレフィックスのみがページに表示されます。すべての AS ピアリングと状態を表示するには、フィルタに [アクティブ (Active)] を含めるか、またはフィルタをリセットして、[アクティブ (Active)] (ただし変更されていない) プレフィックスも含むプレフィックスの完全なセットを表示します。

次の詳細情報が表示されます。

- [プレフィックス (Prefix)] : 選択した ASN のすべてのプレフィックスを一覧表示します。
- [登録 (Subscribed)] : レポートが生成された時点のサブスクリプションステータスを表示します。
- [RIR情報 (RIR Information)] : IPv4 プレフィックスに使用できる場合は、Whois 情報が表示されます。この列は現在、IPv6 プレフィックスには適用されません。
- [ヘルス (Health)] : IPv4 プレフィックスでは、RIR 情報または ROA レコードが使用できない場合、または関連付けられていない場合、[注意が必要 (Needs Attention)]。IPv6 プレフィックスでは、関連付けられている ROE レコードがない場合、[注意が必要 (Needs Attention)]。
- [プレフィックス状態 (Prefix State)] : レポートインスタンスが生成された時点のプレフィックスステータスを表示します。プレフィックスがアクティブであるが、前日から変更されている場合、状態は [アクティブで変更済み (Active Changed)] になります。
 - [アクティブ (Active)] : プレフィックスは ASN から発信されていることが確認されています。これは、最初に生成されたレポートインスタンスであるか、最後のレポートインスタンス以降、このプレフィックスについて何も変更されていません。
 - [アクティブで変更済み (Active Changed)] : プレフィックスはアクティブでしたが、最後のレポートインスタンス以降に変更されました。
 - [新規 (New)] : これは新しい ASN プレフィックスです。このプレフィックスは、以前のレポートインスタンスにはありませんでした。

- [削除済み (Deleted)] : プレフィックスは、最後のレポートインスタンス以降に取り消されています。
- [RPSLステータス (RPSL Status)] : レポートインスタンスが生成された時点の RPSL 情報を表示します。RPSL 情報が見つかり、発信元 ASN が発信元であることが確認された ASN と一致する場合、RPSL ステータスは [有効 (Valid)] です。RPSL レコードが見つかり、レコード内の発信元 ASN が確認された発信元 ASN と一致しない場合、RPSL ステータスは [不一致 (Mismatch)] です。プレフィックスに関連付けられた RPSL レコードがない場合、ステータスは [見つかりません (Not Found)] です。
- [ROAステータス (ROA Status)] : [期限切れ間近 (Expiring Soon)] は、プレフィックスに関連付けられた ROA レコードが 1 日以内に期限切れになることを示します。必要に応じてレコードを更新できるように、[期限切れ間近 (Expiring Soon)] ステータスの列をフィルタリングすることもできます。[ROA期限切れROA数 (ROA Expiring ROA Count)] 列を表示して、選択したステータスに関連付けられているレコードの数を確認します。
- [RIR状態 (RIR State)] : レポートインスタンスが生成された時点のプレフィックスの RIR 情報の状態を表示します。RIR 情報が見つかり、発信元 ASN が発信元であることが確認された ASN と一致する場合、RIR ステータスは [有効 (Valid)] です。RIR 情報が見つかり、レコード内の発信元 ASN が確認された発信元 ASN と一致しない場合、RIR ステータスは [不一致 (Mismatch)] です。プレフィックスの RIR 情報が見つからない場合、ステータスは [見つかりません (Not Found)] です。
- [有効なRPSL (Valid RPSL)] : プレフィックスの有効な RPSL レコードの数を示します。
- [期限切れROA (Expiring ROA)] : 1 日以内にそのプレフィックスに対して期限切れになる ROA レコードの数を示します。
- [ピアカウント (Peer Count)] : プレフィックスをアドバタイズしているピアの数を示します。



第 10 章

プレフィックスのモニタ

- [プレフィックスの概要 \(59 ページ\)](#)
- [プレフィックスの追加 \(59 ページ\)](#)
- [すべてのプレフィックスの表示 \(60 ページ\)](#)
- [プレフィックスの詳細の表示 \(61 ページ\)](#)
- [プレフィックストラフィックの詳細の表示 \(67 ページ\)](#)

プレフィックスの概要

Crosswork Cloud Network Insights を開始する際は、まずプレフィックスの追加から始めます。プレフィックスを追加すると、[プレフィックス (prefixes)] ウィンドウに、プレフィックス、関連ポリシー、および大規模ネットワークのモニタリングに役立つその他の情報の統合ビューが表示されます。[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] ウィンドウ：

- プレフィックス情報を保存および追跡する場所を提供します。
- プレフィックスの状態、アラームステータス、およびプレフィックスの詳細が表示されます。
- 世界中の監視ポイントからプレフィックスをモニタし、単一の監視ポイントのモニタリングシステムでは見過ごされる可能性のある地域のイベントを検出します。
- プレフィックスを登録または登録解除できます。

プレフィックスの追加

ステップ 1 メインウィンドウで、[プレフィックス (Prefixes)] をクリックします。

ステップ 2 [プレフィックスへの登録 (Subscribe to Prefixes)] をクリックします。

ステップ 3 次のいずれかのタブをクリックします。

- [手動 (Manual)]: 登録するプレフィックスの IP アドレスを入力します。複数のプレフィックスを追加するには、それぞれのプレフィックスの間にカンマ (,) を入力します。/8 より小さいプレフィックスマスクは追加できません。たとえば、1.1.0.0/3 などのプレフィックスは追加できません。
- [ASNルックアップ (ASNLookup)]: 関連付けられたプレフィックスを検索する ASN を入力します。
- [CSVの上書き (CSV Overwrite)]: プレフィックス情報を含む CSV ファイルをアップロードします。詳細については、[構成ファイルのアップロード \(251 ページ\)](#) を参照してください。

ステップ 4 [マニュアル (Manual)]または[ASNルックアップ (ASNLookup)]を選択した場合は、必要な情報を入力した後、[次へ (Next)]をクリックします。

ステップ 5 以前にポリシーを作成した場合は、[ポリシー (Policy)]ドロップダウンリストからプレフィックスに関連付けるポリシーを選択します。詳細については、[Crosswork Cloud Network Insightsポリシーの追加 \(101 ページ\)](#) を参照してください。

(注) プレフィックスは1つのポリシーにのみ関連付けることができます。

ステップ 6 (任意) [タグ (Tags)]フィールドに意味のあるテキストを入力します。

(注) 複数のプレフィックスを入力した場合は、指定したポリシーとタグがすべてのプレフィックスに適用されます。

ステップ 7 変更内容を確認し、[送信 (Submit)]をクリックして変更を適用します。

すべてのプレフィックスの表示

次の手順に従って、すべてのプレフィックスを表示できます。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)]>[モニタ (Monitor)]>[プレフィックス (Prefixes)]の順にクリックします。

Crosswork Cloud Network Insights では、次の列に情報を持つプレフィックスのリストが表示されます。

- [プレフィックス (Prefix)]: プレフィックスの IP アドレス。
- [ポリシー (Policy)]: プレフィックスに関連付けられたポリシー。
- [タグ (Tags)]: プレフィックスに関連付けられたタグのリスト。
- [アクティブなアラーム (Active Alarms)]: プレフィックスに関連付けられたアクティブなアラームの数。
- [シビラティ (重大度) (Severity)]: プレフィックスに関連付けられたアラームレベル ([高 (High)]、[中 (Medium)]、または[低 (Low)])。
- [最後のアクティブなアラーム (Last Active Alarm)]: プレフィックスに関連付けられた最後のアクティブなアラームのアラームタイプ、日、時刻。

- ステップ2** 特定のプレフィックスに関する詳細を表示するには、プレフィックスのIPアドレスをクリックします。[プレフィックスの詳細の表示 \(61 ページ\)](#) を参照してください。
- ステップ3** 新しいプレフィックスを追加するには、[プレフィックスへの登録 (Subscribe to Prefixes)] をクリックします。[プレフィックスの追加 \(87 ページ\)](#) を参照してください。

プレフィックスの詳細の表示

特定のプレフィックスに関する詳細情報を表示できます。

- ステップ1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックします。
- ステップ2** 特定のプレフィックスに関する詳細を表示するには、プレフィックスのIPアドレスをクリックします。
- ステップ3** プレフィックスに関する詳細を表示するには、次のいずれかのタブをクリックします。
- [概要 (Overview)] : プレフィックスに関する要約情報が含まれています。詳細については、[プレフィックスの概要の詳細 \(61 ページ\)](#) を参照してください。
 - [アラーム (Alarms)] : プレフィックスに関連付けられたアラームに関する詳細を提供します。詳細については、[プレフィックスアラームの詳細 \(62 ページ\)](#) を参照してください。
 - [BGP更新 (BGP Updates)] : アラームをトリガーしたBGP更新に関する詳細が含まれています。詳細については、[プレフィックス BGP 更新の詳細 \(63 ページ\)](#) を参照してください。
 - [検索グラス (Looking Glass)] : プレフィックスの検索グラスの情報が含まれています。詳細については、[プレフィックス検索グラスの詳細 \(64 ページ\)](#) を参照してください。
 - [ROA] : プレフィックスに関連付けられたすべての既知のROAに関する詳細が含まれています。詳細については、[プレフィックス ROA の詳細 \(64 ページ\)](#) を参照してください。
 - [RPSL] : プレフィックスに関連付けられたルーティングポリシー仕様言語 (RPSL) のデータが含まれています。詳細については、[プレフィックス RPSL の詳細 \(65 ページ\)](#) を参照してください。

プレフィックスの概要の詳細

プレフィックスの概要の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスのIPアドレスをクリックしてから、[概要 (Overview)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、プレフィックスの概要の詳細が表示されます。

表 14: プレフィックスの概要の詳細のフィールドに関する説明

フィールド	説明
リンクされたポリシー (Linked Policy)	プレフィックスに関連付けられたポリシー。
最終変更日 (Last Modified)	プレフィックスが最後に変更された日時。
タグ	プレフィックスに適用されるユーザ指定のタグ。
最後のアクティブなアラーム (Last Active Alarm)	プレフィックスに関連付けられた最後のアクティブなアラームのリスト。
要約 (Summary)	ピアの地理的な位置と数を示すマップを含む要約データ。
有効なRPSLカバレッジ (Valid RPSL coverage)	Crosswork Cloud Network Insights によって観察された ASN と一致する発信元 ASN を持つ、このプレフィックスの RPSL レコードの総数。詳細については、 プレフィックス RPSL の詳細 (65 ページ) を参照してください。
ピア (Peers)	ピアの数と、ピアの場所を示すマップ。ピアの表形式のビューを表示するには、[テーブル (Table)] をクリックします。
連絡先 (Contacts)	プレフィックスの連絡先情報。
発信元 (Origins)	観察された値とその発信元の詳細。
観察 (Observed)	観察値とその算出元。
アップストリーム (Upstream)	アップストリームの詳細とその取得元。
注記 (Notes)	プレフィックスに関連付けられたユーザ入力メモ。

プレフィックスアラームの詳細

プレフィックスアラームの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスの IP アドレスをクリックしてから、[アラーム (Alarms)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、プレフィックスのアラームの詳細が表示されます。

表 15: プレフィックスアラームの詳細のフィールドに関する説明

フィールド	説明
アラームの状態 (Alarm state)	次のアラームの状態のいずれかをクリックします。 <ul style="list-style-type: none"> [アクティブ (Active)] : Crosswork Cloud Network Insights では、優先度順にソートされたすべてのアクティブなアラームのリストが表示されます。 [確認済み (Acknowledged)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべての確認済みアラームのリストが表示されます。
アラームの詳細 (Alarm Details)	アラームの詳細。
# ピア (# Peers)	違反をレポートしたピアの数。
シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。
注記 (Notes)	アラームについて入力されたメモ。

プレフィックス BGP 更新の詳細

プレフィックスの BGP 更新の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスの IP アドレスをクリックしてから、[BGP更新 (BGP Updates)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、プレフィックスの BGP 更新の詳細が表示されます。

表 16: プレフィックスの BGP 更新のフィールドに関する説明

フィールド	説明
タイムフレーム	[タイムフレーム (Timeframe)] ドロップダウンリストから値を選択して、特定のタイムフレームを指定します。
ピア AS (Peer AS)	BGP 更新を受信したピア AS。
プレフィックス (Prefix)	プレフィックス。
AS パス (AS Path)	AS ルーティングパス。

フィールド	説明
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
更新のタイプ (Update Type)	BGP 更新のタイプ。
最終更新日 (Last Updated)	前回の BGP 更新の日時。

プレフィックス検索グラスの詳細

プレフィックス検索グラスの詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスの IP アドレスをクリックしてから、[検索グラス (Looking Glass)] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、検索グラスの詳細が表示されます。

表 17: プレフィックス検索グラスのフィールドに関する説明

フィールド	説明
ピア AS (Peer AS)	ピア AS。
ピア (Peer)	ピアを識別するために使用されるが、その ID は非公開のままに維持するピア識別子。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合)。
最終変更日 (Last Modified)	プレフィックスが最後に変更された日時。

プレフィックス ROA の詳細

プレフィックス ROA の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスの IP アドレスをクリックしてから、[ROA] タブをクリックします。

Crosswork Cloud Network Insights では、次の表に示すように、プレフィックスの ROA の詳細が表示されます。

表 18: プレフィックス ROA の詳細のフィールドに関する説明

フィールド	説明
ROA プレフィックス (ROA prefix)	ROA が AS のアドバタイズを許可するベース IP プレフィックス。ROA は、最大長によって決定されるベースプレフィックスのサブネットの範囲をカバーできます。
最大長 (Max Length)	ROA が AS のアドバタイズを許可する最も具体的な IP プレフィックスの最大プレフィックス長。表示しているプレフィックスのサブネットの長さが、リストされている ROA レコードの最大プレフィックス長よりも長い場合があります。この場合テキストが赤色になり、ROA レコードの最大長はプレフィックスをカバーしません。
送信元 (Source)	ROA を公開した組織。
発信元ASN (Origin ASN)	プレフィックスの発信が ROA によって許可される AS 番号。
ROA ステータス (ROA Status)	ROA のステータスは次のいずれかになります。 <ul style="list-style-type: none"> • [有効 (Valid)] : ROA 証明書は有効です。 • [期限切れ (Expired)] : 現在の時刻が ROA の <i>not-after</i> または <i>end</i> の時刻を過ぎています。 • [不明 (Unknown)] : このプレフィックスには一致する ROA がありません。
開始 (Start)	この ROA が有効と見なされる開始日時。黄色のテキストは、開始日が現在の日付より後であることを示します。
終了 (End)	この ROA が有効と見なされる終了日時。赤色のテキストは、終了日がすでに過ぎていることを示します。

プレフィックス RPSL の詳細

プレフィックス RPSL の詳細を表示するには、メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックし、プレフィックスの IP アドレスをクリックしてから、[RPSL] タブをクリックします。

Crosswork Cloud Network Insights では、プレフィックス通知を RPSL データベースと比較し、次の表に示すように、プレフィックス RPSL の詳細が表示されます。

表 19: プレフィックス RPSL の詳細のフィールドに関する説明

フィールド	説明
最後のスキャン (Last Scan)	<p>Crosswork Cloud Network Insights が RPSL データベースを最後にスキャンした日時。[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] では、RPSL データベースが 1 日に 1 回スキャンされます。</p> <p>Crosswork Cloud Network Insights が各 RPSL データベースをスキャンした特定の日時を表示するには、日付をクリックします。これにより、Crosswork Cloud Network Insights が最後に RPSL データベースからデータを取得したのはどの時点かを判断できます。</p>
送信元 (Source)	Crosswork Cloud Network Insights がこのレコードを取得した RPSL データベースソース。プレフィックスは複数の RPSL データベースにレコードを持つことができるため、Crosswork Cloud Network Insights で、各データベースソースが新しい行に表示されます。
発信元ASN (Origin ASN)	RPSL レコードで指定されたプレフィックスの発信元 ASN。
説明 (Description)	RPSL route / route6 レコード内の <i>descr</i> 属性。通常、ルートレコードに関する説明が含まれています。
Member Of	PSL route/route6 レコードの <i>member-of</i> 属性。これは、route/route6 レコードが関連付けられているルートセットを示します。

フィールド	説明
分類 (Classification)	<p>プレフィックスの RPSL レコードの分類。Crosswork Cloud Network Insights がプレフィックスと完全に一致する RPSL レコードを検出できない場合、その親に対応する RPSL レコードを調べて分類を決定します。分類値は次のいずれかになります。</p> <ul style="list-style-type: none"> • [不一致 (Mismatch)]: プレフィックスの発信元 ASN が RPSL データベースで指定されたものとは異なることを、Crosswork Cloud Network Insights が判断したことを示します。[概要 (Overview)] タブには、このプレフィックスで観察された ASN が表示されますが、これは RPSL データベースの発信元 ASN と一致しません。 • [有効 (Valid)]: プレフィックスはそのプレフィックスの RPSL レコードで指定されている発信元 ASN から発信されていることを、Crosswork Cloud Network Insights が検証したことを示します。 • [部分一致 (Partial Match)]: プレフィックスはそのプレフィックスの親の RPSL レコードの発信元 ASN として指定された ASN から発信されていることを、Crosswork Cloud Network Insights が検証したことを示します。部分一致の分類には、この分類に一致する親プレフィックスも含まれます。 • [RPSLなし (No RPSL)]: RPSL データベースでプレフィックスまたはその親の RPSL レコードを、Crosswork Cloud Network Insights が検出しなかったことを示します。
最終更新日 (Last Updated)	プレフィックスまたはその親の RPSL レコード内で最後に変更された属性の日時。

プレフィックストラフィックの詳細の表示

1つまたは複数のプレフィックスのトラフィックの詳細を表示できます。

- ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックします。
- ステップ 2** 選択したデバイス、デバイスグループ、またはタググループに関連するプレフィックスをフィルタリングして表示します。特定のプレフィックス基準を入力して検索を実行することもできます。次のいずれかのタブを選択します。

- [関連するプレフィックス (Relevant Prefixes)] : デバイスまたはデバイスグループ別のプレフィックスのリストを表示するには、このタブを選択します。
- [タグ別にグループ化 (Grouped by Tag)] : 割り当てられたタグによるプレフィックスのリストを表示するには、このタブを選択します。
- [すべて検索 (Search All)] : 追加のプレフィックス検索条件を入力するには、このタブを選択します。

ステップ 3 複数のプレフィックスのトラフィックの詳細を比較するには、プレフィックスの横にあるチェックボックスをオンにし、テーブルの上部にある [トラフィックの比較 (Traffic Comparison)] をクリックします。



第 11 章

BGP 更新のモニタ

- BGP 更新の表示 (69 ページ)

BGP 更新の表示

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [BGP 更新 (BGP Updates)] の順にクリックします。

ステップ 2 [タイムフレーム (Timeframe)] ドロップダウンリストから、特定の期間中の変更を表示する値を選択します。

二重軸のインタラクティブグラフには、その時間範囲中に発生した BGP のアドバタイズメントと取り消しが表示されます。アドバタイズメントの数がグラフの左側に表示されます。取り消しの数がグラフの右側に表示されます。

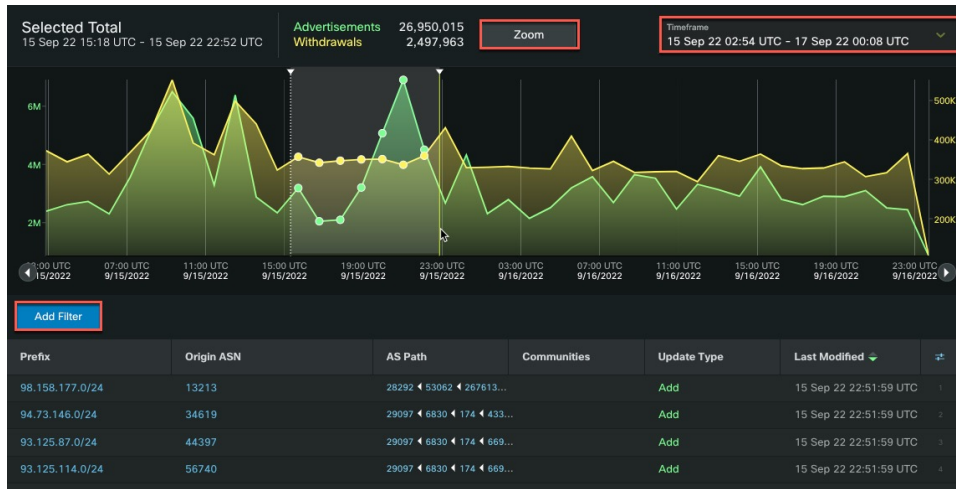
ステップ 3 特定の時間範囲 (10 分以上とする) をさらに拡大するには、開始点をクリックし、期間の最後までドラッグします。次に、[ズーム (Zoom)] をクリックします。テーブルには選択したデータのみが表示されます。

ステップ 4 このデータをフィルタリングするには、[フィルタの追加 (Add Filter)] をクリックします。

(注) [ASパス (AS Path)] 列の丸いアイコン内の数字は、繰り返し AS を示します。たとえば、次の例は、パス内の 2 つの 20764 ホップを示しています：

25291 ◀ 2914 ◀ 174 ◀ 20764 ②

図 1: BGP 更新ページ





第 12 章

デバイスのモニタリング

- デバイス ステータスの表示 (71 ページ)
- デバイス分析の詳細の表示 (72 ページ)
- Trust Insights の詳細の表示 (72 ページ)
- デバイス インベントリの表示 (76 ページ)
- デバイスの変更の表示 (76 ページ)
- デバイスソフトウェアの変更の表示 (77 ページ)
- デバイスパッケージの一致しないファイルの表示 (79 ページ)
- ファイル異常の表示 (80 ページ)
- デバイスの機能の表示 (80 ページ)

デバイス ステータスの表示

デバイスのステータスを表示して、接続やエラーを表示できます。

ステップ 1 メインウィンドウで、[モニタ (Monitor)] > [デバイス (Devices)] の順にクリックします。
以前に追加されたデバイスのリストが表示されます。

ステップ 2 [デバイス (Device)] 列に表示されているデバイス名をクリックします。

詳細なデバイス情報が表示されます。デフォルトでは、[ステータス (Status)] タブが選択され、デバイスに関する概要情報が表示されます。(ライセンスを所有しているアプリケーションに応じて、個別の製品タブも表示されます)。

ステップ 3 [ステータス (Status)] ページで、接続エラーがないことを確認します。緑色の矢印は、接続が機能していることを示します。

1. アプリケーションと Crosswork Data Gateway 間の接続が機能していることを確認します。
2. Crosswork Data Gateway とデバイス間の接続を確認します。

ステップ 4 任意のフィールドにカーソルを合わせると、詳細が表示されます。

ステップ 5 デバイスステータスを含む .json ファイルをエクスポートするには、[ステータスレポートのエクスポート (Export Status Report)] をクリックします。

デバイス分析の詳細の表示

追加したデバイスの受信 (RX) および送信 (TX) のトラフィック情報を表示できます。



(注) Netflow データは 5 分ごとにシステムに送信されるため、グラフに表示されるデータは 5 分遅れる場合があります。

ステップ 1 メインウィンドウで、[トラフィック分析 (Traffic Analysis)]>[モニター (Monitor)]>[デバイス (Devices)] の順にクリックします。

以前に追加されたデバイスのリストが表示されます。

ステップ 2 詳細を表示するデバイスの名前をクリックします。デフォルトでは、[トラフィック分析 (Traffic Analysis)] タブが表示されます。

ステップ 3 デフォルトでは、[グラフ (Graphs)] タブが開き、RX および TX のトラフィックメトリックが表示されます。[時間 (Time)] ドロップダウンリストから、トラフィック情報を表示するタイムフレームを選択します。

ステップ 4 変更を加えたら、[更新 (Refresh)] アイコンをクリックしてデータを更新します。

ステップ 5 デバイスインターフェイスのトラフィックの詳細を表示するには、[インターフェイス (Interfaces)] タブをクリックします。

ステップ 6 インターフェイスの特定の RX および TX データを表示するには、インターフェイス名をクリックします。

ステップ 7 インターフェイスを内部または外部として指定するには、1 つ以上のインターフェイスの横にあるチェックボックスをオンにして、[外部設定 (Set External)] または [内部設定 (Set Internal)] を選択します。

[タイプ (Type)] 列が更新され、インターフェイスタイプが表示されます。

Trust Insights の詳細の表示

以前に追加したデバイスの Crosswork Cloud Trust Insights の詳細を表示できます。

ステップ 1 メインウィンドウで、[トラストインサイト (Trust Insights)]>[モニタ (Monitor)]>[デバイス (Devices)] の順にクリックします。

以前に追加されたデバイスのリストが表示されます。

ステップ2 詳細を表示するデバイスの名前をクリックします。

ステップ3 デフォルトでは、[トラストインサイト (Trust Insights)]タブが開きます。デバイスの詳細ページの残りの部分には、個別のタブにまとめられた情報が含まれています。次の表に、各タブに表示されるデバイスの詳細情報を示します。

表 20: *Trust Insights* のデバイスの詳細な説明

タブ	説明
プラットフォーム	

タブ	説明
	<p><i>show platform</i> CLI コマンドの出力と同様の情報が表示されます。</p> <p>詳細を表示するには、次のタブをクリックします。</p> <ul style="list-style-type: none"> • [ハードウェア (Hardware)]: ハードウェアノード、タイプ、状態、HA 状態、最新の確認日時の情報がリストされます。 <p>[ノード (Node)]列の名前をクリックすると、そのノードに関する特定の情報が表示されます。Crosswork Cloud Trust Insights では、この個別のコンポーネントが以前に観察された場所の履歴が表示されます。ハードウェアコンポーネントの履歴は、確認されたシリアル番号に基づいて、一定期間にわたってシステム全体で個々のハードウェア FRU を追跡します。</p> <ul style="list-style-type: none"> • [パッケージインサイト (Package Insights)]: 非アクティブ化された、またはコミットされていないデバイス上のパッケージが一覧表示されます。状態は次のいずれかになります。 <ul style="list-style-type: none"> • [アクティブ - 非コミット (Active - Uncommitted)]: パッケージはデバイスでアクティブに実行されています。これらの変更を保存する場合は、デバイスをリブートする前にパッケージをコミットします。 • [非アクティブ化 (Deactivated)]: パッケージはデバイスでアクティブに実行されていませんこの変更をコミットできます。そうしないと、デバイスがリブートした後、または手動でアクティブ化された後に、パッケージが再びアクティブになります。 • [パッケージ (Packages)]: すべてのソフトウェアパッケージが一覧表示されます。詳細については、デバイスソフトウェアの変更の表示 (77 ページ) を参照してください。 • [不一致ファイル (Mismatched Files)]: このデバイス上の不一致ファイルのリストが表示されます。詳細については、デバイスパッケージの一致しないファイルの表示 (79 ページ) を参照してください。

タブ	説明
インベントリ	シリアル番号、モデル、ファームウェアなどのデバイスハードウェアの詳細情報が一覧表示されます。
変更内容	デバイスに加えられたハードウェアおよびソフトウェアの変更が表示されます。詳細については、 デバイスの変更の表示 (76 ページ) を参照してください。

デバイスインベントリの表示

Crosswork Cloud Trust Insights では、ハードウェアインベントリに関する詳細を表示できます。これは、ハードウェアの問題をトラブルシューティングする場合に役立ちます。

ステップ 1 Crosswork Cloud Trust Insights のメインウィンドウで、[トラストインサイト (Trust Insights)] > [モニタ (Monitor)] > [デバイス (Devices)] の順にクリックします。

Crosswork Cloud Trust Insights では、以前に追加されたデバイスのリストが表示されます。詳細については、[デバイスの追加 \(173 ページ\)](#) を参照してください。

ステップ 2 インベントリの詳細を表示するデバイスの名前をクリックします。

デバイス名の横に [接続済み (Connected)] が表示されている場合、Crosswork Data Gateway はデバイスに正常に接続しています。

ステップ 3 [Inventory] タブをクリックします。

Crosswork Cloud Trust Insights では、選択したデバイスに関連付けられたすべてのハードウェアが表示されます。

デバイスの変更の表示

デバイスの変更を表示して、ハードウェアおよびソフトウェアの変更が行われたタイミングを把握できます。

ステップ 1 メインウィンドウで、[トラストインサイト (Trust Insights)] > [モニタ (Monitor)] > [デバイス (Devices)] の順にクリックします。

Crosswork Cloud Trust Insights では、以前に追加されたデバイスのリストが表示されます。詳細については、[デバイスの追加 \(173 ページ\)](#) を参照してください。

ステップ2 変更を表示するデバイスの名前をクリックします。

Crosswork Cloud Trust Insights では、デバイスに関する概要情報が表示されます。

ステップ3 [変更 (Changes)] タブをクリックします。

Tust Insights では、選択したデバイスの履歴タイムラインで観察されたイベントが強調表示されます。

ステップ4 デバイスの変更を表示するタイムフレームをクリックします。

ステップ5 [ハードウェア (Hardware)] をクリックすると、選択したタイムフレームのハードウェア変更の詳細が表示されます。

ステップ6 [ソフトウェア (Software)] をクリックすると、選択したタイムフレームのソフトウェア変更の詳細が表示されます。

ステップ7 [変更のみ (Changes Only)] をクリックすると、選択した期間の開始から終了までに変更された値のみが表示されます。

デバイスソフトウェアの変更の表示

Crosswork Cloud Trust Insights は、デバイスで行われたソフトウェアの変更を把握する方法を提供します。デバイスに加えられた特定のソフトウェアの変更を表示し、既知の適正な値 (KGV) と現在実行中のデバイスとの間にソフトウェアの不一致がある場所を観察できます。

ステップ1 メインウィンドウで、[トラストインサイト (Trust Insights)]>[モニタ (Monitor)]>[デバイス (Devices)] の順にクリックします。

Crosswork Cloud Trust Insights では、以前に追加されたデバイスのリストが表示されます。デバイスを追加するには、[デバイスの追加 \(173 ページ\)](#) を参照してください。

ステップ2 変更を表示するデバイスの名前をクリックします。

ステップ3 デフォルトでは、[トラストインサイト (Trust Insights)] タブが開きます。

ステップ4 [プラットフォーム (Platform)] タブで、グラフの下に表示される [パッケージ (Packages)] をクリックします。

Crosswork Cloud Trust Insights では、すべてのソフトウェアパッケージが一覧表示されます。

[パッケージの完全性 (Package Integrity)] 列には、Crosswork Cloud Trust Insights が次のいずれかの値を表示します。

- [変更の検出 (Changes detected)] : 適切なソフトウェアパッケージがインストールされましたが、インストール後に変更が行われたことを示します。
- [不一致 (Mismatch)] : インストールされているソフトウェアパッケージが、既知の適正な値 (KGV) と一致しないことを示します。
- [不一致と変更の検出 (Mismatch and changes detected)] : インストールされているソフトウェアパッケージが KGV と一致せず、インストール後に変更が行われたことを示します。

- [OK] : インストールされているソフトウェアパッケージが KGV と一致します。
- [未サポート (Not supported)] : ソフトウェアパッケージのフィンガープリントがドシエにありません。デバイスで使用可能な場合は、パッケージの完全性の測定をサポートする SMU をインストールする必要があります。

(注) Cisco IOS XR リリース 7.3.1 以降のリリースでは、パッケージのフィンガープリントがサポートされています。この機能は、各パッケージの既知の適正な値 (KGV) を使用して、インストール可能なパッケージの真正性を確認するのに役立ちます。インストールされ実行中のソフトウェアは、パッケージが正規品であるかどうかを判断するために KGV と比較されます。

- [KGVデータなし (No KGV data)] : パッケージのフィンガープリントが KGV にないため、Crosswork Cloud Trust Insights はソフトウェアパッケージを KGV と比較できません。Crosswork Cloud Trust Insights はパッケージを認識しません。

ステップ 5 [パッケージの完全性 (Package Integrity)] 列のリンクをクリックすると、デバイス上のソフトウェアファイルとパッケージに関する追加情報が表示されます。

Crosswork Cloud Trust Insights では、次の詳細情報を含むソフトウェアの完全性の分析が表示されます。

- [パッケージの署名分析 (Package Signature Analysis)] : パッケージの署名で検出された変更に関する詳細が表示されます。Crosswork Cloud Trust Insights はインストールされたパッケージを評価し、パッケージの署名が信頼できるかどうかを示す測定値を表示します。次のフィールドはパッケージ署名の変更を示し、いずれかのハッシュが一致しない場合はすぐに検証できます。
 - [既知の適正な値のハッシュ (Known Good Values Hash)] : シスコで指定された値、または以前に Crosswork Cloud Trust Insights で指定された値。
 - [パッケージインストールハッシュ (Package Install Hash)] : パッケージがインストールされた時点での値。
 - [パッケージランタイムハッシュ (Package Runtime Hash)] : ランタイム時のパッケージの値。
- [ファイル署名分析 (File Signature Analysis)] : ファイル署名で検出された変更に関する詳細が表示されます。不一致を含む各ファイルは、不一致に関する詳細とともに表示されます。ファイルに不一致がない場合、そのファイルはリストに表示されません。列に表示されるハッシュを表示して、不一致が発生した場所を確認できます。このデバイス上の不一致ファイルのリストをすばやく表示するには、[不一致ファイル (Mismatched Files)] タブをクリックします ([デバイスパッケージの一致しないファイルの表示 \(79 ページ\)](#) を参照)。

デバイスパッケージの一致しないファイルの表示

Crosswork Cloud Trust Insights を使用すると、特定のデバイスの一致しないパッケージファイルのリストをすばやく表示できます。不一致ファイルは、既知の適正な値 (KGV) とデバイスで現在動作しているものとの間のソフトウェアの不一致を示します。

ステップ 1 メインウィンドウで、[トラストインサイト (Trust Insights)] > [モニタ (Monitor)] > [デバイス (Devices)] の順にクリックします。

Crosswork Cloud Trust Insights では、以前に追加されたデバイスのリストが表示されます。デバイスを追加するには、[デバイスの追加 \(173 ページ\)](#) を参照してください。

ステップ 2 不一致ファイルを表示するデバイスの名前をクリックします。

ステップ 3 デフォルトでは、[トラストインサイト (Trust Insights)] タブが開きます。

ステップ 4 [プラットフォーム (Platform)] タブで、グラフの下に表示される [不一致ファイル (Mismatched Files)] をクリックします。

Crosswork Cloud Trust Insights では、そのデバイスで検出された不一致ファイルがすべて一覧表示されます。

[不一致ステータス (Mismatch Status)] 列には、Crosswork Cloud Trust Insights が次のいずれかの値を表示します。

- [ランタイム (Runtime)] : KGV 値がランタイム中のファイルの値と一致しません。
- [ディスク上 (OnDisk)] : KGV 値は、現在ディスクにあるファイルコンテンツのハッシュと一致しません。
- [ディスク上およびランタイム (OnDisk & Runtime)] : KGV 値は、ランタイム時のファイルの値およびパッケージのインストール時の値とは一致しません。
- [不明 (Unknown)] : Crosswork Cloud Trust Insights は KGV 値を特定できません。

ステップ 5 [不一致ステータス (Mismatch Status)] 列で、ステータス値をクリックします。

- a) [履歴 (History)] タブをクリックすると、ファイルの詳細が表示されます。列に表示されるハッシュを確認して、不一致が発生した場所をすばやく確認できます。
- b) [不一致のその他の場所 (Seen Elsewhere)] タブをクリックすると、この不一致ファイルもあるデバイスのリストが表示されます。

ファイル異常の表示



(注) 次の Cisco IOS XR バージョンを実行しているデバイスがサポートされています。

- 7.4.1
- 7.4.2
- 7.5.2

Cisco IOS XR デバイスの悪意のあるアクティビティまたは改ざんをモニタするために、特定のデバイスの不明なファイルのリストを表示できます。一般に、「予期しない」ファイルや、一般的な IOS XR ファイルから大幅に逸脱したファイルは、不明なファイルとしてフラグが付けられます。次に例を示します。

- 既知の KGV ファイル名と一致しないファイル。
- メタデータが変更されているが、SHAsum が同じままのファイル。
- 既知のハッシュを持つが、ファイル名またはパスが KGV と一致しないファイル。

ステップ 1 メインウィンドウで、[トラストインサイト (Trust Insights)] > [モニタ (Monitor)] > [デバイス (Devices)] の順にクリックします。

Crosswork Cloud Trust Insights では、以前に追加されたデバイスのリストが表示されます。デバイスを追加するには、[デバイスの追加 \(173 ページ\)](#) を参照してください。

ステップ 2 不明なファイルを表示するデバイスの名前をクリックします。

ステップ 3 デフォルトでは、[トラストインサイト (Trust Insights)] タブが開きます。

ステップ 4 [プラットフォーム (Platform)] タブで、グラフの下に表示される [不明なファイル (Unknown Files)] をクリックします。

Crosswork Cloud Trust Insights は、そのデバイスで検出されたすべての不明なファイルの詳細を一覧表示します。

デバイスの機能の表示

Crosswork Cloud Trust Insights では、デバイスをアップグレードすることで追加できる機能に関する詳細を表示できます。

ステップ 1 メインウィンドウで、[トラストインサイト (Trust Insights)]>[モニタ (Monitor)]>[デバイス (Devices)] の順にクリックします。

ステップ 2 機能を表示するデバイスの名前をクリックします。

ステップ 3 [機能 (Capabilities)] タブをクリックします。

デバイスが最新の場合、Crosswork Cloud Trust Insights では次のメッセージが表示されます。

現在のデバイス機能は最新です。

デバイスが最新でない場合、[アップグレード後 (After Upgrade)] ボタンが表示されます。

Crosswork Cloud Trust Insights では、機能のリストと、選択したデバイスで使用できない機能、使用可能な機能、アクティブな機能、インストールされている機能を示すキーが表示されます。

ステップ 4 [アップグレード後 (After Upgrade)] をクリックすると、デバイスのアップグレード後に使用できる追加機能が表示されます。



第 13 章

インターフェイスのモニタ

- ・ [インターフェイストラフィックの詳細の表示 \(83 ページ\)](#)

インターフェイストラフィックの詳細の表示

デバイスを追加すると、Crosswork Cloud Traffic Analysis はインターフェイスに関する情報を収集します。インターフェイスに関するトラフィックの詳細を表示できます。

ステップ 1 メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [モニタ (Monitor)] > [インターフェイス (Interfaces)] の順にクリックします。

ステップ 2 トラフィックの詳細を表示するインターフェイス名をクリックします。

Crosswork Cloud Traffic Analysis では、受信 (RX) および送信 (TX) のトラフィック情報が表示されます。



第 **IV** 部

Crosswork Cloud の設定

- [プレフィックスの設定 \(87 ページ\)](#)
- [ASN の設定 \(91 ページ\)](#)
- [ピアの設定 \(93 ページ\)](#)
- [ポリシーの設定 \(101 ページ\)](#)
- [通知エンドポイントの設定 \(109 ページ\)](#)
- [デバイスの設定 \(173 ページ\)](#)
- [Crosswork Data Gateways の設定 \(193 ページ\)](#)
- [複数の宛先への NetFlow トラフィックの送信 \(201 ページ\)](#)
- [クレデンシャルの設定 \(203 ページ\)](#)
- [デバイスグループの設定 \(205 ページ\)](#)
- [既知の適正なファイルの設定 \(207 ページ\)](#)
- [レポートの設定 \(211 ページ\)](#)



第 14 章

プレフィックスの設定

- [プレフィックスの追加 \(87 ページ\)](#)
- [プレフィックスの編集およびリンク解除 \(88 ページ\)](#)
- [プレフィックスの削除および登録解除 \(88 ページ\)](#)
- [プレフィックス通知の一時的な抑制 \(89 ページ\)](#)

プレフィックスの追加

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [プレフィックス (Prefixes)] の順にクリックします。

ステップ 2 [プレフィックスへの登録 (Subscribe to Prefixes)] をクリックします。

ステップ 3 次のいずれかのタブをクリックします。

- [手動 (Manual)] : 登録するプレフィックスの IP アドレスを入力します。複数のプレフィックスを追加するには、それぞれのプレフィックスの間にカンマ (,) を入力します。/8 より小さいプレフィックスマスクは追加できません。たとえば、1.1.0.0/3 などのプレフィックスは追加できません。
- [ASNルックアップ (ASNLookup)] : 関連付けられたプレフィックスを検索する ASN を入力します。
- [CSVの上書き (CSV Overwrite)] : プレフィックス情報を含む CSV ファイルをアップロードします。詳細については、[構成ファイルのアップロード \(251 ページ\)](#) を参照してください。

ステップ 4 [マニュアル (Manual)] または [ASNルックアップ (ASNLookup)] を選択した場合は、必要な情報を入力した後、[次へ (Next)] をクリックします。

ステップ 5 以前にポリシーを作成した場合は、[ポリシー (Policy)] ドロップダウンリストからプレフィックスに関連付けるポリシーを選択します。詳細については、[Crosswork Cloud Network Insights ポリシーの追加 \(101 ページ\)](#) を参照してください。

(注) プレフィックスは 1 つのポリシーにのみ関連付けることができます。

ステップ 6 (任意) [タグ (Tags)] フィールドに意味のあるテキストを入力します。

- (注) 複数のプレフィックスを入力した場合、Crosswork Cloud Network Insights は指定したポリシーとタグをすべてのプレフィックスに適用します。

ステップ7 変更内容を確認し、[送信 (Submit)] をクリックして変更を適用します。

プレフィックスの編集およびリンク解除

各プレフィックスに関連付けられたタグを追加または削除することで、プレフィックスを編集できます。ポリシーからプレフィックスを削除することもできます。

- ステップ1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [モニタ (Monitor)] > [プレフィックス (Prefixes)] の順にクリックします。
- ステップ2** 編集する1つ以上のプレフィックスの横にあるチェックボックスをオンにし、[編集 (Edit)] をクリックします。
- (注) 編集するプレフィックスを複数選択した場合、Crosswork Cloud Network Insights は選択したすべてのプレフィックスに変更を適用します。
- ステップ3** 変更内容を適用するには、[送信 (Submit)] をクリックします。
- ステップ4** ポリシーからプレフィックスを削除するには、1つ以上のプレフィックスの横にあるチェックボックスをオンにし、[リンク解除 (Unlink)] をクリックします。
- ステップ5** プレフィックスのリンクを解除することを確認し、[リンク解除 (Unlink)] をクリックします。
- (注) プレフィックスのリンク解除を行う場合、そのプレフィックスは Crosswork Cloud Network Insights のプレフィックスのリストに残り、編集もできますが、モニターすることはできません。または、プレフィックスの登録解除を行うことで、Crosswork Cloud Network Insights からプレフィックスを削除することもできます。詳細については、[プレフィックスの削除および登録解除 \(88 ページ\)](#) を参照してください。

プレフィックスの削除および登録解除

プレフィックスを削除する前に、現在の構成をエクスポートして保存することを推奨します。[構成ファイルのダウンロード \(252 ページ\)](#) を参照してください。

プレフィックスのリンク解除を行うことができます。これにより、プレフィックスのリストにプレフィックスが保持されますが、プレフィックスをモニタまたは編集することはできません。または、プレフィックスの登録解除を行って、プレフィックスを削除することもできます。次の手順では、プレフィックスの登録を解除する方法について説明します。

-
- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)]>[構成 (Configuration)]>[プレフィックス (Prefixes)]の順にクリックします。
- ステップ 2** 削除するプレフィックスの隣にあるチェックボックスをオンにし、[登録解除 (Unsubscribe)]をクリックします。
- ステップ 3** 確認ダイアログボックスで、[登録解除 (Unsubscribe)]をクリックします。
-

プレフィックス通知の一時的な抑制

一時停止プレフィックス機能は、リンクされたポリシー違反によってトリガーされるプレフィックスのアラーム通知を一時的に抑制します。たとえば、ネットワークのメンテナンス操作中にアラーム通知を受信しない方がよい場合です。登録を解除し、後でプレフィックスをポリシーにリンクするのではなく、プレフィックスを一定時間「一時停止」できます。

一時停止プレフィックス機能を有効にする場合は、次の動作に注意してください。

- 登録されたプレフィックスは、最大 90 日間一時停止できます。
- 関連するポリシーで違反が発生した場合、Crosswork Cloud Network Insights は一時停止されたプレフィックスのアラーム通知を送信しません。
- アラームは [アクティブ (Active)]アラームページに表示されません。ただし、アラームの [履歴 (History)]ページには引き続き表示されます。
- 次の条件が満たされると、Crosswork Cloud Network Insights はクリアされたアラーム通知を送信します。
 - アラームは、プレフィックスが一時停止される前にアクティブでした。
 - プレフィックスが一時停止中にアラームがクリアされました。



(注) Crosswork Cloud Network Insights は、プレフィックスが再開するまで、それ以降のアラーム通知を送信しません。

- プレフィックスの再開後：
 - 以前に抑制されたアラーム通知がプレフィックスが再開する前にクリアされた場合、Crosswork Cloud Network Insights はそのアラーム通知を送信しません。
 - 以前に抑制されたアクティブなアラーム通知がまだアクティブ状態である場合、Crosswork Cloud Network Insights はそのアラーム通知を送信します。

-
- ステップ1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ポリシー (Policies)] > [ポリシー名 (Policy-name)] の順にクリックしてから、[プレフィックス (Prefixes)] タブをクリックします。
 - ステップ2 一時的に通知を停止する 1 つ以上のプレフィックスの横にあるチェックボックスをオンにします。
 - ステップ3 [プレフィックスの一時停止 (Pause Prefix)] をクリックします。
 - ステップ4 [一時停止期間 (Pause Duration)] ドロップダウンリストから、このプレフィックスのアラーム通知を停止する時間範囲 (1 週間、1 ヶ月、2 ヶ月、または 3 ヶ月) を選択します。
 - ステップ5 [一時停止 (Pause)] をクリックします。プレフィックスのステータスには、[一時停止 (Paused)] とプレフィックスが再開されるタイミングが表示されます。プレフィックスの一時停止をキャンセルするには、プレフィックスの横にあるチェックボックスをオンにして、[プレフィックスの再開 (Resume Prefix)] をクリックします。
-



第 15 章

ASN の設定

- [監視する ASN を追加する \(91 ページ\)](#)

監視する ASN を追加する

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ASN (ASNs)] の順にクリックします。
- ステップ 2** [ASN のモニター (Monitor ASNs)] ボタンをクリックします。
- ステップ 3** [ASN (ASNs)] フィールドに、ASN を入力します。複数の ASN を追加するには、各 ASN の間にカンマ (,) を入力します。
- ステップ 4** [次へ (Next)] をクリックします。
- ステップ 5** 以前にポリシーを作成した場合は、[ポリシー (Policy)] ドロップダウンリストから ASN に関連付けるポリシーを選択します。詳細については、[ポリシーの設定 \(101 ページ\)](#) を参照してください。
- (注) ASN は 1 つのポリシーにのみ関連付けることができます。
- ステップ 6** (任意) [タグ (Tags)] フィールドに意味のあるテキストを入力します。
- (注) 複数の ASN を入力した場合は、Crosswork Cloud Network Insights は指定したポリシーとタグをすべての ASN に適用します。
- ステップ 7** 変更内容を確認し、[保存 (Save)] をクリックして変更を適用します。
-



第 16 章

ピアの設定

- [ピアのインポート \(93 ページ\)](#)
- [ピアの追加 \(94 ページ\)](#)
- [ピアの詳細の表示 \(94 ページ\)](#)
- [ピアデバイスの設定 \(97 ページ\)](#)
- [ピアの編集 \(98 ページ\)](#)
- [ピアの無効化 \(99 ページ\)](#)
- [ピアの削除 \(100 ページ\)](#)

ピアのインポート

組織でBGPmonの既存のピア構成が有効になっている場合は、BGPmonからピアをインポートできます。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。

ステップ 2 [Peermonのインポート (Peermon Import)] をクリックします。

ステップ 3 Peermon テーブルに各ピアに関連付けられた電子メールアドレスを入力し、[要求 (Request)] をクリックします。

Crosswork Cloud Network Insights は、入力したアドレスに確認メールを送信します。

ステップ 4 電子メールの承認リンクをクリックすると、BGPmon から Crosswork Cloud Network Insights にピア構成がインポートされます。

クリックする前に確認メールの期限が切れた場合は、[インポートの再起動 (Restart Import)] をクリックすることで、確認メールを再送信できます。

承認リンクをクリックすると、Crosswork Cloud Network Insights はピアをBGPmonから転送し、ピア情報を正常にインポートした後にメッセージを表示します。インポートされたピアが[ピア (Peers)]メニューに表示されます。

ピアの追加

これは、Crosswork Cloud にピアを追加する際の最初の手順です。

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。
- ステップ 2** [ピアの追加 (Add Peer)] をクリックします。
- ステップ 3** 次の表に示すフィールドに入力します。

フィールド	説明
IP	ピアの IP アドレス。
名前 (Name)	ピアの一意の名前。ピア名は、他のピアのいずれとも一致してはなりません。
ASN	ピアが属する ASN。
市区町村郡 (City)	ピアが位置している市区町村。
国 (Country)	ピアが位置している国。
連絡先の電子メール (Contact Email)	ピアの連絡先電子メールアドレス。
説明 (Description)	ピアの説明。
ポリシー (Policy)	ピアに関連付けるポリシーを選択します。
タグ (Tags)	(任意) ピアに適用する意味のあるテキストを入力します。

- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** シスコのルートサーバと ASN の詳細を取得します。詳細については、[ピアの詳細の表示 \(94 ページ\)](#) を参照してください。
- ステップ 6** ピアデバイスを設定します。詳細については、[ピアデバイスの設定 \(97 ページ\)](#) を参照してください。

ピアの詳細の表示

特定のピアに関する詳細情報を表示できます。また、ピアデバイスの設定に必要なシスコのルートサーバおよび ASN 情報を取得することもできます ([ピアデバイスの設定 \(97 ページ\)](#) を参照)。

ステップ 1 メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。

ステップ 2 特定のピアに関する詳細を表示するには、そのピアの IP アドレスをクリックします。Crosswork Cloud Network Insights では、次の表に示すように、ピアに関する詳細が表示されます。

(注) このページから、対応するボタンをクリックして、このピアを [ピアの編集](#)、[ピアの無効化](#)、または [ピアの削除](#) することもできます。

表 21: 概要

フィールド	説明
リンクされたポリシー (Linked Policy)	プレフィックスに関連付けられたポリシー。
更新された統計 (Stats Updated)	統計情報が前回更新された時間。
[確立/ドロップされたセッション (Sessions Established/Dropped)]	ルートサーバのピアと自身のピアの間の BGP セッションが確立/ドロップされた回数。
[最後のリセット (Last Reset)]	セッションが最後にリセットされた時刻。
最後のリセットの理由	BGP セッションがリセットされた理由。
最後のアクティブなアラーム (Last Active Alarm)	ピアに関連付けられた最後のアクティブなアラーム。アラームをクリックすると、詳細が表示されます。最後のアクティブなアラームのリストを表示するには、[すべて表示 (View All)] をクリックします。
[このピア (This Peer)]	ピアに関する情報が表示されます。
BGPセッション (BGP Session)	現在の BGP セッションの情報を表示します。
[ルートサーバとASN (Route Server and ASN)]	確立された、または確立しようとしている BGP セッションがピアにあるルートサーバのピアルータに関する情報。この情報は、ピアデバイスを設定するために必要です。詳細については、 ピアデバイスの設定 (97 ページ) を参照してください。
Number of Prefixes	ピアで受け入れられるプレフィックスの平均数を表示する 7 日間のタイムライン。

表 22: アラーム

フィールド	説明
アラームの状態 (Alarm state)	次のアラームの状態のいずれかをクリックします。 <ul style="list-style-type: none"> [アクティブ (Active)] : Crosswork Cloud Network Insights では、優先度順にソートされたすべてのアクティブなアラームのリストが表示されます。 [確認済み (Acknowledged)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべての確認済みアラームのリストが表示されます。
表示 (View)	[表示 (View)] をクリックすると、アラームに関する詳細が表示されます。
ルール (Rule)	違反したルール。
シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
アクティブ化 (Activated)	アラームの発生時刻。

表 23: [BGP更新 (BGP Updates)]

フィールド	説明
タイムフレーム	[タイムフレーム (Timeframe)] ドロップダウンリストから値を選択して、タイムフレームを指定します。
アドバタイズメント/取り消し	タイムフレーム中に確認されたアドバタイズメントと取り消しの合計数。
プレフィックス (Prefix)	BGP 更新の受信元になっているプレフィックス IP アドレス。
発信元ASN (Origin ASN)	発信元であることが確認されたASN。
AS パス (AS Path)	AS ルーティングパス。
コミュニティ (Communities)	コミュニティのパス属性 (該当する場合) 。
更新のタイプ (Update Type)	BGP 更新のタイプ。
最終変更日 (Last Modified)	前回の BGP 更新の日時。

ピアデバイスの設定

次のテンプレートを使用して、ピアデバイスに構成を適用できます。

Cisco IOS XE

```
router bgp <asn>
  bgp router-id <router-id>
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor <route-server-ipv4> remote-as 65179
  neighbor <route-server-ipv4> description Cisco CrossWork Route Server IPv4
  neighbor <route-server-ipv4> ebgp-multihop 255
  neighbor <route-server-ipv4> update-source <src-interface>
  !
  neighbor <route-server-ipv6> remote-as 65179
  neighbor <route-server-ipv6> description Cisco CrossWork Route Server IPv6
  neighbor <route-server-ipv6> ebgp-multihop 255
  neighbor <route-server-ipv6> update-source <src-interface>
  !
  address-family ipv4
    neighbor 172.31.20.53 activate
    neighbor 172.31.20.53 send-community both
    neighbor 172.31.20.53 filter-list 2 in
    neighbor 172.31.20.53 filter-list 1 out
  exit-address-family
  !
  address-family ipv6
    neighbor 172.31.20.53 activate
    neighbor 172.31.20.53 send-community both
    neighbor 172.31.20.53 filter-list 2 in
    neighbor 172.31.20.53 filter-list 1 out
  exit-address-family
  !
  ip as-path access-list 1 permit .*
  ip as-path access-list 2 deny .*
```

ここで

- <asn> は、ネットワークの BGP AS 番号です。
- <router-id> は、ネットワークの BPG ルータ ID です。
- <src-interface> は、ネットワークの BGP 送信元インターフェイスです。

次の IPv4/IPv6 情報は、UI を使用してピアが追加された後に生成されます。詳細については、[ピアの追加 \(94 ページ\)](#) および [ピアの詳細の表示 \(94 ページ\)](#) を参照してください。

- <route-server-ipv4> は、シスコのルートサーバの IPv4 アドレスです。
- <route-server-ipv6> は、シスコのルートサーバの IPv6 アドレスです。

Cisco IOS XR

```

router bgp <asn>
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
  !
  neighbor <route-server-ipv4>
    remote-as 65179
    bgp router-id <router-id>
    ebgp-multihop 255
    description Cisco CrossWork Route Server IPv4
    update-source <src-interface>
    address-family ipv4 unicast
    route-policy DROP in
    route-policy PASS out
  !
  !
  neighbor <route-server-ipv6>
    remote-as 65179
    ebgp-multihop 255
    description Cisco CrossWork Route Server IPv6
    update-source <src-interface>
    address-family ipv6 unicast
    route-policy DROP in
    route-policy PASS out
  !
route-policy PASS
  pass
end-policy
!
route-policy DROP
  drop
end-policy
!

```

ここで

- *<asn>* は、ネットワークの BGP AS 番号です。
- *<router-id>* は、ネットワークの BPG ルータ ID です。
- *<src-interface>* は、ネットワークの BGP 送信元インターフェイスです。

次の IPv4/IPv6 情報は、UI を使用してピアが追加された後に生成されます。詳細については、[ピアの追加 \(94 ページ\)](#) および [ピアの詳細の表示 \(94 ページ\)](#) を参照してください。

- *<route-server-ipv4>* は、シスコのルートサーバの IPv4 アドレスです。
- *<route-server-ipv6>* は、シスコのルートサーバの IPv6 アドレスです。

ピアの編集

以前に追加またはインポートしたピアを編集できます。

-
- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。
- ステップ 2** 1 つのピアを編集するには、ピアの IP アドレスをクリックしてから、[編集 (Edit)] をクリックします。
単一のピアを編集する場合、ピアの名前、市区町村、国、連絡先、説明、ポリシー、タグを変更できます。
- ステップ 3** フィールドを変更し、[保存 (Save)] をクリックします。
- ステップ 4** ピアグループを変更して同じ変更を適用するには、編集する各ピアの横にあるチェックボックスをオンにして、[編集 (Edit)] をクリックします。
複数のピアを編集する場合、ピアに割り当てられているポリシーとタグを変更し、すべてのピアを非アクティブ化またはアクティブ化できます。
- ステップ 5** フィールドのいずれかを変更し、[送信 (Submit)] をクリックします。
-

ピアの無効化

ピアを無効にすると、Crosswork Cloud Network Insights はピアからの情報収集を一時的に停止し、Crosswork Cloud Network Insights のルートサーバーとピアルータ間の BGP セッションを終了します。Crosswork Cloud Network Insights は、ピア構成をデータベースに保持しますが、ピアの統計情報 (BGP セッションステータス、IPv4 と IPv6 プレフィックスの数など) は破棄します。

後でピアを有効にして、データ収集を再開できます。

または、ピアを削除して、Crosswork Cloud Network Insights から削除することもできます。ピアを削除した後は、そのデータを回復できません。[ピアの削除 \(100ページ\)](#) を参照してください。

-
- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。
- ステップ 2** 非アクティブにするピアの IP アドレスをクリックします。
- ステップ 3** [無効 (Disable)] をクリックします。
ピアが無効にされたことを示すメッセージが表示されます。
無効になっているピアを有効にすることができます。ピアを再び有効にすると、Crosswork Cloud Network Insights は保存されたピア構成を使用し、ピアルータと Crosswork Cloud Network Insights のルートサーバー間で BGP ピアリングセッションが再開されます。ピアを有効にした後、ピアの詳細ページに統計情報が表示されるまでに最大 30 分かかる場合があります。
- ステップ 4** ピアのデータ収集を再開するには、[有効 (Enable)] をクリックします。

ピアが有効になったことを示すメッセージが表示され、Crosswork Cloud Network Insights はピアのデータ収集を再開します。

ピアの削除

ピアを削除すると、すべてのピアデータが Crosswork Cloud Network Insights から削除されます。Crosswork Cloud Network Insights は、そのルートサーバーから BGP ピア構成を削除し、Crosswork Cloud Network Insights とピアルータ間の BGP セッションを終了します。

ピアに関連付けられたすべてのピアデータは破棄され、回復できません。削除されたピアを再アクティブ化することはできません。

または、ピアを無効にすることもできます。この場合、Crosswork Cloud Network Insights がピアからの情報収集を一時的に停止します。[ピアの無効化 \(99 ページ\)](#) を参照してください。

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [ピア (Peers)] の順にクリックします。
 - ステップ 2** 削除するピアの隣にあるチェックボックスをオンにするか、IP アドレスをクリックし、[削除 (Remove)] をクリックします。
 - ステップ 3** [削除 (Remove)] をクリックすることで、ピアの削除が確定します。
ピアとその以前に収集されたデータが Crosswork Cloud Network Insights から削除されます。
-



第 17 章



ポリシーの設定

- [ポリシーの概要](#) (101 ページ)
- [Crosswork Cloud Network Insights ポリシー](#) (101 ページ)
- [Crosswork Cloud Traffic Analysis ポリシー](#) (106 ページ)

ポリシーの概要

ポリシーとアラームは、予期しない動作を警告することができます。これは、考えられる設定ミス、悪意のあるルーティングアクティビティ、およびネットワーク使用率の問題を特定するのに役立ちます。ポリシーを使用することで、ネットワーク動作（ルーティングの正常性、使用率など）がモニターできます。ポリシーを作成するには、しきい値を指定して一連のルールを定義します。ルール違反が発生し、しきい値を超えた場合、Crosswork Cloud は多数の[通知エンドポイント](#)について送信できる[アラーム](#)についてをアクティブにします。

メインウィンドウで、次のいずれかの Crosswork Cloud アプリケーションに移動して、ポリシーを作成、変更、または表示します。

- Crosswork Cloud Traffic Analysis— > [設定 (Configure)] > [ポリシー (Policies)]
- Crosswork Cloud Network Insights— > [設定 (Configure)] > [ポリシー (Policies)]

Crosswork Cloud Network Insights ポリシー

Crosswork Cloud Network Insights ポリシーの追加



(注) 場合によっては、新しいポリシーを作成するのではなく、既存のポリシーを複製し、わずかな変更を加えたほうが効率的なこともあります。詳細については、[Crosswork Cloud Network Insights ポリシーの管理](#) (104 ページ) を参照してください。


- ステップ1** メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ3** 次のいずれかのポリシータイプをクリックします。 [アラームタイプ \(346 ページ\)](#)
- [ASNポリシー (ASN Policy)]
 - [プレフィックスポリシー (Prefix Policy)]
 - [ピアポリシー (Peer Policy)]
- ステップ4** [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ5** ポリシー内のルールに違反したときに通知を受信する通知エンドポイントを追加するには、[エンドポイントの追加 (Add Endpoint)] をクリックします。
- ステップ6** プレフィックスポリシーの作成を選択した場合は、[想定されるASパスエディタ (Expected AS Path Editor)] セクションで、次のフィールドに値を入力します。
- [発信元ASN (Origin ASNs)] : プレフィックスがアドバタイズされるルートである ASN 発信元。
 - [アップストリームASN (Upstream ASNs)] : 1 ホップ前の ASN。
 - [設定 (Configure)] をクリックして、有効な AS パスのパターンを入力します。Crosswork Cloud Network Insights は、指定された ASN のパターン (想定される AS 番号のシーケンスの順序) と、アドバタイズされたプレフィックスの AS パスを比較し、一致しない場合に検出します。
- ステップ7** [ルール (Rules)] セクションで、[ルールの追加 (Add Rule)] をクリックし、ポリシーに適用する 1 つ以上のルールを選択します。アラームの詳細については、[アラームの説明 \(23 ページ\)](#) を参照してください。
- a) (プレフィックスポリシーの場合のみ) 特定の Crosswork Cloud サブスクリプションでは、[すべてのピア (All Peers)] と [マイピア (My Peers)] の 2 つのプレフィックス ポリシー ルール カテゴリを使用できます。[サブスクリプションプランのオプションの表示 \(273 ページ\)](#) [マイピア (My Peers)] ルールはピアからの 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 \(94 ページ\)](#)
- プレフィックスポリシーに含めるすべてのルールをオンにし、[保存 (Save)] をクリックします。

図 2: プレフィックス ポリシー ルール : [すべてのピア (All Peers)] および [マイピア (My Peers)]

Add Policy Prefix Rules
Select rules to activate for this policy

All Peers	My Peers
<input type="checkbox"/> AS Origin Violation	<input type="checkbox"/> AS Origin Violation - My Peers
<input type="checkbox"/> AS Path Length Violation	<input type="checkbox"/> AS Path Length Violation - My Peers
<input type="checkbox"/> New AS Path Edge	<input type="checkbox"/> Parent Aggregate Change - My Peers
<input type="checkbox"/> Parent Aggregate Change	<input type="checkbox"/> Prefix Advertisement - My Peers
<input type="checkbox"/> Prefix Advertisement	<input type="checkbox"/> Prefix Withdrawal - My Peers
<input type="checkbox"/> Prefix Withdrawal	<input type="checkbox"/> Upstream AS Change - My Peers
<input type="checkbox"/> ROA Expiry	<input type="checkbox"/> Valid AS Path Violation - My Peers
<input type="checkbox"/> ROA Failure	
<input type="checkbox"/> ROA Not Found	
<input type="checkbox"/> Subprefix Advertisement	
<input type="checkbox"/> Upstream AS Change	
<input type="checkbox"/> Valid AS Path Violation	

ステップ 8 ルールごとに、次を指定します。

- ルールが [有効 (Enabled)] (デフォルト) か [無効 (Disabled)] かを指定します。
- [解決するピア (Peers to Resolve)] : アラームを消す前に特定のイベントを検出する必要がある一意のピアの数を入力します。
- [トリガーするピア (Peers to Trigger)] : アラームをトリガーする前に特定のイベントを検出する必要がある一意のピアの数を入力します。
- [シビラティ (重大度) (Severity)] : アラームのシビラティ (重大度) レベルを選択します。

ステップ 9 [エンドポイント (Endpoints)] セクションで、[エンドポイントの追加 (Add Endpoint)] をクリックします。

ステップ 10 [エンドポイントタイプ (Endpoint Type)] ドロップダウンリストからエンドポイントタイプを選択します。

ステップ 11 [エンドポイント (Endpoint)] フィールドをクリックしてから、既存のエンドポイントを選択するか、[エンドポイントの追加 (Add Endpoint)] をクリックして、必要なフィールドに入力します。


エンドポイントはいつでも設定できます。詳細については、[通知エンドポイントの設定 \(109ページ\)](#) を参照してください。

ステップ 12 [メモ (Notes)] フィールドに、必要なメモを入力します。

ステップ 13 [保存 (Save)] をクリックします。

Crosswork Cloud Network Insights ポリシーの管理

ポリシーを表示、変更、または複製するには、次の手順を実行します。

ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。

ステップ 2 複製や管理をする、またはさらに詳細を表示するポリシーの名前をクリックします。Crosswork Cloud Network Insights では、次の表に示すように、ポリシーに関する詳細が表示されます。

表 24: ポリシーの詳細のフィールドに関する説明

タブ	フィールド	説明
概要 [概要 (Overview)] タブには、指定したポリシーに関する詳細が含まれています。	[想定される発信元ASN (Expected Origin ASNs)]	ポリシーの作成時に指定した ASN 発信元は、Crosswork Cloud Network Insights が想定します。
	[想定されるアップストリームASN (Expected Upstream ASNs)]	ポリシーの作成時に指定したアップストリーム ASN。
	[有効な AS パスのパターン (Valid AS Path Pattern)]	ポリシーの作成時に指定した有効な AS パスのパターン。
	ルール	ポリシー内のルールのリスト。Crosswork Cloud Network Insights では、各ルールのアクティブなアラームの数など、各ルールに関する詳細が表示されます。ルールの特定のアラームを表示するには、いずれかのルールで[アクティブなアラーム (Active Alarms)] をクリックします。
プレフィックス (Prefixes) [プレフィックス (Prefixes)] タブには、ポリシーに関連付けられたプレフィックスに関する詳細が含まれています。	プレフィックス (Prefix)	プレフィックス IP アドレスが一覧表示されます。プレフィックスの詳細を表示するには、IP アドレスをクリックします。詳細については、 プレフィックスの詳細の表示 (61 ページ) を参照してください。 追加のプレフィックスをポリシーにリンクするには、[プレフィックスのリンク (Link Prefixes)] をクリックします。
	タグ	プレフィックスに関連付けられたタグが一覧表示されます。

タブ	フィールド	説明
アラーム [アラーム (Alarms)] タブには、関連付けられたアラームに関する詳細が含まれています。	アラームの状態 (Alarm state)	次のアラームの状態のいずれかをクリックします。 <ul style="list-style-type: none"> • [アクティブ (Active)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべてのアクティブなアラームのリストが表示されます。 • [確認済み (Acknowledged)] : Crosswork Cloud Network Insights では、優先順位でソートされたすべての確認済みアラームのリストが表示されます。 • [履歴 (History)] : Crosswork Cloud Network Insights では、[タイムフレーム (Timeframe)] ドロップダウンリストから時間範囲を指定できる履歴アラームのリストが表示されます。 アラームを確認またはスヌーズするには、アラームの横にあるチェックボックスをオンにして、[確認 (Acknowledge)] または [スヌーズ (Snooze)] をクリックします。
	アラームの詳細 (Alarm Details)	アラームの詳細。
	トリガー	アラームをトリガーしたプレフィックスまたは ASN。
	ルール (Rule)	違反したルール。
	# ピア (# Peers)	違反をレポートしたピアの数。
	シビラティ (重大度) (Severity)	設定されたアラームのシビラティ (重大度) レベル。
	アクティブ化 (Activated)	アラームの発生時刻。
	注記 (Notes)	ユーザが入力したメモ。

ステップ 3 ポリシーを変更するには、[編集 (Edit)] をクリックします。

- a) 必要に応じて、通知エンドポイント、発信元およびアップストリーム ASN、AS パスパターン、およびルールを更新します。
- b) [保存 (Save)] をクリックします。

ステップ 4 ポリシーを削除するには、[削除 (Remove)] をクリックします。削除を確認するために、再度 [削除 (Remove)] をクリックします。

ステップ 5 既存のポリシーをコピーするには、[複製 (Duplicate)] をクリックします。

- a) デフォルトでは、新しいポリシーの名前は [コピー (Copy of)] で始まり、その後に複製されたポリシーの名前が続きます。
- b) 必要な変更を加えて、[保存 (Save)] をクリックします。

Crosswork Cloud Traffic Analysis ポリシー

Crosswork Cloud Traffic Analysis ポリシーの追加


Crosswork Cloud Traffic Analysis は、次の 2 つのポリシーを自動的に作成します。

- [ゲートウェイ接続 \(36 ページ\)](#) : Crosswork Cloud への Crosswork Data Gateway の接続をモニターします。
- [デバイスの接続性 \(37 ページ\)](#) : Crosswork Data Gateway へのデバイスの接続をモニターします。

TX、RX、およびジャンボプレフィックスの使用率をモニターする追加のポリシーを作成するには、次の手順を実行します。



- (注) 場合によっては、新しいポリシーを作成するのではなく、既存のポリシーを複製し、わずかな変更を加えたほうが効率的なこともあります。詳細については、[Crosswork Cloud Traffic Analysis ポリシーの管理 \(107 ページ\)](#) を参照してください。

ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。

ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。

ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。

ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。

ステップ 5 作成するインターフェイスポリシーを確認します。

- **[インターフェイス TX 使用率 (Interface TX Utilization)]** : 送信トラフィック情報をモニターします。

- [インターフェイス RX 使用率 (Interface RX Utilization)]: 受信トラフィック情報をモニターします。
- [プレフィックス使用率 (Prefix Utilization)]: ジャンボプレフィックスの使用率をモニターします。

- ステップ 6** ルールごとに、スライダを動かして、アラームをトリガーする使用率の範囲と重要度レベルを指定します。
- ステップ 7** [Next] をクリックします。
- ステップ 8** [データ (Data)] で、[追加 (Add)] をクリックして、モニターするインターフェイスを選択します。
- ステップ 9** [モニターするインターフェイスの選択 (Select Interfaces to Monitor)] ページに表示される指示に従い、[追加 (Add)] をクリックします。
- ステップ 10** [アクション (Actions)] で、(ルールがトリガーされた後に) 送信するすべての通知タイプが設定されるまで、[通知の追加 (Add Notification)] をクリックします。
- ステップ 11** [保存 (Save)] をクリックします。

Crosswork Cloud Traffic Analysis ポリシーの管理

ポリシーを表示、変更、または複製するには、次の手順を実行します。


- ステップ 1** メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2** ゲートウェイ接続ポリシーまたはデバイス接続ポリシーを変更するには、それぞれのウィンドウで [詳細 (Details)] をクリックします。詳細については、「[ゲートウェイ接続 \(36 ページ\)](#)」および「[デバイスの接続性 \(37 ページ\)](#)」を参照してください。
- ステップ 3** ユーザーが作成したポリシーを複製、管理、または表示するには、ポリシー名をクリックします。Crosswork Cloud Traffic Analysis では、次の表に示すように、ポリシーに関する詳細が表示されます。

表 25: ポリシーの詳細のフィールドに関する説明

タブ	フィールド	説明
概要 [概要 (Overview)] タブには、指定したポリシーに関する詳細が含まれています。	Triggers	このポリシーに設定されているインターフェイスのルールを表示します。
	データ	このポリシーのモニター対象インターフェイスを表示します。
	アクション (Actions)	このポリシーに設定されているエンドポイント通知を表示します。

タブ	フィールド	説明
アラーム [アラーム (Alarms)]タブには、ポリシーに関連付けられたアラームに関する詳細が含まれています。	[アラーム (Alarms)]の状態タブ	次のアラームの状態のいずれかをクリックします。 <ul style="list-style-type: none"> • [アクティブ (Active)]: 優先順位でソートされたすべてのアクティブなアラームのリストが表示されます。 • [確認済み (Acknowledged)]: 優先順位でソートされたすべての確認済みアラームのリストが表示されます。 • [履歴 (History)]: [タイムフレーム (Timeframe)]ドロップダウンリストから時間範囲を指定できる履歴アラームのリストが表示されます。 アラームを確認またはスヌーズするには、アラームの横にあるチェックボックスをオンにして、[確認 (Acknowledge)]または[スヌーズ (Snooze)]をクリックします。

ステップ 4 ポリシーを変更するには、[編集 (Edit)]をクリックします。

- 必要に応じて、インターフェイスルール、モニター対象インターフェイス、および設定されたエンドポイント通知を更新します。
- [保存 (Save)]をクリックします。

ステップ 5 ポリシーを削除するには、[削除 (Remove)]をクリックします。削除を確認するために、再度[削除 (Remove)]をクリックします。

ステップ 6 既存のポリシーをコピーするには、[複製 (Duplicate)]をクリックします。

- デフォルトでは、新しいポリシーの名前は[コピー (Copy of)]で始まり、その後に複製されたポリシーの名前が続きます。
- [編集 (Edit)]をクリックして必要な変更を行ったら、[保存 (Save)]をクリックします。



第 18 章

通知エンドポイントの設定

- [通知エンドポイントについて \(109 ページ\)](#)
- [通知エンドポイントの設定 \(110 ページ\)](#)
- [エンドポイントの確認コードの再送信 \(113 ページ\)](#)
- [通知メッセージの例 \(113 ページ\)](#)

通知エンドポイントについて

ポリシーの作成中に、ポリシー内のルールに違反した場合にアラーム通知を受信する複数のエンドポイントを設定できます。

次の通知エンドポイントタイプを使用できます。

- E メール
- Google ストレージ
- Amazon S3
- SMS
- Slack
- WebEx
- Microsoft Teams
- PagerDuty

エンドポイント通知の内容

アラーム通知情報の内容と配信は、エンドポイントの通知タイプによって異なります。通知メッセージに含まれる情報のタイプは、Raw データまたは要約データに分類されます。

生データ (Raw Data)

Amazon S3 と Google ストレージの通知エンドポイントの場合、情報は未加工の形式で一連の JSON (JavaScript Object Notation) オブジェクトとして提供されます。JSON オブジェクトは、システムに表示されるアラーム通知イベントを表します。これらのイベントは、現在の時間枠

(現在の 1 分間など) に対応するオブジェクトとして、設定された S3 とクラウドストレージのバケットに書き込まれます。指定した時間帯に配信されたイベントがない場合、JSON オブジェクトは書き込まれません。[アラームタイプ別 Amazon S3 と Google ストレージのエンドポイント通知の例 \(115 ページ\)](#) の例を参考にしてください。

要約データ


メッセージには、一定期間に発生したイベントの要約が含まれます。通常、メッセージには、アラーム遷移イベントの総数、最初のいくつかのイベントからの特定のアラームの詳細、およびその他のイベントを表示するためのリンクが含まれます。表示される正確な形式とアラームの詳細は、エンドポイントタイプと、対応するメッセージサイズの制約によって異なります (たとえば、SMS エンドポイントでは総数を表示するスペースしかないため、特定のアラームの詳細は含まれません)。

エラー処理

エンドポイントが通知の受信に失敗した場合は、成功するか、通知がシステムに存在しなくなるまで、Crosswork Cloud は通知の配信を試みます。後者の場合、通知エンドポイントは配信されません。

通知エンドポイントの設定

ポリシー内のルールに違反した場合に通知を受信するエンドポイントを設定できます。ポリシーを作成するときに、ポリシーに含まれる各ルールのエンドポイントを指定できます。エンドポイントはいつでも設定できます。これにより、次の手順で説明するように、選択可能なエンドポイントのリストが作成されます。

ステップ 1 メインウィンドウで、 > [グローバル (Global)] > [通知 (Notifications)] をクリックします。

ステップ 2 ページ上部のオプションのいずれかをクリックして、作成するエンドポイントのタイプを選択します。

- E メール
- Google ストレージ (「[Google ストレージエンドポイントの設定 \(111 ページ\)](#)」を参照)
- Amazon S3
- Slack
- SMS
- WebEx (「[Webex エンドポイントの設定 \(112 ページ\)](#)」を参照)
- Microsoft Teams
- PagerDuty

(注) [通知メッセージの例 \(113 ページ\)](#) も参照してください。

ステップ 3 [typeのエンドポイントの追加 (Add type Endpoint)] をクリックします。

ステップ4 エンドポイントの名前を入力します。

ステップ5 エンドポイントが [有効 (Enabled)] (デフォルト) か [無効 (Disabled)] かを選択します。

ステップ6 ステップ2 で選択したエンドポイントタイプに必要な情報を入力します。

ステップ7 (任意) メモを入力します。

ステップ8 [保存 (Save)] をクリックします。

ステップ9 Crosswork Cloud から確認コードを受信したら、[確認コード (Verification Code)] フィールドにコードを入力し、[確認 (Verify)] をクリックします。


[今はスキップ (Skip for Now)] を選択すると、Crosswork Cloud はエンドポイントが作成しますが、確認コードを入力してエンドポイントを確認するまで、エンドポイントに通知は送信されません。

Google ストレージエンドポイントの設定

Crosswork Cloud を設定して、通知ログを Google Cloud Storage に送信するようにすることもできます。

始める前に

- Google Cloud Storage アカウントと、すべてのアラーム通知情報の送信先となる既存の [Cloud Storage バケット](#) が必要です。
- Google Cloud Storage バケットに対する Crosswork Cloud のアクセスを許可するには、[サービスアカウントキー](#) ファイル (JSON 形式) を作成してください。このファイルは、Google ストレージの通知エンドポイント設定の一部としてアップロードする必要があります。

ステップ1 Crosswork Cloud で、 > [グローバル (Global)] > [通知 (Notifications)] > [Google ストレージ (Google Storage)] タブの順にクリックし、[Google ストレージエンドポイントの追加 (Add Google Storage Endpoint)] をクリックします。

ステップ2 次の手順を実行します。

- a) 通知の名前を入力します。
- b) オプションを [有効 (ENABLED)] に切り替えます。
- c) Google Cloud Storage バケットの名前を入力します。
- d) 通知ログを保存するバケット内に特定のフォルダがある場合は、パスを入力します。
- e) Google Cloud Storage へのアクセスを可能にする JSON キーファイルをアップロードします。

ステップ3 [保存 (Save)] をクリックします。

Google Cloud Storage バケット内のファイルの場所とプロパティの例 :

Webex エンドポイントの設定

Buckets > gcp-stor-staging > notifications_bdd92688-659b-462e-8ce0-ee31df2b49fa_ [複製]

LIVE OBJECT VERSION HISTORY

[DOWNLOAD](#) [EDIT METADATA](#) [EDIT ACCESS](#) [DELETE](#)

Overview	
Type	text/plain; charset=utf-8
Size	73 KB
Created	Jun 30, 2023, 12:32:15 PM
Last modified	Jun 30, 2023, 12:32:15 PM
Storage class	Standard
Custom time	—
Public URL ?	Not applicable
Authenticated URL ?	https://storage.cloud.google.com/gcp-stor-staging/notifications_bdd92688-659b-462e-8ce0-ee31df2b49fa_ [複製]
gsutil URI ?	gs://gcp-stor-staging/notifications_bdd92688-659b-462e-8ce0-ee31df2b49fa_ [複製]
Permissions	
Public access	Not public
Protection	
Version history ?	—
Retention policy	None
Hold status	None ✎
Encryption type	Google-managed

(注) ログファイルの内容の例については、[アラームタイプ別 Amazon S3 と Google ストレージのエンドポイント通知の例 \(115 ページ\)](#) を参照してください。


Webex エンドポイントの設定

Webex スペースに通知を送信するように、Crosswork Cloud を設定できます。この手順では、ウェブフックを作成し、UI で通知エンドポイントを設定する方法について説明します。

始める前に

apphub.webex.com アカウントを持ち、ウェブフックを作成する Webex スペース (ルーム) のメンバーである必要があります。

- ステップ 1 <https://apphub.webex.com> にログインします。
- ステップ 2 [着信ウェブフック (Incoming Webhooks)] を検索します。[着信ウェブフック (Incoming Webhooks)] アプリケーションが一覧表示されます。
- ステップ 3 [着信ウェブフック (Incoming Webhooks)] アプリケーションをクリックします。
- ステップ 4 [着信ウェブフック (Incoming Webhooks)] ページで、[接続 (Connect)] をクリックします。
- ステップ 5 複数の項目に対する権限を要求するウィンドウが表示され、同意する場合は、[同意 (Accept)] をクリックします。
- ステップ 6 ページを下にスクロールし、表示されたスペースに新しいウェブフック名を入力し、ドロップダウンリストから Webex スペースを選択します。

- ステップ 7** [追加 (Add)] をクリックします。[ウェブフック URL (Webhook URL)] フィールドに値が入力されます。
- ステップ 8** 後で使用するために、新しく作成したウェブフック URL をコピーします。
- ステップ 9** Crosswork Cloudで、 > [グローバル (Global)] > [通知 (Notifications)] をクリックします。
- ステップ 10** [Webex] を選択し、[Webexエンドポイントの作成 (Create Webex Endpoint)] をクリックします。
- ステップ 11** エンドポイントの名前を入力します。
- ステップ 12** [ウェブフック URL (Webhook URL)] フィールドに、前にコピーしたウェブフック URL を貼り付けます。
- ```
https://webexapis.com/v1/webhooks/incoming/<new_webhook_ID>
```
- ステップ 13** [保存 (Save)] をクリックします。
- 新しいエンドポイントを設定したことを示す通知を Webex スペースで受信します。
- ステップ 14** エンドポイントを確認すると、エンドポイントがアクティブ状態に変わり、新しい通知を処理します。

---

## エンドポイントの確認コードの再送信

Crosswork Cloud Network Insights からの通知を受信するようにエンドポイントを設定したら、最初に確認コードを入力してエンドポイントを確認する必要があります。次の手順に従って、確認コードを再送信できます。

- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [通知エンドポイント (Notification Endpoints)] の順にクリックします。
- ステップ 2** 以前に入力したエンドポイントの名前をクリックします。
- ステップ 3** [確認 (Verify)] をクリックします。
- Crosswork Cloud Network Insights が確認コードを再送信します。
- ステップ 4** Crosswork Cloud Network Insights から確認コードを受信したら、[確認コード (Verification Code)] フィールドにコードを入力し、[確認 (Verify)] をクリックします。

---

## 通知メッセージの例

通知エンドポイントを設定すると、Crosswork Cloud Network Insights は指定したエンドポイントに通知メッセージを送信します。次の例は、各エンドポイントタイプのサンプルメッセージを示しています。

## 電子メールのエンドポイント通知の例

通知エンドポイントを設定し、タイプを [電子メール (Email)] に指定すると、アラーム条件が満たされた場合に、Crosswork Cloud Network Insights は次の例のような電子メールメッセージを送信します。

```
You are subscribed to alarm notifications for crosswork.cisco.com.

There is 1 alarm transition event for AutomationOnly8 organization.
=====

08 - AS Path Length Violation
=====
Rule: AS Path Length Violation
Alarm Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a
Expected Prefix: 84.205.80.0/24
Priority: High
Condition: Active
State: ACTIVE
Last Activated: 2021-09-30 23:18:35 UTC
Last Deactivated: 2021-09-30 23:15:20 UTC
Expected Minimum Path Length: 1
Expected Maximum Path Length: 2
Activate Peer Threshold Count: 2
Observed Min AS-PATH: 3
Observed Max AS-PATH: 8
Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation

=====

To change your notification settings, please log in to https://crosswork.cisco.com.
```

## スラックのエンドポイント通知の例

通知エンドポイントを設定し、タイプに [Slack] を指定すると、アラーム条件が満たされたときに、Crosswork Cloud Network Insights は次の例のような Slack メッセージを送信します。

```
You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.
=====
Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UT
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH:
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation
=====

To change your notification settings, please log in to https://crosswork.cisco.com.
```

## Microsoft Teams のエンドポイント通知の例

通知エンドポイントを設定し、タイプに [Microsoft Teams] を指定すると、アラーム条件が満たされたときに、Crosswork Cloud Network Insights は次の例のようなメッセージを送信します。

```
You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.
```

```
Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UTC,
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH: 3,
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation
```

```
=====
To change your notification settings, please log in to https://crosswork.cisco.com.
```

## Cisco Webex のエンドポイント通知の例

通知エンドポイントを設定し、タイプに [Webex] を指定すると、アラーム条件が満たされたときに、Crosswork Cloud は次の例のような Webex メッセージを送信します。

```
You are subscribed to alarm notifications for crosswork.cisco.com.
There is 1 alarm transition event for AutomationOnly8 organization.
```

```
=====
Policy: 08 - AS Path Length Violation, Rule: AS Path Length Violation, Alarm
Details: https://crosswork.cisco.com/#/extRoute/alarm/00db6966-9bf2-441b-b940-8259b7f8131a, Expected Prefix: 84.205.80.0/24,
Priority: High, Condition: Active, State: ACTIVE, Last Activated: 2021-09-30 23:18:35 UTC, Last Deactivated: 2021-09-30 23:15:20 UTC,
Expected Minimum Path Length: 1, Expected Maximum Path Length: 2, Activate Peer Threshold Count: 2, Observed Min AS-PATH: 3,
Observed Max AS-PATH: 8, Reporting Peers Count: 21
Tags: common tag | prefix policy | 08 - AS Path Length Violation
```

```
=====
To change your notification settings, please log in to https://crosswork.cisco.com.
```

## アラームタイプ別 Amazon S3 と Google ストレージのエンドポイント通知の例

次のセクションでは、各アラームタイプの Amazon S3 と Google ストレージの通知ログメッセージの例を示します。

### AS 発信元違反の例

次に、AS 発信元違反アラームに関する Amazon S3 と Google ストレージの通知ログメッセージ例を示します。

```
{
 "activatedAt": "2023-02-04T03:02:19Z",
 "alarmId": "04aa5831-7e62-45cb-a123-3d5e9c019330",
```

```
"clearedAt": "2023-02-04T03:01:41Z",
"expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 1523
]
},
"monitoredPrefix": "31.1.1.0/24",
"observed": {
 "allViolationPeers": [
 {
 "asn": 6008,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 21
 },
 {
 "asn": 6009,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 22
 },
 {
 "asn": 6005,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 6007,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 20
 },
 {
 "asn": 6002,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 6004,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 6001,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 6000,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 },
 {
 "asn": 6006,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 19
 },
 {
 "asn": 6003,
 "at": "2023-02-04T03:00:58Z",

```

```

 "peerId": 3,
 "peerIp": "10.11.12.3"
 }
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "963b86db-329d-4cba-a38a-3fc19ddd330d",
"policyName": "02 - AS Origin Violation",
"rule": "ALARM_RULE_AS_ORIGIN_VIOLATION",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "02 - AS Origin Violation"
],
"transitionedAt": "2023-02-04T03:02:19Z"
}
{
 "activatedAt": "2023-02-04T03:02:19Z",
 "alarmId": "9ea271fb-1976-450f-b653-d3d188426b6e",
 "clearedAt": "2023-02-04T03:01:42Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 1523
]
 },
 "monitoredPrefix": "2002:1f01:100::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 6009,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 30
 },
 {
 "asn": 6004,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 25
 },
 {
 "asn": 6001,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 23
 },
 {
 "asn": 6006,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 27
 },
 {
 "asn": 6000,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 },
 {
 "asn": 6003,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 24
 }
]
 }
}

```

```

 {
 "asn": 6005,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 26
 },
 {
 "asn": 6008,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 29
 },
 {
 "asn": 6007,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 28
 },
 {
 "asn": 6011,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 32
 },
 {
 "asn": 6002,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 6010,
 "at": "2023-02-04T03:00:58Z",
 "peerId": 31
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "963b86db-329d-4cba-a38a-3fc19ddd330d",
"policyName": "02 - AS Origin Violation",
"rule": "ALARM_RULE_AS_ORIGIN_VIOLATION",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "02 - AS Origin Violation"
],
"transitionedAt": "2023-02-04T03:02:19Z"
}

```

## AS パス長違反の例

次に、AS パス長違反アラームに関する Amazon S3 と Google ストレージの通知ログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:09:32Z",
 "alarmId": "38a07db7-776e-4b4a-a186-b7d4bd9b045c",
 "clearedAt": "2023-02-04T03:08:53Z",
 "expected": {
 "maxAsPathLength": 2,
 "minAsPathLength": 1,
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
 },
}

```



```
"monitoredPrefix": "145.25.0.0/16",
"observed": {
 "allViolationPeers": [
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 19
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 20
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 21
 },
 {
 "asPath": [
 902,
 602,
```

```

 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 22
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
}
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "bc4298d2-1a52-4339-83e8-1d8932e1fe61",
"policyName": "03 - AS Path Length Violation",
"rule": "ALARM_RULE_AS_PATH_LENGTH_VIOLATION",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",

```

```
"tags": [
 "common tag",
 "prefix policy",
 "03 - AS Path Length Violation"
],
"transitionedAt": "2023-02-04T03:09:32Z"
}
{
 "activatedAt": "2023-02-04T03:09:32Z",
 "alarmId": "e44e6834-7877-435c-9068-169e56cae5aa",
 "clearedAt": "2023-02-04T03:08:53Z",
 "expected": {
 "maxAsPathLength": 2,
 "minAsPathLength": 1,
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
 },
 "monitoredPrefix": "2002:9119::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 23
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 24
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 25
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 26
 }
]
 }
}
```

```
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 27
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 28
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 29
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 30
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 31
},
{
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
```

```

 "peerId": 32
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asPath": [
 902,
 602,
 22
],
 "asPathLength": 3,
 "asn": 22,
 "at": "2023-02-04T03:06:32Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
 "allViolationPeersCount": 12
 },
 "orgName": "AutomationOnly5",
 "policyId": "bc4298d2-1a52-4339-83e8-1d8932e1fe61",
 "policyName": "03 - AS Path Length Violation",
 "rule": "ALARM_RULE_AS_PATH_LENGTH_VIOLATION",
 "severity": "ALARM_SEVERITY_RED",
 "state": "ALARM_STATE_ACTIVE",
 "tags": [
 "common tag",
 "prefix policy",
 "03 - AS Path Length Violation"
],
 "transitionedAt": "2023-02-04T03:09:32Z"
}

```

## DNS ルートサーバーの取り消しの例

次に、DNS ルートサーバーの取り消しアラームに関する Amazon S3 と Google ストレージの通知ログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T06:16:17Z",
 "alarmId": "5161f679-8e4e-4b95-a979-1788b3444136",
 "monitoredPeer": {
 "peerIp": "2000::30:100:10",
 "peerName": "Root DNS IPv6",
 "sessionId": "9b3f0207-a484-465b-886b-0c8bbcefb8bc"
 },
 "observed": {
 "withdrawnPrefix": "2001:503:ba3e::/48"
 },
 "orgName": "AutomationOnly5",
 "policyId": "3fb1473d-a1cb-43f2-b232-6a3cb470051b",
 "policyName": "20 - DNS Root Server Withdrawal",
 "rule": "ALARM_RULE_DNS_ROOT_SERVER_WITHDRAWAL",
}

```

```

"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"transitionedAt": "2023-02-04T06:16:17Z"
}
{
"activatedAt": "2023-02-04T06:16:17Z",
"alarmId": "b87dc535-7151-4728-90f2-0b24b979d4b8",
"monitoredPeer": {
"peerIp": "10.31.32.1",
"peerName": "Root DNS IPv4",
"sessionId": "c5dcf2d2-99b7-4565-8b29-9b30f20ed2f7"
},
"observed": {
"withdrawnPrefix": "198.41.0.0/24"
},
"orgName": "AutomationOnly5",
"policyId": "3fb1473d-a1cb-43f2-b232-6a3cb470051b",
"policyName": "20 - DNS Root Server Withdrawal",
"rule": "ALARM_RULE_DNS_ROOT_SERVER_WITHDRAWAL",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"transitionedAt": "2023-02-04T06:16:17Z"
}
}

```

## 新しい AS パスのエッジの例

次に、新しい AS パスのエッジアラームに関する Amazon S3 通知と Google ストレージのログメッセージ例を示します。

```

{
"activatedAt": "2023-02-04T03:11:17Z",
"alarmId": "4b9eb669-774d-4a6d-bed5-d559248953e8",
"expected": {
"numPeersToTrigger": 1
},
"monitoredPrefix": "88.88.109.0/24",
"observed": {
"allViolationPeers": [
{
"asPath": [
916,
700,
620,
36
],
"asn": 36,
"at": "2023-02-04T01:34:59Z",
"peerId": 1,
"peerIp": "10.11.12.1",
"suspiciousEdges": [
{
"edgeId": {
"fromAs": 36,
"toAs": 620
},
"firstSeen": "2023-02-04T01:34:59Z",
"lastSeen": "2023-02-04T01:34:59Z",
"peerCount": 2,
"prefixCount": 2,
"prefixList": [
"2002:5858:6d00::/48",
"88.88.109.0/24"
]
}
]
}
]
}
}

```

```
 },
 {
 "edgeId": {
 "fromAs": 620,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 621,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 19,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 621
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
],
 {
 "edgeId": {
 "fromAs": 621,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 619,
 36
]
}
```

```

],
"asn": 36,
"at": "2023-02-04T01:34:59Z",
"peerId": 2,
"peerIp": "10.11.12.2",
"suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 619
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 },
 {
 "edgeId": {
 "fromAs": 619,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 622,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 20,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 622
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 622,

```



```

 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 623,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 21,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 623
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 },
 {
 "edgeId": {
 "fromAs": 623,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 624,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 22,

```

```

"suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 624
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 624,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
],
{
 "asPath": [
 916,
 700,
 618,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 3,
 "peerIp": "10.11.12.3",
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 618
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 618,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 }
]
}

```

```

 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
}
},
{
 "asPath": [
 916,
 700,
 617,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 4,
 "peerIp": "10.11.12.4",
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 617
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 617,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
}
},
{
 "asPath": [
 916,
 700,
 616,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 5,
 "peerIp": "10.11.12.5",
 "suspiciousEdges": [
 {

```

```

 "edgeId": {
 "fromAs": 36,
 "toAs": 616
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 616,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 }
],
{
 "asPath": [
 916,
 700,
 615,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 7,
 "peerIp": "10.31.32.1",
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 615
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
],
 {
 "edgeId": {
 "fromAs": 615,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 }
}

```

```

 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
}
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "3755ed13-6498-4cc6-9798-a1264d03b402",
"policyName": "04 - New AS Path Edge",
"rule": "ALARM_RULE_NEW_AS_PATH_EDGE",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "04 - New AS Path Edge"
],
"transitionedAt": "2023-02-04T03:11:17Z"
}
{
 "activatedAt": "2023-02-04T03:11:17Z",
 "alarmId": "9a1ab970-144b-4256-a864-4eb26e698844",
 "expected": {
 "numPeersToTrigger": 1
 },
 "monitoredPrefix": "2002:5858:6d00::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asPath": [
 916,
 700,
 616,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 23,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 616
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
],
 "edgeId": {
 "fromAs": 616,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 }
]
 }
}

```

```

 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 }
}
},
{
 "asPath": [
 916,
 700,
 618,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 24,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 618
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 618,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 619,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 25,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,

```

```
 "toAs": 619
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 },
 {
 "edgeId": {
 "fromAs": 619,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 620,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 26,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 620
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 }
],
 {
 "edgeId": {
 "fromAs": 620,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
}
```

```

]
 }
]
},
{
 "asPath": [
 916,
 700,
 621,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 27,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 621
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 621,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 622,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 28,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 622
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,

```



```
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 622,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 623,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 29,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 623
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "2002:5858:6d00::/48",
 "88.88.109.0/24"
]
 },
 {
 "edgeId": {
 "fromAs": 623,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
}
],
{
```

```

"asPath": [
 916,
 700,
 624,
 36
],
"asn": 36,
"at": "2023-02-04T01:34:59Z",
"peerId": 30,
"suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 624
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 624,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 625,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 31,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 625
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 1,
 "prefixCount": 1,
 "prefixList": [
 "2002:5858:6d00::/48"
]
 }
],
}

```

```

 {
 "edgeId": {
 "fromAs": 625,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 1,
 "prefixCount": 1,
 "prefixList": [
 "2002:5858:6d00::/48"
]
 }
],
},
{
 "asPath": [
 916,
 700,
 626,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 32,
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 626
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 1,
 "prefixCount": 1,
 "prefixList": [
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 626,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 1,
 "prefixCount": 1,
 "prefixList": [
 "2002:5858:6d00::/48"
]
 }
]
},
{
 "asPath": [
 916,
 700,
 617,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 6,

```

```

"peerIp": "2000::20:100:10",
"suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 617
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 617,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
],
{
 "asPath": [
 916,
 700,
 615,
 36
],
 "asn": 36,
 "at": "2023-02-04T01:34:59Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10",
 "suspiciousEdges": [
 {
 "edgeId": {
 "fromAs": 36,
 "toAs": 615
 },
 "firstSeen": "2023-02-04T01:34:59Z",
 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 },
 {
 "edgeId": {
 "fromAs": 615,
 "toAs": 700
 },
 "firstSeen": "2023-02-04T01:34:59Z",

```

```

 "lastSeen": "2023-02-04T01:34:59Z",
 "peerCount": 2,
 "prefixCount": 2,
 "prefixList": [
 "88.88.109.0/24",
 "2002:5858:6d00::/48"
]
 }
}
],
"allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "3755ed13-6498-4cc6-9798-a1264d03b402",
"policyName": "04 - New AS Path Edge",
"rule": "ALARM_RULE_NEW_AS_PATH_EDGE",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "04 - New AS Path Edge"
],
"transitionedAt": "2023-02-04T03:11:17Z"
}

```

## 親集約の変更例

次に、**親集約変更**アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T05:23:55Z",
 "alarmId": "928315c2-c804-47dc-bc52-e2282e605753",
 "expected": {
 "allowedAggregates": [
 "2002::/16",
 "2002::/17",
 "2002:57e8::/36"
],
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 1000
],
 "originAsnsUsage": "ALARM_USAGE_EXCLUDE"
 },
 "monitoredPrefix": "2002:57e8::/48",
 "observed": {
 "allViolationPeers": [
 {
 "peerId": 23
 },
 {
 "peerId": 24
 },
 {
 "peerId": 25
 },
 {
 "peerId": 26
 }
],
 }
}

```

```
{
 "peerId": 27
},
{
 "peerId": 28
},
{
 "peerId": 29
},
{
 "peerId": 30
},
{
 "peerId": 31
},
{
 "peerId": 32
},
{
 "peerId": 6
},
{
 "peerId": 8
}
],
"allViolationPeersCount": 12,
"lastViolationPeers": [
 {
 "asn": 6002,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 6010,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 31
 },
 {
 "asn": 6009,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 30
 },
 {
 "asn": 6003,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 24
 },
 {
 "asn": 6011,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 32
 },
 {
 "asn": 6005,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 26
 },
 {
 "asn": 6007,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 28
 },
 {
```

```

 "asn": 6004,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 25
 },
 {
 "asn": 6006,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 27
 },
 {
 "asn": 6000,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 },
 {
 "asn": 6001,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 23
 },
 {
 "asn": 6008,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 29
 }
],
 "lastViolationPeersCount": 12,
 "lastViolationPrefix": "2002:57e8::/36",
 "violationPrefixesCount": 3
},
"orgName": "AutomationOnly5",
"policyId": "3dd434f4-92fe-447f-b7e8-129b09cff9da",
"policyName": "17 - Parent Aggregate Change - Test 3",
"rule": "ALARM_RULE_PARENT_AGGREGATE_CHANGE",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "17 - Parent Aggregate Change"
],
"transitionedAt": "2023-02-04T05:23:55Z"
}
{
 "activatedAt": "2023-02-04T05:23:55Z",
 "alarmId": "c3d24f64-5814-463e-855f-da56545a621f",
 "expected": {
 "allowedAggregates": [
 "87.232.0.0/22"
],
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 1000
],
 "originAsnsUsage": "ALARM_USAGE_EXCLUDE"
 },
 "monitoredPrefix": "87.232.0.0/24",
 "observed": {
 "allViolationPeers": [
 {
 "peerId": 1
 },
 {

```

```
 "peerId": 19
 },
 {
 "peerId": 2
 },
 {
 "peerId": 20
 },
 {
 "peerId": 21
 },
 {
 "peerId": 22
 },
 {
 "peerId": 3
 },
 {
 "peerId": 4
 },
 {
 "peerId": 5
 },
 {
 "peerId": 7
 }
],
"allViolationPeersCount": 10,
"lastViolationPeers": [
 {
 "asn": 6004,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 6008,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 21
 },
 {
 "asn": 6009,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 22
 },
 {
 "asn": 6002,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 6003,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 6005,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
```



```

 "asn": 6006,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 19
 },
 {
 "asn": 6001,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 6000,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 },
 {
 "asn": 6007,
 "at": "2023-02-04T05:03:37Z",
 "peerId": 20
 }
],
 "lastViolationPeersCount": 10,
 "lastViolationPrefix": "87.232.0.0/22",
 "violationPrefixesCount": 1
},
"orgName": "AutomationOnly5",
"policyId": "3dd434f4-92fe-447f-b7e8-129b09cff9da",
"policyName": "17 - Parent Aggregate Change - Test 3",
"rule": "ALARM_RULE_PARENT_AGGREGATE_CHANGE",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "17 - Parent Aggregate Change"
],
"transitionedAt": "2023-02-04T05:23:55Z"
}

```

## ピアでアドバタイズされたプレフィックス数の例

次に、ピアでアドバタイズされたプレフィックス数アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T06:18:37Z",
 "alarmId": "139a7983-36ba-4d17-8371-2480290f3799",
 "expected": {
 "prefixCounts": [
 {
 "addressFamily": "ALARM_BGP_AF_IPV4",
 "maxPrefixes": 100,
 "minPrefixes": 10
 }
]
 },
 "monitoredPeer": {
 "ciscoPeerIp": "104.236.154.30",
 "ciscoPeerName": "RS06",
 "peerIp": "10.11.12.1",
 "peerName": "BGP-1",
 "sessionId": "de26c09c-15f6-435f-9044-c9a89fdc7bed"
 }
}

```

```

 },
 "observed": {
 "prefixCounts": [
 {
 "addressFamily": "ALARM_BGP_AF_IPV4",
 "prefixCount": 2000
 }
]
 },
 "orgName": "AutomationOnly5",
 "policyId": "482de3d2-8550-4b84-a0ab-3b3e36f5869a",
 "policyName": "22 - Peer Advertised Prefix Count",
 "rule": "ALARM_RULE_ADVERTISED_PREFIX_COUNT",
 "severity": "ALARM_SEVERITY_RED",
 "state": "ALARM_STATE_ACTIVE",
 "transitionedAt": "2023-02-04T06:18:37Z"
 }
}

```

## ピアの停止の例

次に、ピアの停止アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T06:17:05Z",
 "alarmId": "b654ced0-5357-4eb7-b3c9-27cbd24a8f65",
 "monitoredPeer": {
 "ciscoPeerIp": "3.21.42.66",
 "ciscoPeerName": "RS95",
 "peerIp": "10.11.12.2",
 "peerName": "BGP-2",
 "sessionId": "29651423-e603-4a11-89b7-37500e40e562"
 },
 "observed": {
 "lastUpdatedAt": "2019-10-03T22:30:00Z"
 },
 "orgName": "AutomationOnly5",
 "policyId": "ff3b620d-33a9-49c0-9e33-b99b53c55b1d",
 "policyName": "21 - Peer Down",
 "rule": "ALARM_RULE_PEER_DOWN",
 "severity": "ALARM_SEVERITY_YELLOW",
 "state": "ALARM_STATE_ACTIVE",
 "transitionedAt": "2023-02-04T06:17:05Z"
}

```

## プレフィックス アドバタイズメントの例

次に、プレフィックス アドバタイズメントアラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:16:25Z",
 "alarmId": "79222047-4954-4b6e-a339-9d01bfb06434",
 "clearedAt": "2023-02-04T03:15:47Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
 },
 "monitoredPrefix": "218.56.100.0/28",
 "observed": {
 "allViolationPeers": [
 {

```

```
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 19
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 20
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 21
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 22
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "4d4816b9-e579-4209-a907-8d909aaf1f0",
"policyName": "05 - Prefix Advertisement",
"rule": "ALARM_RULE_PREFIX_ADVERTISEMENT",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
```

```
"tags": [
 "common tag",
 "prefix policy",
 "05 - Prefix Advertisement"
],
"transitionedAt": "2023-02-04T03:16:25Z"
}
{
"activatedAt": "2023-02-04T03:16:25Z",
"alarmId": "ba974865-7e94-4623-ad8f-d660acf7d69f",
"clearedAt": "2023-02-04T03:15:47Z",
"expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
},
"monitoredPrefix": "2002:da38:6400::/48",
"observed": {
 "allViolationPeers": [
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 23
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 24
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 25
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 26
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 27
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 28
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 29
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 30
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 31
 },
 {

```

```

 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 32
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 20,
 "at": "2023-02-04T03:15:04Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "4d4816b9-e579-4209-a907-8d909aafaf0",
"policyName": "05 - Prefix Advertisement",
"rule": "ALARM_RULE_PREFIX_ADVERTISEMENT",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "05 - Prefix Advertisement"
],
"transitionedAt": "2023-02-04T03:16:25Z"
}

```

## プレフィックス取り消しの例

次に、プレフィックス取り消しアラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:20:36Z",
 "alarmId": "2e12713b-4ecf-4d59-868a-00f07aba47ae",
 "clearedAt": "2023-02-04T03:19:55Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
 },
 "monitoredPrefix": "100.200.1.0/24",
 "observed": {
 "allViolationPeers": [
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 19
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 20
 },
 {

```

```

 "at": "2023-02-04T03:19:13Z",
 "peerId": 21
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 22
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 9
},
"orgName": "AutomationOnly5",
"policyId": "16105783-75c8-4c98-be71-b0a758645f41",
"policyName": "06 - Prefix Withdrawal",
"rule": "ALARM_RULE_PREFIX_WITHDRAWAL",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "06 - Prefix Withdrawal"
],
"transitionedAt": "2023-02-04T03:20:36Z"
}
{
"activatedAt": "2023-02-04T03:20:36Z",
"alarmId": "3c4cf6e0-e6f2-475d-9030-4bc51a7e0550",
"clearedAt": "2023-02-04T03:19:55Z",
"expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
},
"monitoredPrefix": "2002:64c8:100::/48",
"observed": {
 "allViolationPeers": [
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 23
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 24
 },
 {
 "at": "2023-02-04T03:19:13Z",

```

```

 "peerId": 25
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 26
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 27
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 28
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 29
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 30
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 31
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 32
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "at": "2023-02-04T03:19:13Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "16105783-75c8-4c98-be71-b0a758645f41",
"policyName": "06 - Prefix Withdrawal",
"rule": "ALARM_RULE_PREFIX_WITHDRAWAL",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "06 - Prefix Withdrawal"
],
"transitionedAt": "2023-02-04T03:20:36Z"
}

```

## 禁止された IP プレフィックスの例

次に、**禁止された IP プレフィックス**（フル Bogons）アラームに関する Amazon S3 と Google ストレージの通知ログメッセージ例を示します。

## 禁止された IP プレフィックスの例

```

{
 "activatedAt": "2023-02-04T06:11:31Z",
 "alarmId": "a077c6cd-5a74-4378-8d60-e8acb39ae2c7",
 "clearedAt": "2023-02-04T06:09:26Z",
 "monitoredPeer": {
 "ciscoPeerIp": "104.236.154.30",
 "ciscoPeerName": "RS06",
 "peerIp": "10.11.12.5",
 "peerName": "FullBogon-1",
 "sessionId": "f5327ffb-221f-49d6-b8a2-2b812d02d35e"
 },
 "observed": {
 "lastViolationPeerPrefix": {
 "at": "2023-02-04T06:07:33Z",
 "bogonDetails": {
 "bogonType": "ALARM_BOGON_TYPE_FULL_BOGON",
 "prohibitedPrefixBlock": "5.44.248.0/21"
 },
 "prefix": "5.44.248.0/21"
 },
 "violationPrefixesCount": 1
 },
 "orgName": "AutomationOnly5",
 "policyId": "d011c5e4-54a1-41bb-8c7f-963d9caab208",
 "policyName": "19 - Prohibited IP Prefix - FullBogon",
 "rule": "ALARM_RULE_PROHIBITED_IP_PREFIX",
 "severity": "ALARM_SEVERITY_YELLOW",
 "state": "ALARM_STATE_ACTIVE",
 "transitionedAt": "2023-02-04T06:11:31Z"
}
{
 "activatedAt": "2023-02-04T06:11:31Z",
 "alarmId": "142659ed-15f1-4d60-b2d6-3d0da5c75b17",
 "clearedAt": "2023-02-04T06:09:26Z",
 "monitoredPeer": {
 "ciscoPeerIp": "2604:a880:1:20::2de:1001",
 "ciscoPeerName": "RS06",
 "peerIp": "2000::20:100:10",
 "peerName": "FullBogon-2",
 "sessionId": "639f069d-9ccd-46d0-b8b2-77054a199ce8"
 },
 "observed": {
 "lastViolationPeerPrefix": {
 "at": "2023-02-04T06:07:33Z",
 "bogonDetails": {
 "bogonType": "ALARM_BOGON_TYPE_FULL_BOGON",
 "prohibitedPrefixBlock": "2001:506:101::/48"
 },
 "prefix": "2001:506:101::/48"
 },
 "violationPrefixesCount": 1
 },
 "orgName": "AutomationOnly5",
 "policyId": "d011c5e4-54a1-41bb-8c7f-963d9caab208",
 "policyName": "19 - Prohibited IP Prefix - FullBogon",
 "rule": "ALARM_RULE_PROHIBITED_IP_PREFIX",
 "severity": "ALARM_SEVERITY_YELLOW",
 "state": "ALARM_STATE_ACTIVE",
 "transitionedAt": "2023-02-04T06:11:31Z"
}

```



## ROA の有効期限の例

次に、**ROA の有効期限**アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```
{
 "activatedAt": "2023-02-04T03:27:02Z",
 "alarmId": "9f8eb76a-3eff-4e8b-809e-53bf0fd56ebe",
 "clearedAt": "2023-02-04T03:26:20Z",
 "expected": {
 "numPeersToTrigger": 1
 },
 "monitoredPrefix": "2002:101:7700::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 23
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 24
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 25
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 26
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 27
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 28
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 29
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 30
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 31
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",

```

```

 "peerId": 32
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
"allViolationPeersCount": 12,
"roas": [
 {
 "asn": 33,
 "maxLength": 48,
 "notAfter": "2023-02-17T03:49:38Z",
 "notBefore": "2022-02-03T03:49:38Z",
 "prefix": "2002:101:7700::/48",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 },
 {
 "asn": 33,
 "maxLength": 48,
 "notAfter": "2023-02-17T19:24:49Z",
 "notBefore": "2022-02-03T19:24:49Z",
 "prefix": "2002:101:7700::/48",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 },
 {
 "asn": 33,
 "maxLength": 48,
 "notAfter": "2023-02-18T01:34:59Z",
 "notBefore": "2022-02-04T01:34:58Z",
 "prefix": "2002:101:7700::/48",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 }
]
},
"orgName": "AutomationOnly5",
"policyId": "d3d47d8c-fee7-45ab-baee-3a860128aa65",
"policyName": "08 - ROA Expiry",
"rule": "ALARM_RULE_ROA_EXPIRY",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "08 - ROA Expiry"
],
"transitionedAt": "2023-02-04T03:27:02Z"
}
{
 "activatedAt": "2023-02-04T03:27:02Z",
 "alarmId": "e85e68ad-e16d-4892-9fb9-c71bd92f9caf",
 "clearedAt": "2023-02-04T03:26:20Z",
 "expected": {

```

```
"numPeersToTrigger": 1
},
"monitoredPrefix": "210.176.151.0/24",
"observed": {
 "allViolationPeers": [
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 19
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 20
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 21
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 22
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 33,
 "at": "2023-02-04T03:25:38Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 10,
 "roas": [
```

```

 {
 "asn": 33,
 "maxLength": 24,
 "notAfter": "2023-02-17T03:49:38Z",
 "notBefore": "2022-02-03T03:49:38Z",
 "prefix": "210.176.151.0/24",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 },
 {
 "asn": 33,
 "maxLength": 24,
 "notAfter": "2023-02-17T19:24:49Z",
 "notBefore": "2022-02-03T19:24:49Z",
 "prefix": "210.176.151.0/24",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 },
 {
 "asn": 33,
 "maxLength": 24,
 "notAfter": "2023-02-18T01:34:58Z",
 "notBefore": "2022-02-04T01:34:58Z",
 "prefix": "210.176.151.0/24",
 "rpkiStatus": "ALARM_ROA_VALID",
 "trustAnchor": "ALARM_AFRINIC"
 }
]
},
"orgName": "AutomationOnly5",
"policyId": "d3d47d8c-fee7-45ab-baee-3a860128aa65",
"policyName": "08 - ROA Expiry",
"rule": "ALARM_RULE_ROA_EXPIRY",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "08 - ROA Expiry"
],
"transitionedAt": "2023-02-04T03:27:02Z"
}

```

## ROA が見つからない例

次に、ROA が見つからない場合のアラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:22:07Z",
 "alarmId": "992266a8-bc34-4e6f-b396-6f0c956886ae",
 "monitoredPrefix": "2.2.2.2/32",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",

```

```
 "peerId": 19
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 20
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 21
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 22
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "588687b4-4e2c-44d6-8f93-56957139b4f4",
"policyName": "07 - ROA Not Found",
"rule": "ALARM_RULE_ROA_NOT_FOUND",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "07 - ROA Not Found"
],
"transitionedAt": "2023-02-04T03:22:07Z"
}
}
```

```
"activatedAt": "2023-02-04T03:22:07Z",
"alarmId": "c7ff225d-f4e0-49d7-b607-f9d4f98b346f",
"monitoredPrefix": "2002:202:202::/48",
"observed": {
 "allViolationPeers": [
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 23
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 24
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 25
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 26
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 27
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 28
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 29
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 30
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 31
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 32
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 31,
 "at": "2023-02-04T01:34:58Z",

```

```

 "peerId": 8,
 "peerIp": "2000::30:100:10"
 },
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "588687b4-4e2c-44d6-8f93-56957139b4f4",
"policyName": "07 - ROA Not Found",
"rule": "ALARM_RULE_ROA_NOT_FOUND",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "07 - ROA Not Found"
],
"transitionedAt": "2023-02-04T03:22:07Z"
}

```

## ROA 障害の例

次に、**ROA 障害**アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:31:32Z",
 "alarmId": "358c3f57-80b8-4685-baec-7d913f39988e",
 "clearedAt": "2023-02-04T03:30:51Z",
 "expected": {
 "numPeersToTrigger": 1,
 "originAsns": [
 24,
 1136
]
 },
 "monitoredPrefix": "194.45.8.0/22",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 19
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 20
 },
 {
 "asn": 23,

```

```

 "at": "2023-02-04T03:30:09Z",
 "peerId": 21
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 22
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 10
 },
 "orgName": "AutomationOnly5",
 "policyId": "0510e174-1553-4c12-ac9e-be68118c8bd2",
 "policyName": "09 - ROA Failure",
 "rule": "ALARM_RULE_ROA_FAILURE",
 "severity": "ALARM_SEVERITY_RED",
 "state": "ALARM_STATE_ACTIVE",
 "tags": [
 "common tag",
 "prefix policy",
 "09 - ROA Failure"
],
 "transitionedAt": "2023-02-04T03:31:32Z"
}
{
 "activatedAt": "2023-02-04T03:31:32Z",
 "alarmId": "4e0b7398-ae54-408e-95fc-e7bb17a7d952",
 "clearedAt": "2023-02-04T03:30:51Z",
 "expected": {
 "numPeersToTrigger": 1,
 "originAsns": [
 24
]
 },
 "monitoredPrefix": "2002:c22d:800::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",

```



```
 "peerId": 23
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 24
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 25
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 26
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 27
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 28
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 29
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 30
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 31
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 32
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asn": 23,
 "at": "2023-02-04T03:30:09Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "0510e174-1553-4c12-ac9e-be68118c8bd2",
```

```

 "policyName": "09 - ROA Failure",
 "rule": "ALARM_RULE_ROA_FAILURE",
 "severity": "ALARM_SEVERITY_RED",
 "state": "ALARM_STATE_ACTIVE",
 "tags": [
 "common tag",
 "prefix policy",
 "09 - ROA Failure"
],
 "transitionedAt": "2023-02-04T03:31:32Z"
 }
}

```

## サブプレフィックス アドバタイズメントの例

次に、サブプレフィックス アドバタイズメントアラームに関する Amazon S3 通知と Google ストレージのログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:48:07Z",
 "alarmId": "4f90ba05-d16e-4cb1-8bfe-f9bb54fc96dd",
 "clearedAt": "2023-02-04T03:47:26Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 754,
 755,
 1000,
 6000,
 6001,
 6002,
 6003,
 6004,
 6005,
 6006,
 6007,
 6008,
 6009,
 6010,
 6011,
 9541,
 9542,
 9543,
 12654,
 12655,
 28642,
 30175,
 45031,
 49622
],
 "originAsnsUsage": "ALARM_USAGE_IGNORE"
 },
 "monitoredPrefix": "2002:1764:100::/48",
 "observed": {
 "allViolationPeers": [
 {
 "peerId": 28
 },
 {
 "peerId": 29
 }
],
 "allViolationPeersCount": 2,
 }
}

```

```

 "lastViolationPeers": [
 {
 "asn": 6000,
 "at": "2023-02-04T03:45:01Z",
 "peerId": 28
 },
 {
 "asn": 6001,
 "at": "2023-02-04T03:45:02Z",
 "peerId": 29
 }
],
 "lastViolationPeersCount": 2,
 "lastViolationPrefix": "2002:1764:100::/49",
 "violationPrefixesCount": 10
 },
 "orgName": "AutomationOnly5",
 "policyId": "634cc992-80f5-488e-bd42-bcb61217be9f",
 "policyName": "12 - Subprefix Advertisement - Default",
 "rule": "ALARM_RULE_SUBPREFIX_ADVERTISEMENT",
 "severity": "ALARM_SEVERITY_GRAY",
 "state": "ALARM_STATE_ACTIVE",
 "tags": [
 "common tag",
 "prefix policy",
 "12 - Subprefix Advertisement"
],
 "transitionedAt": "2023-02-04T03:48:07Z"
}
{
 "activatedAt": "2023-02-04T03:48:07Z",
 "alarmId": "6e1e50ff-e57f-4a2b-9814-7c5a71b01b1d",
 "clearedAt": "2023-02-04T03:47:26Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "originAsns": [
 754,
 755,
 1000,
 6000,
 6001,
 6002,
 6003,
 6004,
 6005,
 6006,
 6007,
 6008,
 6009,
 6010,
 6011,
 9541,
 9542,
 9543,
 12654,
 12655,
 28642,
 30175,
 45031,
 49622
]
 },
 "originAsnsUsage": "ALARM_USAGE_IGNORE"
},

```

```

"monitoredPrefix": "23.100.1.0/24",
"observed": {
 "allViolationPeers": [
 {
 "peerId": 1
 },
 {
 "peerId": 19
 }
],
 "allViolationPeersCount": 2,
 "lastViolationPeers": [
 {
 "asn": 6000,
 "at": "2023-02-04T03:45:01Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 6001,
 "at": "2023-02-04T03:45:01Z",
 "peerId": 19
 }
],
 "lastViolationPeersCount": 2,
 "lastViolationPrefix": "23.100.1.0/25",
 "violationPrefixesCount": 8
},
"orgName": "AutomationOnly5",
"policyId": "634cc992-80f5-488e-bd42-bcb61217be9f",
"policyName": "12 - Subprefix Advertisement - Default",
"rule": "ALARM_RULE_SUBPREFIX_ADVERTISEMENT",
"severity": "ALARM_SEVERITY_GRAY",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "12 - Subprefix Advertisement"
],
"transitionedAt": "2023-02-04T03:48:07Z"
}

```

## 予期しない AS プレフィックスの例

次に、予期しない AS プレフィックスアラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T02:58:11Z",
 "alarmId": "6a6be977-ecf3-423c-bf4e-fc9118659a69",
 "clearedAt": "2023-02-04T02:57:43Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2
 },
 "monitoredAsn": 601,
 "observed": {
 "allViolationPeers": [
 {
 "peerId": 1
 },
 {
 "peerId": 2
 }
]
 }
}

```

```
 },
 {
 "peerId": 3
 },
 {
 "peerId": 4
 },
 {
 "peerId": 5
 },
 {
 "peerId": 7
 },
 {
 "peerId": 19
 },
 {
 "peerId": 20
 },
 {
 "peerId": 21
 },
 {
 "peerId": 22
 }
],
 "allViolationPeersCount": 10,
 "lastViolationPeers": [
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 19
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 20
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 21
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 22
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 3,
```

```

 "peerIp": "10.11.12.3"
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 601,
 "at": "2023-02-04T02:55:11Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "lastViolationPeersCount": 10,
 "lastViolationPrefix": "101.1.1.0/24",
 "violationPrefixesCount": 1
 },
 "orgName": "AutomationOnly5",
 "policyId": "5e3288f9-6e6d-4df7-a862-b638e2d17b9f",
 "policyName": "01 - Unexpected AS Prefix",
 "rule": "ALARM_RULE_UNEXPECTED_AS_PREFIX",
 "severity": "ALARM_SEVERITY_RED",
 "state": "ALARM_STATE_ACTIVE",
 "tags": [
 "common tag",
 "asn policy",
 "01 - Unexpected AS Prefix"
],
 "transitionedAt": "2023-02-04T02:58:11Z"
}

```

## アップストリーム AS の変更例

次に、アップストリーム AS 変更アラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:36:49Z",
 "alarmId": "82f76592-14ca-42ef-b446-149c1d4be731",
 "clearedAt": "2023-02-04T03:36:09Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "upstreamAsns": [
 12345
]
 },
 "monitoredPrefix": "2002:ab64:1100::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asn": 6504,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 }
]
 }
}

```

```
 },
 {
 "asn": 6503,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 23
 },
 {
 "asn": 6508,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 27
 },
 {
 "asn": 6502,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 },
 {
 "asn": 6509,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 28
 },
 {
 "asn": 6505,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 24
 },
 {
 "asn": 6510,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 29
 },
 {
 "asn": 6507,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 26
 },
 {
 "asn": 6512,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 31
 },
 {
 "asn": 6513,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 32
 },
 {
 "asn": 6506,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 25
 },
 {
 "asn": 6511,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 30
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "c37b83be-0213-4bb2-b391-7f02b3cec061",
"policyName": "10 - Upstream AS Change",
"rule": "ALARM_RULE_UPSTREAM_AS_CHANGE",
```

```

"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "10 - Upstream AS Change"
],
"transitionedAt": "2023-02-04T03:36:49Z"
}
{
"activatedAt": "2023-02-04T03:36:49Z",
"alarmId": "a778b4be-e23f-42d8-8880-5402f59c1495",
"clearedAt": "2023-02-04T03:36:09Z",
"expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "upstreamAsns": [
 12345
]
},
"monitoredPrefix": "171.100.17.0/24",
"observed": {
 "allViolationPeers": [
 {
 "asn": 6505,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asn": 6503,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asn": 6504,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asn": 6509,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 20
 },
 {
 "asn": 6508,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 19
 },
 {
 "asn": 6507,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asn": 6511,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 22
 },
 {
 "asn": 6502,

```



```

 "at": "2023-02-04T03:33:54Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 },
 {
 "asn": 6510,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 21
 },
 {
 "asn": 6506,
 "at": "2023-02-04T03:33:54Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 }
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "c37b83be-0213-4bb2-b391-7f02b3cec061",
"policyName": "10 - Upstream AS Change",
"rule": "ALARM_RULE_UPSTREAM_AS_CHANGE",
"severity": "ALARM_SEVERITY_RED",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "10 - Upstream AS Change"
],
"transitionedAt": "2023-02-04T03:36:49Z"
}

```

## 有効な AS パスの例

次に、有効な AS パスアラームに関する Amazon S3 通知と Google ストレージ通知のログメッセージ例を示します。

```

{
 "activatedAt": "2023-02-04T03:42:08Z",
 "alarmId": "7cc0e8d0-cef5-422f-a9b9-e6dd227e2bfc",
 "clearedAt": "2023-02-04T03:41:08Z",
 "expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "validAsPathPattern": "108 (999|400) 705"
 },
 "monitoredPrefix": "2002:dc45:500::/48",
 "observed": {
 "allViolationPeers": [
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 23
 },
 {
 "asPath": [
 108,
 500,

```

```
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 24
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 25
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 26
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 27
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 28
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 29
},
{
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
```

```
 "peerId": 30
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 31
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 32
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 6,
 "peerIp": "2000::20:100:10"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 8,
 "peerIp": "2000::30:100:10"
 }
],
 "allViolationPeersCount": 12
},
"orgName": "AutomationOnly5",
"policyId": "1b1d7a95-1104-4434-8f72-33ba216a7e7f",
"policyName": "11 - Valid AS Path",
"rule": "ALARM_RULE_VALID_AS_PATH_VIOLATION",
"severity": "ALARM_SEVERITY_YELLOW",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "11 - Valid AS Path"
],
"transitionedAt": "2023-02-04T03:42:08Z"
}
{
 "activatedAt": "2023-02-04T03:42:08Z",
 "alarmId": "86304e9c-50ce-4ec2-89a2-2c84ab10658b",
 "clearedAt": "2023-02-04T03:41:08Z",
```

```
"expected": {
 "numPeersToClear": 1,
 "numPeersToTrigger": 2,
 "validAsPathPattern": "108 (999|400) 705"
},
"monitoredPrefix": "220.69.5.0/24",
"observed": {
 "allViolationPeers": [
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 1,
 "peerIp": "10.11.12.1"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 19
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 2,
 "peerIp": "10.11.12.2"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 20
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 21
 },
 {
 "asPath": [
 108,
 500,
```

```

 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 22
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 3,
 "peerIp": "10.11.12.3"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 4,
 "peerIp": "10.11.12.4"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 5,
 "peerIp": "10.11.12.5"
 },
 {
 "asPath": [
 108,
 500,
 755
],
 "asn": 755,
 "at": "2023-02-04T03:39:27Z",
 "peerId": 7,
 "peerIp": "10.31.32.1"
 }
],
 "allViolationPeersCount": 10
},
"orgName": "AutomationOnly5",
"policyId": "1b1d7a95-1104-4434-8f72-33ba216a7e7f",
"policyName": "11 - Valid AS Path",
"rule": "ALARM_RULE_VALID_AS_PATH_VIOLATION",
"severity": "ALARM_SEVERITY_YELLOW",
"state": "ALARM_STATE_ACTIVE",
"tags": [
 "common tag",
 "prefix policy",
 "11 - Valid AS Path"
],

```

```
"transitionedAt": "2023-02-04T03:42:08Z"
}
```



## 第 19 章

# デバイスの設定

- [デバイスの追加](#) (173 ページ)
- [トラフィック分析用のデバイスを追加するための前提条件](#) (176 ページ)
- [Crosswork Traffic Analysis 用の外部インターフェイスの指定](#) (182 ページ)
- [Crosswork Trust Insights にデバイスを追加するための前提条件](#) (182 ページ)
- [Trust Insights の信頼ドシエ情報](#) (187 ページ)
- [デバイスの無効化](#) (189 ページ)
- [デバイスの削除](#) (190 ページ)
- [削除されたデバイスの復元](#) (190 ページ)

## デバイスの追加

デバイスを追加するには、次の手順を実行します。

- ステップ 1** メインウィンドウで、[モニタ (Monitor)] > [デバイス (Devices)] または [設定 (Configure)] > [デバイス (Devices)] をクリックします。もしくは、[設定 (Configure)] > [データゲートウェイ (Data Gateways)] > [data\_gateway\_instance] の順に移動して、Crosswork Data Gateway にデバイスを追加、リンクすることもできます。
- ステップ 2** [Add Device] をクリックします。
- ステップ 3** CSV ファイルを使用してデバイスをインポートするには、[CSVのインポート (CSV Import)] をクリックします。
- ステップ 4** 単一のデバイスをインポートするには、次のフィールドに入力します。

表 26: デバイスの追加のフィールドに関する説明

| フィールド               | 説明                                                             |
|---------------------|----------------------------------------------------------------|
| デバイス名 (Device Name) | デバイスの表示名<br><br>(注) データプライバシー上の理由から、このフィールドはデバイスから自動的に入力されません。 |

| フィールド                           | 説明                                                                                                                                                                                                                                                                               |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 説明 (Description)                | (任意) デバイスの説明を追加します。                                                                                                                                                                                                                                                              |
| ホストネーム (Hostname)               | Crosswork Data Gateway によって使用される DNS FQDN または IP アドレス。                                                                                                                                                                                                                           |
| SSH ポート (SSH Port)              | (任意) SSH アクセス用の TCP ポート。デフォルトは TCP/22 です。Crosswork Cloud Traffic Analysis に SSH アクセスは必要ありません。                                                                                                                                                                                    |
| クレデンシャル : SSH (Credential: SSH) | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル : SSH (Credential: SSH)] ドロップダウンリストから選択できます。新しいクレデンシャルグループを作成するには、[クレデンシャル : SSH (Credential: SSH)] ドロップダウンリストから [新しいクレデンシャルの追加 (Add New Credential)] を選択します。クレデンシャルグループの詳細については、 <a href="#">クレデンシャルの作成 (203 ページ)</a> を参照してください。                |
| デバイスグループ (Device Group)         | Crosswork Cloud Traffic Analysis 専用。以前にデバイスグループを作成した場合は、[デバイスグループ (Device Group)] ドロップダウンリストから選択できます。新しいデバイスグループを作成するには、[デバイスグループ (Device Group)] ドロップダウンリストから [新しいデバイスグループの追加 (Add new device group)] を選択します。デバイスグループの詳細については、 <a href="#">デバイスグループの設定 (205 ページ)</a> を参照してください。 |
| 市区町村郡 (City)                    | (任意) デバイスの位置情報の市区町村。                                                                                                                                                                                                                                                             |
| 参照先 (Location)                  | (任意) 論理サイト識別子。                                                                                                                                                                                                                                                                   |
| 国 (Country)                     | (任意) デバイスの位置情報の国。                                                                                                                                                                                                                                                                |
| デバイスのタイムゾーン (Device Timezone)   | (任意) デバイスに対してローカルなタイムゾーン。                                                                                                                                                                                                                                                        |
| タグ (Tags)                       | (任意) デバイスのグループ化と識別に役立つタグを指定します。たとえば、システム内のルータタイプ ( <i>edge</i> など) を識別するテキストを入力する場合があります。                                                                                                                                                                                        |

残りのフィールドは、有効なライセンスがある Crosswork Cloud アプリケーションによって異なります。オプションとして、Crosswork Cloud Trust Insights の Crosswork Data Gateway インスタンスと Crosswork Cloud Traffic Analysis の Crosswork Data Gateway インスタンスの両方にデバイスをリンクすることもできます。



表 27: トラストインサイトのデバイスの追加のフィールドに関する説明

| フィールド                                                   | 説明                                                                                                                                                          |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [データゲートウェイ : トラストインサイト (Data Gateway: Trust Insights) ] | スイッチを [オン (On) ] に切り替え、デバイスの Crosswork Data Gateway インスタンスを選択します。Crosswork Data Gateway を追加するには、 <a href="#">「Crosswork Data Gateway の情報の追加」</a> を参照してください。 |

表 28: トラフィック分析のデバイスの追加のフィールドに関する説明

| フィールド                                                 | 説明                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| データゲートウェイ : トラフィック分析 (Data Gateway: Traffic Analysis) | スイッチを [オン (On) ] に切り替え、デバイスの NetFlow Data Gateway インスタンスを選択します。                                                                                                                                                                                                                   |
| NetFlow 送信元アドレス (NetFlow Source Address)              | NetFlow 送信元アドレスを入力します。                                                                                                                                                                                                                                                            |
| ASN                                                   | ASN を入力します。値はプライベート ASN の範囲 (64512 ~ 65535) である必要があります。                                                                                                                                                                                                                           |
| SNMPアドレス (SNMP Address)                               | SNMP アドレスを入力しない場合は、NetFlow アドレスが使用されます。                                                                                                                                                                                                                                           |
| クレデンシャル : SNMP (Credential: SNMP)                     | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル : SNMP (Credential: SNMP) ] ドロップダウンリストから選択できます。追加するデバイスの新しいクレデンシャルグループを作成するには、[クレデンシャル : SNMP (Credential: SNMP) ] ドロップダウンリストから [新しいクレデンシャルの追加 (Add New Credential) ] を選択します。クレデンシャルグループの詳細については、 <a href="#">クレデンシャルの作成 (203 ページ)</a> を参照してください。 |
| BGPルータIDのIPアドレス (BGP Router ID IP Address)            | —                                                                                                                                                                                                                                                                                 |
| クレデンシャル : BGP (Credential: BGP)                       | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル : BGP (Credential: BGP) ] ドロップダウンリストから選択できます。追加するデバイスの新しいクレデンシャルグループを作成するには、[クレデンシャル : BGP (Credential: BGP) ] ドロップダウンリストから [新しいクレデンシャルの追加 (Add New Credential) ] を選択します。クレデンシャルグループの詳細については、 <a href="#">クレデンシャルの作成 (203 ページ)</a> を参照してください。     |

(注) すべての BGP プレフィックスを Cisco Crosswork Data Gateway と共有する必要があります。

ステップ 5 [保存 (Save)] をクリックします。

保存操作が完了した後、メインウィンドウで [モニタ (Monitor)] > [デバイス (Devices)] または [設定 (Configure)] > [デバイス (Devices)] をクリックすると、デバイスが表示されます。

## トラフィック分析用のデバイスを追加するための前提条件

トラフィック分析にデバイスを追加する前に、デバイスに SSH と次のプロトコルが設定されていることを確認します。

表 29: プロトコル設定

| プロトコル             | 例                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP              | <a href="#">SNMP の構成例 (176 ページ)</a>                                                                                                                                              |
| BGP               | <a href="#">Cisco IOS デバイス用 BGP の構成例 (177 ページ)</a>                                                                                                                               |
| ネットワーク フロー モニタリング | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS XR デバイス用 Netflow の構成例 (179 ページ)</a></li> <li>• <a href="#">Cisco IOS XR デバイス用 IPFIX の構成例 (180 ページ)</a></li> </ul> |

デバイスが特定のコマンドを制限するように設定されている場合は、次の CLI コマンドが許可されていることを確認します。

- `show platform security integrity dossier`
- `show version`

以下のセクションには、構成例が含まれています。

### SNMP の構成例

次のコードは、SNMP の構成例を示しています。

- SNMPv2 の構成例 :

```
snmp-server community flow123 RO
```

前の例では、**flow123** が SNMP コミュニティの構成と一致する必要があります。

- SNMPv3 の構成例

- 認証なし、プライバシーなしの SNMPv3 の場合 :

```
snmp-server group [groupname] v3 noauth
snmp-server user [username] [groupname] v3
```

- 認証あり、プライバシーなしの SNMPv3 の場合 :

```
snmp-server group [groupname] v3 auth
snmp-server user [username] [groupname] auth [md5|sha] <auth-password>
```

- 認証あり、プライバシーありの SNMPv3 の場合 :

```
snmp-server group [groupname] v3 priv
snmp-server user [username] [groupname] auth [md5|sha] <auth-password> priv [aes
128] <priv-password>
```

Crosswork Cloud Traffic Analysis は、プライバシープロトコルに対してのみ SNMPv3 128 ビットをサポートします。

- (任意) **snmp-server view** コマンドを使用して、SNMPv3 アクセスを制限できます。次のコマンド例は、Crosswork Cloud Traffic Analysis によって読み取られる SNMP のオブジェクト識別子 (OID) を示しています。

```
snmp-server view [view_name] 1.3.6.1.2.1.1 included
snmp-server view [view_name] 1.3.6.1.2.1.2 included
snmp-server view [view_name] 1.3.6.1.2.1.31 included

snmp-server group [groupname] v3 [noauth|auth|priv] read [view_name]
```

## Cisco IOS デバイス用 BGP の構成例

次のコードは、Cisco IOS デバイスの BGP 構成の例です。



- (注) すべての BGP プレフィックスを Cisco Crosswork Data Gateway と共有する必要があります。

### Cisco IOS XE

```
router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
Crosswork Cloud UI
>>
bgp router-id <router-id>
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor <CDG-ipv4-address> remote-as <CDG-asn> << This must match the ASN of the CDG
in the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv4-address> description Cisco CrossWork Cloud CDG IPv4
neighbor <CDG-ipv4-address> ebgp-multihop 255
neighbor <CDG-ipv4-address> update-source <src-interface>
!
neighbor <CDG-ipv6-address> remote-as <CDG-asn> << This must match the ASN of the CDG
in the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv6-address> description Cisco CrossWork Cloud CDG IPv6
neighbor <CDG-ipv6-address> ebgp-multihop 255
neighbor <CDG-ipv6-address> update-source <src-interface>
!
address-family ipv4
neighbor <CDG-ipv4-address> activate
neighbor <CDG-ipv4-address> send-community both
neighbor <CDG-ipv4-address> filter-list 2 in
```

```

 neighbor <CDG-ipv4-address> filter-list 1 out
 exit-address-family
 !
 address-family ipv6
 neighbor <CDG-ipv6-address> activate
 neighbor <CDG-ipv6-address> send-community both
 neighbor <CDG-ipv6-address> filter-list 2 in
 neighbor <CDG-ipv6-address> filter-list 1 out
 exit-address-family
 !
 ip as-path access-list 1 permit .* <<All BGP prefixes from the device must be shared
 with Cisco CrossWork Cloud CDG>>
 ip as-path access-list 2 deny .*
 !

```

### Cisco IOS XR

```

router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
 Crosswork Cloud UI
>>
 bgp router-id <router-id>
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
 !
 neighbor <CDG-ipv4-address>
 remote-as <CDG-asn> << This must match the ASN of the CDG in the Crosswork Cloud
 UI. It should be a Private ASN number. >>

 ebgp-multihop 255
 description Cisco CrossWork Cloud CDG IPv4
 update-source <src-interface>
 address-family ipv4 unicast
 route-policy DROP in
 route-policy PASS out
 !
 neighbor <route-server-ipv6>
 remote-as <CDG-asn> << This must match the ASN of the CDG in the Crosswork Cloud UI.
 It should be a Private ASN number. >>

 ebgp-multihop 255
 description Cisco CrossWork Route Server IPv6
 update-source <src-interface>
 address-family ipv6 unicast
 route-policy DROP in
 route-policy PASS out
 !
 route-policy PASS
 pass
 end-policy
 !
 route-policy DROP
 drop
 end-policy
 !

```

### ここで

- <asn> は、ネットワークの BGP AS 番号です。
- <router-id> は、ネットワークの BPG ルータ ID です。

- <CDG-asn>は、CDG の BGP ASN 番号です。これは、プライベートASN番号である必要があります
- <src-interface> は、ネットワークの BGP 送信元インターフェイスです。
- <CDG-ipv4-address> は CDG の IPv4 アドレスです。
- <CDG-ipv6-address> は CDG の IPv6 アドレスです。

## Cisco IOS XR デバイス用 Netflow の構成例

次のコードは、Cisco IOS XR デバイス用 Netflow の構成例です。

### IPv4 の例 :

```
flow exporter-map ccni
packet-length 1468
version v9
 options sampler-table timeout 15
 template data timeout 15
 template options timeout 15
!
transport udp 2055
source GigabitEthernet0/0/0/0
destination 172.24.96.171 << this is the IP address of the CDG >>
!
flow monitor-map ccni
record ipv4
exporter ccni
cache entries 1000000
cache timeout active 12
cache timeout update 15
!
sampler-map ccni-sampler
random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
ipv4 address 172.24.96.141 255.255.255.128
flow ipv4 monitor ccni sampler ccni-sampler ingress
```

IPv4 接続を介して NetFlow IPv6 レコードをエクスポートする例 :



(注) この例では、192.0.2.169 が Crosswork Data Gateway の IPv4 アドレスです。

```
flow exporter-map ccni
packet-length 1468
version v9
 options sampler-table timeout 15
 template data timeout 15
 template options timeout 15
!
transport udp 2055
source GigabitEthernet0/0/0/0
destination 192.0.2.169 << this is the IP address of the CDG >>
!
flow monitor-map ccni-ipv6
record ipv6
```

```

exporter ccni
cache entries 1000000
cache timeout active 12
cache timeout update 15
!
sampler-map ccni-sampler
random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
ipv6 address 2001:100:100::1/64
flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress

```

### IPv4 および IPv6 の適用例 :

```

flow exporter-map ccni
packet-length 1468
version v9
options sampler-table timeout 15
template data timeout 15
template options timeout 15
!
transport udp 2055
source GigabitEthernet 0/0/0/0
destination 172.24.96.171 << this is the IP address of the CDG >>
!
flow monitor-map ccni
record ipv4
exporter ccni
cache entries 1000000
cache timeout active 12
cache timeout update 15
!
flow monitor-map ccni-ipv6
record ipv6
exporter ccni
cache entries 1000000
cache timeout active 12
cache timeout update 15

sampler-map ccni-sampler
random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0

ipv4 address 172.24.96.141 255.255.255.128
ipv6 address 2001:100:100::1/64
flow ipv4 monitor ccni sampler ccni-sampler ingress
flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress

```

## Cisco IOS XR デバイス用 IPFIX の構成例

次のコードは、Cisco IOS XR デバイス用 IPFIX の構成例です。

```

flow exporter-map ccni
packet-length 1468
version ipfix
options sampler-table timeout 15
template data timeout 15
template options timeout 15

```

```
!
transport udp 2055
source GigabitEthernet0/0/0/0
destination 172.24.96.184
!
flow monitor-map ccni
record ipv4
exporter ccni
cache entries 1000000
cache timeout active 3
cache timeout update 3
!
sampler-map ccni-sampler
random 1 out-of 1000
!
interface TenGigE0/0/0/16
description internal interface
ipv4 address 182.1.0.1 255.255.255.0
flow ipv4 monitor ccni sampler ccni-sampler ingress
!
interface TenGigE0/0/0/27
description external interface
ipv4 address 184.1.0.1 255.255.255.0
flow ipv4 monitor ccni sampler ccni-sampler ingress
```

## トラフィック分析で使用される SNMP の識別子

Crosswork Cloud Traffic Analysis の特定の SNMP ビューを作成する場合、次のリストに、Crosswork Cloud Traffic Analysis が使用する SNMP オブジェクト識別子 (OID) が含まれています。

- sysDescr : 1.3.6.1.2.1.1.1.0
- sysObjectID : 1.3.6.1.2.1.1.2.0
- sysUpTime : 1.3.6.1.2.1.1.3.0
- sysName : 1.3.6.1.2.1.1.5.0
- sysLocation : 1.3.6.1.2.1.1.6.0
- ifDescr : 1.3.6.1.2.1.2.2.1.2
- ifType : 1.3.6.1.2.1.2.2.1.3
- ifSpeed : 1.3.6.1.2.1.2.2.1.5
- ifOperStatus : 1.3.6.1.2.1.2.2.1.8
- ifName : 1.3.6.1.2.1.31.1.1.1.1
- ifHCSpeed : 1.3.6.1.2.1.31.1.1.1.15
- ifHCInOctets : 1.3.6.1.2.1.31.1.1.1.6
- ifHCOctets : 1.3.6.1.2.1.31.1.1.1.10

# Crosswork Traffic Analysis 用の外部インターフェ이스の指定

デバイスを追加したら、SNMP ステータスを確認し、1 つ以上のインターフェイスを外部インターフェイスとして設定する必要があります。Crosswork Cloud Traffic Analysis は、外部インターフェイスを指定するまでトラフィックデータを表示できません。

**ステップ 1** メインウィンドウで、[設定 (Configure)] > [デバイス (Devices)] の順にクリックします。

**ステップ 2** [デバイス (Device)] 列に表示されているデバイス名をクリックします。

**ステップ 3** Crosswork Data Gateway とデバイス間に表示される SNMP の上にカーソルを合わせて、ステータスが [接続済み (Connected)] になっていることを確認します。

デフォルトでは、すべてのインターフェイスが内部インターフェイスとして指定されています。デバイスの外部インターフェイスを選択し、外部として指定する必要があります。

**ステップ 4** [トラフィック分析 (Traffic Analysis)] タブをクリックしてから、[インターフェイス (Interfaces)] をクリックします。

**ステップ 5** 1 つ以上の外部インターフェイスを選択し、[外部の設定 (Set External)] をクリックします。

Crosswork Cloud Traffic Analysis は、インターフェイスを外部インターフェイスとして認識します。

# Crosswork Trust Insights にデバイスを追加するための前提条件

Cisco IOS XR ルータを Crosswork Cloud Trust Insights に追加する前に、次のルータ設定を確認する必要があります。

- デバイスに IOS XR の必要なサポートされるイメージがあることを確認します。サポートされるイメージについては、『[Cisco Crosswork Cloud Release Notes](#)』[英語]を参照してください。
- 登録キーと証明書が IOS XR 内で適切に生成されていることを確認します。詳細については、[Crosswork Trust Insights のルータ構成の確認 \(183 ページ\)](#)を参照してください。
- 制限付き特権ユーザを設定していることを確認します。詳細については、[Crosswork Trust Insights の制限付き権限のユーザの設定 \(186 ページ\)](#)を参照してください。



## Crosswork Trust Insights のルータ構成の確認

Crosswork Cloud Trust Insights を使用する前に、Cisco IOS XR ルータが信頼情報にアクセスできるように正しく設定されていることを確認する必要があります。次の手順に従って、ルータが Crosswork Cloud Trust Insights に正しく設定されていることを確認します。



(注) 次の例は、Crosswork Cloud Trust Insights を有効にするために必要な最小限の Cisco IOS XR 構成です。その他の構成例については、Crosswork Cloud Trust Insights を有効にするプラットフォームに対応する構成ガイドを参照してください。構成ガイドへの直接リンクについては、[関連ハードウェアのマニュアル](#)を参照してください。

**ステップ 1** ルータにログインし、次のコマンドを入力します。

```
ios# show running-config
```

**ステップ 2** 出力に次の構成要素が含まれていることを確認します。

- ホストネーム
- DNS ドメイン名 (DNS domain name)
- 有効化された SSH サーバ
- SSH で有効化された Netconf-yang
- インバウンド SSH アクセス用に設定され、到達可能な有効な IP インターフェイス
- 適切な静的デフォルトルートの設定

次の出力例は、表示される内容を示しています。

```
hostname xr9kv-001
domain name test.cisco.com
!
netconf-yang agent
 ssh
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 192.168.1.123 255.255.255.0
!
router static
 address-family ipv4 unicast
 0.0.0.0/0 192.168.1.1
!
!
ssh server v2
ssh server netconf vrf default
```

**ステップ 3** SSH でルータに到達できることを確認します。

**ステップ 4** system-root-key と system-enroll-key の両方のキーペアを生成するには、次の動作モードのコマンドを入力します。

```

RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-root-key
Tue Apr 21 22:45:55.400 UTC
The name for the keys will be: system-root-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-enroll-key
Tue Apr 21 22:46:24.943 UTC
The name for the keys will be: system-enroll-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]
RP/0/RP0/CPU0:xr9kv-001#

```

生成されたキーは Cisco IOS XR オペレーティングシステム内に安全に保存され、構成には表示されません。

**ステップ 5** Crosswork Cloud Trust Insights にルータを追加するために必要な証明書を生成して登録するには、次の構成を追加します。

```

crypto ca trustpoint system-trustpoint
 keypair rsa system-enroll-key
 ca-keypair rsa system-root-key
 ip-address 1.1.1.1
 subject-name CN=cisco.com
 lifetime certificate 720
 enrollment url self
 message-digest sha256
 lifetime ca-certificate 720
!
```

(注) 上記の例では、CA 証明書のライフタイムは 2 年（720 日）に設定され、登録証明書のライフタイムも 2 年に設定されています。

**ステップ 6** 署名操作と Crosswork Cloud Trust Insights への登録に必要な証明書を認証および登録するには、次のコマンドを入力します。

```

RP/0/RP0/CPU0:xr9kv-001#crypto ca authenticate system-trustpoint
Tue Apr 21 22:47:46.935 UTC
% The subject name in the certificate will include: xr9kv-001.test.cisco.com
 Serial Number : 25:34
 Subject:
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
 Issued By :
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
 Validity Start : 22:47:47 UTC Tue Apr 21 2020
 Validity End : 22:47:47 UTC Wed Apr 21 2021
 SHA1 Fingerprint:
 6C20DBEC569808F21A06E779A219C39B1F20E182
RP/0/RP0/CPU0:xr9kv-001#

```

```

RP/0/RP0/CPU0:xr9kv-001#crypto ca enroll system-trustpoint

```



```
Vesi57DQxgHlo2lk4EBsZsDv7oW9OsrTx7rib/kCyA5hTsEpw3oZ20Qp+91QY+vY7NUIQKx78RYkPiQNeOjQqibR0M1Rj
G1go4ZTDI4IxsdgXm/xxiX3scTqu1q/XVY3v5uEjT2zao0nZAU6z3PQKDSyHDxg3yIDskFMj74HI6hUJsA1U+Qj+mw9DcK
aypjQ8y7ZchLeeQQIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwID+DAgBgNVHSUBAf8EFjAUBgg
rBgEFBQcDAQYIKwYBBQUHAWIwHQYDVR0OBbYEFHJJ3dCXoGGWD2yZ8JQ3f/A/8XqxMA0GCSqGSIb3DQEBcWUAA4IBAQBm
z5YfGTbNAXPHJCxA9w8HUHyrlMlKB6wMKT0AUoWBj6HvXJXoA
H5cs7uF3Zw4QjY28HaaxkMPR6338VbGi3DnyIOf1Hc6/XRfNBi3eMYcSNyRRgtvQSmTzM7A3CrSOiFlMmdPCdYIeoFiMd
M3uIZzfMe1EnONeteV1bs+Te29utYXzb6QWjW0oJZ6/6g4cauo6jkhC/SNsRh3b/+8YMzxAHgzRFg+rm/O6cYa3jNCopjR
JqeFfmNuISgU9LIsmzkt3/4n4uiAj4aAqWAc7YG0dzWdwiXUwJ3Q7TrMS8R8AaLUN47nYzm0QfUwNbUDkST2XjIGV90J
vH3E2CnAX+j"]
}
}
```

これにより、信頼情報を取得するためにルータが正しく設定されていることが確認されます。

**ステップ 8** 署名操作で問題が発生した場合は、次のコマンドを使用して既存の証明書とキーをクリアします。

```
crypto key zeroize rsa <name of key>
clear crypto ca certificates system-trustpoint
crypto ca cancel-enroll system-trustpoint
```

**ステップ 9** 有効期限が切れる前に証明書を更新するには、次のコマンドを使用します。

```
clear crypto ca certificate system-trustpoint
crypto key zeroize rsa system-enroll-key
crypto key generate rsa system-enroll-key
crypto ca authenticate system-trustpoint
crypto ca enroll system-trustpoint
```

(注) 証明書を更新する前に登録キーを再生成します。署名 CA 証明書および登録証明書のライフタイムは、**crypto ca trustpoint**の構成を使用して設定されます。

## Crosswork Trust Insights の制限付き権限のユーザの設定

Cisco IOS XR ルータの不正操作または構成変更を防ぐには、デバイスへのアクセスに使用するクレデンシャルに制限付きの権限を付与する必要があります。trust dossier コマンドと signing コマンドを実行するために必要な最小限の許可を可能にするために、デバイスに次の構成（推奨されるタスクグループとユーザの構成など）があることを確認します。

Cisco IOS XR リリース 7.3.1 以降のリリースでは、次のコマンドがサポートされています。

```
!
taskgroup alltasks-dossier
task read sysmgr
task read system
task read dossier
task read pkg-mgmt
task read basic-services
task read config-services
task execute dossier
task execute basic-services
!
```

Cisco IOS XR リリース 7.3.1 より前のリリースでは、次のコマンドがサポートされています。

```
!
taskgroup alltasks-dossier
task read sysmgr
task read system
```

```

task read pkg-mgmt
task read basic-services
task read config-services
task execute crypto
task execute dossier
task execute basic-services
!
usergroup dossier-group
 taskgroup alltasks-dossier
!
username dossier
 group dossier-group
 secret 10 <not shown here>
!
```

この構成により、次のものが作成されます。

- ドシエの収集および署名操作を有効にするために必要なすべてのタスクを定義する **alltasks-dossier** タスクグループ。必要に応じてタスクグループの名前を変更できます。
- タスク権限が割り当てられる **dossier-group** ユーザグループ。必要に応じて、ユーザグループ名を変更できます。
- 適切なタスクグループ権限を持つ **dossier** ユーザ。必要に応じて、ユーザの名前を変更できます。適切なクレデンシャル（秘密）を指定していることを確認します。

この構成を適用すると、Crosswork Cloud Trust Insights でこの情報を使用して新しいクレデンシャルグループを作成できます。詳細については、「クレデンシャルの作成」を参照してください。

## Trust Insights の信頼ドシエ情報

Crosswork Cloud Trust Insights にデバイスを追加すると、信頼情報を含むドシエが Crosswork Data Gateway 経由でルータから取得されます。信頼ドシエ（json 形式）は SSH 経由で収集され、Crosswork Cloud Trust Insights 登録キーで署名されます。Crosswork Data Gateway が Crosswork Cloud Trust Insights に転送する信頼ドシエには、次の情報が含まれています。

- Cisco IOS のバージョンとプラットフォームの出力
- アンチリプレイナンス
- システム ハードウェア インベントリ
- ファイル システム インベントリ



(注) ファイル システム インベントリは、Cisco IOS XR リリース 7.9.1 以降のリリースでサポートされています。

- ハードウェアインベントリ用のセキュアな固有デバイス識別子（SUCI）証明書
- ソフトウェア パッケージ インベントリ

- リブート履歴
- ロールバック履歴

## Trust Insights のデバイスドシエのデータ収集

次の手順では、最新のデバイス情報を取得するためにアドホックドシエ収集を開始する方法について説明します。デフォルトでは、デバイスドシエ収集は 12 時間ごとに行われます。ドシエ収集頻度を変更する、または 1 つ以上のデバイスの収集を無効にするには、[デバイスドシエ収集頻度の変更 \(188 ページ\)](#) を参照してください。

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [設定 (Configure)] > [デバイス (Devices)] の順にクリックします。

**ステップ 2** ドシエの収集を実施するデバイスの名前をクリックします。

**ステップ 3** [トラストインサイト (Trust Insights)] タブをクリックします。

**ステップ 4** [ドシエの収集 (Collect Dossier)] をクリックします。

ドシエの収集が完了するまでに数分かかることがあることを示す Informational (情報提供) メッセージが表示され、[ドシエの収集 (Collect Dossier)] ボタンの下に要求に関するテキストが表示されます。

ドシエ収集が完了すると、UI でのデバイスデータが更新されます。

## デバイスドシエ収集頻度の変更

1 つ以上のデバイスのドシエ収集頻度を変更できます。



(注) この手順は Crosswork Cloud Trust Insights デバイスにのみ適用されます。

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [設定 (Configure)] > [デバイス (Devices)] の順にクリックします。

**ステップ 2** ドシエ収集の頻度を変更する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

**ステップ 3** [コレクション (Collection)] をクリックします。

(注) Crosswork Cloud は、Trust Insights デバイスのみを表示します。Trust Insights に属していないデバイスを選択した場合、そのデバイスは表示されません。

**ステップ 4** [有効 (Enabled)] / [無効 (Disabled)] トグルスイッチが [有効 (Enabled)] に設定されていることを確認します。[無効 (Disabled)] を選択すると、今後のドシエ収集が停止されます。

**ステップ 5** [頻度 (Frequency)] ドロップダウンリストから、収集を実行する頻度を選択します。デバイスの [新しい頻度 (New Frequency)] 列と [新しいステータス (New Status)] 列が適切に更新されることに注意してください。

**ステップ 6** [保存 (Save)] をクリックします。

## Trust Insights 用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング

次の手順では、Crosswork Data Gateway と Crosswork Cloud Trust Insights デバイス間の接続の問題を解決する方法について説明します。

**ステップ 1** メインウィンドウで、[デバイス (Devices)] をクリックしてから、Crosswork Data Gateway への接続を表示するデバイスをクリックします。

**ステップ 2** [ステータス (Status)] タブをクリックします。

**ステップ 3** Crosswork Data Gateway とデバイス間の接続がエラーを示す赤色で、ファイアウォールがある場合は、`cdg.crosswork.cisco.com` および `crosswork.cisco.com` を許可するように設定されていることを確認します。

Crosswork Data Gateway とデバイス間の接続をテストして修正します。

**ステップ 4** Crosswork Data Gateway とデバイス間の [SSH] の矢印が接続の正常性を示す緑色であることを確認します。[SSH] の矢印が赤色の場合、Crosswork Data Gateway はデバイスに接続できません。次のエラーを修正します。

- ルータの SSH 構成が正しいことを確認します。詳細については、[Crosswork Trust Insights のルータ構成の確認 \(183 ページ\)](#) を参照してください。
- Crosswork Cloud Trust Insights で入力したクレデンシャルが、ルータに設定されているクレデンシャルと一致していることを確認します。[SSH] リンクにカーソルを合わせ、青色のハイパーリンクをクリックして、そのデバイスのクレデンシャルに移動します。

**ステップ 5** Crosswork Data Gateway とデバイス間の [トラストデータ (Trust Data)] の矢印が接続の正常性を示す緑色であることを確認します。

## デバイスの無効化

デバイスを無効にすると、情報の収集が一時的に停止します。以前に収集されたデバイスデータは保持されます。

または、デバイスを削除して、デバイスとそのデータを完全に削除することもできます。デバイスを削除した後は、そのデータを回復できません。[デバイスの削除 \(190 ページ\)](#) を参照してください。

- 
- ステップ 1** メインウィンドウで、[モニタ (Monitor)] > [デバイス (Devices)] または [設定 (Configure)] > [デバイス (Devices)] をクリックします。
- ステップ 2** 非アクティブ化にする 1 つ以上のデバイスの横にあるチェックボックスをオンにし、[無効化 (Disable)] をクリックします。
- デバイスが非アクティブ化されたことを示すメッセージが表示されます。
- 以前に非アクティブ化されたデバイスを再アクティブ化できます。デバイスを再アクティブ化した後、デバイスの詳細ページに統計情報が表示されるまでに最大 30 分かかる場合があります。
- ステップ 3** デバイスのデータ収集を再開するには、デバイスを選択し、[有効化 (Enable)] をクリックします。
- デバイスがアクティブ化されたことを示すメッセージが表示され、デバイスのデータ収集が再開されます。
- 

## デバイスの削除

デバイスを削除すると、システムにより以前に収集されたすべてのデバイスデータが削除されます。デバイスを削除した後は、データを回復できません。

または、デバイスを無効にしてデータ収集を一時的に停止し、以前に収集したデバイスデータを保持することもできます。[デバイスの無効化 \(189 ページ\)](#) を参照してください。

- 
- ステップ 1** メインウィンドウで、[モニタ (Monitor)] > [デバイス (Devices)] または [設定 (Configure)] > [デバイス (Devices)] をクリックします。
- ステップ 2** 削除するデバイスの名前をクリックします。
- ステップ 3** [削除] をクリックします。
- ステップ 4** デバイスを削除することを確認するには、[削除 (Remove)] をクリックします。
- デバイスとその以前に収集されたデータが削除されます。
- ステップ 5** 最近削除されたデバイスを復元するには、[削除されたデバイスの復元 \(190 ページ\)](#) を参照してください。
- 

## 削除されたデバイスの復元

以前に削除したデバイスを復元できます。デバイスを削除すると、Crosswork Cloud は必要に応じてすぐに再度追加できるように、デバイスを約 7 日間記憶します。

- 
- ステップ 1** メインウィンドウで、[設定 (Configure)] > [デバイスの削除 (Removed Devices)] の順にクリックします。



デバイスを削除してから7日を超える場合、[削除済みデバイス (Removed Devices)] のリストに表示されないことがあります。[デバイスの追加 \(173 ページ\)](#) の説明に従って、デバイスを再度追加する必要があります。

**ステップ 2** 再度追加するデバイスの横にある [復元 (Restore)] をクリックします。

デバイスが復元されます。

---





## 第 20 章

# Crosswork Data Gateways の設定

- [Crosswork Data Gateway のインストール](#) (193 ページ)
- [Crosswork Data Gateway の情報の追加](#) (194 ページ)
- [Data Gateway の正常性の表示](#) (195 ページ)
- [トラフィックデバイスと Crosswork Data Gateway とのリンク](#) (195 ページ)
- [トラフィックデバイスと Crosswork Data Gateway とのリンクの削除](#) (196 ページ)
- [トラフィック分析用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング](#) (196 ページ)
- [Crosswork Data Gateway へのデバイスのリンク](#) (198 ページ)
- [Crosswork Data Gateway へのデバイスリンクの削除](#) (198 ページ)
- [Crosswork Data Gateways の非アクティブ化](#) (199 ページ)
- [Crosswork Data Gateways の削除](#) (199 ページ)

## Crosswork Data Gateway のインストール



(注) Crosswork Data Gateway は Crosswork Cloud Traffic Analysis と Crosswork Cloud Trust Insights にも必要です。Crosswork Cloud Network Insights には必要ありません。

Crosswork Cloud はそのデータに依存しているため、最初に Crosswork Data Gateway をインストールする必要があります。Crosswork Cloud でサポートされている Crosswork Data Gateway のバージョンについては、[Cisco Crosswork Data Gateway Release Notes](#) を参照してください。

**ステップ 1** [Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications](#) の説明に従って Crosswork Data Gateway をインストールします。

**ステップ 2** [Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications](#) の説明に従って Crosswork Data Gateway から [登録パッケージの取得とエクスポート](#) します。

Crosswork Data Gateway の登録データを取得したら、Crosswork Cloud にログインできます。



## Crosswork Data Gateway の情報の追加

クラウドデータゲートウェイの展開プロセスの一環として、新しい仮想マシンを展開した後に一意の登録ファイルが作成されます。json 登録ファイルには、Crosswork Data Gateway を Crosswork Cloud に登録する際に使用される一意のデジタル証明書が含まれています。Crosswork Data Gateway をインストールして登録データをダウンロードしたら、次に説明するようにその情報を追加する必要があります。



(注) Crosswork Data Gateway の出力トラフィックでファイアウォールを使用する場合は、ファイアウォールの構成で `cdg.crosswork.cisco.com` および `crosswork.cisco.com` が許可されていることを確認します。

**ステップ 1** メインウィンドウから、次のいずれかを実行します。

- Crosswork Cloud Traffic Analysisについては、 > [設定 (Configure)] > [データゲートウェイ (Data Gateways)] の順に選択してから、[データゲートウェイの追加 (Add Data Gateway)] をクリックします。
- Crosswork Cloud Trust Insightsについては、 > [設定 (Configure)] > [データゲートウェイ (Data Gateways)] の順に選択してから、[データゲートウェイの追加 (Add Data Gateway)] をクリックします。

**ステップ 2** [登録 (Registration File)] をクリックして、Crosswork Data Gateway からダウンロードした登録データファイルをアップロードし、.json ファイルの場所に移動してから、[次へ (Next)] をクリックします。

**ステップ 3** Crosswork Data Gateway の名前を入力します。

**ステップ 4** [アプリケーション (Application)] フィールドで、この Crosswork Data Gateway インスタンスを使用している該当 Crosswork Cloud アプリケーションが正しいものかどうか確認します。各 Crosswork Data Gateway は、1 つの Crosswork Cloud アプリケーションにのみ適用できます。

**ステップ 5** 残りの必須フィールドに入力してから、[次へ (Next)] をクリックします。

**ステップ 6** (オプション) タグ名を入力し、[新しい項目 (New Item)] をクリックします (または既存のタグ名から選択します)。これにより、同じタグを持つ Crosswork Data Gateway をグループ化できます。その後、[次へ (Next)] をクリックします。

**ステップ 7** 複数の NIC があり、そのうちの 1 つをサウスバウンドトラフィックと通信するようにする場合は、このウィンドウで設定します。

**ステップ 8** 入力した Crosswork Data Gateway の情報を確認してから、[次へ (Next)] をクリックします。

**ステップ 9** [承認 (Accept)] をクリックして、セキュリティ証明書を受け入れます。

Crosswork Data Gateway の追加に成功したことを示すメッセージが表示されます。

**ステップ 10** 数分後、Crosswork Data Gatewayが正常に接続されていることを確認します。[データゲートウェイ (Data Gateways)] をクリックし、続けて Crosswork Data Gateway の名前をクリックして、追加した Crosswork Data Gateway について次の値を確認します。

- [接続 (Connectivity)] : [セッションアップ (Session Up)]
- 管理状態 : 有効
- コンテナイメージ : 一致

変更を表示するには、更新が必要な場合があります。

## Data Gateway の正常性の表示

Crosswork Data Gateway インスタンスの正常性をすばやく表示できます。メインウィンドウの [設定 (Configure)] で、[データゲートウェイ (Data Gateways)] をクリックします。正常性を表示する Crosswork Data Gateway インスタンスをクリックします。

Crosswork Data Gateway の収集情報と正常性情報が表示されます。接続ステータス、アプリケーションがダウンロードされた日時、および最後のデータ収集が行われた日時を表示できます。

[コンテナイメージ (Container Image)] フィールドは、次の値を使用して Docker イメージのステータスを示します。

- [一致 (Matched)] : Data Gateway は公開されている最新の Docker イメージを実行しています。
- [不一致 (Mismatched)] : Data Gateway は古い Docker イメージを実行しています。
- [なし (Missing)] : Docker イメージがダウンロードされていません。

[コンテナイメージ (Container Image)] フィールドの上にマウスを合わせて、Docker イメージタグを表示することもできます。

## トラフィックデバイスと Crosswork Data Gateway とのリンク

追加した各デバイスのドシエを収集する Crosswork Data Gateway インスタンスを選択できます。このタスクを実行する前に、Crosswork Data Gateway を追加する必要があります。参照先

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** デバイスにリンクする Crosswork Data Gateway インスタンスをクリックします。

**ステップ 3** [リンクされたトラフィックデバイス (Linked Traffic Devices)] タブをクリックします。

以前に Crosswork Data Gateway にリンクされていたデバイスのリストが表示されます。

**ステップ 4** Crosswork Data Gateway にリンクするデバイスを選択し、[トラフィックデバイスのリンク (Link Traffic Devices)] をクリックします。

デバイスが Crosswork Data Gateway にリンクされると、自動的に収集がスケジュールされます。収集のステータスと次の収集間隔を確認するには、[データゲートウェイ (Data Gateway)] ページの [概要 (Overview)] タブを確認します。

---

## トラフィックデバイスと Crosswork Data Gateway とのリンクの削除

以前に設定した Crosswork Data Gateway へのデバイスリンクを削除できます。

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** デバイスへのリンクを解除する Crosswork Data Gateway インスタンスをクリックします。

**ステップ 3** [リンクされたトラフィックデバイス (Linked Traffic Devices)] タブをクリックします。

**ステップ 4** リンクを解除する 1 つ以上のデバイスのチェックボックスをオンにし、[リンク解除 (Unlink)] をクリックします。

Crosswork Data Gateway では、リンクを解除したデバイスのドシエは収集されなくなります。

---

## トラフィック分析用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング

次の手順では、Crosswork Data Gateway と Crosswork Cloud Traffic Analysis デバイス間の接続の問題を解決する方法について説明します。

**ステップ 1** メインウィンドウで、[デバイス (Devices)] をクリックしてから、Crosswork Data Gateway への接続を表示するデバイスをクリックします。

**ステップ 2** [ステータス (Status)] タブをクリックします。

**ステップ 3** Crosswork Data Gateway とデバイス間のすべての接続がエラーを示す赤色で、ファイアウォールがある場合は、`cdg.crosswork.cisco.com` および `crosswork.cisco.com` を許可するように設定されていることを確認します。

Crosswork Data Gateway とデバイス間の接続をテストして修正します。

**ステップ 4** Crosswork Data Gateway とデバイス間の [SNMP] の矢印が接続の正常性を示す緑色であることを確認します。

[SNMP] の矢印が赤色の場合、Crosswork Data Gateway はデバイスに接続できません。次のエラーを修正します。

- ルータの SNMP 構成が正しいことを確認します。詳細については、[SNMP の構成例 \(176 ページ\)](#) を参照してください。
- Crosswork Cloud Traffic Analysis で入力したクレデンシャルが、ルータに設定されているクレデンシャルと一致していることを確認します。[SNMP] リンクの上にカーソルを合わせ、青色のハイパーリンクをクリックして、そのデバイスのクレデンシャルに移動します。
- SNMP ビューを作成した場合は、正しい SNMP のオブジェクト識別子 (OID) を指定したことを確認します。[トラフィック分析で使用される SNMP の識別子 \(181 ページ\)](#) を参照してください。
- 入力した SNMP の IP アドレスが正しいことを確認してください。[編集 (Edit) ] をクリックし、Crosswork Cloud Traffic Analysis セクションまでスクロールして [SNMP アドレス (SNMP Address) ] フィールドを確認します。

**ステップ 5** Crosswork Data Gateway とデバイス間の [BGP] の矢印が、接続の正常性を示す緑色であることを確認します。

[BGP] の矢印が赤色の場合は、次のエラーを修正します。

- BGP ピアの IP アドレスが正しいことを確認します。[編集 (Edit) ] をクリックし、Crosswork Cloud Traffic Analysis セクションまでスクロールして、[BGP ルータ ID の IP アドレス (BGP Router ID IP Address) ] フィールドを確認します。
- BGP のクレデンシャルを使用している場合は、Crosswork Cloud Traffic Analysis で入力したクレデンシャルがルータで設定されているクレデンシャルと一致していることを確認します。
- デバイス構成に Crosswork Data Gateway の IP アドレスと Crosswork Data Gateway の ASN (デフォルトの ASN は 65000) が含まれていること、およびそれらがネイバーであることを確認します。
- Crosswork Data Gateway とデバイス間の BGP セッションが外部 BGP (e-BGP) セッションであることを確認します。

(注) Crosswork Data Gateway とデバイス間の [SSH] 接続は、Crosswork Cloud Traffic Analysis には必要ありません。

**ステップ 6** Crosswork Data Gateway とデバイス間の [トラフィックデータ (Traffic Data) ] の矢印が、接続の正常性を示す緑色であることを確認します。

Crosswork Data Gateway とデバイス間の [トラフィックデータ (Traffic Data) ] の矢印が赤色の場合は、ルータの NetFlow 構成、特にポート番号 (255) と NetFlow データのエクスポート元の IP アドレスを確認します。[NetFlow 送信元アドレス (NetFlow Source Address) ] フィールドで指定した IP アドレスが、NetFlow レコードのエクスポート元の IP アドレスと一致していることを確認します。

**ステップ 7** すべての接続が緑色で、トラフィックデータが表示されない場合は、内部インターフェイスと外部インターフェイスが正しく設定されていることを確認します。[Crosswork Traffic Analysis 用の外部インターフェイスの指定 \(182 ページ\)](#) を参照してください。

---

## Crosswork Data Gateway へのデバイスのリンク

Crosswork Cloud Trust Insights または Crosswork Cloud Traffic Analysis に追加した各デバイスのドシエを収集する Crosswork Data Gateway インスタンスを選択できます。このタスクを実行する前に、Crosswork Data Gateway を追加する必要があります。[Crosswork Data Gateway の情報の追加 \(17 ページ\)](#) を参照してください。

---

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** デバイスにリンクする Crosswork Data Gateway インスタンスをクリックします。

**ステップ 3** [リンクされた信頼デバイス (Linked Trust Devices)] または [リンクされたトラフィックデバイス (Linked Traffic Devices)] タブをクリックします。

以前に Crosswork Data Gateway にリンクされていたデバイスのリストが表示されます。

**ステップ 4** [信頼デバイスのリンク (Link Trust Devices)] または [トラフィックデバイスのリンク (Link Traffic Devices)] をクリックします。

**ステップ 5** Crosswork Data Gateway にリンクするデバイスを選択し、[選択したリンク (Link Selected)] をクリックします。

デバイスが Crosswork Data Gateway にリンクされると、自動的に収集がスケジュールされます。収集のステータスと次の収集間隔を確認するには、[データゲートウェイ (Data Gateway)] ページの [概要 (Overview)] タブを確認します。

---

## Crosswork Data Gateway へのデバイスリンクの削除

以前に設定した Crosswork Data Gateway へのデバイスリンクを削除できます。

---

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** デバイスへのリンクを解除する Crosswork Data Gateway インスタンスをクリックします。

**ステップ 3** [リンクされた信頼デバイス (Linked Trust Devices)] または [リンクされたトラフィックデバイス (Linked Traffic Devices)] タブをクリックします。

**ステップ 4** リンクを解除するデバイスのボックスをオンにしてから、[リンク解除 (Unlink)] をクリックします。



Crosswork Data Gateway では、リンクを解除したデバイスのドシエは収集されなくなります。

---

## Crosswork Data Gateways の非アクティブ化

Crosswork Data Gateway を非アクティブ化することができます。これにより、Crosswork Data Gateway の情報は保持されますが、Crosswork Data Gateway が Crosswork Cloud にネットワークデータを送信することはできなくなります。

Crosswork Data Gateway を削除して、そのデータとともに完全に削除するには、[Crosswork Data Gateways の削除 \(199 ページ\)](#) を参照してください。

---

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** 非アクティブ化する Crosswork Data Gateway インスタンスをクリックしてから、[非アクティブ化 (Deactivate)] をクリックします。

---

## Crosswork Data Gateways の削除

Crosswork Data Gateway を削除することで、完全に削除できます。また、Crosswork Data Gateway を非アクティブ化することもできます。これにより、Crosswork Data Gateway の情報は保持されますが、Crosswork Data Gateway はネットワークデータを Crosswork Cloud に送信できなくなります。

---

**ステップ 1** メインウィンドウで、[データゲートウェイ (Data Gateways)] をクリックします。

**ステップ 2** 削除する Crosswork Data Gateway インスタンスをクリックします。

**ステップ 3** [削除 (Remove)] をクリックします。Crosswork Data Gateway は削除されます。

---





## 第 21 章

# 複数の宛先への NetFlow トラフィックの送信

- [複数の宛先への NetFlow トラフィックの送信 \(201 ページ\)](#)

## 複数の宛先への NetFlow トラフィックの送信

リソースを節約するために、すべての NetFlow データを 1 つの宛先 (Crosswork Data Gateway など) に送信し、他のデバイスに転送することができます。Crosswork Traffic Analysis を使用すると、NetFlow トラフィックを複数の IPv4 アドレスの宛先に転送できます。



- (注) OpenStack プラットフォーム (OSP) を使用して Crosswork Data Gateway が展開されている場合、この機能はサポートされません。

**ステップ 1** Crosswork Traffic Analysis から、**[設定 (Configure)]** > **[フローレプリケーション (Flow Replication)]** をクリックします。

**ステップ 2** **[追加 (Add)]** をクリックします。

**ステップ 3** グローバル転送アドレスを入力します。グローバル転送アドレスに加えて、データゲートウェイとデバイスを指定できます。

- (注) Crosswork Traffic Analysis は、最も詳細な設定を優先します。たとえば、Crosswork Traffic Analysis は、データゲートウェイ設定よりもデバイス設定を優先します。

**ステップ 4** **[保存 (Save)]** をクリックします。





## 第 22 章

# クレデンシャルの設定

---

- [クレデンシャルの作成](#) (203 ページ)
- [クレデンシャルの編集](#) (203 ページ)
- [デバイスとクレデンシャルとのリンク](#) (204 ページ)

## クレデンシャルの作成

デバイスごとにこの情報を手動で入力する代わりに、デバイスのグループ間で共有されるクレデンシャルを指定できます。クレデンシャルを作成すると、実稼働環境で複数のルータが単一のログインクレデンシャルを利用できます。このログインクレデンシャルは、TACACS+ や RADIUS などの外部認証サービスで定義できます。

- 
- ステップ 1** メインウィンドウで、[Configure (設定)] > [クレデンシャル (Credentials)] の順にクリックします。
  - ステップ 2** [クレデンシャルの追加 (Add Credential)] をクリックします。
  - ステップ 3** クレデンシャルの名前を入力してから、クレデンシャルタイプを選択し、必須フィールドに入力します。
  - ステップ 4** [保存 (Save)] をクリックします。

これで、追加したデバイスにこのクレデンシャルを適用できます。

---

## クレデンシャルの編集

以前に作成したクレデンシャルを編集できます。

---

- ステップ 1** メインウィンドウで、[Configure (設定)] > [クレデンシャル (Credentials)] の順にクリックします。
- ステップ 2** 編集するクレデンシャルの名前をクリックします。
- ステップ 3** [編集 (Edit)] をクリックします。
- ステップ 4** 必要な変更を行い、[保存 (Save)] をクリックします。

**ステップ 5** このクレデンシャルにデバイスをリンクするには、[デバイスのリンク (Link Devices) ] をクリックします。

クレデンシャルが変更内容で更新されます。

---

## デバイスとクレデンシャルとのリンク

以前に追加したデバイスをクレデンシャルグループにリンクできます。これにより、選択したデバイスに以前に割り当てられたクレデンシャルが上書きされます。

---

**ステップ 1** メインウィンドウで、[Configure (設定) ] > [クレデンシャル (Credentials) ] の順にクリックします。

**ステップ 2** デバイスをリンクするクレデンシャルの名前をクリックします。

選択したクレデンシャルにリンクできるデバイスが表示されます。指定したクレデンシャルがデバイスに対して有効でない場合、デバイスはリストに表示されません。

**ステップ 3** [デバイスのリンク (Link Devices) ] をクリックします。

**ステップ 4** クレデンシャルにリンクするデバイスを 1 つ以上選択し、[リンク (Link) ] をクリックします。

---



## 第 23 章

# デバイスグループの設定

---

・ [デバイスグループの作成 \(205 ページ\)](#)

## デバイスグループの作成

デバイスグループを作成すると、同様のデバイスタイプのグループでアクションを表示および実行できます。デバイスは、1つのデバイスグループにのみ属することができます。

- 
- ステップ1 メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [設定 (Configure)] > [デバイスグループ (Device Groups)] の順にクリックします。
  - ステップ2 [デバイスグループの追加 (Add Device Group)] をクリックします。
  - ステップ3 デバイスグループの名前と説明 (任意) を入力します。
  - ステップ4 [保存 (Save)] をクリックします。
  - ステップ5 作成したばかりのデバイスグループの名前をクリックします。
  - ステップ6 デバイスグループにデバイスを追加するには、[デバイスのリンク (Link Devices)] をクリックします。
  - ステップ7 デバイスグループに追加するデバイスを選択し、[リンク (Link)] をクリックします。

デバイスは、1つのデバイスグループにのみ属することができます。以前に別のデバイスグループに追加されたデバイスがある場合、それらのデバイスは前のデバイスグループから削除され、選択したデバイスグループに追加されます。

---







## 第 24 章

# 既知の適正なファイルの設定

- [既知の適正なファイルについて \(207 ページ\)](#)
- [既知の適正なファイルの追加 \(207 ページ\)](#)
- [既知の適正なファイルの無効化 \(208 ページ\)](#)
- [既知の適正なファイルの削除 \(208 ページ\)](#)

## 既知の適正なファイルについて

Crosswork Cloud Trust Insights は、Cisco IOS XR ルータからの既知の適正な値 (KGV) の測定の完全性を自動的に解釈して確認します。また、Crosswork Cloud Trust Insights では、自己確認済みで既知の適正なデータがあると認定済みのファイルを指定することもできます。

既知の適正なファイルのリストを維持することで、デバイスが想定どおりの構成で動作していることを確認できます。詳細については、[既知の適正なファイルの追加 \(207 ページ\)](#) を参照してください。

## 既知の適正なファイルの追加

既知の適正なファイルを Crosswork Cloud Trust Insights に追加することで、それらをより簡単に見つけて追跡できます。

- ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [設定 (Configure)] > [既知の適正なファイル (Known Good Files)] の順にクリックします。
- ステップ 2** [ファイルの追加 (Add File)] をクリックします。
- ステップ 3** 既知の適正なファイルを保存するデバイスを選択します。
- ステップ 4** デバイステーブルをフィルタリングするには、[フィルタの追加 (Add Filter)] をクリックし、フィルタ値を入力してから、[保存 (Save)] をクリックします。
- ステップ 5** デバイスを選択してから、[次へ (Next)] をクリックします。

Crosswork Cloud Trust Insights では、指定したデバイスのドシエ収集のリストが表示されます。

**ステップ 6** 特定のタイムフレームのドシエ収集を検索するには、[タイムフレーム (Timeframe)] ドロップダウンリストから値を選択します。

デバイスで署名キーが変更された場合は、ドシエ収集の横にオレンジ色のアイコンが表示されます。アイコンの上にカーソルを合わせると、変更内容に関する詳細が表示されます。

**ステップ 7** ドシエ収集を選択して、[次へ (Next)] をクリックします。

Crosswork Cloud Trust Insights では、既知のものとは異なる KGV を持つファイルのリストが表示されます (最大 1,000 ファイル)。

**ステップ 8** 既知の適正なファイルとして指定する 1 つ以上のファイル (最大 1,000 ファイル) を選択し、[送信 (Submit)] をクリックします。

1,000 を超えるファイルを追加するには、必要に応じてステップ 8 を繰り返します。

選択したファイルが既知の適正なファイルのテーブルに表示されます。

---

## 既知の適正なファイルの無効化

以前に追加した既知の適正なファイルが無効にすることができます。既知の適正なファイルを削除するかどうか定かではない場合は、そのファイルが無効にして既知の適正なファイルのテーブルに残すことができますが、システムは既知の適正なファイルを認識しなくなります。

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [設定 (Configure)] > [既知の適正なファイル (Known Good Files)] の順にクリックします。

**ステップ 2** 1 つ以上のファイルを選択し、[無効化 (Disable)] をクリックします。

Crosswork Cloud Trust Insights は、ファイルの状態を [無効 (Disabled)] に変更します。

---

## 既知の適正なファイルの削除

以前に追加された既知の適正なファイルは削除できます。既知の適正なファイルを削除するかどうか不明な場合は、無効にすることができます。詳細については、[既知の適正なファイルの無効化 \(208 ページ\)](#) を参照してください。

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [設定 (Configure)] > [既知の適正なファイル (Known Good Files)] の順にクリックします。

**ステップ 2** 1 つ以上のファイルを選択し、[削除 (Remove)] をクリックします。

**ステップ 3** 既知の適正なファイルを削除することを確認するには、[削除 (Remove)] をクリックします。

---





## 第 25 章

# レポートの設定

ここでは、次の内容について説明します。

- [ASN ルーティングレポートの設定 \(211 ページ\)](#)
- [オンデマンドでのレポートの生成 \(213 ページ\)](#)

## ASN ルーティングレポートの設定

ASN ルーティングレポートには、自律システムのルートアナウンスとピアリング関係の変更の概要がわかりやすく表示されます。ASN ルーティングレポートは、ASN の現在の状態をキャプチャし、最後のレポートインスタンスが生成された時点からの変更を強調表示します。レポートは毎日実行されますが、オンデマンドでトリガーすることもできます。

Crosswork Cloud は、選択した ASN の次の情報を収集して保持します。

- プレフィックス BGP アナウンス
- ASN ピア
- RIR、ROA、および RPSL プレフィックス情報

レポートインスタンスをエンドポイントに送信するだけでなく、その内容を UI で表示できます。詳細については、[日次 ASN 変更の表示 \(ASN ルーティングレポート\) \(55 ページ\)](#) を参照してください。

### 特記事項

- レポートは、レポート設定を参照します。レポートインスタンスは、レポートの1つのインスタンスを実行した結果であり、生成されたデータが含まれます。
- レポートインスタンスが生成されるたびに、最後に生成されたレポートとデータが比較されます。レポートインスタンスには、最後のレポートからの変更の要約が含まれます。最後に生成されたレポートは、日次レポートまたは手動で生成されたレポートのいずれかです。
- 個々のレポートインスタンスは 30 日間保存され、その後システムから削除されます。

- レポート設定ごとに保存できるレポートインスタンスの合計数は30に制限されています。レポートインスタンスの合計には、日次レポートとオンデマンドで生成されたレポートの両方が含まれます。詳細については、[オンデマンドでのレポートの生成 \(213 ページ\)](#) を参照してください。
- ASN ルーティングレポートを無効にすると ([外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [レポート (Reports)] をクリックし、ASN ルーティングレポート名をクリックして [無効 (Disable)] を選択)、日次レポートインスタンスが今後生成されないようにすることができます。エージアウトしない限り、以前のすべてのレポートインスタンスは引き続き使用できます。ただし、ASN ルーティングレポートを削除すると ([外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [レポート (Reports)] をクリックし、ASN ルーティングレポート名をクリックして [削除 (Delete)] を選択)、以前のレポートインスタンスもすべて削除されます。
- 後でレポート設定に関連付けられている ASN の登録を解除すると、新しいレポートインスタンスは生成されません。ただし、以前のレポートインスタンスは引き続き表示できます。
- 有料の Crosswork Cloud サブスクリプションが期限切れになると、レポートインスタンスはエージアウトして、削除されます。
- レポート設定をインポートまたはエクスポートすることもできます。詳細については、[構成ファイルのインポートとエクスポート \(251 ページ\)](#) を参照してください。

### 始める前に

レポートを設定する前に、対象の ASN に登録する必要があります。詳細については、[ASN の設定 \(91 ページ\)](#) を参照してください。

- 
- ステップ 1** 対象の ASN に登録していることを確認します。
- ステップ 2** メインメニューで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [レポート (Reports)] の順にクリックします。
- ステップ 3** [追加 (Add)] をクリックします。
- ステップ 4** [名前 (Name)] フィールドにレポート名を入力します。レポートが生成されると、そのレポートインスタンスの名前は「<report name>-<month>-<day>-<timestamp>」になります。たとえば、レポート名を ASN7100 に設定し、レポートインスタンスが 2021 年 7 月 4 日 10:00 UTC に生成された場合、そのレポートインスタンスに付けられる名前は ASN7100-Jul-04-10:00-UTC です。
- ステップ 5** ASN とタグを入力します。
- ステップ 6** [エンドポイントの追加 (Add Endpoint)] をクリックし、日次レポートの送信先となるエンドポイントを追加します。
- (注) S3 エンドポイント設定はサポートされていません。
- ステップ 7** [保存 (Save)] をクリックします。最初のレポートは、指定したエンドポイントに翌日に送信されます。
-

# オンデマンドでのレポートの生成

日次レポートに加えて、オンデマンドでレポートを生成できます。このレポートには、最後に生成されたレポート以降の変更がリストされます。

## 始める前に

レポートを手動で生成する前に、ASNルーティングレポートを設定する必要があります。詳細については、[ASNルーティングレポートの設定 \(211 ページ\)](#) を参照してください。

- 
- ステップ 1** メインウィンドウで、[外部ルーティング分析 (External Routing Analytics)] > [設定 (Configure)] > [レポート (Reports)] の順にクリックします。
  - ステップ 2** 設定済みのレポート名をクリックします。
  - ステップ 3** [生成 (Generate)] をクリックします。
  - ステップ 4** この特定のレポートインスタンスの一意のレポート名を入力し、[レポートの生成 (Generate Report)] をクリックします。

(注) 名前が入力されていない場合、Crosswork Cloud は自動的に名前を生成します (<configured-report-name>-<month>-<day>-<timestamp>)。たとえば、設定された日次レポート名が ASN7100 で、手動レポートインスタンスが 2021 年 7 月 4 日 10:00 UTC に生成された場合、そのレポートインスタンスに付けられる名前は ASN7100-Jul-04-10:00-UTC です。

- ステップ 5** [レポート処理に進む (Go To Reports)] をクリックし、[レポートステータス (Report Status)] が [処理中 (In Progress)] であることを確認します。通常、レポートは 5 分以内に生成されます。レポートの準備が整うと、[レポート (Reports)] ページが自動的に更新されます。

---

## 次のタスク

[日次 ASN 変更の表示 \(ASN ルーティングレポート\) \(55 ページ\)](#)







## 第 **V** 部

# Crosswork 外部分析ツールを使用する

- [プレフィックスパストポロジの表示 \(217 ページ\)](#)





## 第 26 章

# プレフィックスパストポロジの表示

- [プレフィックスパストポロジの表示 \(217 ページ\)](#)
- [パストポロジの変更を比較 \(220 ページ\)](#)

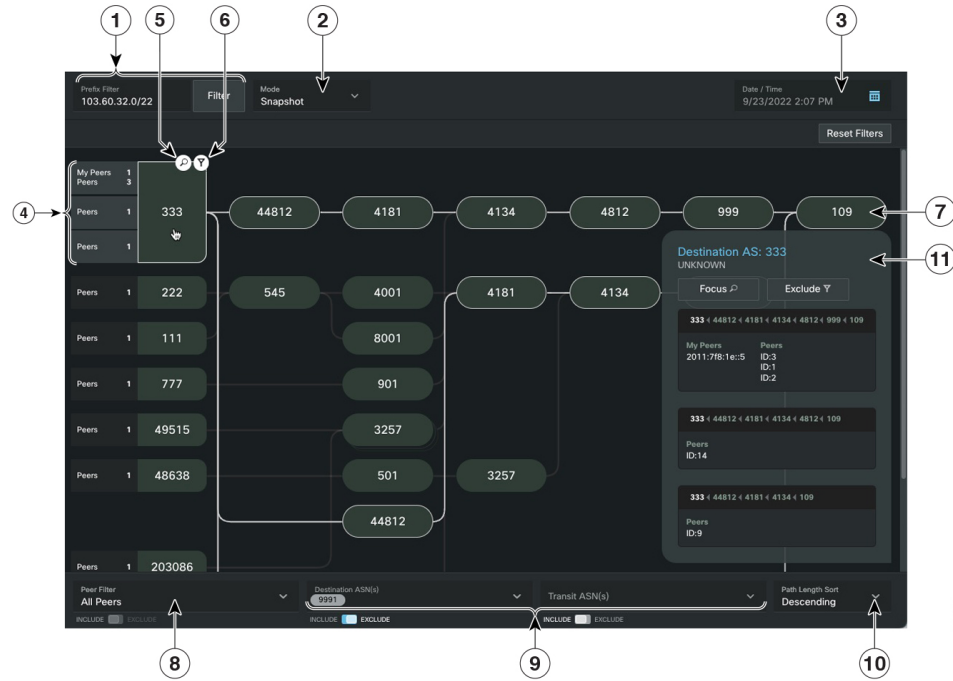
## プレフィックスパストポロジの表示

パストポロジツールは、選択した時間にプレフィックスの AS パスでアドバタイズされるすべてのピア、トランジット、および発信元 ASN の要約トポロジビューを表示します。また、プレフィックスパストポロジを視覚化すると、特定の基準を満たす AS パスを特定することにより、パスの優先順位の変更など、ネットワーク計画の関連事項を決定するときにも役立ちます。マイピアが定義されている場合 ([構成 (Configure)] > [ピア (Peers)] > [ピアの追加 (Add Peers)] )、視覚的な支援により、すぐに概要が表示され、担当しているピアの BGP の不良構成を簡単に識別して対処することができます。もう 1 つの利点としては、ステートフルな URL により、フィルタ処理されたビューを簡単に共有できることです。トポロジビューに適用されるすべてのタイプの並べ替えまたはフィルタには、特定の URL が割り当てられ、共有できません。

- ステップ 1** メインウィンドウで、[外部ルートの分析 (External Routing Analysis)] > [ツール (Tools)] > [パストポロジ (Path Topology)] をクリックします。
- ステップ 2** プレフィックスを入力して、[表示 (View)] をクリックします。このページには、入力したプレフィックスと、デフォルトでは現在の時刻でフィルタリングされたパストポロジが表示されます。パスは、ASN 宛先から送信元まで (左から右へ) 表示されます。個々の ASN を強調表示すると、関連するパスが強調表示されます。

例

図 3: Path Topology



(注) このガイドのHTMLバージョンを表示している場合は、画像をクリックしてフルサイズで表示してください。

| 引き出し線番号 | 説明                                                                                                                                                                                                                                                                                                  |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | パストポロジは、ここに入力されたプレフィックスに基づいてフィルタリングされます。新しいプレフィックスを入力するたびに、[フィルタ (Filter)] をクリックして結果を表示します。                                                                                                                                                                                                         |
| 2       | [スナップショット (Snapshot)] モードでは、[日時 (Date/Time)] フィールドに表示されている時刻の ASN パストポロジが表示されます。<br><br>[時間比較 (Time Comparison)] モードでは、2つのタイムスタンプ間の変化を比較できます。このモードが選択されている場合は、ベースラインと比較の日付を選択します。パストポロジは、ベースラインの日付から比較の日付までに発生したパス、ノード、およびピアの変更を表示して示します。詳細については、 <a href="#">パストポロジの変更を比較 (220 ページ)</a> を参照してください。 |



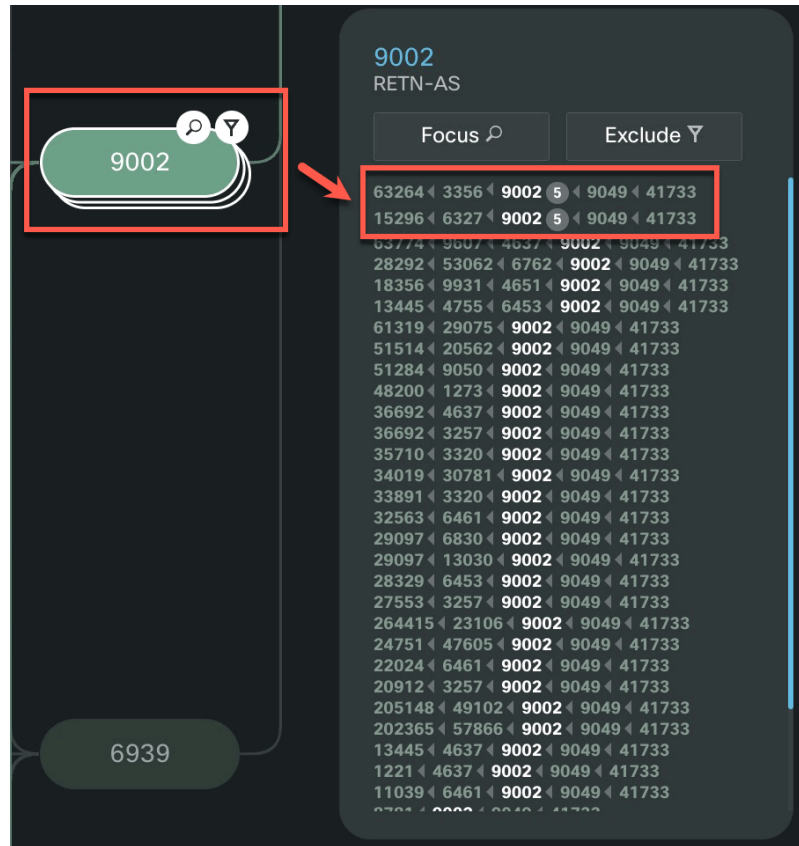
| 引き出し線番号 | 説明                                                                                                                                                                                                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3       | 選択した日時のプレフィックスパストポロジビューを表示します。この領域をクリックして、表示する他の日付と時刻を設定します。                                                                                                                                                                                                                                                               |
| 4       | 同じ宛先ASNを持つ特定のパスをアドバタイズするピアの数を要約します。この例では、3つのパスがあります。ピアとパスの詳細を確認するには、宛先ASNをクリックします。                                                                                                                                                                                                                                         |
| 5       |  をクリックして、選択したASNのみを含むパスに注目します。このASNが含まれていない他のすべてのパスは、トポロジから削除されます。                                                                                                                                                                        |
| 6       |  をクリックして、選択したASNを含むパスを視覚的に除外します。このASNを含むすべてのパスがトポロジから削除されます。                                                                                                                                                                              |
| 7       | 発信元ASN。                                                                                                                                                                                                                                                                                                                    |
| 8       | 組織に属するピア（マイピア）によってアドバタイズされたASパスのトポロジのみを表示するか、すべてのピアによってアドバタイズされたASパスのトポロジのみを表示するかを選択できます。[マイピア（My Peers）]ビューでは、ピアがプレフィックスに対してアドバタイズしているASパスを簡単に表示できるため、ルーティング設定に役立ちます。                                                                                                                                                     |
| 9       | 複数の宛先ASNまたは中継ASNを選択し、パストポロジで視覚的に除外または注目することができます。                                                                                                                                                                                                                                                                          |
| 10      | ホップ数（パスの長さ）に応じて、パスを降順または昇順で視覚的に並べ替えることができます。                                                                                                                                                                                                                                                                               |
| 11      | このウィンドウは、ASNをクリックすると表示されます。ASN名と未加工パスデータが表示されます（該当する場合はパススタッフィングカウントを示します。ASNパススタッフィングの例を参照してください。宛先ASNが選択されている場合、このパスをアドバタイズしているピアも表示されます。このウィンドウから、次のことも実行できます。 <ul style="list-style-type: none"> <li>パストポロジからASNを視覚的に注目するか除外するかを選択します。</li> <li>[ASN]リンクをクリックして[ASN詳細（ASN Details）]ページを表示し、詳細なASN情報を取得できます。</li> </ul> |

図 4: ASN パススタッキングの例



スタックされた ASN ノードは、ASN がパスに複数回挿入されたことを示します。

## パストポロジの変更を比較

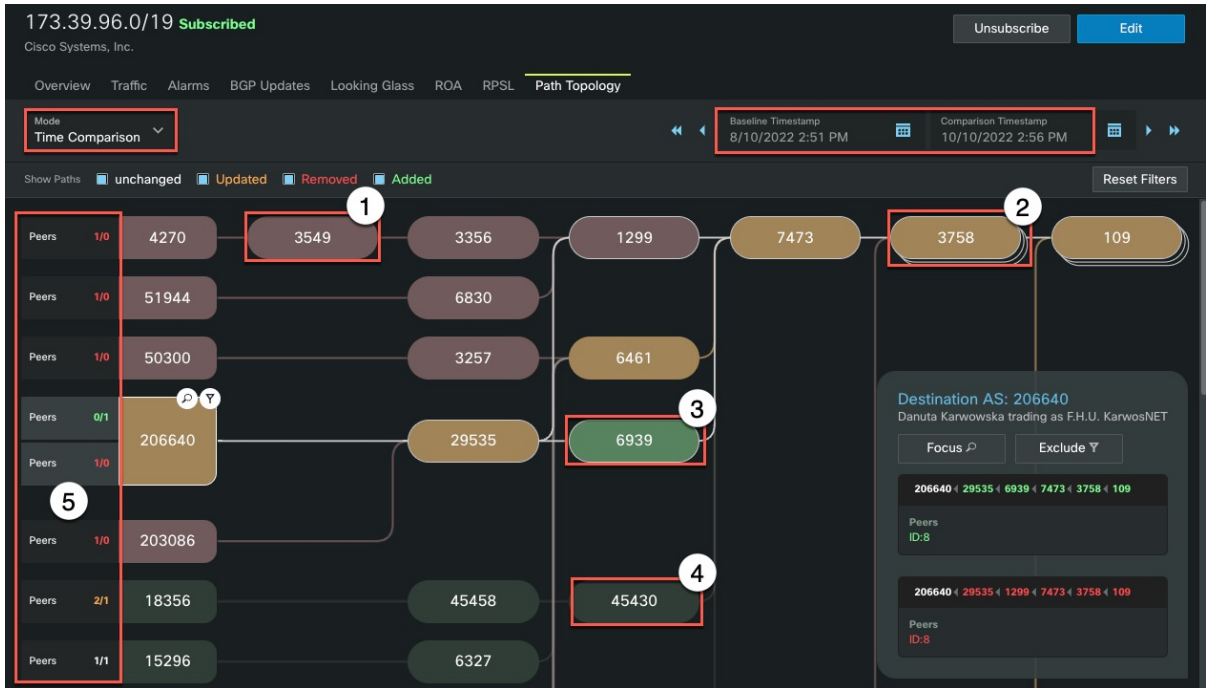
パストポロジツールは、指定された時間内にプレフィックスのルーティングトラフィックで発生した可能性のある問題（たとえば、AS パスの変更による帯域幅や遅延の問題）をトラブルシューティングする上で役立つ情報を提供します。ネットワーク障害が発生し、何が変更されたかを調査するとします。問題が発生した時刻の前後のトポロジを比較することにより、ASN ノードトポロジおよびピアのパスの変更を表示できます。

パストポロジの変更を表示するには、次の手順を実行します。

- ステップ 1 [パストポロジ (Path Topology)] ウィンドウで、[モード (Mode)] ドロップダウンリストから [時間比較 (Time Comparison)] を選択します。
- ステップ 2 [ベースラインタイムスタンプ (Baseline Timestamp)] フィールドをクリックし、パストポロジ変更の参照として使用する日時を選択します。一重矢印または二重矢印を使用して、時間を 1 分または 5 分進めたり戻したりすることができます。

**ステップ 3** [比較タイムスタンプ (Comparison Timestamp)] フィールドをクリックし、ベースラインタイムスタンプとの比較に使用する日時を選択します。

時間比較モードでは、トポロジの変更はさまざまなASNノードの色を使用して強調表示され、パスの変更はさまざまなピアテキストの色を使用して強調表示されます (数/IDでピアを表示)。次の例と、各色が示す内容の説明を参照してください。



(注) 画像をクリックすると、フルサイズで表示されます。

| 引き出し線番号          | 説明                                                                                   |
|------------------|--------------------------------------------------------------------------------------|
| <b>AS ノードの変更</b> |                                                                                      |
| 1                | 削除された AS ノード (赤色) : そのホップに AS ノードがあったアダプタイズされた AS パスが、ベースラインタイムスタンプの後に取り消されたことを示します。 |

| 引き出し線番号                                                                                                                                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2                                                                                                                                                | <p>更新された AS ノード（黄色/茶色）：両方のタイムスタンプで、そのホップの ASN が 1 つ以上の他の AS パスに存在していたことを示しますが、いくつかの変更があったことを示します。</p> <ul style="list-style-type: none"> <li>• <b>パス数の変更</b>：アドバタイズされた一部の新しい AS パスにはこの AS ノード/ホップが含まれ、AS ノード/ホップでアドバタイズされた一部の古い AS パスは、ベースラインタイムスタンプのしばらく後に取り消されました。</li> <li>• <b>パススタッフィングの変更</b>：この AS ノード/ホップは次のいずれかでした。 <ul style="list-style-type: none"> <li>• 以前は 1 つ以上の AS パスにスタッフィングされていて、現在はスタッフィングされていない</li> <li>• 現在は 1 つ以上の AS パスにスタッフィングされていて、以前はスタッフィングされていない</li> <li>• 現在および以前に 1 つ以上の AS パスにスタッフィングされていたが、数が変更された</li> </ul> </li> </ul> |
| 3                                                                                                                                                | <p>追加された AS ノード（緑色）：そのホップの AS ノードが、ベースラインタイムスタンプの後にアドバタイズされた 1 つ以上の新しい AS パスに存在するが、ベースライン時には存在しなかったことを示します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 4                                                                                                                                                | <p>変更されていない AS ノード（深緑色/灰色）：そのホップの AS ノードが、両方のタイムスタンプでアドバタイズされた 1 つ以上の他の AS パスに存在することを示します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p><b>ピア数の変更</b></p> <p>パスをアドバタイズするピアの数の変更は、その AS パスを終了したピア ASN の隣にテキストで注釈が付けられます。ピア変更のシンタックスは、<i>before_peer_count/after_peer_count</i> です。</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 5                                                                                                                                                | <ul style="list-style-type: none"> <li>• <b>0/n（緑色）</b>：ベースライン時にピアがこのパスをアドバタイズしていなかったが、比較時には <i>n</i> 個のピアがパスをアドバタイズしていたことを示します。</li> <li>• <b>n/0（赤色）</b>：ベースライン時に <i>n</i> 個のピアがこのパスをアドバタイズしていたが、比較時にはピアがパスをアドバタイズしていなかったことを示します。</li> <li>• <b>b/a（黄色）</b>：ベースライン時に <i>b</i> 個のピアがこのパスをアドバタイズし、比較時には <i>a</i> 個のピアがパスをアドバタイズしていたことを示します。</li> <li>• <b>n/n（白色）</b>：パスをアドバタイズするピアの数に、ベースライン時より後、比較時以前に変化がなかったことを示します。</li> </ul>                                                                                                                           |





## 第 **VI** 部

# Crosswork トラフィック分析ツールを使用する

- [インターフェイス使用率の最適化 \(225 ページ\)](#)
- [トラフィックのドリルダウン \(227 ページ\)](#)
- [ピア探査 \(229 ページ\)](#)
- [トラフィックの比較 \(233 ページ\)](#)





## 第 27 章

# インターフェイス使用率の最適化

・インターフェイス使用率の最適化 (225 ページ)

## インターフェイス使用率の最適化

使用率の高いトラフィックをデバイスグループ内の他のインターフェイスに迂回させることで、ネットワークを最適化できます。推奨ツールは、送信使用率が 80% を超えるネットワーク エッジインターフェイスを分析します。（たとえば、エッジインターフェイスの送信使用率が 20% で受信使用率が 90% の場合、エッジインターフェイスは分析対象の一部として考慮されません。）このツールは、全体的な使用率を正規化するために、過度に使用されているエッジインターフェイスからのトラフィックを十分に使用されていないエッジインターフェイスに転送できるプレフィックスの推奨リストを提供します。使用率の予測は、元のトラフィックフローに基づく推定値です。これらの推奨事項を使用して、ネットワークトラフィックの負荷を最適に分散する方法を決定できます。

**ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [推奨事項 (Recommendations)] の順にクリックします。

**ステップ 2** [デバイスグループ (Device Group)] ドロップダウンメニューからデバイスグループを選択すると、そのデバイスに含まれている、見込みのあるプレフィックスのみが表示されます。このページには、次の情報が表示されます。

- [タイムフレーム (Timeframe)] ドロップダウンリストで選択した期間中のプレフィックス、送信トラフィックレート、およびインターフェイス使用状況。
- トラフィックをオフロードし、輻輳を緩和するために使用できる代替インターフェイス。
- デバイスグループ内のデバイスに推奨事項が手動で設定されている場合の予測されるインターフェイス使用率。これらの予測は、元のトラフィックフローに基づく推定値。

**ステップ 3** プレフィックスを分析から除外するには、[プレフィックスを無視 (Ignore Prefix)] をクリックします。プレフィックスを元に戻すには、[無視 (Ignored)] タブに移動し、[追跡の再開 (Resume Tracking)] をクリックします。





## 第 28 章

# トラフィックのドリルダウン

- ・ [トラフィックのドリルダウン \(227 ページ\)](#)

## トラフィックのドリルダウン

トラフィック ドリルダウン ツールを使用すると、インターフェイスの容量と、それに貢献しているトラフィックソースを簡単に表示できます。

**ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [トラフィックのドリルダウン (Traffic Drilldown)] をクリックします。

**ステップ 2** 次のいずれかのオプションをクリックします。

- a) [デバイスセントリック (Device Centric)] : デバイスのリストを表示します。そこから、デバイス使用率、デバイスグループ、容量、TX/RX SNMP トラフィック、タグなどのデバイス情報を表示できます。

(注) デバイスの [使用率 (Utilization)] 列をフィルタリングするには、[フィルタの編集 (Edit Filter)] をクリックし、0 ~ 100 のスケールのいずれかの端をスライドして、表示する使用率の範囲を指定します。Crosswork Cloud Traffic Analysis は、デバイス上のすべてのインターフェイスの中で最も高い使用率を使用して使用率を決定します。個々のインターフェイスの使用率を表示するには、デバイス名をクリックします。次の値が有効です。

- バランス : すべてのインターフェイスの使用率は 50% 未満です。
  - スキュード : 任意のインターフェイスでの最高使用率は 50% 以上、80% 未満です。
  - 不均衡 : 少なくとも 1 つのインターフェイスの使用率が 80% を超えています。
1. デバイスのインターフェイスの詳細を表示するには、デバイス名をクリックします。デバイスのインターフェイスのリストが表示され、個々のインターフェイス情報が表示されます。
  2. インターフェイスの ASN またはプレフィックス情報を表示するには、インターフェイスをクリックし、[内訳 (Breakdown)] フィルタリストから適切なオプションを選択します。

- b) [プレフィックスセントリック (Prefix Centric) ]: タグ、TX/RX Netflow トラフィック、および総トラフィックを表示できるプレフィックスのリストを表示します。
1. プレフィックスデバイスの詳細を表示するには、プレフィックスをクリックします。デバイス情報が表示されます。
  2. デバイスインターフェイスの詳細を表示するには、デバイス名をクリックします。
-



## 第 29 章

# ピア探査

- ピア探査の概要 (229 ページ)
- 推奨されるピアの検索 (229 ページ)
- ピアの最適化 (230 ページ)
- 推奨されるピアの無視 (231 ページ)

## ピア探査の概要



(注) この機能は、Crosswork Traffic Analysis 専用です。

ピア探査ツールを使用すると、大量のトラフィックが送受信されているピア ASN が表示されます。現在のピアを選択し、トラフィックを移動できる他のピアをすばやく確認するのに役立ちます。たとえば、サービスプロバイダーがトラフィックスループットに対してより多くの料金を請求する場合、トラフィックをそのピアからより安価な別のピアに移動することもできます。ピア探査は、トラフィックを移動できる他のピアを識別するのに役立ちます。



(注) この機能を使用するには、Advanced ライセンスが必要です。詳細については、[sales@crosswork.cisco.com](mailto:sales@crosswork.cisco.com) までお問い合わせください。

## 推奨されるピアの検索

現在ピアリングされていないが、大量のトラフィックを送信している ASN のリストを表示できます。これは、ピアリングする必要があるが、そうになっていない ASN を把握するのに役立ちます。



(注) この機能を使用するには、Advanced ライセンスが必要です。詳細については、[sales@crosswork.cisco.com](mailto:sales@crosswork.cisco.com) までお問い合わせください。

**ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [ピア探査 (Peer Prospecting)] の順にクリックします。

デフォルトでは、[非ピア (Non-Peers)] オプションが選択されています。これは、現在ピアではないすべての ASN がテーブルに含まれていることを示します。

**ステップ 2** [フィルタ基準 (Filter By)] フィールドで、次のいずれかのオプションを選択します。

- [デバイスグループ (Device Group)] : [デバイスグループ (Device Group)] をクリックし、ドロップダウンリストからデバイスグループを選択すると、そのデバイスグループに含まれている、見込みのあるピアのみが表示されます。
- [デバイス (Device)] : [デバイス (Device)] をクリックし、ドロップダウンリストからデバイスを選択すると、そのデバイスタイプの見込みのあるピアのみが表示されます。

**ステップ 3** 表示するトラフィック集約値を以下から選択します。

- [両方 (Both)] : 特定の ASN のすべてのトラフィックの RX、TX、および合計データを集約します。
- [中継 (Transit)] : ASN がトラフィックの送信元または宛先ではなく、パスのどこかにある中間ピアである場合に、RX、TX、および合計データを集約します。中継データを確認することで、たとえば、特定の ASN とのピアリングによってトラフィックパスが短縮できるかどうかを判断できます。
- [宛先/送信元 (To/From)] : 送信元 ASN および宛先 ASN の Rx、Tx、および合計データを集約します。

**ステップ 4** 特定の期間のデータを表示するには、[タイムフレーム (Timeframe)] ドロップダウンリストから時間を選択します。

テーブルには、見込みのあるピアになる可能性のある ASN のリストが含まれています。デフォルトでは、テーブルは全トラフィックデータの降順に編成されます。

**ステップ 5** 見込みのあるピアのリストから ASN を非表示にするには、[無視 (Ignore)] をクリックします。詳細については、[推奨されるピアの無視 \(231 ページ\)](#) を参照してください。

**ステップ 6** [見込み (Prospect)] 列の ASN をクリックすると、その ASN に関する詳細が表示されます。

## ピアの最適化

ピアリングしている ASN を表示し、ネットワークを最適化するためにトラフィックを移動できる他のピアがあるかどうかを確認できます。





(注) この機能を使用するには、Advanced ライセンスが必要です。詳細については、[sales@crosswork.cisco.com](mailto:sales@crosswork.cisco.com) までお問い合わせください。

- ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [ピア探査 (Peer Prospecting)] の順にクリックします。
- ステップ 2** [ピアの最適化 (Optimize Peer)] をクリックし、最適化するピアの ASN を入力するか、します。
- ステップ 3** [フィルタ基準 (Filter By)] フィールドで、次のいずれかのオプションを選択します。
- [デバイスグループ (Device Group)] : [デバイスグループ (Device Group)] をクリックし、ドロップダウンリストからデバイスグループを選択すると、そのデバイスグループに含まれている、見込みのあるピアのみが表示されます。
  - [デバイス (Device)] : [デバイス (Device)] をクリックし、ドロップダウンリストからデバイスを選択すると、そのデバイスタイプの見込みのあるピアのみが表示されます。
- ステップ 4** 表示するトラフィック集約値を以下から選択します。
- [両方 (Both)] : 特定の ASN のすべてのトラフィックの RX、TX、および合計データを集約します。
  - [中継 (Transit)] : ASN がトラフィックの送信元または宛先ではなく、パスのどこかにある中間ピアである場合に、RX、TX、および合計データを集約します。中継データを確認することで、たとえば、特定の ASN とのピアリングによってトラフィックパスが短縮できるかどうかを判断できます。
  - [宛先/送信元 (To/From)] : 送信元 ASN および宛先 ASN の RX、TX、および合計データを集約します。
- ステップ 5** 特定の期間のデータを表示するには、[タイムフレーム (Timeframe)] ドロップダウンリストから時間を選択します。
- テーブルには、見込みのあるピアになる可能性のある ASN のリストが含まれています。デフォルトでは、テーブルは全トラフィックデータの降順に編成されます。
- ステップ 6** 見込みのあるピアのリストから ASN を非表示にするには、[無視 (Ignore)] をクリックします。
- ステップ 7** [見込み (Prospect)] 列の ASN をクリックすると、その ASN に関する詳細が表示されます。

## 推奨されるピアの無視

推奨されるピアを無視することで、[ピア探査 (Peer Prospecting)] ページの推奨のリストに表示されなくなります。これは、見込みのあるピアとしてリストされている ASN とピアリングできないか、ピアリングすべきでないことがわかっている場合に役立ちます。



---

(注) この機能を使用するには、Advanced ライセンスが必要です。詳細については、[sales@crosswork.cisco.com](mailto:sales@crosswork.cisco.com) までお問い合わせください。

---

---

**ステップ1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [ピア探査 (Peer Prospecting)] の順にクリックします。

デフォルトでは、[推奨 (Recommendations)] オプションが選択されています。これは、現在ピアではないすべての推奨 ASN がテーブルに含まれていることを示します。

**ステップ2** テーブルで、無視する ASN の [アクション (Action)] 列の下にある [無視 (IGNORE)] をクリックします。

ASN がテーブルから削除されます。

**ステップ3** ページ上部の [無視 (Ignored)] をクリックすると、無視するように選択した ASN 候補のリストが表示されます。

**ステップ4** ASN の無視を解除するには、推奨される候補 ASN のリストに移動する ASN の [アクション (Action)] 列の下にある [含める (INCLUDE)] をクリックします。

ASN が [無視 (Ignored)] テーブルから削除され、[推奨 (Recommendations)] テーブルに表示されます。

---



## 第 30 章

# トラフィックの比較

- [トラフィックの比較 \(233 ページ\)](#)

## トラフィックの比較

ASN、プレフィックス、デバイス、インターフェイスなどの類似オブジェクト間のトラフィックを比較できます。トラフィックの視覚的な比較をすばやく表示すると、オブジェクト間のトラフィックの違いを確認するのに役立ちます。

- ステップ 1** メインウィンドウで、[トラフィック分析 (Traffic Analysis)] > [ツール (Tools)] > [トラフィックの比較 (Traffic Comparison)] をクリックします。
- ステップ 2** [オブジェクト (Object)] ドロップダウンリストから、トラフィックを比較するオブジェクトタイプを選択します。
- ステップ 3** [時間 (Time)] ドロップダウンリストから、トラフィックを比較するタイムフレームを選択します。
- [更新 (Updated)] ボックスは、トラフィックデータが最後に更新された時刻を示します。トラフィック情報を更新するには、更新アイコンをクリックします。
- ステップ 4** ステップ 2 で [ASN] を選択した場合は、次のいずれかのトラフィック値を選択して表示します。
- [中継 (Transit)] : ASN がトラフィックの送信元または宛先ではなく、パスのどこかにある中間ピアである場合に、Rx、Tx、および合計データを集約します。中継データを確認することで、たとえば、特定の ASN とのピアリングによってトラフィックパスが短縮できるかどうかを判断できます。
  - [両方 (Both)] : 特定の ASN のすべてのトラフィックの Rx、Tx、および合計データを集約します。
  - [宛先/送信元 (To/From)] : 送信元 ASN および宛先 ASN の Rx、Tx、および合計データを集約します。
- ステップ 5** [追加 (Add)] をクリックして、比較するオブジェクトを選択します。ステップ 2 で選択したオブジェクトタイプに対応するオブジェクトを選択できます。
- 各オブジェクトはカンマで区切ります。

ステップ 6 [保存 (Save) ] をクリックします。

---



## 第 **VII** 部

# Crosswork Trust Insights ツールを使用する

- [デバイスの比較 \(237 ページ\)](#)
- [パッケージの検索 \(239 ページ\)](#)
- [ハードウェアの検索 \(241 ページ\)](#)





## 第 31 章

# デバイスの比較

- [デバイスの比較について \(237 ページ\)](#)
- [デバイスの比較 \(237 ページ\)](#)

## デバイスの比較について

Crosswork Cloud Trust Insights では、デバイスをすばやく比較して、実行中のソフトウェアの違いを確認できます。

## デバイスの比較

デバイスを簡単に比較して、違いを表示できます。

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [デバイスの比較 (Device Comparison)] をクリックします。

**ステップ 2** 他のデバイスを比較する基準として使用するデバイスを選択します。

Crosswork Cloud Trust Insights では、選択した基準デバイスと比較した他のすべてのデバイスとそれらの違いを一覧にした以下に説明する表が表示されます。

表 30: デバイスの比較のフィールドに関する説明

| フィールド             | 説明                           |
|-------------------|------------------------------|
| 価格偏差 (Deviations) | 基準デバイスと比較したデバイスの違いまたは価格偏差の数。 |
| デバイス (Device)     | 基準デバイスと比較されるデバイスの名前。         |
| 参照先 (Location)    | デバイスの場所。                     |
| モデル (Model)       | デバイスのモデル。                    |

| フィールド                                                  | 説明                                                                                                                                                  |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| バージョン (Version)                                        | デバイスで実行しているソフトウェアのバージョンです。                                                                                                                          |
| ソフトウェアの違い (最初の 500) (Software Differences (FIRST 500)) | <p>基準デバイスと比較したデバイスのソフトウェアの違いのリスト。500 を超えるソフトウェアの違いがある場合は、最初の 500 件だけが表示されます。</p> <p>選択したデバイスを基準デバイスに一致させるために必要な特定の変更を表示するには、青色のハイパーリンクをクリックします。</p> |

デフォルトでは、テーブルは、選択した基準デバイスと比較した各デバイスの違いまたは価格偏差の数に従ってソートされます。

**ステップ 3** デバイスを検索するには、[クイック検索 (Quick Search)] フィールドに文字を入力します。

Crosswork Cloud Trust Insights では、入力した検索条件に一致するデバイスのみが表示されます。

**ステップ 4** 基準デバイスとは異なるデバイスのリストと相違点の概要を表示するには、[パンチリストの表示 (View Punchlist)] をクリックします。

**ステップ 5** CSV ファイルにリストをエクスポートするには、[CSVのエクスポート (Export CSV)] をクリックします。





## 第 32 章

# パッケージの検索

---

- [パッケージの検索 \(239 ページ\)](#)

## パッケージの検索

Crosswork Cloud Trust Insights では、インストールされている SMU パッケージをすばやく見つけることができます。これは、ソフトウェアのバージョンを交換したり、SMU を更新してセキュリティの脆弱性を修正したりする場合に役立ちます。

---

**ステップ 1** メインウィンドウで、[トラストインサイト (Trust Insights)] > [パッケージの検索 (Find Package)] の順にクリックします。

**ステップ 2** [表示 (View)] フィールドで、次のオプションのいずれかを選択します。

- [検索 (Search)] : すべてのパッケージを検索します。
- [コミット済みだがアクティブ化されていない (Committed but Not Activated)] : コミットされているがアクティブ化されていないパッケージを検索します。

**ステップ 3** 検索対象の文字を 3 つ以上入力します。

**ステップ 4** 次のオプションのいずれかを選択します。

- [含める (Include)] : 入力した文字を含むパッケージを検索します。
- [除外する (Exclude)] : 入力した文字を含まないパッケージを検索します。

Crosswork Cloud Trust Insights では、指定した条件に一致するパッケージが表示されます。

---





## 第 33 章

# ハードウェアの検索

---

- [ハードウェアの検索 \(241 ページ\)](#)
- [ハードウェアの変更の表示 \(241 ページ\)](#)
- [ハードウェアインベントリの表示 \(242 ページ\)](#)

## ハードウェアの検索

Crosswork Cloud Trust Insights は、ハードウェアをすばやく見つけるのに役立ちます。これは、当社のハードウェアに関する特定の情報を表示する場合に役立ちます。

- 
- ステップ 1** メインウィンドウで、[ツール (Tools)] > [ハードウェアの検索 (Find Hardware)] の順にクリックします。
  - ステップ 2** [フィルタの追加 (Add Filter)] をクリックします。
  - ステップ 3** [フィルタ (Filter)] フィールドで、検索する属性を選択します。
  - ステップ 4** [フィルタ値 (Filter Value)] フィールドに、検索する値を入力します。
  - ステップ 5** [保存 (Save)] をクリックします。

テーブルには、入力した検索属性に一致するすべてのハードウェアが表示されます。

---

## ハードウェアの変更の表示

Crosswork Cloud Trust Insights は、最後に受信した信頼ドシエにデバイスによって反映されたハードウェアの変更を表示する簡単な方法を提供します。Crosswork Cloud Trust Insights を使用すると、運用ライフサイクルを通じて実稼働システムの変更を検出および追跡できます。

- 
- ステップ 1** Crosswork Cloud Trust Insights のメインウィンドウで、[デバイス (Devices)] をクリックします。

Trust Insights に、以前に追加されたデバイスのリストが表示されます。詳細については、[デバイスの追加 \(173 ページ\)](#) を参照してください。

**ステップ 2** ハードウェアの変更を表示するデバイス名をクリックします。

**ステップ 3** [変更 (Changes) ] タブをクリックします。

Crosswork Cloud Trust Insights では、選択したデバイスの履歴タイムラインで観察されたイベントが強調表示されます。

**ステップ 4** 指定した時間の変更を表示するには、[タイムフレーム (Timeframe) ]の横にあるオプションをクリックします。

---

## ハードウェアインベントリの表示

Crosswork Cloud Trust Insights は、最後に受信した信頼ドシエにデバイスによって反映されたハードウェアインベントリを表示する簡単な方法を提供します。

---

**ステップ 1** Crosswork Cloud Trust Insights のメインウィンドウで、[デバイス (Devices) ] をクリックします。

Trust Insights に、以前に追加されたデバイスのリストが表示されます。詳細については、[デバイスの追加 \(173 ページ\)](#) を参照してください。

**ステップ 2** ハードウェア情報を表示するデバイス名をクリックします。

デフォルトでは、[ハードウェア (Hardware) ] が選択され、ハードウェア情報が表示されます。

**ステップ 3** [ノード (Node) ] 列の名前をクリックすると、そのノードに関する特定の情報が表示されます。Crosswork Cloud Trust Insights では、この個別のコンポーネントが以前に観察された場所の履歴が表示されます。ハードウェアコンポーネントの履歴は、確認されたシリアル番号に基づいて、一定期間にわたってシステム全体で個々のハードウェア FRU を追跡します。

---



## 第 VIII 部

### 管理タスク

- [ユーザーの管理 \(245 ページ\)](#)
- [ライセンスの管理 \(249 ページ\)](#)
- [構成ファイルのインポートとエクスポート \(251 ページ\)](#)
- [実行されたアクションのリストの表示 \(253 ページ\)](#)
- [製品のヘルプとサポートの取得 \(255 ページ\)](#)
- [Crosswork Cloud API \(257 ページ\)](#)





## 第 34 章

# ユーザーの管理

---

- [ユーザの追加 \(245 ページ\)](#)
- [ユーザの役割 \(246 ページ\)](#)
- [ユーザ権限の変更 \(246 ページ\)](#)
- [ユーザプロフィールの表示 \(247 ページ\)](#)

## ユーザの追加

ユーザを追加するには、管理者権限が必要です。

ユーザはCisco.comのユーザ名とパスワードを入力してログインする必要があるため、Cisco.comアカウントが必要です。

---

**ステップ 1** メインウィンドウで、左下隅の [設定 (Settings)] をクリックします。

**ステップ 2** [ユーザ (Users)] をクリックします。

(注) [ユーザ (Users)] メニューは、管理者権限を持つユーザに対してのみ表示されます。

**ステップ 3** [ユーザの追加 (Add User)] をクリックします。

**ステップ 4** ユーザが [有効 (Enabled)] (デフォルト) か [無効 (Disabled)] かを指定します。

無効になっているユーザはログインできません。

**ステップ 5** Cisco.com ユーザプロフィールで指定されたユーザの電子メールアドレスを入力します。

複数のユーザを追加するには、各電子メールアドレスをスペース、カンマ (,)、またはセミコロン (;) で区切ります。

**ステップ 6** ユーザが実行できるタスクを決定するユーザのロールを選択します。詳細については、[ユーザの役割 \(246 ページ\)](#) を参照してください。

**ステップ 7** [プロバイダー (Provider)] フィールドには、管理者であるユーザが属しているのと同じプロバイダーが表示されます。

ステップ 8 [保存 (Save) ]をクリックします。

## ユーザの役割

ユーザロールは、ユーザがタスクを実行するために必要な権限を定義します。次の表に、権限を持つユーザロールとタスクを示します。

表 31: ユーザロールおよび権限の説明

| ユーザ ロール   | 権限                           |
|-----------|------------------------------|
| Admin     | ユーザの追加と編集を含むすべてのタスクを実行できます。  |
| 読み取り/書き込み | ユーザの追加と編集を除くすべてのタスクを実行できます。  |
| 読み取り専用    | すべてのデータを読み取り、ユーザ設定のみを変更できます。 |

## ユーザ権限の変更

ユーザが実行できるタスクを決定するには、ユーザのロールを変更します。ユーザ権限を変更するには、管理者権限が必要です。

ステップ 1 メインウィンドウで、左下隅の [設定 (Settings) ]をクリックします。

ステップ 2 [ユーザ (Users) ]をクリックします。

(注) [ユーザ (Users) ]メニューは、管理者権限を持つユーザに対してのみ表示されます。

ステップ 3 権限を変更するユーザーのチェックボックスをオンにします。複数のユーザーを同時にオンにできます。

ステップ 4 [編集 (Edit) ]をクリックします。

ステップ 5 ユーザーの権限を一時停止するには、最初の [値の編集 (Edit Value) ]チェックボックスをオンにして、ドロップダウンの [状態 (State) ]リストから [無効 (Disabled) ]を選択します。ステータスを [有効 (Enabled) ]に変更するまで、ユーザはログインできません。

ステップ 6 ユーザーのロールを変更するには、2番目の [値の編集 (Edit Value) ]チェックボックスをオンにして、ドロップダウンの [ロール (Role) ]リストから役割を選択します。各ロールが実行できるタスクの詳細については、[ユーザの役割 \(246 ページ\)](#) を参照してください。

ステップ 7 [Next] をクリックします。

ステップ 8 変更を確認し、[保存 (Save) ]をクリックします。



## ユーザプロフィールの表示

ユーザプロフィールを表示して、ロール、ステータス、および最後のログインを確認できます。ユーザプロフィールを表示するには、管理者権限が必要です。

---

**ステップ 1** メインウィンドウで、左下隅の [設定 (Settings)] をクリックします。

**ステップ 2** [ユーザ (Users)] をクリックします。

(注) [ユーザ (Users)] メニューは、管理者権限を持つユーザに対してのみ表示されます。

テーブルには、すべてのユーザとそのロール、ステータス、および最後のログインがリストされます。

**ステップ 3** ユーザのアクセスを変更するには、ユーザの電子メールアドレスをクリックします。詳細については、[ユーザ権限の変更 \(246 ページ\)](#) を参照してください。

---





## 第 35 章

# ライセンスの管理

- サブスクリプションまたはトライアルをアクティブ化する (249 ページ)
- 組織名の変更 (250 ページ)

## サブスクリプションまたはトライアルをアクティブ化する

Crosswork Cloud でサブスクリプションをアクティブ化できます。



(注) サブスクリプションをアクティブ化するには、管理者権限が必要です。詳細については、「[ユーザの役割 \(246 ページ\)](#)」を参照してください。

### 始める前に

サブスクリプションをアクティブ化するには、Crosswork Cloud サブスクリプションの購入後に提供されるか、メールで送られてくる 1 つ以上のサブスクリプション ID が必要です。

**ステップ 1** メインウィンドウで、左下隅の  [設定 (Settings)] アイコンをクリックします。

**ステップ 2** [ライセンス (Licensing)] をクリックします。

**ステップ 3** サブスクリプションをアクティブ化するには：

- a) [資格 (Entitlement)] > [外部ルート分析 (External Route Analysis)]、[信頼インサイト (Trust Insights)]、または [トラフィック分析 (Traffic Analysis)] タブをクリックします。
- b) [サブスクリプションの請求 (Claim Subscription)] をクリックし、テキストボックスにサブスクリプション ID を入力します。複数のサブスクリプション ID を追加するには、各 ID をカンマで区切るか、各 ID を新しい行に入力します。

**ステップ 4** Crosswork Cloud 製品のトライアルバージョンをリクエストするには：

- a) [トライアル (Trial)] タブをクリックします。

- b) 試したいCrosswork Cloud製品の横にある[リクエスト (Request)]をクリックします。条件に同意し、[トライアルを開始 (Start Trial)]をクリックします。
- 

## 組織名の変更

組織の名前を変更できます。

---

**ステップ1** メインウィンドウで、左下隅の  [設定 (Settings)] アイコンをクリックします。

**ステップ2** [ライセンス (Licensing)] をクリックします。

**ステップ3** [編集 (Edit)] をクリックします。

**ステップ4** 新しい組織名を入力し、[保存 (Save)] をクリックします。

---



## 第 36 章

# 構成ファイルのインポートとエクスポート

- [構成ファイルのアップロード \(251 ページ\)](#)
- [構成ファイルのダウンロード \(252 ページ\)](#)

## 構成ファイルのアップロード

プレフィックス、ASN、ポリシー、および通知設定を含む構成ファイルをアップロードできます。構成ファイルをアップロードすると、同じタイプの既存のデータが上書きされます。たとえば、以前にプレフィックスを追加し、構成ファイルに空のプレフィックスが含まれている場合、既存のプレフィックスは削除されます。



- (注) 新しい構成ファイルのアップロードなど、大幅な構成変更を行う前に、既存の構成ファイルをダウンロードして保存し、バックアップファイルとして使用することを推奨します。詳細については、[構成ファイルのダウンロード \(252 ページ\)](#) を参照してください。

**ステップ 1** メインウィンドウで、左下隅の [設定 (Settings)] をクリックします。

**ステップ 2** [インポート/エクスポート (Import/Export)] をクリックします。

**ステップ 3** [構成ファイルのアップロード (Upload Config File)] をクリックして、JSON 構成ファイルの場所に移動します。

指定したリンクをクリックして、サンプル JSON 構成ファイルをダウンロードすることもできます。

**ステップ 4** [次へ (Next)] をクリックします。

**ステップ 5** 適切なタブに移動して、構成ファイルの内容をプレビューし、追加および削除される情報を確認します。

**ステップ 6** [送信 (Submit)] をクリックします。

# 構成ファイルのダウンロード

## 始める前に

大幅な構成変更を行う前に、バックアップファイルとして使用する構成ファイルをダウンロードして保存することを推奨します。



---

(注) 大幅な変更と拡張のため、2019年11月12日より前に構成ファイルをダウンロードした場合は、新しい構成ファイルをダウンロードする必要があります。2019年11月12日より前にダウンロードされた構成ファイルには大きな違いがあり、アップロードできません。

---

---

**ステップ1** メインウィンドウで、左下隅の [設定 (Settings)] をクリックします。

**ステップ2** [インポート/エクスポート (Import/Export)] をクリックします。

**ステップ3** [構成のエクスポート (Export Configuration)] をクリックして、JSON 構成ファイルをダウンロードします。  
構成ファイル (.json) が保存されます。

---




## 第 37 章

# 実行されたアクションのリストの表示

・ [実行されたアクションのリストの表示 \(253 ページ\)](#)

## 実行されたアクションのリストの表示

Crosswork Cloud アプリケーションで実行されたすべてのアクションのリストを表示できます。これにより、どのような変更が行われたか、誰が変更を行ったか、および変更が行われた日時をよりよく把握できます。

**ステップ 1** メインウィンドウで、左下隅にある [アクティビティログ (ActivityLog) ] アイコン (  ) をクリックします。

デフォルトでは、すべての変更が表示されます。

**ステップ 2** 指定した期間のアクティビティを表示するには、[タイムフレーム (Timeframe) ] ドロップダウンリストから期間を選択します。

**ステップ 3** 特定の変更を表示するには、次のいずれかをクリックします。

- [ASN (ASNs) ]
- 資格情報
- データゲートウェイ
- デバイス (Devices)
- デバイス グループ (Device Groups)
- エンドポイント
- インターフェイス
- Peers
- ポリシー
- プレフィックス (Prefixes)

- レポート
  - Users
-






## 第 38 章

# 製品のヘルプとサポートの取得

- サポート ケースのオープン (255 ページ)
- 製品フィードバックの送信 (255 ページ)
- シスコ コミュニティ フォーラムへのアクセス (255 ページ)


## サポート ケースのオープン

Crosswork Cloud では、製品内からサポートケースを開くことができます。

メインウィンドウから、[ヘルプとサポート (Help and Support) ]  アイコン > [サポート (Support) ] > [サポートへの問い合わせを開く (Open a Support Case) ] をクリックします。新しいブラウザウィンドウが開き、Support Case Manager が表示されます。


## 製品フィードバックの送信

Crosswork Cloud 製品に関するフィードバックをお待ちしております。また、当社の取り組みについてご意見をいただければ幸いです。

メインウィンドウから、[ヘルプとサポート (Help and Support) ]  アイコン > [サポート (Support) ] > [製品のフィードバック (Product Feedback) ] をクリックします。

## シスコ コミュニティ フォーラムへのアクセス

シスコ コミュニティ フォーラムにアクセスして、よくある質問、製品発表、およびその他の製品情報にアクセスできます。このフォーラムでは、他の製品ユーザと学習、共有、コラボレーションすることもできます。

メインウィンドウから、[ヘルプとサポート (Help and Support) ]  アイコン > [サポート (Support) ] > [コミュニティフォーラム (Community Forum) ] をクリックします。新しいブラウザウィンドウが開き、Crosswork Cloud のフォーラムが表示されます。





## 第 39 章

# Crosswork Cloud API


- [Crosswork Cloud API の概要 \(257 ページ\)](#)
- [API ヘルプおよびドキュメント \(257 ページ\)](#)
- [API の使用開始 \(258 ページ\)](#)
- [API キーの定義 \(258 ページ\)](#)
- [Crosswork Cloud Network Insights クライアントスクリプト \(259 ページ\)](#)
- [Crosswork トラフィック分析クライアントスクリプトの例 \(266 ページ\)](#)


## Crosswork Cloud API の概要

Crosswork Cloud API は、ネットワーク管理および運用アプリケーションで API を使用するプログラマ向けです。

Crosswork Cloud Network Insights API により、プレフィックスまたは ASN への登録、通知エンドポイントの設定、アラームがトリガーされる条件の指定などの設定タスクを実行できます。Crosswork Cloud Traffic Analysis API はトラフィック統計を取得します。


## API ヘルプおよびドキュメント

Crosswork Cloud API ドキュメントにアクセスするには、Crosswork Cloud にログインする必要があります。API コールの定義とドキュメントを表示するには、[ヘルプとサポート (Help and Support)]  アイコン > [API] に移動するか、<https://crosswork.cisco.com/apiDoc/CiscoCrossworkCloudAPI> [英語] に移動します。

こちらから [シスココミュニティに参加](#)して、Crosswork Developer Hub にアクセスしてください。[ヘルプとサポート (Help and Support)]  アイコン > [サポート (Support)] > [コミュニティフォーラム (Community Forum)] に移動して、シスココミュニティにアクセスすることもできます。Crosswork Cloud ディスカッションを識別しやすくするために、必ず「Crosswork」ラベルを使用して登録してください。

## API の使用開始

Crosswork Cloud API にアクセスするには、管理者権限が必要です。管理者権限がない場合、API オプションは表示されません。ユーザー権限の変更については、[ユーザ権限の変更（246 ページ）](#) を参照してください。

API コール の定義とドキュメントを表示するには、Crosswork Cloud にログインし、[ヘルプとサポート (Help & Support)]  [API] をクリックするか、または <https://crosswork.cisco.com/apiDoc/CiscoCrossworkCloudAPI> にアクセスする必要があります。

API の使用を開始するには、次のタスクを実行します。

---

**ステップ 1** API キーを要求するには、Crosswork Cloud Network Insights ウィンドウの右上隅にあるユーザのイニシャルをクリックしてから、[APIキー/トークン (API Key / Tokens)] をクリックします。

**ステップ 2** [APIキーの追加 (Add API Key)] をクリックします。

**ステップ 3** API キーの名前、説明 (任意)、および API キーの開始日と終了日を入力し、[保存 (Save)] をクリックします。

**ステップ 4** [作成 (Create)] をクリックします。

新しい API キーが作成され、Crosswork Cloud アプリケーションでキーの詳細が表示されます。これは、キーが表示される唯一の機会です。

**ステップ 5** [コピー (Copy)] をクリックして API キーをコピーし、安全な場所に保存できるようにします。

(注) API キーをパスワードのように保護します。API キーはアカウントへのアクセスを提供するため、必ず安全に保管してください。

**ステップ 6** 使用を開始する方法の例については、[Crosswork Cloud Network Insights クライアントスクリプト例（260 ページ）](#) および [Crosswork トラフィック分析クライアントスクリプトの例（266 ページ）](#) のセクションを参照してください。

---

## API キーの定義

Crosswork Cloud API キーは次の設定は次のとおりです。

- API キーは、16 進数で符号化された 32 バイトの対称キーです。クライアントアプリケーションは API キーを使用して、Crosswork Cloud Network Insights または Crosswork Cloud Traffic Analysis 宛ての REST API 要求に署名します。
- API キー識別子 (ID) は、キーの一意的な値であり、署名済みの各要求に含める必要があります。Crosswork Cloud サービスは、キー ID を使用して API キーのコピーを取得し、着信要求を確認します。



- (注) パスワードと同じように API キーを保護します。API キーはアカウントへのアクセスを提供するため、必ず安全に保管してください。

クライアントアプリケーションは API キーを使用して、Crosswork Cloud に送信されるすべての要求に署名します。各要求には以下にものが含まれます。

- 署名要求
- API キー ID
- 署名を決定するために使用されるフィールドの詳細を示すメタデータ

Crosswork Cloud は REST API 要求を受信すると、次の手順を実行します。

1. 要求されたパラメータを抽出します。
2. API キー ID を使用して、API キーと関連するメタデータを取得します。
3. 署名を再計算します。
4. 計算された署名を要求された署名と比較します。
5. 計算された署名と要求された署名が一致する場合、Crosswork Cloud は要求を転送します。署名が一致しない場合、Crosswork Cloud は要求を拒否します。

## Crosswork Cloud Network Insights クライアントスクリプト

このセクションには、Crosswork Cloud Network Insights クライアントスクリプトの使用法の例と情報が含まれています。

### クライアントスクリプトのオプション

クライアントスクリプトの実行時には、次のオプションを使用できます。

```
(ramius) ~> ./crosswork.py -h
usage: crosswork.py [-h] [--uri URI] --key KEY --keyid KEYID
 [--payload PAYLOAD] [--method {GET,POST}] [--host HOST]
 [--port PORT]
```

Exercise the REST API.

```
optional arguments:
 -h, --help show this help message and exit
 --uri URI The URI to run
 --key KEY A Cisco Crosswork Network Insights API Key
 --keyid KEYID A Cisco Crosswork Network Insights API Key ID
 --payload PAYLOAD The name of a file containing JSON data for POST API
 requests. Note: This option is available only for POST
 commands.
 --method {GET,POST} The HTTP method for the request
 --host HOST The Cisco Crosswork Network Insights URL
```

```
--port PORT The Cisco Crosswork Network Insights port number
(ramius) ~>
```

## Crosswork Cloud Network Insights クライアントスクリプト例

次のクライアントスクリプトの例は Python で記述されており、Crosswork Cloud Network Insights の REST API コールを作成、署名、および実行する方法を示しています。

```
#!/usr/bin/env python3

#
Copyright 2019 Cisco Systems Inc.
#
Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at
#
http://www.apache.org/licenses/LICENSE-2.0
#
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
#

import argparse
import binascii
import datetime
import hashlib
import hmac
import json
from typing import Dict, Any

import requests
import rfc3339
import sys
import urllib

from string import Template
from urllib.parse import urlparse

class Signature(object):
 # The order and white space usage is very important. Any change
 # can alter the signature and cause the request to fail.
 SIGNATURE_TEMPLATE = Template("""\
$param_method
$param_uri
$param_query_parameters
$param_key_id
$param_timestamp
$param_signature_version
$param_content_sha256
$param_content_type
$param_content_length""")

 def __init__(self, exrest):
 self.exrest = exrest

 def sign(self):
 exrest = self.exrest
```

```
string_to_sign = self.SIGNATURE_TEMPLATE.substitute({
 "param_method": exrest.method.upper(),
 "param_uri": exrest.url_encoded_uri,
 "param_query_parameters": exrest.url_encoded_query_parameters,
 "param_key_id": exrest.key_id,
 "param_timestamp": exrest.timestamp,
 "param_signature_version": exrest.signature_version,
 "param_content_sha256": exrest.content_sha256,
 "param_content_type": exrest.content_type,
 "param_content_length": exrest.content_length
})

Decode the key and create the signature.
secret_key_data = binascii.unhexlify(exrest.key)
hasher = hmac.new(secret_key_data, msg=string_to_sign.encode('utf-8'),
digestmod=hashlib.sha256)
signature = binascii.hexlify(hasher.digest())
return signature.decode('utf-8')
```

```
class ExRest(object):
 SIGNATURE_VERSION = "1.0"
 CONTENT_TYPE = "application/json"

 HEADER_CONTENT_TYPE = "Content-Type"
 HEADER_CONTENT_LENGTH = "Content-Length"
 HEADER_SIGNATURE_VERSION = "X-Cisco-Crosswork-Cloud-Signature-Version"
 HEADER_TIMESTAMP = "Timestamp"
 HEADER_AUTHORIZATION = "Authorization"

 def __init__(self):
 # Input arguments to the script.
 self.uri = None
 self.payload = None
 self.method = None
 self.host = None
 self.port = None
 self.key = None
 self.key_id = None

 # Values used to calculate the signature.
 self.url_encoded_uri = None
 self.url_encoded_query_parameters = None
 self.timestamp = None
 self.content_sha256 = None
 self.content_length = 0
 self.content_type = self.CONTENT_TYPE
 self.signature_version = self.SIGNATURE_VERSION

 def run(self):
 # Calculate the full URI to be run.
 uri = self.uri[1:] if self.uri.startswith("/") else self.uri
 self.uri = f"https://{self.host}:{self.port}/{uri}"

 # The url encoded uri is used when calculating the request signature.
 parsed_uri = urlparse(self.uri)
 self.url_encoded_uri = urllib.parse.quote(parsed_uri.path, safe='')
 self.url_encoded_query_parameters = urllib.parse.quote(parsed_uri.query)

 # Calculate the rfc3339 timestamp for the request.
 now = datetime.datetime.now()
 self.timestamp = rfc3339.rfc3339(now)
```

```

 # Calculate the SHA256 of the body of the request, even if the body is empty.
 self.content_sha256, self.content_length, payload_contents =
self.calculate_content_sha256(self.payload)

 # Calculate a signature for the request.
 signer = Signature(self)
 request_signature_b64 = signer.sign()

 # Create the request object and set the required http headers.
 headers = dict()

 headers[self.HEADER_AUTHORIZATION] = "hmac {}:{}".format(self.key_id,
request_signature_b64)
 headers[self.HEADER_TIMESTAMP] = self.timestamp
 headers[self.HEADER_CONTENT_TYPE] = self.content_type
 headers[self.HEADER_SIGNATURE_VERSION] = self.SIGNATURE_VERSION

 session = requests.Session()

 response = session.request(self.method, self.uri, data=payload_contents,
headers=headers)

 parsed_response: Dict[str, Any] = dict()
 if len(response.content) > 0:
 content = response.content.decode('utf-8')
 try:
 parsed_response = json.loads(content)
 except ValueError:
 parsed_response = dict()
 parsed_response["Message"] = content.strip()

 if response.status_code != 200:
 parsed_response["HttpStatus"] = response.status_code

 print(json.dumps(parsed_response, indent=2))

def calculate_content_sha256(self, payload):
 if payload:
 try:
 with open(payload) as fd:
 payload_contents = fd.read()
 except Exception as error:
 raise Exception(f'Cannot read payload file {payload}: {error}')
 else:
 payload_contents = ""

 hasher = hashlib.sha256()
 hasher.update(payload_contents.encode('utf-8'))

 content_sha256 = binascii.hexlify(hasher.digest())

 return content_sha256.decode('utf-8'), len(payload_contents), payload_contents

def main():
 parser = argparse.ArgumentParser(description="Exercise the REST API.")

 parser.add_argument("--uri", default="/api/beta/trufalse/1/200",
 help="The URI to run")

 parser.add_argument("--key", required=True,
 help="A Cisco Crosswork Network Insights API Key")

 parser.add_argument("--keyid", required=True,

```



```
 help="A Cisco Crosswork Network Insights API Key ID")

 parser.add_argument("--payload",
 help="The name of a file containing JSON data for POST API requests")

 parser.add_argument("--method", choices=["GET", "POST"], default="GET",
 help="The HTTP method for the request")

 parser.add_argument("--host", default="crosswork.cisco.com",
 help="The Cisco Crosswork Network Insights URL")

 parser.add_argument("--port", type=int, default=443,
 help="The Cisco Crosswork Network Insights port number")

 # Parse the arguments
 args = parser.parse_args()

 exrest = ExRest()

 exrest.uri = args.uri
 exrest.payload = args.payload
 exrest.method = args.method
 exrest.host = args.host
 exrest.port = args.port
 exrest.key = args.key
 exrest.key_id = args.keyid

 exrest.run()


if __name__ == "__main__":
 sys.exit(main())
```

## クライアントスクリプトの使用方法

この例では、次のタスクについて説明します：

- クライアントスクリプトから簡単なコールを行います。
- ペイロードオプションと設定ファイルを使用して、POST コマンドでプレフィックスを追加します。

### 始める前に

スクリプトを実行する前に、APIキーを要求します（[APIの使用開始（258ページ）](#)を参照）。APIの詳細については、Crosswork Cloud UI から  をクリックし、API リンクをクリックしてください。

**ステップ1** 次のスクリプトを実行します。

```
crosswork.py --uri '/api/beta/sourcedata?prefix=64.54.195.0%2F24&max=5' --key '<yourKeyHere>' --keyid '<yourKeyIdHere>'
```

結果の例：

```

{
 "data": [
 {
 "prefix": "64.54.195.0/24",
 "action": "ADD",
 "peerRemoteAsn": 22024,
 "timestamp": "2021-10-20T18:32:03Z",
 "origin": "IGP",
 "originAs": 5653,
 "asPath": [
 {
 "asn": [
 22024
]
 },
 {
 "asn": [
 6461
]
 },
 {
 "asn": [
 5653
]
 }
],
 "unicastPrefixType": "ADJ_RIB_IN",
 "nextHop": "4.4.94.118/32",
 "peerRemoteId": "549",
 "roaGenTime": "2021-06-29T05:25:53.844840001Z"
 },
 {
 "prefix": "64.54.195.0/24",
 "action": "ADD",
 "peerRemoteAsn": 202365,
 "timestamp": "2022-01-21T10:25:58Z",
 "origin": "IGP",
 "originAs": 5653,
 "med": {},
 "communities": [
 3792306480,
 3792306677,
 57866,
 41441,
 41441
],
 "asPath": [
 {
 "asn": [
 202365
]
 },
 {
 "asn": [
 57866
]
 },
 {
 "asn": [
 6461
]
 },
 {
 "asn": [

```

```

 5653
]
 }
],
"unicastPrefixType": "ADJ_RIB_IN",
"nextHop": "5.255.90.109/32",
"peerRemoteId": "248",
"roaGenTime": "2021-10-05T10:07:45.504885118Z"
},
(truncated)

```

## ステップ2 POST コマンドと設定ファイルでプレフィックスを追加します：

```
crosswork.py --uri '/api/beta/provision' --key '<yourKeyHere>' --keyid '<yourKeyIdHere>' --payload
"config.json" --method "POST"
```

### config.json ファイルのコンテンツ例：

```

{
 "operations": [
 {
 "setPrefixRequest": {
 "prefix": "4.4.4.4/32"
 },
 "o_creat": true,
 "o_excl": true
 },
 {
 "setPrefixRequest": {
 "prefix": "5.5.5.5/32"
 },
 "o_creat": true,
 "o_excl": true
 },
 {
 "setPrefixRequest": {
 "prefix": "6.6.6.6/32"
 },
 "o_creat": true,
 "o_excl": true
 },
 {
 "setPrefixRequest": {
 "prefix": "2001:30:102::/48"
 },
 "o_creat": true,
 "o_excl": true
 }
]
}

```

### 結果の例：

```

{
 "results": [
 {
 "setPrefixResponse": {
 "prefix": "4.4.4.4/32"
 }
 },
 {
 "setPrefixResponse": {
 "prefix": "5.5.5.5/32"
 }
 }
],
}

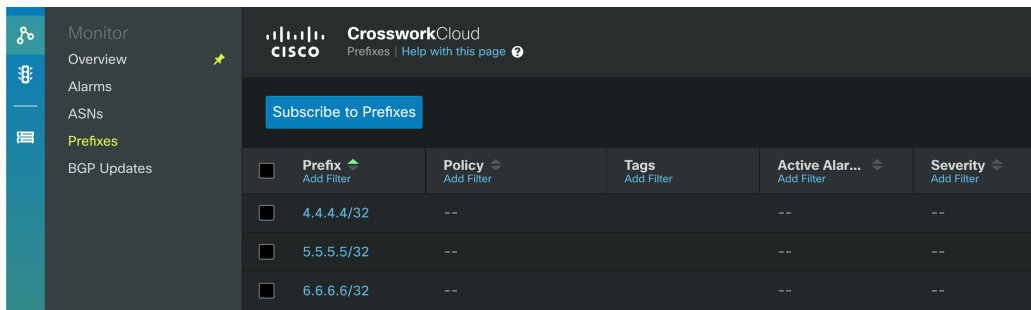
```

```

{
 "setPrefixResponse": {
 "prefix": "6.6.6.6/32"
 }
},
{
 "setPrefixResponse": {
 "prefix": "2001:30:102::/48"
 }
}
]
}

```

UI 結果の例 :



## Crosswork トラフィック分析クライアントスクリプトの例

次のスクリプトの例は、Python で記述されています。Crosswork Traffic Analysis API を実行するには、`python/get_traffic_example.py` および `python/cctrainic/cctrainic.py` が必要です。`get_traffic_example.py` を実行する前に、次のことを行う必要があります。

1. Python の依存関係をインストールします : `pip3 install -r requirements.txt`
2. API ベアラートークン (`export TOKEN=<token string>`) を設定します
3. `get_traffic_example.py` ファイルを編集します。次の値を正しい値に置き換えます : `api_version`、`device_name`、`start` および `end`。

`get_traffic_example.py` ファイルを編集した後、スクリプトを実行します : `python3 get_traffic_example.py`

スクリプトの例 : `get_traffic_example.py`

```

get_traffic_example.py

import os
import sys
from cctrainic import CCTrafficRestClient

host = "https://crosswork.cisco.com"

```

```
api_version = "beta"
device_name = "flow-automation-1"

start and end may be supplied as:
- ISO 8601 datetime string
- unix timestamp in seconds since 1970
- now
- "<number> <unit> ago" where unit can be: "seconds", "minutes", "hours", "days".
start = "7 days ago"
end = "now"

if "TOKEN" in os.environ:
 token = os.environ["TOKEN"]
else:
 print("Bearer token not found. Set bearer token with: export TOKEN=<token string>")
 sys.exit(-1)

client = CCTrafficRestClient(host, token, version=api_version, debug=False)

print(f"GetDevice for {device_name}")
device_info = client.GetDevice(device_name)
device_id = device_info["deviceId"]
print(f"Found device ID for {device_name}: {device_id}")

print(f"Traffic by interface for {device_name}")
traffic_for_my_device = client.GetInterfaceCounterTrafficTotals(start, end, device_id)
interface_name = traffic_for_my_device[0]["interfaces"][0]["interfaceName"]

print(f"Traffic by ASN for {device_name}/{interface_name}")
asn_traffic_for_my_device_interface = client.GetNetFlowTrafficTotalsByDevice(start, end,
 device_id, interface=interface_name, asn_breakdown=True)

print(f"Traffic by Prefix for {device_name}/{interface_name}")
prefix_traffic_for_my_device_interface = client.GetNetFlowTrafficTotalsByDevice(start,
 end, device_id, interface=interface_name, prefix_breakdown=True)

asn = asn_traffic_for_my_device_interface[0]["interfaces"][0]["asns"][0]["asn"]
device_prefix =
prefix_traffic_for_my_device_interface[0]["interfaces"][0]["prefixes"][0]["prefix"]

print(f"Traffic by Prefix for {device_name}/{interface_name} ASN {asn}")
prefix_traffic_for_my_device_interface_asn = client.GetNetFlowTrafficTotalsByDevice(
 start, end, device_id, interface=interface_name, asn=asn, asn_breakdown=True)

print(f"Traffic by Prefix")
prefix_traffic = client.GetNetFlowTrafficTotalsByPrefix(start, end)
prefix = prefix_traffic[0]["prefix"]

print(f"Traffic by Device for {prefix}")
device_traffic_for_prefix = client.GetNetFlowTrafficTotalsByPrefix(start, end, prefix)

print(f"Time series for {device_name}")
time_series_for_device = client.GetInterfaceCounterTrafficTimeSeries(start, end, device_id)

print(f"Time series for {device_name}/{interface_name}")
time_series_for_interface = client.GetInterfaceCounterTrafficTimeSeries(start, end,
 device_id, interface=interface_name)

print(f"Time series for {device_name}/{interface_name} {device_prefix}")
time_series_for_prefix = client.GetNetFlowTrafficTimeSeriesByDevice(start, end, device_id,
 interface=interface_name, prefix=device_prefix)

print(f"Time series for {device_name}/{interface_name} {asn}")
```

```
time_series_for_asn = client.GetNetFlowTrafficTimeSeriesByDevice(start, end, device_id,
 interface=interface_name, asn=asn)
```

### スクリプトの例 : cctrainc.py

```
cctrainc.py
Contains a very simple REST client to demonstrate how to call the Crosswork Cloud
Traffic APIs
Copyright (c) 2021 Cisco Systems, Inc. and others. All rights reserved.

import requests
from .util import UrlEncode

import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

class CCTrafficRestClient:

 def __init__(self, host: str, token, version: str = "v1", debug: bool = False):
 self.version = version
 self.host = host
 self.debug = debug
 self.headers = {"content-type": "application/json", "Authorization": f"Bearer
{token}"}

 def DoApiCall(self, url):
 if self.debug == True:
 print(url)
 response = requests.get(url, headers=self.headers, verify=False)
 if self.debug == True:
 print(response.status_code)
 print(response.content)
 return response

 def GetDevice(self, device_name: str):
 url = f"{self.host}/api/{self.version}/devices?name={device_name}"
 response = self.DoApiCall(url)
 if response.status_code != 200:
 return ""
 return response.json()["devices"][0]["deviceInfo"]

 def GetInterfaceCounterTrafficTotals(self, start: str, end: str, device_id: str =
 ""):
 start = UrlEncode(start)
 end = UrlEncode(end)

 if device_id == "":
 url = f"{self.host}/api/{self.version}/devices/statistics/totals"
 else:
 url =
f"{self.host}/api/{self.version}/devices/{device_id}/interfaces/statistics/totals"

 url += f"?format=totals&timeStart={start}&timeEnd={end}"
 response = self.DoApiCall(url)
 if response.status_code != 200:
 return ""
 return response.json()["devices"]

 def GetNetFlowTrafficTotalsByDevice(self, start: str, end: str, device_id: str,
 interface: str,
 asn: int = 0, prefix: str = "", asn_breakdown:
bool = False, prefix_breakdown: bool = False):
 interface = UrlEncode(UrlEncode(interface))
 prefix = UrlEncode(UrlEncode(prefix))
```

```
 start = UrlEncode(start)
 end = UrlEncode(end)

 if asn != 0:
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}/prefixes"

 elif asn_breakdown:
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns"

 elif prefix_breakdown:
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/prefixes"

 url += f"?format=totals&timeStart={start}&timeEnd={end}"
 response = self.DoApiCall(url)
 if response.status_code != 200:
 return ""
 return response.json()["devices"]

 def GetNetFlowTrafficTotalsByPrefix(self, start: str, end: str, prefix: str = "",
device_id: str = ""):
 prefix = UrlEncode(UrlEncode(prefix))
 start = UrlEncode(start)
 end = UrlEncode(end)

 if prefix == "":
 url = f"{self.host}/api/{self.version}/traffic/prefixes"
 elif device_id == "":
 url = f"{self.host}/api/{self.version}/traffic/prefixes/{prefix}/devices"
 else:
 url =
f"{self.host}/api/{self.version}/traffic/prefixes/{prefix}/devices/{device_id}/interfaces"

 url += f"?format=totals&timeStart={start}&timeEnd={end}"
 response = requests.get(url, headers=self.headers, verify=False)
 if response.status_code != 200:
 return ""
 return response.json()["prefixes"]

 def GetInterfaceCounterTrafficTimeSeries(self, start: str, end: str, device_id: str,
interface: str = ""):
 interface = UrlEncode(UrlEncode(interface))
 start = UrlEncode(start)
 end = UrlEncode(end)

 if interface == "":
 url = f"{self.host}/api/{self.version}/devices/{device_id}/statistics/totals"

 else:
 url =
f"{self.host}/api/{self.version}/devices/{device_id}/interfaces/{interface}/statistics/totals"

 url += f"?format=timeseries&timeStart={start}&timeEnd={end}"
 response = requests.get(url, headers=self.headers, verify=False)
 if response.status_code != 200:
 return ""
 return response.json()["devices"]

 def GetNetFlowTrafficTimeSeriesByDevice(self, start: str, end: str, device_id: str,
```

```
interface: str, asn: int = 0, prefix: str = ""):
 interface = UrlEncode(UrlEncode(interface))
 prefix = UrlEncode(UrlEncode(prefix))
 start = UrlEncode(start)
 end = UrlEncode(end)

 if asn == 0 and prefix != "":
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/prefixes/{prefix}"

 elif asn != 0 and prefix == "":
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}"

 else:
 url =
f"{self.host}/api/{self.version}/traffic/devices/{device_id}/interfaces/{interface}/asns/{asn}/prefixes/{prefix}"

 url += f"?format=timeseries&timeStart={start}&timeEnd={end}"
 response = self.DoApiCall(url)
 if response.status_code != 200:
 return ""
 return response.json()["devices"]
```





## 第 IX 部

# サブスクリプションの購入および管理

- サブスクリプションプランのオプションの表示 (273 ページ)
- Crosswork Cloud を購入する (275 ページ)
- サブスクリプションまたはトライアルをアクティブ化する (283 ページ)
- サブスクリプションとライセンスの表示 (285 ページ)
- サブスクリプションの変更 (287 ページ)
- サブスクリプションを別の組織に転送 (289 ページ)
- 組織名の変更 (291 ページ)






## 第 40 章

# サブスクリプションプランのオプションの表示

- [サブスクリプションプランのオプションの表示](#) (273 ページ)
- [無料のサブスクリプションプランの要件](#) (273 ページ)

## サブスクリプションプランのオプションの表示

利用可能なサブスクリプションプランと含まれている機能を表示するには、[こちら](#)をクリックするか、 > [購入 (Purchase)] > [階層情報 (Tier Information)] タブをクリックします。各製品タブ内でカテゴリを展開し、各層で利用可能なさまざまな機能を比較できます。

サブスクリプションを購入する場合は、『[Purchase through a Cisco Partner or Reseller](#)』[英語]または「[Purchase through Amazon Web Services \(AWS\) Marketplace](#)」[英語]を参照してください。

各 Crosswork Cloud 製品の詳細については、次のいずれかのデータシートを参照してください。


- [Crosswork External Route Analysis](#) (ネットワークインサイト)
- [Crosswork Traffic Analysis](#)
- [Crosswork Trust Insights](#)

## 無料のサブスクリプションプランの要件

無料のサブスクリプションプランを維持するには、次の要件の少なくとも1つを満たす必要があります。

- 組織のユーザーは、過去 90 日以内に Crosswork Cloud にログインする必要があります。
- 組織は、Crosswork Cloud Network Insights でアクティブなピア (完全なインターネットルーティングテーブルを使用) を維持する必要があります。
- 組織には、別のモジュールのアクティブな資格が必要です。

自動終了を回避するには、シスコパートナーまたはリセラーを通じて、Crosswork Cloud Network Insights で監視する IP ルートプレフィックスを少なくとも 1 つ購入するか、[Amazon Web Services \(AWS\) Marketplace](#) から購入してください。

無料のサブスクリプションプランで利用できる機能については、[ここ](#) をクリックするか、Crosswork Cloud 内の  > [購入 (Purchase)] > [サブスクリプション階層 (Subscription Tiers)] タブに移動します。



## 第 41 章

# Crosswork Cloud を購入する

Cisco Crosswork Cloud サブスクリプションは、次のいずれかの方法で購入できます。

- [Amazon Web Services \(AWS\) マーケットプレイスでの購入 \(275 ページ\)](#)
- [AWS Marketplace から直接購入 \(278 ページ\)](#)
- [シスコパートナーまたはリセラーを通じての購入 \(281 ページ\)](#)
- [購入に関する問題のトラブルシューティング \(281 ページ\)](#)

## Amazon Web Services (AWS) マーケットプレイスでの購入

The screenshot displays the Cisco Crosswork Cloud purchase interface. The main content area is titled 'Purchase' and includes a 'Purchase Crosswork Cloud Products' section. Three product cards are visible: 'NetworkInsights', 'TrustInsights', and 'TrafficAnalysis'. Each card has a 'Purchase' button. The 'NetworkInsights' card also features a 'Tier Selection' section with radio buttons for 'Premier', 'Advantage', and 'Essentials'. A sidebar on the left contains navigation links for 'Global', 'Purchase', 'Licensing', 'Users', 'Tools', and 'Import / Export'. A 'Contact Sales Team' button is located in the top right corner.



---

(注) いずれかの画像をクリックすると、フルサイズで表示されます。

---

### 始める前に

Crosswork Cloud を購入する最も簡単な方法は、Crosswork Cloud 内の AWS Marketplace を使用することです。AWS Marketplace から Crosswork Cloud を直接購入するには、[AWS Marketplace から直接購入](#)をクリックします。

次のアカウントを設定してください。


- [Cisco Connection Online \(CCO\)](#)
- [Crosswork Cloud](#)
- [AWS Marketplace](#) : 有効な AWS の [支払い方法](#) を設定し、最新のものにする **必要** があります。そうしないと、エラーが発生します。



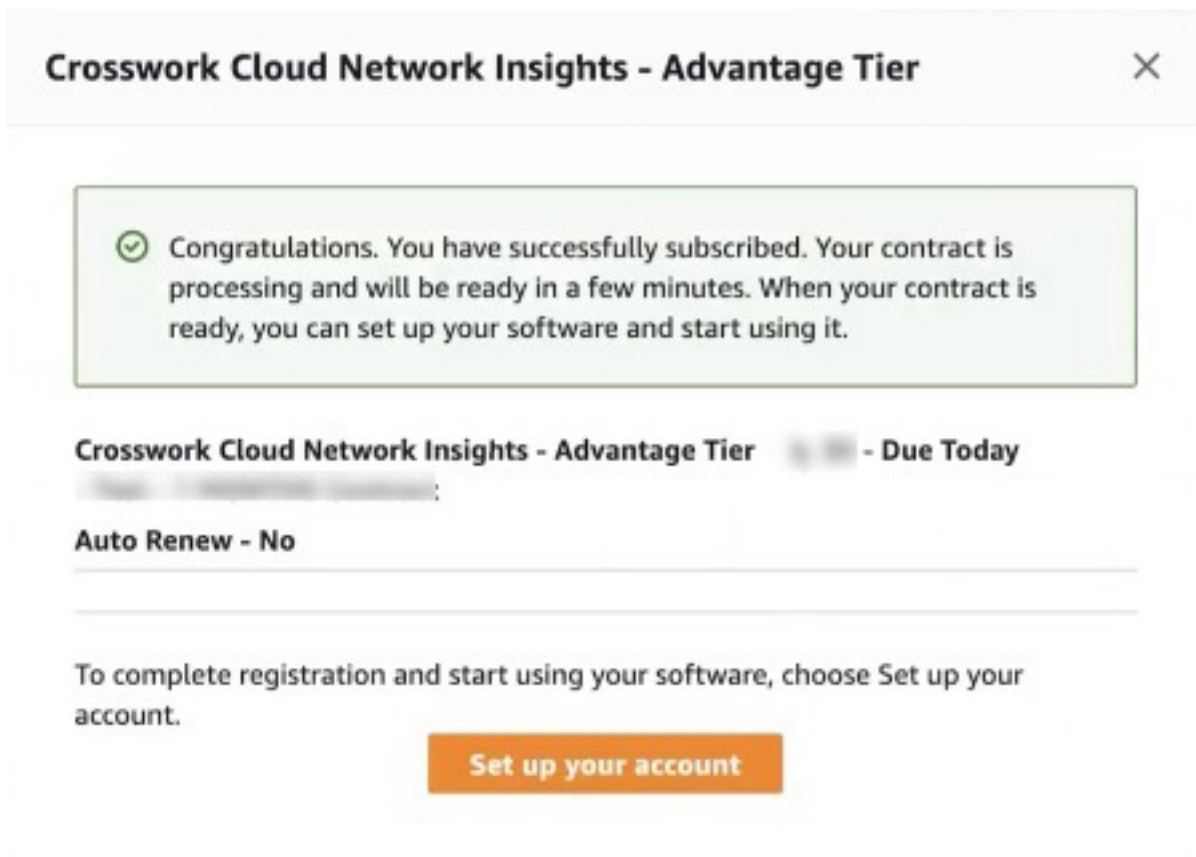
---

(注) この手順では、これらのアカウントがすでに設定され、Crosswork Cloud にログインしていることを前提としています。

---

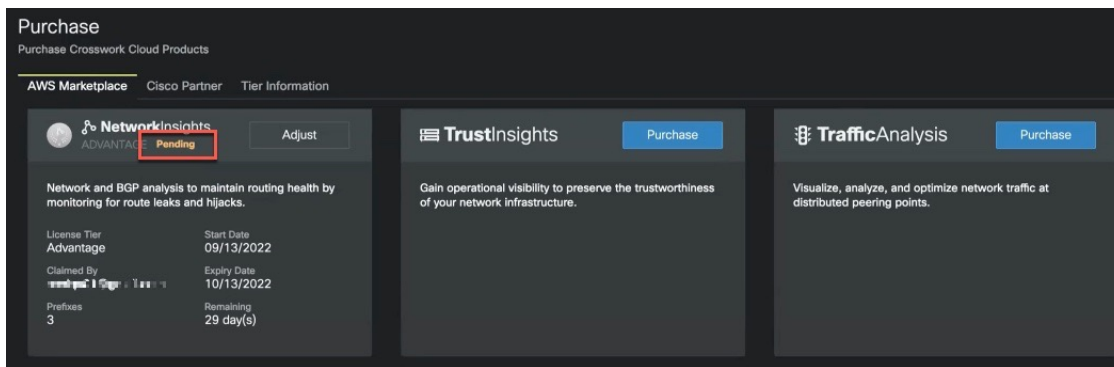
- 
- ステップ 1** メインウィンドウで、左下隅の  [購入 (Purchase) ] アイコンをクリックします。
- ステップ 2** [AWS Marketplace] タブをクリックします。
- ステップ 3** Crosswork Cloud Network Insights を購入する場合は、適切なライセンスの階層 (Premier、Advantage、Essentials) を選択し、[購入 (Purchase) ] をクリックします。それ以外の場合は、Crosswork Cloud Trust Insights または Crosswork Cloud Traffic Analysis のいずれかの [購入 (Purchase) ] をクリックします。
- AWS Marketplace ウェブサイトに移動します。
- ステップ 4** AWS Marketplace にログインします。Crosswork Cloud 製品の購入ページが表示されます。
- ステップ 5** [購入オプションの表示 (View purchase options) ] をクリックし、すべての必須フィールドに入力します。
- ステップ 6** [連絡先の作成 (Create contact) ] をクリックして、情報を確認します。
- ステップ 7** [今すぐ支払う (Pay Now) ] をクリックします。正常終了メッセージが表示されます。
- ステップ 8** [アカウントの設定 (Set up your account) ] をクリックすると、Crosswork Cloud の [購入 (Purchasing) ] ページに移動します。

例 :



**ステップ 9** Crosswork Cloud 製品は、AWS Marketplace のすべてのデータの詳細を受信するまで、ステータスが数分間保留中になる場合があります。

例 :



**ステップ 10** [購入 (Purchase)] > [ライセンス (Licensing)] > [資格 (Entitlement)] タブ > [<Crosswork-Cloud-Product>] に移動して、サブスクリプションを確認します。製品とサブスクリプションの詳細が表にリストされているはずです。

**ステップ 11** Crosswork Cloud サブスクリプションの購入が正常に完了すると、サブスクリプション ID が記載されたメールが届きます。後で Crosswork Cloud の資格をアクティブ化するために必要な場合に備えて、電子

メールのコピーを保持し、ID を保存します。詳細については、[サブスクリプションまたはトライアルをアクティブ化する \(249 ページ\)](#) を参照してください。

## AWS Marketplace から直接購入

AWS Marketplace から Crosswork Cloud を直接購入するには、次の手順を実行します。

### 始める前に

[AWS Marketplace](#) アカウントを持ち、支払い方法が設定されていることを確認する必要があります。

AWS Marketplace から Crosswork Cloud を直接購入する手順を以下で説明します。組織用に、または誰かの代理で Crosswork Cloud を購入する場合は、管理者（エンドユーザー）の電子メールアドレスを手元に用意してください。自身が Crosswork Cloud の管理者になる場合は、購入プロセスを効率的に進めるために次のアカウントを設定してください。

- [Cisco Connection Online \(CCO\)](#)
- [Crosswork Cloud](#)

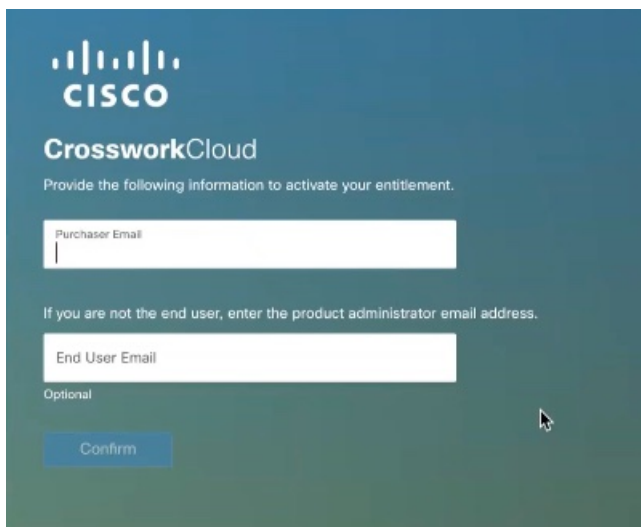


(注) CCO または Crosswork Cloud アカウントに登録していない場合は、購入プロセス中にそれぞれの Web サイトの登録画面に移動します。

- ステップ 1** アカウントに支払い方法が設定されていない場合は、[AWS Marketplace](#) にログインして支払い方法を設定します。
- ステップ 2** [検索 (Search)] フィールドに **Crosswork Cloud** と入力し、購入する製品を選択します。
- ステップ 3** [購入オプションの表示 (View purchase options)] をクリックし、すべての必須フィールドに入力します。
- ステップ 4** [連絡先の作成 (Create contact)] をクリックして、情報を確認します。
- ステップ 5** [今すぐ支払う (Pay Now)] をクリックします。正常終了メッセージが表示されます。
- ステップ 6** [アカウントの設定 (Set up your account)] をクリックすると、Crosswork Cloud の [購入 (Purchasing)] ページに移動します。
- ステップ 7** Crosswork Cloud に現在ログインしていない場合は、電子メールアドレスを入力します。エンドユーザーにならない場合は、次のウィンドウに製品の管理者の電子メールアドレスを入力し、[確認 (Confirm)] をクリックします。

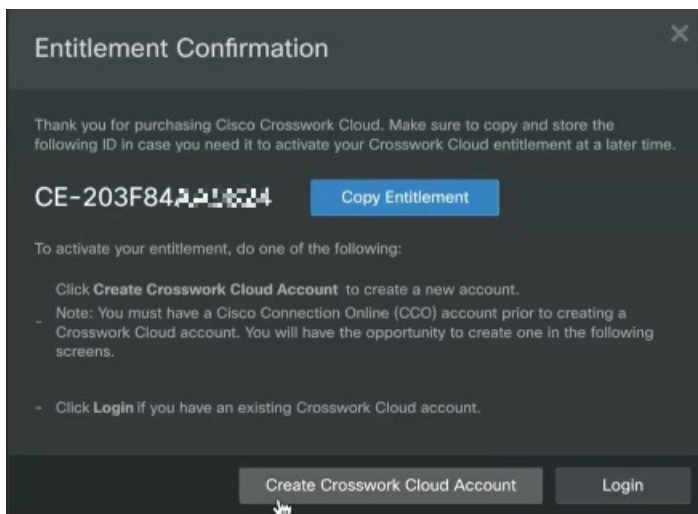
例：





- ステップ 8** いくつかの情報と資格 ID を含む電子メールアドレスの両方に電子メールが送信されます。Crosswork Cloud の管理者は、後で Crosswork Cloud の資格をアクティブ化するために必要な場合に備えて、電子メールのコピーを保持し、資格 ID を保存する必要があります。詳細については、「[サブスクリプションまたはトライアルをアクティブ化する \(249 ページ\)](#)」を参照してください。

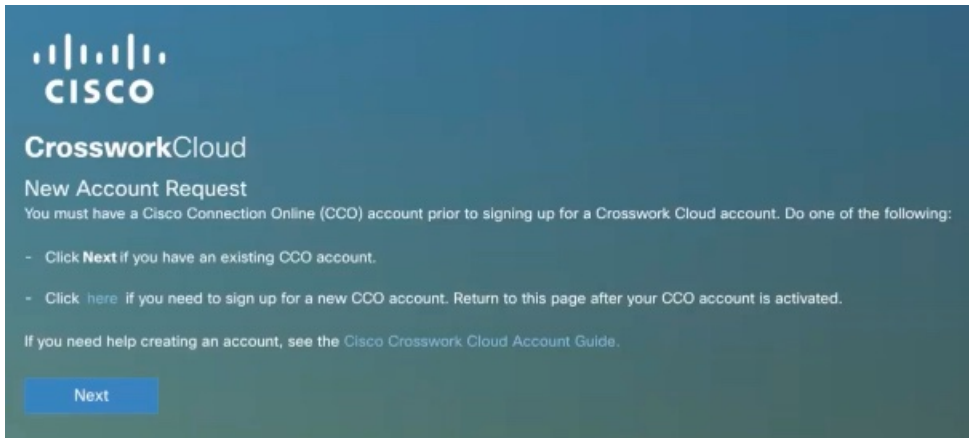
図 5: 資格確認の例



これ以降、購入者が Crosswork Cloud アカウントを作成しない限り、Crosswork Cloud の管理者は次の手順を実行する必要があります。

- ステップ 9** Crosswork Cloud アカウントをお持ちでない場合は、[Crosswork Cloud アカウントの作成 (Create Crosswork Cloud Account)] をクリックし、プロンプトに従ってアカウントを作成し、組織の設定を行います。Crosswork Cloud アカウントをお持ちの場合は、**ステップ 10** に進みます。

例 :



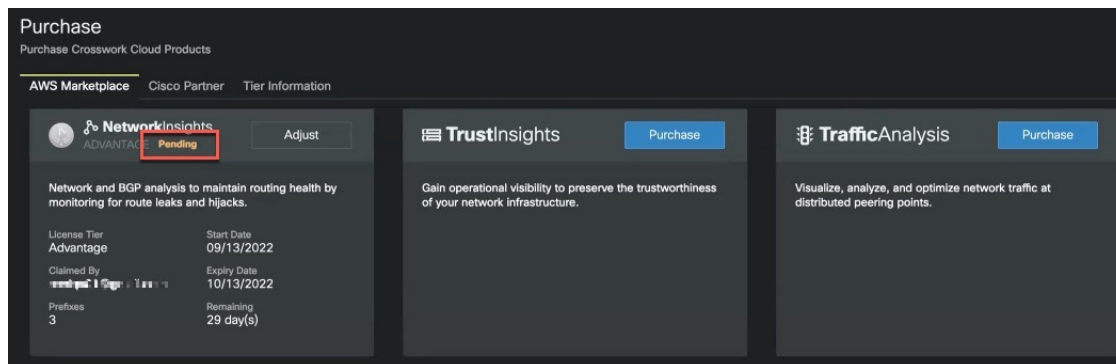
- (注) CCOアカウントを作成すると（または既存のCCOアカウントがある場合）、Crosswork Cloud アカウントを作成するために情報を入力するように求められます。

ステップ 10 Crosswork Cloud アカウントをお持ちの場合は、[ログイン (Login)] をクリックします。

**ステップ 11** ログイン情報を入力し、[ログイン (Login)] をクリックします。サブスクリプションが要求されたことを示す成功メッセージが表示されます。

**ステップ 12** [OK] をクリックして、メッセージを閉じます。[Crosswork Cloudの購入 (Crosswork Cloud Purchase)] ページが表示されます。資格は、以前に設定したテナント組織に自動的に関連付けられます。Crosswork Cloud 製品は、AWS Marketplace のすべてのデータの詳細を受信するまで、ステータスが**保留中**になる場合があります。

例：



**ステップ 13** [購入 (Purchase)] [👏] アイコン > [ライセンス (Licensing)] > [資格 (Entitlement)] タブ > [<Crosswork-Cloud-Product>] に移動して、サブスクリプションを確認します。製品とサブスクリプションの詳細が表にリストされているはずですが、

## シスコパートナーまたはリセラーを通じての購入

シスコパートナーまたはリセラーを通じて Crosswork Cloud を購入するには：

**ステップ 1** メインウィンドウで、左下隅の [👏] [購入 (Purchase)] アイコンをクリックします。


**ステップ 2** [販売購入 (Sales Purchase)] タブをクリックします。

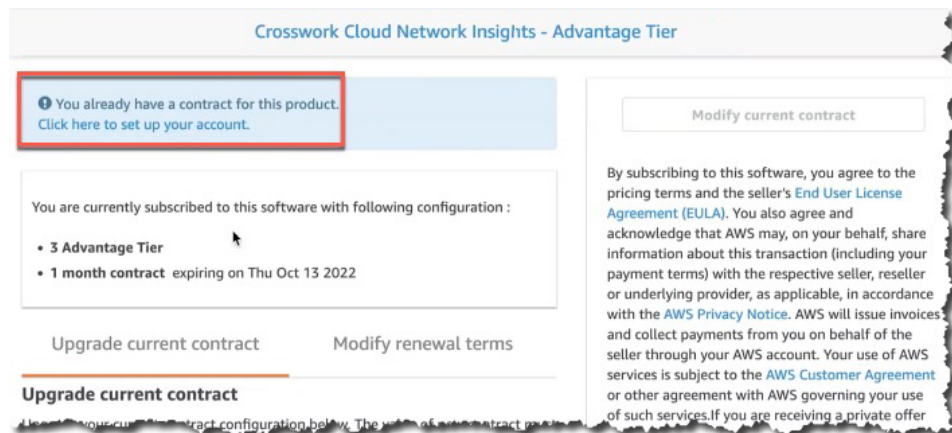
**ステップ 3** [営業チームに連絡 (Contact Sales Team)] をクリックします。

**ステップ 4** 購入したい Crosswork Cloud 製品を選択し、[送信 (Send)] をクリックします。

## 購入に関する問題のトラブルシューティング

このトピックでは、AWS Marketplace での購入に関する問題に遭遇したときにチェックできる役立つヒントや項目について説明します。購入に関する問題が解決しない場合は、[👏] > [購入サポート (Purchasing Support)] > [支払いサポート (Payment Support)] をクリックし、発生している問題の説明を入力して、[送信 (Submit)] をクリックします。

- AWS Marketplace で支払い方法が設定されていることを確認します。AWS Marketplace で利用できる有効な支払い方法の詳細については、<https://aws.amazon.com/premiumsupport/knowledge-center/accepted-payment-methods/> にアクセスしてください。
- Crosswork Cloud で、製品のステータスが**保留中**のままになっている場合は、ページを更新して、[購入 (Purchase)]  アイコン > [ライセンス (Licensing)] > [資格 (Entitlement)] タブ > [<Crosswork-Cloud-product>] をクリックし、製品がリストされているかどうかを確認します。Crosswork Cloud が AWS のサブスクリプション情報を取得するまでに数分かかる場合があります。
- AWS Marketplace で Crosswork Cloud 製品の購入ページに再度アクセスし、[Click here to set up your account] を選択して、購入プロセスを再開します。





## 第 42 章

# サブスクリプションまたはトライアルをアクティブ化する

- ・サブスクリプションまたはトライアルをアクティブ化する (283 ページ)

## サブスクリプションまたはトライアルをアクティブ化する

Crosswork Cloud でサブスクリプションをアクティブ化できます。



- (注) サブスクリプションをアクティブ化するには、管理者権限が必要です。詳細については、「[ユーザの役割 \(246 ページ\)](#)」を参照してください。

### 始める前に

サブスクリプションをアクティブ化するには、Crosswork Cloud サブスクリプションの購入後に提供されるか、メールで送られてくる 1 つ以上のサブスクリプション ID が必要です。

**ステップ 1** メインウィンドウで、左下隅の  [設定 (Settings)] アイコンをクリックします。

**ステップ 2** [ライセンス (Licensing)] をクリックします。

**ステップ 3** サブスクリプションをアクティブ化するには：

- [資格 (Entitlement)] > [外部ルート分析 (External Route Analysis)]、[信頼インサイト (Trust Insights)]、または [トラフィック分析 (Traffic Analysis)] タブをクリックします。
- [サブスクリプションの請求 (Claim Subscription)] をクリックし、テキストボックスにサブスクリプション ID を入力します。複数のサブスクリプション ID を追加するには、各 ID をカンマで区切るか、各 ID を新しい行に入力します。

**ステップ 4** Crosswork Cloud 製品のトライアルバージョンをリクエストするには：

- [トライアル (Trial)] タブをクリックします。

- b) 試したいCisco Crosswork Cloud製品の横にある[リクエスト (Request)]をクリックします。条件に同意し、[トライアルを開始 (Start Trial)]をクリックします。
-



## 第 43 章


# サブスクリプションとライセンスの表示

---

- [サブスクリプションとトライアルの詳細の表示 \(285 ページ\)](#)

## サブスクリプションとトライアルの詳細の表示

サブスクリプション、現在のライセンス、および有効なトライアルに関する詳細を表示するには、次の手順を実行します。

- 
- ステップ 1** メインウィンドウで、左下隅の  [設定 (Settings)] アイコンをクリックします。
  - ステップ 2** [ライセンス (Licensing)] をクリックします。
  - ステップ 3** サブスクリプションとライセンスの詳細を表示するには、[資格 (Entitlement)] タブをクリックし、興味のある Crosswork Cloud 製品を選択します。
  - ステップ 4** アクティブで利用可能なトライアルの数を表示するには、[トライアル (Trials)] タブをクリックします。
- 

### 次のタスク

サブスクリプションをキャンセルまたは更新するには、[サブスクリプションの変更 \(287 ページ\)](#) を参照してください。







## 第 44 章

# サブスクリプションの変更

- ・サブスクリプションの更新 (287 ページ)

## サブスクリプションの更新

許可されるプレフィックスの数 (Crosswork 外部ルート分析用) を増やす、または Crosswork Cloud サブスクリプションをキャンセルするには、次の手順を実行します。



(注) AWS Marketplace で購入したサブスクリプションを別の階層に変更するには、まず古いサブスクリプションをキャンセルしてから新しいサブスクリプションを購入する必要があります。

**ステップ 1** メインウィンドウで、左下隅の  [購入 (Purchase)] アイコンをクリックします。

**ステップ 2** AWS でサブスクリプションを購入した場合：

- [AWS 購入 (AWS Purchase)] タブをクリックします。
- サブスクリプションを変更する製品の [調整 (Adjust)] をクリックします。AWS Marketplace ウェブサイトに移動します。
- [購入オプションの表示 (View purchase options)] をクリックし、必要な変更を加えます。
- [現在の契約の変更 (Modify current contract)] をクリックします。Crosswork Cloud サブスクリプションの変更が正常に完了すると、確認メールが届きます。

**ステップ 3** サブスクリプションをシスコパートナーまたはリセラーを通じて購入した場合は、右上隅にある [営業チームに連絡 (Contact Sales Team)] をクリックして、サブスクリプションの変更をサポートする Crosswork Cloud の担当者に連絡してください。







## 第 45 章

# サブスクリプションを別の組織に転送

・サブスクリプションを別の組織に転送 (289 ページ)

## サブスクリプションを別の組織に転送

サブスクリプションを別の組織に移動するには、最初に以前の組織からサブスクリプション ID を削除してから、それを新しい組織に割り当てる必要があります。

- ステップ 1 別の組織に転送する前に、資格 ID が手元にあることを確認してください。資格 ID は、Crosswork Cloud アカウントが設定されたときに、最初に Crosswork Cloud の管理者に電子メールで送信されています。
- ステップ 2 現在サブスクリプションに関連付けられている組織にログインし、[購入 (Purchase)]  アイコン > [ライセンス (Licensing)] に移動します。
- ステップ 3 [資格 (Entitlement)] タブ > [<Crosswork-Cloud-product>] をクリックします。
- ステップ 4 移行するサブスクリプションの横にあるチェックボックスをオンにします。
- ステップ 5 表示される [削除 (Remove)] リンクをクリックします。
- ステップ 6 確認ウィンドウで [削除 (Remove)] をクリックして、サブスクリプションの削除を確認します。
- ステップ 7 登録する組織に移動し、[購入 (Purchase)]  アイコン > [ライセンス (Licensing)] に移動します。
- ステップ 8 [資格 (Entitlement)] タブ > [<Crosswork-Cloud-product>] をクリックします。
- ステップ 9 ページの右上にある、[サブスクリプションの請求 (Claim Subscription)] をクリックします。
- ステップ 10 資格 ID を入力し、[請求 (Claim)] をクリックします。





## 第 46 章


# 組織名の変更

---

- [組織名の変更 \(291 ページ\)](#)

## 組織名の変更

組織の名前を変更できます。

- 
- ステップ 1** メインウィンドウで、左下隅の  [設定 (Settings)] アイコンをクリックします。
  - ステップ 2** [ライセンス (Licensing)] をクリックします。
  - ステップ 3** [編集 (Edit)] をクリックします。
  - ステップ 4** 新しい組織名を入力し、[保存 (Save)] をクリックします。
-





## 第 **X** 部

# ユーザ設定の変更

- [ユーザ設定の変更 \(295 ページ\)](#)







## 第 47 章

# ユーザ設定の変更

---

- ユーザーインターフェイスのテーマの変更 (295 ページ)
- タイムゾーンの変更 (295 ページ)

## ユーザーインターフェイスのテーマの変更

次の3つのユーザーインターフェイスのテーマのいずれかを選択できます。

- ダーク (デフォルト)
- 低
- 高コントラスト

次の手順に従って、テーマを変更します。

---

**ステップ 1** 右上隅にあるユーザのイニシャルをクリックし、[設定 (My Settings)] を選択します。

**ステップ 2** [テーマ (Theme)] ドロップダウンリストからテーマを選択し、[保存 (Save)] をクリックします。

---

## タイムゾーンの変更

システムのタイムゾーンを変更できます。

---

**ステップ 1** 右上隅にあるユーザのイニシャルをクリックし、[設定 (My Settings)] を選択します。

**ステップ 2** [タイムゾーン (Timezone)] ドロップダウンリストからタイムゾーンを選択し、[保存 (Save)] をクリックします。

---





## 第 **XI** 部

### アラームの説明

- アラームの説明 (299 ページ)
- 予期しないASプレフィックス (Unexpected AS Prefix) (301 ページ)
- AS発信元違反 (AS Origin Violation) (303 ページ)
- 新しいASパスのエッジ (New AS Path Edge) (305 ページ)
- ASパス長違反 (AS Path Length Violation) (307 ページ)
- 親集約の変更 (Parent Aggregate Change) (309 ページ)
- プレフィックスアドバタイズメント (Prefix Advertisement) (311 ページ)
- プレフィックスの取り消し (Prefix Withdrawal) (313 ページ)
- ROAの有効期限 (ROA Expiry) (315 ページ)
- ROA障害 (ROA Failure) (317 ページ)
- ROAが見つからない (ROA Not Found) (319 ページ)
- DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal) (321 ページ)
- サブプレフィックスアドバタイズメント (SubPrefix Advertisement) (323 ページ)
- アップストリームASの変更 (Upstream AS Change) (325 ページ)
- 有効なASパス違反 (Valid AS Path Violation) (327 ページ)
- ピアの停止 (Peer Down) (329 ページ)
- 禁止されたIPプレフィックス (Prohibited IP Prefix) (331 ページ)
- ゲートウェイ接続 (333 ページ)
- デバイスの接続性 (335 ページ)
- インターフェイス TX の使用率 (337 ページ)
- インターフェイス RX の使用率 (339 ページ)

- プレフィックス使用率 (341 ページ)



## 第 48 章

# アラームの説明

- [アラームの説明 \(299 ページ\)](#)

## アラームの説明

このセクションには、アラームとリンクされた説明のリストが含まれています。アラームは、ポリシーのルール違反が発生するとトリガーされます。ポリシーの設定方法の詳細については、次のいずれかのトピックを参照してください。

- [Crosswork Cloud Network Insightsポリシーの追加 \(101 ページ\)](#)
- [Crosswork Cloud Traffic Analysisポリシーの追加 \(106 ページ\)](#)

表 32: *Crosswork Cloud Network Insights* アラーム

|                                                                |                                                                          |                                                                       |
|----------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <a href="#">予期しないASプレフィックス (Unexpected AS Prefix) (23 ページ)</a> | <a href="#">プレフィックスの取り消し (Prefix Withdrawal) (28 ページ)</a>                | <a href="#">アップストリームASの変更 (Upstream AS Change) (33 ページ)</a>           |
| <a href="#">AS発信元違反 (AS Origin Violation) (24 ページ)</a>         | <a href="#">ROAの有効期限 (ROA Expiry) (29 ページ)</a>                           | <a href="#">有効なASパス違反 (Valid AS Path Violation) (34 ページ)</a>          |
| <a href="#">新しいASパスのエッジ (New AS Path Edge) (25 ページ)</a>        | <a href="#">ROA障害 (ROA Failure) (30 ページ)</a>                             | <a href="#">ピアの停止 (Peer Down) (35 ページ)</a>                            |
| <a href="#">ASパス長違反 (AS Path Length Violation) (26 ページ)</a>    | <a href="#">ROAが見つからない (ROA Not Found) (30 ページ)</a>                      | <a href="#">アドバタイズされたプレフィックスの数 (Advertised Prefix Count) (35 ページ)</a> |
| <a href="#">親集約の変更 (Parent Aggregate Change) (27 ページ)</a>      | <a href="#">DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal) (31 ページ)</a> | <a href="#">禁止されたIPプレフィックス (Prohibited IP Prefix) (36 ページ)</a>        |

|                                                  |                                                       |  |
|--------------------------------------------------|-------------------------------------------------------|--|
| プレフィックスアドバタイズメント (Prefix Advertisement) (28 ページ) | サブプレフィックスアドバタイズメント (SubPrefix Advertisement) (32 ページ) |  |
|--------------------------------------------------|-------------------------------------------------------|--|

表 33: *Crosswork Cloud Traffic Analysis* アラーム

|                           |                     |                           |
|---------------------------|---------------------|---------------------------|
| ゲートウェイ接続 (36 ページ)         | デバイスの接続性 (37 ページ)   | インターフェイス TX の使用率 (38 ページ) |
| インターフェイス RX の使用率 (39 ページ) | プレフィックス使用率 (39 ページ) |                           |



## 第 49 章

# 予期しないASプレフィックス (Unexpected AS Prefix)

- [予期しないASプレフィックス \(Unexpected AS Prefix\)](#) (301 ページ)

## 予期しないASプレフィックス (Unexpected AS Prefix)

このアラームは、新しいプレフィックスが以前になかった AS の予期しない変更を検出します。モニタ対象の BGP AS から発信されるプレフィックスは、ピアしきい値の対象となる組織によって登録されていない場合、違反プレフィックスです。

### 考えられる検出される問題

このアラームは、新しいプレフィックスが以前に観察されなかった AS の予期しない変更またはルートリークのスナリオを特定するのに役立ちます。

### 関連するアラームルールの設定

このアラームルールを ASN 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)] > [ASNポリシー (ASN Policy)] > [ルールの追加 (Add Rule)] > [予期しないASプレフィックス (Unexpected AS Prefix)] )。

- [アラームのしきい値](#) (アドバタイズされたプレフィックスごと)
- [プレフィックスの設定](#)

### 例

[予期しないASプレフィックス (Unexpected AS Prefix)] アラームルールを使用して ASN ポリシーを作成し、モニタ対象の AS 15169 にリンクします。また、AS 15169 から発信されると予想されるすべてのプレフィックスにも登録されます。設定不備により、プレフィックス 8.8.0.0/24 が AS からリークされます。同時に、プレフィックス 9.9.0.0/24 は正しくアドバタイズされませんが、登録されません。ピアのしきい値に応じて、これらのイベントは両方ともアラームをト

リガーします。その後、プレフィックス 8.8.0.0/24 を取り消すように設定を修正し、アラームをクリアするプレフィックス 9.9.0.0/24 に登録できます。





## 第 50 章

# AS発信元違反（AS Origin Violation）

- [AS発信元違反（AS Origin Violation）](#)（303 ページ）

## AS発信元違反（AS Origin Violation）

このアラームは、発信元 AS を持つモニタ対象プレフィックスのアドバタイズメントが [AS発信元リスト（AS Origin List）] にない場合に検出します。これは違反アドバタイズメントであり、特にアドバタイズメントの AS パス長が正規のアドバタイズメントよりも短い場合に、プレフィックスハイジャックの試みを表す可能性があります。



- (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（94 ページ）](#) 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（101 ページ）](#)、

### 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プレフィックスハイジャックの特定に役立ちます。

### 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発信元違反（AS Origin Violation）]）。

- [アラームのしきい値](#)
- 許可された発信元 ASN

**例**

プレフィックス 8.8.8.0/24 の [AS発信元違反 (AS Origin Violation) ]アラームルールでプレフィックスポリシーを作成し、[AS発信元リスト (AS Origin List) ]フィールド値が 15169 で設定されています。しかし、確認された BGP 更新が 8.8.8.0/24 および 109 の発信元 AS で受信されます。AS 109 が [AS発信元リスト (AS Origin List) ]に含まれていないために、このアラームがトリガーされます。



## 第 51 章

# 新しいASパスのエッジ (New AS Path Edge)

- [新しいASパスのエッジ \(New AS Path Edge\)](#) (305 ページ)

## 新しいASパスのエッジ (New AS Path Edge)

このアラームは、以前に確認されていない新しい AS ピアリングを検出します。

中間者 (MITM) 攻撃では、攻撃者が自身の AS をプレフィックスの AS パスに挿入し、AS を介してプレフィックスのトラフィックを誘導します。攻撃の検出を回避するために、MITM 攻撃は通常短命で、少数のプレフィックスをターゲットとします。

一時的な AS ピアリングの別の原因として、すぐに修正されるオペレータエラーが考えられます。



- (注) AS ピアリング関係は、多くのピアによってアドバタイズされた多数のプレフィックスの AS パスに存在するか、または長期間存続しますが、正当なネットワーク設定の変更である可能性が高く、Crosswork Cloud Network Insights ではこれらのアラートは表示されません。

### 考えられる検出される問題

このアラームは、潜在的な MITM 攻撃またはオペレータエラーの特定に役立ちます。

### 例

[新しいASパスのエッジ (New AS Path Edge)] 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 にリンクします。アラームは、Crosswork Cloud Network Insights が、疑わしい AS ピアリング (すべてのプレフィックスのすべてのパスで以前に確認されていないピアリング、または新しいピアリング) を含む AS パスでプレフィックス 8.8.0.0/24 がアドバタイズされたことを検出したときにトリガーされます。一定の時間が経過すると、Crosswork Cloud Network Insights は、これらの AS ピアリング関係が長期間存続していると判断します。ピアリング関係が長期間存続していると判断されると、アラームはクリアされます。





## 第 52 章

# ASパス長違反（AS Path Length Violation）

- [ASパス長違反（AS Path Length Violation）](#)（307 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（94 ページ）](#) 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（101 ページ）](#)、

### 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) ] 。

- [アラームのしきい値](#)
- [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せん。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。



## 第 53 章

# 親集約の変更（Parent Aggregate Change）

- ・親集約の変更（Parent Aggregate Change）（309 ページ）

## 親集約の変更（Parent Aggregate Change）

このアラームは、予期しないスーパーネットまたはしきい値違反を検出します。

ネットワークオペレータは通常、アドバタイズされたプレフィックスの直接のスーパーネットプレフィックス（集約またはサマリー）、およびその他の集約された上位スーパーネット、およびそれらの発信元 AS を認識しています。ユーザは、Classless inter-domain routing（CIDR）プレフィックス長を指定して、予想される IPv4 および IPv4 スーパーネットのセットを少なくとも 1 つ設定する必要があります。ユーザは、許可された送信元 AS のリストから、観測された集約が発信されるように強制することもできます。



- (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（94 ページ）](#) 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（101 ページ）](#)、

### 考えられる検出される問題

このアラームは、サマリープレフィックスの誤った取り消しやルートリークを特定するのに役立ちます。

### 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) ] > [親集約の変更 (Parent Aggregate Change) ]。

- [アラームのしきい値](#) (アドバタイズされた集約ごと)
- [許可された発信元ASN (Allowed Origin ASNs) ] (オプション)
- [許可されるIPv4/IPv6スーパーネット (Allowed IPv4/IPv6 supernets) ]

#### 例

[親集約の変更 (Parent Aggregate Change) ] 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 にリンクします。ポリシーは、許可された IPv4 集約プレフィックス長 [22, 9] および許可された発信元 AS 3356 で設定されます。次のイベントがアラームをトリガーします。

- 予想されるスーパーネット 8.8.0.0/22 がハイジャックされます (プレフィックスは予期しない発信元 AS から発信されます)。
- 集約、プレフィックス 8.8.0.0/20 がアドバタイズされ、潜在的なリークとして識別されます。

リークまたはハイジャックが解決されるか、ユーザがアラーム設定を変更して、これらの集約アドバタイズメントが正当であることを示すと、アラームはクリアされます。





## 第 54 章

# プレフィックスアドバタイズメント (Prefix Advertisement)

・ [プレフィックスアドバタイズメント \(Prefix Advertisement\)](#) (311 ページ)

## プレフィックスアドバタイズメント (Prefix Advertisement)

このアラームは、モニタ対象プレフィックスの優先 BGP パスでの予期しない変更を検出します。したがって、プレフィックスのアドバタイズされたパスの BGP 属性に対する予期しない変更をモニタし、潜在的なルートリークの広がりを確認できます。



(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 \(94 ページ\)](#) 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 \(101 ページ\)](#)、

### 考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスの優先 BGP パスの変更を特定するのに役立ちます。

### 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) ]>[プレフィックスアドバタイズメント (Prefix Advertisement) ]。

- [アラームのしきい値](#)



## 第 55 章

# プレフィックスの取り消し (Prefix Withdrawal)

- [プレフィックスの取り消し \(Prefix Withdrawal\)](#) (313 ページ)

## プレフィックスの取り消し (Prefix Withdrawal)

このアラームは、ピアがプレフィックスを取り消した場合に検出します。

少数の BGP ピアからのプレフィックスの取り消しは、プレフィックスに到達する複数のパスがあるため、必ずしもプレフィックスが到達不能であることを意味しません。ただし、多数のピアが地理的エリアのプレフィックスを取り消すと、プレフィックスの到達可能性が低下する可能性があります。ルータのフラップによるノイズを抑制するために、このアラームのしきい値を他のアラームよりも高く設定することをお勧めします。



- (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 \(94 ページ\)](#) 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 (101 ページ) 、

### 考えられる検出される問題

このアラームは、プレフィックスの取り消しにつながる設定不備を特定するのに役立ちます。

### 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) ] > [プレフィックスの取り消し (Prefix Withdrawal) ]。

- [アラームのしきい値](#)



## 第 56 章

# ROAの有効期限（ROA Expiry）

- ROAの有効期限（ROA Expiry）（315 ページ）

## ROAの有効期限（ROA Expiry）

このアラームは、Route Origin Authorization（ROA）レコードの有効期限が切れる前に警告します。ROA レコードは、リソース（アドバタイズされたプレフィックス）の所有権を主張するオペレータによって作成され、地域インターネットレジストリ（RIR）またはルーティング資産データベース（RADB）などの他のサービスによって暗号化されて配布されます。詳細については、[ripe.net](http://ripe.net) を参照してください。

ROA レコードの有効期限切れの何日前にアラートを送信するかを指定できます。これは、情報提供を目的とするアラームです。新しいレコードを作成するアクションを実行して、ルータによるプレフィックスの考えられるフィルタリングを回避できます。このアラームは、プレフィックスが ROA レコードでカバーされていて、現在と設定したトリガー間隔の間（現在 + [有効期限が切れる前にトリガーする日数（Days to Trigger Before Expiration）]）のどの時点でも、プレフィックスに有効な ROA レコードがない場合にアクティブになります。特に、期限切れのレコードと期限が切れていないレコードが混在している場合、設定された間隔内のいずれかの時点で期限が切れていないカバーしているレコードが存在する限り、アラームはアクティブになりません。

### 考えられる検出される問題

このアラームは、保留中の ROA カバレッジの欠如を検出します。

### 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）] > [ROAの有効期限（ROA Expiry）]）。

- ROA レコードの期限が切れる前にトリガーする日数。

**例**

[ROAの有効期限 (ROA Expiry)] 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、[有効期限が切れる前にトリガーする日数 (Days to Trigger Before Expiration)] に 30 を指定して、プレフィックス 8.8.0.0/24 にリンクします。このアラームは、プレフィックス 8.8.0.0/24 が複数の ROA レコードでカバーされている場合にトリガーされ、Crosswork Cloud Network Insights はこれらすべてのレコードがすでに期限切れになっているか、または 30 日未満で期限切れになることを検出します。アラームをクリアするには、トリガー時間間隔をカバーする 8.8.0.0/24 に対して少なくとも 1 つの ROA レコードを作成する必要があります。



## 第 57 章

# ROA障害（ROA Failure）

- [ROA障害（ROA Failure）](#)（317 ページ）

## ROA障害（ROA Failure）

このアラームは、モニタ対象プレフィックスの [ROA 有効性状態](#)が無効かどうかを示します。発信元 AS がプレフィックスをカバーする ROA レコードにない、モニタ対象プレフィックスのアドバタイズメントは、違反アドバタイズメントです。アラームは、プレフィックスの観測されたすべての送信元 ASN を含む ROA レコードの追加、またはすべてのレコードの期限切れのいずれかによりクリアされます。具体的には、このアラームは、ROA レコードがない（存在しない、またはすべてが期限切れになっている）場合はアクティブになりません。

ROA の詳細については、[ripe.net](#) を参照してください。

### 考えられる検出される問題

このアラームは、プレフィックスハイジャックの試行を特定するのに役立ちます。

### 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）]>[ROA障害（ROA Failure）]）。

- [アラームのしきい値](#)







## 第 58 章

# ROAが見つからない (ROA Not Found)

---

- [ROAが見つからない \(ROA Not Found\)](#) (319 ページ)

## ROAが見つからない (ROA Not Found)

プレフィックスは、それをカバーする複数のROAレコードを持つことができます。このアラームは、モニタ対象のプレフィックスにROAレコードがない（存在しない、または期限切れになっている）場合にトリガーされます。これにより、RTRプロトコルを実装するルータによってプレフィックスがドロップされることを回避できます。

ROAの詳細については、[ripe.net](http://ripe.net)を参照してください。

### 考えられる検出される問題

これは、モニタ対象のプレフィックスにROAレコードがないことをユーザに警告する情報アラームです。

ROAが見つからない (ROA Not Found)



## 第 59 章

# DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)

• [DNSルートプレフィックスの取り消し \(DNS Root Prefix Withdrawal\)](#) (321 ページ)

## DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)

IANAによって割り当てられ、OpenDNSとGoogleによって提供されるサーバーを含むパブリックDNSルートサーバーは、通常のルーティング操作がパブリックインターネットルーティングに参加するために必要です。このアラームは、DNSサーバアドレスが属する一連のプレフィックス（ネットブロック）をモニタします。セット内のいずれかのプレフィックスが取り消されると、ユーザに警告します。



(注) このアラームは[プレフィックスの取り消し (Prefix Withdrawal)]アラームとは異なります。これらのプレフィックスは、ユーザがサブスクリプションで消費するプレフィックスの合計量に追加されず、アラームルールにリンクされたピアからの取り消しだからです。

### 考えられる検出される問題

このアラームは、既知のルートDNSサーバプレフィックスがモニタ対象ピアのルーティングテーブルから削除されたかどうかを検出します。このアラームは、DNSルートサーバーの撤回につながるインターネットルータの不良構成を特定するのに役立ちます。

### 関連するアラームルールの設定

このアラームルールをピア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)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal)] )。

- 監視対象の DNS ルートサーバー

#### 例

[DNSルートプレフィックスの取り消し (DNS Root Prefix Withdrawal) ] アラームルールを使用してピアポリシーを作成し、ピア RTR1 にリンクします。プレフィックス 198.41.0.0/24 (A ルートサーバ) および 2001:7fd::/48 (K ルートサーバ) に対するアラートを受け取ることを選択します。アラームは、これらのプレフィックスのいずれかが RTR1 によって取り消されるとアクティブになり、両方がアドバタイズされるとクリアされます。



## 第 60 章

# サブプレフィックスアドバタイズメント (SubPrefix Advertisement)

- [サブプレフィックスアドバタイズメント \(SubPrefix Advertisement\)](#) (323 ページ)

## サブプレフィックスアドバタイズメント (SubPrefix Advertisement)

ハイジャッカーは、ルータが新しいサブプレフィックスをインストールすることで、モニタ対象プレフィックスによってカバーされる IP スペースの一部のトラフィックをリダイレクトできます。これは、ルータが具体的ではないルートよりも具体的なルートを優先するためです。ハイジャッカーは、既存のサブプレフィックスの新しいルートをインストールすることもできます。これらのハイジャックの試行を検出するために、サブプレフィックスの許可された発信元 ASN のリストを設定できます。このアラームの場合、違反アドバタイズメントは、アドバタイズされたサブプレフィックスとそのピアのしきい値のいずれかが違反している場合です。

### 考えられる検出される問題

このアラームは、ルートリークまたはモニタ対象プレフィックスのサブプレフィックスのハイジャックを特定するのに役立ちます。

### 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)] > [サブプレフィックスアドバタイズメント (SubPrefix Advertisement)] )。

- [プレフィックスの設定](#)
- アドバタイズされたサブプレフィックスごとのしきい値 (Peers to Resolve および Peers to Trigger) [アラームのしきい値 \(347 ページ\)](#)

- 許可された発信元 ASN



---

(注) 発信元 ASN リストを無視するには、[発信元ASNリストを使用 (Use Origin ASNs)] オプションを [いいえ (No)] に切り替えます。発信元 ASN リストが無視されると、すべての ASN に対してアラームがトリガーされます。

---

- IPv4/IPv6 の最大長：設定された IPv4/IPv6 の最大長よりも長いサブプレフィックスマスクを無視するオプションを使用できます。IPv4 の最大長は 8 より大きく、IPv6 の最大長は 16 より大きい必要があります。

### 例

[サブプレフィックスアドバタイズメント (Subprefix Advertisement)] 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 にリンクします。次のサブプレフィックスアドバタイズメントが発生し、アラームがトリガーされます。

- 予期しないサブプレフィックス 8.8.0.5/30 がアドバタイズされます。この場合、このプレフィックスは新しい管理組織に割り当てられ、新しい発信元 AS から初めてアドバタイズされます。このアラームをクリアするには、サブプレフィックス 8.8.0.5/30 を登録するように Crosswork Cloud Network Insights を設定するか、または新しい発信元 AS を許可された発信元 ASN のリストに追加します。
- 予期しないサブプレフィックス 8.8.0.4/30 がアドバタイズされます。これは、ルートリークまたはハイジャックのいずれかを示している可能性があります。このアラームをクリアするには、8.8.0.4/30 を取り消す必要があります。



## 第 61 章

# アップストリームASの変更（Upstream AS Change）

- ・ [アップストリームASの変更（Upstream AS Change）](#)（325 ページ）

## アップストリームASの変更（Upstream AS Change）

BGP オペレータは、アウトバウンドポリシー（たとえば、どのアップストリーム AS がプレフィックスを伝播できるか）によってピアリング関係を制御できます。このアラームは、プレフィックスを伝播しない既存のピアへのルートリークを検出します。ユーザは、許可されたアップストリーム ASN のリストを設定する必要があります。リストにないアップストリーム AS パスに 1 ホップが残っている ASN を持つモニタ対象プレフィックスのアドバタイズメントは、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（MyPeers）]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（MyPeers）]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（94 ページ）](#) 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（101 ページ） 、

### 考えられる検出される問題

このアラームは、モニタ対象プレフィックスのルートリークを特定するのに役立ちます。

### 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) ]>[アップストリームASの変更 (Upstream AS Change) ]。

- [アラームのしきい値](#)
- [許可されるアップストリームASN (Allowed upstream ASNs) ]

#### 例

[アップストリームASの変更 (Upstream AS Change) ]アラームルールで許可されたアップストリームASN[293,1221]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にリンクします。プレフィックス8.8.0.0/24は、ASパス[2711, 1299, 3356]を持つピアによってアドバタイズされます。AS1299は許可されたアップストリームASNではないため、しきい値が適用されて、アラームがトリガーされます。違反しているASパスを持つルートが取り消されるか、許可されたアップストリームASNのリストにAS1229が追加されると、アラームはクリアされます。





## 第 62 章

# 有効なASパス違反 (Valid AS Path Violation)

- [有効なASパス違反 \(Valid AS Path Violation\)](#) (327 ページ)

## 有効なASパス違反 (Valid AS Path Violation)

このアラームは、プレフィックスアドバタイズメント AS パスが指定された ASN パターンと一致しない場合に検出します。

Crosswork Network Insights は、設定された**有効な AS パスパターン**を、アドバタイズされたプレフィックスの AS パスと比較します。ASN パターンは、スペースで区切った AS 番号を順に並べた予測されるシーケンスであり、107 3462 109 のように発信元 AS で終わります。演算子を使用して複雑なパターンを表現できます。パターンが一致しない場合は、Crosswork Network Insights はアラームをトリガーしてアクティブにします。



- (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 \(94 ページ\)](#) 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 (101 ページ) 、

パターンの例 : [0-]\* 806 \* 200

- 有効な AS パス : 1900 1731 806 100 200
- 違反 AS パス : 1900 1731 807 100 200
- 違反 AS パス : 1900 1731 806 150 100 200

### 考えられる検出される問題

このアラームは、潜在的なMITM攻撃または遅延の低下を示す予期しないBGP ASパスの変更を検出します。

### 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)] > [有効なASパス違反 (Valid AS Path Violation)] )。

- [アラームのしきい値](#)



## 第 63 章

# ピアの停止 (Peer Down)

---

- [ピアの停止 \(Peer Down\)](#) (329 ページ)

## ピアの停止 (Peer Down)

このアラームは、Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションの状態をモニタします。Crosswork Cloud Network Insights とモニタ対象ピアとの間のピアリングセッションが、予測されていた確立状態でない場合に、問題が発生する可能性があります。ピアリングセッションが確立状態になると、アラームはクリアされます。

### 考えられる検出される問題

このアラームは、モニタ対象ピアでの BGP プロセスの問題、またはピアリングに影響を与えるハードウェアやソフトウェアの問題を特定するのに役立ちます。

ピアの停止 (Peer Down)



## 第 64 章

# 禁止されたIPプレフィックス (Prohibited IP Prefix)

- [禁止されたIPプレフィックス \(Prohibited IP Prefix\)](#) (331 ページ)

## 禁止されたIPプレフィックス (Prohibited IP Prefix)

このアラームは、監視対象ピアの Routing Information Base (RIB) にインストールされているパブリック IP ルーティングスペースに禁止されたプレフィックスがあるか、または監視対象ピアがそれを転送している場合に検出します。

Bogon は、予約されているか、地域インターネットレジストリ (RIR) に割り当てられていないため、パブリックではない IP アドレスブロックです。[フルBogon (Full bogons)] には、RIR に割り当てられているが、RIR によって特定のネットワークに割り当てられていないアドレスブロックも含まれます。禁止されたプレフィックスのアドバタイズメントをルータでフィルタリングすることをお勧めします。ユーザーは、このアラームを使用して、Bogon アドバタイズメントについてのみアラートを受け取るように選択できます。

### 考えられる検出される問題

このアラームは、ルータに対する DoS 攻撃の特定に役立ちます。

### 関連するアラームルールの設定

このアラームルールをピアポリシー設定に追加する場合は、[Bogon (Bogons)] または [フル Bogon (Full bogons)] を選択します ([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)] > [ピアポリシー (Peer Policy)] > [ルールの追加 (Add Rule)] > [禁止されたIPプレフィックス (Prohibited IP Prefix)] )。

### 例

[禁止されたIPプレフィックス (Prohibited IP Prefix)] アラームルールでオプション [Bogons] を使用してピアポリシーを作成し、ピア RTR1 にリンクします。RTR1 が 10.0.0.0/24 ([RFC1918](#))

による BOGON) を Crosswork Cloud Network Insights にアドバタイズすると、アラームはアクティブになりますが、2001:221::/32 (フル Bogons) がアドバタイズされるとアクティブになりません。



## 第 65 章

# ゲートウェイ接続

・ゲートウェイ接続 (333 ページ)

## ゲートウェイ接続

Crosswork Data Gateway が Crosswork Cloud Traffic Analysis 用にインストールされると、Crosswork Data Gateway と Crosswork Cloud の間の接続をモニターするポリシーが自動的に作成されます。Crosswork Data Gateway が Crosswork Cloud への接続を失った場合（レポート間隔内で Crosswork Cloud との通信に失敗した場合）、アラームが生成され、Crosswork Cloud Traffic Analysis [アラーム (Alarms)] ページに表示されます (🔍) > [モニター (Monitor)] > [アラーム (Alarms)]。

ゲートウェイ接続の詳細を表示したり、アラーム重大度レベル、モニター対象ゲートウェイのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。

**ステップ 1** 🔍 > [構成 (Configure)] > [ポリシー (Policies)] の順に選択します。

[ゲートウェイ接続 (Gateway Connectivity)] で、アクティブなアラームの数、モニター対象のゲートウェイの数、および最新のアクティブなアラームを持つゲートウェイを表示できます。

**ステップ 2** [ゲートウェイ接続 (Gateway Connectivity)] で、[詳細 (Details)] をクリックします。

**ステップ 3** デフォルトでは、[概要 (Overview)] タブに現在のゲートウェイ接続ポリシーの設定が表示されます。

**ステップ 4** アラームの詳細を表示するには、[アラーム (Alarms)] タブをクリックします。このページから、[ゲートウェイ接続の喪失 (Lost Gateway Connection)] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active)]、[確認 (Acknowledge)]、または [履歴 (History)] のタブ間を移動したりできます。

**ステップ 5** アラームの重大度やモニター対象ゲートウェイのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit)] をクリックします。

- [トリガー (Triggers)] > [ゲートウェイルール (Gateway Rules)] > [重大度 (Severity)] ドロップダウンメニューで、重大度を選択します。
- [データ (Data)] で、[変更 (Modify)] をクリックして、モニターまたは無視するゲートウェイを更新します。

- c) **[アクション (Actions)]** で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて \(109 ページ\)](#) を参照してください。
  - d) **[保存 (Save)]** をクリックします。
-






## 第 66 章


# デバイスの接続性

• [デバイスの接続性](#) (335 ページ)

## デバイスの接続性

デバイスが Crosswork Data Gateway にリンクされて Crosswork Cloud Traffic Analysis に追加されると、Crosswork Data Gateway とそのデバイス間の接続をモニターするためのポリシーが自動的に作成されます。Crosswork Data Gateway がデバイスとの接続を失うと、アラームが生成され、**Crosswork Cloud Traffic Analysis** [アラーム (Alarms) ] ページに表示されます (  > [モニター (Monitor) ] > [アラーム (Alarms) ] ) 。

デバイス接続の詳細を表示したり、重大度レベル、モニター対象デバイスのリスト、または通知エンドポイントを更新したりするには、次の手順を実行します。

**ステップ 1**  > [構成 (Configure) ] > [ポリシー (Policies) ] の順に選択します。

[デバイス接続 (Device Connectivity) ] で、アクティブなアラームの数、モニター対象のデバイスの数、および最新のアクティブなアラームを持つデバイスを表示できます。

**ステップ 2** [デバイス接続 (Device Connectivity) ] で、[詳細 (Details) ] をクリックします。

**ステップ 3** デフォルトでは、[概要 (Overview) ] タブに現在のデバイス接続のポリシー設定が表示されます。

**ステップ 4** アラームの詳細を表示するには、[アラーム (Alarms) ] タブをクリックします。このページから、[デバイス接続の喪失 (Lost Device Connection) ] アラームをクリックして特定のアラームの詳細を確認したり、[アクティブ (Active) ]、[確認 (Acknowledge) ]、または[履歴 (History) ] のタブ間を移動したりできます。

**ステップ 5** アラームの重大度やモニター対象デバイスのリストを変更したり、エンドポイント通知の設定をしたりするには、[編集 (Edit) ] をクリックします。

- a) [トリガー (Triggers) ] > [デバイスルール (Device Rules) ] > [重大度 (Severity) ] ドロップダウンメニューで、重大度を選択します。
- b) [データ (Data) ] で、[変更 (Modify) ] をクリックして、モニターまたは無視するデバイスを更新します。

- c) **[アクション (Actions)]** で、既存のエンドポイント通知を変更、もしくはさらに追加できます。設定できるエンドポイント通知のタイプの詳細については、[通知エンドポイントについて \(109 ページ\)](#) を参照してください。
  - d) **[保存 (Save)]** をクリックします。
-




## 第 67 章

# インターフェイス TX の使用率

・ [インターフェイス TX の使用率 \(337 ページ\)](#)

## インターフェイス TX の使用率

このアラームは、送信トラフィック情報をモニターし、インターフェイスの TX 使用率が指定した範囲外の場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールを追加 (Add Rules)] をクリックします。
- ステップ 5 [インターフェイス TX の使用率 (Interface TX Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。






## 第 68 章

# インターフェイス RX の使用率

・ [インターフェイス RX の使用率 \(339 ページ\)](#)

## インターフェイス RX の使用率

このアラームは、受信トラフィック情報をモニターし、インターフェイスの RX 使用率が指定した範囲外になった場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1 メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2 [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3 [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4 [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5 [インターフェイス RX の使用率 (Interface RX Utilization)] をクリックします。
- ステップ 6 [Next] をクリックします。
- ステップ 7 デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8 このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9 [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10 その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。






## 第 69 章

# プレフィックス使用率

- [プレフィックス使用率 \(341 ページ\)](#)

## プレフィックス使用率

このアラームは、プレフィックスのキャパシティをモニターするもので、モニター対象インターフェイスのプレフィックスの1つが合計キャパシティのうち最大となるパーセンテージを超えた場合にトリガーされます。このアラームを設定するには、次の手順を実行します。

- ステップ 1** メインウィンドウで、 > [設定 (Configure)] > [ポリシー (Policies)] の順にクリックします。
- ステップ 2** [ポリシーを追加 (Add Policy)] をクリックします。
- ステップ 3** [名前 (Name)] フィールドでポリシー名を入力します。
- ステップ 4** [トリガー (Triggers)] で、[ルールの追加 (Add Rules)] をクリックします。
- ステップ 5** [プレフィックス使用率 (Prefix Utilization)] をクリックします。
- ステップ 6** [Next] をクリックします。
- ステップ 7** デフォルトでは、ルールが有効になっています。ルールをまだ使用しない場合は、スイッチを [無効 (DISABLED)] に切り替えます。
- ステップ 8** このアラームをトリガーする使用率の範囲を示すには、スライダを使用します。使用率が赤色と ALARM テキストで示される範囲内にある場合、Crosswork Cloud から通知が届きます。
- ステップ 9** [重大度 (Severity)] ドロップダウンリストで、このアラームに定義する重大度を選択します。
- ステップ 10** その他の必要なインターフェイスおよびエンドポイント通知の設定を行い、[保存 (Save)] をクリックします。







## 付録 **A**

# アラームについて

---



(注) 使用可能なアラームのリストを表示するには、[アラームの説明 \(23 ページ\)](#) を参照してください。

---

ここでは、次の内容について説明します。

- [アラームライフサイクル \(343 ページ\)](#)
- [アラームの状態 \(344 ページ\)](#)
- [アラーム通知 \(345 ページ\)](#)
- [アラームタイプ \(346 ページ\)](#)
- [アラームのしきい値 \(347 ページ\)](#)

## アラームライフサイクル

Crosswork Cloud Network Insights は、完全に設定されたアラームポリシーの各ルールのアラームインスタンスを作成します。完全に設定されたアラームポリシーには1つ以上のルールがあり、アラームポリシータイプに応じて、1つ以上のプレフィックス、ASN、またはそれに関連付けられたピアがあります。

各アラームインスタンスにはライフサイクルがあり、作成後にさまざまな状態の間で遷移します。次の図は、各状態から発生する遷移を示しています。詳細については、[アラームの状態 \(344 ページ\)](#) を参照してください。



(注) 各アラームインスタンスは、[設定済み (Configured)] 状態でライフサイクルを開始します。

---



| アラームステータス           | 説明                                                                                                                                                                                                                                                                                                                             |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 承認済み (Acknowledged) | この状態では、アラームが認識され、承認されたことをユーザに示します。[アクティブ (Active)] または [スヌーズ (Snoozed)] 状態のアラームは、[承認済み (Acknowledged)] としてマークできます。<br><br>(注) <ul style="list-style-type: none"> <li>• [承認済み (Acknowledged)] 状態のアラームは、アクティブなアラームのリストに表示されません。</li> <li>• 別のアクティブなアラートがある場合、[承認済み (Acknowledged)] 状態のアラームは [アクティブ (Active)] 状態に戻ります。</li> </ul> |
| クリア (Clear)         | アラームはアクティブではありません。[クリア (Clear)] 状態はエフェメラル状態です。アラームインスタンスは、30 秒の保留時間後に [設定済み (Configured)] 状態に遷移します。                                                                                                                                                                                                                            |
| スヌーズ (Snoozed)      | [アクティブ (Active)] または [承認済み (Acknowledged)] 状態のアラームは、指定された期間、ユーザが [スヌーズ (Snoozed)] 状態としてマークできます。この期間中、アラームはアクティブアラームリストに表示されます。ただし、アラーム条件がクリアされると、通知エンドポイント (設定されている場合) に通知が送信されます。                                                                                                                                             |
| 未設定 (Unconfigured)  | アラームは [未設定 (Unconfigured)] 状態に遷移し、ユーザがアラームポリシーまたはアラームインスタンスに対応するルールを削除すると、最終的に削除されます。[未設定 (Unconfigured)] 状態はエフェメラル状態であり、アラームインスタンスは 30 秒の保留時間後に削除されます。                                                                                                                                                                        |



- (注)
  - アラームインスタンスは、アラーム検出レイヤから受信したイベントに応じてのみ、[アクティブ (Active)] または [クリア (Clear)] 状態に遷移できます。

## アラーム通知

ポリシールールに違反すると、アラーム通知が1つ以上のエンドポイントに送信されるように設定できます ([通知エンドポイントの設定 \(110ページ\)](#) を参照)。通知には、アラーム状態とアラームイベントデータに関する情報が含まれます。

次のいずれかのアラーム状態が変化すると、通知が送信されます。

- アクティブからクリアへ
- 設定済みからアクティブへ

- 承認済みからクリアへ
- スヌーズからクリアへ

アラームが再びアクティブになり、すでに次のいずれかの状態になっている場合、通知は生成されません。

- Active
- スヌーズ (Snoozed)
- 承認済み (Acknowledged)

#### 関連リンク

- [通知エンドポイントについて \(109 ページ\)](#)

## アラームタイプ

アラームは、次の3つのタイプに分類されます。

| タイプ              | 説明                                                                                                                                                                                                                                       |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASN              | 自律システム番号 (ASN) タイプのアラームは、設定された BGP 自律システム (AS) の状態をモニタします。これらのアラームは通常、ASNからの予期しないプレフィックスを検出し、予期される条件に違反した場合に警告するために使用されます。たとえば、アラームがアクティブになるのは、以前に確認されておらず、設定済みの ASN から発信されてはならない新しいプレフィックスを Crosswork Cloud Network Insights が検出した場合です。 |
| ピア (PEER)        | ピアタイプのアラームは、設定されたピアとそのルーティング情報ベース (RIB) の状態をモニタします。これらのアラームは、ピアモニタリングを設定した場合に使用されます。たとえば、アラームがアクティブになるのは、設定されたパラメータの範囲外の RIB で多数のプレフィックスを Crosswork Cloud Network Insights が検出した場合です。                                                    |
| プレフィックス (PREFIX) | プレフィックスタイプのアラームは、プレフィックスの送信元 ASN や AS パス属性の長さなど、設定されたプレフィックスの状態とその BGP 属性の数をモニタします。これは最も一般的なアラームタイプであり、監視されているプレフィックスの不明なイベントを検出するように設計されています。プレフィックスタイプのアラームのセットは、設定されたプレフィックスの ROA ステータス (VALID、INVALID、または ABOUT-TO-EXPIRE) もモニタします。  |

## アラームのしきい値

アラームのしきい値は、アラームの感度を制御するために使用されます。一部のアラームが少数の観測された変更によってトリガーされることが多く、「誤アラーム」と見なされる場合は、アラームのしきい値を構成することを検討してください。

モニタ対象の AS、ピア、またはプレフィックスに関連する一連の条件に対する違反を Crosswork Cloud Network Insights が検出すると、アラームがトリガーされます (アクティブ)。すべての条件に違反しなくなると、アラームはクリアされます。データは多くの BGP ピアから収集されるため、Crosswork Cloud Network Insights はプレフィックスまたは AS の状態の複数のビューにアクセスできます。これらのビューは常に同じであるとは限りません。また、少数のピア (ルータのフラップによって発生するピアなど) で頻繁に状態が変化すると、大量のアラームノイズが発生する可能性があります。しきい値は、ノイズ減衰メカニズムとして機能できます。

アラームノイズを減衰させるために、特定のアラームルールに対して次のピアカウントしきい値を設定できます。

[トリガーするピア (Peers to Trigger)]: アラームがアクティブになる条件違反を報告するために必要な違反ピアの最小数。例: [トリガーするピア (Peers to Trigger)] しきい値が [プレフィックスの取り消し (Prefix Withdrawal)] アラームに対して 1 に設定されています。外部ルーティング分析がアクティブなプレフィックスの取り消しアラームを発行する前に、プレフィックスが取り消されたことを報告するピアの数が 1 を超える必要があります。

[解決するピア (Peers to Resolve)]: アラームがアクティブ化された後も、アクティブのままになります。アラームは、違反ピア数が [解決するピア (Peers to Resolve)] のしきい値以下になるまで、すべての新しい条件違反で再度トリガーされます (たとえば、これは違反アドバタイズメントの取り消しまたは [解決するピア (Peers to Resolve)] のしきい値の増加によって発生する可能性があります)。その後でアラームは [クリア (Clear)] 状態になります。



(注) [解決するピア (Peers to Resolve) ]のしきい値は、[トリガーするピア (Peers to Trigger) ]のしきい値よりも小さくする必要があります。

図 7: 例 : 想定されるASパス (Expected AS Path) ]アラームルールのしきい値オプション

Name: PolicyABC Policy Type: Prefix

Policy Notification Endpoints 0 Add Endpoint

Expected AS Path Editor

Origin ASNs Upstream ASNs

Enter a comma (,) as you type an ASN to commit it

Edit Valid AS Path Pattern --

Rules 1 Add Rule

Prefix Withdrawal  
DISABLED  ENABLED

Peers to Resolve 0 Peers to Trigger 1 Severity High

Rule Specific Notification Endpoints 0 Add Endpoint

Notes







## 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。