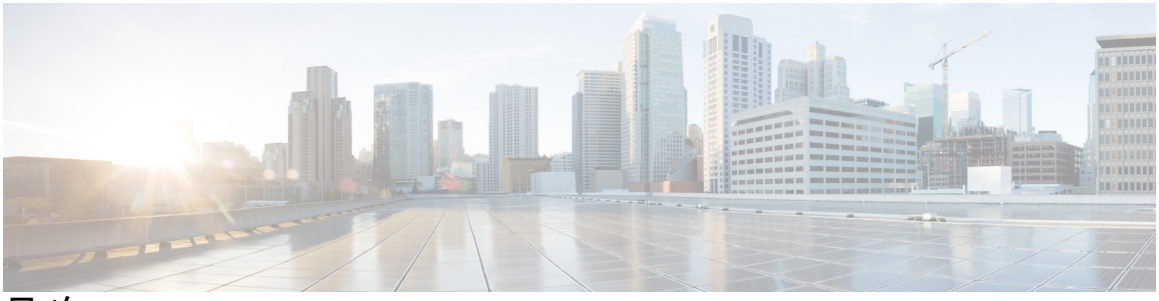
Cisco Crosswork Cloud クイックスタートガイド

初版：2023 年 5 月 3 日

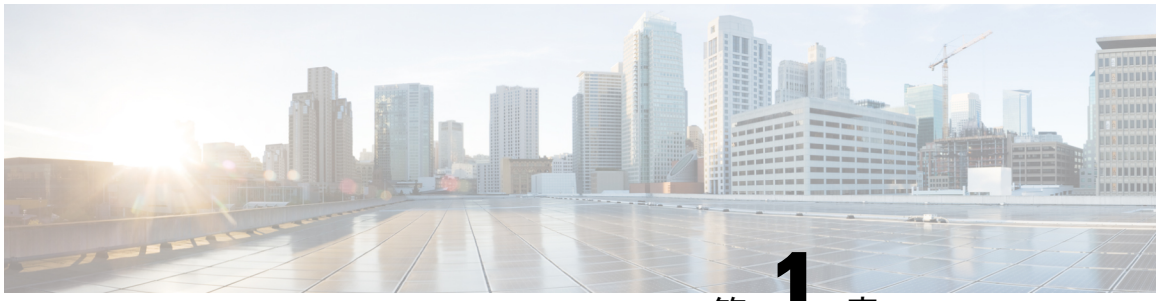
最終更新：2023 年 8 月 1 日

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/



目 次

?



第 1 章

概要

このマニュアルでは、Cisco Crosswork Cloud を設定して使用を開始するために必要な手順の概要について説明します。

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。

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。
- ピアリング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。

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。

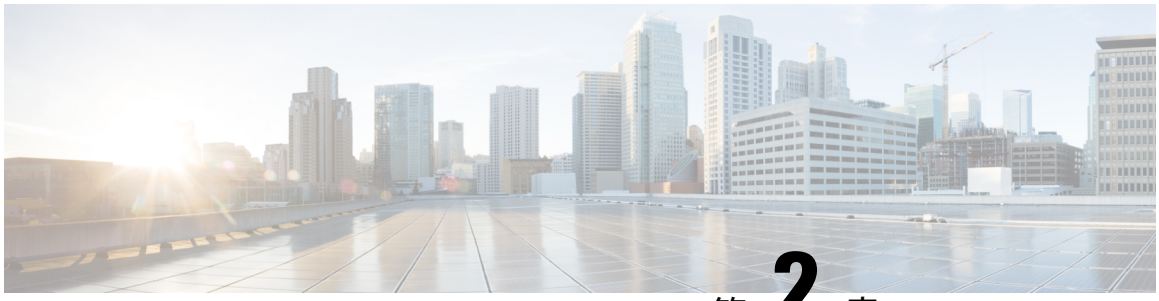
Crosswork Cloud Trust Insights は、ネットワークの現在の状況と過去の状況を把握するのに役立ちます。また、次のことがわかります。

- 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。

Cisco Crosswork Data Gateway について

Crosswork Data Gateway は、デバイスからのデータの安全な収集を促進するために、カスタマーネットワーク内で簡単に展開および維持できるゲートウェイとして設計されており、外部クラウドリソースへの直接接続は不要です。Crosswork Data Gateway は、VMware ESXi などの一般的な仮想化環境での導入を合理化するように設計されており、導入後は Crosswork Cloud サービスによって完全に管理されます。また、Crosswork Cloud アプリケーションの展開と管理の運用およびメンテナンス要件を最小限に抑えるように設計されています。Crosswork Cloud では複数の Cloud Data Gateway を管理できるため、Crosswork Cloud Traffic Analysis および Crosswork Cloud Trust Insights では、ピアリングトラフィックデータのスケーラブルな展開を容易にサポートでき、収集を簡単に地理的に分離し、管理コストを最小限に抑えながら、大規模な実稼働ネットワークからの証拠収集を信頼できます。



第 2 章

Crosswork Cloud のセットアップ

このセクションでは、Crosswork Cloud を初めて使用する場合の最初の手順について説明します。

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。

ユーザの追加

管理者権限がある場合は、Cisco.com アカウントを持つユーザーを追加できます。

ステップ 1 メインウィンドウで、 > **[ユーザー（Users）]** > **[ユーザーの追加（Add User）]**をクリックします。

ステップ 2 選択を [有効（Enabled）]（デフォルト）に切り替えます。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 3 1 つ以上のユーザーの電子メールアドレス（Cisco.com ユーザープロファイルで指定）を、スペース、カンマ、またはセミコロンで区切って入力します。

ステップ 4 [ロール（Role）] ドロップダウンメニューからユーザーのアクセスを選択します。詳細については、「ユーザーロール」を参照してください。

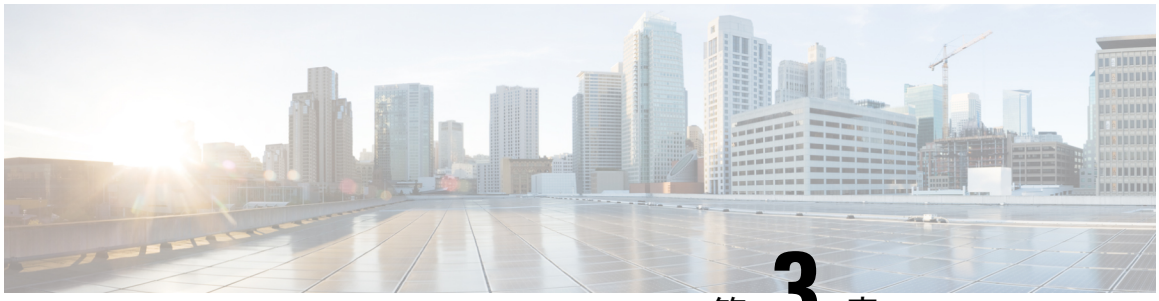
ステップ 5 [保存（Save）] をクリックします。

組織テナントのセットアップ

ステップ 1 管理者として最初にログインすると、組織名の入力を求めるページが表示されます。組織名を入力し、[次へ（Next）] をクリックします。

ステップ 2 個人プロファイルのプリファレンスを設定し、[送信（Submit）] をクリックします。

（注） ある時点でサブスクリプションを別の組織に移動する場合は、「サブスクリプションを別の組織に転送」の記載に従い、サブスクリプション ID を削除する必要があります。



第 3 章

Crosswork Cloud Network Insights の使用開始

このワークフローでは、すぐに Crosswork Cloud Network Insights の使用を開始するためのタスクの概要を示します。

概要 Crosswork Cloud Network Insights

Crosswork Cloud Network Insights では、ハードウェアのセットアップは不要です。Crosswork Cloud Network Insights の使用をすぐに開始するには、次の情報のみ必要です。

- モニターする ASN とプレフィックスのリスト
- アラートを受け取る BGP 更新のタイプ

（注） BGPmon からピアを移行する場合は、「ピアのインポート」を参照してください。

表 *1 : Crosswork Cloud Network Insights* の使用開始ワークフローの概要

手順	操作	手順と注記
1	モニターする ASN とプレフィックスを収集します。	—

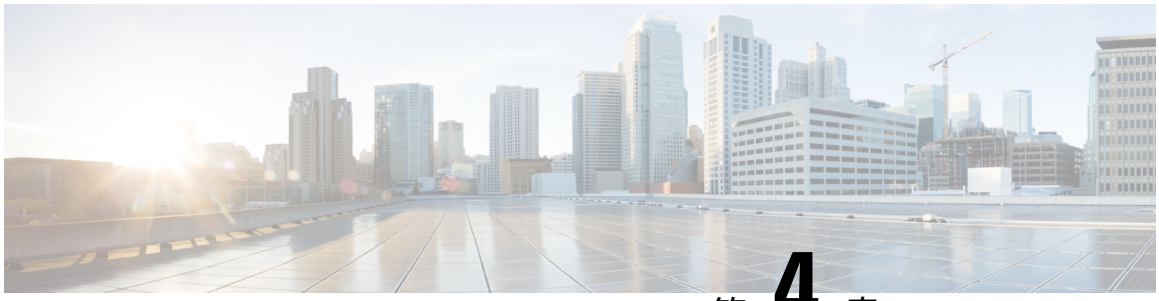
手順	操作	手順と注記
2	**Express Setup** を使用して、モニターする ASN とプレフィックスをすばやく追加します。デフォルトでは、Crosswork Cloud は、アラートを受け取る BGP 更新のアラームをトリガーできる最も一般的なルールを使用してポリシーを作成します。 次のポリシーとルールが作成されます。 • ASN ポリシー • [予期しないASプレフィックス（Unexpected AS Prefix）] • プレフィックスポリシー • [AS発信元違反（AS Origin Violation）] • [サブプレフィックスアドバタイズメント（SubPrefix Advertisement）] • [プレフィックスの取り消し（Prefix Withdrawal）] • [ROA障害（ROA Failure）] • [ROAの有効期限（ROA Expiry）]	• 外部ルーティングの Express Setup の使用  > [Express Setup]

手順	操作	手順と注記
3	ポリシーを微調整します。BGP アドバタイズメントの外観を定義し、外観が異なる場合は通知するポリシーを作成します。 • さらにポリシーを作成する必要がありますか。「ポリシーのタイプ」は何にしますか。 • 追加する必要があるルールのタイプは何ですか。 • アラームが多すぎますか。しきい値を変更する必要がありますか。	

手順	操作	手順と注記
		• [アラーム（Alarms）]：作成したポリシーによってトリガーされたアクティブなアラームを表示します。https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-network-automation/b_cisco-crosswork-cloud-user-guide/m_monitor-alarms-external-routing-analytics.html#id_92402  >[モニター（Monitor）]>[アラーム（Alarms）] • [ポリシー（Policies）]：関心のあるBGP更新のアラームのみを生成するポリシーを作成および変更します。https://www.cisco.com/content/en/us/td/docs/cloud-systems-management/crosswork-network-automation/b_cisco-crosswork-cloud-user-guide/m_configure-policies-external-routing-analytics.html  **>[設定（Configure）]>[ポリシー（Policies）]** • [通知エンドポイント（Notification Endpoints）]：アラーム通知を受信する方法または場所を定義します。https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-network-automation/b_cisco-crosswork-cloud-user-guide/m_configure-notification-endpoints-external-routing-analytics.html#Cisco_Concept.dita_5c0dc7eb-c953-4f83-8d9a-7056d73ec3c1 これらは、ポリシーの設定時に定義することも、次の場所に移動して定義することもできます。  **>[グローバル（Global）]>[通知（Notifications）]** • [ASNルーティングレポート（ASN Routing Reports）]：自律システムのルートアナウンスおよびピアリング関係の変更を強調表示する日次レポートを作成および受信します（またはオンデマンドで生成します）。

手順	操作	手順と注記
		https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/crosswork-network-automation/b_cisco-crosswork-cloud-user-guide/m_configure-reports.html  > **[設定（Configure）]** > **[レポート（Reports）]**

手順	操作	手順と注記
4	BGP ルーティングを表示および分析します。 • ASN BGP アドバタイズメントを受信しているのは誰ですか。 • AS パスはどのように表示されますか。目的の宛先に到達していますか。 • トラブルシュートを行い、アラームの原因となった可能性のあるイベントを特定するのに役立ちます。 • API を使用して、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。詳細については、API マニュアル（>[マニュアル（Documentation）] > [API（APIs）]）を参照してください。	• プレフィックス検索グラス：現在のピア、AS パス、およびコミュニティを表示します。 **> [モニター（Monitor）] > [プレフィックス（Prefixes）] > *[プレフィックス IP アドレス（prefix-ip-address）]* > [検索グラス（Looking Glass）]** タブ • ASN 検索グラス：現在のプレフィックスとレポートピアを表示します。 **> [モニター（Monitor）] > [ASN（ASNs）] > *[ASN 名（asn-name）]* > [検索グラス（Looking Glass）]** タブ • プレフィックスパストポロジ：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 を可視化できます。パストポロジツールでは、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をトラブルシュートする上で役立つ情報も得られます。 **> [ツール（Tools）] > [パストポロジ（Path Topology）]** • アラーム：ポリシーのいずれかの条件が満たされるとアクティブなアラームを確認できます。 >[モニター（Monitor）]>[アラーム（Alarms）] • BGP 更新：該当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。 **> [モニター（Monitor）] > [BGP 更新（BGP Updates）]**



第 4 章

Crosswork Cloud Traffic Analysis の使用開始

このワークフローでは、すぐに Crosswork Cloud Traffic Analysis の使用を開始するためのタスクの概要を示します。

Crosswork Cloud Traffic Analysis ではデータ収集に Crosswork Data Gateway が使用されるため、ワークフローには、Crosswork Data Gateway のインストールおよびセットアップ方法に関する概要情報も含まれています。

- 概要 Crosswork Cloud Traffic Analysis （13 ページ）

概要 Crosswork Cloud Traffic Analysis

表 *2 : Crosswork Cloud Traffic Analysis* のセットアップおよび使用開始ワークフローの概要

手順	操作	Crosswork Cloud のナビゲーションと注記
Crosswork Data Gateway 次の手順は、Crosswork Cloud の外部で実行されます。		
1	Crosswork Data Gateway の要件を確認します。	インストール要件
2	Crosswork Data Gateway のインストール中に必要な情報を収集します。次の点を確認してください。 • Crosswork Data Gateway が Crosswork Cloud（管理インターフェイス）に接続できるネットワーク • Crosswork Data Gateway がデバイスに接続できるネットワーク（オプションのサウスバウンドインターフェイス） • 各インターフェイスの IP アドレス情報 • プロキシ（インターネットへの接続が必要な場合）	展開パラメータとシナリオ

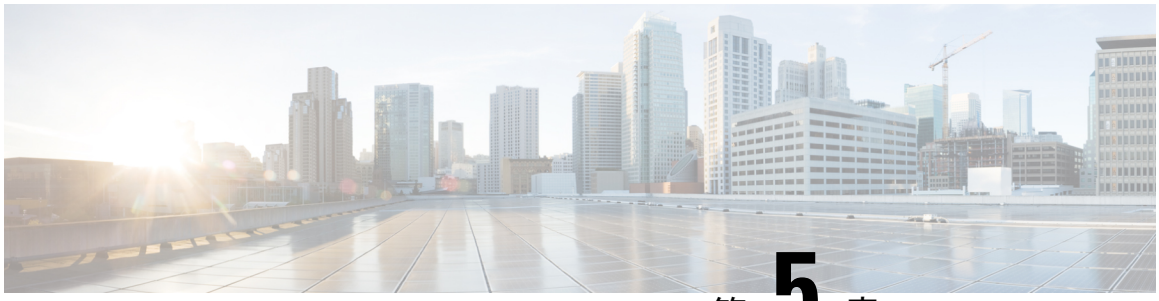
手順	操作	Crosswork Cloud のナビゲーションと注記
3	Crosswork Data Gateway をインストールします。	• サポートされているすべてのプラットフォームの詳細な手順については、Crosswork Data Gateway のインストールを参照してください。 • クイックリファレンスとして、vCenter vSphere クライアントを使用した Crosswork Data Gateway のインストール （29 ページ）も参照できます。この例では、サポートされている Crosswork Data Gateway の最新のイメージを取得して、インストールが成功したことを確認します。
4	Crosswork Data Gateway から、登録パッケージ（.json ファイル）を取得し、後でアクセスできる場所にダウンロードします。.json 登録ファイルには、Crosswork Data Gateway を Crosswork Cloud に登録するために使用される一意のデジタル証明書が含まれています。	登録パッケージの取得とエクスポート
Crosswork Cloud Traffic Analysis 次の手順は、Crosswork Cloud Traffic Analysis 内で実行されます。 （注） 環境が設定されていることを確認するために、Crosswork Cloud トラフィック分析セットアップチェックリスト（ > [セットアップチェックリスト（Setup Checklist）]）を使用することもできます。		
5	登録パッケージをアップロードして Crosswork Data Gateway を Crosswork Cloud Traffic Analysis に登録します。 （注） 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。これは、この Crosswork Data Gateway インスタンスを Crosswork Cloud Trust Insights に使用できないことを意味します。	Crosswork Data Gateway 情報の追加 **> [設定（Configure）] > [データゲートウェイ（Data Gateways）] > [データゲートウェイの追加（Add Data Gateway）] > [登録ファイル（Registration File）]**

手順	操作	Crosswork Cloud のナビゲーションと注記
5	Crosswork Cloud Traffic Analysis 用のデバイスで BGP、SNMP、およびネットワーク フロー モニタリング プロトコルを設定します。	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
6	デバイスを追加するときに使用する BGP、SSH（任意）、および SNMP のデバイスログイン情報を追加します。	クレデンシャルの作成 > [設定（Configure）] > [ログイン情報（Credentials）] > [ログイン情報の追加（Add Credential）]
7	デバイスを追加します。 （注） デバイスがすでに Crosswork Cloud に追加されている場合は、デバイスを Crosswork Cloud Trust Insights にリンクするだけです。 > [データゲートウェイ（Data Gateways）] > ***[データゲートウェイ名（data-gateway-name）]*** > [リンク済みトラフィックデバイス（Linked Traffic Devices）]	• デバイスの追加 > [設定（Configure）] > [デバイス（Devices）] > [デバイスの追加（Add Device）] • すべての接続が稼働していることを確認します。 > [設定（Configure）] > [デバイス（Devices）] > [デバイス名（device_name）] > [ステータス（Status）] タブ
8	外部インターフェイスを指定します。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。	外部インターフェイスの指定 > [設定（Configure）] > [デバイス（Devices）] > [デバイス名（device_name）] > [トラフィック分析（Traffic Analysis）] タブ > [インターフェイス（Interfaces）]
9	正常なトラフィックの外観を定義し、外観が異なる場合は通知するポリシーを表示し、作成します。	ポリシー > [設定（Configure）] > [ポリシー（Policies）]
次のステップ セットアップが完了し、Crosswork Cloud Traffic Analysis の使用を開始できます。		

手順	操作	Crosswork Cloud のナビゲーションと注記
10	トラフィックのモニタリングを開始し、輻輳ポイントと機会を簡単に特定して、BGP トラフィックのロードバランシングと最適化を改善します。 • 輻輳が発生していますか。輻輳に役立つ変更は何ですか。 • アドバタイズメントを分割して、トラフィックフローをピア間で移動できますか。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。 • 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。 • どこで、誰とピアリングする必要がありますか。	

手順	操作	Crosswork Cloud のナビゲーションと注記
		トラフィック情報の表示： • デバイス分析の詳細の表示 • インターフェイストラフィックの詳細の表示 • ASN トラフィックの詳細の表示 • プレフィックストラフィックの詳細の表示 使用できるツール： • インターフェイス使用率の最適化：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。 • 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。 • トラフィックのドリルダウン：このツールを使用すると、インターフェイスの容量と、容量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。 • ピア探査：この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

手順	操作	Crosswork Cloud のナビゲーションと注記
		他のピアをすばやく確認するのに役立ちます。



第 5 章

Crosswork Cloud Trust Insights の使用開始

このワークフローでは、すぐに Crosswork Cloud Trust Insights の使用を開始するためのタスクの概要を示します。

Crosswork Cloud Trust Insights ではデータ収集に Crosswork Data Gateway が使用されるため、ワークフローには、Crosswork Data Gateway のインストールおよびセットアップ方法に関する概要情報も含まれています。

- 概要 Crosswork Cloud Trust Insights （19 ページ）

概要 Crosswork Cloud Trust Insights

表 *3 : Crosswork Cloud Trust Insights* のセットアップおよび使用開始ワークフローの概要

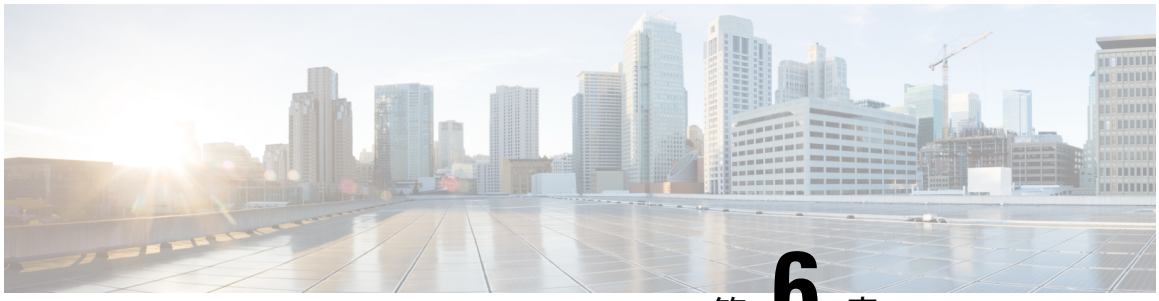
手順	操作	手順と注記
Crosswork Data Gateway		
1	Crosswork Data Gateway の要件を確認します。	インストール要件
2	Crosswork Data Gateway のインストール中に必要な情報を収集します。次の点を確認してください。 • Crosswork Data Gateway が Crosswork Cloud（管理インターフェイス）に接続できるネットワーク • Crosswork Data Gateway がデバイスに接続できるネットワーク（オプションのサウスバウンドインターフェイス） • 各インターフェイスの IP アドレス情報 • プロキシ（インターネットへの接続が必要な場合）	展開パラメータとシナリオ

手順	操作	手順と注記
3	Crosswork Data Gateway をインストールします。	• サポートされているすべてのプラットフォームの詳細な手順については、Crosswork Data Gateway のインストールを参照してください。 • クイックリファレンスとして、vCenter vSphere クライアントを使用した Crosswork Data Gateway のインストール （29 ページ）も参照できます。この例では、サポートされている Crosswork Data Gateway の最新のイメージを取得して、インストールが成功したことを確認します。
4	Crosswork Data Gateway から、登録パッケージ（.json ファイル）を取得し、後でアクセスできる場所にダウンロードします。.json 登録ファイルには、Crosswork Data Gateway を Crosswork Cloud に登録するために使用される一意のデジタル証明書が含まれています。	登録パッケージの取得とエクスポート
Crosswork Cloud Trust Insights		
5	登録パッケージをアップロードして Crosswork Data Gateway を Crosswork Cloud Trust Insights に登録します。 （注） 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。これは、この Crosswork Data Gateway インスタンスを Crosswork Cloud Traffic Analysis に使用できないことを意味します。	Crosswork Data Gateway 情報の追加 **> [設定（Configure）] > [データゲートウェイ（Data Gateways）] > [データゲートウェイの追加（Add Data Gateway）] > [登録ファイル（Registration File）]**
6	Cisco IOS XR でサポートされているイメージ、登録キー、証明書、および Crosswork Cloud Trust Insights の要件がすべて揃っていることを確認します。	• Cisco IOS XR でサポートされるイメージ • ルータ構成の確認

手順	操作	手順と注記
7	Cisco IOS XR ルータに対する不正な操作や設定の変更を防ぐために、Crosswork Trust Insights のデバイスへのアクセスが制限されているユーザーを設定します。	制限付き権限のユーザーの設定
8	ドシエ収集を開始して最新のデバイス情報を取得します。	Trust Insights のデバイスドシエのデータ収集 > [設定（Configure）] > [デバイス（Devices）] > [デバイス名（device-name）] > [Trust Insights] > [ドシエの収集（Collect Dossier）]
9	デバイスを追加します。 （注） デバイスがすでに Crosswork Cloud に追加されている場合は、Crosswork Cloud Trust Insights（ > **[データゲートウェイ（Data Gateways）] > *[データゲートウェイ名（data-gateway-name）]*** > [リンク済み信頼デバイス（Linked Trust Devices）] タブにリンクするだけです。	• デバイスの追加 **[デバイス（Devices）] > [デバイスの追加（Add Device）]** • すべての接続が稼働していることを確認します。 [デバイス（Devices）] > [デバイス名（device_name）] > [ステータス（Status）] タブ （注） 次の情報を入力する必要があります。 • 名前 • ホスト名（Hostname） • デバイスのタイムゾーン • データ ゲートウェイ • ログイン情報グループ（前の手順で定義）

手順	操作	手順と注記
10	デバイスを追加するときに使用するデバイスログイン情報プロファイルを追加します。	クレデンシャルの作成 > [設定（Configure）] > [ログイン情報（Credentials）] > [ログイン情報の追加（Add Credential）]
11	デバイスを追加すると、収集プロセスが開始されます。データが収集されるまでしばらく待ってから、デバイスのデータ収集が成功したことを確認します。	> [モニター（Monitor）] > [デバイス（Devices）] > ***[デバイス名（device-name）]*** **[Trust Insights]** タブ
次のステップ		
10	ソフトウェアを確認し、ランタイム署名分析を表示します。 • ソフトウェアインベントリに、デバイスの正しい IOS XR インベントリが反映されていますか。 • ソフトウェアパッケージに検証済みのソフトウェア署名が表示されますか（IMA「Observed Running」） • ソフトウェアパッチ（SMU）は、実稼働システム全体に正常に展開されていますか。 • ソフトウェアはコンプライアンスに準拠していますか。	> [モニター（Monitor）] > [デバイス（Devices）] > ***[デバイス名（device-name）]*** **[Trust Insights]** タブ
12	ハードウェアインベントリを確認します。	デバイス インベントリの表示 > [モニター（Monitor）] > [デバイス（Devices）] > ***[デバイス名（device-name）]*** **[Trust Insights]** タブ。[Inventory] タブをクリックします。
11	システムで確認された変更履歴を表示します。 • スケジュールされたメンテナンスが完了したことを確認します。 • 既知のネットワークの問題をさらに調査します。 • デバイスの再起動または設定変更を表示します。 • ソフトウェアはコンプライアンスに準拠していますか。	デバイスの変更の表示 > [モニター（Monitor）] > [デバイス（Devices）] > ***[デバイス名（device-name）]*** **[Trust Insights]** タブ。[変更（Changes）] タブをクリックします。

手順	操作	手順と注記
12	単一のデバイスが基準として使用されるように選択されているデバイス構成を比較します。実稼働環境内に展開された同様のデバイスにインストールされているソフトウェアパッケージ間の違いを特定します。 逸脱したデバイスをコンプライアンスに適合させるために、推奨される変更の「パンチリスト」を生成します。	デバイスの比較  > [ツール（Tools）] > [デバイスの比較（Device Comparison）]



第 6 章

Crosswork Cloud のトラブルシュート

Crosswork Data Gateway 接続のトラブルシュート

次の手順は、Crosswork Data Gateway と Crosswork Cloud の接続の問題をトラブルシュートするのに役立ちます。

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）] をクリックしてから、接続を確認する Crosswork Data Gateway をクリックします。

ステップ 2 [接続（Connectivity）] フィールドに [セッションアップ（Session Up）] と表示されていることを確認します。

これは、Crosswork Data Gateway がクラウドに接続されていることを示します。

ステップ 3 Crosswork Data Gateway にリンクされているデバイスが少なくとも 1 つあることを確認します。

ステップ 4 メインウィンドウで、[デバイス（Devices）] をクリックし、Crosswork Data Gateway にリンクされているデバイスをクリックします。

ステップ 5 [ステータス（Status）] タブをクリックします。

ステップ 6 Crosswork Cloud と Crosswork Data Gateway の間の接続リンクが、接続が機能していることを示す緑色になっていることを確認します。

接続リンクが、エラーがあることを示す赤色の場合、Crosswork Data Gateway はクラウドに接続されていません。

ステップ 7 SSH を使用して、ユーザー名 **dg-admin** と Crosswork Data Gateway のインストール時に指定したパスワードで Crosswork Data Gateway にログインします。

ステップ 8 Crosswork Data Gateway メインメニューに移動し、[バイタル（Vitals）]>[コントローラ到達可能性（Controller Reachability）] を選択し、確立されたセッションがあることを確認します。これにより、Crosswork Data Gateway がデフォルトゲートウェイと DNS サーバーに到達できることが確認されます。

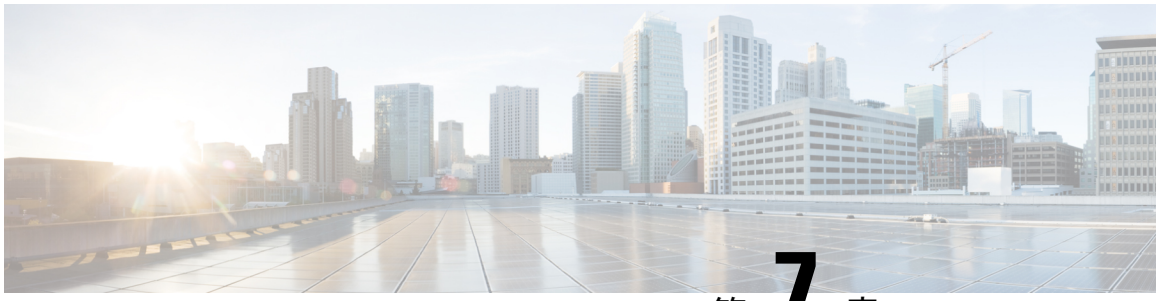
コントローラの到達可能性テストが失敗した場合、次のいずれかの問題が原因である可能性が高いです。

- Crosswork Data Gateway からインターネットにアクセスできるようにルーティングが正しく設定されていない。
- Crosswork Cloud と Crosswork Data Gateway の間のファイアウォールが通信を妨げている可能性がある。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。
- Web プロキシが通信を妨げている可能性がある。Web プロキシがある場合は、Crosswork Data Gateway のインストール時に必要な情報を設定しておく必要があります。Crosswork Cloud と Crosswork Data Gateway の間の通信を許可するように、Crosswork Data Gateway を再インストールして Web プロキシを設定します。

ステップ 9 Crosswork Data Gateway メインメニューから [Dockerコンテナ（Docker Containers）] を選択し、次のいずれかのイメージが表示されていることを確認します。

- Crosswork Cloud Trust Insights の cti-image
- Crosswork Cloud Traffic Analysis の cfi-image

これにより、Crosswork Data Gateway は Crosswork Cloud から必要なイメージをダウンロードできます。



第 7 章

サブスクリプションプラン

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

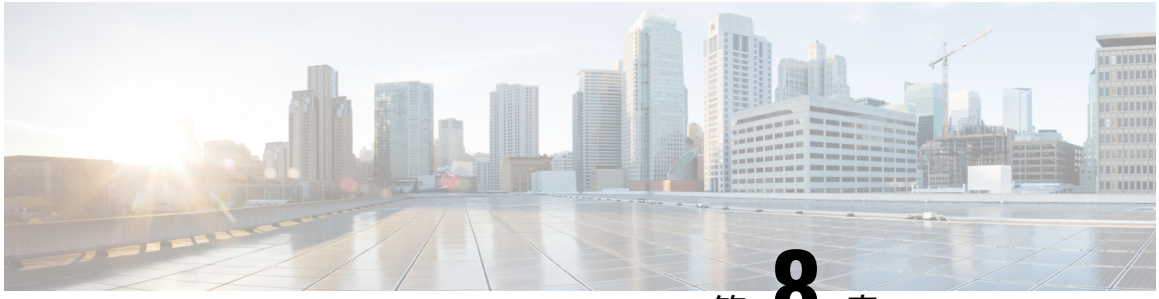
無料のサブスクリプションプランの要件

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 8 章

補足情報

vCenter vSphere クライアントを使用した Crosswork Data Gateway のインストール

Crosswork Data Gateway は通常、ネットワーク管理サービスの提供に使用されるのと同じ仮想化インフラストラクチャ内に展開されます。詳細な要件については、Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applicationsガイドのインストール要件セクションを参照してください。

展開前に、次の情報または要件が満たされていることを確認します。

	要件
☐	HTTPS/TLS Crosswork Data Gateway は、HTTPS/TLS を使用して外部クラウドサービスに接続できる必要があります。
☐	プロキシ（インターネットへのアクセスに必要な場合）
☐	ルータへの直接 SSH アクセス Crosswork Data Gateway は、SSH プロトコルを使用してデータドシエ収集のためにルータに接続します。管理ネットワークとルータ間のアクセスを制限するように設計されているファイアウォールポリシーでは、Crosswork Data Gateway からルータへの SSH アクセスを許可するように調整する必要があります。SSH 収集は通常、ルータの IPv4 または IPv6 管理イーサネットアドレスを対象としていますが、インバウンド SSH アクセスを許可するルータ上の任意の IP アドレスも使用できます。
☐	管理インターフェイスの IP アドレス

	要件
☐	（任意）サウスバウンド インターフェイスの IP アドレス
☐	OVF テンプレート情報（ステップ 3 を参照）

さまざまなプラットフォーム（VMware、OpenStack、Amazon EC2 など）に Crosswork Data Gateway をインストールできます。次の手順は、vCenter vSphere Client を使用して Crosswork Data Gateway VM を展開するためのクイックリファレンスとして使用することを目的としています。考えられるエントリの例が示されており、ユーザーが VMware vCenter OVA のインストールに精通していることを前提としています。他のプラットフォームに関する詳細なガイダンスまたは情報が必要な場合は、次のマニュアルを参照してください。

- Cisco Crosswork Data Gateway Release Notes
- Cisco Crosswork Data Gateway Installation and Configuration Guide for Cloud Applications

ステップ 1 Crosswork Data Gateway イメージ（*.ova）ファイルをダウンロードして、ファイルの保存場所をメモします。ファイルの拡張子が .dms の場合は、.ova に変更します。

ステップ 2 vCenter vSphere Client にログインし、[アクション（Actions）] > [OVFテンプレートの展開（Deploy OVF Template）] を選択します。

ステップ 3 [OVFテンプレートの展開（Deploy OVF Template）] ウィザードのプロンプトに従います。

表 *4: OVF* テンプレートの展開

ステップ	説明	例
OVF テンプレートの選択	Cisco Software Download サイトからダウンロードした OVA イメージファイルを選択します。	[ローカルファイル（Local File）] > [ファイルの選択（Choose File）] > [ダウンロード（Downloads）] > [cw-na-dg-4.5.0-19-release-20230119.uefi.ova]
名前とフォルダの選択	デフォルトを受け入れるか、この Crosswork Data Gateway VM の任意の名前（デフォルトは OVA ファイル名から取得）を入力し、VM を配置するデータセンターを選択します。	• Crosswork Data Gateway VM 名：***Crosswork Data Gateway 4.5*** • データセンター：***ABCcompany_lab***
コンピューティングリソースの選択	データセンター内で、VM を展開するホスト（物理サーバー）を選択します。	***ABCcompany_hostserver1.com***
詳細の確認	VMware vCenter Server によって OVA が検証され（ネットワーク速度によっては 1 分かかる場合があります）、確認用の詳細を含むこの画面が表示されます。	—

ステップ	説明	例
ライセンス契約	ライセンス契約を確認します。	—
コンフィギュレーション	展開構成として [Crosswork Cloud] を選択します。 （注） これは、必ずしもデフォルトで選択されているとは限らないため、[Crosswork Cloud] が選択されていることを確認します。別のオプションを選択した場合は、展開を最初から開始する必要があります。	**Crosswork Cloud**
ストレージの選択（Select Storage）	仮想ディスクとフォーマットを選択します。 デフォルトでは、最初の仮想ディスクが選択されます。空きディスク容量が最も多いディスクを選択するのが理想的です。 [互換性（Compatibility）] の下にエラーがないことを確認します。	• 実稼働環境の場合、[シックプロビジョニングLazy Zeroed（Thick Provision Lazy Zeroed）] を選択します。 • 開発環境の場合、[シンプロビジョニング（Thin Provision）] を選択します。
ネットワークの選択（Select networks）	トラフィックの送信に使用する予定の vNIC の数に基づいて、送信元ネットワークごとに適切な宛先ネットワークを選択します。I vNIC0から順に、使用する宛先ネットワークを選択してください。未使用の vNIC は、デフォルト値のままにしてください。 • 1 つの vNIC：すべてのトラフィックが vNIC0 で送信されます。 • 2 つの vNIC：管理トラフィックは vNIC0 で、データトラフィックは vNIC1 で送信されます。 • 3 つの vNIC：管理トラフィックは vNIC0 で、ノースバウンドデータ トラフィックは vNIC1 で、サウスバウンドデータ トラフィックは vNIC2 で送信されます。	次の例では、すべてのトラフィックが vNIC0 で送信されます。次の「**テンプレートのカスタマイズ**」ステップで 1 つのアクティブな vNIC のみを選択した場合、vNIC1 と vNIC2 のエントリは無視されます。

ステップ	説明	例
テンプレートのカスタマイズ	IP アドレス、vNIC ロールの割り当てなどを設定します。	

ステップ	説明	例
		すくなくとも、以下のオプションを設定する必要があります。 • [ホスト情報（Host Information）] > [ホスト名（Hostname）] : ***Cisco-CDG*** • [ホスト情報（Host Information）] > [説明（Description）] : ***TrustInsights-CDG*** • [ホスト情報（Host Information）] > [アクティブなvNIC（Active vNICs）] • すべてのパスフレーズ （注） これらのロールとパスワードは、Crosswork Data Gateway にログインするために使用されます。 • vNIC0 IPv4 または IPv6 アドレス情報 : ***172.23.291.12*** （最後のステップで）複数の vNIC をアクティブにすることを選択した場合は、他の vNIC（vNIC1 および vNIC2）の詳細を入力します。それ以外の場合は、他の vNIC セクションをスキップします。 • [DNSサーバー（DNS Servers）] > [DNSアドレス（DNS Address）] : ***171.70.168.183*** • [DNSサーバー（DNS Servers）] > [DNS検索ドメイン（DNS Search Domain）] : ***cisco.com*** • [NTPv4サーバー（NTPv4 Servers）] > [NTPv4サーバー（NTPv4Servers）] : ***ntp.esl.cisco.com*** • [コントローラの設定（Controller Setting）] > [Crossworkコントローラ IP（Crosswork Controller IP）] （注） **crosswork.cisco.com** と入力します。 • [コントローラの設定（Controller Setting）] > [Crossworkコントローラポート（Crosswork Controller Port）]

ステップ	説明	例
		（注） **443** と入力します。 • プロキシまたはファイアウォールを使用する場合は、[プロキシサーバーのURL（Proxy Server URL）]。 詳細については、展開パラメータとシナリオを参照してください。
終了準備の完了	設定のサマリーを確認する。	—

ステップ 4 vCenter vSphere クライアントの [最近のタスク（Recent Tasks）] タブで、[OVFテンプレートの展開（Deploy OVF template）] ジョブと [OVFパッケージのインポート（Import OVF package）] ジョブのステータスを確認します。

ステップ 5 展開ステータスが 100% の場合は、VM をクリックし、[アクション（Actions）] > [電源（Power）] > [電源オン（Power On）] の順に選択します。

ステップ 6 5 分後、vCenter 経由で Crosswork Data Gateway にアクセスして、インストールが成功したことを確認します。

a) VM を右クリックし、[コンソールを開く（Open Console）] を選択します。

a) ユーザー名（割り当てられたロールに応じて **dg-admin** または **dg-oper**）と、対応するパスワード（インストールプロセスで作成したパスワード）を入力し、**Enter** を押します。

ステップ 7 SSH 経由で Crosswork Data Gateway VM にアクセスできることを確認します。

a) Crosswork Data Gateway 管理 IP にアクセスできるワークステーション端末から、ssh *<username>*@*<ManagementNetworkIP>* コマンドを実行します。

ここで、<username> は **dg-admin** または **dg-oper** であり、<ManagementNetworkIP> は IPv4 または IPv6 形式です。

b) パスワード（OVF テンプレートウィザードで入力したパスフレーズ情報）を入力します。

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