



## Cisco Catalyst SD-WAN の統合

最終更新：2025 年 7 月 8 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/>

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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)

© 2025 Cisco Systems, Inc. All rights reserved.



## 目次

### Full Cisco Trademarks with Software License ?

---

#### 第 1 章

最初にお読みください 1

---

#### 第 2 章

Cisco IOS XE (SD-WAN) および Cisco Catalyst SD-WAN リリースにおける新機能 3

---

#### 第 3 章

Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合 5

Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合 6

Cisco Cyber Vision との統合に関する情報 6

Cisco Cyber Vision アプリケーション 6

デバイスで Cisco Cyber Vision アプリケーションがダウンロードおよびインストールされる  
仕組み 7

Cisco Cyber Vision Center の使用 8

Cisco Cyber Vision との統合でサポートされるプラットフォーム 8

Cisco Cyber Vision との統合の前提条件 8

Cisco Cyber Vision との統合に関するガイドライン 9

Cisco Cyber Vision との統合に関する制限事項 9

Cisco Cyber Vision との統合の設定（概要） 10

ネットワーク階層内の Cisco Cyber Vision Center への接続設定 11

Cyber Vision 機能を追加した設定グループプロファイルの作成 12

設定グループへの Cyber Vision 機能の追加 15

Cisco Cyber Vision 機能を追加した設定グループの展開 15

Cisco SD-WAN Manager が Cisco Cyber Vision Center に接続されたことを確認する 17

CLI を使用して Cisco Cyber Vision アプリケーションがデバイスで動作していることを確認  
する 18

|                                         |    |
|-----------------------------------------|----|
| デバイスでの Cisco Cyber Vision アプリケーションのモニター | 19 |
|-----------------------------------------|----|

## 第 4 章

### Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合 21

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合                   | 22 |
| Cisco Secure Equipment Access との統合に関する情報                                    | 22 |
| Cisco Secure Equipment Access との統合のメリット                                     | 23 |
| Cisco Secure Equipment Access アプリケーション                                      | 23 |
| Cisco Secure Equipment ソリューションへのオンボードプロセス                                   | 24 |
| Cisco Secure Equipment Access ソリューションの利用                                    | 25 |
| Cisco Secure Equipment Access との統合でサポートされるプラットフォーム                          | 25 |
| Cisco Secure Equipment Access との統合の前提条件                                     | 26 |
| Cisco Secure Equipment Access との統合に関するガイドライン                                | 27 |
| Cisco Secure Equipment Access との統合に関する制限事項                                  | 27 |
| Cisco Secure Equipment Access との統合の設定（概要）                                   | 27 |
| ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定                        | 28 |
| SEA 機能を使用した設定グループプロファイルの作成                                                  | 29 |
| 設定グループへの Cisco SEA 機能の追加                                                    | 33 |
| Cisco SEA 機能を追加した設定グループの展開                                                  | 33 |
| Cisco SD-WAN Manager が Cisco Secure Equipment Access クラウドポータルに接続していることを確認する | 34 |
| CLI を使用して Cisco Secure Equipment Access アプリケーションがデバイスで動作していることを確認する         | 35 |
| デバイス上の Cisco Secure Equipment Access アプリケーションのモニター                          | 36 |

## 第 5 章

### サードパーティのカスタムアプリケーションと Cisco Catalyst SD-WAN の統合 39

|                                                      |    |
|------------------------------------------------------|----|
| サードパーティのカスタムアプリケーションと Cisco Catalyst SD-WAN の統合      | 40 |
| Cisco Catalyst SD-WAN とサードパーティのカスタムアプリケーションの統合に関する情報 | 40 |
| サードパーティのカスタムアプリケーションとの統合でサポートされるプラットフォーム             | 41 |
| サードパーティのカスタムアプリケーションとの統合における前提条件                     | 41 |
| サードパーティのカスタムアプリケーションとの統合に関するガイドライン                   | 42 |

|                                                 |    |
|-------------------------------------------------|----|
| サードパーティのカスタムアプリケーションとの統合に関する制約事項                | 42 |
| サードパーティのカスタムアプリケーションとの統合の設定（概要）                 | 42 |
| デバイスでの Cisco IOx のアクティブ化                        | 43 |
| カスタムアプリケーションを追加した設定グループプロファイルの作成                | 43 |
| 設定グループへのカスタムアプリケーション機能の追加                       | 46 |
| カスタムアプリケーション機能を追加した設定グループの展開                    | 47 |
| CLIを使用してサードパーティのカスタムアプリケーションがデバイスで動作していることを確認する | 47 |
| デバイスでサードパーティのカスタムアプリケーションをモニターする                | 49 |
| サードパーティのカスタムアプリケーションのアンインストール                   | 50 |





# 第 1 章

## 最初にお読みください



- (注) 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage から Cisco Catalyst SD-WAN Manager への変更、Cisco vAnalytics から Cisco Catalyst SD-WAN Analytics への変更、Cisco vBond から Cisco Catalyst SD-WAN Validator への変更、Cisco vSmart から Cisco Catalyst SD-WAN コントローラへの変更、および Cisco コントローラから Cisco Catalyst SD-WAN 制御コンポーネントへの変更。**すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

### 参考資料

- [Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#) [英語]
- [Cisco Catalyst SD-WAN Device Compatibility](#) [英語]

### ユーザーマニュアル

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#) [英語]

### 通信、サービス、およびその他の情報

- [Cisco Profile Manager](#) で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、[シスコサービス](#)にアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリケーション、製品、ソリューション、サービスをお求めの場合は、[Cisco DevNet](#) にアクセスしてください。

- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、[Cisco Bug Search Tool](#) にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#) にアクセスしてください。

### マニュアルに関するフィードバック

シスコのテクニカルマニュアルに関するフィードバックを提供するには、それぞれのオンラインマニュアルの右側のペインにあるフィードバックフォームを使用してください。



## 第 2 章

# Cisco IOS XE (SD-WAN) および Cisco Catalyst SD-WAN リリースにおける新機能

シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次のリンクには、コンフィギュレーションガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されているリリースごとの新機能と変更された機能が含まれています。Cisco Catalyst SD-WAN ソリューションに関する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

[What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x](#) [英語]

[What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x](#) [英語]

[What's New in Cisco SD-WAN \(vEdge\) Release 20.x](#) [英語]

[What's New in Cisco SD-WAN \(vEdge\) Release 19.x](#) [英語]





## 第 3 章

# Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合

---

- [Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合 \(6 ページ\)](#)
- [Cisco Cyber Vision との統合に関する情報 \(6 ページ\)](#)
- [Cisco Cyber Vision アプリケーション \(6 ページ\)](#)
- [デバイスで Cisco Cyber Vision アプリケーションがダウンロードおよびインストールされる仕組み \(7 ページ\)](#)
- [Cisco Cyber Vision Center の使用 \(8 ページ\)](#)
- [Cisco Cyber Vision との統合でサポートされるプラットフォーム \(8 ページ\)](#)
- [Cisco Cyber Vision との統合の前提条件 \(8 ページ\)](#)
- [Cisco Cyber Vision との統合に関するガイドライン \(9 ページ\)](#)
- [Cisco Cyber Vision との統合に関する制限事項 \(9 ページ\)](#)
- [Cisco Cyber Vision との統合の設定 \(概要\) \(10 ページ\)](#)
- [Cisco SD-WAN Manager が Cisco Cyber Vision Center に接続されたことを確認する \(17 ページ\)](#)
- [CLI を使用して Cisco Cyber Vision アプリケーションがデバイスで動作していることを確認する \(18 ページ\)](#)
- [デバイスでの Cisco Cyber Vision アプリケーションのモニター \(19 ページ\)](#)

# Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合

表 1: 機能の履歴

| 機能名                     | リリース情報                                                                                                                                           | 機能説明                                                                                                                                                                                           |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Cyber Vision との統合 | <p>Cisco IOS XE Catalyst SD-WAN リリース 17.15.1a</p> <p>Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.1</p> <p>Cisco Cyber Vision Center リリース 5.0.0</p> | Cisco SD-WAN Manager は、Cisco Cyber Vision ネットワーク セキュリティ ソリューションとの統合をサポートします。1 つまたは複数のインターフェイスのトラフィックをモニターして、セキュリティ上の懸念事項を分析するためにトラフィックを Cisco Cyber Vision Center に送信するようにネットワーク内のデバイスを設定できます。 |

## Cisco Cyber Vision との統合に関する情報

Cisco SD-WAN Manager は、ネットワーク セキュリティ ソリューションである Cisco Cyber Vision との統合をサポートしています。Cisco Cyber Vision は、グローバルネットワークのセキュリティステータスを可視化し、ネットワーク内のデバイスが安全なポスチャを維持するために注意が必要なタイミングを示し、セキュリティポリシーの設定などを支援します。ブラウザベースのマネージャは、Cisco Cyber Vision Center と呼ばれます。Cisco Cyber Vision のドキュメントは、[こちら](#)で入手できます。

### 統合の価値

この統合により、Cisco SD-WAN Manager を使用してネットワーク内のデバイスがセンサーとして動作するように設定したり、Cisco Cyber Vision の用語を使用したりできるようになります。センサーとは、1 つまたは複数のインターフェイスのトラフィックをモニターして、セキュリティ上の懸念事項を分析するためにトラフィックを Cisco Cyber Vision Center に送信するように設定するデバイス（ルータなど）です。こうしたセンサーは、Cisco Cyber Vision でネットワーク内のセキュリティ脅威を管理できるようにするための重要な部分です。

## Cisco Cyber Vision アプリケーション

ネットワークデバイスで有効にできる多くの機能とは対照的に、Cisco Cyber Vision 機能は Cisco IOS XE Catalyst SD-WAN ソフトウェアリリースの一部として組み込まれていません。

デバイスで Cisco Cyber Vision を有効にすると、デバイスでは Cisco Cyber Vision アプリケーションがダウンロード後にインストールされます。これは、Docker コンテナで動作する Cisco IOx アプリケーションです。他の Cisco IOx アプリケーションと同様に、Cisco Cyber Vision ア

アプリケーションは Cisco IOS XE Catalyst SD-WAN と連携して動作し、追加の機能を提供します。

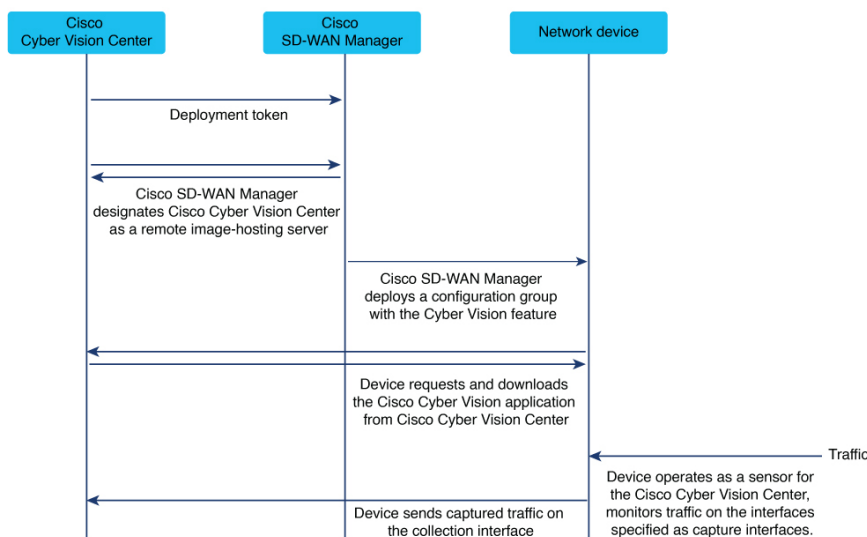
インストールが正常に完了すると、デバイスは Cisco Cyber Vision のセンサーとして動作します。このデバイスが Cisco Cyber Vision Center のセンサーリストに表示されます。

## デバイスで Cisco Cyber Vision アプリケーションがダウンロードおよびインストールされる仕組み

Cisco Cyber Vision との統合の場合、Cisco SD-WAN Manager は Cisco Cyber Vision Center を Cisco Cyber Vision アプリケーションのリモートイメージホスティングサーバーとして指定します。

### アプリケーションのインストールプロセスの概要

図 1: Cisco Cyber Vision と Cisco Catalyst SD-WAN の統合



1. ネットワーク階層内の [Cisco Cyber Vision Center への接続設定 \(11 ページ\)](#) に記載の手順の前提条件で示されているように、Cisco Cyber Vision Center にログインして、展開トークンと呼ばれるタイプのトークンを生成します。
2. ネットワーク階層内の [Cisco Cyber Vision Center への接続設定 \(11 ページ\)](#) に記載の手順を完了すると、Cisco SD-WAN Manager は展開トークンの情報を使用して、Cisco Cyber Vision Center を Cisco Cyber Vision アプリケーションのホストとして指定します。

Cisco SD-WAN Manager は Cisco Cyber Vision Center をアプリケーションのダウンロード元のホストとして指定するために、Cisco Cyber Vision Center をリモートサーバーとして追加します。追加されると、**[Maintenance] > [Software Repository]** ページの **[Remote server]** タブに表示されます。[Cisco Cyber Vision との統合に関するガイドライン \(9 ページ\)](#) で説明されているように、このサーバーは編集または削除しないでください。

3. Cisco Cyber Vision の設定をネットワーク内のデバイスにプッシュすると、デバイスが Cisco Cyber Vision Center に接続されて、Cisco Cyber Vision アプリケーションがダウンロードされます。
4. デバイスではアプリケーションがインストールされた後に、アクティブ化されます。これにより、デバイスが Cisco Cyber Vision Center のセンサーとして機能できるようになります。

## Cisco Cyber Vision Center の使用

ここで説明する手順を実行すると、デバイスが Cisco Cyber Vision Center のセンサーとして機能できるようになります。設定が完了したら、Cisco Cyber Vision Center を使用して、Cisco Catalyst SD-WAN で管理しているネットワークのセキュリティをモニターします。詳細については、最新の [Cisco Cyber Vision GUI アドミニストレーションガイド \[英語\]](#) を参照してください。

## Cisco Cyber Vision との統合でサポートされるプラットフォーム

表 2: サポートされるプラットフォーム

| プラットフォームシリーズ                   | モデル                                  | サポート対象の最低バージョン                              |
|--------------------------------|--------------------------------------|---------------------------------------------|
| Cisco Catalyst IR1100 高耐久性シリーズ | IR 1101                              | Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.15.1 |
| Cisco Catalyst IR1800 高耐久性シリーズ | IR1821<br>IR1831<br>IR1833<br>IR1835 | Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.16.1 |

## Cisco Cyber Vision との統合の前提条件

### Cisco Cyber Vision Center のバージョン

Cisco Cyber Vision Center リリース 5.0.0 以降

### Cisco Cyber Vision Center へのネットワーク到達可能性

Cisco Cyber Vision 機能を追加した設定グループを展開する前に、ネットワーク内のデバイスが Cisco Cyber Vision Center に到達できることを確認します。

この要件があるため、デバイスと Cisco Cyber Vision Center を連携させるための設定は、次の 2 段階のプロセスになります。

1. 設定グループを一連のデバイスに展開して、Cisco Cyber Vision Center への到達可能性を確立します。
2. 設定グループを一連のデバイスに展開して、デバイスで Cisco Cyber Vision を有効にします。

前の手順で到達可能性を確立したら、その手順でを使用したものと同じ設定グループを変更して Cisco Cyber Vision 機能を追加し、その設定グループをデバイスに展開できます。

Cisco Cyber Vision 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco Cyber Vision Center への到達可能性を確立します。

### 仮想ポートグループ

Cisco Cyber Vision アプリケーションでは、仮想ポートグループ (VPG) インターフェイス 5 および 6 が使用可能である必要があります。これらの VPG インターフェイスが別のアプリケーションで使用するよう設定されていないことを確認してください。

## Cisco Cyber Vision との統合に関するガイドライン

リモートサーバーは削除しないでください

Cisco SD-WAN Manager では、1 つ以上の Cisco Cyber Vision Center インスタンスが **[Maintenance]** > **[Software Repository]** ページの **[Remote server]** タブにサーバーとして追加されます。

これらのリモートサーバーは編集または削除しないでください。

## Cisco Cyber Vision との統合に関する制限事項

### Cisco IOx アプリケーションの制限事項

デバイスが Cisco Cyber Vision アプリケーションを実行している場合、他の Cisco IOx アプリケーションを実行することはできません。

同じトークンを使用して、**Cisco Cyber Vision Center** にデバイスを複数回オンボードすることはできません

この制限事項は、Cisco Catalyst SD-WAN Manager リリース 20.16.x にのみ適用されます。

ネットワーク階層内の **Cisco Cyber Vision Center** への接続設定（11 ページ）で説明されているように、Cisco SD-WAN Manager は Cisco Cyber Vision で作成された展開トークンを使用して、Cisco Cyber Vision Center とのセキュアなリンク（手順内では接続と呼ばれます）を確立します。Cisco SD-WAN Manager と Cisco Cyber Vision Center の間にこのような接続を複数設定できます。

Cisco Catalyst SD-WAN Manager リリース 20.16.x を使用する場合、1 つの展開トークンを使用して 1 回だけネットワーク内のデバイスを Cisco Cyber Vision Center にオンボードできます。

Cisco Cyber Vision Center インスタンスからデバイスをアンインストールする場合、新しいトークンを使用して同じ Cisco Cyber Vision Center インスタンスにデバイスを再展開する必要があります。Cisco SD-WAN Manager では、これは Cisco Cyber Vision Center への新しい接続を使用することを意味します。

別の **Cisco Cyber Vision Center** インスタンスにデバイスを移動するには、デバイスから **Cyber Vision** アプリケーションをアンインストールする必要があります。

この制限事項は、Cisco Catalyst SD-WAN Manager リリース 20.15.x および Cisco Catalyst SD-WAN Manager リリース 20.16.x に適用されます。

Cisco Cyber Vision のインスタンスにオンボードしたデバイスを Cisco Cyber Vision の別のインスタンスに移動する必要がある場合は、最初に Cyber Vision 機能が搭載されていないデバイスに設定をプッシュする必要があります。これにより、デバイスから Cyber Vision アプリケーションがアンインストールされます。次に、新しい Cisco Cyber Vision インスタンスを示すデバイスに新しい設定をプッシュします。

## Cisco Cyber Vision との統合の設定（概要）

### 手順

- 
- ステップ 1 ネットワーク階層内の **Cisco Cyber Vision Center** への接続設定（11 ページ）
  - ステップ 2 **Cyber Vision** 機能を追加した設定グループプロファイルの作成（12 ページ）
  - ステップ 3 設定グループへの **Cyber Vision** 機能の追加（15 ページ）
  - ステップ 4 **Cisco Cyber Vision** 機能を追加した設定グループの展開（15 ページ）
-

### 次のタスク

設定手順が完了すると、デバイスで実行されている Cisco Cyber Vision アプリケーションのアクティビティをモニターできます。[デバイスでの Cisco Cyber Vision アプリケーションのモニター \(19 ページ\)](#) を参照してください。

## ネットワーク階層内の Cisco Cyber Vision Center への接続設定

### 始める前に

- 展開トークン

Cisco Cyber Vision Center で 1 つ以上の展開トークンを作成して、デバイスが Cisco Cyber Vision Center とのセキュアなリンクを確立できるようにします。次の表では、サポートされるプラットフォームの種類に応じて必要なトークンタイプを示します。

表 3: プラットフォームに必要なトークンタイプ

| プラットフォーム                       | トークンタイプ           |
|--------------------------------|-------------------|
| Cisco Catalyst IR1101 高耐久性シリーズ | cviox-aarch64.tar |

展開トークンの作成に関する詳細は、最新の[Cisco Cyber Vision GUI アドミニストレーションガイド \[英語\]](#) を参照してください。

トークンテキストをコピーし、手順でできるように準備しておきます。

- 接続

Cisco Cyber Vision と連携するネットワーク内のデバイスは、ネットワークを経由して Cisco Cyber Vision Center に到達する必要があります。ネットワークトポロジがこの到達可能性を提供していることを確認します。

### 手順

**ステップ 1** Cisco SD-WAN Manager メニューから、**[Configuration] > [Network Hierarchy]** を選択します。

**ステップ 2** **[External Services]** をクリックします。

**ステップ 3** **[Cyber Vision]** ペインで **[Add Cyber Vision Center]** をクリックします。

**ステップ 4** Cisco Cyber Vision 接続のテーブルで、次のように入力します。

| フィールド | 説明                             |
|-------|--------------------------------|
| Name  | Cisco Cyber Vision Center の名前。 |

| フィールド                  | 説明                                                                          |
|------------------------|-----------------------------------------------------------------------------|
| IP Address or Hostname | Cisco Cyber Vision Center をホストするサーバーの IP アドレス。<br>(注)<br>ホスト名を入力することはできません。 |
| Token                  | 前提条件に記載されているように、Cisco Cyber Vision Center からコピーした展開トークンに貼り付けます。             |
| VPN                    | ネットワーク内のデバイスが Cisco Cyber Vision Center に接続するための VPN。                       |

ステップ 5 [Save] をクリックします。

トークンに含まれている情報を使用して、Cisco SD-WAN Manager はリモート イメージ ホスティング サーバーの 1 つとしてサーバーを自動的に設定します。このサーバーは、**[Maintenance]>[Software Repository]** ページの **[Remote server]** タブに表示されます。[デバイスで Cisco Cyber Vision アプリケーションがダウンロードおよびインストールされる仕組み \(7 ページ\)](#) を参照してください。

## Cyber Vision 機能を追加した設定グループプロファイルの作成

始める前に

**[Configuration]>[Configuration Groups]** ページで、次のいずれかを選択します。

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択します。

### 手順

ステップ 1 Cisco SD-WAN Manager のメニューから、**[Configuration]>[Configuration Groups]** を選択します。

ステップ 2 その他のプロファイルで [Cyber Vision](#) 機能を作成して設定します。

1. この機能の名前と説明を入力します。

表 4: 名前と説明

| フィールド       | 説明                             |
|-------------|--------------------------------|
| Name        | Cisco Cyber Vision Center の名前。 |
| Description | 任意で説明を追加します。                   |

## 2. 基本の設定フィールドを入力します。

表 5: 基本設定

| フィールド                       | 説明                                                                                                                                      |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Cyber Vision Center         | ドロップダウンリストで、以前に設定した接続リストから Cisco Cyber Vision Center 接続を選択します。「 <a href="#">ネットワーク階層内の Cisco Cyber Vision Center への接続設定</a> 」を参照してください。 |
| Monitoring Source Interface | [Add] をクリックして、トラフィックのモニタリングで使用するデバイスのインターフェイスを入力します。デバイスでモニターするネットワークやトラフィックに応じて選択します。<br><br>例：VLAN インターフェイス、セルラーインターフェイス、WAN インターフェイス |

## 3. [Advanced Configuration] エリアは、[SD-WAN] ソリューションオプションで [Cyber Vision] 機能を設定している場合にのみ表示されます。[SD-Routing] ソリューションオプションの場合は表示されません。

このエリアのフィールドでは変数を使用するように事前設定されており、ユーザーは設定グループを展開するときに各デバイス固有の情報を入力できます。[Cisco Cyber Vision 機能を追加した設定グループの展開（15 ページ）](#)を参照してください。ただし、変数を使用する代わりに、グローバルデバイス値を使用することもできます。

表 6: 詳細設定

| フィールド                         | 説明                                    |
|-------------------------------|---------------------------------------|
| Capture Interface IP          | 分析対象のトラフィックをキャプチャするインターフェイスの IP アドレス。 |
| Capture Interface Subnet Mask | 分析対象のトラフィックをキャプチャするインターフェイスのサブネットマスク。 |

| フィールド                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Collection Interface (Sensor to Center) IP | <p>キャプチャされたトラフィックを Cisco Cyber Vision Center に送信する収集インターフェイスの IP アドレスを入力します。この IP アドレスが [Collection Interface Subnet Mask] フィールドで定義されたサブネットマスク内にあることを確認してください。</p> <p>(注)</p> <p>同じサービス VPN を介して Cisco Cyber Vision Center に接続しているデバイスごとに、収集インターフェイスの一意の IP アドレスを入力します。</p> <p>単一のサービス VPN 内の各インターフェイスでは、一意の IP アドレスを使用する必要があります。</p> <p>Cisco Cyber Vision Center との通信用に設定されたサービス VPN を表示する方法については、「<a href="#">ネットワーク階層内の Cisco Cyber Vision Center への接続設定</a>」を参照してください。</p> |
| Collection Interface Subnet Mask           | <p>キャプチャされたトラフィックを Cisco Cyber Vision Center に送信する収集インターフェイスのサブネットマスク。このサブネットマスクは、デバイスと Cisco Cyber Vision Center 間の通信に使用されるサービス VPN のアドレス空間を定義します。</p>                                                                                                                                                                                                                                                                                                                         |
| VPG5 (Virtual Port Group) IP Address       | <p>[Collection Interface Subnet Mask] フィールドで定義されたサブネットマスク内の IP アドレス。これは、収集インターフェイスと同じネットワークのアドレスです。</p> <p>(注)</p> <p>同じサービス VPN を介して Cisco Cyber Vision Center に接続しているデバイスごとに、VPG5 の一意の IP アドレスを入力します。</p> <p>単一のサービス VPN 内の各インターフェイスでは、一意の IP アドレスを使用する必要があります。</p>                                                                                                                                                                                                           |
| VPG6 (Virtual Port Group) IP Address       | <p>このフィールドは事前設定されており、編集できません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 次のタスク

「[Deploy a configuration group](#)」[英語] も参照してください。

## 設定グループへの Cyber Vision 機能の追加

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。

**ステップ 2** [solution] ドロップダウンリストで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択し、このソリューションの設定グループのみを表示します。

**ステップ 3** [Configuration Groups] タブをクリックします。

**ステップ 4** 設定グループを作成する必要がある場合は、『Cisco Catalyst SD-WAN Configuration Groups』の「[Using Configuration Groups](#)」[英語] で説明されている手順に従います。

**ステップ 5** 既存の設定グループの場合は、[Add Profile] をクリックして、設定グループに [Other Profile] を追加します。

**ステップ 6** 設定グループで [Other Profile] ドロップダウンリストを見つけて、Cisco Cyber Vision プロファイルを選択します。

## Cisco Cyber Vision 機能を追加した設定グループの展開

### 始める前に

- Cisco Cyber Vision 機能を追加した設定グループを展開する前に、[Cisco Cyber Vision との統合でサポートされるプラットフォーム（8 ページ）](#) を参照してください。
- Cisco Cyber Vision 機能を追加した設定グループを展開する前に、ネットワーク内のデバイスが Cisco Cyber Vision Center に到達できることを確認します。これには次の 2 つの手順が必要です。

1. 設定グループを展開して、Cisco Cyber Vision Center への到達可能性を確立します。
2. 設定グループを展開して、デバイスで Cisco Cyber Vision を有効にします。

前の手順で到達可能性を確立したら、その手順でを使用したものと同じ設定グループを変更して Cisco Cyber Vision 機能を追加し、その設定グループをデバイスに展開できます。

[Cisco Cyber Vision との統合の前提条件（8 ページ）](#) を参照してください。



- (注) Cisco Cyber Vision 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco Cyber Vision Center への到達可能性を確立します。

## 手順

**ステップ 1** 『Cisco Catalyst SD-WAN Configuration Groups』の「[standard configuration group deployment procedure](#)」[英語]に従って、ネットワーク内のデバイスに設定グループを展開します。

**ステップ 2** SD-WAN ソリューションタイプのデバイスに展開する場合は、展開時にルータごとに [CV\_SDWAN] ペインでデバイス固有の変数を入力します。

SD-Routing ソリューションタイプのデバイスに展開する場合は、この手順をスキップしてください。

| フィールド                 | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| collection_int_ip     | <p>キャプチャされたトラフィックを Cisco Cyber Vision Center に送信する収集インターフェイスの IP アドレスを入力します。この IP アドレスが [collection_int_subnet] フィールドで定義されたサブネットマスク内にあることを確認してください。</p> <p>(注)</p> <p>同じサービス VPN を介して Cisco Cyber Vision Center に接続しているデバイスごとに、収集インターフェイスの一意の IP アドレスを入力します。</p> <p>単一のサービス VPN 内の各インターフェイスでは、一意の IP アドレスを使用する必要があります。</p> <p>Cisco Cyber Vision Center との通信用に設定されたサービス VPN を表示する方法については、<a href="#">ネットワーク階層内の Cisco Cyber Vision Center への接続設定 (11 ページ)</a> を参照してください。</p> |
| collection_int_subnet | <p>キャプチャされたトラフィックを Cisco Cyber Vision Center に送信する収集インターフェイスのサブネットマスク。このサブネットマスクは、デバイスと Cisco Cyber Vision Center 間の通信に使用されるサービス VPN のアドレス空間を定義します。</p>                                                                                                                                                                                                                                                                                                                      |

| フィールド   | 説明                                                                                                                                                                                                                                                         |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vpg5-ip | <p>[collection_int_subnet] フィールドで定義されたサブネットマスク内の IP アドレス。これは、収集インターフェイスと同じネットワークのアドレスです。</p> <p>(注)</p> <p>同じサービス VPN を介して Cisco Cyber Vision Center に接続しているデバイスごとに、VPG5 の一意の IP アドレスを入力します。</p> <p>単一のサービス VPN 内の各インターフェイスでは、一意の IP アドレスを使用する必要があります。</p> |

**ステップ 3** デバイスに Cisco Cyber Vision アプリケーションをインストールする際に進行状況をモニターするには、インストールのログメッセージを表示します。

1. 右上近くにあるタスクリストボタンをクリックします。
2. [Deploy configuration group] タスクをクリックします。  
この操作により、各デバイスに関する展開の進行状況を示すページが開きます。
3. デバイスの横にある [Action] 列のログアイコンをクリックします。

[View Logs] ペインが開き、そのデバイスに関する展開の進行状況が表示されます。展開が完了し、デバイスと Cisco Cyber Vision サーバーとの接続が確立されると、「Config Group successfully deployed to device,」といった成功メッセージがログに表示されます。

Cisco Cyber Vision 機能を追加した設定グループをはじめてデバイスに展開すると、デバイスで Cisco Cyber Vision アプリケーションのインストールがトリガーされます。デバイスで Cisco Cyber Vision アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco Cyber Vision のセンサーとして動作します。このデバイスが Cisco Cyber Vision Center のセンサーリストに表示されます。これを確認する方法については、[Cisco SD-WAN Manager が Cisco Cyber Vision Center に接続されたことを確認する \(17 ページ\)](#) を参照してください。

## Cisco SD-WAN Manager が Cisco Cyber Vision Center に接続されたことを確認する

Cisco Cyber Vision 機能を追加した設定グループを作成した場合、その設定グループをデバイスに展開すると、デバイスで Cisco Cyber Vision アプリケーションのインストールがトリガーされます。デバイスで Cisco Cyber Vision アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco Cyber Vision のセンサーとして動作します。このデバイスが Cisco Cyber Vision Center のセンサーリストに表示されます。  
「[Cisco Cyber Vision アプリケーション](#)」を参照してください。

CLI を使用して Cisco Cyber Vision アプリケーションがデバイスで動作していることを確認する

### 始める前に

Cisco Cyber Vision 機能を追加した設定グループを 1 つ以上のデバイスに展開します。Cisco Cyber Vision 機能を追加した設定グループの展開 (15 ページ) を参照してください。

### 手順

**ステップ 1** Cisco Cyber Vision Center にログインします。

**ステップ 2** アクティブなセンサーを表示します。詳細については、最新の [Cisco Cyber Vision GUI アドミニストレーション ガイド \[英語\]](#) を参照してください。

各デバイスは、センサーのリストに個別に表示されます。

## CLI を使用して Cisco Cyber Vision アプリケーションがデバイスで動作していることを確認する

この検証方法は、SD-WAN または SD-Routing ソリューションのデバイスに適用できます。

### 始める前に

Cisco Cyber Vision 機能を追加した設定グループを 1 つ以上のデバイスに展開します。Cisco Cyber Vision 機能を追加した設定グループの展開 (15 ページ) を参照してください。

### 手順

**ステップ 1** Cisco Cyber Vision アプリケーションを実行しているデバイスで、次のコマンドを実行します。

```
Device# show iox-service
```

**ステップ 2** 前のステップのコマンドの出力に基づいて、次のいずれかを実行します。

- コマンド出力に IOxman サービスが実行中であることが示されている場合は、次の手順に進みます。
- コマンド出力に IOxman サービスが実行中ではないと表示される場合は、Cisco Cyber Vision アプリケーションが正しく動作していないことを示します。アプリケーションを再インストールします。Cisco Cyber Vision 機能を追加した設定グループの展開 (15 ページ) を参照してください。

**ステップ 3** 同じデバイスで、次のコマンドを実行します。実行中の状態であるとコマンド出力に表示される場合は、Cisco Cyber Vision アプリケーションが正しく動作していることを示します。

```
Device# show app-hosting detail appid cv
```

### 例

この例では、Cisco Cyber Vision アプリケーションがインストールされ、動作しています。ここではコマンド出力が省略されることに注意してください。

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)           : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)   : Running
Libvirtd 5.5.0             : Running
Dockerd v19.03.13-ce      : Running

Device# show app-hosting detail appid cv
App id                      : cv
Owner                      : iox
State                      : RUNNING
...
```

## デバイスでの Cisco Cyber Vision アプリケーションのモニター

### 始める前に

Cisco Cyber Vision 機能を追加した設定グループを 1 つ以上のデバイスに展開します。[Cisco Cyber Vision 機能を追加した設定グループの展開 \(15 ページ\)](#) を参照してください。

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。

**ステップ 2** SD-WAN ソリューションの対象デバイス名をクリックします。

(注)

このモニタリング方法は、SD-WAN ソリューションのデバイスには適用できますが、SD-Routing ソリューションのデバイスには適用できません。

**ステップ 3** **[Real Time]** タブをクリックします。

**ステップ 4** **[Device Options]** フィールドに次のいずれかのアプリケーションホスティングコマンドを入力して、デバイスで実行されている Cisco Cyber Vision アプリケーションのリソース使用状況やその他の詳細を表示します。

- アプリケーション ホスティングの詳細
- アプリケーション ホスティングの稼働率
- アプリケーション ホスティング ネットワークの稼働率

- アプリケーション ホスティング ストレージの使用率
  - アプリケーション ホスティング プロセス
  - アプリケーション ホスティングでアタッチされるデバイス
  - アプリケーション ホスティング ネットワーク インターフェイス
  - アプリケーション ホスティング ゲスト ルート
-



## 第 4 章

# Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合

---

- [Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合 \(22 ページ\)](#)
- [Cisco Secure Equipment Access との統合に関する情報 \(22 ページ\)](#)
- [Cisco Secure Equipment Access アプリケーション \(23 ページ\)](#)
- [Cisco Secure Equipment ソリューションへのオンボードプロセス \(24 ページ\)](#)
- [Cisco Secure Equipment Access ソリューションの利用 \(25 ページ\)](#)
- [Cisco Secure Equipment Access との統合でサポートされるプラットフォーム \(25 ページ\)](#)
- [Cisco Secure Equipment Access との統合の前提条件 \(26 ページ\)](#)
- [Cisco Secure Equipment Access との統合に関するガイドライン \(27 ページ\)](#)
- [Cisco Secure Equipment Access との統合に関する制限事項 \(27 ページ\)](#)
- [Cisco Secure Equipment Access との統合の設定 \(概要\) \(27 ページ\)](#)
- [Cisco SD-WAN Manager が Cisco Secure Equipment Access クラウドポータルに接続していることを確認する \(34 ページ\)](#)
- [CLI を使用して Cisco Secure Equipment Access アプリケーションがデバイスで動作していることを確認する \(35 ページ\)](#)
- [デバイス上の Cisco Secure Equipment Access アプリケーションのモニター \(36 ページ\)](#)

# Cisco Secure Equipment Access と Cisco Catalyst SD-WAN の統合

表 7: 機能の履歴

| 機能名                                | リリース情報                                                                                   | 機能説明                                                                                                                                                                                                                                                                                                  |
|------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Secure Equipment Access との統合 | Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a<br>Cisco Catalyst SD-WAN Manager リリース 20.16.1 | Cisco Secure Equipment Access (SEA) は、ネットワーク接続されたアセットへのリモートアクセスを提供するソリューションです。アセットには、サーバー、Industrial Internet of Things (IIoT) デバイスなど、IPアドレスによって到達可能なものをすべて含めることができます。<br><br>Cisco Catalyst SD-WAN との統合により、Cisco SD-WAN Manager を使用して Cisco Catalyst SD-WAN ネットワーク内に Cisco SEA ソリューションを展開できるようになります。 |

## Cisco Secure Equipment Access との統合に関する情報

Cisco Secure Equipment Access (SEA) は、ネットワーク接続されたアセットへのリモートアクセスを提供するソリューションです。アセットには、サーバー、Industrial Internet of Things (IIoT) デバイスなど、IPアドレスによって到達可能なものをすべて含めることができます。Cisco Catalyst SD-WAN との統合により、Cisco SD-WAN Manager を使用して次のことが可能になります。

- Cisco Catalyst SD-WAN オーバーレイネットワーク内にあるルータなどのデバイスに SEA エージェントをインストールする
- オーバーレイネットワーク内のデバイスと Cisco Secure Equipment Access クラウドポータル間の接続を設定する
- リモートアセットがデバイスに接続する方法を設定する

デバイスに SEA エージェントをインストールして、ここで説明した接続を設定すると、他のリモートアクセスタスクは Cisco SEA に対して通常どおり動作します。Cisco DevNet サイトの「[Secure Equipment Access Overview](#)」[英語]を参照してください。

## Cisco Secure Equipment Access との統合のメリット

時間とコストのかかるサイト訪問を行うことなく、運用テクノロジー（OT）のアセットを設定、管理、障害対応するためには、リモートアクセスが欠かせません。Cisco Secure Equipment（SEA）は、ゼロトラストネットワークアクセス（ZTNA）ソリューションのすべてのメリットと、運用環境への大規模展開を簡素化するネットワークアーキテクチャを融合したものです。インストールと管理のための専用ハードウェアや、設定と保守を行うための複雑なファイアウォールルールはありません。包括的なセキュリティ機能、高度なサイバーセキュリティ制御、アイデンティティとコンテキストに基づき簡単に作成できるポリシーを備えています。

Cisco SEA には、次に示すような多くのメリットがあります。

- 運用の効率化

運用チームは、OT アセットが NAT 境界の背後にある場合でも簡単にリモートアクセスできます。

- シンプルな設置と拡張性

既存のルータやスイッチを使用して運用するため、専用アプライアンスや複雑なファイアウォール設定は必要ありません。

- 強力なセキュリティ制御

MFA と SSO でユーザーを認証します。Cisco SEA は、各ユーザーのセキュリティ態勢を検証し、関連するアセットへのアクセスのみを提供します。

- 最小権限アクセス

特定のプロトコルのみを使用し、指定された時間にのみ特定のデバイスにアクセスすることを厳選されたユーザーに許可します。

- 監査証跡

セッションを記録し、調査とコンプライアンスのために監査証跡を作成します。

## Cisco Secure Equipment Access アプリケーション

### SEA エージェントのインストール

Cisco Secure Equipment Access（SEA）エージェントと呼ばれる Cisco IOx アプリケーションは、デバイス（ネットワーク内のルータ）に Cisco SEA の機能を提供します。Cisco SD-WAN Manager を介してデバイスで Cisco SEA を有効にすると、デバイスでは Cisco SEA アプリケーションがダウンロード後にインストールされます。

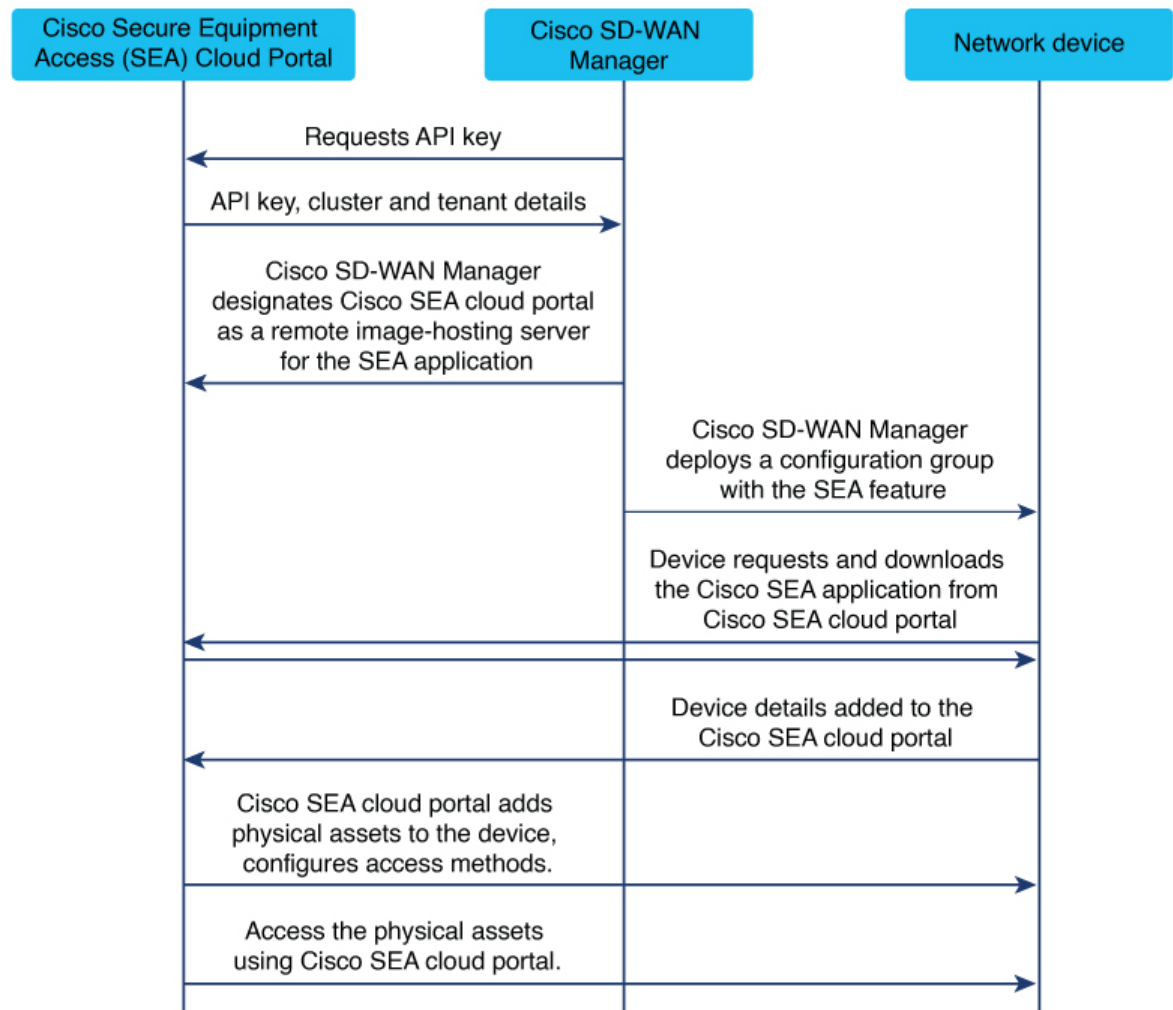
### Cisco SEA クラウドポータル

Cisco SEA エージェントのインストールが正常に完了すると、デバイスは Cisco SEA クラウドポータルと通信します。通信するデバイスは、Cisco SEA クラウドポータルのデバイスリストに表示されます。

## Cisco Secure Equipment ソリューションへのオンボードプロセス

### オンボードプロセスの概要

図 2: Cisco Secure Equipment Access と Cisco Catalyst



の統合

1. 接続を確立するための API キーの取得

ネットワーク階層での [Cisco Secure Equipment Access ポータルへの接続の設定](#) (28 ページ) の手順の前提条件に従い Cisco SEA クラウドポータルにログインして、API キーを生成します。

## 2. Cisco SEA アプリケーションのイメージホスティング サーバーの指定

[ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定](#) (28 ページ) の手順を完了すると、Cisco SD-WAN Manager では API キー情報に基づいて、Cisco SEA クラウドポータルが Cisco SEA アプリケーションのリモートイメージ ホスティング サーバーとして指定されます。

アプリケーションのダウンロード元のホストとして Cisco SEA を指定するために、Cisco SD-WAN Manager では Cisco SEA クラウドポータルがリモートサーバーとして追加されます。追加されると、[Maintenance] > [Software Repository] ページの [Remote server] タブに表示されます。[Cisco Secure Equipment Access との統合に関するガイドライン](#) (27 ページ) で説明されているように、このサーバーは編集または削除しないでください。

## 3. Cisco SEA アプリケーションのダウンロード

Cisco SEA の設定をネットワーク内のデバイスにプッシュすると、デバイスが Cisco SEA クラウドポータルに接続されて、Cisco SEA アプリケーションがダウンロードされます。

## 4. アプリケーションのアクティブ化

デバイスではアプリケーションがインストールされた後に、アクティブ化されます。これにより、デバイスが Cisco SEA ソリューションの一部として機能できるようになります。

# Cisco Secure Equipment Access ソリューションの利用

ここで説明する手順を実行すると、デバイスを Cisco Secure Equipment Access ソリューションの一部として機能させることができます。この設定が完了したら、Cisco SEA を使用してリモートアセットへのアクセスを管理します。詳細については、Cisco DevNet サイトの [Cisco Secure Equipment Access のマニュアル](#) [英語] を参照してください。

# Cisco Secure Equipment Access との統合でサポートされるプラットフォーム

表 8: サポートされるプラットフォーム

| プラットフォーム シリーズ                      | モデル                   |
|------------------------------------|-----------------------|
| Cisco Catalyst IR1100 高耐久性シリーズ ルータ | Cisco Catalyst IR1101 |

| プラットフォーム シリーズ                      | モデル                   |
|------------------------------------|-----------------------|
| Cisco Catalyst IR1800 高耐久性シリーズ ルータ | Cisco Catalyst IR1821 |
|                                    | Cisco Catalyst IR1831 |
|                                    | Cisco Catalyst IR1833 |
|                                    | Cisco Catalyst IR1835 |

## Cisco Secure Equipment Access との統合の前提条件

### Cisco Secure Equipment Access ポータルへのネットワーク到達可能性

Cisco SEA 機能を追加した設定グループを展開する前に、Cisco SEA エージェント アプリケーションを実行するネットワーク内のルータが Cisco SEA クラウドポータルにネットワーク経由で到達できることを確認してください。

この要件があるため、デバイスと Cisco SEA を連携させるための設定は、次の 2 段階のプロセスになります。

1. 設定グループを一連のデバイスに展開して、Cisco SEA クラウドポータルへの到達可能性を確立します。
2. 設定グループを一連のデバイスに展開して、デバイスで Cisco SEA を有効にします。

前の手順で到達可能性を確立したら、その手順で使用したのと同じ設定グループを変更して Cisco SEA 機能を追加し、その設定グループをデバイスに展開できます。

Cisco SEA 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco SEA クラウドポータルへの到達可能性を確立します。

### 仮想ポート グループ インターフェイス

Cisco SEA アプリケーションでは、仮想ポートグループ (VPG) インターフェイス 7～10 が使用可能である必要があります。これらの VPG インターフェイスが別のアプリケーションで使用するよう設定されていないことを確認してください。

Cisco SEA アプリケーションは、Cisco SEA クラウドポータルに接続するために VPG インターフェイス 7 を使用し、リモートアセットに接続するために VPG インターフェイス 8～10 を予約します。仮想ポートグループに適用される制限については、[Cisco Secure Equipment Access との統合に関する制限事項 \(27 ページ\)](#) を参照してください。

### 仮想ポート グループ インターフェイス 7 の IP アドレス

Cisco SEA クラウドポータルに VPG インターフェイス 7 を接続するための IP アドレスをルータごとに設定します。

# Cisco Secure Equipment Access との統合に関するガイドライン

リモートサーバーは削除しないでください

Cisco SD-WAN Manager では、Cisco SEA ポータルインスタンスが[Maintenance] > [Software Repository]ページの [Remote server] タブにサーバーとして追加されます。

これらのリモートサーバーは編集または削除しないでください。

## Cisco Secure Equipment Access との統合に関する制限事項

### 単一の Cisco SEA クラウドポータル

Cisco SD-WAN Manager は、単一の Cisco SEA クラウドポータルにのみ接続できます。

### 単一の Cisco SD-WAN Manager

Cisco SEA クラウドポータルで定義されているように、1つの組織は1つの Cisco SD-WAN Manager にのみ接続できます。Cisco SD-WAN Manager インスタンスは単一の組織を表すため、これはマルチテナント環境で動作する Cisco SEA クラウドポータルに影響を及ぼします。

### 仮想ポートグループ（VPG）およびリモートアセット接続

Cisco SEA アプリケーションは、Cisco SEA クラウドポータルに接続するために VPG インターフェイス 7 を使用し、アセットに接続するために VPG インターフェイス 8 ～ 10 を予約します。単一の VPG インターフェイス（8、9、10 のいずれか）は、単一のリモートアセットネットワークへの接続を提供できます。リモートアセットネットワークには、複数のアセットを含めることができます。

## Cisco Secure Equipment Access との統合の設定（概要）

### 手順

- 
- ステップ 1 ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定（28 ページ）
  - ステップ 2 SEA 機能を使用した設定グループプロファイルの作成（29 ページ）
  - ステップ 3 設定グループへの Cisco SEA 機能の追加（33 ページ）
  - ステップ 4 Cisco SEA 機能を追加した設定グループの展開（33 ページ）
-

### 次のタスク

設定手順が完了すると、デバイスで実行されている Cisco SEA アプリケーションのアクティビティをモニターできます。[デバイス上の Cisco Secure Equipment Access アプリケーションのモニター \(36 ページ\)](#) を参照してください。

## ネットワーク階層での Cisco Secure Equipment Access ポータルへの接続の設定

### 始める前に

#### • API キー

Cisco SEA クラウドポータルで API キーを作成して、デバイスが Cisco SEA クラウドポータルとセキュアなリンクを確立できるようにします。

API キーの作成の詳細については、Cisco DevNet サイトの [Cisco Secure Equipment Access のマニュアル \[英語\]](#) を参照してください。API キーを生成する際、外部コントローラと統合するためのキーを有効にするオプションがある場合は、そのオプションを選択します。

API キーをコピーして、手順で使用できるように準備しておきます。

#### • 接続

Cisco SEA と連携するネットワーク内のデバイスは、ネットワークを経由して Cisco SEA クラウドポータルに到達する必要があります。ネットワークトポロジがこの到達可能性を提供していることを確認します。

### 手順

**ステップ 1** Cisco SD-WAN Manager メニューから、**[Configuration] > [Network Hierarchy]** を選択します。

**ステップ 2** **[External Services]** をクリックします。

**ステップ 3** **[Secure Equipment Access Cloud]** ペインで、次のように入力します。

表 9: **[Secure Equipment Access Cloud]** ペイン

| フィールド               | 説明                                                                                                                                                                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cluster access type | API キーオプションを選択します。 <ul style="list-style-type: none"> <li>• <b>[Manual]</b> : API キーを Cisco SEA クラウドポータルからコピーして、手動で入力します。</li> <li>• <b>[Auto]</b> : Cisco SEA クラウドポータルから API キーを自動的に取得します。</li> </ul> |

| フィールド                                  | 説明                                                                                                                                                                                |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| API Key                                | <p>(このフィールドは、[Cluster access type] で [Manual] を選択した場合に表示されます。)</p> <p>Cisco SEA クラウドポータルで生成した API キーを入力します。</p>                                                                   |
| Select Secure Equipment Access Cluster | <p>(このフィールドは、[Cluster access type] で [Auto] を選択した場合に表示されます。)</p> <p>お使いの Cisco SEA クラウドポータルのアカウントに関連付けられているクラスタ名を選択します。[Connect] をクリックし、Cisco SEA クラウドポータルのログイン情報を使ってログインします。</p> |
| VPN                                    | デバイスと Cisco SEA クラウドポータル間の到達可能性を提供する VPN。                                                                                                                                         |
| Proxy                                  | ネットワーク内のデバイスが、デバイスと Cisco SEA クラウドポータル間の接続にプロキシを必要とする場合は、プロキシの IP アドレスを入力します。                                                                                                     |

**ステップ 4** [Save] をクリックします。

API キーに含まれている情報を使用して、Cisco SD-WAN Manager はリモート イメージ ホスティング サーバーの 1 つとしてサーバーを自動的に設定します。このサーバーは、**[Maintenance] > [Software Repository]** ページの **[Remote server]** タブに表示されます。[Cisco Secure Equipment ソリューションへのオンボードプロセス \(24 ページ\)](#) を参照してください。

## SEA 機能を使用した設定グループプロファイルの作成

始める前に

**[Configuration] > [Configuration Groups]** ページで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択します。

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。

**ステップ 2** その他のプロファイルで [SEA](#) 機能を作成して設定します。

1. この機能の名前と説明を入力します。

表 10: 名前と説明

| フィールド       | 説明           |
|-------------|--------------|
| Name        | 機能の名前。       |
| Description | 任意で説明を追加します。 |

- 仮想ポートグループ（VPG）7を使用して、Cisco SEA エージェントとホストデバイスの物理インターフェイス間の接続を設定します。これは、Cisco SEA エージェントが Cisco SEA クラウドポータルに到達できるようにするために必要です。

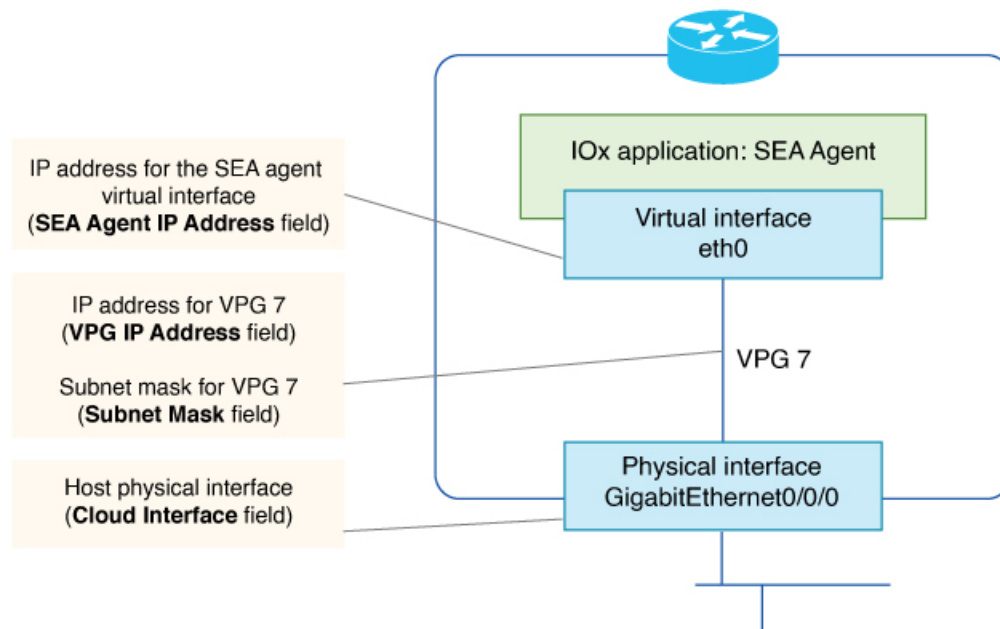


表 11: 基本設定

| フィールド          | 説明                                                                                                                             |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| VPG IP Address | 仮想ポートグループ（VPG）7に割り当てる IP アドレス。この VPG は、Cisco SEA エージェントとホストデバイスの物理インターフェイス間の仮想リンクです。<br>例：10.100.1.1                           |
| Subnet Mask    | Cisco SEA クラウドポータルに接続する VPG インターフェイス 7 のサブネットマスク。このフィールドと [VPG IP Address] によって、VPG 7 ネットワークのアドレス空間が定義されます。<br>例：255.255.252.0 |

| フィールド                | 説明                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEA Agent IP Address | <p>VPG 7 にマッピングするために Cisco SEA クラウドエージェントに割り当てる IP アドレス。[VPG IP Address] と [Subnet Mask] で定義したアドレス空間内のアドレスを入力します。</p> <p>例：10.100.1.2</p>                                                                                                                                                                                                                  |
| Cloud Interface      | <p>SD-Routing ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。</p> <p>デバイスが Cisco SEA クラウドポータルに接続するために使用する物理インターフェイスを入力します。インターフェイスタイプにはセルラーを含めることができます。</p> <p>例：GigabitEthernet0/0/0</p> <p>例：Cellular0/1/0</p> <p>(注)</p> <p>SD-WAN ソリューション (SD-Routing ソリューションではない) を設定するデバイスの場合、VPG はホストデバイスと Cisco SD-WAN Manager 間の制御接続に使用されるホストインターフェイスに自動的に接続されます。</p> |

3. 必要に応じて、アセットに接続するためのアセットネットワークを 1 つ以上設定します。

表 12: アセット アクセス ネットワーク (任意)

| フィールド              | 説明                                                                                                                                                                                                                                       |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add Access Network | <p>最大 3 つのアセットネットワークの接続を設定します。各アセットネットワークには、複数のアセットを含めることができます。</p>                                                                                                                                                                      |
| Service VPN        | <p>(SD-WAN ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。)</p> <p>アセットが複数の異なるサービス VPN に分散している場合は、必要に応じて各サービス VPN をここに追加します。</p> <p>(注)</p> <p>(a) Cisco SEA クラウドポータルとの接続に使用されるサービス VPN と、(b) ここで設定する各サービス VPN 間の接続を提供するようにルートリークを設定します。</p> |
| Asset Interface    | <p>(SD-Routing ソリューションで使用する SEA 機能を設定するときに、このフィールドが表示されます。)</p> <p>デバイスがアセットネットワークに接続するために使用している物理インターフェイス。</p>                                                                                                                          |

| フィールド                | 説明                                                                                                             |
|----------------------|----------------------------------------------------------------------------------------------------------------|
| VPG IP Address       | ルータの VPG インターフェイスに割り当てる IP アドレス。                                                                               |
| SEA Agent IP Address | ルータのそれぞれの VPG インターフェイスにマッピングするために、SEA アセットエージェントに割り当てる IP アドレス。このアドレスは、アセットの VPG インターフェイスと同じネットワーク内にある必要があります。 |
| Subnet Mask          | VPG サブネットマスク。                                                                                                  |
| Action               | 削除オプションを使用するとテーブルの行が削除され、アセットネットワークの設定が削除されます。                                                                 |

4. Cisco SEA ポータルのドメイン名を解決できるネットワーク内の DNS サーバーを設定します。

表 13: ネームサーバー

| フィールド           | 説明                                                                                                                                                                                                                                                                       |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add Name Server | <p>Cisco SEA ポータルのドメイン名を解決できるネットワーク内の DNS サーバーを設定します。[Add Name Server] をクリックすると、ネームサーバーが追加されます。</p> <p>Cisco SEA ポータルのドメイン名については、「<a href="#">Network ports and protocols</a>」[英語] を参照してください。</p> <p>これは必須フィールドです。ネームサーバーを設定しないと、設定を保存できません。</p> <p>ネームサーバー名の最大数 : 5</p> |
| Name Server     | ドメインネームサーバーの IP アドレス。                                                                                                                                                                                                                                                    |
| Action          | 削除オプションを使用するとテーブルの行が削除され、ネームサーバーが削除されます。                                                                                                                                                                                                                                 |

## 次のタスク

「[Deploy a configuration group](#)」[英語] も参照してください。

## 設定グループへの Cisco SEA 機能の追加

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。

**ステップ 2** [solution] ドロップダウンリストで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択し、このソリューションの設定グループのみを表示します。

**ステップ 3** [Configuration Groups] タブをクリックします。

**ステップ 4** 設定グループを作成する必要がある場合は、『Cisco Catalyst SD-WAN Configuration Groups』の「[Using Configuration Groups](#)」[英語] で説明されている手順に従います。

**ステップ 5** 既存の設定グループの場合は、[Add Profile] をクリックして、設定グループに [Other Profile] を追加します。

**ステップ 6** 設定グループで [Other Profile] ドロップダウンリストを見つけて、Cisco SEA プロファイルを選択します。

## Cisco SEA 機能を追加した設定グループの展開

### 始める前に

- Cisco SEA 機能を追加した設定グループを展開する前に、[Cisco Secure Equipment Access との統合でサポートされるプラットフォーム（25 ページ）](#) を参照してください。
- Cisco SEA 機能を追加した設定グループを展開する前に、Cisco SEA エージェントを実行するデバイスごとに、デバイスが Cisco SEA クラウドポータルにネットワーク経由で到達できることを確認してください。これには次の 2 つの手順が必要です。

1. 設定グループを展開して、CiscoSEA クラウドポータルへの到達可能性を確立します。
2. 設定グループを展開して、デバイスで Cisco SEA を有効にします。

前の手順で到達可能性を確立したら、その手順でを使用したものと同じ設定グループを変更して Cisco SEA 機能を追加し、その設定グループをデバイスに展開できます。

[Cisco Secure Equipment Access との統合の前提条件（26 ページ）](#) を参照してください。



- (注) Cisco SEA 機能が組み込まれており、すでにデバイスに展開済みの設定グループにデバイスを追加する場合にも、これと同じ要件が適用されます。設定グループを追加のデバイスに展開する場合は、上記の点に注意して、まず追加のデバイスで Cisco SEA クラウドポータルへの到達可能性を確立します。

## 手順

**ステップ 1** 『Cisco Catalyst SD-WAN Configuration Groups』の「[standard configuration group deployment procedure](#)」[英語]に従って、ネットワーク内のデバイスに設定グループを展開します。

**ステップ 2** SD-WAN ソリューションタイプのデバイスに展開する場合は、展開時にルータごとにデバイス固有の変数を必要に応じて入力します。

SD-Routing ソリューションタイプのデバイスに展開する場合は、この手順をスキップしてください。

**ステップ 3** デバイスに Cisco SEA アプリケーションをインストールする際に進行状況をモニターするには、インストールのログメッセージを表示します。

1. 右上近くにあるタスクリストボタンをクリックします。

2. [Deploy configuration group] タスクをクリックします。

この操作により、各デバイスに関する展開の進行状況を示すページが開きます。

3. デバイスの横にある [Action] 列のログアイコンをクリックします。

[View Logs] ペインが開き、そのデバイスに関する展開の進行状況が表示されます。展開が完了し、デバイスと Cisco SEA クラウドポータルとの接続が確立されると、「Config Group successfully deployed to device,」といった成功メッセージがログに表示されます。

Cisco SEA 機能を追加した設定グループをはじめてデバイスに展開すると、デバイスで Cisco SEA アプリケーションのインストールがトリガーされます。デバイスで Cisco SEA アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco SEA ソリューションの一部として動作します。

# Cisco SD-WAN Manager が Cisco Secure Equipment Access クラウドポータルに接続していることを確認する

Cisco SEA 機能を追加した設定グループを作成した場合、その設定グループをデバイスに展開すると、デバイスで Cisco SEA アプリケーションのインストールがトリガーされます。デバイ

スで Cisco SEA アプリケーションのインストールが完了するまで数分かかります。インストールが正常に完了すると、デバイスは Cisco SEA ソリューションの一部として動作します。

#### 始める前に

Cisco SEA 機能を追加した設定グループを 1 つ以上のデバイスに展開します。[Cisco SEA 機能を追加した設定グループの展開 \(33 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** Cisco SEA クラウドポータルにログインします。

**ステップ 2** デバイスリストを表示します。詳細については、Cisco DevNet サイトの [Cisco Secure Equipment Access のマニュアル](#) [英語] を参照してください。

## CLI を使用して Cisco Secure Equipment Access アプリケーションがデバイスで動作していることを確認する

この検証方法は、SD-WAN または SD-Routing ソリューションのデバイスに適用できます。

#### 始める前に

Cisco Secure Equipment Access 機能を追加した設定グループを 1 つ以上のデバイスに展開します。[Cisco SEA 機能を追加した設定グループの展開 \(33 ページ\)](#) を参照してください。

#### 手順

**ステップ 1** Cisco Secure Equipment Access アプリケーションを実行しているデバイスで、次のコマンドを実行します。

```
Device# show iox-service
```

**ステップ 2** 前のステップのコマンドの出力に基づいて、次のいずれかを実行します。

- コマンド出力に IOxman サービスが実行中であることが示されている場合は、次の手順に進みます。
- コマンド出力に IOxman サービスが実行中でないが表示される場合は、Cisco Secure Equipment Access アプリケーションが正しく動作していないことを示します。アプリケーションを再インストールします。[Cisco SEA 機能を追加した設定グループの展開 \(33 ページ\)](#) を参照してください。

**ステップ 3** 同じデバイスで、次のコマンドを実行します。実行中の状態であるとコマンド出力に表示される場合は、Cisco Secure Equipment Access アプリケーションが正しく動作していることを示します。

```
Device# show app-hosting detail appid sea
```

### 例

この例では、Cisco Secure Equipment Access アプリケーションがインストールされ、動作しています。ここではコマンド出力が省略されることに注意してください。

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)           : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)   : Running
Libvirt 5.5.0              : Running
Dockerd v19.03.13-ce       : Running

Device# show app-hosting detail appid sea
App id          : sea
Owner           : iox
State           : RUNNING
...
```

## デバイス上の Cisco Secure Equipment Access アプリケーションのモニター

### 始める前に

Cisco Secure Equipment Access 機能を追加した設定グループを 1 つ以上のデバイスに展開します。[Cisco SEA 機能を追加した設定グループの展開 \(33 ページ\)](#) を参照してください。

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。

**ステップ 2** SD-WAN ソリューションの対象デバイス名をクリックします。

#### (注)

このモニタリング方法は、SD-WAN ソリューションのデバイスには適用できますが、SD-Routing ソリューションのデバイスには適用できません。

**ステップ 3** **[Real Time]** タブをクリックします。

**ステップ 4** **[DeviceOptions]** フィールドに次のいずれかのアプリケーションホスティングコマンドを入力して、デバイスで実行されている Cisco Secure Equipment Access アプリケーションのリソース使用状況やその他の詳細を表示します。

- アプリケーション ホスティングの詳細

- アプリケーション ホスティングの稼働率
  - アプリケーション ホスティング ネットワークの稼働率
  - アプリケーション ホスティング ストレージの使用率
  - アプリケーション ホスティング プロセス
  - アプリケーション ホスティングでアタッチされるデバイス
  - アプリケーション ホスティング ネットワーク インターフェイス
  - アプリケーション ホスティング ゲスト ルート
-





## 第 5 章

# サードパーティのカスタムアプリケーションと Cisco Catalyst SD-WAN の統合

---

- サードパーティのカスタムアプリケーションと Cisco Catalyst SD-WAN の統合 (40 ページ)
- Cisco Catalyst SD-WAN とサードパーティのカスタムアプリケーションの統合に関する情報 (40 ページ)
- サードパーティのカスタムアプリケーションとの統合でサポートされるプラットフォーム (41 ページ)
- サードパーティのカスタムアプリケーションとの統合における前提条件 (41 ページ)
- サードパーティのカスタムアプリケーションとの統合に関するガイドライン (42 ページ)
- サードパーティのカスタムアプリケーションとの統合に関する制約事項 (42 ページ)
- サードパーティのカスタムアプリケーションとの統合の設定 (概要) (42 ページ)
- CLI を使用してサードパーティのカスタムアプリケーションがデバイスで動作していることを確認する (47 ページ)
- デバイスでサードパーティのカスタムアプリケーションをモニターする (49 ページ)
- サードパーティのカスタムアプリケーションのアンインストール (50 ページ)

# サードパーティのカスタムアプリケーションと Cisco Catalyst SD-WAN の統合

表 14: 機能の履歴

| 機能名                      | リリース情報                                                                                   | 機能説明                                                                                                                                                |
|--------------------------|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| サードパーティのカスタムアプリケーションとの統合 | Cisco IOS XE Catalyst SD-WAN リリース 17.16.1a<br>Cisco Catalyst SD-WAN Manager リリース 20.16.1 | Cisco SD-WAN Manager では、サードパーティが開発した Cisco IOx アプリケーションとの統合がサポートされています。こうしたカスタムアプリケーションによって、Cisco IOS XE Catalyst SD-WAN ソフトウェアを実行するデバイスに機能が追加されます。 |

## Cisco Catalyst SD-WAN とサードパーティのカスタムアプリケーションの統合に関する情報

Cisco SD-WAN Manager では、サードパーティが開発した Cisco IOx アプリケーションとの統合がサポートされています。これらはカスタムアプリケーションと呼ばれ、Cisco IOS XE Catalyst SD-WAN ソフトウェアを実行するデバイスに機能を追加します。

### 接続

Cisco IOx アプリケーションは、Docker コンテナ内のデバイスで動作します。このアプリケーションには、次のような他のデータソースやコンポーネントへの接続設定が組み込まれている場合と、組み込まれていない場合があります。

- デバイスのシリアルポート

[カスタムアプリケーションを追加した設定グループプロファイルの作成 \(43 ページ\)](#) に記載されているシリアルポートの設定を参照してください。

- アプリケーションサーバー

[カスタムアプリケーションを追加した設定グループプロファイルの作成 \(43 ページ\)](#) に記載されているネットワークの設定パラメーターを参照してください。

### 仮想ポート グループ インターフェイス

サードパーティが開発したカスタムアプリケーションにネットワーク要件がある場合、Cisco SD-WAN Manager では可用性に基づいて、11 ~ 22 の範囲で仮想ポートグループ (VPG) インターフェイスが使用されます。特定の VPG インターフェイスを予約する必要はありません。

# サードパーティのカスタムアプリケーションとの統合でサポートされるプラットフォーム

表 15: サポートされるプラットフォーム

| プラットフォーム シリーズ                          | モデル                                                                                              | サポート対象の最低バージョン                                                                                       |
|----------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Cisco Catalyst IR1100 高耐久性<br>シリーズ ルータ | Cisco Catalyst IR1101                                                                            | Cisco IOS XE Catalyst SD-WAN<br>リリース 17.16.1a<br><br>Cisco Catalyst SD-WAN 制御コ<br>ンポーネントリリース 20.16.1 |
| Cisco Catalyst IR1800 高耐久性<br>シリーズ ルータ | Cisco Catalyst IR1821<br>Cisco Catalyst IR1831<br>Cisco Catalyst IR1833<br>Cisco Catalyst IR1835 | Cisco IOS XE Catalyst SD-WAN<br>リリース 17.16.1a<br><br>Cisco Catalyst SD-WAN 制御コ<br>ンポーネントリリース 20.16.1 |

## サードパーティのカスタムアプリケーションとの統合における前提条件

### リソース要件

サードパーティが開発したカスタムアプリケーションで必要とされる CPU、メモリ、ストレージリソースが各デバイスに備わっていることを確認します。リソース要件は、カスタムアプリケーションの詳細によって全く異なります。

### デバイスでの Cisco IOx のアクティブ化

サードパーティのカスタムアプリケーションをインストールする前に、デバイスで Cisco IOx をアクティブ化します。[デバイスでの Cisco IOx のアクティブ化 \(43 ページ\)](#) を参照してください。

# サードパーティのカスタムアプリケーションとの統合に関するガイドライン

## サードパーティのカスタムアプリケーションとの統合に関する制約事項

### アップグレードの制限事項

Cisco SD-WAN Manager は、カスタムアプリケーションのアップグレードをサポートしていません。新しいバージョンにアップグレードするには、現在のバージョンをアンインストールしてから、新しいバージョンのアプリケーションをインストールします。[サードパーティのカスタムアプリケーションのアンインストール \(50 ページ\)](#) を参照してください。

### アプリケーションの再起動

Cisco SD-WAN Manager では、サードパーティが開発したカスタムアプリケーションを再起動できません。

## サードパーティのカスタムアプリケーションとの統合の設定（概要）

### 手順

---

ステップ 1 [デバイスでの Cisco IOx のアクティブ化 \(43 ページ\)](#)

ステップ 2 [カスタムアプリケーションを追加した設定グループプロファイルの作成 \(43 ページ\)](#)

ステップ 3 [設定グループへのカスタムアプリケーション機能の追加 \(46 ページ\)](#)

ステップ 4 [カスタムアプリケーション機能を追加した設定グループの展開 \(47 ページ\)](#)

---

### 次のタスク

設定手順が完了すると、デバイスで実行されているアプリケーションのアクティビティをモニターできます。[デバイスでサードパーティのカスタムアプリケーションをモニターする \(49 ページ\)](#) を参照してください。

## デバイスでの Cisco IOx のアクティブ化

この手順を実行すると、サードパーティのカスタム Cisco IOx アプリケーションを実行するために必要なデバイスで Cisco IOx がアクティブ化されます。

### 手順

---

**ステップ 1** CLI アドオンプロファイルを使用して設定グループを作成します。

**ステップ 2** CLI アドオンプロファイルに **iox** コマンドを含めて、Cisco IOx をアクティブ化します。

```
iox
```

**ステップ 3** 『Cisco Catalyst SD-WAN Configuration Groups』の「[standard configuration group deployment procedure](#)」[英語]に従って、サードパーティのカスタム Cisco IOx アプリケーションをインストールする前に、デバイスに設定グループを展開します。

---

## カスタムアプリケーションを追加した設定グループプロファイルの作成

サードパーティが開発するのは独自のカスタムアプリケーションであるため、Cisco SD-WAN Manager は共通の標準規格と照らし合わせて設定を検証できません。アプリケーションが正常に動作するように、アプリケーションの要件に従ってここでパラメータを設定してください。

### 始める前に

[Configuration] > [Configuration Groups] ページで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択します。

### 手順

---

**ステップ 1** Cisco SD-WAN Manager のメニューから、[Configuration] > [Configuration Groups] を選択します。

**ステップ 2** その他のプロファイルで [カスタムアプリケーション](#) 機能を作成して設定します。

1. この機能の名前と説明を入力します。

表 16: 名前と説明

| フィールド       | 説明           |
|-------------|--------------|
| Name        | 機能の名前。       |
| Description | 任意で説明を追加します。 |

## 2. 基本設定は必須です。

表 17: 基本設定

| フィールド            | 説明                                                                                                                                                                             |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Name | カスタムアプリケーションの名前を入力します。大文字または小文字を使用できますが、スペースや特殊文字は使用できません。<br><br>この名前は、 <b>[Monitor] &gt; [Logs] &gt; [Events]</b> ページでイベント詳細の一部として表示されます。                                    |
| Virtual Image    | ドロップダウンリストからカスタムアプリケーションのイメージファイルを選択します。<br><br>このリストには、 <b>[Maintenance] &gt; [Software Repository] &gt; [Virtual Images]</b> で仮想イメージのリポジトリにアップロードしたカスタムアプリケーションのイメージが表示されます。 |

3. カスタムアプリケーションにネットワーク設定の要件がある場合は、**[Add Configuration]** をクリックして、ネットワーク接続の詳細を最大 3 つ入力します。アプリケーションがサーバーと通信する場合、これにより Cisco IOx アプリケーションと

- アプリケーションが動作しているデバイスや
- サーバーなどの任意の外部アセット間の通信が設定されます。

SD-WAN ソリューションのオプションは次のとおりです。

表 18: ネットワークの設定、SD-WAN ソリューション

| フィールド          | 説明                                                                                                                  |
|----------------|---------------------------------------------------------------------------------------------------------------------|
| Name           | 接続を設定するエンティティを説明する名前。                                                                                               |
| Service VPN    | アプリケーションと (a) デバイスまたは (b) 外部アセット間を接続するサービス VPN。                                                                     |
| VPG IP Address | カスタムアプリケーションとデバイスの仮想ポートグループ (VPG) インターフェイスまたは外部アセット間の通信用に、 <b>[Subnet Mask]</b> フィールドで定義したサブネットマスク内の IP アドレスを入力します。 |

| フィールド                  | 説明                                                                                                    |
|------------------------|-------------------------------------------------------------------------------------------------------|
| Application IP Address | デバイスの VPG インターフェイスにマッピングするために、カスタムアプリケーションに割り当てる IP アドレス。                                             |
| Subnet Mask            | VPG インターフェイスのサブネットマスク。サブネットマスクは、カスタムアプリケーションとデバイス VPG インターフェイスまたは外部アセット間の通信用に、サービス VPN のアドレス空間を定義します。 |
| Action                 | 行の削除オプションを指定します。                                                                                      |

SD-Routing ソリューションのオプションは次のとおりです。

表 19: ネットワークの設定、SD-Routing ソリューション

| フィールド                        | 説明                                                     |
|------------------------------|--------------------------------------------------------|
| <b>Network Configuration</b> |                                                        |
| Name                         | 接続を設定するエンティティを説明する名前。                                  |
| Communication Interface      | アプリケーションと (a) デバイスまたは (b) 外部アセット間を接続する物理または仮想インターフェイス。 |
| Action                       | 行の削除オプションを指定します。                                       |

- 一部のカスタムアプリケーションでは、情報をグローバル変数またはデバイス固有の変数として渡す必要があります。変数を追加するには、[Add Variable] をクリックして詳細を入力します。

キーと値の有効なペアは、カスタムアプリケーションの仕様に完全に依存します。変数の設定については、カスタムアプリケーションのデベロッパーにお問い合わせください。これらの値では大文字と小文字が区別されます。

変数の最大数：10

表 20: 環境変数

| フィールド  | 説明                                                |
|--------|---------------------------------------------------|
| Key    | 変数のキー名。                                           |
| Value  | 変数の値各デバイスに固有のキー値を指定するには、[Device Specific] を選択します。 |
| Action | 行の削除オプションを指定します。                                  |

- 一部のカスタムアプリケーションでは、シリアルインターフェイスを介して提供されるデータ入力を使用されます。このオプションは、プラットフォームで使用可能な任意のシリアルポートをサポートします。

データソースを追加するには、[Add Data Source] をクリックし、シリアルポートを入力します。

シリアルポートの最大数：7

表 21: データ設定

| フィールド       | 説明                                                                                       |
|-------------|------------------------------------------------------------------------------------------|
| Serial Line | デバイスで使用可能なシリアルポートを入力します。シリアルポートの詳細については、プラットフォームのマニュアルを参照してください。<br><br>例：/dev/ttySerial |
| Action      | 行の削除オプションを指定します。                                                                         |

### 次のタスク

「[Deploy a configuration group](#)」[英語] も参照してください。

## 設定グループへのカスタムアプリケーション機能の追加

### 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。

**ステップ 2** [solution] ドロップダウンリストで、

- [SD-WAN] または
- [SD-Routing]

をソリューションタイプとして選択し、このソリューションの設定グループのみを表示します。

**ステップ 3** [Configuration Groups] タブをクリックします。

**ステップ 4** 設定グループを作成する必要がある場合は、『Cisco Catalyst SD-WAN Configuration Groups』の「[Using Configuration Groups](#)」[英語] で説明されている手順に従います。

**ステップ 5** 既存の設定グループの場合は、[Add Profile] をクリックして、設定グループに [Other Profile] を追加します。

**ステップ 6** 設定グループで [Other Profile] ドロップダウンリストを見つけて、カスタム アプリケーション プロファイルを選択します。

## カスタムアプリケーション機能を追加した設定グループの展開

### 始める前に

カスタムアプリケーション機能を追加した設定グループを展開する前に、[サードパーティのカスタムアプリケーションとの統合でサポートされるプラットフォーム（41 ページ）](#)を参照してください。

設定グループを展開する前に、デバイスで Cisco IOx をアクティブ化します。[デバイスでの Cisco IOx のアクティブ化（43 ページ）](#)を参照してください。

### 手順

**ステップ 1** 『Cisco Catalyst SD-WAN Configuration Groups』の「[standard configuration group deployment procedure](#)」[英語]に従って、ネットワーク内のデバイスに設定グループを展開します。

**ステップ 2** SD-WAN ソリューションタイプのデバイスに展開する場合は、展開時にルータごとに該当するデバイス固有の変数を入力します。

**ステップ 3** デバイスにアプリケーションをインストールする際に進行状況をモニターするには、インストールのログメッセージを表示します。

1. 右上近くにあるタスクリストボタンをクリックします。

2. [Deploy configuration group] タスクをクリックします。

この操作により、各デバイスに関する展開の進行状況を示すページが開きます。

3. デバイスの横にある [Action] 列のログアイコンをクリックします。

[View Logs] ペインが開き、そのデバイスに関する展開の進行状況が表示されます。展開が完了すると、「Config Group successfully deployed to device,」といった成功メッセージがログに表示されます。

カスタムアプリケーション機能を追加した設定グループをはじめてデバイスに展開すると、デバイスでアプリケーションのインストールがトリガーされます。

## CLI を使用してサードパーティのカスタムアプリケーションがデバイスで動作していることを確認する

この検証方法は、SD-WAN または SD-Routing ソリューションのデバイスに適用できます。

## 始める前に

カスタムアプリケーション機能を追加した設定グループを1つ以上のデバイスに展開します。  
[カスタムアプリケーション機能を追加した設定グループの展開 \(47 ページ\)](#) を参照してください。

## 手順

**ステップ 1** Cisco IOx アプリケーションを実行しているデバイスで、次のコマンドを実行します。

```
Device# show iox-service
```

**ステップ 2** 前のステップのコマンドの出力に基づいて、次のいずれかを実行します。

- コマンド出力に IOxman サービスが実行中であることが示されている場合は、次の手順に進みます。
- コマンド出力に IOxman サービスが実行中でないが表示される場合は、Cisco IOx アプリケーションが正しく動作していないことを示します。アプリケーションを再インストールします。[カスタムアプリケーション機能を追加した設定グループの展開 \(47 ページ\)](#) を参照してください。

**ステップ 3** 同じデバイスで、次のコマンドを実行します。確認しているアプリケーションが実行中の状態がであると出力に表示される場合は、そのアプリケーションが正常に動作していることを示します。

```
Device# show app-hosting detail appid application-id
```

## 例

カスタムアプリケーション機能に入力するアプリケーション名によって、コマンド出力に表示されるアプリケーションIDが決まります。[カスタムアプリケーションを追加した設定グループプロファイルの作成 \(43 ページ\)](#) を参照してください。この例では、アプリケーション ID は abc です。

ここではコマンド出力が省略されます。

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)           : Running
IOx service (HA)           : Not Supported
IOx service (IOxman)       : Running
IOx service (Sec storage)   : Running
Libvirt 5.5.0              : Running
Dockerd v19.03.13-ce      : Running
```

```
Device# show app-hosting detail appid abc
App id           : abc
Owner            : iox
State            : RUNNING
...
```

# デバイスでサードパーティのカスタムアプリケーションをモニターする

## 始める前に

カスタムアプリケーション機能を追加した設定グループを1つ以上のデバイスに展開します。[カスタムアプリケーション機能を追加した設定グループの展開 \(47 ページ\)](#) を参照してください。

## 手順

**ステップ 1** Cisco SD-WAN Manager のメニューから **[Monitor] > [Devices]** の順に選択します。

**ステップ 2** SD-WAN ソリューションの対象デバイス名をクリックします。

(注)

このモニタリング方法は、SD-WAN ソリューションのデバイスには適用できますが、SD-Routing ソリューションのデバイスには適用できません。

**ステップ 3** **[Real Time]** タブをクリックします。

**ステップ 4** **[Device Options]** フィールドに次のいずれかのアプリケーションホスティングコマンドを入力して、デバイスで実行されているアプリケーション（サードパーティが開発したカスタムアプリケーションなど）のリソース使用状況やその他の詳細を表示します。

- アプリケーション ホスティングの詳細
- アプリケーション ホスティングの稼働率
- アプリケーション ホスティング ネットワークの稼働率
- アプリケーション ホスティング ストレージの使用率
- アプリケーション ホスティング プロセス
- アプリケーション ホスティングでアタッチされるデバイス
- アプリケーション ホスティング ネットワーク インターフェイス
- アプリケーション ホスティング ゲスト ルート

# サードパーティのカスタムアプリケーションのアンインストール

サードパーティが開発したカスタムアプリケーションのアンインストールは、そのアプリケーションがインストールされていることが前提になります。[サードパーティのカスタムアプリケーションとの統合の設定（概要）（42 ページ）](#) を参照してください。

## 手順

**ステップ 1** 設定グループからカスタムアプリケーション機能を削除します。

- a) Cisco SD-WAN Manager のメニューから、**[Configuration] > [Configuration Groups]** を選択します。
- b) **[Configuration Groups]** タブをクリックします。
- c) 設定グループの横にある **[Actions]** 列の矢印をクリックして行を展開し、アタッチされているプロファイルを表示します。
- d) **[Other Profile]** ドロップダウンリストの横にある鉛筆アイコンをクリックして、プロファイルを編集します。
- e) プロファイル内で、カスタムアプリケーション機能を削除します。

**ステップ 2** 設定グループをデバイスに展開します。[カスタムアプリケーション機能を追加した設定グループの展開（47 ページ）](#) を参照してください。

この手順を実行すると、展開されたデバイスからカスタムアプリケーションがアンインストールされます。

## 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。