

# Cisco Threat Response(CTR)とESAの統合

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ 1 : \[Network\] > \[Cloud Service Settings\]に移動します](#)

[ステップ2:\[Edit Settings\]をクリックします](#)

[ステップ3:\[Enable\]チェックボックスと\[Threat Response Server\]チェックボックスをオンにします](#)

[ステップ4 : 変更を送信して確定する](#)

[ステップ5:CTRポータルにログインし、ESAで要求される登録トークンを生成します](#)

[ステップ6 : 登録トークン \( CTRポータルから生成 \) をESAに貼り付けます](#)

[ステップ7:ESAデバイスがSSEポータルにあることを確認します](#)

[ステップ8:CTRポータルに移動し、新しいESAモジュールを追加します](#)

[確認](#)

[トラブルシューティング](#)

[ESAデバイスがCTRポータルに表示されない](#)

[CTR調査でESAからのデータが表示されない](#)

[ESAが登録トークンを要求していない](#)

[無効または期限切れのトークンが原因で登録に失敗しました](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Threat Response(CTR)をEメールセキュリティアプライアンス(ESA)と統合するプロセスと、CTR調査を実行するためにこれを検証する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Threat Response
- Eメールセキュリティアプライアンス

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CTRアカウント
- Cisco Security Services Exchange
- ソフトウェアバージョン13.0.0-392上のESA C100V

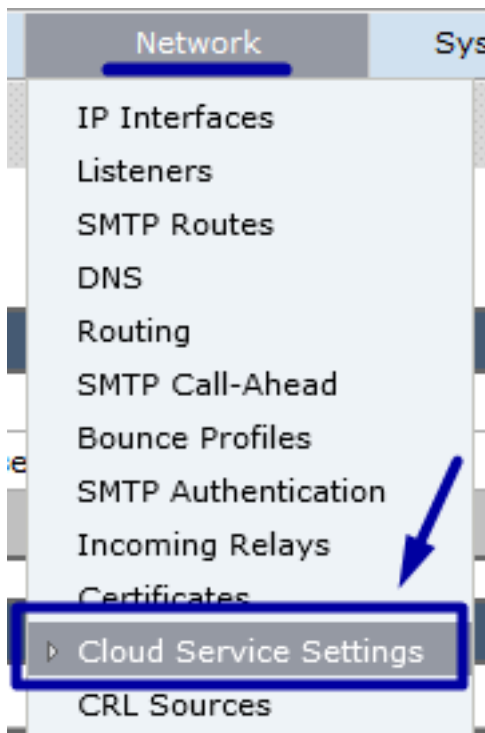
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

統合CTRとESAを設定するには、Eメールセキュリティ仮想アプライアンス(ESA)にログインし、次の手順に従います。

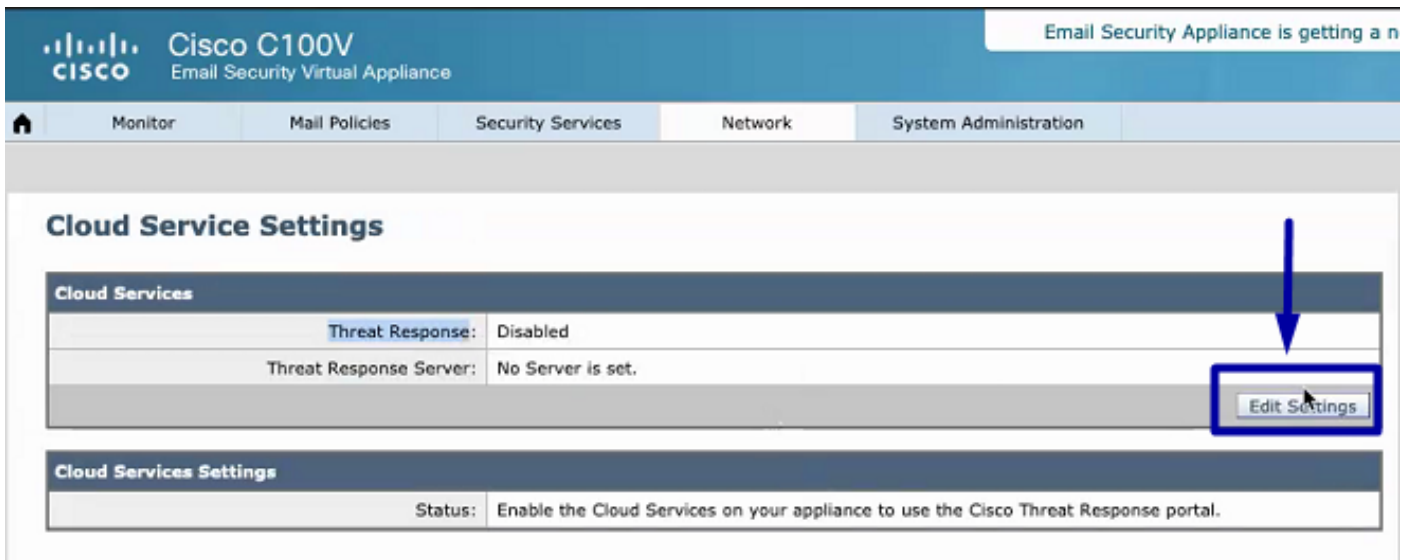
### ステップ 1： [Network] > [Cloud Service Settings]に移動します

ESAで、コンテキストメニュー[Network] > [Cloud Service Settings]に移動し、図に示すように現在の[Threat Response Status (Disabled / Enabled)]を表示します。



### ステップ2:[Edit Settings]をクリックします

ESAの脅威応答機能が無効になるまで、この機能を有効にするには、図に示すように[Edit Settings]をクリックします。



### ステップ3:[Enable]チェックボックスと[Threat Response Server]チェックボックスをオンにします

[Enable]チェックボックスをオンにしてから、[Threat Response Server]を選択します。次の図を参照してください。

#### Cloud Service Settings

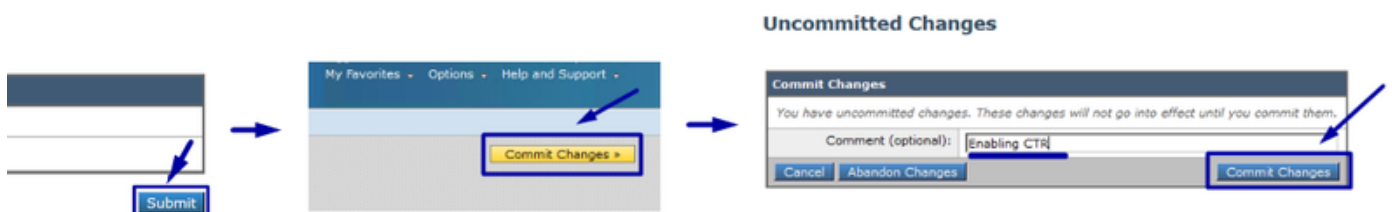


注：Threat Response Server (THREAT) URL のデフォルト選択は AMERICAS (api-sse.cisco.com) です。ヨーロッパの企業では、ドロップダウンメニューをクリックして [EUROPE (api.eu.sse.itd.cisco.com)] を選択します

### ステップ4：変更を送信して確定する

変更を保存して適用するには、変更を送信して確定する必要があります。次の図に示すように、ESA インターフェイスが更新されると、統合を登録するために登録トークンが要求されます。

注：成功メッセージが表示されます。変更がコミットされました。



## Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

## Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

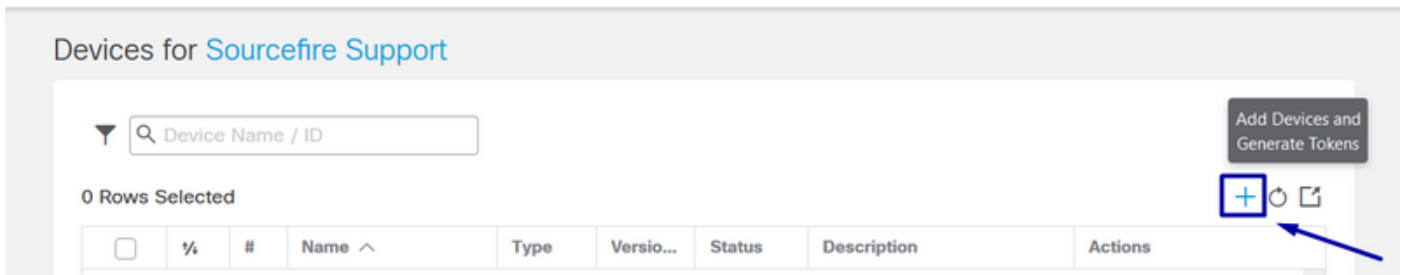
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
<a href="#">Register</a>	

ステップ5:CTRポータルにログインし、ESAで要求される登録トークンを生成します

1.- CTRポータルで、[Modules ( モジュール ) ] > [Devices ( デバイス ) ] > [Manage Devices ( デバイスの管理 ) ]に移動し、次の図を参照してください。

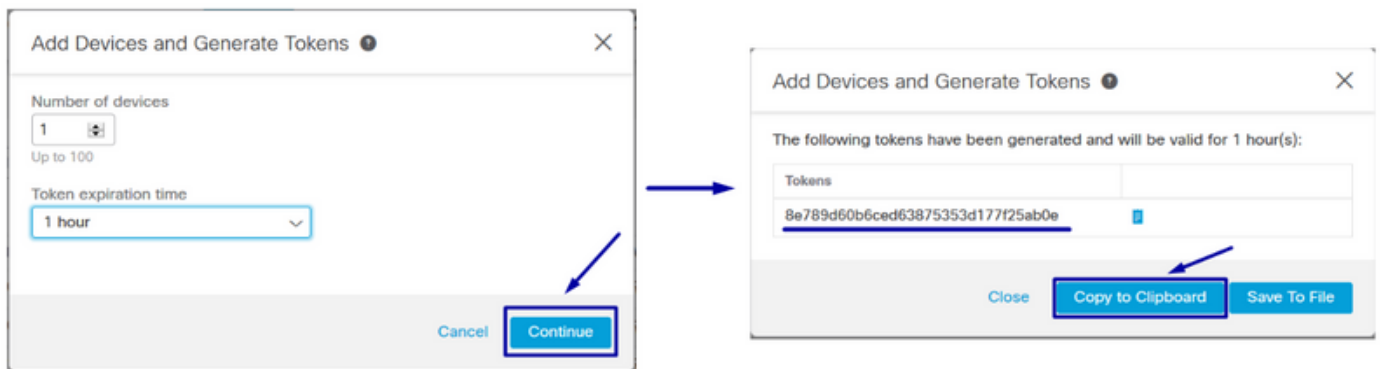
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation, the breadcrumb 'Settings > Devices' is shown. The 'Devices' section contains a 'Manage Devices' button (highlighted with a blue box and arrow) and a 'Reload Devices' button. A sidebar on the left shows a menu with 'Settings', 'Your Account', 'Devices' (highlighted with a blue box and arrow), 'API Clients', and '> Modules'.

2.- [デバイスの管理(Manage Devices)]リンクをクリックすると、セキュリティサービス交換 (SSE)にリダイレクトされます。次の図に示すように、[デバイスの追加(Add Devices)]アイコンと [トークンの生成(Generate Tokens)]アイコンをクリックします。



3.- [Continue]をクリックしてトークンを生成し、トークンが生成されたら、図に示すように [Copy to Clipboard]をクリックします。

ヒント：追加するデバイスの数(1 ~ 100)を選択し、トークンの有効期限 ( 1時間、2時間、4時間、6時間、8時間、12時間、01日、02日、03日、04日、および05日 )も選択できます。



### ステップ6：登録トークン（CTRポータルから生成）をESAに貼り付けます

Registration Tokenが生成されたら、次の図のように、ESAの[Cloud Services Settings]セクションに貼り付けます。

注：成功メッセージが表示されます。Cisco Threat Responseポータルへのアプライアンスの登録要求が開始されます。しばらくしてこのページに戻り、アプライアンスのステータスを確認します。

### Cloud Service Settings



## Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

### Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

### Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

## ステップ7:ESAデバイスがSSEポータルにあることを確認します

SSEポータル([CTR] > [Modules] > [Devices] > [Manage Devices])に移動し、[Search]タブでESAデバイスを確認します ( 図を参照 )。

Security Services Exchange Audit Log Brenda Marquez

### Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registered	ESA	<a href="#">/</a> <a href="#">🗑️</a> <a href="#">🗨️</a>

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34  
Created: 2020-05-11 20:41:05 UTC

## ステップ8:CTRポータルに移動し、新しいESAモジュールを追加します

1.- CTRポータルで、図に示すように、[Modules] > [Add New Module]に移動します。

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

### Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

#### Your Configurations

[+](#)  
Add New Module

**Amp** AMP for Endpoints  
AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Edit](#) [Learn More](#)

2.- モジュールタイプを選択します。この場合、モジュールは次の図のようにEメールセキュリティアプライアンスモジュールです。

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

## Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

**Amp** AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#) [Learn More](#) · [Free Trial](#)

**Esa** Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#) [Learn More](#)

3. –フィールドを入力します。図に示すように、[Module Name]、[Registered Device] ( 以前に登録したデバイスを選択 )、[Request Timeframe (days)]、および[Save]をクリックします。

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

**Add New Email Security Appliance Module**

Module Name\*

Registered Device\*

esa03.mex-amp.inlab  
Type ESA  
ID 874141f7-903f-4be9-b14e-45a7f34a2032  
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

**Quick Start** [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it . After this is completed, you add the ESA module.

**Prerequisite:** ESA running minimum AsyncOS 13.0 0-314 (LD) release.

**Note:** Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
  - Module Name** - Leave the default name or enter a name that is meaningful to you.
  - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
  - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

確認



CTRとESAの統合を確認するには、テスト電子メールを送信します。この電子メールは、ESAからも確認できます。[Monitor] > [Message Tracking]に移動し、テスト電子メールを検索します。この場合、Eメールの件名を下の画像としてフィルタリングしました。

The screenshot shows the Cisco C100V Message Tracking interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The 'Message Tracking' section is active, displaying search criteria and results.

**Search**

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With [ ]

Envelope Recipient: ? Begins With [ ]

Subject: Begins With test test

Message Received:  Last Day  Last Week  Custom Range

Start Date: 05/13/2020 Time: 13:00 and End Date: 05/14/2020 Time: 13:42 (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

**Results** Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com  
RECIPIENT: testingBren@cisco.com  
SUBJECT: test test  
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

これで、CTRポータルから調査を実行し、[Investigate]に移動して、図に示すように電子メールの回答を使用できます。



Investigation 1 of 1 enrichments complete

email\_subject:"test test"

Investigate Clear Reset What can I search for?

Relations Graph · Filters: Show All, Expanded · Showing 6 nodes

IP

Target Email

Email Subject test test

Cisco Message ID 8

Domain cisco.com

Email Address mgmt01@cisco.c...

Sightings

My Environment Global

1 Sighting in My Environment

First Seen: May 14, 2020 13:23:57 UTC

Last Seen: May 14, 2020 13:23:57 UTC

Module enriched this investigation

esa03 ----- Email Security Appliance

1 Sighting, 0 Judgements

Observables

test test

Email Subject

My Environment Global

1 Sighting in My Environment

First Seen: May 14, 2020 13:23:57 UTC

Last Seen: May 14, 2020 13:23:57 UTC

Sightings (1)

Module	Observed	Description	Confidence	Severity	Details
esa03 -----	Email Security Appliance	9 hours ago	Incoming m essage (Del ivered)	High	Low

ヒント：他の電子メールの回答に対して、次の図と同じ構文を使用できます。

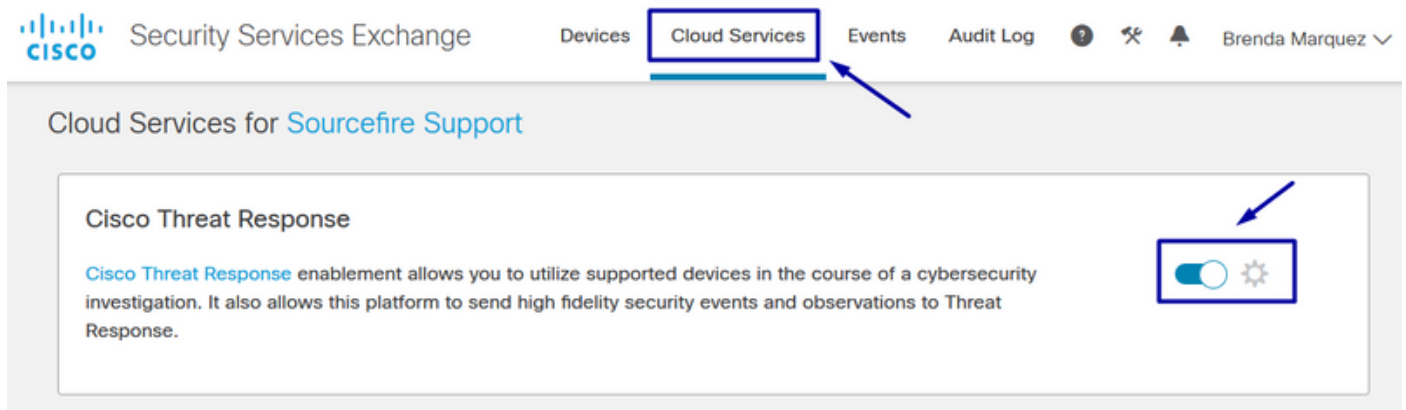
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

## トラブルシューティング

CESのお客様、またはSMAを介してESAデバイスを管理する場合は、SMAを介してのみThreat Responseに接続できます。SMAがAsyncOS 12.5以降を実行していることを確認してください。SMAでESAを管理せず、ESAを直接統合する場合は、AsyncOSバージョン13.0以降であることを確認します。

### ESAデバイスがCTRポータルに表示されない

ESAモジュールがCTRポータルに追加されている間にESAデバイスが[Registered Device]ドロップダウンに表示されない場合は、CTRがSSEで有効になっていることを確認し、CTRで[Modules] > [Devices] > [Manage Devices]に移動してCTRを有効します。



## CTR調査でESAからのデータが表示されない

次のことを確認してください。

- 調査の構文が正しく、上記の「Verify」セクションにEメールの回答が示されています。
- 適切なThreat Response Server(THREAT)またはクラウド ( 南・北・中央アメリカ/ヨーロッパ ) を選択しました。

## ESAが登録トークンを要求していない

Threat Responseが有効になっている場合は、変更を確定してください。有効になっていない場合は、変更はESAの[Threat Response]セクションに適用されません。

## 無効または期限切れのトークンが原因で登録に失敗しました

トークンが正しいクラウドから生成されていることを確認してください。

ESAにヨーロッパ(EU)クラウドを使用する場合は、次の方法でトークンを生成します。  
<https://admin.eu.sse.itd.cisco.com/>

ESAにアメリカ(NAM)クラウドを使用する場合は、次の方法でトークンを生成します。  
<https://admin.sse.itd.cisco.com/>

また、登録トークンには有効期限があります ( 統合を完了するのに最も便利な時間を選択してください ) 。

## 関連情報

- この記事の情報は、『[Cisco Threat Response and ESA Integration\(Cisco Threat Response and ESA Integration\)](#)』ビデオで確認できます。
- [テクニカル サポートとドキュメント – Cisco Systems](#)