



Cisco Secure Firewall 4200 ASA スタートアップガイド

最終更新：2025 年 10 月 22 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/>



第 1 章

はじめる前に

ASDM を使用して ASA を設定します。

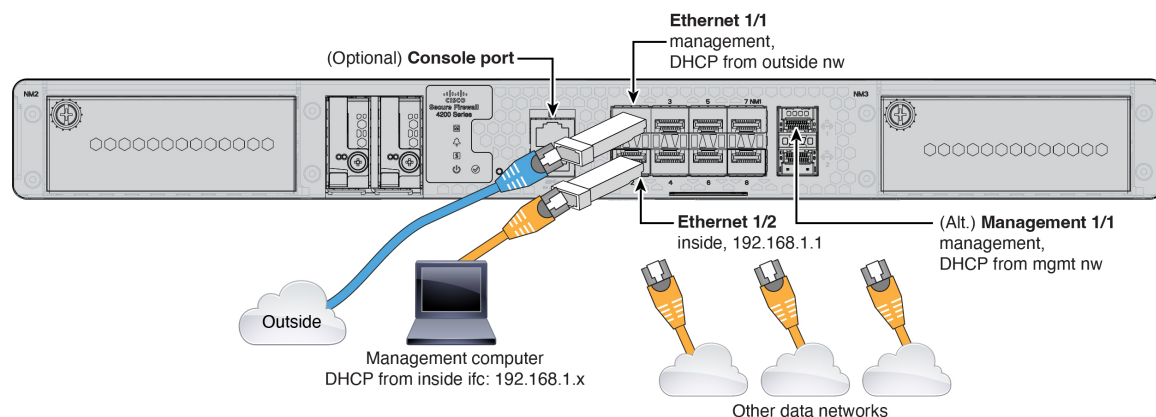


(注) Cisco Secure Firewall 4200 は、アプライアンスモードでのみ実行されます。FXOS をシャーシマネージャとして使用するプラットフォームモードはサポートされていません。アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。

- [ファイアウォールのケーブル接続 \(1 ページ\)](#)
- [ファイアウォールの電源の投入 \(2 ページ\)](#)
- [インストールされているアプリケーション \(Firewall Threat Defense または ASA\) の確認 \(3 ページ\)](#)
- [ASA CLI へのアクセス \(4 ページ\)](#)
- [ライセンスの取得 \(6 ページ\)](#)

ファイアウォールのケーブル接続

- (オプション) コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。
- データインターフェイスおよびオプションの管理ポートに SFP を取り付けます。組み込みポートは、SFP/SFP+/SFP28 モジュールを必要とする 1/10/25 Gb SFP28 ポートです。
- 詳細については、[ハードウェア設置ガイド](#)を参照してください。



ファイアウォールの電源の投入

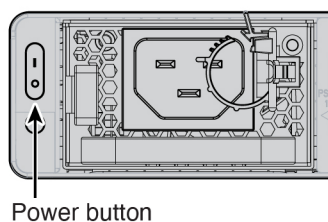
システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。ロッカー電源スイッチは、ソフト通知を提供します。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。

手順

ステップ 1 電源コードをファイアウォールに接続し、電源コンセントに接続します。

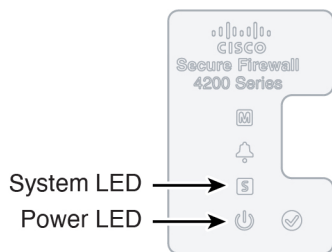
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 1: 電源ボタン



ステップ 3 LED の現在のステータスを確認します。

図 2: LED



- 電源 LED：緑色に点灯している場合は、ファイアウォールの電源がオンになっていることを意味します。
- システム（S）LED：次の動作を参照してください。

表 1: システム（S）LED の動作

LED の動作	説明	デバイスの電源を入れた後の時間（分：秒）
緑色で高速点滅	起動中	01:00
オレンジ色で高速点滅（エラー状態）	起動に失敗しました	01:00
緑色で点灯	アプリケーションがロードされました	15:00 ～ 30:00
オレンジ色で点灯（エラー状態）	アプリケーションのロードに失敗しました	15:00 ～ 30:00

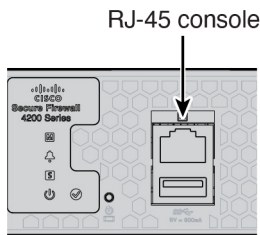
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

Firewall Threat Defense と ASA の両方のアプリケーションが、ハードウェアでサポートされています。コンソールポートに接続し、出荷時にインストールされているアプリケーションを確認します。

手順

ステップ 1 コンソールポートに接続します。

図 3: コンソール ポート



ステップ 2 CLI プロンプトを参照して、ファイアウォールで Firewall Threat Defense または ASA が実行されているかどうかを確認します。

Firewall Threat Defense

Firepower ログイン (FXOS) プロンプトが表示されます。ログインして新しいパスワードを設定せずに、切断することができます。

```
firepower login:
```

ASA

ASA プロンプトが表示されます。

```
ciscoasa>
```

ステップ 3 間違ったアプリケーションが実行されている場合は、[Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド](#)を参照してください。

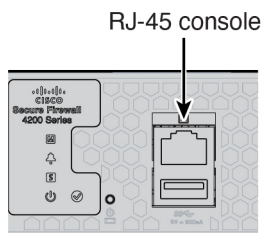
ASA CLI へのアクセス

設定またはトラブルシューティングのために CLI にアクセスする必要がある場合があります。

手順

ステップ 1 コンソールポートに接続します。

図 4: コンソールポート



ステップ 2 ユーザー実行モードで ASA CLI に接続します。このモードでは、多くの **show** コマンドを使用できます。

```
ciscoasa>
```

ステップ 3 特権 EXEC モードにアクセスします。このパスワード保護モードでは、コンフィギュレーションモードへのアクセスなどのさまざまなアクションを実行できます。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 5 FXOS CLI にアクセスします。この CLI は、ハードウェアレベルでのトラブルシューティングに使用します。

connect fxos [admin]

- **admin** : 管理者レベルのアクセスを提供します。このオプションを指定しないと、読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーションコマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー一名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

ライセンスの取得

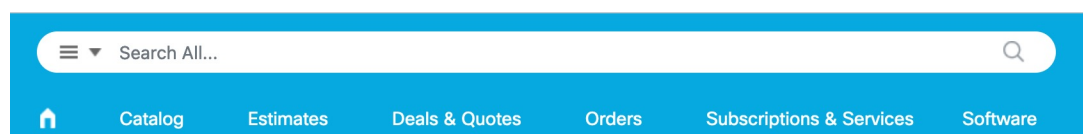
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンシングアカウントにリンクされています。[Smart Software Manager](#) にアカウントがない場合は、リンクをクリックして[新しいアカウントを設定します](#)。

Cisco ASA には次のライセンスがあります。

- Essentials：必須
- セキュリティ コンテキスト
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）
- Cisco Secure Client

1. 自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索（Search All）] フィールドを使用します。

図 5: ライセンス検索



2. 次のライセンス PID を検索します。



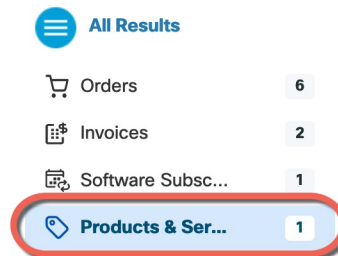
(注) PID が見つからない場合は、注文に手動で PID を追加できます。

- Essentials：自動的に含まれます。
- 5 コンテキスト：L-FPR4200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR4200-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。

- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4200-ASA-CAR=
- Cisco Secure Client：『[Cisco Secure Client Ordering Guide](#)』を参照してください。ASAでは、このライセンスを直接有効にしないでください。

3. 結果から、[製品とサービス（Products & Services）]を選択します。

図 6: 結果





第 2 章

基本ポリシーの設定

ライセンスを設定し、ASDM ウィザードを使用してデフォルト設定に追加します。

- (任意) IP アドレスの変更 (9 ページ)
- ASDM へのログイン (10 ページ)
- ライセンスの設定 (11 ページ)
- Startup Wizard による ASA の設定 (15 ページ)

(任意) IP アドレスの変更

デフォルトでは、次のインターフェイスから ASDM を起動できます。

- イーサネット 1/2 : 192.168.1.1
- 管理 1/1 : DHCP からの IP アドレス

デフォルトの IP アドレスを使用できない場合は、ASA CLI でイーサネット 1/2 インターフェイスの IP アドレスを設定できます。

手順

ステップ 1 コンソールポートに接続し、グローバルコンフィギュレーションモードにアクセスします。[ASACLI へのアクセス \(4 ページ\)](#) を参照してください。

ステップ 2 選択した IP アドレスを使用してデフォルト設定を復元します。

configure factory-default [*ip_address* [*mask*]]

例 :

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
```

```

Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

```

ステップ3 デフォルト コンフィギュレーションをフラッシュメモリに保存します。

write memory

ASDM へのログイン

ASDM を起動して、ASA を設定できるようにします。

手順

ステップ1 ブラウザに次の URL のいずれかを入力します。

- **https://192.168.1.1** : 内部 (Ethernet 1/2) インターフェイスの IP アドレス。
- **https://management_ip** : DHCP から割り当てられた管理 1/1 インターフェイスの IP アドレス。

(注)

必ず **https://** を指定してください。

[Cisco ASDM] Web ページが表示されます。ASA に証明書がインストールされていないために、ブラウザのセキュリティ警告が表示されることがありますが、これらの警告は無視して、Web ページにアクセスできます。

ステップ2 [ASDMランチャーのインストール (Install ASDM Launcher)] をクリックします。

ステップ3 画面の指示に従い、ASDM を起動します。

[Cisco ASDM-IDMランチャー (Cisco ASDM-IDM Launcher)] が表示されます。

ステップ4 ユーザー名とパスワードのフィールドを空のままにして、[OK] をクリックします。

メイン ASDM ウィンドウが表示されます。

ライセンスの設定

Smart Software Manager でファイアウォールを登録します。

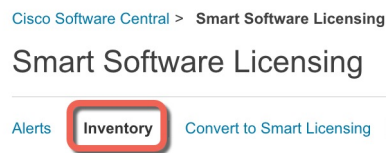
始める前に

[ライセンスの取得 \(6 ページ\)](#) に従ってファイアウォールのライセンスを取得します。

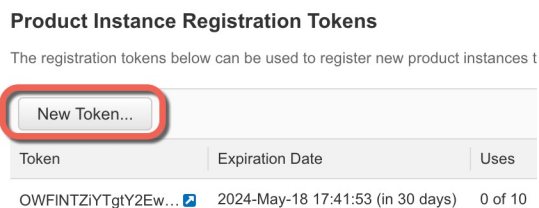
手順

ステップ 1 [Cisco Smart Software Manager](#) で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

- a) [インベントリ (Inventory)] をクリックします。



- b) [一般 (General)] タブで、[新しいトークン (New Token)] をクリックします。



- c) [登録トークンを作成 (Create Registration Token)] ダイアログボックスで、以下の設定値を入力してから [トークンを作成 (Create Token)] をクリックします。

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

☒ Allow export-controlled functionality on the products registered with this token ⓘ

• 説明

- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして[トークン（Token）]ダイアログボックスを開き、トークンIDをクリップボードにコピーできるようにします。ASAの登録が必要なおきに後の手順で使用するために、このトークンを準備しておきます。

図 7: トークンの表示

General Licenses Product Instances Event Log

Virtual Account

Description:

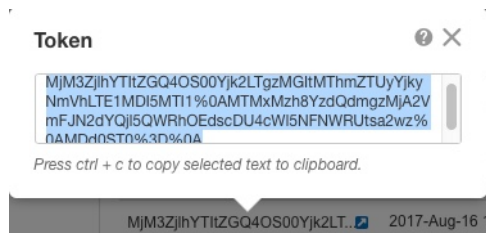
Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

Token	Expiration Date	Uses	Export-Controlled
OWFINTZIYtgY2Ew.	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

図 8: トークンのコピー



ステップ 2 ASDM で、[設定 (Configuration)] > [デバイス管理 (Device Management)] > [ライセンシング (Licensing)] > [スマートライセンシング (Smart Licensing)] の順に選択します。

ステップ 3 ライセンスと資格を設定します。

- a) [スマートライセンス設定の有効化 (Enable Smart license configuration)] をオンにします。
- b) [機能階層 (Feature Tier)] ドロップダウンリストから [Essentials] を選択します。

使用できるのは Essentials 階層だけです。

- c) (任意) [コンテキスト (Context)] ライセンスの場合、コンテキストの数を入力します。

2 コンテキストはライセンスなしで使用できます。コンテキストの最大数は、モデルによって異なります。

- Cisco Secure Firewall 1210 : 5 コンテキスト
- Cisco Secure Firewall 1220 : 10 コンテキスト

たとえば、Firepower 1220 で最大 10 のコンテキストを使用するには、コンテキストの数として 8 を入力します。この値は、デフォルトの 2 に追加されます。

- Cisco Secure Firewall 4200 : 250 コンテキスト

たとえば、Cisco Secure Firewall 4215 で最大 100 のコンテキストを使用するには、コンテキストの数として 98 を入力します。この値は、デフォルトの 2 に追加されます。

- d) (任意) Diameter、GTP/GPRS、SCTP インスペクションの [キャリアの有効化 (Enable Carrier)] をオンにします。
- e) [適用 (Apply)] をクリックします。
- f) ツールバーの [保存 (Save)] アイコンをクリックします。

ステップ 4 [登録 (Register)] をクリックします。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for Smart Licensing using Call Home, go to [Smart Call-Home](#). If you are using Smart Transport, configure

☒ Enable Smart license configuration

Feature Tier: Essentials

Context: 3

☐ Enable strong-encryption protocol

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Transport ☐ Call Home ☒ Smart Transport

Configure Transport URL

☒ Default ☐ Custom URL

Registration

Proxy URL

Proxy Port

Registration Status:

Register Renew ID Certificate Renew Authorization

Effective Running Licenses

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	512	
Inside Hosts	Unlimited	
Failover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Disabled	
Security Contexts	5	
Carrier	Disabled	
Secure Client Premium Peers	150	
Secure Client Essentials	Disabled	
Other VPN Peers	150	
Total VPN Peers	150	
Secure Client for Mobile	Enabled	
Secure Client for Cisco VPN Phone	Enabled	
Advanced Endpoint Assessment	Enabled	
Shared License	Disabled	
Total TLS Proxy Sessions	220	

Reset Apply

ステップ5 [ID トークン (ID Token)] フィールドの [Cisco Smart Software Manager](#) に登録トークンを入力します。

Smart License Registration

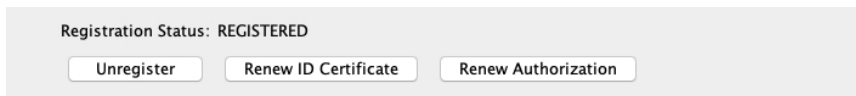
ID Token:

☐ Force registration

Help Cancel Register

ステップ6 [登録 (Register)] をクリックします。

ライセンスステータスが更新されると、ASDMによってページが更新されます。また、登録が失敗した場合などには、**[モニタリング (Monitoring)] > [プロパティ (Properties)] > [スマートライセンス (Smart License)]** の順に選択して、ライセンスステータスを確認できます。



ステップ 7 ASDM を終了し、再起動します。

ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

Startup Wizard による ASA の設定

ASDM を使用する際、基本機能および拡張機能の設定にウィザードを使用できます。Startup Wizard はデフォルト設定に基づいています。

- 内部→外部トラフィックフロー
- 内部から外部へのすべてのトラフィック用のインターフェイス PAT。

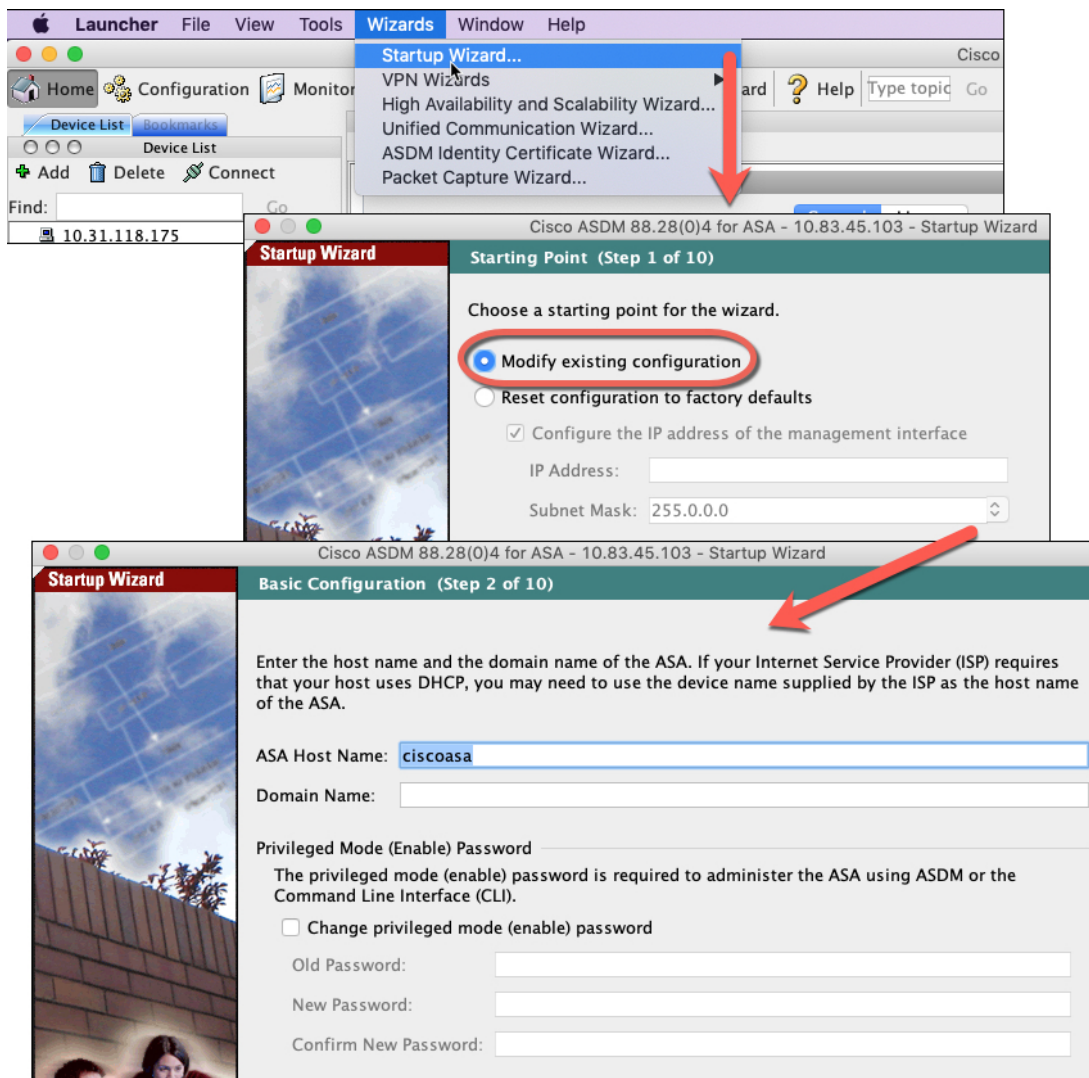
[Startup Wizard] では、手順を追って以下を設定できます。

- イネーブル パスワード
- インターフェイス（内部および外部のインターフェイス IP アドレスの設定やインターフェイスの有効化など）
- スタティック ルート
- DHCP サーバー
- その他...

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[既存の設定の変更（Modify existing configuration）] オプションボタンをクリックします。

Startup Wizard による ASA の設定



ステップ2 各ページで [次へ (Next)] をクリックして、必要な機能を設定します。

ステップ3 その他のウィザードについては、[ASDMの一般的な操作のコンフィギュレーションガイド](#)を参照してください。

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。