



はじめる前に

ミッドレンジの Cisco Secure Firewall 3100 は、進化する世界をサポートします。これにより、ハイブリッドな作業とゼロトラストが実用化され、高い投資回収率を確保する柔軟性が得られます。Cisco Secure Firewall 3100 は、脅威対策重視型セキュリティアプライアンスです。このアプライアンスは、脅威に対する優れた防御機能とビジネスの復元力を提供します。Advanced Threat 機能が有効になっている場合でも、ファイアウォールの複数のユースケースに対して優れたパフォーマンスを提供します。これらのパフォーマンス機能は、ファイアウォール、暗号化、および脅威検査機能を最適化する専用ハードウェアと組み合わせた最新の CPU アーキテクチャによって実現されています。Cisco Secure Firewall 3100 は、インターネットエッジからデータセンターおよびプライベートクラウドまで幅広いユースケースに対応します。Cisco Secure Firewall 3100 はマルチインスタンスとクラスタリングをサポートしており、組織の成長に伴うニーズに合わせて拡張できるパフォーマンスの向上を実現します。

ASDM を使用して ASA を設定します。

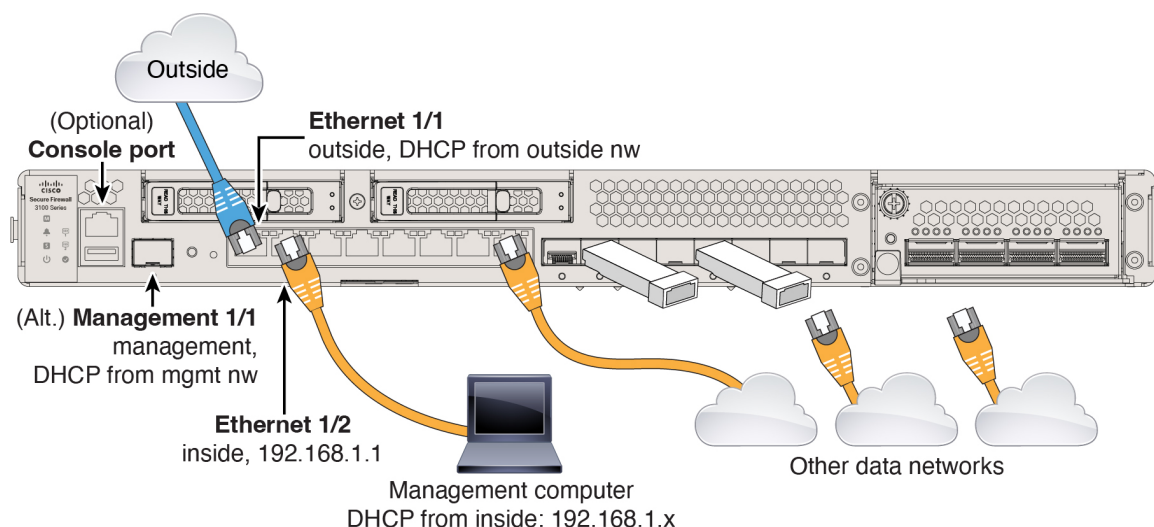


(注) Cisco Secure Firewall 3100 は、アプライアンスモードでのみ実行されます。FXOS をシャーシマネージャとして使用するプラットフォームモードはサポートされていません。アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。

- [ファイアウォールのケーブル接続 \(2 ページ\)](#)
- [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 \(4 ページ\)](#)
- [ASA CLI へのアクセス \(5 ページ\)](#)
- [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) コンソールアダプタを入手します。シャーシには DB-9 - RJ-45 シリアルケーブルが付属しているため、接続するにはサードパーティの DB-9 - USB シリアルケーブルの購入が必要になる場合があります。
- (オプション) 管理 1/1 に SFP を取り付けます。これは SFP/SFP+ モジュールを必要とする 1/10-Gbps ポートです。
- SFP をイーサネット 1/9 以上に取り付けます。これらの固定ポートは SFP/SFP+ モジュールを必要とする 1/10-Gbps 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。
- (オプション) コンソールアダプタの取得：ファイアウォールには DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するにはサードパーティの DB-9-to-USB シリアルケーブルの購入が必要になる場合があります。
- SFP/SFP+ モジュールをイーサネット 1/9 以降のポートに取り付けます。
- 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

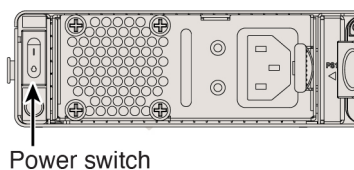
システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されます。ロッカー電源スイッチは、ソフト通知を提供します。これにより、システムのグレースフルシャットダウンがサポートされ、システムソフトウェアおよびデータの破損のリスクが軽減されます。

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。

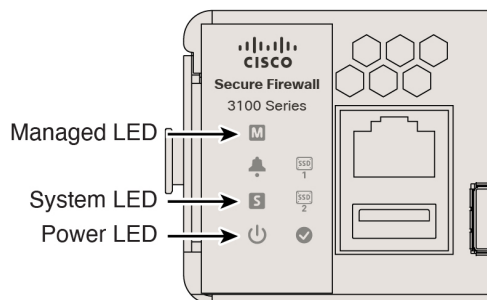
ステップ2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 1:電源スイッチ



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：緑色で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

LED の動作	説明	デバイスの電源を入れた後の時間（分:秒）
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

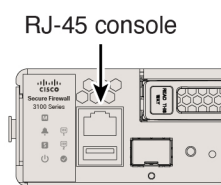
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

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。

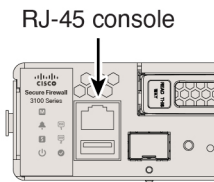
ASA CLI へのアクセス

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

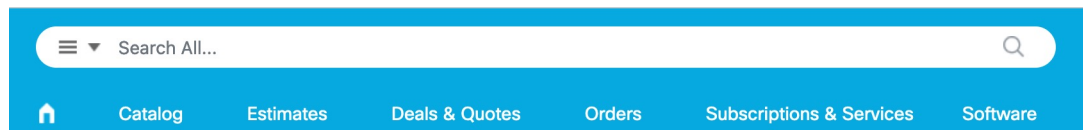
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンシングアカウントにリンクされています。[Smart Software Manager](#) にアカウントがない場合は、リンクをクリックして[新しいアカウント](#)を設定します。

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

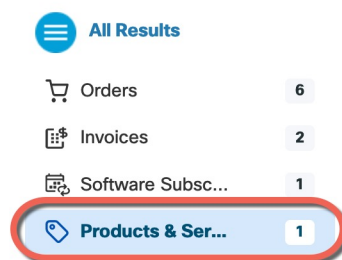
1. 自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 5: ライセンス検索



2. ライセンス PID を検索します。必要な PID については、発注ガイドを参照してください。
3. 結果から、[製品とサービス (Products & Services)] を選択します。

図 6: 結果



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。