コマンドライン インターフェイス（CLI）の使用方法

次のトピックでは、Secure Firewall Threat Defenseデバイスのコマンドライン インターフェイス（CLI）を使用する方法と、コマンドリファレンストピックの解釈方法について説明します。基本的なシステム設定およびトラブルシューティングに CLI を使用します。

（注） Secure Firewall Management Centerまたは Secure Firewall デバイスマネージャを使用して設定変更を展開する場合は、長時間実行されるコマンド（膨大な繰り返し回数やサイズの ping など）に 脅威に対する防御 CLI を使用しないでください。これらのコマンドが原因で展開が失敗する可能性があります。

CLI（コマンドライン インターフェイス）へのログイン

CLIにログインするには、SSHクライアントを使用して、管理IPアドレスに接続します。**admin** ユーザー名（デフォルトのパスワードはAdmin123です）または別のCLIのユーザー アカウントを使用してログインします。

SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。SSHアクセスを有効にするには、デバイスマネージャ（Management CenterまたはDevice Manager）を使用して、特定のデータインターフェイスへのSSH接続を許可します。診断インターフェイスに SSH 接続することはできません。

configure user add コマンドを使用して CLI にログイン可能なユーザーアカウントを作成できます。ただし、これらのユーザはCLIのみにログインできます。Device Manager Webインターフェイスにはログインできません。CLIはローカル認証のみをサポートします。外部認証を使用して CLI にアクセスすることはできません。

コンソールポートアクセス

SSHの他に、デバイスのコンソールポートに直接接続することもできます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いてPCをコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

コンソール ポートでアクセスする最初の CLI は、デバイス タイプによって異なります。

- ASA ハードウェア プラットフォーム：コンソールポートの CLI は通常の 脅威に対する防御 CLI です。
- その他のハードウェア プラットフォーム：コンソールポートの CLI は Secure Firewall eXtensible オペレーティングシステム です（FXOS）。**connect** コマンドを使用して 脅威に対する防御 CLI にアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。 Firepower 2100 の場合、FXOS CLI で設定を行うことはできません。 基本設定、モニタリング、および通常のシステムのトラブルシューティングには 脅威に対する防御CLIを使用します。FXOSコマンドの詳細については、Firepower 4100 および 9300 の FXOS コマンドに関する情報を参照してください。その他のモデルの FXOS コマンドについては、FXOS のトラブルシューティング ガイドを参照してください。

コマンド モード

脅威に対する防御 デバイスの CLI にはさまざまなモードがあります。これらのモードは、単一の CLI のサブモードではなく、実際には別の CLI です。どのモードになっているかは、コマンドプロンプトで確認できます。

通常の Threat Defense CLI

この CLI は、脅威に対する防御 の管理設定とトラブルシューティングに使用します。

```
>
```

診断 CLI

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の show コマンドや、ASA 5506W-X ワイヤレスアクセスポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。この CLI には 2 つのサブモードがあり、特権 EXEC モードの方が使用できるコマンドが多くなります。

このモードを開始するには、脅威に対する防御 CLI で **system support diagnostic-cli** コマンドを使用します。

- ユーザー EXEC モード。プロンプトには、実行コンフィギュレーションで定義されているシステムホスト名が反映されます。

  ```
  firepower>
  ```

- 特権 EXEC モード。このモードを開始するには、**enable** コマンドを入力します（パスワードプロンプトに対してパスワードを入力せずに Enter を押します）。このモードではパスワードを設定できないことに注意してください。アクセスは、脅威に対する防御 CLI へのアカウントログインによってのみ保護されます。ただし、ユーザーは特権 EXEC モードでコンフィギュレーション モードを開始できないため、追加のパスワード保護は必要ありません。

  ```
  firepower#
  ```

エキスパート モード

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、脅威に対する防御 CLI で **expert** コマンドを使用します。

管理者ユーザーでログインする場合、プロンプトは username@hostname です。別のユーザーを使用する場合は、ホスト名のみが表示されます。ホスト名は、管理インターフェイスに対して設定された名前です。次に例を示します。

```
admin@firepower:~$
```

FXOS CLI

ASA ハードウェアモデルを除き、FXOS はシャーシ全体を制御するオペレーティング システムです。モデルによっては、設定とトラブルシューティングにFXOSを使用します。FXOS から 脅威に対する防御 CLI にアクセスするには、**connect** コマンドを使用します。

すべてのアプライアンスモードモデル（Firepower 4100/9300 以外のモデル）では、**connect fxos** コマンドを使用して 脅威に対する防御 CLI から FXOS CLI に移動できます。

FXOS コマンドプロンプトは次のようになりますが、プロンプトはモードによって変化します。FXOS CLI の使用方法の詳細については、FXOS のドキュメントを参照してください。

```
Firepower-module2>
Firepower-module2#
```

構文の書式

コマンド構文の説明には、次の表記法を使用しています。

表記法	説明
command	**Command** テキストは、記載されているとおりに入力するコマンドおよびキーワードを示しています。
variable	*Variable* テキストは、ユーザーが値を指定する引数です。
[x]	角カッコの中の要素は、省略可能です（キーワードや引数）。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの入力

コンソールポートまたは SSH セッションを使用して CLI にログインすると、次のコマンドプロンプトが表示されます。

```
>
```

コマンドを実行するには、プロンプトでコマンドを入力して Enter キーを押します。その他の機能には次のものがあります。

- コマンド履歴のスクロール：上下矢印キーを使用すると、すでに入力したコマンドをスクロールできます。履歴でコマンドを再入力、または編集して再入力できます。
- コマンドの完成：部分的な文字列を入力してコマンドまたはキーワードを完成させるには、スペースキーまたは Tab キーを押します。コマンドを完成させるには、部分的な文字列が 1 つのコマンドまたはキーワードに一致する必要があります。
- コマンドの省略：通常の CLI では、コマンドを省略できません。完全なコマンド文字列を入力する必要があります。ただし診断 CLI では、ほとんどのコマンドは、コマンド固有の最少の文字列に短縮できます。たとえば、**show version** の代わりに **show ver** を入力できます。
- コマンド出力の停止：コマンドが大量の出力を生成する場合は、q キーを押すと出力を終了できます。
- 長時間実行コマンドの停止：コマンドが十分な速度で出力を返さず、別のコマンドを試すことにした場合は、Ctrl+C を押します。

show コマンド出力のフィルタリング

出力をフィルタリングコマンドにパイピングすると、**show** コマンドの出力をフィルタリングできます。出力のパイピングはすべての **show** コマンドで使用できますが、大量のテキストを生成するコマンドを処理する場合に最も役立ちます。

フィルタリング機能を使用するには、次の形式を使用します。この場合、show コマンドの後の縦棒 | はパイプ文字であり、コマンドに含まれ、構文の説明の一部ではありません。フィルタリングオプションはコマンドの | 文字の後に入力します。

show *command* | {**grep** | **include** | **exclude** | **begin**} 正規表現

フィルタリングコマンド

次のフィルタリングコマンドを使用できます。

- **grep**：パターンと一致する行のみを表示します。
- **include**：パターンと一致する行のみを表示します。
- **exclude**：パターンと一致するすべての行を除外し、その他のすべての行を表示します。
- **begin**：パターンを含む最初の行を検索し、その行と後続のすべての行を表示します。

regular_expression

通常は単純なテキスト文字列である正規表現です。式を一重引用符または二重引用符で囲まないでください。式の一部と見なされます。また、末尾のスペースは式に含まれます。

次に、**show access-list** コマンドの出力を変更して、inside1_2 インターフェイスに適用されるルールだけを表示する例を示します。

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
 rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
 rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
 rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
 rule-id 268435458
event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
 rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
 rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xc1579ed7
```

```
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
```

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **?** ：すべてのコマンドのリストを表示します。
- command_name：コマンドのオプションを表示します。 **?** たとえば、**show ?** のようになります。
- string：文字列に一致するコマンドまたはキーワードを表示します。**?** たとえば、**n?** は、文字 n で始まるすべてのコマンドを表示します。
- command_name を使用して、コマンドのシンタックスと限定された使用法の情報を表示します。**help** ヘルプページがあるコマンドを表示するには、**help ?** と入力します。

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