CHAPTER 1

CLI 設定ガイドについて

この章では、Cisco IPS CLI について説明します。内容は次のとおりです。

- 「センサー CLI 設定ガイド」（P.1-1）
- 「センサーの設定手順」（P.1-1）
- 「ユーザ ロール」（P.1-3）
- 「CLI の動作」（P.1-5）
- 「コマンドラインの編集」（P.1-6）
- 「IPS コマンド モード」（P.1-7）
- 「正規表現の構文」（P.1-8）
- 「一般的な CLI コマンド」（P.1-10）
- 「CLI のキーワード」（P.1-11）

センサー CLI 設定ガイド

このマニュアルは、Cisco IPS 7.0 CLI のタスクベースのコンフィギュレーション ガイドです。このマニュアル中で「センサー」という用語は、AIM IPS、AIP SSM、IDSM2、NME IPS のように、明示的に特定のアプライアンスまたはモジュールを指す場合を除き、すべてのモデルを指します。

全 IPS コマンドのアルファベット順リストについては、『*Command Reference for Cisco Intrusion Prevention System 7.0*』を参照してください。Cisco.com での IPS 7.0 の全マニュアルの参照方法については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.0*』を参照してください。

センサーは、IPS マネージャを使用して設定することもできます。IPS マネージャの使用方法を説明しているマニュアルへのアクセス方法の詳細については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.0*』を参照してください。

センサーの設定手順

センサーを設定するには、次のタスクを実行します。

1. センサーにログインします。
2. センサーを初期化します。

   setup コマンドを実行してセンサーを初期化します。

3. センサーの初期化を確認します。
4. サービス アカウントを作成します。

   サービス アカウントは、TAC が指示する特別なデバッグの状況で必要なものです。

注意 サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用して新しいパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

5. センサーのライセンスを有効化します。
6. ユーザおよび信頼できるホストの追加など、その他の初期タスクを実行します。
7. 必要に応じて、インターフェイス設定を変更します。

   インターフェイスは初期化時に設定します。
8. 必要に応じて、仮想センサーを追加または削除します。

   仮想センサーは初期化時に設定します。

   AIM IPS および NME IPS は、仮想化をサポートしません。
9. イベント アクション規則を設定します。
10. 侵入防御用のシグニチャを設定します。
11. グローバル相関用にセンサーを設定します。
12. 異常検知を設定します。

    デフォルト値を使用して異常検知を実行することも、ネットワークのニーズに合わせて実行することもできます。
13. すべての外部製品のインターフェイスを設定します。

    CSA MC は Cisco IPS でサポートされる唯一の外部製品です。
14. IP ロギングを設定します。
15. ブロッキングを設定します。
16. 使用する場合は、SNMP を設定します。
17. センサーをスムーズに実行し続けるためのその他のタスクを実行します。
18. 新しいシグニチャ アップデートおよびサービス パックで IPS ソフトウェアをアップグレードします。
19. 必要に応じて、アプリケーション パーティションのイメージおよびメンテナンス パーティションのイメージを再作成します。

詳細情報

- センサーにログインする手順については、第 2 章「センサーへのログイン」を参照してください。
- **setup** コマンドを使用してセンサーを初期化する手順については、第 3 章「センサーの初期化」を参照してください。
- センサーの初期化を確認する手順については、「初期化の確認」（P.3-27）を参照してください。
- ライセンス キーを入手し、インストールする手順については、「ライセンス キーのインストール」（P.4-56）を参照してください。
- センサーを設定する手順については、第 4 章「センサーのセットアップ」を参照してください。

- サービス アカウントを作成する手順については、「サービス アカウントの作成」（P.4-22）を参照してください。
- センサー上でインターフェイスを設定する手順については、第 6 章「インターフェイスの設定」を参照してください。
- センサー上で仮想センサーを設定する手順については、第 5 章「仮想センサーの設定」を参照してください。
- イベント アクション規則ポリシーを設定する手順については、第 7 章「イベント アクション規則の設定」を参照してください。
- 侵入防御のためのシグニチャを設定する手順については、第 8 章「シグニチャの定義」を参照してください。
- グローバル相関を設定する手順については、第 10 章「グローバル相関の設定」を参照してください。
- 異常検出ポリシーを設定する手順については、第 9 章「異常検出の設定」を参照してください。
- 外部製品のインターフェイスを設定する手順については、第 11 章「外部製品インターフェイスの設定」を参照してください。
- IP ロギングを設定する手順については、第 12 章「IP ロギングの設定」を参照してください。
- センサー上でブロッキングを設定する手順については、第 14 章「Attack Response Controller でのブロッキングとレート制限の設定」を参照してください。
- センサー上で SNMP を設定する手順については、第 15 章「SNMP の設定」を参照してください。
- 管理手順については、第 17 章「センサーの管理タスク」を参照してください。
- Cisco IPS ソフトウェアの入手方法の詳細については、第 22 章「ソフトウェアの入手」を参照してください。
- システム イメージの使用手順については、第 23 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。
- モジュールに固有の手順については、次の章を参照してください。
  - 第 18 章「AIM IPS の設定」
  - 第 19 章「AIP SSM の設定」
  - 第 20 章「IDSM2 の設定」
  - 第 21 章「NME IPS の設定」

ユーザ ロール

（注）　すべての IPS プラットフォームで、許可される同時 CLI セッション数は 10 です。

Cisco IPS CLI では、複数のユーザが同時にログインできます。ローカル センサーでは、ユーザの作成および削除を行えます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザにはロールが関連付けられており、ロールによって、そのユーザで実行できること、および変更できないものが制御されます。

CLI は、administrator、operator、viewer、service という 4 つのユーザ ロールをサポートします。各ロールの権限レベルは異なるため、メニューと使用できるコマンドがロールごとに異なります。

- **管理者（Administrator）**：このユーザ ロールは、最高レベルの権限を持っています。管理者は、無制限の表示アクセス権を持ち、次の機能を実行できます。
  - ユーザの追加およびパスワードの割り当て
  - 物理的なインターフェイスおよび仮想センサーの制御のイネーブル化とディセーブル化
  - 物理センシング インターフェイスの仮想センサーへの割り当て
  - 設定エージェントまたは表示エージェントとしてセンサーへの接続を許可されているホストのリストの変更
  - センサーのアドレス設定の変更
  - シグニチャの調整
  - 仮想センサーへの設定の割り当て
  - ルータの管理
- **オペレータ（Operator）**：このユーザ ロールは、2 番目に高い権限を持っています。オペレータは、無制限の表示アクセス権を持ち、次の機能を実行できます。
  - パスワードの変更
  - シグニチャの調整
  - ルータの管理
  - 仮想センサーへの設定の割り当て
- **ビューア（Viewer）**：このユーザ ロールは、最も低いレベルの権限を持ちます。ビューアは、設定とイベント データを表示でき、自分のパスワードを変更できます。

ヒント モニタリング アプリケーションに必要なのは、センサーに対するビューア アクセス権だけです。CLI を使用して、ユーザ アカウントにビューア権限を設定してから、イベント ビューアがこのアカウントを使用してセンサーに接続するように設定します。

- **サービス（Service）**：このユーザ ロールは、CLI に直接アクセスできません。サービス アカウント ユーザは、bash シェルに直接ログインされます。このアカウントは、サポートとトラブルシューティングの目的だけに使用されます。不正な変更はサポートされず、適切な動作を保証するために、デバイスのイメージを再作成する必要があります。サービス ロールを持つユーザは 1 つだけ作成できます。

  サービス アカウントにログインすると、次の警告が表示されます。

```
****************************** WARNING ************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
***************************************************************************
```

（注） サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。管理者権限のあるユーザだけが、サービス アカウントを編集できます。

（注） サービス アカウントで **su-** を実行し、ユーザ root に切り替えることもできます。root のパスワードはサービス アカウントのパスワードと同期されます。一部のトラブルシューティング手順では、root ユーザとしてコマンドを実行する必要があります。

CLI の動作

次のヒントは、Cisco IPS CLI を使用する上で役立ちます。

プロンプト

- CLI コマンドの入力を求めるプロンプトは変更できません。
- システムが質問を表示する場合やユーザ入力を待機する場合には、ユーザ インタラクティブ プロンプトが表示されます。角カッコ [ ] の中にデフォルト入力が表示されます。デフォルト入力をそのまま使用する場合は、Enter キーを押します。

ヘルプ

- コマンドのヘルプを表示するには、コマンドの後ろに **?** と 入力します。

  次に、? 関数を使用する例を示します。

```
sensor# configure ?
terminal     Configure from the terminal
sensor# configure
```

  （注） ヘルプの表示からプロンプトに戻ると、以前に入力したコマンドが ? なしで表示されます。

- 入力を完了していないトークンの後ろに **?** を 入力すると、コマンドを完成させるトークンが表示されます。トークンと ? の間に末尾のスペースがある場合、不明確なコマンドというエラーが表示されます。

```
sensor# show c ?
% Ambiguous command: "show c"
```

  スペースなしでトークンを入力した場合は、補完に使用できるトークンの選択肢（ヘルプの説明なし）が表示されます。

```
sensor# show c?
clock configuration
sensor# show c
```

- ヘルプでは、現在のモードで使用可能なコマンドだけが表示されます。

タブ補完

- タブ補完およびヘルプでは、現在のモードで使用可能なコマンドだけが表示されます。
- コマンドの完全な構文が不明な場合は、コマンドの一部を入力して Tab を押すと、コマンドを完成させることができます。
- タブ補完と一致するコマンドが複数ある場合は、何も表示されません。

呼び出し

- あるモードで入力されたコマンドを呼び出すには、↑または↓キーを使用するか、Ctrl キーを押した状態で P または Ctrl キーを押した状態で N キーを押します。

  （注） ヘルプとタブ補完の要求は、呼び出しリストには記録されません。

- 空のプロンプトは、呼び出しリストの末尾を表します。

大文字と小文字の区別

- CLI では、大文字と小文字は区別されませんが、エコーバックは大文字または小文字で入力したとおりに表示されます。たとえば、次のように入力したとします。

  ```
  sensor# CONF
  ```

  Tab を押すと、センサーには次のように表示されます。

  ```
  sensor# CONFigure
  ```

（注）　CLI コマンドでは大文字と小文字が区別されませんが、値では大文字と小文字が区別されます。シグニチャ内に正規表現を作成する場合は、この点に注意してください。「STRING」の正規表現は、パケットに表示される「string」とは異なります。

表示オプション

- –More– は、端末の出力が割り当てられた表示領域を超過したことを示すインタラクティブなプロンプトです。残りの出力を表示するには、スペースバーを押して出力の次のページを表示するか、Enter を押して一度に 1 行ずつ出力を表示します。
- 現在の行の内容をクリアして空白のコマンドラインに戻すには、Ctrl キーを押した状態で C キーを押します。

詳細情報

CLI コマンドの正規表現構文に関する詳細については、「正規表現の構文」（P.1-8）を参照してください。

コマンドラインの編集

表 1-1 では、Cisco IPS CLI で提供されるコマンド ライン編集機能について説明します。

表 1-1　コマンドラインの編集

キー	説明
Tab	途中まで入力したコマンド名エントリの入力補完を行います。文字の一意のセットを入力して Tab を押すと、システムが自動的に完全なコマンド名を入力します。複数のコマンドに該当する文字列を入力した場合、エラーを示すためにブザー音が鳴ります。一部のみ入力したコマンド名（スペースなし）の直後に疑問符（?）を入力してください。入力した文字列で始まるコマンドのリストが表示されます。
Backspace	カーソルの左にある文字を消去します。
Enter	コマンド ラインで Enter を押すと、コマンドが実行されます。端末画面の ---More--- プロンプトで Enter を押すと、1 行下にスクロールします。
スペースバー	端末画面でより多くの出力が表示されます。画面に ---More--- というプロンプトが表示された場合、スペースバーを押すと、次の画面が表示されます。
左矢印	カーソルを 1 文字分だけ後退させます。複数行にわたってコマンドを入力するときは、←キーを繰り返し押してシステム プロンプトまでスクロール バックして、コマンド エントリの先頭まで移動できます。
右矢印	カーソルを 1 文字分だけ進めます。
上矢印または Ctrl+P	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。

表 1-1　コマンドラインの編集 （続き）

キー	説明
下矢印または Ctrl+N	↑または Ctrl+P を使用してコマンドを呼び出したあと、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
Ctrl+A	カーソルを行の先頭に移動します。
Ctrl+B	カーソルを 1 文字分だけ後退させます。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+E	カーソルをコマンドラインの末尾に移動します。
Ctrl+F	カーソルを 1 文字分だけ進めます。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+L	画面をクリアして、システム プロンプトとコマンド ラインを再表示します。
Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Ctrl+U	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+V	直後に続くキーストロークを、編集キー *ではなく*コマンド エントリとして扱うようにシステムに示すコードを挿入します。
Ctrl+W	カーソルの左にある単語を削除します。
Ctrl+Y	削除バッファから最新のエントリを呼び出します。削除バッファには最後に削除したか切り取った 10 項目が格納されます。
Ctrl+Z	コンフィギュレーション モードを終了し、EXEC プロンプトに戻ります。
Esc+B	単語 1 つ分だけカーソルを後退させます。
Esc+C	カーソルの場所にある単語を大文字にします。
Esc+D	カーソルの位置から単語の末尾までを削除します。
Esc+F	単語 1 つ分だけカーソルを進めます。
Esc+L	カーソルの場所にある単語を小文字にします。
Esc+U	カーソルの位置から単語の末尾までを大文字にします。

IPS コマンド モード

Cisco IPS CLI には、次のコマンド モードがあります。

- 特権 EXEC：CLI インターフェイスにログインすると開始されます。
- グローバル コンフィギュレーション：特権 EXEC モードから **configure terminal** と入力すると開始されます。

  コマンド プロンプトは `sensor(config)#` です。
- サービス モード コンフィギュレーション：グローバル コンフィギュレーション モードから **service** *service-name* と入力すると開始されます。

  コマンド プロンプトは `sensor(config-ser)#` で、`ser` はサービス名の最初の 3 文字です。
- 複数インスタンス サービス モード：グローバル コンフィギュレーション モードから **service** *service-name log-instance-name* と入力すると開始されます。

コマンド プロンプトは sensor(config-log)# で、log はログ インスタンス名の最初の 3 文字です。システムの複数インスタンス サービスは異常検出、シグニチャ検出、およびイベント アクション規則だけです。

正規表現の構文

（注）　この項の構文は、CLI コマンドの一部として使用される正規表現だけに適用されます。シグニチャで使用される正規表現には適用されません。

正規表現は、一致する文字列を検索するために使用されるテキスト パターンです。正規表現にはプレーン テキストと特殊文字の組み合わせが含まれ、実行する検索の内容を表します。たとえば、数字を検索する場合の正規表現は [0-9] です。角カッコは、比較対象の文字が角カッコで囲まれた文字のいずれかに一致する必要があることを表します。0 と 9 の間のダッシュ（-）は、0 から 9 までの範囲を表します。したがって、この正規表現は 0 から 9 までの間の任意の文字、つまり数字に一致します。

特定の特殊文字を検索する場合は、その特殊文字の前にバックスラッシュを使用する必要があります。たとえば、「¥*」という単一文字の正規表現は、1 つのアスタリスクに一致します。

ここで定義されている正規表現は、POSIX Extended Regular Expression 定義のサブセットと類似しています。特に、[..]、[==]、および [::] という表現はサポートされていません。また、単一文字を表すエスケープ表現はサポートされています。各文字は、それぞれに対応する 16 進数値で表現できます。たとえば、¥x61 は「a」に対応しているので、文字列「a」を表すエスケープ表現は ¥x61 になります。

正規表現では、大文字と小文字が区別されます。「STRING」または「string」に一致させるには、正規表現 [Ss][Tt][Rr][Ii][Nn][Gg] を使用します。

表 1-2 に、特殊文字のリストを示します。

表 1-2　正規表現の構文

文字	説明
^	文字列の先頭です。「^A」は、文字列の先頭でのみ「A」に一致します。
^	左角カッコ（[）の直後に置かれます。角カッコ内の他の文字をターゲット文字列から除外します。[^0-9] という表現は、ターゲット文字が数字でないことを表します。
$	文字列の最後と一致します。「abc$」は、文字列の末尾にある部分文字列「abc」にのみ一致します。
|	この文字の左右どちらにある表現もターゲット文字列に一致します。表現「a|b」は、「a」と「b」のどちらにも一致します。
.	任意の文字と一致します。
*	表現の中でアスタリスクの左側にある文字が 0 回以上一致することを表します。
+	アスタリスクに似ていますが、表現の中で + 記号の左側にある文字と少なくとも 1 回の一致が必要です。
?	その左側の文字と 0 回または 1 回一致します。
()	パターンが評価される順番に影響します。また、一致した部分文字列を別の表現に置き換える際のタグ付き表現としても使用されます。

表 1-2　正規表現の構文 （続き）

文字	説明
[]	囲まれた文字のいずれかをターゲット文字と照合することを示します。
¥	エスケープ文字がないと特殊文字として解釈される文字を指定できます。 ¥xHH は、その値が (HH)、つまり 16 進数値 [0-9A-Fa-f] で表される値と同じ文字を示します。値は、ゼロ以外でなければなりません。 BEL は ¥x07、BS は ¥x08、FF は ¥x0C、LF は ¥x0A、CR は ¥x0D、TAB は ¥x09、VT は ¥x0B と同じです。 それ以外の文字「c」について、「¥c」は特殊文字として解釈されない場合の「c」と同じです。

次の例は、特殊文字を示しています。

- **a*** は、a が任意の回数（0 回を含む）続いている文字列と一致します。
- **a+** では、文字列が一致するためには、文字 a が少なくとも 1 文字含まれていることが必要です。
- **ba?b** は、文字列 bb または bab と一致します。
- **¥**** は、アスタリスク（*）が任意の回数続いている文字列と一致します。

複数文字パターンとともに量指定子を使用するには、パターンをカッコで囲みます。

- **(ab)*** は、複数文字ストリング ab の任意の回数の出現と一致します。
- **([A-Za-z][0-9])+** は、英数字ペアの 1 つ以上のインスタンスに一致しますが、存在しない場合には一致しません（空の文字列とは一致しません）。

量指定子（*、+、または ?）を使用した一致の順序は、最長構造優先です。ネストした構造は、外側から内側に一致します。連結された構造は、構造の左側から一致します。そのため、この正規表現は A9b3 に一致しますが、9Ab3 には一致しません。これは、英文字が数字の前に指定されているためです。

また、単一文字または複数文字のパターンをカッコで囲むことにより、パターンを記憶して正規表現内の別の場所で使用できるようにすることができます。

出現済みのパターンを呼び出す正規表現を作成するには、カッコを使用することで特定のパターンを記憶することを示し、バックスラッシュ（¥）の後に数字を続けることで記憶されているパターンを再利用します。数字は、正規表現パターン内でのカッコの出現位置を指定します。正規表現内の複数のパターンを記憶させた場合、¥1 は最初に記憶されたパターン、¥2 は 2 番目に記憶されたパターンとなります。

次の正規表現では、後方参照のためにカッコを使用しています。

- **a(.)bc(.)¥1¥2** は、*a*、任意の 1 文字、*bc*、任意の 1 文字、最初の*任意の*文字、2 番目の*任意の*文字が順番に並んだ文字列に一致します。

  たとえば、aZbcTZT に一致します。ソフトウェアは、最初の文字が Z であることと、2 番目の文字が T であることを記憶し、この Z と T をその後の正規表現の中で使用します。

一般的な CLI コマンド

次の CLI コマンドは、Cisco IPS 7.0 の一般的な CLI コマンドです。

- **configure terminal**：グローバル コンフィギュレーション モードを開始します。

  グローバル コンフィギュレーション コマンドは、1 つのプロトコルやインターフェイスではなく、システム全体に影響する機能に適用されます。

```
sensor# configure terminal
sensor(config)#
```

- **service**：コンフィギュレーション サブモード analysis-engine、anomaly-detection、authentication、event-action-rules、external-product-interfaces, health-monitor、host、interface、logger、network-access、notification、signature-definition、ssh-known-hosts、trusted-certificates、および web-server を開始します。

  （注） anomaly-detection、event-action-rules、および signature-definition サブモードは複数インスタンス サービスです。それぞれに 1 つのインスタンスを事前定義できます。anomaly-detection の事前定義インスタンス名は ad0 です。event-action-rules の事前定義インスタンス名は rules0 です。signature-definition の事前定義インスタンス名は sig0 です。AIM IPS と NME IPS は事前定義されたインスタンスだけをサポートします。その他のセンサーはすべて追加インスタンスの作成をサポートします。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)#
```

- **end**：コンフィギュレーション モードまたはコンフィギュレーション サブモードを終了します。トップ レベルの EXEC メニューに戻ります。

```
sensor# configure terminal
sensor(config)# end
sensor#
```

- **exit**：コンフィギュレーション モードを終了するか、またはアクティブなターミナル セッションを終了して EXEC モードを終了します。前のメニュー セッションに戻ります。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# exit
sensor(config)# exit
sensor#
```

CLI のキーワード

一般的に、コマンドの **no** 形式によって機能や関数をディセーブルにすることができます。キーワード **no** なしでそのコマンドを使用すると、ディセーブルになっていた機能または関数をイネーブルにすることができます。たとえば、コマンド **ssh host-key** *ip_address* は既知ホスト テーブルにエントリを追加し、コマンド **no ssh host-key** *ip_address* は既知ホスト テーブルからエントリを削除します。コマンドの **no** 形式の詳細な説明については、各コマンドを参照してください。

サービス コンフィギュレーション コマンドには、default 形式もあります。コマンドの設定をデフォルトに戻すには、コマンドの **default** 形式を使用します。このキーワードは、アプリケーション コンフィギュレーションに使用される **service** サブメニューに適用されます。コマンドに **default** を付けて入力すると、パラメータがデフォルト値にリセットされます。**default** キーワードを使用できるのは、コンフィギュレーション ファイルでデフォルト値を指定するコマンドだけです。