CHAPTER 1

CLI コンフィギュレーション ガイドの概要

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、IPS CLI とその使用方法について説明します。次のような構成になっています。

このマニュアルについて

このマニュアルは、Cisco IPS 7.1 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。「センサー」および「IPS SSP」という用語は、このマニュアル全体を通して同じ意味で使用されます。

アルファベット順のすべての IPS コマンドのリストについては、『*Command Reference for Cisco Intrusion Prevention System 7.1*』を参照してください。Cisco.com 上にあるすべての IPS 7.1 マニュアルの場所については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.1*』を参照してください。

IPS SSP 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については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.1*』を参照してください。

IPS SSP の設定手順

IPS SSP を設定するには、次のタスクを実行します。

1. IPS SSP にログインします。
2. IPS SSP を初期化します。**setup** コマンドを実行して IPS SSP を初期化します。
3. IPS SSP 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 の指示で行われる特別なデバッグ状況で必要になります。
5. IPS SSP のライセンスを設定します。
6. ユーザおよび信頼できるホストの追加など、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中に設定します。
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中に設定します。
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. 異常検出を設定します。異常検出は、デフォルト値を使用して実行することも、ネットワークのニーズに合わせて調整することもできます。
13. 外部製品インターフェイスをセットアップします。Cisco IPS でサポートされている外部製品は CSA MC だけです。
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. SNMP を使用する場合は、それを設定します。
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

- IPS SSP へのログイン手順については、第 2 章「IPS SSP 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 IPS SSP を初期化する手順については、第 3 章「IPS SSP の初期化」を参照してください。
- IPS SSP の初期化を確認する手順については、「初期化の確認」（P.3-12）を参照してください。
- ライセンス キーの取得およびインストールの手順については、「ライセンス キーのインストール」（P.4-42）を参照してください。
- IPS SSP のセットアップ手順については、第 4 章「IPS SSP のセットアップ」を参照してください。
- サービス アカウントの作成手順については、「サービス アカウントの作成」（P.4-16）を参照してください。
- IPS SSP 上のインターフェイスの設定手順については、第 5 章「インターフェイスの設定」を参照してください。
- IPS SSP 上の仮想センサーの設定手順については、第 6 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の設定手順については、第 8 章「イベント アクション規則の設定」を参照してください。
- 侵入防御用のシグニチャの設定手順については、第 7 章「シグニチャの定義」を参照してください。
- グローバル相関の設定手順については、第 10 章「グローバル相関の設定」を参照してください。
- 異常検出ポリシーの設定手順については、第 9 章「異常検出の設定」を参照してください。
- 外部製品インターフェイスのセットアップ手順については、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 ロギングの設定手順については、第 12 章「IP ロギングの設定」を参照してください。
- IPS SSP 上のブロッキングの設定手順については、第 14 章「Attack Response Controller でのブロッキングおよびレート制限の設定」を参照してください。
- IPS SSP 上の SNMP の設定手順については、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「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 19 章「Cisco IPS ソフトウェアの概要」を参照してください。
- イメージの操作手順については、第 20 章「IPS SSP システム イメージのインストール」を参照してください。
- IPS SSP 固有の手順については、第 18 章「IPS SSP の設定」を参照してください。

ユーザ ロール

Cisco IPS 7.1 の 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。ユーザ アカウントは一度に 1 つしか変更できません。各ユーザはロールに関連付けられ、それにより、変更できるものとできないものが決定されます。

CLI では、4 つのユーザ ロール（administrator、operator、viewer、および service）がサポートされています。ロールごとに権限レベルが異なるため、ロールによってメニューおよび使用可能なコマンドは変化します。

- **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
  - 物理インターフェイスと仮想センサーの制御のイネーブル化とディセーブル化
  - 仮想センサーへの物理的なセンシング インターフェイスの割り当て
  - 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できます。

- **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を目的とした場合にのみ使用します。権限のない変更はサポートされず、正しい動作を保証するにはデバイスのイメージが再作成される必要があります。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。管理者権限を持つユーザのみが、サービス アカウントを編集できます。

（注） サービス アカウントでは、**su-** を実行して root ユーザに切り替わることもできます。root パスワードは、サービス アカウント パスワードに同期されています。一部のトラブルシューティング手順では、コマンドを root ユーザで実行する必要があります。

CLI の動作

Cisco IPS CLI を使用する際に役立つヒントを次に示します。

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 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、? 機能の使用例を示します。

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

  プロンプトがヘルプの表示から復帰すると、前に入力したコマンドが ? 抜きで表示されます。

- また、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 ? の間にスペースが存在すると、コマンドがあいまいであることを示す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すれば、トークンの候補が表示されます（ヘルプの説明は表示されません）。

  ```
  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。
- タブ補完で複数のコマンドが一致する場合は、何も表示されません。

呼び出し

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

  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
  ```

  この状態で Tab を押すと、センサーは次を表示します。

  ```
  sensor# CONFigure
  ```

  CLI コマンドには大文字と小文字の区別はありませんが、値の大文字と小文字は区別されます。シグニチャ内の正規表現を作成する際には、このことにご注意ください。「STRING」という正規表現では、パケット内にある「string」と一致しません。

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、Space 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 ラインに戻るには、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の構文の詳細については、「正規表現の構文」（P.1-7）を参照してください。

コマンド ラインの編集

表 1-1 に、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	途中まで入力されたコマンド名を補完します。一意の文字列を入力して Tab を押すと、システムによってコマンド名が補完されます。複数のコマンド候補のある文字列を入力していた場合、システムからエラーを知らせるビープ音が鳴ります。途中まで入力したコマンドの直後に疑問符（?）を入力してください（間にスペースは入れない）。その文字列で始まるコマンドの一覧が表示されます。
Back Space	カーソルの左にある文字を消去します。
Enter	コマンド ラインでは、Enter を押すとコマンドが処理されます。端末画面上の ---More--- プロンプトでは、Enter を押すと 1 行下へスクロールします。
Space	端末画面上の出力の続きを表示できます。画面に ---More--- 行が表示されているときに Space を押して、次の画面を表示します。
←	カーソルを 1 文字左に移動します。1 行を超えるコマンドを入力した場合、←キーを繰り返し押すことで、システム プロンプトまでスクロール バックし、コマンド エントリの先頭を確認できます。
→	カーソルを 1 文字右に移動します。
↑ 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。
↓ 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 文字前進させます。
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、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。

表 1-1　コマンド ラインの編集 （続き）

キー	説明
Ctrl+V	直後に続くキーストロークを、編集キーとして *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	削除バッファ内の最新のエントリを呼び出します。削除バッファには、最後に削除または切り取りが行われた 10 個の項目が格納されています。
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	カーソルを 1 単語後退させます。
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	カーソルを 1 単語前進させます。
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したときに開始されます。
- 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** を入力して開始されます。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* を入力して開始されます。コマンド プロンプトは、`sensor(config-ser)#` です。ここで、`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* を入力して開始されます。コマンド プロンプトは、`sensor(config-log)#` です。ここで、`log` はログ インスタンス名の最初の 3 文字です。システム内の複数インスタンス サービスは、異常検出、シグニチャ定義、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） ここに記載された構文は、CLI コマンドの一部として使用される正規表現にのみ適用されます。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。正規表現は、プレーン テキストと特殊文字の組み合わせで構成され、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 ～ 9 の任意の文字、つまり、任意の数字と一致します。

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」と「string」のどちらにも一致させるには、「[Ss][Tt][Rr][Ii][Nn][Gg]」という正規表現を使用します。

表 1-2 に、特殊文字の一覧を示します。

表 1-2　正規表現の構文

文字	説明
^	文字列の先頭。「^A」という表現は、文字列の先頭にある「A」にのみ一致します。
^	左角カッコ（[）の直後。角カッコ内の残りの文字をターゲット文字列との一致から除外します。「[^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。
$	文字列の末尾と一致します。「abc$」という表現は、文字列の末尾にある部分文字列「abc」にのみ一致します。
|	両側の表現がターゲット文字列に一致できます。「a|b」という表現は、「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。
*	表現内のアスタリスクの左の文字が 0 回以上一致することを表します。
+	* に似ていますが、表現内の + 記号の左の文字と少なくとも 1 回一致する必要があります。
?	この記号の左の文字と 0 または 1 回一致する必要があります。
()	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。
[]	一連の文字を囲むことにより、囲まれた文字のいずれかとターゲット文字が一致することを示します。
\	何もしなければ特別な意味に解釈される文字を、普通の文字として指定できます。 \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。 その他の任意の文字「c」の場合、「\c」は「c」と同じであり、特別な意味に解釈されることはありません。

次に、特殊文字の使用例を示します。

- **a*** は、文字 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、一致するために、文字列内に文字 a が少なくとも 1 つ存在している必要があります。
- **ba?b** は、bb または bab の文字列と一致します。
- ***** は、任意の数の連続したアスタリスク（*）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、連続した任意の数の複数文字文字列 ab と一致します。
- **([A-Za-z][0-9])+** は、英数字ペアのインスタンスが 1 つ以上連続している文字列と一致します（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*、任意の文字、*bc*、任意の文字と続いた後、最初の*任意*の文字と 2 番目の*任意*の文字が再び現れる文字列と一致します。

  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

次に、Cisco IPS 7.1 の一般的な CLI コマンドを示します。

- **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、個々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を及ぼす機能に適用されます。

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

- **service**：次のコンフィギュレーション サブモードを開始します。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。

  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、事前定義されたインスタンスが 1 つあります。anomaly-detection の場合、事前定義されたインスタンスの名前は ad0 です。event-action-rules の場合、事前定義されたインスタンスの名前は rules0 です。signature-definition の場合、事前定義されたインスタンスの名前は sig0 です。

  ```
  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 モードまたは任意の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** : 任意のコンフィギュレーション モードを終了するか、アクティブなターミナル セッションを閉じて 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* はエントリを既知ホスト テーブルに追加し、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。各コマンドの **no** 形式の動作の詳細については、それぞれの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 **default** 形式を使用すると、コマンドの設定がデフォルトに戻ります。このキーワードは、アプリケーションの設定に使用される **service** サブメニュー コマンドに適用されます。コマンドで **default** を入力すると、パラメータがデフォルト値にリセットされます。**default** キーワードは、コンフィギュレーション ファイル内でデフォルト値を指定するコマンドにのみ使用できます。