Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.1

Text Part Number: OL-19892-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Intrusion Prevention System Sensor CLI コンフィギュレーション ガイド for IPS 7.1
© 2010-2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010–2012, シスコシステムズ合同会社 .
All rights reserved

CONTENTS

内容 xxi

対象読者 xxi

マニュアルの構成 xxi

表記法 xxiii

関連資料 xxiii

マニュアルの入手方法およびテクニカル サポート xxiv

CHAPTER 1 **CLI コンフィギュレーション ガイドの概要** 1-1

このマニュアルについて 1-1

IPS SSP の設定手順 1-2

ユーザ ロール 1-3

CLI の動作 1-4

コマンド ラインの編集 1-6

IPS コマンド モード 1-7

正規表現の構文 1-7

一般的な CLI コマンド 1-9

CLI のキーワード 1-10

CHAPTER 2 **IPS SSP へのログイン** 2-1

サポートされるユーザ ロール 2-1

IPS SSP へのログイン 2-2

Telnet または SSH を使用したログイン 2-3

CHAPTER 3 **IPS SSP の初期化** 3-1

初期化について 3-1

簡易セットアップ モード 3-2

System Configuration Dialog 3-2

センサーの基本的なセットアップ 3-4

IPS SSP の高度なセットアップ 3-7

初期化の確認 3-12

CHAPTER 4 **IPS SSP のセットアップ**

ネットワーク設定値の変更
- ホスト名の変更
- IP アドレス、ネットマスク、およびゲートウェイの変更
- Telnet のイネーブル化とディセーブル化
- アクセス リストの変更 4-5
- FTP タイムアウトの変更 4-7
- ログイン バナーの追加 4-8
- グローバル相関用の DNS サーバとプロキシ サーバの設定 4-10

Web サーバ設定の変更 4-12

ユーザ パラメータの設定 4-13
- ユーザの追加と削除 4-14
- サービス アカウントの作成 4-16
- パスワードの設定 4-17
- ユーザ権限レベルの変更 4-17
- ユーザ ステータスの表示 4-18
- パスワード ポリシーの設定 4-19
- アカウント ロッキングの設定 4-20

IPS SSP パスワードの回復 4-21
- IPS SSP パスワードの回復 4-22
- パスワード回復のディセーブル化 4-22
- パスワード回復の状態の確認 4-23
- パスワード回復のトラブルシューティング 4-24

時刻の設定 4-24
- 時刻源と IPS SSP 4-24
- IPS SSP のクロックと適応型セキュリティ アプライアンスのクロックの同期化 4-25
- IPS SSP 上の時刻の修正 4-25
- IPS SSP 上の時刻の設定 4-25
  - システム クロックの表示 4-26
  - 繰り返しサマータイム設定の設定 4-26
  - 非繰り返しサマータイム設定の設定 4-28
  - 時間帯設定の設定 4-30
- NTP の設定 4-31
  - Cisco ルータを NTP サーバにする設定 4-31
  - センサーで NTP 時刻源を使用するための設定 4-32

SSH の設定 4-34
- SSH について 4-34
- SSH 既知ホスト リストへのホストの追加 4-35
- SSH 認証公開キーの追加 4-36

新しい SSH サーバ キーの生成 4-38
TLS の設定 4-39
TLS について 4-39
TLS の信頼できるホストの追加 4-40
サーバ証明書の表示と生成 4-41
ライセンス キーのインストール 4-42
ライセンス キーについて 4-42
IPS 製品用のサービス プログラム 4-43
ライセンス キーの取得とインストール 4-44

CHAPTER 5 インターフェイスの設定 5-1
IPS SSP インターフェイスについて 5-1
物理インターフェイスの設定 5-2
無差別モード 5-3
インライン インターフェイス モード 5-4
インターフェイス通知の設定 5-4
インターフェイス統計情報の表示 5-5

CHAPTER 6 仮想センサーの設定 6-1
分析エンジンについて 6-1
仮想センサーについて 6-2
仮想化の利点および制約事項 6-2
IPS SSP 上での仮想センサーの追加、編集、および削除 6-3
IPS SSP と仮想化 6-3
IPS SSP 仮想センサーの設定手順 6-3
仮想センサーの作成 6-4
適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て 6-6
仮想センサーの編集と削除 6-9
グローバル変数の設定 6-11

CHAPTER 7 シグニチャの定義 7-1
セキュリティ ポリシーについて 7-1
シグニチャ定義ポリシーの操作 7-1
シグニチャについて 7-3
シグニチャ変数の設定 7-4
シグニチャ変数について 7-4
シグニチャ変数の追加、編集、および削除 7-4

シグニチャの設定 7-6
シグニチャ定義オプション 7-6
無差別デルタ 7-7
アラート頻度の設定 7-7
アラート重大度の設定 7-9
イベント カウンタの設定 7-11
シグニチャ忠実度レーティングの設定 7-12
シグニチャのステータスの設定 7-13
シグニチャの脆弱性のある OS の設定 7-14
シグニチャへのアクションの割り当て 7-16
AIC シグニチャの設定 7-18
AIC エンジンについて 7-18
AIC エンジンとセンサーのパフォーマンス 7-19
アプリケーション ポリシーの設定 7-20
AIC 要求メソッド シグニチャ 7-21
AIC MIME 定義コンテンツ タイプ シグニチャ 7-22
AIC 転送符号化シグニチャ 7-25
AIC FTP コマンド シグニチャ 7-26
AIC シグニチャの作成 7-27
IP フラグメント再構成の設定 7-29
IP フラグメント再構成について 7-29
IP フラグメント再構成シグニチャと設定可能なパラメータ 7-29
IP フラグメント再構成パラメータの設定 7-31
IP フラグメント再構成の方式の設定 7-32
TCP ストリーム再構成の設定 7-33
TCP ストリーム再構成について 7-33
TCP ストリーム再構成シグニチャと設定可能なパラメータ 7-34
TCP ストリーム再構成シグニチャの設定 7-39
TCP ストリーム再構成のモードの設定 7-40
IP ロギングの設定 7-41
カスタム シグニチャの作成 7-42
カスタム シグニチャの作成手順 7-42
String TCP エンジン シグニチャの例 7-43
Service HTTP エンジン シグニチャの例 7-46
Meta エンジン シグニチャの例 7-49
Atomic IP Advanced エンジン シグニチャの例 7-53
String XL エンジンの一致オフセット シグニチャの例 7-54
String XL エンジンの最小一致長シグニチャの例 7-57

CHAPTER 8 イベント アクション規則の設定 8-1

セキュリティ ポリシーについて 8-1
イベント アクション ルールについて 8-2
シグニチャ イベント アクション プロセッサ 8-2
イベント アクション 8-4
イベント アクション ルールの設定手順 8-6
イベント アクション ルール ポリシーの使用 8-7
イベント アクション変数 8-8
イベント アクション変数について 8-9
イベント アクション変数の追加、編集、および削除 8-10
ターゲットの価値レーティングの設定 8-12
リスク レーティングの計算 8-12
脅威レーティングについて 8-13
ターゲットの価値レーティングの追加、編集、および削除 8-14
イベント アクション オーバーライドの設定 8-16
イベント アクション オーバーライドについて 8-16
パケットのインライン拒否について 8-16
イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化 8-17
イベント アクション フィルタの設定 8-20
イベント アクション フィルタについて 8-20
イベント アクション フィルタの設定 8-21
OS ID の設定 8-26
パッシブ OS フィンガープリントについて 8-26
パッシブ OS フィンガープリントの設定に関する留意事項 8-27
設定された OS マップの追加、編集、削除、および移動 8-28
OS ID の表示とクリア 8-32
一般設定 8-33
イベント アクション サマライズについて 8-33
イベント アクション集約について 8-33
一般設定 8-34
拒否攻撃者リストの設定 8-35
拒否攻撃者リストへの拒否攻撃者エントリの追加 8-36
拒否攻撃者リストのモニタリングとクリア 8-37
イベントのモニタリング 8-39
イベントの表示 8-39
イベント ストアからのイベントのクリア 8-42

CHAPTER 9 異常検出の設定 9-1

セキュリティ ポリシー 9-2
異常検出について 9-2
ワーム 9-2
異常検出モード 9-3
異常検出ゾーン 9-4
異常検出の設定手順 9-5
異常検出シグニチャ 9-6
異常検出ポリシーの使用 9-8
異常検出動作の設定 9-10
内部ゾーンの設定 9-11
内部ゾーンについて 9-11
内部ゾーンの設定 9-11
内部ゾーンに対する TCP プロトコルの設定 9-13
内部ゾーンに対する UDP プロトコルの設定 9-15
内部ゾーンに対する他のプロトコルの設定 9-18
不正ゾーンの設定 9-20
不正ゾーンについて 9-20
不正ゾーンの設定 9-20
不正ゾーンに対する TCP プロトコルの設定 9-21
不正ゾーンに対する UDP プロトコルの設定 9-24
不正ゾーンに対する他のプロトコルの設定 9-26
外部ゾーンの設定 9-28
外部ゾーンについて 9-29
外部ゾーンの設定 9-29
外部ゾーンに対する TCP プロトコルの設定 9-30
外部ゾーンに対する UDP プロトコルの設定 9-32
外部ゾーンに対するその他のプロトコルの設定 9-35
学習受け入れモードの設定 9-37
KB およびヒストグラム 9-37
学習受け入れモードの設定 9-38
KB ファイルの操作 9-40
KB ファイルの表示 9-40
手動による KB の保存およびロード 9-41
KB のコピー、名前変更、および消去 9-42
2 つの KB 間の違いの表示 9-44
KB のしきい値の表示 9-45
異常検出の統計情報の表示 9-47

異常検出の無効 9-49

CHAPTER 10 グローバル相関の設定 10-1

グローバル相関について 10-1

SensorBase ネットワークへの参加 10-2

レピュテーションについて 10-3

ネットワーク参加について 10-4

有効性について 10-5

レピュテーションとリスク レーティング 10-5

グローバル相関の機能と目的 10-6

グローバル相関の要件 10-6

グローバル相関のセンサー ヘルス メトリックについて 10-7

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定 10-8

グローバル相関インスペクションおよびレピュテーション フィルタリングについて 10-8

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定 10-9

ネットワーク参加の設定 10-11

グローバル相関のトラブルシューティング 10-13

グローバル相関のディセーブル化 10-13

CHAPTER 11 外部製品インターフェイスの設定 11-1

外部製品インターフェイスについて 11-1

CSA MC について 11-2

外部製品インターフェイスの問題 11-3

IPS インターフェイスをサポートする CSA MC の設定 11-4

外部製品インターフェイスとポスチャ ACL の追加 11-5

外部製品インターフェイスのトラブルシューティング 11-9

CHAPTER 12 IP ロギングの設定 12-1

IP ロギングについて 12-1

自動 IP ロギングの設定 12-2

特定の IP アドレスに対する手動 IP ロギングの設定 12-4

IP ログの内容の表示 12-5

動作している IP ログの停止 12-6

表示する IP ログ ファイルのコピー 12-8

CHAPTER 13 インターフェイスのライブ トラフィックの表示とキャプチャ 13-1
パケットの表示とキャプチャについて 13-1
インターフェイスのライブ トラフィックの表示 13-2
インターフェイスのライブ トラフィックのキャプチャ 13-4
パケット ファイルのコピー 13-7
パケット ファイルの消去 13-8

CHAPTER 14 Attack Response Controller でのブロッキングおよびレート制限の設定 14-1
ブロッキングについて 14-2
レート制限について 14-4
レート制限のサービス ポリシーについて 14-5
ARC を設定する前に 14-5
サポートされるデバイス数 14-6
ブロッキング プロパティの設定 14-7
センサー自体のブロックの許可 14-8
ブロッキングのディセーブル 14-9
最大ブロックエントリ数の指定 14-11
ブロック時間の指定 14-13
ACL ロギングのイネーブル化 14-14
NVRAM への書き込みのイネーブル化 14-15
すべてのブロッキング イベントおよびエラーのロギング 14-17
ブロッキング インターフェイスの最大数の設定 14-18
絶対にブロックしないアドレスの設定 14-19
ユーザ プロファイルの設定 14-21
ブロッキングおよびレート制限デバイスの設定 14-22
センサーによるデバイスの管理方法 14-22
センサーで Cisco ルータを管理するための設定 14-23
ルータと ACL 14-23
センサーで Cisco ルータを管理するための設定 14-24
センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定 14-26
スイッチと VACL 14-26
センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定 14-27
センサーで Cisco ファイアウォールを管理するための設定 14-28
センサーをマスター ブロッキング センサーにする設定 14-29
ホスト ブロッキングの設定 14-32
ネットワーク ブロッキングの設定 14-33

接続ブロッキングの設定 14-34
ブロックされているホストおよび接続のリストの取得 14-35

CHAPTER 15 SNMP の設定 15-1
SNMP について 15-1
SNMP の設定 15-2
SNMP トラップの設定 15-4
サポート対象 MIB 15-6

CHAPTER 16 コンフィギュレーション ファイルの操作 16-1
現在の設定の表示 16-1
現在のサブモード コンフィギュレーションの表示 16-3
現在の設定の出力のフィルタ処理 16-16
現在のサブモード コンフィギュレーションの出力のフィルタ処理 16-18
論理ファイルの内容の表示 16-19
リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元 16-22
バックアップ コンフィギュレーション ファイルの作成と使用 16-24
コンフィギュレーション ファイルの消去 16-25

CHAPTER 17 管理タスク 17-1
IPS SSP パスワードの回復 17-2
IPS SSP パスワードの回復 17-2
パスワード回復のディセーブル化 17-3
パスワード回復の状態の確認 17-3
パスワード回復のトラブルシューティング 17-4
センサー データベースのクリア 17-4
ヘルス ステータス情報の設定 17-5
センサーの全体的なヘルス ステータスの表示 17-10
バナー ログインの作成 17-10
CLI セッションの終了 17-11
ターミナル プロパティの変更 17-12
イベントの設定 17-13
イベントの表示 17-13
イベント ストアからのイベントのクリア 17-16
システム クロックの表示 17-16
拒否攻撃者リストのクリア 17-17
ポリシー リストの表示 17-19

統計情報の表示 17-20
技術サポート情報の表示 17-30
バージョン情報の表示 17-31
ネットワークの接続性の診断 17-34
コマンド履歴の表示 17-34
IP パケットのルートのトレース 17-35
サブモード設定の表示 17-36

CHAPTER 18 IPS SSP の設定 18-1
IPS SSP の設定手順 18-1
IPS SSP の初期化の確認 18-2
IPS SSP の仮想センサーの作成 18-3
IPS SSP と仮想化 18-3
IPS SSP 仮想センサーの設定手順 18-4
仮想センサーの作成 18-4
適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て 18-6
IPS SSP のリロード、シャットダウン、リセット、および復旧 18-9
ヘルスおよびステータス情報 18-10
IPS スイッチポートで停止したトラフィック フロー 18-13
フェールオーバー シナリオ 18-14

CHAPTER 19 Cisco IPS ソフトウェアの概要 19-1
IPS 7.1(1)E4 のファイル 19-1
Cisco IPS ソフトウェアの入手方法 19-2
IPS ソフトウェアのバージョン管理 19-3
IPS ソフトウェア リリースの例 19-6
アップグレードの注意事項と警告 19-8
IPS マニュアルへのアクセス 19-9
Cisco Security Intelligence Operations 19-10
Cisco.com からのライセンス キーの取得 19-10
ライセンスについて 19-10
IPS 製品用のサービス プログラム 19-11
IDM または IME を使用したライセンス キーの取得とインストール 19-12
CLI を使用したライセンス キーの取得とインストール 19-13

CHAPTER 20 IPS SSP システム イメージのインストール 20-1
IPS 7.1(1)E4 のファイル 20-1

サポートされる FTP および HTTP/HTTPS サーバ 20-2
ROMMON について 20-2
TFTP サーバ 20-3
シリアル ポートへの接続 20-3
IPS SSP システム イメージのインストール 20-4
hw-module コマンドを使用したシステム イメージのインストール 20-4
ROMMON を使用したシステム イメージのインストール 20-6
リカバリ パーティションのアップグレード 20-9
アプリケーション パーティションの復旧 20-10
アプリケーション パーティションについて 20-10
IPS SSP アプリケーション パーティション イメージの復旧 20-11

APPENDIX A システム アーキテクチャについて A-1
Cisco IPS の目的 A-1
システム設計 A-2
システム アプリケーション A-3
ユーザ対話 A-4
セキュリティ機能 A-4
MainApp A-5
MainApp について A-5
MainApp の役割 A-6
イベント ストア A-6
イベント ストアについて A-6
イベントのデータ構造 A-7
IPS イベント A-8
NotificationApp A-9
CtlTransSource A-11
Attack Response Controller A-12
ARC について A-12
ARC の機能 A-13
サポートされているブロッキング デバイス A-15
ACL と VACL A-15
再起動時の状態の維持 A-16
接続ベースおよび無条件のブロッキング A-17
シスコのファイアウォールによるブロッキング A-17
Catalyst スイッチによるブロッキング A-18
ロガー A-19
AuthenticationApp A-19

AuthenticationApp について A-19
ユーザの認証 A-20
センサーにおける認証の設定 A-20
TLS および SSH 信頼関係の管理 A-20
Web サーバ A-22
SensorApp A-22
SensorApp について A-22
インライン、正規化、およびイベント リスク レーティング機能 A-24
SensorApp の新機能 A-25
パケット フロー A-25
シグニチャ イベント アクション プロセッサ A-26
CollaborationApp A-27
CollaborationApp について A-28
アップデート コンポーネント A-28
error イベント A-29
CLI A-29
CLI について A-30
ユーザ ロール A-30
サービス アカウント A-31
通信 A-31
IDIOM A-32
IDCONF A-32
SDEE A-33
CIDEE A-33
IDAPI A-34
Cisco IPS のファイル構造 A-34
Cisco IPS アプリケーションの概要 A-35

APPENDIX B **シグニチャ エンジンの概要 B-1**
シグニチャ エンジンの概要 B-2
Master エンジン B-4
一般的なパラメータ B-5
アラート頻度 B-7
イベント アクション B-8
正規表現の構文 B-10
AIC エンジン B-11
AIC エンジンについて B-11
AIC エンジンとセンサーのパフォーマンス B-11
AIC エンジンのパラメータ B-12

Atomic エンジン B-12
Atomic ARP エンジン B-13
Atomic IP Advanced エンジン B-14
Atomic IP Advanced エンジンの概要 B-14
Atomic IP Advanced エンジンに関する制約事項 B-15
Atomic IP Advanced エンジンのパラメータ B-15
Atomic IP エンジン B-23
Atomic IPv6 エンジン B-26
Fixed エンジン B-27
Flood エンジン B-30
Meta エンジン B-31
Multi String エンジン B-32
ノーマライザ エンジン B-33
ノーマライザ エンジンの概要 B-34
ノーマライザ エンジンのパラメータ B-35
Service エンジン B-36
Service エンジンの概要 B-36
Service DNS エンジン B-36
Service FTP エンジン B-38
Service Generic エンジン B-38
Service H225 エンジン B-40
Service HTTP エンジン B-42
Service IDENT エンジン B-44
Service MSRPC エンジン B-45
Service MSSQL エンジン B-46
Service NTP エンジン B-47
Service P2P エンジン B-47
Service RPC エンジン B-48
Service SMB Advanced エンジン B-49
Service SNMP エンジン B-51
Service SSH エンジン B-52
Service TNS エンジン B-53
State エンジン B-54
String エンジン B-56
String XL エンジン B-59
Sweep エンジン B-62
Sweep エンジン B-62
Sweep Other TCP エンジン B-64

Traffic Anomaly エンジン B-65
Traffic ICMP エンジン B-67
Trojan エンジン B-68

APPENDIX C トラブルシューティングに関するヒントと手順 C-1
Bug Toolkit C-2
予防保守 C-2
予防保守の概要 C-2
バックアップ コンフィギュレーション ファイルの作成と使用 C-3
リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元 C-3
サービス アカウントの作成 C-5
ディザスタ リカバリ C-6
パスワード回復 C-8
IPS SSP パスワードの回復 C-8
パスワード回復のディセーブル化 C-9
パスワード回復の状態の確認 C-9
パスワード回復のトラブルシューティング C-10
時刻源 C-10
時刻源と IPS SSP C-10
IPS SSP のクロックと適応型セキュリティ デバイスのクロックの同期化 C-11
IPS SSP が NTP サーバと同期していることを確認する C-11
IPS SSP の時刻の修正 C-12
仮想化の利点および制約事項 C-12
サポート対象 MIB C-13
グローバル相関のトラブルシューティング C-13
異常検出をディセーブルにする場合 C-14
分析エンジン応答なし C-15
外部製品インターフェイスのトラブルシューティング C-16
外部製品インターフェイスに関する問題 C-16
外部製品インターフェイスのトラブルシューティングのヒント C-17
センサーのトラブルシューティング C-17
接続不良のトラブルシューティング C-17
分析エンジンがビジー状態になる C-18
通信の問題 C-18
Telnet または SSH でセンサーの CLI にアクセスできない C-19
設定が誤っているアクセス リストの修正 C-21
重複している IP アドレスがインターフェイスをシャットダウンする C-22

SensorApp とアラート C-23
SensorApp が実行しない C-23
物理的な接続性、SPAN、または VACL ポートの問題 C-25
アラートを表示できない C-27
センサーがパケットを監視しない C-28
破損した SensorApp 設定のクリーンアップ C-29
ブロッキング C-30
ブロッキングのトラブルシューティング C-30
ARC が実行中であることを確認する C-31
ARC 接続がアクティブであることを確認する C-32
デバイスのアクセスに関する問題点 C-34
ネットワーク デバイス上のインターフェイスおよび方向を確認する C-35
ネットワーク デバイスへの SSH 接続を有効にする C-36
シグニチャに対してブロッキングが発生していない C-37
マスター ブロッキング センサーの設定を確認する C-38
ロギング C-39
ロギングの概要 C-39
デバッグ ロギングをイネーブルにする C-40
ゾーン名 C-43
SysLog に cidLog メッセージを転送する C-44
ソフトウェアのアップグレード C-45
アップグレード エラー C-45
適用するアップデートと前提条件 C-46
自動アップデートに関する問題 C-46
センサーに格納されたアップデートを使用してセンサーを更新する C-47
IPS SSP のトラブルシューティング C-48
フェールオーバー シナリオ C-48
ヘルスおよびステータス情報 C-49
IPS スイッチポートで停止したトラフィック フロー C-52
情報の収集 C-52
ヘルスおよびネットワーク セキュリティ情報 C-53
技術サポート情報 C-53
show tech-support コマンドの概要 C-54
技術サポート情報の表示 C-54
技術サポート コマンドの出力 C-55
バージョン情報 C-57
show version コマンドの概要 C-57
バージョン情報の表示 C-57
統計情報 C-60
show statistics コマンドの概要 C-60

統計情報の表示 C-61
インターフェイス情報 C-70
show interfaces コマンドの概要 C-71
インターフェイス コマンドの出力 C-71
イベント情報 C-72
センサーのイベント C-72
show events コマンドの概要 C-72
イベントの表示 C-73
イベントのクリア C-76
cidDump スクリプト C-76
Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス C-77

APPENDIX D CLI のエラー メッセージ D-1
CLI のエラー メッセージ D-1
CLI 検証エラー メッセージ D-5

APPENDIX E Cisco IPS 7.1 で使用されるオープン ソース ライセンス ファイル E-A
内容 E-A
bash 3.2 E-B
busybox 1.13.1 E-G
cracklib 2.8.12 E-L
curl 7.18.2 1 E-Q
diffutils 2.8.1 E-R
e2fsprogs 1.39 E-W
Expat XML parser 2.0.1 E-AB
expect 5.4.3 E-AB
glibc 2.9 E-AB
gnupg 1.4.5 E-AF
hotplug 2004_03_29 E-AJ
i2c-tools 3.0.2 E-AO
ipmiutil 2.3.3 E-AT
iptables 1.4.1 E-AT
kernel 2.6.29.1 E-AY
libpcap 0.9.8 E-BH
libtecla 1.4.1 E-BI
Linux-Pam 1.0.1 E-BI

lm_sensors 3.0.2 E-BJ
module-init-tools 3.2.2 1.0.0.0900084 E-BO
Ncurses 5.6 E-BS
net-snmp 5.4.1 E-BT
NTP 4.2.4p5 E-BX
openssh 5.1p1 E-CA
openssl 0.9.8j E-CG
pciutils 3.0.1 E-CJ
procps 3.2.7 E-CP
sysfsutils 2.1.0 E-CT
sysstat 8.1.3 E-CU
tcl 8.4.9 E-CY
tcpdump 3.9.8 1.0.1.0801182 E-CZ
tipc 1.7.6-bundle E-CZ
util-linux 2.12r E-DB
zlib 1.2.3 E-DC

GLOSSARY

INDEX

はじめに

内容

このマニュアルでは、Cisco IPS 7.1 CLI を使用してセンサーを設定する方法について説明します。Cisco Intrusion Prevention System 7.1 のマニュアル セットの一部です。展開された略語と IPS 関連の用語を記載した用語集が含まれています。このマニュアル内では、「IPS SSP」と「センサー」が同じ意味で使用されます。このマニュアルは、「関連資料」（P.xxiii）に記載されている資料と一緒に使用してください。次のような構成になっています。

- 「対象読者」（P.xxi）
- 「マニュアルの構成」（P.xxi）
- 「関連資料」（P.xxiii）
- 「マニュアルの入手方法およびテクニカル サポート」（P.xxiv）

対象読者

このマニュアルは、次の作業を実行する必要のある管理者を対象にしています。

- CLI を使用した侵入防御用センサーの設定。
- IPS センサーによるネットワークのセキュリティ保護。
- ネットワークへの侵入の防御とそれに続くアラートのモニタ。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

項	タイトル	説明
1	「CLI コンフィギュレーション ガイドの概要」	この CLI コンフィギュレーション ガイドの目的について説明します。
2	「IPS SSP へのログイン」	IPS SSP へのログイン方法について説明します。
3	「IPS SSP の初期化」	**setup** コマンドを使用して IPS SSP を初期化する方法について説明します。
4	「IPS SSP のセットアップ」	CLI を使用して IPS SSP 上の初期設定値を設定する方法について説明します。

項	タイトル	説明
5	「インターフェイスの設定」	無差別、インライン、インライン VLAN ペア、および VLAN グループのインターフェイスを設定する方法について説明します。
6	「仮想センサーの設定」	仮想センサーの設定方法について説明します。
7	「イベント アクション規則の設定」	IPS SSP 上のイベント アクション規則ポリシーを設定する方法について説明します。
8	「シグニチャの定義」	シグニチャを追加、複製、編集する方法について説明します。
9	「異常検出の設定」	IPS SSP 上の異常検出ポリシーを設定する方法について説明します。
10	「グローバル相関の設定」	IPS SSP のグローバル相関機能を設定する方法について説明します。
11	「外部製品インターフェイスの設定」	CSA MC 用の外部製品インターフェイスを設定する方法について説明します。
12	「IP ロギングの設定」	IPS SSP 上の IP ロギングを設定する方法について説明します。
13	「インターフェイスのライブ トラフィックの表示とキャプチャ」	IPS SSP インターフェイス上でライブ トラフィックの表示とキャプチャを行う方法について説明します。
14	「Attack Response Controller でのブロッキングおよびレート制限の設定」	Cisco ルータやスイッチ上でブロッキングとレート制限を設定する方法、およびマスター ブロッキング センサーを設定する方法について説明します。
15	「SNMP の設定」	IPS SSP 上の SNMP を設定する方法について説明します。
16	「コンフィギュレーション ファイルの操作」	IPS SSP 上のコンフィギュレーション ファイルを使用する方法について説明します。
17	「管理タスク」	IPS SSP の動作を維持し、その状態を最新に保つのに役立つ各種管理手順について説明します。
19	「IPS SSP の設定」	IPS SSP を設定する方法について説明します。
22	「Cisco IPS ソフトウェアの概要」	最新の IPS ソフトウェアを入手できる場所、および命名規則について説明します。
23	「IPS SSP システム イメージのインストール」	IPS SSP をアップグレードし、そのイメージを再作成する方法について説明します。
A	「システム アーキテクチャについて」	IPS システム アーキテクチャについて説明します。
B	「シグニチャ エンジンの概要」	IPS シグニチャ エンジンとそれらのパラメータについて説明します。
C	「トラブルシューティングに関するヒントと手順」	IPS のハードウェアとソフトウェアに関するトラブルシューティングのヒントが記載されています。
D	「CLI のエラー メッセージ」	CLI エラー メッセージの一覧が示されています。
E	「Cisco IPS 7.1 で使用されるオープン ソース ライセンス ファイル」	IPS で使用されるオープン ソース ライセンス ファイルの一覧が示されています。
	「Glossary」	IPS の略語と用語が記載されています。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	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は、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス *時間を節約する方法*です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「*警告*」の意味です。人為ミスを予防するための注意事項が記述されています。**

関連資料

Cisco IPS 7.1 のすべてのマニュアルの一覧およびそれらの場所については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/ips/7.0/roadmap/19889_01.html

Cisco ASA 5500 シリーズのすべてのマニュアルの一覧およびそれらの場所については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

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」（P.1-1）
- 「IPS SSP の設定手順」（P.1-2）
- 「ユーザ ロール」（P.1-3）
- 「CLI の動作」（P.1-4）
- 「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.1-7）
- 「一般的な CLI コマンド」（P.1-9）
- 「CLI のキーワード」（P.1-10）

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。

CHAPTER 2

IPS SSP へのログイン

（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。

（注） すべての IPS プラットフォームで、同時に 10 個のログイン セッションを利用できます。

この章では、IPS SSP にログインする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。

- 「サポートされるユーザ ロール」（P.2-1）
- 「IPS SSP へのログイン」（P.2-2）
- 「Telnet または SSH を使用したログイン」（P.2-3）

サポートされるユーザ ロール

次のユーザ権限でログインできます。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

  サービス 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センサー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。

詳細情報

- 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。
- ユーザの追加および削除の手順については、「ユーザ パラメータの設定」（P.4-13）を参照してください。

IPS SSP へのログイン

適応型セキュリティ アプライアンスから IPS SSP にログインします。

適応型セキュリティ アプライアンスから IPS SSP へのセッションを確立するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

（注）　適応型セキュリティ アプライアンスがマルチモードで動作中の場合は、作業を続ける前に、**change system** コマンドを使用してシステム レベル プロンプトに移動します。

ステップ 2　IPS SSP に対してセッションを開始します。60 秒以内にログインしないと、セッションはタイムアウトします。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 3　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。このモジュールに初めてログインすると、それらを変更するように求められます。最初に UNIX パスワード（**cisco**）を入力する必要があります。その後、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
```

```
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
ips-ssp#
```

ステップ 4　セッションを終了して適応型セキュリティ アプライアンスのプロンプトに戻るには、次のいずれかを実行します。

- **exit** を入力します。
- Ctrl キーと Shift キーを押した状態で 6 を押してから x を押します（**Ctrl^X** と表現されます）。

詳細情報

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。

Telnet または SSH を使用したログイン

（注）　**setup** コマンドを使用して IPS SSP を初期化し、Telnet をイネーブルにした後は、SSH または Telnet を使用してログインできます。

Telnet または SSH を使用して IPS SSP にログインするには、次の手順を実行します。

ステップ 1　SSH または Telnet を使用してネットワーク経由で IPS SSP にログインします。

ssh *sensor_ip_address*
telnet *sensor_ip_address*

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

```
login: ******
Password: ******
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable law s and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
ips-ssp#
```

詳細情報

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。

CHAPTER 3

IPS SSP の初期化

（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、**setup** コマンドを使用して IPS SSP を初期化する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。

- 「初期化について」（P.3-1）
- 「簡易セットアップ モード」（P.3-2）
- 「System Configuration Dialog」（P.3-2）
- 「センサーの基本的なセットアップ」（P.3-4）
- 「IPS SSP の高度なセットアップ」（P.3-7）
- 「初期化の確認」（P.3-12）

初期化について

（注） **setup** コマンドを使用するには、管理者である必要があります。

IPS SSP をネットワーク上に設置した後、それを **setup** コマンドで初期化して、ネットワーク経由で通信できるようにする必要があります。**setup** コマンドを使用して初期化するまで、IDM または IME を使用して IPS SSP を設定することはできません。

setup コマンドでは、ホスト名、IP インターフェイス、アクセス コントロール リスト、グローバル相関サーバ、時刻設定など、センサーの基本設定を設定できます。続けて CLI の高度なセットアップを使用して、Telnet のイネーブル化、Web サーバの設定、および仮想センサーとインターフェイスの割り当てとイネーブル化を行うことができます。あるいは、IDM または IME で Startup Wizard を使用することもできます。

注意　グローバル相関機能が動作するには、有効なセンサー ライセンスを取得している必要があります。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

簡易セットアップ モード

コンソール ケーブルを使用してセンサーに接続したとき、センサーの基本的なネットワーク設定がまだ設定されていなければ、センサーは自動的に **setup** コマンドをコールします。次の状態では、センサーは自動セットアップをコールしません。

- すでに初期化が正常に完了している場合。
- センサーを復元またはダウンロードした場合。
- 自動セットアップを使用してセンサーを正常に設定した後にホスト設定をデフォルトに設定した場合。

setup コマンドを入力すると、システムのコンソール画面に対話形式のダイアログ、System Configuration Dialog が表示されます。System Configuration Dialog に従って設定プロセスを進めます。各プロンプトの隣に表示されるカッコ内の値は、最後に設定された値で、デフォルト値として使用されます。

System Configuration Dialog

setup コマンドを入力すると、システムのコンソール画面に対話形式のダイアログ、System Configuration Dialog が表示されます。System Configuration Dialog に従って設定プロセスを進めます。

各プロンプトの隣に表示されるカッコ内の値は、現在の値を示しています。

変更するオプションにたどり着くまで、System Configuration Dialog を進めます。変更しない項目のデフォルト設定を受け入れるには、**Enter** を押します。

System Configuration Dialog を中断して変更を行わずに EXEC プロンプトに戻るには、Ctrl を押した状態で C を押します。

System Configuration Dialog では、プロンプトごとにヘルプ テキストも提供されます。ヘルプ テキストにアクセスするには、プロンプトで **?** を入力します。

変更を最後まで行うと、セットアップ セッション中に作成した設定が System Configuration Dialog によって表示されます。さらに、この設定を使用するかどうかも確認されます。**yes** を入力すると、設定が保存されます。**no** を入力すると、設定は保存されずにプロセスが再開されます。このプロンプトにはデフォルトがありません。**yes** か **no** を入力する必要があります。

繰り返しモードまたは日付モードのいずれかでサマータイムを設定できます。繰り返しモードを選択すると、開始日と終了日は、週、曜日、月、および時刻に基づきます。日付モードを選択すると、開始日と終了日は、月、曜日、年、および時刻に基づきます。ディセーブルを選択すると、サマータイムはオフになります。

（注）　システムがアプライアンスで、なおかつ NTP を使用していない場合は、System Configuration Dialog で日付と時刻のみを設定します。

（注）　System Configuration Dialog は対話型のダイアログです。デフォルトの設定が表示されます。

例 3-1 に、System Configuration Dialog の例を示します。

例 3-1　System Configuration Dialog の例

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Wed Nov 11 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.0.2.0/24,255.255.0]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Global Correlation?[no]:
DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Global Correlation?[no]:
HTTP proxy server IP address[128.107.241.169]:
HTTP proxy server Port number[8080]:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
```

```
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.We do not collect the data content of traffic
or other sensitive business or personal information.All data is aggregated and sent via
secure HTTP to the Cisco SensorBase Network servers in periodic intervals.All data shared
with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
* Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs.promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
* Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

センサーの基本的なセットアップ

setup コマンドを使用してセンサーの基本的なセットアップを実施し、その後に CLI、IDM、または IME を使用してセンサーのセットアップを完了させることができます。

setup コマンドを使用してセンサーの基本的なセットアップを実施するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。

ステップ 2　センサーに初めてログインしたとき、デフォルトのパスワードを変更するよう求められます。パスワードは最低 8 文字で、強力なパスワードにする必要があります。辞書にある単語は使用しないでください。パスワードを変更すると、基本セットアップが開始されます。

ステップ 3　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 4　ホスト名を指定します。ホスト名は 64 文字までの文字列で、大文字と小文字が区別されます。数字、「_」、および「-」は使用できますが、スペースは使用できません。デフォルトは sensor です。

ステップ 5　IP インターフェイスを指定します。IP インターフェイスは、*X.X.X.X/nn*,*Y.Y.Y.Y*（IP アドレス / ネットマスク , ゲートウェイ）の形式になります。ここで、*X.X.X.X* はセンサーの IP アドレスを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです。*nn* はネットマスクのビット数を示します。*Y.Y.Y.Y* はデフォルト ゲートウェイを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです。

ステップ 6　**yes** を入力してネットワーク アクセス リストを修正します。

a. エントリを削除する場合は、エントリの番号を入力して Enter を押します。そうでない場合は、Enter を押して Permit 行に移動します。

b. アクセス リストに追加するネットワークの IP アドレスおよびネットマスクを入力します。

たとえば、10.0.0.0/8 は 10.0.0.0 ネットワーク上のすべての IP アドレス（10.0.0.0 ～ 10.255.255.255）を許可します。10.1.1.0/24 は 10.1.1.0 サブネット上の IP アドレス（10.1.1.0 ～ 10.1.1.255）のみを許可します。ネットワーク全体ではなく、単一 IP アドレスへのアクセスを許可する場合は、32 ビットのネットマスクを使用します。たとえば、10.1.1.1/32 は 10.1.1.1 アドレスのみを許可します。

c. アクセス リストに追加するすべてのネットワークが追加されるまで、ステップ b を繰り返します。その後、空の permit 行で Enter を押して次のステップに進みます。

ステップ 7　グローバル相関が動作するには、DNS サーバまたは HTTP プロキシ サーバを設定する必要があります。

a. **yes** を入力して DNS サーバを追加し、DNS サーバの IP アドレスを入力します。

b. **yes** を入力して HTTP プロキシ サーバを追加し、HTTP プロキシ サーバの IP アドレスとポート番号を入力します。

注意　グローバル相関機能が動作するには、有効なセンサー ライセンスを所有している必要があります。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、アップデートは試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

ステップ 8　**yes** を入力して、システム クロック設定を修正します。

a. **yes** を入力して、サマータイム設定を修正します。

（注）　サマータイムは、DST とも呼ばれます。サマータイムを採用していない地域の場合は、ステップ m に進みます。

b. **yes** を入力して米国サマータイム デフォルトを選択します。あるいは、**no** を入力し、recurring、date、または disable を選択してサマータイム設定の設定方法を指定します。デフォルトは recurring です。

c. recurring を選択した場合は、サマータイム設定の開始月を指定します。有効な値は january、february、march、april、may、june、july、august、september、october、november、december です。デフォルトは march です。

d. サマータイム設定の開始週を指定します。有効な値は first、second、third、fourth、fifth、last です。デフォルトは second です。

e. サマータイム設定の開始曜日を指定します。有効な値は sunday、monday、tuesday、wednesday、thursday、friday、saturday です。デフォルトは sunday です。

f. サマータイム設定の開始時刻を指定します。デフォルトは 02:00:00 です。

（注）　デフォルトの定期的なサマータイム パラメータはアメリカ合衆国の時間帯用です。デフォルト値では、開始時刻が 3 月の第 2 日曜日の午前 2:00、終了時刻が 11 月の第 1 日曜日の午前 2:00 です。デフォルトのサマータイム オフセットは 60 分です。

g. サマータイム設定の終了月を指定します。有効な値は january、february、march、april、may、june、july、august、september、october、november、december です。デフォルトは november です。

h. サマータイム設定の終了週を指定します。有効な値は first、second、third、fourth、fifth、last です。デフォルトは first です。

i. サマータイム設定の終了曜日を指定します。有効な値は sunday、monday、tuesday、wednesday、thursday、friday、saturday です。デフォルトは sunday です。

j. サマータイム設定の終了時刻を指定します。デフォルトは 02:00:00 です。

k. DST ゾーンを指定します。ゾーン名には、[A-Za-z0-9()+:,_/-]+$ のパターンを持つ 24 文字までの文字列を使用できます。

l. サマータイム オフセットを指定します。協定世界時（UTC）からのサマータイム オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。デフォルトは 60 です。

m. **yes** を入力してシステム時間帯を修正します。

n. 標準時の時間帯名を指定します。ゾーン名には 24 文字までの文字列を使用できます。

o. 標準時の時間帯オフセットを指定します。UTC からの標準時の時間帯オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。デフォルトは 0 です。

p. NTP を使用する場合は、**yes** を入力します。認証された NTP を使用するには、NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。これらがこの時点で存在しない場合は、後で NTP を設定できます。あるいは、未認証の NTP を選択することもできます。

ステップ 9　**off**、**partial**、または **full** を入力して、SensorBase Network Participation に参加します。

- off：SensorBase ネットワークにデータは提供されません。
- partial：SensorBase ネットワークにデータが提供されます。ただし、潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。
- full：除外指定した攻撃者 / 攻撃対象の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

SensorBase Network Participation の注意事項が表示されます。これには、SensorBase ネットワークに参加することにより何が起こるかが説明されています。

ステップ 10　**yes** を入力して、SensorBase ネットワークに参加します。

```
The following configuration was entered.
service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name sensor126
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
```

```
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.89.143.92 key-id 1
exit
service global-correlation
network-participation full
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

ステップ 11　**2** を入力して設定を保存します（あるいは、**3** を入力して、CLI を使用した高度なセットアップを続けて行います）。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 12　時刻設定を変更した場合は、**yes** を入力してセンサーをリブートします。

詳細情報

最新の IPS ソフトウェアを入手する手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

IPS SSP の高度なセットアップ

注意　IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

IPS SSP の高度なセットアップを続けて行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IPS SSP へのセッションを確立します。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1.Escape character sequence is 'CTRL-^X'.
```

```
login: cisco
Password:
Last login: Fri Jan 14 04:14:54 from 10.77.25.187
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, xport, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S.laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.
asa#
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　**3** を入力して、高度なセットアップにアクセスします。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトではディセーブルになっています。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　Web サーバは、デフォルトで TLS/SSL 暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** を入力して、インターフェイスと仮想センサーの設定を修正します。

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　**1** を入力して、インターフェイス設定を編集します。

（注）　IPS SSP 上でインターフェイスを設定する必要はありません。[Modify interface default-vlan] 設定は無視します。IPS SSP の場合、仮想センサー間のトラフィックの分離は、他のセンサーとは異なる方法で設定されます。

```
  [1] Modify interface default-vlan.
Option:
```

ステップ 8　Enter を押して、インターフェイスと仮想センサーのトップレベルの設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 9　2 を入力して、仮想センサー設定を編集します。

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

ステップ 10　2 を入力して、仮想センサー vs0 の設定を修正します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

ステップ 11　1 を入力して、PortChannel0/0 を仮想センサー vs0 に追加します。

（注）　複数の仮想センサーがサポートされます。適応型セキュリティ アプライアンスは、特定の仮想センサーにパケットを誘導することも、パケットを送信してデフォルトの仮想センサーにモニタさせることもできます。PortChannel0/0 を割り当てた仮想センサーがデフォルトの仮想センサーになります。PortChannel0/0 は vs0 に割り当てることを推奨しますが、必要に応じて、別の仮想センサーに割り当ててかまいません。

ステップ 12　Enter を押して、仮想センサーのメイン メニューに戻ります。

ステップ 13　3 を入力して、仮想センサーを作成します。

```
Name[]:
```

ステップ 14　仮想センサーの名前と説明を入力します。

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

ステップ 15　1 を入力して、既存の異常検出設定 ad0 を使用します。

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

ステップ 16　2 を入力して、シグニチャ定義のコンフィギュレーション ファイルを作成します。

ステップ 17　シグニチャ定義設定の名前として **newSig** を入力します。

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

ステップ 18　**1** を入力して、既存のイベントアクション規則設定 rules0 を使用します。

（注）　PortChannel0/0 が vs0 に割り当てられていない場合、PortChannel0/0 をこの新しい仮想センサーに割り当てるよう求められます。

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

ステップ 19　Enter を押して、インターフェイスと仮想センサーの設定メニューに戻ります。

```
Modify default threat prevention settings?[no]:
```

ステップ 20　デフォルトの脅威防御設定を修正する場合は、**yes** を入力します。

（注）　このセンサーには、ハイ リスク レーティングのアラートにパケット拒否イベント アクションを追加する組み込みのオーバーライドが付属しています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 21　yes を入力して、すべての仮想センサー上の自動脅威防御をディセーブルにします。

```
The following configuration was entered.

service host
network-settings
host-ip 192.0.2.0/24,255.255.0
host-name ips-ssm
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
```

```
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 22　**2** を入力して設定を保存します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 23　IPS SSP をリブートします。

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 24　**yes** を入力して、リブートを続行します。

ステップ 25　リブート後、センサーにログインし、自己署名 X.509 証明書（TLS で必要）を表示します。

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 26　証明書のフィンガープリントを書き留めます。Web ブラウザで HTTPS を使用してこの IPS SSP に接続する際に証明書の信頼性を確認するためにフィンガープリントが必要です。これで、IPS SSP に侵入防御を設定する準備ができました。

詳細情報

- IPS SSP 上の仮想センサー用にトラフィックを割り当てる手順については、「IPS SSP の仮想センサーの作成」（P.18-3）を参照してください。
- ASA ソフトウェアの詳細については、次の URL にある ASA のユーザ マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

初期化の確認

IPS SSP の初期化が完了したことを確認するには、次の手順を実行します。

ステップ 1　IPS SSP にログインします。

ステップ 2　設定を表示します。

```
ips-ssp# show configuration
! ------------------------------
! Current configuration last modified Wed Jun 30 20:05:09 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S486.0   2010-04-29
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1006 0
alert-severity informational
exit
signatures 1102 0
alert-severity informational
exit
signatures 1104 0
alert-severity informational
exit
signatures 60000 0
promisc-delta 5
engine atomic-ip
exit
exit
exit
```

```
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

（注）　**more current-config** コマンドを使用して、設定を表示することもできます。

ステップ 3　自己署名 X.509 証明書（TLS で必要）を表示します。

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 4　証明書のフィンガープリントを書き留めます。Web ブラウザでこのセンサーに接続する際に証明書の信頼性を確認するためにフィンガープリントが必要です。

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。
- **more current-config** コマンドの使用手順については、「現在の設定の表示」（P.16-1）を参照してください。
- TLS フィンガープリントの詳細については、「TLS の設定」（P.4-39）を参照してください。

CHAPTER 4

IPS SSP のセットアップ

（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、初期化情報の変更、ユーザの追加と削除、時刻の設定と NTP のセットアップ、サービス アカウントの作成、SSH と TLS の設定、ライセンス キーのインストールなど、IPS SSP のセットアップ手順について説明します。この章は、次のような構成になっています。

- 「ネットワーク設定値の変更」（P.4-1）
- 「Web サーバ設定の変更」（P.4-12）
- 「ユーザ パラメータの設定」（P.4-13）
- 「IPS SSP パスワードの回復」（P.4-21）
- 「時刻の設定」（P.4-24）
- 「SSH の設定」（P.4-34）
- 「TLS の設定」（P.4-39）
- 「ライセンス キーのインストール」（P.4-42）

ネットワーク設定値の変更

（注） これらの設定値のほとんどは、**setup** コマンドを使用して IPS SSP を初期化した際に設定済みです。詳細については、第 3 章「IPS SSP の初期化」を参照してください。

IPS SSP を初期化した後、**setup** コマンドで設定したネットワーク設定値を変更することが必要になる場合があります。ここでは、ネットワーク設定値を変更する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。

- 「ホスト名の変更」（P.4-2）
- 「IP アドレス、ネットマスク、およびゲートウェイの変更」（P.4-3）
- 「Telnet のイネーブル化とディセーブル化」（P.4-4）

- 「アクセス リストの変更」（P.4-5）
- 「FTP タイムアウトの変更」（P.4-7）
- 「ログイン バナーの追加」（P.4-8）
- 「グローバル相関用の DNS サーバとプロキシ サーバの設定」（P.4-10）

ホスト名の変更

setup コマンドの実行を完了した後、サービス ホスト サブモードで **host-name** *host_name* コマンドを使用して、IPS SSP のホスト名を変更します。デフォルトは sensor です。

（注）　現在のセッションおよび他の既存のセッションの CLI プロンプトは、新しいホスト名に更新されません。それ以降の CLI ログイン セッションでは、プロンプトに新しいホスト名が反映されます。

IPS SSP ホスト名を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　IPS SSP ホスト名を変更します。

```
ips-ssp(config-hos-net)# host-name ips-ssp
```

ステップ 4　新しいホスト名を確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,255.255.0 default:
      192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 5　ホスト名をデフォルトの設定に戻すには、コマンドの **default** 形式を使用します。

```
ips-ssp(config-hos-net)# default host-name
```

ステップ 6　デフォルトのホスト名への変更を確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,255.255.0 default:
      192.168.1.2/24,192.168.1.1
      host-name: sensor <defaulted>
```

```
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

IP アドレス、ネットマスク、およびゲートウェイの変更

setup コマンドの実行を完了した後、サービス ホスト サブモードで **host-ip** *ip_address/netmask,default_gateway* コマンドを使用して IP アドレス、ネットマスク、およびデフォルト ゲートウェイを変更します。デフォルトは、192.168.1.2/24,192.168.1.1 です。

host-ip は、X.X.X.X/nn,Y.Y.Y.Y（IP アドレス / ネットマスク / ゲートウェイ）の形式になります。ここで、X.X.X.X は IPS SSP の IP アドレスを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです（X = 0 ～ 255）。nn はネットマスクのビット数を示します。Y.Y.Y.Y はデフォルト ゲートウェイを示し、ピリオドで区切られた 4 つのオクテットで記述される 32 ビット アドレスです（Y = 0 ～ 255）。

IP アドレス、ネットマスク、およびデフォルト ゲートウェイを変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　IP アドレス、ネットマスク、デフォルト ゲートウェイを変更します。

```
ips-ssp(config-hos-net)# host-ip 192.0.2.0/24255.255.255.0
```

（注）　デフォルト ゲートウェイは、IPS SSP の IP アドレスと同じサブネット内に存在する必要があります。存在しないと、IPS SSP からエラーが出力され、その設定変更は適用されません。

ステップ 4　新しい情報を確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.0.2.0/24255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
```

```
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
```

ステップ 5　この情報をデフォルトの設定に戻すには、コマンドの **default** 形式を使用します。

```
ips-ssp(config-hos-net)# default host-ip
```

ステップ 6　ホスト IP がデフォルトの 192.168.1.2/24,192.168.1.1 になっていることを確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.168.1.2/24,192.168.1.1 <defaulted>
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

Telnet のイネーブル化とディセーブル化

サービス ホスト サブモードで **telnet-option {enabled | disabled}** コマンドを使用して、IPS SSP へのリモート アクセス用に Telnet をイネーブルにします。デフォルトではディセーブルになっています。

注意　Telnet はセキュアなアクセス サービスではないため、デフォルトでは無効になっています。ただし、IPS SSP 上でセキュアなサービスである SSH が常時実行されています。

Telnet サービスをイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　Telnet サービスをイネーブルにします。

```
ips-ssp(config-hos-net)# telnet-option enabled
ips-ssp(config-hos-net)#
```

ステップ 4　Telnet がイネーブルに設定されたことを確認します。

```
ips-ssp(config-hos-net)# show settings
  network-settings
  ------------------------------------------------
    host-ip: 192.0.2.0/24,255.255.255.0
    default: 192.168.1.2/24,192.168.1.1
    host-name: ips-ssp default: sensor
    telnet-option: enabled default: disabled
    access-list (min: 0, max: 512, current: 1)
    ------------------------------------------------
       network-address: 0.0.0.0/0
       ------------------------------------------------
    ------------------------------------------------
    ftp-timeout: 300 seconds <defaulted>
    login-banner-text: <defaulted>
------------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 5　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

（注）　IPS SSP に Telnet 接続するには、Telnet をイネーブルにし、Telnet クライアントの接続を許可するアクセス リストを設定する必要があります。

詳細情報

アクセス リストの設定手順については、「アクセス リストの変更」（P.4-5）を参照してください。

アクセス リストの変更

サービス ホスト サブモードで **access-list** *ip_address/netmask* コマンドを使用して、アクセス リスト（IPS SSP へのアクセスを許可されるホストおよびネットワークのリスト）を設定します。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。デフォルトのアクセス リストは空です。

次のホストが、アクセス リストにエントリされている必要があります。

- IPS SSP に Telnet 接続する必要のあるホスト。
- IPS SSP との間で SSH を使用する必要のあるホスト。
- Web ブラウザから IPS SSP にアクセスする必要のあるホスト（IDM や IME など）。
- IPS SSP にアクセスする必要のある管理ステーション（CSM など）。
- IPS SSP がマスター ブロッキング センサーの場合、ブロッキング転送センサーの IP アドレスがリストにエントリされている必要があります。

アクセス リストを修正するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　エントリをアクセス リストに追加します。単一ホストのネットマスクは 32 です。

```
ips-ssp(config-hos-net)# access-list 10.89.146.110/32
```

ステップ 4　アクセス リストに行った変更を確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.168.1.2/24,192.168.1.1 <defaulted>
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      -----------------------------------------------
         network-address: 10.1.9.0/24
         -----------------------------------------------
         network-address: 10.89.146.110/32
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
```

ステップ 5　エントリをアクセス リストから削除します。

```
ips-ssp(config-hos-net)# no access-list 10.89.146.110/32
```

ステップ 6　エントリが削除されていることを確認します。リスト内にホストが存在しなくなります。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.168.1.2/24,192.168.1.1 <defaulted>
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 10.1.9.0/24
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 7　値をデフォルトに戻します。

```
ips-ssp(config-hos-net)# default access-list
```

ステップ 8　値がデフォルトに戻っていることを確認します。リスト内にはホストもネットワークも存在しなくなっています。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
```

```
      host-ip: 192.0.2.0/24,255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 9　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 10　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

FTP タイムアウトの変更

サービス ホスト サブモードで **ftp-timeout** コマンドを使用して、FTP タイムアウトの秒数を変更します。この秒数は、IPS SSP が FTP サーバと通信しているときに、FTP クライアントがタイムアウトするまでの待ち時間です。デフォルトは 300 秒です。

（注）　FTP クライアントは、FTP サーバからアップデートやコンフィギュレーション ファイルをダウンロードする際に使用できます。

FTP タイムアウトを変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　FTP タイムアウトの秒数を変更します。

```
ips-ssp(config-hos-net)# ftp-timeout 500
```

ステップ 4　FTP タイムアウトの変更を確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
       ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
    ------------------------------------------------
```

```
      ftp-timeout: 500 seconds default: 300
      login-banner-text: <defaulted>
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 5　値をデフォルトに戻します。

```
ips-ssp(config-hos-net)# default ftp-timeout
```

ステップ 6　値がデフォルトに戻っていることを確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.0.2.0/24,255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 0.0.0.0/0
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ログイン バナーの追加

login-banner-text *text_message* コマンドを使用して、ユーザのログイン時に表示されるログイン バナーを追加します。デフォルトはありません。メッセージ内で新しい行を開始するときは、Ctrl キーを押した状態で V キーを押し、Enter を押します。

ログイン バナーを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　バナー ログイン テキストを追加します。

```
ips-ssp(config-hos-net)# login-banner-text This is the banner login text message.
```

ステップ 4　バナー ログイン テキスト メッセージを確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
    ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: This is the banner login text message. default:
   ------------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 5　ログイン バナー テキストを削除するには、コマンドの **no** 形式を使用します。

```
ips-ssp(config-hos-net)# no login-banner-text
```

ステップ 6　ログイン テキストが削除されていることを確認します。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,255.255.255.0
      default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: default:
   ------------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

グローバル相関用の DNS サーバとプロキシ サーバの設定

ネットワーク設定サブモードで **http-proxy**、**dns-primary-server**、**dns-secondary-server**、および **dns-tertiary-server** コマンドを使用して、グローバル相関機能をサポートするようにサーバを設定します。

グローバル相関をサポートするために、HTTP プロキシ サーバか DNS サーバを設定する必要があります。ネットワーク内でプロキシを使用している場合は、グローバル相関更新をダウンロードするためにプロキシ サーバが必要な場合があります。DNS サーバを使用している場合は、グローバル相関更新が成功するために、少なくとも 1 台の到達可能な DNS サーバを設定する必要があります。その他の DNS サーバは、バックアップ サーバとして設定できます。DNS クエリーは、リスト内の最初のサーバに送信されます。そのサーバが到達不能の場合、DNS クエリーは、設定されている次の DNS サーバに送信されます。

注意　グローバル相関が動作するには、DNS サーバまたは HTTP プロキシ サーバが常時設定されている必要があります。

注意　DNS 解決は、グローバル相関更新サーバにアクセスするためにのみサポートされます。

オプション

次のオプションが適用されます。

- **http-proxy {no-proxy | proxy-sensor}**：HTTP プロキシ サーバを設定します。
  - **address** *ip_address*：HTTP プロキシ サーバの IP アドレスを指定します。
  - **port** *port_number*：HTTP プロキシ サーバのポート番号を指定します。
- **dns-primary-server {enabled | disabled}**：DNS プライマリ サーバをイネーブルにします。
  - **address** *ip_address*：DNS プライマリ サーバの IP アドレスを指定します。
- **dns-secondary-server {enabled | disabled}**：DNS セカンダリ サーバをイネーブルにします。
  - **address** *ip_address*：DNS セカンダリ サーバの IP アドレスを指定します。
- **dns-tertiary-server {enabled | disabled}**：DNS ターシャリ サーバをイネーブルにします。
  - **address** *ip_address*：DNS ターシャリ サーバの IP アドレスを指定します。

グローバル相関をサポートするように DNS サーバとプロキシ サーバを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク設定サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
```

ステップ 3　グローバル相関をサポートするようにプロキシ サーバまたは DNS サーバをイネーブルにします。

a.　プロキシ サーバをイネーブルにします。

```
ips-ssp(config-hos-net)# http-proxy proxy-server
ips-ssp(config-hos-net-pro)# address 10.10.10.1
ips-ssp(config-hos-net-pro)# port 65
ips-ssp(config-hos-net-pro)#
```

b. DNS サーバをイネーブルにします。

```
ips-ssp(config-hos-net)# dns-primary-server enabled
ips-ssp(config-hos-net-ena)# address 10.10.10.1
ips-ssp(config-hos-net-ena)#
```

ステップ 4　設定を確認できます。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 192.0.2.0/24,255.255.255.0 default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      -----------------------------------------------
         network-address: 0.0.0.0/0
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
      dns-primary-server
      -----------------------------------------------
         enabled
         -----------------------------------------------
            address: 10.10.10.1
         -----------------------------------------------
      -----------------------------------------------
      dns-secondary-server
      -----------------------------------------------
         disabled
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      dns-tertiary-server
      -----------------------------------------------
         disabled
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      http-proxy
      -----------------------------------------------
         proxy-server
         -----------------------------------------------
            address: 10.10.10.1
            port: 65
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-hos-net)#
```

ステップ 5　ネットワーク設定モードを終了します。

```
ips-ssp(config-hos-net)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

グローバル相関機能の詳細については、第 10 章「グローバル相関の設定」を参照してください。

Web サーバ設定の変更

setup コマンドを実行した後は、Web サーバ ポート、TLS 暗号化を使用するかどうか、HTTP サーバ ヘッダー メッセージといった Web サーバ設定を変更できます。

（注）　デフォルトの Web サーバ ポートは、TLS がイネーブルの場合は 443、TLS がディセーブルの場合は 80 です。

HTTP は、Web クライアントが Web サーバに要求を行う際に使用するプロトコルです。HTTP の仕様では、サーバは各応答において自身の識別情報を示す必要があります。攻撃者は、このプロトコル機能を悪用して偵察を行うことがあります。IPS Web サーバが自身の識別情報を示す際に不用意な応答を提供すると、攻撃者に IPS センサーの存在を知られるおそれがあります。

IPS センサーを装備していることを攻撃者に知られないようにすることを推奨します。特に Web サーバがインターネットからアクセス可能な場合は、情報を一切漏らさない内容に **server-id** を変更してください。

たとえば、ポートをファイアウォール越しに転送して、センサーをリモートでモニタできるようにする場合は、**server-id** を設定する必要があります。

Web サーバ設定を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　Web サーバ モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service web-server
```

ステップ 3　ポート番号を変更します。

```
ips-ssp(config-web)# port 8080
```

ポート番号をデフォルトの 443 から 8080 に変更すると、次のメッセージが表示されます。

```
Warning: The web server's listening port number has changed from 443 to 8080. This change
will not take effect until the web server is re-started
```

ステップ 4　TLS をイネーブルまたはディセーブルにします。

```
ips-ssp(config-web)# enable-tls {true | false}
```

TLS をディセーブルにすると、次のメッセージが表示されます。

```
Warning: TLS protocol support has been disabled. This change will not take effect until
the web server is re-started.
```

ステップ 5　HTTP サーバ ヘッダーを変更します。

```
ips-ssp(config-web)# server-id Nothing to see here. Move along.
```

ステップ 6　Web サーバの変更を確認します。

```
ips-ssp(config-web)# show settings
   enable-tls: true default: true
   port: 8001 default: 443
   server-id: Nothing to see here. Move along. default: HTTP/1.1 compliant
ips-ssp(config-web)#
```

ステップ 7　デフォルトに戻すには、各コマンドの **default** 形式を使用します。

```
ips-ssp(config-web)# default port
ips-ssp(config-web)# default enable-tls
ips-ssp(config-web)# default server-id
```

ステップ 8　デフォルトに置き換えられていることを確認します。

```
ips-ssp(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
   configurable-service (min: 0, max: 99, current: 1)
   -----------------------------------------------
      <protected entry>
      service-name: rdep-event-server
      -----------------------------------------------
         enabled: true default: false
         file-name: event-server <protected>
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-web)#
```

ステップ 9　Web サーバ サブモードを終了します。

```
ips-ssp(config-web)# exit
Apply Changes:?[yes]:
```

ステップ 10　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

（注）　ポートを変更する場合または TLS 設定をイネーブルにする場合は、Web サーバで新しい設定が使用されるように IPS SSP をリセットする必要があります。

詳細情報

IPS SSP をリセットする手順については、「IPS SSP のリロード、シャットダウン、リセット、および復旧」（P.18-9）を参照してください。

ユーザ パラメータの設定

ここでは、サービス アカウントの作成、ユーザの作成、パスワードの設定と回復、権限レベルの指定、およびユーザのリストの表示を行う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。

- 「ユーザの追加と削除」（P.4-14）
- 「サービス アカウントの作成」（P.4-16）
- 「パスワードの設定」（P.4-17）
- 「ユーザ権限レベルの変更」（P.4-17）
- 「ユーザ ステータスの表示」（P.4-18）
- 「パスワード ポリシーの設定」（P.4-19）
- 「アカウント ロッキングの設定」（P.4-20）

ユーザの追加と削除

ローカル システムでユーザを作成するには、**username** コマンドを使用します。新しいユーザの追加、権限レベル（administrator、operator、viewer）の設定、および新規ユーザのパスワードの設定を実行できます。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。これにより、CLI と Web アクセスからユーザが削除されます。

注意　**username** コマンドは、ログインだけを目的としてユーザ名とパスワードの認証を行います。システムにログインしているユーザの削除に、このコマンドは使用できません。自分をシステムから削除するために、このコマンドは使用できません。

パスワードを指定しないと、入力を要求されます。既存のユーザのパスワードを変更するには、**password** コマンドを使用します。既存のユーザの権限を変更するには、**privilege** コマンドを使用します。

ユーザ名はパターン ^[A-Za-z0-9()+:,_/-]+$ に従います。つまり、ユーザ名は必ず英字または数字から始まり、A ～ Z の任意の英字（大文字または小文字）、0 ～ 9 の任意の数字、および - と _ からなる 1 ～ 64 の文字で構成します。パスワードは、センサー管理者によって設定された要件を満たす必要があります。

無効なパスワードを作成すると、次のエラー メッセージが表示されます。

- `Error: setEnableAuthenticationTokenStatus : The password is too short.`
- `Error: setEnableAuthenticationTokenStatus : Failure setting the account's password: it does not contain enough DIFFERENT characters`

（注）　**privilege** コマンドを使用してユーザにサービス権限を与えることはできません。既存のユーザにサービス権限を与えるには、そのユーザを削除してから、**username** コマンドを使用してサービス アカウントを作成します。

ユーザを追加および削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　ユーザのパラメータを指定します。

```
ips-ssp(config)# username username password password privilege
administrator/operator/viewer
```

（注）　ユーザ名はパターン ^[A-Za-z0-9()+:,_/-]+$ に従います。つまり、ユーザ名は必ず英字または数字から始まり、A ～ Z の任意の英字（大文字または小文字）、0 ～ 9 の任意の数字、および - と _ からなる 1 ～ 64 の文字で構成します。パスワードは、センサー管理者によって設定された要件を満たす必要があります。

たとえば、ユーザ「tester」を管理者権限レベルとパスワード「testpassword」で追加するには、次のコマンドを入力します。

（注）　パスワードを平文で表示したくない場合は、パスワード プロンプトが表示されるのを待ちます。ユーザ名と権限を入力するときには、パスワードを入力しません。

```
ips-ssp(config)# username tester privilege administrator
Enter Login Password: ************
Re-enter Login Password: ************
ips-ssp(config)#
```

（注）　ユーザの権限レベルを指定しない場合、そのユーザにはデフォルトのビューア（viewer）権限が割り当てられます。

ステップ 4　ユーザが追加されていることを確認します。ユーザのリストが表示されます。

```
ips-ssp(config)# exit
ips-ssp# show users all
    CLI ID   User         Privilege
*   13491    cisco        administrator
             jsmith       operator
             jtaylor      service
             jroberts     viewer
ips-ssp#
```

ステップ 5　ユーザを削除するには、コマンドの **no** 形式を使用します。

```
ips-ssp# configure terminal
ips-ssp(config)# no username jsmith
```

（注）　このコマンドを使用して、システムから自分を削除することはできません。

ステップ 6　ユーザが削除されたことを確認します。ユーザ `jsmith` が削除されています。

```
ips-ssp(config)# exit
ips-ssp# show users all
    CLI ID   User         Privilege
*   13491    cisco        administrator
             jtaylor      service
             jroberts     viewer
ips-ssp#
```

詳細情報

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。

サービス アカウントの作成

トラブルシューティングの際に使用する TAC 用のサービス アカウントを作成できます。センサーには複数のユーザがアクセスできますが、センサーに対するサービス権限を持てるのは 1 人のユーザだけです。サービス アカウントは、サポートの目的のためにのみ使用します。

root ユーザのパスワードは、サービス アカウントが作成されたときにサービス アカウントのパスワードに同期化されます。root アクセス権限を取得するには、サービス アカウントでログインしてから、**su - root** コマンドで root ユーザに切り替わる必要があります。

注意　TAC の指示に基づく場合を除き、サービス アカウントを使用してセンサーに変更を加えないでください。サービス アカウントを使用してセンサーを設定すると、その設定は TAC のサポート対象外になります。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、他の IPS サービスの適切なパフォーマンスと機能に影響を及ぼします。TAC は、追加のサービスが加えられたセンサーをサポートしません。

注意　サービス アカウントを作成するかどうかは、慎重に検討してください。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。

サービス アカウントを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　サービス アカウントのパラメータを指定します。ユーザ名はパターン ^[A-Za-z0-9()+:,_/-]+$ に従います。つまり、ユーザ名は必ず英字または数字から始まり、A ～ Z の任意の英字（大文字または小文字）、0 ～ 9 の任意の数字、および - と _ からなる 1 ～ 64 の文字で構成します。

```
ips-ssp(config)# user username privilege service
```

ステップ 4　入力を要求されたらパスワードを指定します。パスワードは、センサー管理者によって設定された要件を満たす必要があります。この IPS SSP に対してサービス アカウントがすでに存在する場合は、次のエラー メッセージが表示され、サービス アカウントは作成されません。

```
Error: Only one service account may exist
```

ステップ 5　コンフィギュレーション モードを終了します。

```
ips-ssp(config)# exit
ips-ssp#
```

サービス アカウントを使用して CLI 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 reimaged to guarantee proper operation.
*************************************************************************************
```

パスワードの設定

password コマンドを使用して、ローカル センサー上のパスワードを更新します。このコマンドを使用して、既存のユーザのパスワードを変更したり、ロックされたアカウントのパスワードをリセットすることもできます。有効なパスワードの長さは 8 ～ 32 文字です。スペース以外のすべての文字を使用できます。

パスワードを変更するには、次の手順を実行します。

ステップ 1　他のユーザのパスワードを変更したり、ロックされたアカウントのパスワードをリセットするには、次の手順を実行します。

a. 管理者権限を持つアカウントを使用して CLI にログインします。

b. コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

c. 特定のユーザのパスワードを変更します。

```
ips-ssp(config)# password tester
Enter New Login Password: ******
Re-enter New Login Password: ******
```

（注） この例では、ユーザ「tester」のパスワードを変更します。

ステップ 2　自分のパスワードを変更するには、次の手順を実行します。

a. CLI にログインします。

b. コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

c. 自分のパスワードを変更します。

```
ips-ssp(config)# password
Enter Old Login Password:************
Enter New Login Password: ************
Re-enter New Login Password: ************
```

ユーザ権限レベルの変更

privilege コマンドを使用して、ユーザの権限レベル（administrator、operator、viewer）を変更します。

（注） **privilege** コマンドを使用してユーザにサービス権限を与えることはできません。既存のユーザにサービス権限を与えるには、そのユーザを削除してから、**username** コマンドを使用してサービス アカウントを作成します。サービス権限を持つことができるのは 1 人だけです。

ユーザの権限レベルを変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ユーザ *jsmith* の現在の権限を確認します。

```
ips-ssp# show users all
    CLI ID   User       Privilege
*   13491    cisco      administrator
             jsmith     viewer
             operator   operator
             service    service
             viewer     viewer
ips-ssp#
```

ステップ 3　権限レベルをビューア（viewer）からオペレータ（operator）に変更します。

```
ips-ssp# configure terminal
ips-ssp(config)# privilege user jsmith operator
Warning: The privilege change does not apply to current CLI sessions. It will be applied
to subsequent logins.
ips-ssp(config)#
```

ステップ 4　ユーザの権限が変更されていることを確認します。ユーザ `jsmith` の権限が `viewer` から `operator` に変更されています。

```
ips-ssp(config)# exit
ips-ssp# show users all

    CLI ID   User       Privilege
*   13491    cisco      administrator
             jsmith     operator
             operator   operator
             service    service
             viewer     viewer
ips-ssp#
```

ステップ 5　自分の現在の権限レベルを表示します。

```
ips-ssp# show privilege
Current privilege level is administrator
```

詳細情報

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。

ユーザ ステータスの表示

show users コマンドを使用して、センサーにログインしているすべてのユーザのユーザ名と権限に関する情報を表示します。また、ログイン ステータスに関係なくセンサー上のすべてのユーザ アカウントに関する情報も表示します。* により、現在のユーザが示されます。アカウントがロックされていると、そのユーザ名はカッコで囲まれます。ロックされているアカウントとは、ユーザが正しいパスワードの入力に、設定された試行回数を超えて失敗したことを意味します。

（注）　すべての IPS プラットフォームで、同時に 10 個のログイン セッションを利用できます。

ユーザ情報を表示するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　IPS SSP にログインしているユーザを確認します。

```
ips-ssp# show users
    CLI ID   User       Privilege
*   13491    cisco      administrator
ips-ssp#
```

ステップ 3　すべてのユーザを確認します。ユーザ jsmith のアカウントがロックされています。

```
ips-ssp# show users all
    CLI ID    User        Privilege
*   13491     cisco       administrator
    5824     (jsmith)     viewer
    9802     tester       operator
ips-ssp#
```

ステップ 4　jsmith のアカウントのロックを解除するには、パスワードをリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# password jsmith
Enter New Login Password: ******
Re-enter New Login Password: ******
```

パスワード ポリシーの設定

センサー管理者として、パスワードの作成方法を設定できます。ユーザが作成したすべてのパスワードは、管理者がセットアップしたポリシーに従う必要があります。たとえば、10 文字以上 40 文字以下のパスワードで、少なくとも 2 つの大文字と 2 つの数字が含まれていなければならないというポリシーを設定できます。パスワード ポリシーが設定された後は、各ユーザ アカウントに設定されているすべてのパスワードがこのパスワード ポリシーに従う必要があります。

ログインの試行回数およびパスワードのサイズと最小文字数の要件を設定できます。パスワードの最小文字数は 8 です。パスワードを忘れた場合は、センサー プラットフォームに応じたさまざまな方法でパスワードを回復できます。

注意　パスワード ポリシーに文字セット（大文字や数字など）の最小数を含める場合、必要な文字セットの最小数の合計が最小パスワード サイズを超えることはできません。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

パスワード ポリシーをセットアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　パスワード強度の認証サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service authentication
ips-ssp(config-aut)# password-strength
```

ステップ 3　パスワードに含めなければならない、数字の最小文字数を設定します。範囲は 0 ～ 64 です。

```
ips-ssp(config-aut-pas)# digits-min 6
```

ステップ 4　パスワードに含めなければならない、英数字以外の印刷可能文字の最小文字数を設定します。範囲は 0 ～ 64 です。

```
ips-ssp(config-aut-pas)# other-min 3
```

ステップ 5　パスワードに含めなければならない、大文字の英字の最小文字数を設定します。範囲は 0 ～ 64 です。

```
ips-ssp(config-aut-pas)# uppercase-min 3
```

ステップ 6　パスワードに含めなければならない、小文字の英字の最小文字数を設定します。

```
ips-ssp(config-aut-pas)# lowercase-min 3
```

ステップ 7　アカウントごとに記憶される古いパスワードの数を設定します。新しいパスワードは、アカウントのこれらの古いパスワードのいずれとも一致することはできません。

```
ips-ssp(config-aut-pas)# number-old-passwords 3
```

ステップ 8　新しい設定を確認します。

```
ips-ssp(config-aut-pas)# show settings
   password-strength
   -----------------------------------------------
      size: 8-64 <defaulted>
      digits-min: 6 default: 0
      uppercase-min: 3 default: 0
      lowercase-min: 3 default: 0
      other-min: 3 default: 0
      number-old-passwords: 3 default: 0
   -----------------------------------------------
ips-ssp(config-aut-pas)#
```

アカウント ロッキングの設定

認証サブモードで **attemptLimit** *number* コマンドを使用して、一定回数の試行失敗後にユーザがログインを試行できなくなるようにアカウントをロックします。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。

アカウント ロッキングを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス認証サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service authentication
```

ステップ 3　ユーザがアカウントにログインするために実行可能な試行回数を設定します。

```
ips-ssp(config-aut)# attemptLimit 3
```

ステップ 4　新しい設定を確認します。

```
ips-ssp(config-aut)# show settings
    attemptLimit: 3 defaulted: 0
ips-ssp(config-aut)#
```

ステップ 5　値をシステムのデフォルト設定に戻します。

```
ips-ssp(config-aut)# default attemptLimit
```

ステップ 6　設定がデフォルトに戻っていることを確認します。

```
ips-ssp(config-aut)# show settings
    attemptLimit: 0 <defaulted>
ips-ssp(config-aut)#
```

ステップ 7　アカウントがロックされているユーザがいるかどうかを確認します。ユーザ jsmith は、カッコで囲まれているので、アカウントがロックされています。

（注） attemptLimit が非ゼロの値になっている設定を適用すると、SSH サーバで変更が行われ、センサーとの接続に問題が発生する可能性があります。attemptLimit が非ゼロの場合、SSH サーバは、クライアントがチャレンジ/レスポンス認証をサポートすることを要求します。SSH クライアントが接続した後、パスワードが要求される前に問題が発生する場合は、チャレンジ/レスポンス認証をイネーブルにする必要があります。手順については、SSH クライアントのマニュアルを参照してください。

```
ips-ssp(config-aut)# exit
ips-ssp(config)# exit
ips-ssp# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     (jsmith)   viewer
    9802     tester     operator
```

ステップ 8　jsmith のアカウントのロックを解除するには、パスワードをリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# password jsmith
Enter New Login Password: ******
Re-enter New Login Password: ******
```

IPS SSP パスワードの回復

ここでは、IPS SSP のパスワードを回復する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。

- 「IPS SSP パスワードの回復」（P.4-22）
- 「パスワード回復のディセーブル化」（P.4-22）
- 「パスワード回復の状態の確認」（P.4-23）
- 「パスワード回復のトラブルシューティング」（P.4-24）

IPS SSP パスワードの回復

（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。

CLI または ASDM を使用して IPS SSP のパスワードをデフォルト（**cisco**）にリセットできます。パスワードをリセットすると、IPS SSP がリブートします。リブート中は、IPS サービスを使用できません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、ROMMON confreg ビットを 0x7 に設定してから、IPS SSP をリブートします。この ROMMON ビットにより、GRUB メニューがデフォルトでオプション 2（**パスワードのリセット**）になります。

指定したスロット内のモジュールに搭載されている IPS のバージョンがパスワード回復をサポートしていない場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーから、[Tools] > [IPS Password Reset] を選択します。

（注）　このオプションは、IPS モジュールがインストールされていなければ表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで、[OK] をクリックしてパスワードをデフォルト（**cisco**）にリセットします。ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットに失敗した場合は、ASA と IPS SSP に正しいソフトウェアが搭載されていることを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。IPS SSP がリブートします。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブルになっている IPS SSP 上でパスワード回復を試みた場合、プロセスはエラーも警告も出力せずに進行しますが、パスワードはリセットされません。パスワードを忘れたため IPS SSP にログインできない場合、パスワード回復がディセーブルに設定されていると、IPS SSP のイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。CLI、IDM、または IME を使用してパスワード回復をディセーブルにできます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
ips-ssp# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
ips-ssp(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
ips-ssp(config-hos)# password-recovery disallowed
```

IDM または IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用し、IDM または IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復の状態の確認

show settings | **include password** コマンドを使用して、パスワード回復がイネーブルかどうかを確認します。

パスワード回復がイネーブルかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp (config)# service host
ips-ssp (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタリングされた出力で設定を表示することにより、パスワード回復の状態を確認します。

```
ips-ssp(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
ips-ssp(config-hos)#
```

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行うときは、次の点に注意します。

- ROMMON プロンプト、GRUB メニュー、スイッチ CLI、またはルータ CLI からは、センサー設定内でパスワード回復がディセーブルになっているかどうかを判別できません。パスワード回復を試みると、常に成功しているように見えます。ディセーブルになっていた場合、パスワードは **cisco** にリセットされません。この場合、センサーのイメージを再作成するしか方法はありません。
- パスワード回復は、ホスト設定でディセーブルにできます。外部メカニズムを使用するプラットフォームの場合、コマンドを実行してパスワードをクリアすることができますが、IPS でパスワード回復がディセーブルになっていると、IPS は、パスワード回復が許可されていないことを検出し、外部からの要求を拒否します。
- パスワード回復の状態を確認するには、**show settings | include password** コマンドを使用します。

時刻の設定

ここでは、IPS SSP に信頼できる時刻源を用意することの重要性について説明します。次のような構成になっています。

- 「時刻源と IPS SSP」（P.4-24）
- 「IPS SSP のクロックと適応型セキュリティ アプライアンスのクロックの同期化」（P.4-25）
- 「IPS SSP 上の時刻の修正」（P.4-25）
- 「IPS SSP 上の時刻の設定」（P.4-25）
- 「NTP の設定」（P.4-31）

時刻源と IPS SSP

IPS SSP には、信頼できる時刻源が必要です。すべてのイベント（アラート）に、正しい UTC と現地時間のタイムスタンプが必要です。正確なタイムスタンプがないと、攻撃の後でログを正しく分析できません。IPS SSP を初期化するとき、時間帯とサマータイム設定をセットアップします。IPS SSP 上の時刻を設定する方法は 2 つあります。

- IPS SSP が、自身のクロックを、自身を搭載している適応型セキュリティ アプライアンスのクロックと自動的に同期します。これがデフォルトです。
- 時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように IPS SSP を設定できます。

（注） NTP サーバを使用することを推奨します。認証済みまたは未認証の NTP を使用できます。認証済みの NTP の場合、NTP サーバの IP アドレス、NTP サーバのキー ID、および NTP サーバのキー値が必要です。初期化時に NTP をセットアップすることも、CLI、IDM、IME、または ASDM を使用して NTP を設定することもできます。

IPS SSP のクロックと適応型セキュリティ アプライアンスのクロックの同期化

IPS SSP は、起動するたびに、および親シャーシ（適応型セキュリティ アプライアンス）のクロックが設定されるたびに、自身のシステム クロックを適応型セキュリティ アプライアンスのクロックに同期します。IPS SSP のクロックと適応型セキュリティ アプライアンスのクロックの間では、時間の経過とともに時刻がずれていく傾向があります。この差は、1 日で数秒になることがあります。この問題を回避するには、IPS SSP のクロックと適応型セキュリティ アプライアンスのクロックの両方を外部の NTP サーバに同期させます。IPS SSP のクロックのみ、あるいは適応型セキュリティ アプライアンス シャーシのクロックのみを NTP サーバに同期させた場合は、時刻のずれが発生します。

IPS SSP 上の時刻の修正

保存されているイベントには、その作成時刻がタイムスタンプとして記録されるため、時刻の設定に誤りがあると、それらのイベントに対しても誤った時刻が記録されます。イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。元のセンサーのセットアップ時に、8:00 a.m. と指定すべきところを誤って 8:00 p.m. と指定した場合、それを修正すると、修正後の時刻は現在よりさかのぼった時刻に設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中に IPS SSP を中部時間に設定し、さらにサマータイムをイネーブルにした場合、現地時間が 8:04 p.m. であれば、時刻は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。この場合、時刻を 9:00 a.m. に変更すれば、時計は 09:01:33 CDT と表示されます。ただし、UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。ここにタイムスタンプの問題が生じる原因があります。

イベント レコードのタイムスタンプの整合性を確保するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブをクリアする必要があります。

（注）　イベントは、個別には削除できません。

IPS SSP 上の時刻の設定

ここでは、イベントにタイムスタンプが正しく付けられるように、IPS SSP 上の時刻を設定する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。

- 「システム クロックの表示」（P.4-26）
- 「繰り返しサマータイム設定の設定」（P.4-26）
- 「非繰り返しサマータイム設定の設定」（P.4-28）
- 「時間帯設定の設定」（P.4-30）

システム クロックの表示

show clock [**detail**] コマンドを使用して、システム クロックを表示します。**detail** オプションを使用すると、クロック ソース（NTP またはシステム）と現在のサマータイム設定（設定されている場合）を表示できます。システム クロックは、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックがタイミング ソース（NTP など）によって設定されている場合は、このフラグが設定されます。

表 4-1 に、システム クロック フラグを示します。

表 4-1　システム クロック フラグ

記号	説明
*	時刻は信頼できません。
（空白）	時刻は信頼できます。
.	時刻は信頼できますが、NTP と同期していません。

システム クロックを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
ips-ssp# show clock
*19:04:52 UTC Thu Apr 03 2008
```

ステップ 3　システム クロックを詳細表示します。次の例は、IPS SSP が時刻を NTP から取得し、設定と同期化が行われていることを示しています。

```
ips-ssp# show clock detail
20:09:43 UTC Thu Apr 03 2008
Time source is NTP
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

次の例は、時刻源が設定されていないことを示しています。

```
ips-ssp# show clock detail
*20:09:43 UTC Thu Apr 03 2008
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

繰り返しサマータイム設定の設定

（注）　サマータイムとは、日光節約時間を表す用語です。

summertime-option recurring コマンドを使用して、サマータイム設定に繰り返し切り替わるように IPS SSP を設定します。デフォルトは recurring です。

サマータイム設定に繰り返し切り替わるように IPS SSP を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サマータイムの繰り返しサブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# summertime-option recurring
```

ステップ 3　サマータイムの開始のサブモードを開始します。

```
ips-ssp(config-hos-rec)# start-summertime
```

ステップ 4　サマータイムの開始のパラメータを設定します。

a. サマータイム設定を開始する週の曜日を入力します。

```
ips-ssp(config-hos-rec-sta)# day-of-week monday
```

b. サマータイム設定を開始する月を入力します。

```
ips-ssp(config-hos-rec-sta)# month april
```

c. サマータイム設定を開始する日の時刻を入力します。形式は hh:mm:ss です。

```
ips-ssp(config-hos-rec-sta)# time-of-day 12:00:00
```

d. サマータイム設定を開始する月の週を入力します。値は、first ～ fifth、あるいは last です。

```
ips-ssp(config-hos-rec-sta)# week-of-month first
```

e. 設定値を確認します。

```
ips-ssp(config-hos-rec-sta)# show settings
   start-summertime
   -----------------------------------------------
      month: april default: april
      week-of-month: first default: first
      day-of-week: monday default: sunday
      time-of-day: 12:00:00 default: 02:00:00
   -----------------------------------------------
ips-ssp(config-hos-rec-sta)#
```

ステップ 5　サマータイムの終了のサブモードを開始します。

```
ips-ssp(config-hos-rec-sta)# exit
ips-ssp(config-hos-rec)# end-summertime
```

ステップ 6　サマータイムの終了のパラメータを設定します。

a. サマータイム設定を終了する週の曜日を入力します。

```
ips-ssp(config-hos-rec-end)# day-of-week friday
```

b. サマータイム設定を終了する月を入力します。

```
ips-ssp(config-hos-rec-end)# month october
```

c. サマータイム設定を終了する日の時刻を入力します。形式は hh:mm:ss です。

```
ips-ssp(config-hos-rec-end)# time-of-day 05:15:00
```

d. サマータイム設定を終了する月の週を入力します。値は、first ～ fifth、あるいは last です。

```
ips-ssp(config-hos-rec-end)# week-of-month last
```

e. 設定値を確認します。

```
ips-ssp(config-hos-rec-end)# show settings
   end-summertime
   -----------------------------------------------
      month: october default: october
      week-of-month: last default: last
      day-of-week: friday default: sunday
      time-of-day: 05:15:00 default: 02:00:00
   -----------------------------------------------
ips-ssp(config-hos-rec-end)#
```

ステップ 7　サマータイム中に使用されるローカルの時間帯を指定します。

```
ips-ssp(config-hos-rec-end)# exit
ips-ssp(config-hos-rec)# summertime-zone-name CDT
```

ステップ 8　オフセットを指定します。

```
ips-ssp(config-hos-rec)# offset 60
```

ステップ 9　設定値を確認します。

```
ips-ssp(config-hos-rec)# show settings
   recurring
   -----------------------------------------------
      offset: 60 minutes default: 60
      summertime-zone-name: CDT
      start-summertime
      -----------------------------------------------
         month: april default: april
         week-of-month: first default: first
         day-of-week: monday default: sunday
         time-of-day: 12:00:00 default: 02:00:00
      -----------------------------------------------
      end-summertime
      -----------------------------------------------
         month: october default: october
         week-of-month: last default: last
         day-of-week: friday default: sunday
         time-of-day: 05:15:00 default: 02:00:00
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 10　繰り返しサマータイム サブモードを終了します。

```
ips-ssp(config-hos-rec)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

非繰り返しサマータイム設定の設定

（注）　サマータイムとは、日光節約時間を表す用語です。

summertime-option non-recurring コマンドを使用して、サマータイム設定に一度だけ切り替わるように IPS SSP を設定します。デフォルトは recurring です。

サマータイム設定に一度だけ切り替わるように IPS SSP を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サマータイムの非繰り返しサブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# summertime-option non-recurring
```

ステップ 3　サマータイムの開始のサブモードを開始します。

```
ips-ssp(config-hos-non)# start-summertime
```

ステップ 4　サマータイムの開始のパラメータを設定します。

a. サマータイム設定を開始する日付を入力します。形式は yyyy-mm-dd です。

```
ips-ssp(config-hos-non-sta)# date 2004-05-15
```

b. サマータイム設定を開始する時刻を入力します。形式は hh:mm:ss です。

```
ips-ssp(config-hos-non-sta)# time 12:00:00
```

c. 設定値を確認します。

```
ips-ssp(config-hos-non-sta)# show settings
   start-summertime
   -----------------------------------------------
      date: 2004-05-15
      time: 12:00:00
   -----------------------------------------------
ips-ssp(config-hos-non-sta)#
```

ステップ 5　サマータイムの終了のサブモードを開始します。

```
ips-ssp(config-hos-non-sta)# exit
ips-ssp(config-hos-non)# end-summertime
```

ステップ 6　サマータイムの終了のパラメータを設定します。

a. サマータイム設定を終了する日付を入力します。形式は yyyy-mm-dd です。

```
ips-ssp(config-hos-non-end)# date 2004-10-31
```

b. サマータイム設定を終了する時刻を入力します。形式は hh:mm:ss です。

```
ips-ssp(config-hos-non-end)# time 12:00:00
```

c. 設定値を確認します。

```
ips-ssp(config-hos-non-end)# show settings
   end-summertime
   -----------------------------------------------
      date: 2004-10-31
      time: 12:00:00
   -----------------------------------------------
ips-ssp(config-hos-non-end)#
```

ステップ 7　サマータイム中に使用されるローカルの時間帯を指定します。

```
ips-ssp(config-hos-non-end)# exit
ips-ssp(config-hos-non)# summertime-zone-name CDT
```

ステップ 8　オフセットを指定します。

```
ips-ssp(config-hos-non)# offset 60
```

ステップ 9　設定値を確認します。

```
ips-ssp(config-hos-non)# show settings
   non-recurring
   -----------------------------------------------
      offset: 60 minutes default: 60
      summertime-zone-name: CDT
      start-summertime
      -----------------------------------------------
         date: 2004-05-15
         time: 12:00:00
      -----------------------------------------------
      end-summertime
      -----------------------------------------------
         date: 2004-10-31
         time: 12:00:00
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-hos-non)#
```

ステップ 10　非繰り返しサマータイム サブモードを終了します。

```
ips-ssp(config-hos-non)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

時間帯設定の設定

time-zone-settings コマンドを使用して、IPS SSP 上の時間帯設定を設定します（サマータイム設定の効果がないときに IPS SSP が表示する時間帯名、オフセットなど）。

IPS SSP 上の時間帯設定を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　時間帯設定サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# time-zone-settings
```

ステップ 3　サマータイム設定の効果がないときに常に表示される時間帯名を設定します。デフォルトは UTC です。

```
ips-ssp(config-hos-tim)# standard-time-zone-name CST
```

ステップ 4　オフセットを分単位で設定します。このオフセットは、現地時間を得るために UTC に加算される分数です。デフォルトは 0 です。

```
ips-ssp(config-hos-tim)# offset -360
```

ステップ 5　設定値を確認します。

```
ips-ssp(config-hos-tim)# show settings
   time-zone-settings
   -----------------------------------------------
      offset: -360 minutes default: 0
      standard-time-zone-name: CST default: UTC
   -----------------------------------------------
```

```
ips-ssp(config-hos-tim)#
```

ステップ 6　時間帯設定サブモードを終了します。

```
ips-ssp(config-hos-tim)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

NTP の設定

ここでは、NTP サーバとして Cisco ルータを設定する方法と、時刻源として NTP サーバを使用するように IPS SSP を設定する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。

- 「Cisco ルータを NTP サーバにする設定」（P.4-31）
- 「センサーで NTP 時刻源を使用するための設定」（P.4-32）

Cisco ルータを NTP サーバにする設定

センサーが NTP サーバを時刻源として使用するためには、センサーと NTP サーバの間に認証済みの接続が必要です。センサーがキーの暗号化のためにサポートしているのは、MD5 ハッシュ アルゴリズムのみです。Cisco ルータが NTP サーバとして動作するようにし、その内部クロックを時刻源として使用するには、次の手順を使用します。

注意　センサーの NTP 機能は、NTP サーバとして動作している Cisco ルータと適合するように設計されています。センサーは、その他の NTP サーバと連携できる可能性もありますが、それに関するテストやサポートは行われていません。

（注）　NTP サーバのキー ID とキー値を手元に用意してください。NTP サーバを時刻源として使用するようにセンサーを設定する際に、NTP サーバの IP アドレスと共に必要になります。

Cisco ルータが NTP サーバとして動作するように設定するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
router# configure terminal
```

ステップ 3　キー ID とキー値を作成します。キー ID は、1 から 65535 までの数値です。キー値はテキスト（数字または文字）です。後で暗号化されます。

```
router(config)# ntp authentication-key key_ID md5 key_value
```

例

```
router(config)# ntp authentication-key 100 md5 attack
```

（注）　センサーがサポートするのは MD5 キーのみです。

（注）　すでにルータにキーが存在する場合もあります。他のキーを確認するには、**show running configuration** コマンドを使用します。これらの値は、信頼できるキーとしてステップ 4 で使用されます。

ステップ 4　ステップ 3 で作成したキーを信頼できるキーとして指定（または既存のキーを使用）します。信頼できるキーの ID は、ステップ 3 のキー ID と同じ数値です。

```
router(config)# ntp trusted-key key_ID
```

例

```
router(config)# ntp trusted-key 100
```

ステップ 5　センサーが通信するルータ上のインターフェイスを指定します。

```
router(config)# ntp source interface_name
```

例

```
router(config)# ntp source FastEthernet 1/0
```

ステップ 6　センサーに割り当てる NTP マスター ストラタム番号を指定します。NTP マスター ストラタム番号は、NTP 階層におけるサーバの相対的な位置を示します。1 から 15 までの番号を選択できます。どの番号を選択するかは、センサーに対して重要ではありません。

```
router(config)# ntp master stratum_number
```

例

```
router(config)# ntp master 6
```

センサーで NTP 時刻源を使用するための設定

センサーには、安定した時刻源が必要です。NTP サーバを使用することを推奨します。センサーが NTP サーバを時刻源として使用するように設定するには、次の手順を使用します。認証済みまたは未認証の NTP を使用できます。

（注）　認証済みの NTP の場合、NTP サーバの IP アドレス、NTP サーバのキー ID、および NTP サーバのキー値が必要です。

注意　センサーの NTP 機能は、NTP サーバとして動作している Cisco ルータと適合するように設計されています。センサーは、その他の NTP サーバと連携できる可能性もありますが、それに関するテストやサポートは行われていません。

センサーが NTP サーバを時刻源として使用するように設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　サービス ホスト モードを開始します。

```
ips-ssp(config)# service host
```

ステップ 4　未認証の NTP を設定します。

a. NTP コンフィギュレーション モードを開始します。

```
ips-ssp(config-hos)# ntp-option enabled-ntp-unauthenticated
```

b. NTP サーバの IP アドレスを指定します。

```
ips-ssp(config-hos-ena)# ntp-server ip_address
```

c. 未認証の NTP の設定を確認します。

```
ips-ssp(config-hos-ena)# show settings
   enabled-ntp-unauthenticated
   -----------------------------------------------
      ntp-server: 10.89.147.45
   -----------------------------------------------
ips-ssp(config-hos-ena)#
```

ステップ 5　認証済みの NTP を設定します。

a. NTP コンフィギュレーション モードを開始します。

```
ips-ssp(config-hos)# ntp-option enable
```

b. NTP サーバの IP アドレスとキー ID を指定します。キー ID は、1 から 65535 までの数値です。これは、NTP サーバで設定済みのキー ID です。

```
ips-ssp(config-hos-ena)# ntp-servers ip_address key-id key_ID
```

例

```
ips-ssp(config-hos-ena)# ntp-servers 10.16.0.0 key-id 100
```

c. キー値の NTP サーバを指定します。キー値はテキスト（数字または文字）です。これは、NTP サーバで設定済みのキー値です。

```
ips-ssp(config-hos-ena)# ntp-keys key_ID md5-key key_value
```

例

```
ips-ssp(config-hos-ena)# ntp-keys 100 md5-key attack
```

d. NTP の設定を確認します。

```
ips-ssp(config-hos-ena)# show settings
   enabled
   -----------------------------------------------
      ntp-keys (min: 1, max: 1, current: 1)
      -----------------------------------------------
         key-id: 100
         -----------------------------------------------
            md5-key: attack
         -----------------------------------------------
      -----------------------------------------------
      ntp-servers (min: 1, max: 1, current: 1)
      -----------------------------------------------
         ip-address: 10.16.0.0
         key-id: 100
      -----------------------------------------------
-----------------------------------------------
ips-ssp(config-hos-ena)#
```

ステップ 6　NTP コンフィギュレーション モードを終了します。

```
ips-ssp(config-hos-ena)# exit
ips-ssp(config-hos)# exit
Apply Changes:?[yes]
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

SSH の設定

ここでは、IPS SSP 上の SSH について説明します。次のような構成になっています。

- 「SSH について」（P.4-34）
- 「SSH 既知ホスト リストへのホストの追加」（P.4-35）
- 「SSH 認証公開キーの追加」（P.4-36）
- 「新しい SSH サーバ キーの生成」（P.4-38）

SSH について

SSH は、セキュアでないチャネル上に強力な認証とセキュアな通信を実現します。SSH は、センサーへの接続を暗号化するとともに、正しいセンサーに接続していることを検証できるようにキーを提供します。また、SSH は、センサーがブロッキングのために接続する他のデバイスへの認証済みかつ暗号化されたアクセスも提供します。

SSH は、次の一方または両方を使用してホストまたはネットワークを認証します。

- パスワード
- ユーザ RSA 公開キー

SSH は、次の攻撃を防ぎます。

- IP スプーフィング：リモート ホストが、別の信頼できるホストから発信したかのように偽装したパケットを送信します。

（注）　SSH は、外部へのルータになりすますことのできるローカル ネットワーク上のスプーファさえも防ぎます。

- IP 送信元ルーティング：ホストが、別の信頼できるホストから発信したかのように IP パケットを偽装します。
- DNS スプーフィング：攻撃者がネーム サーバ レコードを偽造します。
- 中継ホストによる平文のパスワードおよびその他のデータの傍受。
- 中継ホストの管理者によるデータの改ざん。
- X 認証データの傍受と X11 サーバへの偽装接続をベースとした攻撃。

（注）　SSH は、パスワードを平文で送信することはありません。

SSH 既知ホスト リストへのホストの追加

センサーが SSH を通じて通信できるホストを認識できるようにするために、ホストを SSH 既知ホスト リストに追加する必要があります。このホストは、アップグレードやファイル コピーのためにセンサーが接続する必要のある SSH サーバと、センサーがブロッキングのために接続する Cisco ルータ、PIX Firewall、Catalyst スイッチなどのその他のホストです。

ssh host-key *ip-address* [*key-modulus-length public-exponent public-modulus*] コマンドを使用して、既知ホスト リストにエントリを追加します。係数、指数、および長さの値がわからない場合は、システムが、要求された IP アドレスの MD5 フィンガープリントと Bubble Babble を表示します。その後、キーをリストに追加するように選択できます。

注意　**ssh host-key** *ip-address* コマンドを使用した場合、指定した IP アドレスにある SSH サーバに接続して、必要なキーがネットワーク経由で取得されます。指定したホストは、コマンドを発行するときにアクセス可能な状態でなければなりません。ホストが到達不能な場合は、フル形式のコマンド（**ssh host-key** *ip-address* [*key-modulus-length public-exponent public-modulus*]）を使用して、攻撃者のキーを受け入れてしまうことを防ぐために表示されたキーのフィンガープリントを確認する必要があります。

（注）　IP アドレスのキーを修正するには、エントリを削除し、再作成する必要があります。エントリを削除するには、コマンドの **no** 形式を使用します。

ホストを SSH 既知ホスト リストに追加するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　エントリを既知ホスト リストに追加します。MD5 フィンガープリントが表示されます。既知ホスト リストに追加するかどうかを確認するプロンプトが表示されます。

```
ips-ssp(config)# ssh host-key 10.16.0.0
MD5 fingerprint is F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble is xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
Would you like to add this to the known hosts table for this host?[yes]
```

コマンドを発行したときにホストがアクセス不能な状態になっていると、次のメッセージが表示されます。

```
Error: getHostSshKey : socket connect failed [4,111]
```

ステップ 4　**yes** を入力して、フィンガープリントを既知ホスト リストに追加します。

ステップ 5　ホストが追加されたことを確認します。

```
ips-ssp(config)# exit
ips-ssp# show ssh host-keys
10.89.146.110
```

ステップ 6　特定の IP アドレスのキーを表示します。

```
ips-ssp# show ssh host-keys 10.16.0.0
1024 35
139306213541835240385332922253968814685684523520114131997839905113640120217816869696708721
704631322844292073851730565044879082670677554157937058485203995572114631296604552161309712
601068614812749969593513740598331393154884988302302182922353335152653860589163651944997842
874583627883277460138506084043415861927
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
ips-ssp#
```

ステップ 7　エントリを削除します。

```
ips-ssp(config)# no ssh host-key 10.16.0.0
```

ステップ 8　ホストが削除されたことを確認します。IP アドレスがリストに表示されなくなります。

```
ips-ssp(config)# exit
ips-ssp# show ssh host-keys
```

SSH 認証公開キーの追加

ssh authorized-key コマンドを使用して、RSA 認証によるローカル SSH サーバへのログインが許可されるクライアント用の公開キーを定義します。認証キーを修正するには、エントリを削除し、再作成する必要があります。エントリを削除するには、コマンドの **no** 形式を使用します。ユーザは、自分のキーの作成と削除しかできません。

オプション

次のオプションが適用されます。

- *id* : 認証キーを一意に識別する 1 ～ 256 文字の文字列。数字、「_」、および「-」を使用できますが、スペースと「?」は使用できません。
- *key-modulus-length* : 511 ～ 2048 の範囲内の ASCII 10 進数。
- *public-exponent* : 3 ～ 2^32 の範囲内の ASCII 10 進数。
- *public-modulus* : (2^(key-modulus-length - 1)) < x < (2^(key-modulus-length)) となる ASCII 10 進数 *x*。

センサーにログインできるユーザごとに、認証公開キーのリストが存在します。対応する RSA 秘密キーのいずれかにアクセスできる SSH クライアントは、パスワードを入力しなくてもユーザとしてセンサーにログインできます。

公開キーの定義には、秘密キーを保存するクライアントで RSA キー生成ツールを使用します。その後、生成された公開キーを一連の 3 つの数字（係数の長さ、公開指数、公開係数）で表示し、それらの数字を **ssh authorized-key** コマンドのパラメータとして入力します。

（注）　自分の SSH 認証キーのリストは自分で設定します。管理者は、センサー上の他のユーザの SSH 認証キーのリストを管理できません。

（注）　SSH 認証キーでは、秘密キーが適切に保護されていれば、パスワードよりもセキュリティが向上します。ベスト プラクティスは、秘密キーをそれが使用されるのと同じホスト上で作成し、パス フレーズと一緒にローカル ファイル システム上に保管することです。パスワードまたはパス フレーズの入力要求を最小限に抑えるには、キー エージェントを使用します。

SSH キーの追加

現在のユーザの SSH 認証キー リストにキー エントリを追加するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在のユーザの認証キー リストにキーを追加します。

```
ips-ssp# configure terminal
ips-ssp(config)# ssh authorized-key system1 1023 37
660222729556609833380897067163729433570828686860008172017802434921804214207813035920829509
101701358480525039993932112503147452768378620911189986653716089813147922086044739911341369
642870682319361928148521864094557416306138786468335115835910404940213136954353396163449793
497050167925831465486221464674219970 57
ips-ssp(config)#
```

ステップ 3　キーが追加されたことを確認します。

```
ips-ssp(config)# exit
ips-ssp# show ssh authorized-keys
system1
ips-ssp#
```

ステップ 4　特定の ID のキーを表示します。

```
ips-ssp# show ssh authorized-keys system1
1023 37 660222729556609833380897067163729433570828686860008172017802434921804214
207813035920829509101701358480525039993932112503147452768378620911189986653716089
813147922086044739911341369642870682319361928148521864094557416306138786468335115
158359104049402131369543533961634497934970501679258314654862214646742199705 7
ips-ssp#
```

ステップ 5　SSH 認証キーのリストからエントリを削除します。

```
ips-ssp# configure terminal
ips-ssp(config)# no ssh authorized-key system1
```

ステップ 6　エントリが削除されたことを確認します。キー system1 がリストに表示されなくなります。

```
ips-ssp(config)# exit
ips-ssp# show ssh authorized-keys
```

ステップ 7　前の ID を入力すると、エラー メッセージが表示されます。

```
ips-ssp# show ssh authorized-keys system1
Error: Requested id does not exist for the current user.
ips-ssp#
```

新しい SSH サーバ キーの生成

ssh generate-key コマンドを使用して、SSH サーバ ホスト キーを変更します。表示されるフィンガープリントは、リモート クライアントが SSH 1.5 を使用している場合、このセンサーとの今後の接続においてリモート SSH クライアントで表示されるものと一致します。

新しい SSH サーバ ホスト キーを生成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　新しいサーバ ホスト キーを生成します。

```
ips-ssp# ssh generate-key
MD5: 93:F5:51:58:C7:FD:40:8C:07:26:5E:29:13:C8:33:AE
Bubble Babble: ximal-sudez-kusot-gosym-levag-fegoc-holez-cakar-kunel-nylis-kyxox
ips-ssp#
```

注意　これ以降は、既存のキーの代わりに新しいキーが使用されるため、引き続き正常に接続するためには、リモート システム上にある既知ホストのテーブルを新しいホスト キーで更新する必要があります。リモート システム上の既知ホスト テーブルは、**ssh host-key** コマンドを使用して更新できます。

ステップ 3　現在の SSH サーバ ホスト キーを表示します。

```
ips-ssp# show ssh server-key
1024 35
13719676542657141950912489578722963006272638980107171558192157384728063753300015859002879807438582486718433236475889995967537052387960937617481217922841521578294902918396220784073177164580350983725947542147721245979717080651071607755601075316931267502386047498744165104121771015276699048043189821787817000064 7
MD5: 93:F5:51:58:C7:FD:40:8C:07:26:5E:29:13:C8:33:AE
Bubble Babble: ximal-sudez-kusot-gosym-levag-fegoc-holez-cakar-kunel-nylis-kyxox
ips-ssp#
```

詳細情報

既知ホスト テーブルの更新手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

TLS の設定

ここでは、センサー上の TLS について説明します。次のような構成になっています。

- 「TLS について」（P.4-39）
- 「TLS の信頼できるホストの追加」（P.4-40）
- 「サーバ証明書の表示と生成」（P.4-41）

TLS について

Cisco IPS には、IDM を実行している Web サーバが含まれます。管理ステーションは、この Web サーバと接続します。ブロッキング転送センサーも、マスター ブロッキング センサーの Web サーバと接続します。セキュリティを提供するために、この Web サーバでは TLS と呼ばれる暗号化プロトコルが使用されます。このプロトコルは、SSL と密接な関係があります。Web ブラウザでは、`https://ip_address` で始まる URL が入力されると、それに対する応答として、TLS プロトコルまたは SSL プロトコルによりホストとの間で暗号化セッションのネゴシエーションが行われます。

注意　Web ブラウザは、初期状態では CA を信頼していないため、IDM が提示する証明書を最初のうちは拒否します。

（注）　IDM は、デフォルトで TLS と SSL の使用がイネーブルになっています。TLS と SSL を使用することを強く推奨します。

TLS による暗号化セッションのネゴシエーション プロセスは、クライアントとサーバとが協調して何度もデータのやり取りを行うことから、「ハンドシェイク」と呼ばれます。サーバからクライアントへ証明書が送信されると、クライアントでは、この証明書に対して、次の 3 つのテストが実行されます。

1. 証明書に記載されている発行元は信頼できるか。

   各 Web ブラウザには、出荷される時点で、信頼されているサードパーティ CA のリストが組み込まれています。証明書に記載されている発行元が、ブラウザにより信頼されている CA のリストに含まれていれば、この最初のテストでは問題なしと判断されます。

2. その日の日付が、証明書の有効期間内にあるか。

   それぞれの証明書には、有効期間を表す 2 つの日付が記載された Validity フィールドがあります。その日の日付がこの期間内に該当すれば、この 2 番目のテストでは問題なしと判断されます。

3. 証明書に記載されているサブジェクトの共通名が、URL ホスト名と一致するか。

   URL ホスト名が、サブジェクトの共通名と比較されます。一致すれば、この 3 番目のテストでは問題なしと判断されます。

Web ブラウザから IDM に接続しようとすると、センサーは独自の証明書を発行しますが（センサーが自分自身の CA）、ブラウザにより信頼されている CA のリストにはそのセンサーが含まれていないため、返された証明書は無効と見なされます。

ブラウザにエラー メッセージが表示された場合の対処方法としては、次の 3 つの選択肢が考えられます。

- サイトへの接続を即座に解除する。
- その他の Web ブラウザ セッション用に証明書を受け入れる。
- 証明書に記載されている発行元を Web ブラウザの信頼 CA リストに追加して、有効期間が経過するまで証明書を信頼する。

最も簡単な方法は、発行元を永続的に信頼することです。ただし、発行元を追加する前に必ず、アウトオブバンド方式を使用して、証明書のフィンガープリントを検証します。これにより、センサーになりすました攻撃者による被害を回避できます。Web ブラウザに表示される証明書のフィンガープリントが、センサーのフィンガープリントと一致するかどうかを確認してください。

注意　センサーの組織名またはホスト名を変更した場合は、センサーの次回リブート時に新しい証明書が生成されます。Web ブラウザから IDM への次回接続時には、手動上書きダイアログボックスが表示されます。この場合は、Internet Explorer および Firefox で、証明書フィンガープリントの検証を再度実行する必要があります。

TLS の信頼できるホストの追加

状況によっては、センサーは、リモート Web サーバとの間に確立するセッションの保護に、TLS/SSL を使用する場合があります。これらのセッションを中間者攻撃から保護するために、リモート Web サーバの TLS 証明書の信頼を確立する必要があります。信頼できる各リモート ホストの TLS 証明書のコピーは、信頼できるホストのリストに保管されます。

tls trusted-host ip-address *ip-address* [**port** *port*] コマンドを使用して、信頼できるホストを信頼できるホストのリストに追加します。このコマンドにより、指定したホスト / ポートから TLS 証明書が取得され、そのフィンガープリントが表示されます。追加予定のホストから直接取得した情報を基に、そのフィンガープリントを受け入れることも拒否することもできます。デフォルトのポートは 443 です。

各証明書は、識別子フィールド（**id**）と一緒に保管されます。IP アドレスとデフォルト ポートの場合、識別子フィールドは **ipaddress** になります。IP アドレスと指定ポートの場合、識別子フィールドは **ipaddress:port** になります。

注意　指定した IP アドレスの TLS に接続して、必要なフィンガープリントがネットワーク経由で取得されます。指定したホストは、コマンドを発行するときにアクセス可能な状態でなければなりません。攻撃者の証明書を受け入れてしまうことがないように、別の方法を使用してそのフィンガープリントが正しいことを確認します。

信頼できるホストを信頼できるホストのリストに追加するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　信頼できるホストを追加します。MD5 と SHA1 のフィンガープリントが表示されます。信頼できるホストを追加するかどうかを確認するプロンプトが表示されます。

```
ips-ssp# configure terminal
ips-ssp(config)# tls trusted-host ip-address 10.16.0.0
Certificate MD5 fingerprint is 4F:BA:15:67:D3:E6:FB:51:8A:C4:57:93:4D:F2:83:FE
Certificate SHA1 fingerprint is B1:6F:F5:DA:F3:7A:FB:FB:93:E9:2D:39:B9:99:08:D4:
47:02:F6:12
Would you like to add this to the trusted certificate table for this host?[yes]:
```

接続を確立できない場合、このトランザクションは失敗します。

```
ips-ssp(config)# tls trusted-host ip-address 10.89.146.110 port 8000
Error: getHostCertificate : socket connect failed [4,111]
```

ステップ 3　**yes** を入力して、フィンガープリントを受け入れます。ホストが TLS の信頼できるホストのリストに追加されています。コマンドが成功した場合、要求した証明書用に保管される証明書 ID が表示されます。

```
Certificate ID: 10.89.146.110 successfully added to the TLS trusted host table.
ips-ssp(config)#
```

ステップ 4　ホストが追加されたことを確認します。

```
ips-ssp(config)# exit
ips-ssp# show tls trusted-hosts
10.89.146.110
ips-ssp#
```

ステップ 5　特定のホストのフィンガープリントを表示します。

```
ips-ssp# show tls trusted-hosts 10.89.146.110
MD5: 4F:BA:15:67:D3:E6:FB:51:8A:C4:57:93:4D:F2:83:FE
SHA1: B1:6F:F5:DA:F3:7A:FB:FB:93:E9:2D:39:B9:99:08:D4:47:02:F6:12
ips-ssp#
```

ステップ 6　信頼できるホストのリストからエントリを削除します。

```
ips-ssp# configure terminal
ips-ssp(config)# no tls trusted-host 10.89.146.110
```

ステップ 7　信頼できるホストのリストからエントリが削除されたことを確認します。IP アドレスがリストに表示されなくなります。

```
ips-ssp(config)# exit
ips-ssp# show tls trusted-hosts
No entries
```

サーバ証明書の表示と生成

TLS 証明書は、センサーの初回起動時に生成されます。**tls generate-key** コマンドを使用して、新しいサーバ自己署名 X.509 証明書を生成します。

（注）　証明書には、センサーの IP アドレスが含まれています。センサーの IP アドレスを変更すると、センサーによって自動的に新しい証明書が生成されます。

注意　新しい証明書は、既存の証明書と置き換わります。したがって、以降の接続に失敗しないために、リモート システム上の信頼できるホストのリストを新しい証明書で更新する必要があります。リモート IPS センサー上の信頼できるホストのリストは、**tls trusted-host** コマンドを使用して更新できます。センサーがマスター ブロッキング センサーである場合は、マスター ブロッキング センサーにブロック要求を送信するリモート センサー上で、信頼できるホストのリストを更新する必要があります。

新しい TLS 証明書を生成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　新しい証明書を生成します。

```
ips-ssp# tls generate-key
MD5 fingerprint is FD:83:6E:41:D3:88:48:1F:44:7F:AF:5D:52:60:89:DE
SHA1 fingerprint is 4A:2B:79:A0:82:8B:65:3A:83:B5:D9:50:C0:8E:F6:C6:B0:30:47:BB
ips-ssp#
```

ステップ 3　キーが生成されたことを確認します。

```
ips-ssp# show tls fingerprint
MD5: FD:83:6E:41:D3:88:48:1F:44:7F:AF:5D:52:60:89:DE
SHA1: 4A:2B:79:A0:82:8B:65:3A:83:B5:D9:50:C0:8E:F6:C6:B0:30:47:BB
ips-ssp#
```

詳細情報

リモート センサー上の信頼できるホストのリストを更新する手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

ライセンス キーのインストール

ここでは、IPS ライセンス キーとそのインストール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。

- 「ライセンス キーについて」（P.4-42）
- 「IPS 製品用のサービス プログラム」（P.4-43）
- 「ライセンス キーの取得とインストール」（P.4-44）

ライセンス キーについて

ライセンス キーなしでもセンサーは動作しますが、シグニチャ アップデートの取得およびグローバル相関機能の使用にはライセンス キーが必要です。ライセンス キーを取得するには、次のものを用意する必要があります。

- Cisco Service for IPS サービス契約：契約を購入するには、リセラー、シスコのサービスまたは製品の営業担当者にお問い合わせください。
- IPS デバイスのシリアル番号：IPS デバイスのシリアル番号を IDM または IME で確認するには、IDM の場合は [Configuration] > [Sensor Management] > [Licensing] を選択し、IME の場合は [Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。または、CLI で **show version** コマンドを使用します。
- 有効な Cisco.com ユーザ名およびパスワード

試用ライセンス キーも利用できます。契約の問題により、センサーにライセンスを設定できない場合は、ライセンスの必要なシグニチャ アップデートをサポートする 60 日間の試用ライセンスを取得できます。

ライセンス キーは、Cisco.com ライセンス サーバから取得できます。取得したライセンス キーは、センサーに配信されます。あるいは、ローカル ファイルで提供されるライセンス キーでライセンス キーを更新することもできます。http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックしてライセンス キーを要求します。

次の場所でライセンス キーのステータスを確認できます。

- [IDM Home] ウィンドウの [Health] タブ上の [Licensing] セクション
- [IDM Licensing] ペイン（[Configuration] > [Licensing]）
- [Licensing] タブ上の [Device Details] セクション内の [IME Home] ページ
- CLI ログイン時のライセンス通知

IDM、IME、または CLI を開始するとき、ライセンス ステータスが必ず通知されます（ライセンス キーが試用かどうか、無効かどうか、有効期限切れかどうか）。ライセンス キーがない、無効、または期限切れの場合、IDM、IME、および CLI を引き続き使用できますが、シグニチャ アップデートをダウンロードすることはできません。

センサー上にすでに有効なライセンスがある場合は、[License] ペイン上の [Download] をクリックすることで、IDM または IME を実行しているコンピュータに自分のライセンス キーのコピーをダウンロードし、ローカル ファイルに保存できます。その後、紛失または破損したライセンスと置き換えることができます。あるいは、センサーのイメージを再作成した後にライセンスを再インストールできます。

IPS 製品用のサービス プログラム

ライセンス キーをダウンロードしたり、最新の IPS シグニチャ アップデートを取得したりするには、IPS 製品用の Cisco Services for IPS サービス契約が必要です。シスコと直接取り引きしている場合は、担当のアカウント マネージャまたはサービス アカウント マネージャに連絡して、Cisco Services for IPS サービス契約を購入します。シスコと直接取り引きしていない場合は、1 ティアまたは 2 ティア パートナーからサービス アカウントを購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

IPS を搭載していない ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合は、SMARTnet 契約を購入する必要があります。

（注） SMARTnet は、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトの NBD ハードウェア交換を提供します。

IPS SSP を搭載して出荷される ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合、あるいは IPS SSP を購入して ASA 5500 シリーズ適応型セキュリティ アプライアンス製品に追加する場合は、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS は、IPS シグニチャ アップデート、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトの NBD ハードウェア交換を提供します。

たとえば、ASA 5585-X を購入した後、IPS の追加が必要になり、ASA-IPS10-K9 を購入する場合は、Cisco Services for IPS サービス契約の購入が必要になります。Cisco Services for IPS サービス契約を結んだ後は、製品シリアル番号を用意して、ライセンス キーを要求する必要があります。

注意 製品を RMA に出したことがある場合、シリアル番号は変更されています。その場合は、新しいシリアル番号用に新しいライセンス キーを取得する必要があります。

ライセンス キーの取得とインストール

（注） 新しいライセンス キーの上に古いライセンス キーをインストールすることはできません。

copy *source-url license_file_name* **license-key** コマンドを使用して、ライセンス キーをセンサーにコピーします。

オプション

次のオプションが適用されます。

- *source-url*：コピー元ファイルの場所を指定します。URL またはキーワードを使用できます。
- *destination-url*：コピー先ファイルの場所を指定します。URL またはキーワードを使用できます。
- **license-key**：サブスクリプション ライセンス ファイルを指定します。
- *license_file_name*：受け取るライセンス ファイルの名前を指定します。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

  （注） FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加する必要があります。

- http: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  http:[[/[username@]location]/directory]/filename
- https: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  https:[[/[username@]location]/directory]/filename

（注） HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

ライセンス キーのインストール

ライセンス キーをインストールするには、次の手順を実行します。

ステップ 1　www.cisco.com/go/license にアクセスしてライセンス キーを要求します。

（注） ライセンス キーを要求するには、有効な Cisco.com ユーザ名とパスワードに加え、Cisco Services for IPS サービス契約も必要です。

ステップ 2　必要なフィールドに入力します。Cisco IPS シグニチャ サブスクリプション サービス ライセンス キーは、指定した電子メール アドレスに電子メールで送信されます。

（注） ライセンス キーは、指定されたシリアル番号を持つ IPS デバイス上でしか動作しないため、正確なシリアル番号を用意する必要があります。

ステップ 3　Web サーバ、FTP サーバ、または SCP サーバが存在するシステムにライセンス キーを保存します。

ステップ 4　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 5　ライセンス キーをセンサーにコピーします。

```
ips-ssp# copy scp://user@192.0.2.1://tftpboot/dev.lic license-key
Password: *******
```

ステップ 6　センサーがライセンスされていることを確認します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40% usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

ips-ssp#
```

CHAPTER 5

インターフェイスの設定

（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 SSP にインターフェイスを設定する手順について説明します。次のような構成になっています。

- 「IPS SSP インターフェイスについて」（P.5-1）
- 「物理インターフェイスの設定」（P.5-2）
- 「無差別モード」（P.5-3）
- 「インライン インターフェイス モード」（P.5-4）
- 「インターフェイス通知の設定」（P.5-4）
- 「インターフェイス統計情報の表示」（P.5-5）

IPS SSP インターフェイスについて

IPS SSP は、管理インターフェイス（コマンド/コントロール）とセンシング インターフェイスの 2 つのインターフェイスを備えています。コマンド/コントロール インターフェイスは、IP アドレスが割り当てられ、IPS SSP を設定するために使用されます。IPS SSP からは、IDM にセキュリティ イベントとステータス イベントを送信するために使用されます。IPS SSP のコマンド/コントロール インターフェイスの名前は、Management0/0 です。

注意 IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

コマンド/コントロール インターフェイスは、常にイネーブルです。特定の物理インターフェイスに常にマッピングされます。コマンド/コントロール インターフェイスを検知インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。

センシング インターフェイスは、セキュリティ違反についてトラフィックを分析するために使用されます。IPS SSP 上には、センシング インターフェイスが 1 つだけ存在します。PortChannel0/0 という名前のバックプレーン インターフェイスです。すべてのバックプレーン インターフェイスは、速度、デュプレックス、および状態の設定が固定されています。これらの設定は、すべてのバックプレーン インターフェイスのデフォルト設定内で保護されています。IPS SSP インターフェイスは、適応型セキュリティ アプライアンス上のセキュリティ コンテキストで設定します。センシング インターフェイスは、常にイネーブルです。

詳細情報

ASA ソフトウェアの詳細については、次の URL にある ASA のユーザ マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

物理インターフェイスの設定

サービス インターフェイス サブモードで **physical-interfaces** *interface_name* コマンドを使用して、インターフェイス PortChannel0/0 の説明を追加します。IPS SSP は、適応型セキュリティ アプライアンス CLI から無差別モード用に設定され、Cisco IPS CLI からは設定されません。設定可能な唯一の **physical-interfaces** オプションは、**description** です。代替 TCP リセット インターフェイスは IPS SSP に適用されず、デュプレックスと速度のオプションは保護され、インターフェイスはすでにイネーブルになっています。

IPS SSP 上のインターフェイスの説明を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　インターフェイス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service interface
```

ステップ 3　使用可能なインターフェイスのリストを表示します。

```
ips-ssp(config-int)# physical-interfaces ?
Management0/0      Management0/0 physical interface.
PortChannel0/0     PortChannel0/0 physical interface.
ips-ssp(config-int)# physical-interfaces
```

ステップ 4　インターフェイスを指定します。

```
ips-ssp(config-int)# physical-interfaces PortChannel0/0
```

ステップ 5　このインターフェイスの説明を追加します。

```
ips-ssp(config-int-phy)# description INT1
```

ステップ 6　設定を確認できます。

（注）　`subinterface-type` が *none*（デフォルト）になっていることを確認します。インライン VLAN ペアは、**subinterface-type** コマンドを使用して設定します。

```
ips-ssp(config-int-phy)# show settings
   <protected entry>
   name: PortChannel0/0
   -----------------------------------------------
      media-type: backplane <protected>
      description: SSP INT default:
      admin-state: enabled <protected>
      duplex: full <protected>
      speed: 10000 <protected>
      alt-tcp-reset-interface
      -------------------------------------------------
         none
         -----------------------------------------------
         -----------------------------------------------
      -------------------------------------------------
   -----------------------------------------------
ips-ssp(config-int-phy)#
```

ステップ 7　インターフェイス サブモードを終了します。

```
ips-ssp(config-int-phy)# exit
ips-ssp(config-int)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

IPS SSP にトラフィックを送信するための手順については、「IPS SSP の仮想センサーの作成」（P.18-3）を参照してください。

無差別モード

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。ただし、無差別モードで運用するときは、アトミック アタック（シングルパケット攻撃）などの特定のタイプの攻撃の場合に、悪意のあるトラフィックがターゲットに到達することをセンサーで阻止できないという短所があります。無差別モードのセンサー デバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に対応するために、ルータやファイアウォールなど、他のネットワーキング デバイスによるサポートが必要となります。このような応答アクションは一部の攻撃を防ぐことはできますが、アトミック アタックでは、無差別モードベースのセンサーが管理対象デバイス（ファイアウォール、スイッチ、ルータなど）に ACL 修正を適用する前に、シングル パケットがターゲット システムに到達する可能性があります。

インライン インターフェイス モード

インライン インターフェイス ペア モードで運用する場合は、IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。遅延が加わるため、パケット転送速度は遅くなります。その結果、センサーは、悪意のあるトラフィックがターゲットに到達する前にそのトラフィックをドロップして攻撃を阻止できるため、保護サービスが提供されます。インライン デバイスは、レイヤ 3 および 4 で情報を処理するだけでなく、より高度な埋め込み型攻撃のパケットの内容およびペイロードも分析します（レイヤ 3 ～ 7）。この詳細な分析では、通常は従来のファイアウォール デバイスを通過する攻撃をシステムが識別し、その攻撃の停止やブロックを行うことができます。

インライン インターフェイス ペア モードでは、パケットはセンサーのペアの 1 つめのインターフェイスを経由して入り、ペアの 2 つめのインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されないかぎり、ペアの 2 つめのインターフェイスに送信されます。

（注）　IPS SSP は、センシング インターフェイスが 1 つしか存在しなくても、インラインで動作するように設定できます。

詳細情報

IPS SSP にトラフィックを送信するための手順については、「IPS SSP の仮想センサーの作成」（P.18-3）を参照してください。

インターフェイス通知の設定

インターフェイス上のパケットのフローをモニタし、そのフローが指定した間隔中に変更（開始/停止）された場合に通知を送信するようにセンサーを設定できます。特定の通知間隔内に欠落パケットのしきい値を設定でき、ステータス イベントがレポートされる前のインターフェイス アイドル遅延も設定できます。サービス インターフェイス サブモードで **interface-notifications** コマンドを使用して、トラフィック通知を設定します。

オプション

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **idle-interface-delay**：通知が送信される前にインターフェイスがアイドル状態でなければならない秒数を指定します。有効な範囲は 5 ～ 3600 です。デフォルトは 30 秒です。
- **missed-percentage-threshold**：通知が送信される前に、指定された間隔内で失われなければならないパケットのパーセンテージを指定します。有効な範囲は 0 ～ 100 です。デフォルトは 0 です。
- **notification-interval**：欠落パケットのパーセンテージを確認する間隔を指定します。有効な範囲は 5 ～ 3600 です。デフォルトは 30 秒です。

インターフェイス通知の設定

インターフェイス通知設定を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
ips-ssp# configure terminal
```

ステップ 3　インターフェイス サブモードを開始します。

```
ips-ssp(config)# service interface
```

ステップ 4　インターフェイス通知サブモードを開始します。

```
ips-ssp(config-int)# interface-notifications
```

ステップ 5　アイドル インターフェイス遅延を指定します。

```
ips-ssp(config-int-int)# idle-interface-delay 60
```

ステップ 6　損失パーセンテージしきい値を指定します。

```
ips-ssp(config-int-int)# missed-percentage-threshold 1
```

ステップ 7　通知間隔を指定します。

```
ips-ssp(config-int-int)# notification-interval 60
```

ステップ 8　設定を確認できます。

```
ips-ssp(config-int-int)# show settings
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 1 percent default: 0
      notification-interval: 60 seconds default: 30
      idle-interface-delay: 60 seconds default: 30
   -----------------------------------------------
ips-ssp(config-int-int)#
```

ステップ 9　インターフェイス通知サブモードを終了します。

```
ips-ssp(config-int-int)# exit
ips-ssp(config-int)# exit
Apply Changes:?[yes]:
```

ステップ 10　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

インターフェイス統計情報の表示

EXEC モードで **show interfaces** [**clear** | **brief**] コマンドを使用して、すべてのシステム インターフェイスの統計情報を表示します。**show interfaces** {**FastEthernet** | **GigabitEthernet** | **Management**} [*slot/port*] コマンドを使用して、特定のインターフェイスの統計情報を表示します。

オプション

次のオプションが適用されます。

- **clear**：（任意）診断をクリアします。
- **brief**：（任意）各インターフェイスのユーザビリティ ステータスの概要を表示します。
- **Management0/0**：この管理インターフェイスの統計情報を表示します。
- **PortChannel0/0**：PortChannel0/0 インターフェイスの統計情報を表示します。
- **Management**：管理インターフェイスの統計情報を表示します。

（注）　*Management* の印の付いた外部ポートを持つプラットフォームでのみ、このキーワードはサポートされます。

インターフェイス統計情報の表示

インターフェイス統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　すべてのインターフェイスの統計情報を表示します。

```
ips-ssp# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 1786269
   Total Bytes Received = 195561352
   Total Multicast Packets Received = 0
   Total Receive Errors = 2
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 639160
   Total Bytes Transmitted = 234623511
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface PortChannel0/0
   Interface function = Sensing interface
   Description =
   Media Type = backplane
   Default Vlan = 0
   InlineMode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Down
   Admin Enabled Status = Enabled
   Link Speed = Auto_10000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 0
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
```

```
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/1
   Interface function = Reserved for future use
ips-ssp#
```

ステップ 3　インターフェイスの概要を簡潔に表示します。* は、インターフェイスがコマンド/コントロール インターフェイスであることを示しています。

```
ips-ssp# show interfaces brief
CC   Interface        Sensing State   Link   Inline Mode   Pair Status
*    Management0/0    Disabled        Up
     PortChannel0/0   Enabled         Down   Unpaired      N/A
ips-ssp#
```

ステップ 4　特定のインターフェイスの統計情報を表示します。

```
ips-ssp# show interfaces PortChannel0/0
MAC statistics from interface PortChannel0/0
   Interface function = Sensing interface
   Description =
   Media Type = backplane
   Default Vlan = 0
   InlineMode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Down
   Admin Enabled Status = Enabled
   Link Speed = Auto_10000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 0
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

ステップ 5　統計情報をクリアします。

```
ips-ssp# show interfaces clear
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_1000
```

```
    Link Duplex = Auto_Full
    Total Packets Received = 1788042
    Total Bytes Received = 195720517
    Total Multicast Packets Received = 0
    Total Receive Errors = 2
    Total Receive FIFO Overruns = 0
    Total Packets Transmitted = 640344
    Total Bytes Transmitted = 234918987
    Total Transmit Errors = 0
    Total Transmit FIFO Overruns = 0
MAC statistics from interface PortChannel0/0
    Interface function = Sensing interface
    Description =
    Media Type = backplane
    Default Vlan = 0
    InlineMode = Unpaired
    Pair Status = N/A
    Hardware Bypass Capable = No
    Hardware Bypass Paired = N/A
    Link Status = Down
    Admin Enabled Status = Enabled
    Link Speed = Auto_10000
    Link Duplex = Auto_Full
    Missed Packet Percentage = 0
    Total Packets Received = 0
    Total Bytes Received = 0
    Total Multicast Packets Received = 0
    Total Broadcast Packets Received = 0
    Total Jumbo Packets Received = 0
    Total Undersize Packets Received = 0
    Total Receive Errors = 0
    Total Receive FIFO Overruns = 0
    Total Packets Transmitted = 0
    Total Bytes Transmitted = 0
    Total Multicast Packets Transmitted = 0
    Total Broadcast Packets Transmitted = 0
    Total Jumbo Packets Transmitted = 0
    Total Undersize Packets Transmitted = 0
    Total Transmit Errors = 0
    Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/1
    Interface function = Reserved for future use
ips-ssp#
```

CHAPTER 6

仮想センサーの設定

（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 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 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、分析エンジンの機能、および仮想センサーの作成、編集、削除方法について説明します。また、インターフェイスを仮想センサーに割り当てる方法についても説明します。この章は、次の内容で構成されています。

- 「分析エンジンについて」（P.6-1）
- 「仮想センサーについて」（P.6-2）
- 「仮想化の利点および制約事項」（P.6-2）
- 「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）
- 「グローバル変数の設定」（P.6-11）

分析エンジンについて

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。

分析エンジンでは、仮想センサーを作成します。各仮想センサーには、一意の名前が割り当てられ、インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループのリストが関連付けられます。定義順序による問題の発生を避けるため、割り当てに競合や重複が存在してはなりません。インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループは、複数の仮想センサーによって処理されるパケットが発生しないように、特定の仮想センサーに割り当てます。各仮想センサーは、固有の名前を持つシグニチャ定義、イベントアクション規則、および異常検出設定にも関連付けられます。どの仮想センサーにも割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、インライン バイパス設定に従って廃棄されます。

（注） Cisco IPS では仮想センサーが 4 つまでサポートされます。デフォルトの仮想センサー vs0 は削除できません。

仮想センサーについて

センサーは 1 つまたは多数のモニタ対象データ ストリームからのデータ入力を受信できます。これらのモニタ対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのどちらでも構いません。たとえば、単一のセンサーでファイアウォールの前からのトラフィック、ファイアウォールの後ろからのトラフィック、またはファイアウォールの前後からのトラフィックを同時にモニタできます。また、単一のセンサーで 1 つ以上のデータ ストリームをモニタできます。この場合、単一のセンサー ポリシーまたは設定がすべてのモニタ対象データストリームに適用されます。

仮想センサーは、一連の設定ポリシーで定義されるデータの集合です。仮想センサーは、インターフェイス コンポーネントで定義される一連のパケットに適用されます。

1 つの仮想センサーで複数のセグメントをモニタすることができ、単一の物理センサー内では仮想センサーごとに異なるポリシーまたは設定を適用できます。分析時には、モニタ対象セグメントごとに異なるポリシーをセットアップできます。また、同じポリシー インスタンス（sig0、rules0、ad0 など）を複数の仮想センサーに適用することもできます。仮想センサーには、インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを割り当てることができます。

（注） デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。デフォルトの仮想センサーに対して変更可能な設定機能は、インターフェイス リスト、異常検出動作モード、および仮想センサーの説明だけです。シグニチャ定義、イベント アクション規則、異常検出ポリシーは変更できません。

仮想化の利点および制約事項

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。
- 固定ストアが制限されます。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

IPS SSP 上での仮想センサーの追加、編集、および削除

ここでは、IPS SSP 上で仮想センサーを作成する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。

- 「IPS SSP と仮想化」（P.6-3）
- 「IPS SSP 仮想センサーの設定手順」（P.6-3）
- 「仮想センサーの作成」（P.6-4）
- 「適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て」（P.6-6）
- 「仮想センサーの編集と削除」（P.6-9）

IPS SSP と仮想化

IPS SSP には、センシング インターフェイスが 1 つ（PortChannel0/0）存在します。複数の仮想センサーを作成する場合は、このインターフェイスを 1 つの仮想センサーにだけ割り当てる必要があります。残りの仮想センサーには、インターフェイスを指定する必要はありません。

注意　IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

仮想センサーを作成した後、**allocate-ips** コマンドを使用して、それらを適応型セキュリティ アプライアンス上のセキュリティ コンテキストにマッピングする必要があります。複数のセキュリティ コンテキストを複数の仮想センサーにマッピングできます。

（注）　**allocate-ips** コマンドは、シングル モードには適用されません。このモードでは、**policy-map** コマンドで名前が指定されているすべての仮想センサーが適応型セキュリティ アプライアンスで受け入れられます。

allocate-ips コマンドは、新しいエントリをセキュリティ コンテキスト データベースに追加します。指定した仮想センサーが存在しないと、警告が出力されます。ただし、設定は受け入れられます。**service-policy** コマンドが処理されるとき、設定が再びチェックされます。仮想センサーが有効でなければ、**fail-open** ポリシーが適用されます。

IPS SSP 仮想センサーの設定手順

次の手順に従って、IPS SSP 上に仮想センサーを作成し、それらを適応型セキュリティ アプライアンスのコンテキストに割り当てます。

1. IPS SSP 上で最大 4 つの仮想センサーを設定します。
2. IPS SSP センシング インターフェイス（PortChannel0/0）を仮想センサーの 1 つに割り当てます。

3. （任意）仮想センサーを適応型セキュリティ アプライアンス上の異なるコンテキストに割り当てます。
4. MPF を使用してトラフィックをターゲットの仮想センサーに誘導します。

仮想センサーの作成

（注）　4 つの仮想センサーを作成できます。

サービス分析エンジン サブモードで **virtual-sensor** *name* コマンドを使用して、IPS SSP 上の仮想センサーを作成します。仮想センサーにポリシー（異常検出、イベント アクション規則、およびシグニチャ定義）を割り当てます。デフォルトのポリシーである ad0、rules0、または sig0 を使用できます。あるいは、新しいポリシーを作成することもできます。その後、IPS SSP のセンシング インターフェイス PortChannel0/0 を 1 つの仮想センサーに割り当てます。

オプション

次のオプションが適用されます。

- **anomaly-detection**：異常検出パラメータを指定します。
  - **anomaly-detection-name** *name*：異常検出ポリシーの名前を指定します。
  - **operational-mode**：異常検出モード（**inactive**、**learn**、**detect**）を指定します。
- **description**：仮想センサーの説明。
- **event-action-rules**：イベント アクション規則ポリシーの名前を指定します。
- **signature-definition**：シグニチャ定義ポリシーの名前を指定します。
- **physical-interface**：物理インターフェイスの名前を指定します。
- **no**：エントリまたは選択を削除します。

仮想センサーの作成

IPS SSP 上で仮想センサーを作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス分析モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)#
```

ステップ 3　仮想センサーを追加します。

```
ips-ssp(config-ana)# virtual-sensor vs1
ips-ssp(config-ana-vir)#
```

ステップ 4　この仮想センサーの説明を追加します。

```
ips-ssp(config-ana-vir)# description virtual sensor 1
```

ステップ 5　異常検出ポリシーと動作モードをこの仮想センサーに割り当てます。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# anomaly-detection-name ad1
ips-ssp(config-ana-vir-ano)# operational-mode learn
```

ステップ 6　イベント アクション規則ポリシーをこの仮想センサーに割り当てます。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(config-ana-vir)# event-action-rules rules1
```

ステップ 7　シグニチャ定義ポリシーをこの仮想センサーに割り当てます。

```
ips-ssp(config-ana-vir)# signature-definition sig1
```

ステップ 8　インターフェイスを 1 つの仮想センサーに割り当てます。

```
ips-ssp(config-ana-vir)# physical-interface PortChannel0/0
```

ステップ 9　仮想センサー設定を確認します。

```
ips-ssp(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: PortChannel0/0
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana-vir)#
```

ステップ 10　分析エンジン モードを終了します。

```
ips-ssp(config-ana-vir)# exit
ips-ssp(config-ana)# exit
Apply Changes:?[yes]:
sensor(config)#
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- 異常検出ポリシーの作成および設定の手順については、「異常検出ポリシーの使用」（P.9-8）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作成および設定の手順については、「イベント アクション ルール ポリシーの使用」（P.8-7）を参照してください。
- シグニチャ定義の作成および設定の手順については、「シグニチャ定義ポリシーの操作」（P.7-1）を参照してください。

適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て

シングルコンテキスト モードの場合、仮想センサーをコンテキストに割り当てる必要はありません。マルチコンテキスト モードの場合、IPS SSP 上に仮想センサーを作成した後、それらの仮想センサーを適応型セキュリティ アプライアンス上のセキュリティ コンテキストに割り当てる必要があります。

オプション

次のオプションが適用されます。

- **[no] allocate-ips** *sensor_name* [*mapped_name*] [**default**]：仮想センサーをセキュリティ コンテキストに割り当てます。サポートされているモードは、マルチ モード、システム コンテキスト、およびコンテキスト サブモードです。

  （注）　同じ仮想センサーを 1 つのコンテキストに 2 回割り当てることはできません。

  - *sensor_name*：IPS SSP 上に設定された仮想センサーの名前を指定します。名前が有効でない場合、警告メッセージが表示されます。
  - *mapped_name*：セキュリティ コンテキストが仮想センサーを認識するための名前を指定します。

    （注）　マッピングされた名前は、仮想センサーの本当の名前をコンテキストから隠すために使用され、一般にセキュリティ上または便宜上の理由から、コンテキスト設定をより一般化するために使用されます。マッピングされた名前を使用しなければ、実際の仮想センサー名が使用されます。コンテキスト内の 2 つの異なる仮想センサーに同じマッピングされた名前を使用することはできません。

  - **no**：センサーの割り当てを解除し、ポリシー マップ設定を検索し、そのセンサーを参照しているすべての IPS サブコマンドを削除します。
  - **default**：この仮想センサーをデフォルトに指定します。仮想センサーを指定しないすべてのレガシー IPS 設定は、この仮想センサーにマッピングされます。

  注意　コンテキストごとに設定できるデフォルト仮想センサーは 1 つのみです。別の仮想センサーをデフォルトに指定する場合は、その前に既存のデフォルト仮想センサーのデフォルト フラグをオフにする必要があります。

  - **clear configure allocate-ips**：設定を削除します。
  - **allocate-ips?**：設定済みの仮想センサーのリストを表示します。

- **show context** [**detail**]：仮想センサーに関する情報を表示するように更新されます。ユーザ コンテキスト モードでは、このコンテキストに割り当てられているすべての仮想センサーのマッピングされた名前を表示するために、新しい行が 1 つ追加されます。システム モードでは、このコンテキストに割り当てられた仮想センサーの本当の名前とマッピングされた名前を表示するために、新しい行が 2 つ追加されます。

適応型セキュリティ アプライアンスのコンテキストへの IPS SSP 仮想センサーの割り当て

複数の仮想センサーを 1 つのコンテキストに割り当てることができます。1 つの仮想センサーは複数のコンテキストで共有することができます。共有した場合、それらのコンテキストは、同じ仮想センサーに対してそれぞれ異なるマッピングされた名前（エイリアス）を使用できます。次の手順では、マルチ モードで 3 つのセキュリティ コンテキストを追加する方法とそれらのセキュリティ コンテキストに仮想センサーを割り当てる方法を示します。

マルチ モードで IPS SSP の仮想センサーを、適応型セキュリティ アプライアンス コンテキストに割り当てるには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　使用可能な仮想センサーのリストを表示します。

```
asa# show ips detail
Sensor Name      Sensor ID
-----------      ---------
vs0              1
vs1              2
asa#
```

ステップ 3　コンフィギュレーション モードを開始します。

```
asa# configure terminal
asa(config)#
```

ステップ 4　マルチ モードを開始します。

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

ステップ 5　3 つのコンテキスト モードをマルチ モードに追加します。

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.101
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.102
asa(config-ctx)#   allocate-interface Management0/0
asa(config-ctx)#   config-url disk0:/admin.cfg
Cryptochecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up .... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.103
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.104
asa(config-ctx)#   config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
asa(config-ctx)#   config-url disk0:/c3.cfg
```

```
WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

ステップ 6　仮想センサーをセキュリティ コンテキストに割り当てます。

```
asa(config)# context admin
asa(config-ctx)#   allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)#   allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

ステップ 7　各コンテキストに MPF を設定します。

（注）　次に、コンテキスト 3（c3）の例を示します。

```
asa(config)# context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

ステップ 8　設定を確認します。

```
asa/c3(config)# exit
asa(config)# changeto system
asa(config)# show ips detail
Sensor Name      Sensor ID        Allocated To     Mapped Name
-----------      ---------        ------------     -----------
vs0              1                admin            adminvs0
                                  c3               c3vs0
vs1              2                c2               c2vs1
                                  c3               c3vs1
asa(config)#
```

設定例

次に、インライン モードですべての IP トラフィックを IPS SSP に迂回させ、何らかの理由で IPS SSP で障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-close
hostname(config-pmap-c)# service-policy my-ids-policy global
```

次に、無差別モードですべての IP トラフィックを IPS SSP に迂回させ、何らかの理由で IPS SSP で障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

仮想センサーの編集と削除

仮想センサーの次のパラメータを編集できます。

- シグニチャ定義ポリシー
- イベント アクション規則ポリシー
- 異常検出ポリシー
- 異常検出動作モード
- 説明
- 物理インターフェイス

仮想センサーを編集または削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　分析エンジン モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)#
```

ステップ 3　仮想センサー vs1 を編集します。

```
ips-ssp(config-ana)# virtual-sensor vs1
ips-ssp(config-ana-vir)#
```

ステップ 4　この仮想センサーの説明を編集します。

```
ips-ssp(config-ana-vir)# description virtual sensor A
```

ステップ 5　この仮想センサーに割り当てられている異常検出ポリシーと動作モードを変更します。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# anomaly-detection-name ad0
ips-ssp(config-ana-vir-ano)# operational-mode learn
```

ステップ 6　この仮想センサーに割り当てられているイベント アクション規則ポリシーを変更します。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(config-ana-vir)# event-action-rules rules0
```

ステップ 7　この仮想センサーに割り当てられているシグニチャ定義ポリシーを変更します。

```
ips-ssp(config-ana-vir)# signature-definition sig0
```

ステップ 8　編集された仮想センサー設定を確認します。

```
ips-ssp(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor A default:
      signature-definition: sig0 default: sig0
      event-action-rules: rules0 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad0 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana-vir)##
```

ステップ 9　仮想センサーを削除します。

```
ips-ssp(config-ana-vir)# exit
ips-ssp(config-ana)# no virtual-sensor vs1
```

ステップ 10　削除された仮想センサーを確認します。デフォルトの仮想センサー vs0 だけが存在します。

```
ips-ssp(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -----------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   -----------------------------------------------
      <protected entry>
      name: vs0 <defaulted>
      -----------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         anomaly-detection
         -----------------------------------------------
            anomaly-detection-name: ad0 <protected>
            operational-mode: detect <defaulted>
         -----------------------------------------------
         physical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana)##
```

ステップ 11　分析エンジン モードを終了します。

```
ips-ssp(config-ana)# exit
ips-ssp(config)#
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- 異常検出ポリシーの作成および設定の詳細については、「異常検出ポリシーの使用」（P.9-8）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作成および設定の詳細については、「イベント アクション ルール ポリシーの使用」（P.8-7）を参照してください。
- シグニチャ定義ポリシーの作成および設定の詳細については、「シグニチャ定義ポリシーの操作」（P.7-1）を参照してください。

グローバル変数の設定

サービス分析エンジン サブモードで **global-parameters** コマンドを使用して、グローバル変数を作成します。

（注）　Cisco IPS でのグローバル変数は、開く IP ログ ファイルの最大数の設定のみです。

オプション

次のオプションが適用されます。

- **ip-logging**：グローバル IP ロギング パラメータを指定します。
  - **max-open-iplog-files**：同時に開くログ ファイルの最大数を指定します。範囲は 20 ～ 100 です。デフォルトは 20 です。

グローバル変数の作成

グローバル変数を作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス分析モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)#
```

ステップ 3　開く IP ログの最大数を表す変数を作成します。

```
ips-ssp(config-ana)# global-parameters
ips-ssp(config-ana-glo)# ip-logging
ips-ssp(config-ana-glo-ip)# max-open-iplog-files 50
```

ステップ 4　グローバル変数設定を確認します。

```
ips-ssp(config-ana-glo-ip)# show settings
   ip-logging
   -----------------------------------------------
      max-open-iplog-files: 50 default: 20
   -----------------------------------------------
ips-ssp(config-ana-glo-ip)#
```

ステップ 5　分析エンジン モードを終了します。

```
ips-ssp(config-ana-glo-ip)# exit
ips-ssp(config-ana-glo)# exit
ips-ssp(config-ana)# exit
ips-ssp(config)#
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

CHAPTER 7

シグニチャの定義

（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 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 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、シグニチャを定義し、作成する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。

- 「セキュリティ ポリシーについて」（P.7-1）
- 「シグニチャ定義ポリシーの操作」（P.7-1）
- 「シグニチャについて」（P.7-3）
- 「シグニチャ変数の設定」（P.7-4）
- 「シグニチャの設定」（P.7-6）
- 「カスタム シグニチャの作成」（P.7-42）

セキュリティ ポリシーについて

複数のセキュリティ ポリシーを作成し、それらを個々の仮想センサーに適用できます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーから構成されます。Cisco IPS には、sig0 という名前のデフォルトのシグニチャ定義ポリシー、rules0 という名前のデフォルトのイベント アクション規則ポリシー、および ad0 という名前のデフォルトの異常検出ポリシーが用意されています。仮想センサーにこれらのデフォルト ポリシーを割り当てることも、新しいポリシーを作成することもできます。複数のセキュリティ ポリシーを使用すれば、それぞれ異なる要件に基づいたセキュリティ ポリシーを作成し、そうしたカスタマイズされたポリシーを VLAN や物理インターフェイスごとに適用することが可能になります。

シグニチャ定義ポリシーの操作

サービス シグニチャ定義モードで **service signature-definition** *name* コマンドを使用して、シグニチャ定義ポリシーを作成します。このシグニチャ定義ポリシーの値は、それらを編集するまでは、デフォルトのシグニチャ定義ポリシー sig0 と同じです。

あるいは、特権 EXEC モードで **copy signature-definition** *source_destination* コマンドを使用して既存のポリシーのコピーを作成してから、必要に応じてその新しいポリシーの値を編集できます。

特権 EXEC モードで **list signature-definition-configurations** コマンドを使用して、シグニチャ定義ポリシーを一覧表示します。

グローバル コンフィギュレーション モードで **no service signature-definition** *name* コマンドを使用して、シグニチャ定義ポリシーを削除します。グローバル コンフィギュレーション モードで **default service signature-definition** *name* コマンドを使用して、シグニチャ定義ポリシーを工場出荷時の設定にリセットします。

シグニチャ定義ポリシーを作成、コピー、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義ポリシーを作成します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition MySig
Editing new instance MySig.
ips-ssp(config-sig)# exit
Apply Changes?[yes]: yes
ips-ssp(config)# exit
```

ステップ 3　または、既存のシグニチャ定義ポリシーを新しいシグニチャ定義ポリシーにコピーします。

```
ips-ssp# copy signature-definition sig0 sig1
ips-ssp#
```

（注）　ポリシーがすでに存在しているか、新しいポリシーに必要な容量が不足していると、エラーが表示されます。

ステップ 4　デフォルトのシグニチャ定義ポリシーの値を受け入れるか、次のようなパラメータの編集を行います。

a.　シグニチャ定義変数を追加します。

b.　一般的なシグニチャ オプションを設定します。

ステップ 5　IPS SSP 上のシグニチャ定義ポリシーのリストを表示します。

```
ips-ssp# list signature-definition-configurations
Signature Definition
   Instance   Size   Virtual Sensor
   sig0       255    vs0
   temp       707    N/A
   MySig      255    N/A
   sig1       141    vs1
ips-ssp#
```

ステップ 6　シグニチャ定義ポリシーを削除します。

```
ips-ssp# configure terminal
ips-ssp(config)# no service signature-definition MySig
ips-ssp(config)# exit
ips-ssp#
```

（注）　デフォルトのシグニチャ定義ポリシー sig0 は削除できません。

ステップ 7　シグニチャ定義ポリシーが削除されていることを確認します。

```
ips-ssp# list signature-definition-configurations
Signature Definition
   Instance   Size   Virtual Sensor
   sig0       255    vs0
   temp       707    N/A
   sig1       141    vs1
ips-ssp#
```

ステップ 8　シグニチャ定義ポリシーを工場出荷時の設定にリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# default service signature-definition sig1
ips-ssp(config)#
```

詳細情報

- シグニチャ変数を追加する手順については、「シグニチャ変数の設定」（P.7-4）を参照してください。
- 一般設定の手順については、「シグニチャの設定」（P.7-6）を参照してください。

シグニチャについて

攻撃またはその他のネットワーク リソースの不正使用は、ネットワークへの侵入として定義付けることができます。シグニチャベースのテクノロジーを使用するセンサーによって、ネットワーク侵入を検出できます。シグニチャは、DoS 攻撃などの典型的な侵入行為を検出するためにセンサーが使用する一連の規則です。センサーは、ネットワーク パケットをスキャンするときに、シグニチャを使って既知の攻撃を検出し、指定されたアクションに従って対応します。

センサーは、一連のシグニチャとネットワーク アクティビティを比較します。一致した場合、イベントのロギングやアラームの送信などのアクションを実行します。センサーでは、既存のシグニチャを変更したり、新しいシグニチャを定義したりできます。

シグニチャ ベースの侵入検出では、偽陽性が生じる場合があります。通常のネットワーク アクティビティでも、悪意のあるアクティビティとして誤解される場合があるためです。たとえば、一部のネットワーク アプリケーションやオペレーティング システムは、多数の ICMP メッセージを送信することがありますが、シグニチャベースの検出システムでは、このメッセージが攻撃者によるネットワーク セグメント特定の試みであると解釈されてしまう可能性があります。シグニチャをチューニングすると、偽陽性を最小限に抑えることができます。

特定のシグニチャを使ってネットワーク トラフィックをモニタするようにセンサーを設定するには、そのシグニチャをイネーブルにする必要があります。デフォルトでは、重要なシグニチャはシグネチャ アップデートのインストール時にイネーブルになります。イネーブルなシグネチャに一致する攻撃が検出されると、センサーはアラートを生成します。生成されたアラートはセンサーのイベント ストアに保存されます。Web ベース クライアントは、アラートやその他のイベントをイベント ストアから取得できます。デフォルトでは、センサーは Informational 以上のすべてのアラートをログに記録します。

シグニチャには、サブシグニチャを持つもの（サブカテゴリに分類されているもの）があります。サブシグニチャを設定した場合、あるサブシグニチャのパラメータを変更しても、変更が適用されるのはそのサブシグニチャだけです。たとえば、シグニチャ 3050 のサブシグニチャ 1 を編集し重大度を変更した場合、重大度の変更はサブシグニチャ 1 だけに適用され、3050 2、3050 3、および 3050 4 には適用されません。

Cisco IPS には、10,000 を超えるデフォルトの組み込みシグニチャが含まれています。組み込みシグネチャのリストにあるシグネチャの名前の変更および削除はできません。ただし、シグネチャをセンシング エンジンから削除して廃棄できます。あとで廃棄されたシグネチャをアクティブにできます。ただし、このプロセスにはセンシング エンジンの設定の再構築が必要です。この再構築には時間がかかり、トラフィックの処理を遅延させる可能性があります。組み込みシグニチャのチューニングは可能です。これには、シグニチャのいくつかのパラメータを変更します。変更された組み込みシグニチャは、チューニング済みシグニチャと呼ばれます。

（注） 使用していないシグネチャを廃棄することを推奨します。廃棄によって、センサーのパフォーマンスが向上します。

カスタム シグニチャと呼ばれるシグニチャを作成できます。カスタム シグニチャ ID は、60000 から始まります。いくつかの項目に対して、カスタム シグニチャを設定できます。たとえば、UDP 接続の文字列との一致やネットワーク フラッドの追跡、スキャンなどです。シグニチャは、モニタするトラフィックの種類に対して特別に設計されたシグニチャ エンジンを使って作成します。

シグニチャ変数の設定

ここでは、シグニチャ変数について説明します。次のような構成になっています。

- 「シグニチャ変数について」（P.7-4）
- 「シグニチャ変数の追加、編集、および削除」（P.7-4）

シグニチャ変数について

複数のシグニチャで同じ値を使用する場合、変数を使用します。変数の値を変更すると、その変数を使用しているすべてのシグニチャでその変数の値が更新されます。このため、シグニチャを設定するときに変数を繰り返し変更しなくて済みます。

（注） 文字列でなく変数を使っていることを示すために、変数をドル記号（$）で始める必要があります。

一部の変数は、シグニチャ システムに対して必須であるため、削除することはできません。変数が保護されている場合は、その変数を選択して編集することはできません。保護されている変数を削除しようとすると、エラー メッセージが表示されます。一度に編集できる変数は 1 つだけです。

シグニチャ変数の追加、編集、および削除

シグニチャ定義サブモードで **variables** コマンドを使用して、シグニチャ変数を作成します。

オプション

次のオプションが適用されます。

- *variable_name*：この変数の名前を示します。有効な名前は、数字と文字のみで構成されます。ハイフン（-）とアンダースコア（_）も使用できます。
- **ip-addr-range**：IP アドレスのグループを表すシステム定義変数を指定します。有効な値は、A.B.C.D-A.B.C.D[,A.B.C.D-A.B.C.D] の形式になります。

- **web-ports**：HTTP トラフィックを検索するポートを表すシステム定義変数を指定します。1 つの変数に複数のポート番号を指定する場合は、エントリ間にカンマを入力します。たとえば、80, 3128, 8000, 8010, 8080, 8888, 24326 と入力します。

シグニチャ変数の追加、編集、および削除

シグニチャ変数を追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　IP アドレスのグループを表すシグニチャ変数を作成します。

```
ips-ssp(config-sig)# variables IPADD ip-addr-range 10.1.1.1-10.1.1.24
```

ステップ 4　Web ポートを表すシグニチャ変数を編集します。WEBPORTS は Web サーバが実行されているポート群で、あらかじめ定義されているものですが、値は編集できます。この変数は、Web ポートが含まれるすべてのシグニチャに影響します。デフォルトは、80, 3128, 8000, 8010, 8080, 8888, 24326 です。

```
ips-ssp(config-sig)# variables WEBPORTS web-ports 80,3128,8000
```

ステップ 5　変更を確認します。

```
ips-ssp(config-sig)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variable-name: IPADD
      -----------------------------------------------
         ip-addr-range: 10.1.1.1-10.1.1.24
      -----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
      -----------------------------------------------
         web-ports: 80,3128,8000 default: 80-80,3128-3128,8000-8000,8010-8010,80
80-8080,8888-8888,24326-24326
      -----------------------------------------------
```

ステップ 6　変数を削除します。

```
ips-ssp(config-sig)# no variables IPADD
```

ステップ 7　変数が削除されていることを確認します。

```
ips-ssp(config-sig)# show settings
   variables (min: 0, max: 256, current: 1)
   -----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
      -----------------------------------------------
         web-ports: 80,3128,8000 default: 80-80,3128-3128,8000-8000,8010-8010,80
80-8080,8888-8888,24326-24326
      -----------------------------------------------
```

ステップ 8　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

シグニチャの設定

ここでは、シグニチャ パラメータを設定する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。

- 「シグニチャ定義オプション」（P.7-6）
- 「アラート頻度の設定」（P.7-7）
- 「アラート重大度の設定」（P.7-9）
- 「イベント カウンタの設定」（P.7-11）
- 「シグニチャ忠実度レーティングの設定」（P.7-12）
- 「シグニチャのステータスの設定」（P.7-13）
- 「シグニチャの脆弱性のある OS の設定」（P.7-14）
- 「シグニチャへのアクションの割り当て」（P.7-16）
- 「AIC シグニチャの設定」（P.7-18）
- 「IP フラグメント再構成の設定」（P.7-29）
- 「TCP ストリーム再構成の設定」（P.7-33）
- 「IP ロギングの設定」（P.7-41）

シグニチャ定義オプション

特定のシグニチャの一般パラメータの設定には、次のオプションが適用されます。

- **alert-frequency**：アラートをグループ化するためのサマリー オプションを設定します。
- **alert-severity**：アラートの重大度を設定します。
- **engine**：シグニチャ エンジンを指定します。アクションはエンジン サブモードのときに割り当てることができます。
- **event-counter**：イベント カウントを設定します。
- **promisc-delta**：アラートの重大度を決定するために使用されるデルタ値を指定します。

注意　シグニチャの無差別デルタ設定を変更することは推奨されません。

- **sig-description**：シグニチャの説明。
- **sig-fidelity-rating**：シグニチャの忠実度のレーティングを指定します。
- **status**：シグニチャのステータスをイネーブルまたは廃棄に設定します。
- **vulnerable-os**：この攻撃シグニチャに対して脆弱な OS タイプのリストを指定します。

詳細情報

- アラート頻度の設定手順については、「アラート頻度の設定」（P.7-7）を参照してください。
- シグニチャ エンジンの詳細については、付録 B「シグニチャ エンジンの概要」を参照してください。

- アクションの割り当て手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。
- イベント カウントの設定手順については、「イベント カウンタの設定」（P.7-11）を参照してください。
- 無差別デルタの詳細については、「無差別デルタ」（P.7-7）を参照してください。
- シグニチャ忠実度レーティングの設定手順については、「シグニチャ忠実度レーティングの設定」（P.7-12）を参照してください。
- シグニチャのイネーブル化とディセーブル化の手順については、「シグニチャのステータスの設定」（P.7-13）を参照してください。
- 脆弱性のある OS の設定手順については、「シグニチャの脆弱性のある OS の設定」（P.7-14）を参照してください。

無差別デルタ

注意　シグニチャの無差別デルタ設定を変更することは推奨されません。

無差別デルタは、無差別モードにおいて特定のアラートのリスク レーティングを引き下げます。センサーはターゲット システムの属性を認識せず、無差別モードではパケットを拒否できないため、管理者がリスク レーティングの高いアラートの調査に集中できるよう、（リスク レーティングの低さに基づいて）無差別アラートの優先順位を下げるのに役立ちます。

インライン モードでは、センサーで攻撃パケットを拒否することができ、それらがターゲット ホストに到達することはないので、ターゲットに脆弱性があったとしても問題になりません。ネットワーク上での攻撃が不可能になっていれば、リスク レーティングの値は引き下げません。

サービス、OS、アプリケーションのいずれにも固有ではないシグニチャの場合、無差別デルタの値は 0 になります。シグニチャが OS、サービス、またはアプリケーションに固有の場合は、カテゴリごとに 5 つのポイントで 5、10、または 15 の無差別デルタが計算されます。

詳細情報

- 無差別モードの詳細については、「無差別モード」（P.5-3）を参照してください。
- リスク レーティングの詳細については、「リスク レーティングの計算」（P.8-12）を参照してください。

アラート頻度の設定

シグニチャ定義サブモードで **alert-frequency** コマンドを使用して、シグニチャのアラート頻度を設定します。**alert-frequency** コマンドは、このシグニチャが起動しているときにセンサーがユーザにアラートを発行する頻度を指定します。

オプション

次のオプションが適用されます。

- *sig_id*：このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。値は 1000 ～ 65000 です。
- *subsig_id*：このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID は、広範なシグニチャをより詳細に識別するために使用します。値は 0 ～ 255 です。

- **summary-mode**：センサーがアラートをグループ化する方法を指定します。
  - **fire-all**：すべてのイベントに対してアラートを起動します。
  - **fire-once**：1 回だけアラートを起動します。
  - **global-summarize**：攻撃者や攻撃対象の数に関係なく 1 回だけアラートが起動されるようにアラートをサマライズします。
  - **summarize**：すべてのアラートをサマライズします。
- **specify-summary-threshold {yes | no}**：サマリーしきい値モードをイネーブルにします。
  - **summary-threshold**：このシグニチャのサマリー アラートが送信される前にセンサーで受信されなければならない最小ヒット数を指定します。値は 0 ～ 65535 です。
  - **summary-interval**：各サマリー アラートで使用される時間間隔（秒数）を指定します。値は 1 ～ 1000 です。
- **summary-key**：このシグニチャをサマライズするストレージ タイプを指定します。
  - **Axxx**：攻撃者のアドレス。
  - **Axxb**：攻撃者のアドレスと攻撃対象のポート。
  - **AxBx**：攻撃者と攻撃対象のアドレス。
  - **AaBb**：攻撃者と攻撃対象のアドレスおよびポート。
  - **xxBx**：攻撃対象のアドレス。
- **specify-global-summary-threshold {yes | no}**：（任意）グローバル サマリーしきい値モードをイネーブルにします。
  - **global-summary-threshold**：アラートがグローバル サマリーにまとめられるイベント数のしきい値を指定します。値は 1 ～ 65535 です。

アラート頻度の設定

シグニチャのアラート頻度パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 9000 0
```

ステップ 4　アラート頻度サブモードを開始します。

```
ips-ssp(config-sig-sig)# alert-frequency
```

ステップ 5　このシグニチャのアラート頻度を指定します。

a. サマリー モードを、たとえば 1 回だけ起動するように設定します。

```
ips-ssp(config-sig-sig-ale)# summary-mode fire-once
ips-ssp(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
ips-ssp(config-sig-sig-ale-fir-yes)# global-summary-threshold 3000
ips-ssp(config-sig-sig-ale-fir-yes)# summary-interval 5000
```

b. サマリー キーを指定します。

```
ips-ssp(config-sig-sig-ale-fir-yes)# exit
ips-ssp(config-sig-sig-ale-fir)# summary-key AxBx
```

c. 設定を確認できます。

```
ips-ssp(config-sig-sig-ale-fir)# show settings
   fire-once
   -----------------------------------------------
      summary-key: AxBx default: Axxx
      specify-global-summary-threshold
      -------------------------------------------------
         yes
         -----------------------------------------------
            global-summary-threshold: 3000 default: 120
            summary-interval: 5000 default: 15
         -----------------------------------------------
      -------------------------------------------------
   -----------------------------------------------
ips-ssp(config-sig-sig-ale-fir)#
```

ステップ 6　アラート頻度サブモードを終了します。

```
ips-ssp(config-sig-sig-ale-fir)# exit
ips-ssp(config-sig-sig-ale)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

アラート重大度の設定

シグニチャ定義サブモードで **alert-severity** コマンドを使用して、シグニチャの重大度を設定します。

オプション

次のオプションが適用されます。

- *sig_id*：このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。値は 1000 ～ 65000 です。
- *subsig_id*：このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID は、広範なシグニチャをより詳細に識別するために使用します。値は 0 ～ 255 です。
- **alert-severity**：アラートの重大度を指定します。
  - **high**：危険なアラート。
  - **medium**：中レベルのアラート（デフォルト）。
  - **low**：低レベルのアラート。
  - **informational**：情報のアラート。

アラート重大度の設定

アラート重大度を設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 9000 0
```

ステップ 4　アラート重大度を割り当てます。

```
ips-ssp(config-sig-sig)# alert-severity medium
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-sig-sig)# show settings
   <protected entry>
   sig-id: 9000
   subsig-id: 0
   -----------------------------------------------
      alert-severity: medium default: medium
      sig-fidelity-rating: 75 <defaulted>
      promisc-delta: 0 <defaulted>
      sig-description
      -----------------------------------------------
         sig-name: Back Door Probe (TCP 12345) <defaulted>
         sig-string-info: SYN to TCP 12345 <defaulted>
         sig-comment: <defaulted>
         alert-traits: 0 <defaulted>
         release: 40 <defaulted>
      -----------------------------------------------
      vulnerable-os: general-os <defaulted>
      engine
      -----------------------------------------------
         atomic-ip
         -----------------------------------------
            event-action: produce-alert <defaulted>
            fragment-status: any <defaulted>
            specify-l4-protocol
            -----------------------------------------
--MORE--
```

ステップ 6　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

イベント カウンタの設定

シグニチャ定義サブモードで **event-counter** コマンドを使用して、センサーがイベントをカウントする方法を設定します。たとえば、センサーが、同じシグニチャが同じアドレス セットに対して 5 回起動した場合にだけアラートを送信するように指定できます。

オプション

次のオプションが適用されます。

- **event-count**：アラートを生成するまでのイベントの発生回数を指定します。有効な範囲は 1 ～ 65535 です。デフォルトは 1 です。
- **event-count-key**：このシグニチャに関するイベントをカウントするストレージ タイプを指定します。
  - **Axxx**：攻撃者のアドレス
  - **AxBx**：攻撃者と攻撃対象のアドレス
  - **Axxb**：攻撃者のアドレスと攻撃対象のポート
  - **xxBx**：攻撃対象のアドレス
  - **AaBb**：攻撃者と攻撃対象のアドレスおよびポート
- **specify-alert-interval {yes | no}**：アラート間隔をイネーブルにします。
  - **alert-interval**：イベント カウントがリセットされるまでに必要な時間（秒数）を指定します。デフォルトは 60 です。

イベント カウンタの設定

イベント カウンタを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　イベント カウンタを設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 9000 0
```

ステップ 4　イベント カウンタ サブモードを開始します。

```
ips-ssp(config-sig-sig)# event-counter
```

ステップ 5　アラートが生成されるまでに必要なイベントの発生回数を指定します。

```
ips-ssp(config-sig-sig-eve)# event-count 2
```

ステップ 6　このシグニチャのイベントをカウントするストレージ タイプを指定します。

```
ips-ssp(config-sig-sig-eve)# event-count-key AxBx
```

ステップ 7　（任意）アラート間隔をイネーブルにします。

```
ips-ssp(config-sig-sig-eve)# specify-alert-interval yes
```

ステップ 8　（任意）イベント カウントがリセットされるまでに必要な時間（秒数）を指定します。

```
ips-ssp(config-sig-sig-eve-yes)# alert-interval 30
```

ステップ 9　設定を確認できます。

```
ips-ssp(config-sig-sig-eve-yes)# exit
ips-ssp(config-sig-sig-eve)# show settings
   event-counter
   -----------------------------------------------
      event-count: 2 default: 1
      event-count-key: AxBx default: Axxx
      specify-alert-interval
      -----------------------------------------------
         yes
         -----------------------------------------------
            alert-interval: 30 default: 60
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-sig-sig-eve)#
```

ステップ 10　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig-eve)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

シグニチャ忠実度レーティングの設定

シグニチャ定義サブモードで **sig-fidelity-rating** コマンドを使用して、シグニチャのシグニチャ忠実度レーティングを設定します。

オプション

次のオプションが適用されます。

- **sig-fidelity-rating**：ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。有効な値は 0 ～ 100 です。

シグニチャ忠実度レーティングの設定

シグニチャのシグニチャ忠実度レーティングを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
```

ステップ 3　設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 12000 0
```

ステップ 4　このシグニチャのシグニチャ忠実度レーティングを指定します。

```
ips-ssp(config-sig-sig)# sig-fidelity-rating 50
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-sig-sig)# show settings
   <protected entry>
   sig-id: 12000
   subsig-id: 0
   -----------------------------------------------
      alert-severity: low <defaulted>
      sig-fidelity-rating: 50 default: 85
      promisc-delta: 15 <defaulted>
      sig-description
      ----------------------------------------------
         sig-name: Gator Spyware Beacon <defaulted>
         sig-string-info: /download/ User-Agent: Gator <defaulted>
         sig-comment: <defaulted>
         alert-traits: 0 <defaulted>
         release: 71 <defaulted>
      ----------------------------------------------
```

ステップ 6　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

シグニチャのステータスの設定

シグニチャ定義サブモードで **status** コマンドを使用して、特定のシグニチャのステータスを指定します。

オプション

次のオプションが適用されます。

- **status**：シグニチャの状態がイネーブルか、ディセーブルか、廃棄かどうかを示します。
  - **enabled {true | false}**：シグニチャをイネーブルにします。
  - **retired {true | false}]**：シグニチャを廃棄にします。
  - **obsoletes** *signature_ID*：このシグニチャによって廃止されている他のシグニチャを表示します。

注意　シグニチャの有効化および廃棄には、30 分以上の時間がかかる場合があります。

シグニチャ ステータスの設定

シグニチャのステータスを変更するには、次の作業を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　設定するシグニチャを選択します。

```
ips-ssp(config-sig)# signatures 12000 0
```

ステップ 4　このシグニチャのステータスを変更します。

```
ips-ssp(config-sig-sig)# status
ips-ssp(config-sig-sig-sta)# enabled true
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true default: false
      retired: false <defaulted>
   -----------------------------------------------
ips-ssp(config-sig-sig-sta)#
```

ステップ 6　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig-sta)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

シグニチャの脆弱性のある OS の設定

シグニチャ定義サブモードで **vulnerable-os** コマンドを使用して、シグニチャの脆弱性のある OS のリストを設定します。

オプション

次のオプションが適用されます。

- **general-os**：すべての OS タイプ
- **ios**：各種 Cisco IOS
- **mac-os**：各種 Macintosh OS
- **netware**：Netware
- **other**：その他すべての OS
- **unix**：各種 UNIX
- **aix**：各種 AIX
- **bsd**：各種 BSD
- **hp-ux**：各種 HP-UX
- **irix**：各種 IRIX
- **linux**：各種 Linux
- **solaris**：各種 Solaris
- **windows**：各種 Microsoft Windows
- **windows-nt-2k-xp**：各種 Microsoft NT、2000、および XP
- **win-nt**：特定の種類の Windows NT

脆弱性のある OS の設定

シグニチャの脆弱性のある OS を設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 6000 0
```

ステップ 4　このシグニチャの脆弱性のある OS を指定します。

```
ips-ssp(config-sig-sig)# vulnerable-os linux|aix
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-sig-sig)# show settings
   sig-id: 60000
   subsig-id: 0
   -----------------------------------------------
      alert-severity: medium <defaulted>
      sig-fidelity-rating: 75 <defaulted>
      promisc-delta: 0 <defaulted>
      sig-description
      ----------------------------------------------
         sig-name: My Sig <defaulted>
         sig-string-info: My Sig Info <defaulted>
         sig-comment: Sig Comment <defaulted>
         alert-traits: 0 <defaulted>
         release: custom <defaulted>
      ----------------------------------------------
      vulnerable-os: aix|linux default: general-os
*---> engine
      ----------------------------------------------
      ----------------------------------------------
      event-counter
      ----------------------------------------------
         event-count: 1 <defaulted>
         event-count-key: Axxx <defaulted>
         specify-alert-interval
         ----------------------------------------------
--MORE--
```

ステップ 6　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

シグニチャへのアクションの割り当て

シグニチャ定義サブモードで **event-action** コマンドを使用して、シグニチャが起動したときにセンサーが実行するアクションを設定します。

オプション

次のオプションが適用されます。

- **event-action :** このシグニチャが起動したときにセンサーが実行するイベント アクションを指定します。
  - **deny-attacker-inline**：（インラインのみ）指定された期間、この攻撃者のアドレスからの現在および将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象ポートがペアになっている現在および将来のパケットを送信しません。
  - **deny-attacker-victim-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象アドレスがペアになっている現在および将来のパケットを送信しません。
  - **deny-connection-inline**：（インラインのみ）この TCP フロー上の現在および将来のパケットを送信しません。
  - **deny-packet-inline**（インラインのみ）現在のパケットを送信しません。
  - **log-attacker-packets**:攻撃者のアドレスが含まれているパケットの IP ロギングを開始します。
  - **log-pair-packets**：攻撃者と攻撃対象のアドレスのペアが含まれているパケットの IP ロギングを開始します。
  - **log-victim-packets**:攻撃対象のアドレスが含まれているパケットの IP ロギングを開始します。
  - **produce-alert**：イベントをアラートとしてイベント ストアに書き込みます。
  - **produce-verbose-alert**：攻撃パケットの符号化されたダンプ（切り詰められる可能性あり）をアラートに含めます。
  - **request-block-connection**：要求を ARC に送信して、この接続をブロックします。
  - **request-block-host**：要求を ARC に送信して、この攻撃者のホストをブロックします。
  - **request-rate-limit**：レート制限要求を ARC に送信して、レート制限を実行します。
  - **request-snmp-trap**：要求をセンサーの通知アプリケーション コンポーネントに送信して、SNMP 通知を実行します。
  - **reset-tcp-connection**：TCP リセットを送信して、TCP フローをハイジャックし、終了します。
  - **modify-packet-inline**：エンド ポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- **event-action-settings**：**external-rate-limit-type** を設定できます。
  - **none**：設定されているレート制限はありません。
  - **percentage**：トラフィックのパーセンテージによるレート制限を設定します（**external-rate-limit-percentage**）。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、または deny-packet-inline をアクションとして追加するイベント アクション オーバーライドの場合、次のアクションが実行される場合があります。

- droppedPacket

- deniedFlow
- tcpOneWayResetSent

パケットのインライン拒否アクションは、アラート内でドロップ パケット アクションとして表示されます。パケットのインライン拒否が TCP 接続に対して発生すると、自動的に接続のインライン拒否アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

接続のインライン拒否が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

イベント アクションの設定

シグニチャのイベント アクションおよびイベント アクション設定を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)#
```

ステップ 3　設定するシグニチャを指定します。

```
ips-ssp(config-sig)# signatures 1200 0
```

ステップ 4　シグニチャ エンジンを指定します（シグニチャ 1200 の場合はノーマライザ エンジンです）。

```
ips-ssp(config-sig-sig)# engine normalizer
```

ステップ 5　イベント アクションを設定します。

```
ips-ssp(config-sig-sig-nor)# event-action produce-alert|request-snmp-trap
```

（注）　シグニチャにイベント アクションを設定するたびに、前の設定は上書きされます。たとえば、シグニチャが起動されるたびに必ずアラートが生成されるようにする場合は、そのアクションを他の必要なイベント アクションと一緒に設定する必要があります。| 記号を使用して、**product-alert|deny-packet-inline|request-snmp-trap** のように複数のイベント アクションを追加します。

ステップ 6　設定を確認できます。

```
ips-ssp(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-snmp-trap default:
produce-alert|deny-packet-inline
```

ステップ 7　レート制限のパーセンテージを指定します。

```
ips-ssp(config-sig-sig-nor)# event-action-settings
ips-ssp(config-sig-sig-nor-eve)# external-rate-limit-type percentage
ips-ssp(config-sig-sig-nor-eve-per)# external-rate-limit-percentage 50
```

ステップ 8　設定を確認できます。

```
ips-ssp(config-sig-sig-nor-eve-per)# show settings
   percentage
   -----------------------------------------------
      external-rate-limit-percentage: 50 default: 100
   -----------------------------------------------
```

ステップ 9　イベント アクション サブモードを終了します。

```
ips-ssp(config-sig-sig-nor-eve-per)# exit
ips-ssp(config-sig-sig-nor-eve)# exit
ips-ssp(config-sig-sig-nor)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 10　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

イベント アクションの詳細については、「イベント アクション」（P.8-4）を参照してください。

AIC シグニチャの設定

ここでは、アプリケーション検査および制御（AIC）シグニチャ、およびその設定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。

- 「AIC エンジンについて」（P.7-18）
- 「AIC エンジンとセンサーのパフォーマンス」（P.7-19）
- 「アプリケーション ポリシーの設定」（P.7-20）
- 「AIC 要求メソッド シグニチャ」（P.7-21）
- 「AIC MIME 定義コンテンツ タイプ シグニチャ」（P.7-22）
- 「AIC 転送符号化シグニチャ」（P.7-25）
- 「AIC FTP コマンド シグニチャ」（P.7-26）
- 「AIC シグニチャの作成」（P.7-27）

AIC エンジンについて

AIC は、Web トラフィックを徹底的に分析できます。HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。また、指定されたポート上でトンネルを作成しようとするインスタント メッセージングや gotomypc などのアプリケーションを管理制御できます。P2P およびインスタント メッセージングが HTTP で動作している場合は、それらのアプリケーションの検査チェックおよびポリシー チェックが可能です。AIC は、FTP トラフィックを検査し、実行されているコマンドを制御する方法も提供します。事前に定義されているシグニチャをイネーブルまたはディセーブルにしたり、カスタム シグニチャによってポリシーを作成したりできます。

（注）　AIC エンジンは、HTTP トラフィックが AIC Web ポート上で受信されたときに動作します。トラフィックが Web トラフィックでも、AIC Web ポート上で受信されなければ、Service HTTP エンジンが実行されます。AIC 検査は、AIC Web ポートとして設定されたポートで、検査対象のトラフィックが HTTP トラフィックであれば、任意のポート上に存在できます。

AIC には、次のカテゴリのシグニチャが含まれます。

- HTTP 要求メソッド
  - 定義要求メソッド
  - 認識される要求メソッド
- MIME タイプ
  - 定義コンテンツ タイプ
  - 認識されるコンテンツ タイプ
- 定義 Web トラフィック ポリシー

  1 つの事前に定義されたシグニチャ 12674 があります。これは、非準拠の HTTP トラフィックが検出されたときに実行するアクションを指定しています。パラメータ Alarm on Non HTTP Traffic は、このシグニチャをイネーブルにします。デフォルトでは、このシグニチャはイネーブルになっています。
- 転送符号化
  - 各メソッドへのアクションの関連付け
  - センサーで認識されるメソッドの一覧表示
  - チャンク符号化エラーが検出されたときにどのアクションを実行する必要があるかの指定
- FTP コマンド
  - FTP コマンドへのアクションの関連付け。

詳細情報

- これらのシグニチャのシグニチャ ID および説明のリストについては、「AIC 要求メソッド シグニチャ」（P.7-21）、「AIC MIME 定義コンテンツ タイプ シグニチャ」（P.7-22）、「AIC 転送符号化シグニチャ」（P.7-25）、および「AIC FTP コマンド シグニチャ」（P.7-26）を参照してください。
- カスタム MIME シグニチャの作成手順については、「AIC シグニチャの作成」（P.7-27）を参照してください。

AIC エンジンとセンサーのパフォーマンス

アプリケーション ポリシーの適用は、独自のセンサー機能です。AIC ポリシーの適用は、悪用、脆弱性、および異常を検査する従来の IPS テクノロジーをベースにしたものではなく、HTTP サービス ポリシーと FTP サービス ポリシーを適用するように設計されています。このポリシー適用に必要な検査動作は、従来の IPS 検査動作と比べて負荷が非常に高くなります。この機能の使用には、パフォーマンスの大幅な低下が伴います。AIC がイネーブルの場合、センサーの全体的な帯域幅キャパシティが減少します。

AIC ポリシーの適用は、IPS デフォルト設定ではディセーブルになっています。AIC ポリシーの適用を有効にする場合は、必要なポリシーだけを慎重に選択し、必要のないポリシーはディセーブルにすることを強く推奨します。また、センサーの検査負荷が最大容量に近くなっている場合は、センサーがオーバーサブスクライブされる可能性があるので、この機能の使用は推奨されません。このタイプのポリシー適用を処理する場合は、適応型セキュリティ アプライアンス ファイアウォールを使用することを推奨します。

アプリケーション ポリシーの設定

シグニチャ定義サブモードで **application-policy** コマンドを使用して、Web AIC 機能をイネーブルにします。レイヤ 4 からレイヤ 7 パケットの検査を提供して Web サービスおよび FTP サービスに関連した悪意のある攻撃を阻止するようにセンサーを設定できます。

オプション

次のオプションが適用されます。

- **ftp-enable {true | false}**：FTP サービスの保護をイネーブルにします。センサーで FTP トラフィックを検査する必要がある場合は、true に設定します。デフォルトは false です。
- **http-policy**：HTTP トラフィックの検査をイネーブルにします。
  - **aic-web-ports**：AIC トラフィックを検索するポートを表す変数を指定します。有効な範囲は 0 ～ 65535 です。0 ～ 65535 の範囲内に収まる、カンマで区切られた整数範囲のリストです（a-b[,c-d]）。範囲の 2 番目の数は、最初の数以上である必要があります。デフォルトは、80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,24326-24326 です。
  - **http-enable {true | false}**：Web サービスの保護をイネーブルにします。RFC に準拠するために、センサーで HTTP トラフィックを検査する必要がある場合は、true に設定します。デフォルトは false です。
  - **max-outstanding-http-requests-per-connection**：接続あたりの最大許容 HTTP 要求数を指定します。有効な値は 1 ～ 16 です。デフォルトは 10 です。

アプリケーション ポリシーの設定

アプリケーション ポリシーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　アプリケーション ポリシー サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
ips-ssp(config-sig)# application-policy
```

ステップ 3　FTP トラフィックの検査をイネーブルにします。

```
ips-ssp(config-sig-app)# ftp-enable true
```

ステップ 4　HTTP アプリケーション ポリシーを設定します。

a. HTTP アプリケーション ポリシー サブモードを開始します。

```
ips-ssp(config-sig-app)# http-policy
```

b. HTTP アプリケーション ポリシーの適用をイネーブルにします。

```
ips-ssp(config-sig-app-htt)# http-enable true
```

c. サーバからの応答を受信せずに未処理状態でいることが可能な、接続あたりの未処理 HTTP 要求の数を指定します。

```
ips-ssp(config-sig-app-htt)# max-outstanding-http-requests-per-connection 5
```

d. AIC ポートを編集します。

```
ips-ssp(config-sig-app-htt)# aic-web-ports 80-80,3128-3128
```

ステップ 5　設定値を確認します。

```
ips-ssp(config-sig-app-htt)# exit
ips-ssp(config-sig-app)# show settings
   application-policy
   -----------------------------------------------
      http-policy
      -----------------------------------------------
         http-enable: true default: false
         max-outstanding-http-requests-per-connection: 5 default: 10
         aic-web-ports: 80-80,3128-3128 default: 80-80,3128-3128,8000-8000,8010-
8010,8080-8080,8888-8888,24326-24326
      -----------------------------------------------
      ftp-enable: true default: false
   -----------------------------------------------
ips-ssp(config-sig-app)#
```

ステップ 6　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-app)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

AIC 要求メソッド シグニチャ

HTTP 要求メソッドには、2 つのカテゴリのシグニチャがあります。

- 定義要求メソッド：アクションが要求メソッドに関連付けられます。シグニチャの拡張と変更ができます（Define Request Method）。
- 認識される要求メソッド：センサーによって認識されるメソッドの一覧を表示します（Recognized Request Methods）。

表 7-1 に、事前に定義されている定義要求メソッド シグニチャを示します。必要な事前定義メソッドを持つシグニチャをイネーブルにします。

表 7-1　要求メソッド シグニチャ

シグニチャ ID	定義要求メソッド
12676	要求メソッドは認識されない
12677	定義要求メソッド PUT
12678	定義要求メソッド CONNECT
12679	定義要求メソッド DELETE
12680	定義要求メソッド GET
12681	定義要求メソッド HEAD
12682	定義要求メソッド OPTIONS
12683	定義要求メソッド POST
12685	定義要求メソッド TRACE
12695	定義要求メソッド INDEX
12696	定義要求メソッド MOVE
12697	定義要求メソッド MKDIR

表 7-1　要求メソッド シグニチャ （続き）

シグニチャ ID	定義要求メソッド
12698	定義要求メソッド COPY
12699	定義要求メソッド EDIT
12700	定義要求メソッド UNEDIT
12701	定義要求メソッド SAVE
12702	定義要求メソッド LOCK
12703	定義要求メソッド UNLOCK
12704	定義要求メソッド REVLABEL
12705	定義要求メソッド REVLOG
12706	定義要求メソッド REVADD
12707	定義要求メソッド REVNUM
12708	定義要求メソッド SETATTRIBUTE
12709	定義要求メソッド GETATTRIBUTENAME
12710	定義要求メソッド GETPROPERTIES
12711	定義要求メソッド STARTENV
12712	定義要求メソッド STOPREV

詳細情報

シグニチャをイネーブルにする手順については、「シグニチャのステータスの設定」（P.7-13）を参照してください。

AIC MIME 定義コンテンツ タイプ シグニチャ

MIME タイプに関連したポリシーは 2 つあります。

- 定義コンテンツ タイプ : 次の場合に対して特定のアクションを関連付けます（Define Content Type）。
  - image/jpeg など、特定の MIME タイプを拒否
  - メッセージ サイズ違反
  - ヘッダーと本体に記述されている MIME タイプが不一致
- 認識されるコンテンツ タイプ（Recognized Content Type）

表 7-2 に、事前に定義されている定義コンテンツ タイプ シグニチャを示します。必要な事前定義コンテンツ タイプを持つシグニチャをイネーブルにします。また、カスタム定義コンテンツ タイプ シグニチャを作成することもできます。

表 7-2　定義コンテンツ タイプ シグニチャ

シグニチャ ID	シグニチャの説明
12621	コンテンツ タイプ image/gif のメッセージ長が無効です。
12622 2	コンテンツ タイプ image/png の検証に失敗しました。
12623 0 12623 1 12623 2	コンテンツ タイプ image/tiff のヘッダー チェック。 コンテンツ タイプ image/tiff のメッセージ長が無効です。 コンテンツ タイプ image/tiff の検証に失敗しました。

表 7-2　定義コンテンツ タイプ シグニチャ （続き）

シグニチャ ID	シグニチャの説明
12624 0	コンテンツ タイプ image/x-3ds のヘッダー チェック。
12624 1	コンテンツ タイプ image/x-3ds のメッセージ長が無効です。
12624 2	コンテンツ タイプ image/x-3ds の検証に失敗しました。
12626 0	コンテンツ タイプ image/x-portable-bitmap のヘッダー チェック。
12626 1	コンテンツ タイプ image/x-portable-bitmap のメッセージ長が無効です。
12626 2	コンテンツ タイプ image/x-portable-bitmap の検証に失敗しました。
12627 0	コンテンツ タイプ image/x-portable-graymap のヘッダー チェック。
12627 1	コンテンツ タイプ image/x-portable-graymap のメッセージ長が無効です。
12627 2	コンテンツ タイプ image/x-portable-graymap の検証に失敗しました。
12628 0	コンテンツ タイプ image/jpeg のヘッダー チェック。
12628 1	コンテンツ タイプ image/jpeg のメッセージ長が無効です。
12628 2	コンテンツ タイプ image/jpeg の検証に失敗しました。
12629 0	コンテンツ タイプ image/cgf のヘッダー チェック。
12629 1	コンテンツ タイプ image/cgf のメッセージ長が無効です。
12631 0	コンテンツ タイプ image/x-xpm のヘッダー チェック。
12631 1	コンテンツ タイプ image/x-xpm のメッセージ長が無効です。
12633 0	コンテンツ タイプ audio/midi のヘッダー チェック。
12633 1	コンテンツ タイプ audio/midi のメッセージ長が無効です。
12633 2	コンテンツ タイプ audio/midi の検証に失敗しました。
12634 0	コンテンツ タイプ audio/basic のヘッダー チェック。
12634 1	コンテンツ タイプ audio/basic のメッセージ長が無効です。
12634 2	コンテンツ タイプ audio/basic の検証に失敗しました。
12635 0	コンテンツ タイプ audio/mpeg のヘッダー チェック。
12635 1	コンテンツ タイプ audio/mpeg のメッセージ長が無効です。
12635 2	コンテンツ タイプ audio/mpeg の検証に失敗しました。
12636 0	コンテンツ タイプ audio/x-adpcm のヘッダー チェック。
12636 1	コンテンツ タイプ audio/x-adpcm のメッセージ長が無効です。
12636 2	コンテンツ タイプ audio/x-adpcm の検証に失敗しました。
12637 0	コンテンツ タイプ audio/x-aiff のヘッダー チェック。
12637 1	コンテンツ タイプ audio/x-aiff のメッセージ長が無効です。
12637 2	コンテンツ タイプ audio/x-aiff の検証に失敗しました。
12638 0	コンテンツ タイプ audio/x-ogg のヘッダー チェック。
12638 1	コンテンツ タイプ audio/x-ogg のメッセージ長が無効です。
12638 2	コンテンツ タイプ audio/x-ogg の検証に失敗しました。
12639 0	コンテンツ タイプ audio/x-wav のヘッダー チェック。
12639 1	コンテンツ タイプ audio/x-wav のメッセージ長が無効です。
12639 2	コンテンツ タイプ audio/x-wav の検証に失敗しました。
12641 0	コンテンツ タイプ text/html のヘッダー チェック。
12641 1	コンテンツ タイプ text/html のメッセージ長が無効です。
12641 2	コンテンツ タイプ text/html の検証に失敗しました。
12642 0	コンテンツ タイプ text/css のヘッダー チェック。
12642 1	コンテンツ タイプ text/css のメッセージ長が無効です。
12643 0	コンテンツ タイプ text/plain のヘッダー チェック。
12643 1	コンテンツ タイプ text/plain のメッセージ長が無効です。

表 7-2　定義コンテンツ タイプ シグニチャ （続き）

シグニチャ ID	シグニチャの説明
12644 0 12644 1	コンテンツ タイプ text/richtext のヘッダー チェック。 コンテンツ タイプ text/richtext のメッセージ長が無効です。
12645 0 12645 1 12645 2	コンテンツ タイプ text/sgml のヘッダー チェック。 コンテンツ タイプ text/sgml のメッセージ長が無効です。 コンテンツ タイプ text/sgml の検証に失敗しました。
12646 0 12646 1 12646 2	コンテンツ タイプ text/xml のヘッダー チェック。 コンテンツ タイプ text/xml のメッセージ長が無効です。 コンテンツ タイプ text/xml の検証に失敗しました。
12648 0 12648 1 12648 2	コンテンツ タイプ video/flc のヘッダー チェック。 コンテンツ タイプ video/flc のメッセージ長が無効です。 コンテンツ タイプ video/flc の検証に失敗しました。
12649 0 12649 1 12649 2	コンテンツ タイプ video/mpeg のヘッダー チェック。 コンテンツ タイプ video/mpeg のメッセージ長が無効です。 コンテンツ タイプ video/mpeg の検証に失敗しました。
12650 0 12650 1	コンテンツ タイプ text/xmcd のヘッダー チェック。 コンテンツ タイプ text/xmcd のメッセージ長が無効です。
12651 0 12651 1 12651 2	コンテンツ タイプ video/quicktime のヘッダー チェック。 コンテンツ タイプ video/quicktime のメッセージ長が無効です。 コンテンツ タイプ video/quicktime の検証に失敗しました。
12652 0 12652 1	コンテンツ タイプ video/sgi のヘッダー チェック。 コンテンツ タイプ video/sgi の検証に失敗しました。
12653 0 12653 1	コンテンツ タイプ video/x-avi のヘッダー チェック。 コンテンツ タイプ video/x-avi のメッセージ長が無効です。
12654 0 12654 1 12654 2	コンテンツ タイプ video/x-fli のヘッダー チェック。 コンテンツ タイプ video/x-fli のメッセージ長が無効です。 コンテンツ タイプ video/x-fli の検証に失敗しました。
12655 0 12655 1 12655 2	コンテンツ タイプ video/x-mng のヘッダー チェック。 コンテンツ タイプ video/x-mng のメッセージ長が無効です。 コンテンツ タイプ video/x-mng の検証に失敗しました。
12656 0 12656 1 12656 2	コンテンツ タイプ application/x-msvideo のヘッダー チェック。 コンテンツ タイプ application/x-msvideo のメッセージ長が無効です。 コンテンツ タイプ application/x-msvideo の検証に失敗しました。
12658 0 12658 1	コンテンツ タイプ application/ms-word のヘッダー チェック。 コンテンツ タイプ application/ms-word のメッセージ長が無効です。
12659 0 12659 1	コンテンツ タイプ application/octet-stream のヘッダー チェック。 コンテンツ タイプ application/octet-stream のメッセージ長が無効です。
12660 0 12660 1 12660 2	コンテンツ タイプ application/postscript のヘッダー チェック。 コンテンツ タイプ application/postscript のメッセージ長が無効です。 コンテンツ タイプ application/postscript の検証に失敗しました。
12661 0 12661 1	コンテンツ タイプ application/vnd.ms-excel のヘッダー チェック。 コンテンツ タイプ application/vnd.ms-excel のメッセージ長が無効です。
12662 0 12662 1	コンテンツ タイプ application/vnd.ms-powerpoint のヘッダー チェック。 コンテンツ タイプ application/vnd.ms-powerpoint のメッセージ長が無効です。

表 7-2　定義コンテンツ タイプ シグニチャ （続き）

シグニチャ ID	シグニチャの説明
12663 0 12663 1 12663 2	コンテンツ タイプ application/zip のヘッダー チェック。 コンテンツ タイプ application/zip のメッセージ長が無効です。 コンテンツ タイプ application/zip の検証に失敗しました。
12664 0 12664 1 12664 2	コンテンツ タイプ application/x-gzip のヘッダー チェック。 コンテンツ タイプ application/x-gzip のメッセージ長が無効です。 コンテンツ タイプ application/x-gzip の検証に失敗しました。
12665 0 12665 1	コンテンツ タイプ application/x-java-archive のヘッダー チェック。 コンテンツ タイプ application/x-java-archive のメッセージ長が無効です。
12666 0 12666 1	コンテンツ タイプ application/x-java-vm のヘッダー チェック。 コンテンツ タイプ application/x-java-vm のメッセージ長が無効です。
12667 0 12667 1 12667 2	コンテンツ タイプ application/pdf のヘッダー チェック。 コンテンツ タイプ application/pdf のメッセージ長が無効です。 コンテンツ タイプ application/pdf の検証に失敗しました。
12668 0 12668 1	コンテンツ タイプ unknown のヘッダー チェック。 コンテンツ タイプ unknown のメッセージ長が無効です。
12669 0 12669 1	コンテンツ タイプ image/x-bitmap のヘッダー チェック。 コンテンツ タイプ image/x-bitmap のメッセージ長が無効です。
12673 0	認識されるコンテンツ タイプ

詳細情報

- シグニチャをイネーブルにする手順については、「シグニチャのステータスの設定」（P.7-13）を参照してください。
- AIC シグニチャの作成手順については、「AIC シグニチャの作成」（P.7-27）を参照してください。

AIC 転送符号化シグニチャ

転送符号化に関連したポリシーは 3 つあります。

- 各メソッドへのアクションの関連付け（Define Transfer Encoding）
- センサーで認識されるメソッドの一覧表示（Recognized Transfer Encodings）
- チャンク符号化エラーが検出されたときにどのアクションを実行する必要があるかの指定（Chunked Transfer Encoding Error）

表 7-3 に、事前に定義されている転送符号化シグニチャを示します。必要な事前定義の転送符号化メソッドを持つシグニチャをイネーブルにします。

表 7-3　転送符号化シグニチャ

シグニチャ ID	転送符号化メソッド
12686	認識される転送符号化
12687	定義転送符号化 Deflate
12688	定義転送符号化 Identity
12689	定義転送符号化 Compress
12690	定義転送符号化 GZIP

表 7-3　転送符号化シグニチャ （続き）

シグニチャ ID	転送符号化メソッド
12693	定義転送符号化 Chunked
12694	チャンク転送符号化エラー

詳細情報

シグニチャをイネーブルにする手順については、「シグニチャのステータスの設定」（P.7-13）を参照してください。

AIC FTP コマンド シグニチャ

表 7-4 に、事前に定義されている FTP コマンド シグニチャを示します。必要な事前定義 FTP コマンドを持つシグニチャをイネーブルにします。

表 7-4　FTP コマンド シグニチャ

シグニチャ ID	FTP コマンド
12900	認識されない FTP コマンド
12901	定義 FTP コマンド abor
12902	定義 FTP コマンド acct
12903	定義 FTP コマンド allo
12904	定義 FTP コマンド appe
12905	定義 FTP コマンド cdup
12906	定義 FTP コマンド cwd
12907	定義 FTP コマンド dele
12908	定義 FTP コマンド help
12909	定義 FTP コマンド list
12910	定義 FTP コマンド mkd
12911	定義 FTP コマンド mode
12912	定義 FTP コマンド nlst
12913	定義 FTP コマンド noop
12914	定義 FTP コマンド pass
12915	定義 FTP コマンド pasv
12916	定義 FTP コマンド port
12917	定義 FTP コマンド pwd
12918	定義 FTP コマンド quit
12919	定義 FTP コマンド rein
12920	定義 FTP コマンド rest
12921	定義 FTP コマンド retr
12922	定義 FTP コマンド rmd
12923	定義 FTP コマンド rnfr
12924	定義 FTP コマンド rnto

表 7-4　FTP コマンド シグニチャ （続き）

シグニチャ ID	FTP コマンド
12925	定義 FTP コマンド site
12926	定義 FTP コマンド smnt
12927	定義 FTP コマンド stat
12928	定義 FTP コマンド stor
12929	定義 FTP コマンド stou
12930	定義 FTP コマンド stru
12931	定義 FTP コマンド syst
12932	定義 FTP コマンド type
12933	定義 FTP コマンド user

詳細情報

シグニチャをイネーブルにする手順については、「シグニチャのステータスの設定」（P.7-13）を参照してください。

AIC シグニチャの作成

次に、AIC エンジンに基づいて MIME タイプ シグニチャを作成する例を示します。

オプション

次のオプションが適用されます。

- **event-action**：アラートがトリガーされたときに実行するアクションを指定します。
  - **deny-attacker-inline**：（インラインのみ）指定された期間、この攻撃者のアドレスからの現在および将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象ポートがペアになっている現在および将来のパケットを送信しません。
  - **deny-attacker-victim-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象アドレスがペアになっている現在および将来のパケットを送信しません。
  - **deny-connection-inline**：（インラインのみ）この TCP フロー上の現在および将来のパケットを送信しません。
  - **deny-packet-inline**（インラインのみ）現在のパケットを送信しません。
  - **log-attacker-packets**：攻撃者のアドレスが含まれているパケットの IP ロギングを開始します。
  - **log-pair-packets**：攻撃者と攻撃対象のアドレスのペアが含まれているパケットの IP ロギングを開始します。
  - **log-victim-packets**：攻撃対象のアドレスが含まれているパケットの IP ロギングを開始します。
  - **produce-alert**：イベントをアラートとしてイベント ストアに書き込みます。
  - **produce-verbose-alert**：攻撃パケットの符号化されたダンプ（切り詰められる可能性あり）をアラートに含めます。
  - **request-block-connection**：要求を ARC に送信して、この接続をブロックします。
  - **request-block-host**：要求を ARC に送信して、この攻撃者のホストをブロックします。
  - **request-rate-limit**：レート制限要求を ARC に送信して、レート制限を実行します。

  - **request-snmp-trap**：要求をセンサーの通知アプリケーション コンポーネントに送信して、SNMP 通知を実行します。
  - **reset-tcp-connection**：TCP リセットを送信して、TCP フローをハイジャックし、終了します。
  - **modify-packet-inline**：エンド ポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- **no**：エントリまたは選択の設定を削除します。
- **signature-type**：必要なシグニチャのタイプを指定します。
  - **content-types**：コンテンツタイプ
  - **define-web-traffic-policy**：Web トラフィック ポリシーの定義
  - **max-outstanding-requests-overrun**：大量の未処理 HTTP 要求が発生していないかの検査
  - **msg-body-pattern**：メッセージ本体のパターン
  - **request-methods**：要求メソッドを処理するシグニチャ タイプ
  - **transfer-encodings**：転送符号化を処理するシグニチャ タイプ

MIME タイプ ポリシーの定義

MIME タイプ ポリシー シグニチャを定義するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　アプリケーション ポリシー適用サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
ips-ssp(config-sig)# signatures 60001 0
ips-ssp(config-sig-sig)# engine application-policy-enforcement-http
```

ステップ 3　イベント アクションを指定します。

```
ips-ssp(config-sig-sig-app)# event-action produce-alert|log-pair-packets
```

ステップ 4　シグニチャ タイプを定義します。

```
ips-ssp(config-sig-sig-app)# signature-type content-type define-content-type
```

ステップ 5　コンテンツ タイプを定義します。

```
ips-ssp(config-sig-sig-app-def)# name MyContent
```

ステップ 6　設定値を確認します。

```
ips-ssp(config-sig-sig-app-def)# show settings
-> define-content-type
   -----------------------------------------------
      name: MyContent
*---> content-type-details
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-sig-sig-app-def)#
```

ステップ 7　シグニチャ サブモードを終了します。

```
ips-ssp(config-sig-sig-app-def)# exit
ips-ssp(config-sig-sig-app)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

IP フラグメント再構成の設定

ここでは、IP フラグメント再構成について説明し、IP フラグメント再構成シグニチャの一覧とその設定可能なパラメータを示します。また、それらのパラメータを設定する方法、および IP フラグメント再構成の方式を設定する方法についても説明します。次のような構成になっています。

- 「IP フラグメント再構成について」（P.7-29）
- 「IP フラグメント再構成シグニチャと設定可能なパラメータ」（P.7-29）
- 「IP フラグメント再構成パラメータの設定」（P.7-31）
- 「IP フラグメント再構成の方式の設定」（P.7-32）

IP フラグメント再構成について

センサーは、複数のパケットにわたってフラグメント化されたデータグラムを再構成するように設定できます。このとき、再構成するデータグラム フラグメントの数と、データグラムについてさらにフラグメントが届くのを待つ時間を判断するために使用する境界値を指定できます。これは、センサーがフレーム送信を受信できなかったことや、無作為にフラグメント化されたデータグラムを生成する攻撃が仕掛けられていることが原因で再構成が不十分なデータグラムに対し、センサーのリソースをすべて割り当ててしまわないようにするためのものです。

（注）　IP フラグメント再構成はシグニチャ単位で設定します。

IP フラグメント再構成シグニチャと設定可能なパラメータ

表 7-5 に、IP フラグメント再構成のために設定できる IP フラグメント再構成シグニチャとその設定可能なパラメータを示します。IP フラグメント再構成シグニチャは、ノーマライザ エンジンの一部です。

表 7-5　IP フラグメント再構成シグニチャ

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1200 IP Fragmentation Buffer Full	システム内のフラグメントの合計数が Max Fragments で設定されたしきい値を超えると起動します。	Max Fragments：10000（0 ～ 42000）	Deny Packet Inline Produce Alert[1]
1201 Fragment Overlap	データグラムに対してキューイングされているフラグメントの間で重複が発生すると起動します。	なし[2]	

表 7-5　IP フラグメント再構成シグニチャ （続き）

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1202 Datagram Too Long	フラグメント データ（オフセットとサイズ）が Max Datagram Size で設定されたしきい値を超えると起動します。	Max Datagram Size：65536（2000 ～ 65536）	Deny Packet Inline Produce Alert[3]
1203 Fragment Overwrite	データグラムに対してキューイングされているフラグメントの間で重複が発生し、その重複しているデータ間に差異がある場合に起動します。[4]	なし	Deny Packet Inline Produce Alert[5]
1204 No Initial Fragment	データグラムが不完全で、先頭フラグメントが失われている場合に起動します。	なし	Deny Packet Inline Produce Alert[6]
1205 Too Many Datagrams	システム内の部分データグラムの合計数が Max Partial Datagrams で設定されたしきい値を超えると起動します。	Max Partial Datagrams：1000（0 ～ 10000）	Deny Packet Inline Produce Alert[7]
1206 Fragment Too Small	1 つのデータグラム内に Min Fragment Size より小さいサイズのフラグメントが Max Small Frags よりも多く存在すると起動します。[8]	Max Small Frags：2（8 ～ 1500） Min Fragment Size：400（1 ～ 8）	Deny Packet Inline Produce Alert[9]
1207 Too Many Fragments	1 つのデータグラム内に Max Fragments per Datagram よりも多くのフラグメントが存在すると起動します。	Max Fragments per Datagram：170（0-8192）	Deny Packet Inline Produce Alert[10]
1208 Incomplete Datagram	データグラムのフラグメントが 1 つでも Fragment Reassembly Timeout の時間内に到着できなかった場合に起動します。[11]	Fragment Reassembly Timeout：60（0 ～ 360）	Deny Packet Inline Produce Alert[12]
1220 Jolt2 Fragment Reassembly DoS attack	複数のフラグメントが受信され、それらすべてが IP データグラムの最終フラグメントであると主張している場合に起動します。	Max Last Fragments：4（1 ～ 50）	Deny Packet Inline Produce Alert[13]
1225 Fragment Flags Invalid	不正な組み合わせのフラグメント フラグが検出されると起動します。	なし[14]	

1. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。このシグニチャをディセーブルにしても、デフォルト値が使用されます。それによりパケットがドロップされたり（インライン モード）、分析されなかったり（無差別モード）しますが、アラートは送信されません。
2. データグラムが完全な複製の場合、このシグニチャは起動しません。完全な複製は、インライン モードでは設定に関係なくドロップされます。Modify Packet Inline は、エンドポイントがデータグラムを処理する方法についてあいまいさが残らないように、重複しているデータをそのうちの 1 つだけ残してすべて削除します。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
3. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。データグラムが Max Datagram Size より大きい場合、設定されたアクションに関係なく、データグラムは IPS で処理されません。
4. これは、きわめて異常なイベントです。
5. Modify Packet Inline は、エンドポイントがデータグラムを処理する方法についてあいまいさが残らないように、重複しているデータをそのうちの 1 つだけ残してすべて削除します。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
6. IPS は、設定に関係なく、先頭フラグメントのないデータグラムは検査しません。Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。

7. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
8. このシグニチャがオンで、小さいフラグメントの数が超過している場合、IPS はデータグラムを検査しません。
9. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
10. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
11. データグラムのパケットが到着するとタイマーが始動します。
12. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
13. Modify Packet Inline と Deny Connection Inline はこのシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。
14. Modify Packet Inline は、それらのフラグを有効な組み合わせに修正します。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このデータグラムのパケットおよびすべての関連するフラグメントをドロップします。

詳細情報

ノーマライザ エンジンの詳細については、「ノーマライザ エンジン」（P.B-33）を参照してください。

IP フラグメント再構成パラメータの設定

特定のシグニチャの IP フラグメント再構成パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　IP フラグメント再構成シグニチャ ID とサブシグニチャ ID を指定します。

```
ips-ssp(config-sig)# signatures 1200 0
```

ステップ 4　エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine normalizer
```

ステップ 5　デフォルト シグニチャの編集サブモードを開始します。

```
ips-ssp(config-sig-sig-nor)# edit-default-sigs-only default-signatures-only
```

ステップ 6　シグニチャ 1200 の任意の IP フラグメント再構成パラメータについて（必要に応じて）デフォルト設定をイネーブルにし、変更します。たとえば、最大フラグメント数を指定します。

```
ips-ssp(config-sig-sig-nor-def)# specify-max-fragments yes
ips-ssp(config-sig-sig-nor-def-yes)# max-fragments 20000
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-sig-sig-nor-def-yes)# show settings
   yes
   -----------------------------------------------
      max-fragments: 20000 default: 10000
   -----------------------------------------------
ips-ssp(config-sig-sig-nor-def-yes)#
```

ステップ 8　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-nor-def-yes)# exit
ips-ssp(config-sig-sig-nor-def)# exit
ips-ssp(config-sig-sig-nor)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

IP フラグメント再構成の方式の設定

シグニチャ定義サブモードで **fragment-reassembly** コマンドを使用して、センサーがフラグメントの再構成に使用する方式を設定します。このオプションは、センサーが無差別モードで動作している場合に設定できます。センサーがインライン モードで動作している場合、方式は NT のみになります。

オプション

次のオプションが適用されます。

- **ip-reassemble-mode**：センサーがフラグメントの再構成に使用する方式をオペレーティング システムに基づいて示します。
  - **nt**：Windows システム。
  - **solaris**：Solaris システム。
  - **linux**：GNU/Linux システム。
  - **bsd**：BSD UNIX システム。

    デフォルトは nt です。

IP フラグメント再構成の方式の設定

IP フラグメント再構成の方式を設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　フラグメント再構成サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
ips-ssp(config-sig)# fragment-reassembly
```

ステップ 3　センサーが IP フラグメントの再構成に使用するオペレーティング システムを設定します。

```
ips-ssp(config-sig-fra)# ip-reassemble-mode linux
```

ステップ 4　設定を確認します。

```
ips-ssp(config-sig-fra)# show settings
   fragment-reassembly
   -----------------------------------------------
      ip-reassemble-mode: linux default: nt
   -----------------------------------------------
ips-ssp(config-sig-fra)#
```

ステップ 5　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-fra)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

TCP ストリーム再構成の設定

ここでは、TCP ストリーム再構成について説明し、TCP ストリーム再構成シグニチャの一覧とその設定可能なパラメータを示します。また、TCP ストリーム シグニチャを設定する方法、および TCP ストリーム再構成のモードを設定する方法についても説明します。次のような構成になっています。

- 「TCP ストリーム再構成について」（P.7-33）
- 「TCP ストリーム再構成シグニチャと設定可能なパラメータ」（P.7-34）
- 「TCP ストリーム再構成シグニチャの設定」（P.7-39）
- 「TCP ストリーム再構成のモードの設定」（P.7-40）

TCP ストリーム再構成について

センサーは、完了した 3 ウェイ ハンドシェイクによって確立された TCP セッションだけをモニタするように設定できます。また、ハンドシェイクの完了まで待つ時間の最大値と、パケットがない場合に接続をモニタし続ける時間も設定できます。これは、有効な TCP セッションが確立していないときにセンサーがアラートを生成しないようにするためのものです。センサーに対する攻撃には、単純に攻撃を繰り返すだけでセンサーにアラートを生成させようとするものがあります。TCP セッションの再構成機能は、センサーに対するこのような攻撃の緩和に役立ちます。

TCP ストリーム再構成パラメータはシグニチャ単位で設定します。TCP ストリーム再構成のモードを設定できます。

TCP ストリーム再構成シグニチャと設定可能なパラメータ

表 7-6 に、TCP ストリーム再構成のために設定できる TCP ストリーム再構成シグニチャとその設定可能なパラメータを示します。TCP ストリーム再構成シグニチャは、ノーマライザ エンジンの一部です。

表 7-6　TCP ストリーム再構成シグニチャ

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1300 TCP Segment Overwrite[1]	重複する TCP セグメント（再送信など）により、このセッションですでに検出されているデータとは異なるデータが送信されると起動します。	—	Deny Connection Inline Product Alert[2]
1301 TCP Inactive Timeout[3]	TCP セッションのアイドル状態が TCP Idle Timeout の時間続くと起動します。	TCP Idle Timeout：3600（15 ～ 3600）	なし[4]
1302 TCP Embryonic Timeout[5]	TCP セッションのスリーウェイ ハンドシェイクが TCP Embryonic Timeout の秒数内で完了しないと起動します。	TCP Embryonic Timeout：15（3 ～ 300）	なし[6]
1303 TCP Closing Timeout[7]	TCP セッションが最初の FIN を受信してから TCP Closed Timeout の秒数以内に完全に閉じないと起動します。	TCP Closed Timeout：5（1 ～ 60）	なし[8]
1304 TCP Max Segments Queued Per Session	セッションに対してキューイングされた無効セグメントの数が TCP Max Queue を超えると起動します。期待されるシーケンスから最も遠いシーケンスが含まれるセグメントがドロップされます。	TCP Max Queue：32（0 ～ 128）	Deny Packet Inline Product Alert[9]
1305 TCP Urgent Flag[10]	TCP 緊急フラグが検出されると起動します。	—	Modify Packet Inline がディセーブル[11]
1306 0 TCP Option Other	TCP Option Number の範囲内の TCP オプションが検出されると起動します。	TCP Option Number：6 ～ 7、9 ～ 255（0 ～ 255 の範囲内での複数の整数範囲）	Modify Packet Inline Produce Alert[12]
1306 1 TCP SACK Allowed Option	TCP 選択 ACK 許可オプションが検出されると起動します。	—	Modify Packet Inline がディセーブル[13]
1306 2 TCP SACK Data Option	TCP 選択 ACK データ オプションが検出されると起動します。	—	Modify Packet Inline がディセーブル[14]

表 7-6　TCP ストリーム再構成シグニチャ （続き）

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1306 3 TCP Timestamp Option	TCP タイムスタンプ オプションが検出されると起動します。	—	Modify Packet Inline がディセーブル[15]
1306 4 TCP Window Scale Option	TCP ウィンドウ スケール オプションが検出されると起動します。	—	Modify Packet Inline がディセーブル[16]
1307 TCP Window Size Variation	TCP の受信ウィンドウの右端が右に移動する（減少する）と起動します。	—	Deny Connection Inline Produce Alert がディセーブル[17]
1308 TTL Varies[18]	セッションの一方向で検出された TTL が確認済みの最小値よりも大きいと起動します。	—	Modify Packet Inline[19]
1309 TCP Reserved Bits Set	TCP ヘッダー上で予約ビット（ECN に使用されるビットも含む）が設定されると起動します。	—	Modify Packet Inline Produce Alert がディセーブル[20]
1310 TCP Retransmit Protection[21]	再送信されたセグメントに元のセグメントとは異なるデータが含まれていることをセンサーが検出すると起動します。	—	Deny Connection Inline Produce Alert[22]
1311 TCP Packet Exceeds MSS	パケットがスリーウェイ ハンドシェイク中に交換された MSS を超えていると起動します。	—	Deny Connection Inline Produce Alert[23]
1312 TCP Min MSS	SYN フラグの含まれるパケット内の MSS 値が TCP Min MSS より小さいと起動します。	TCP Min MSS：400（0 ～ 16000）	Modify Packet Inline がディセーブル[24]
1313 TCP Max MSS	SYN フラグの含まれるパケット内の MSS 値が TCP Max MSS を超えていると起動します。	TCP Max MSS：1460（0 ～ 16000）	Modify Packet Inline がディセーブル[25]
1314 TCP Data SYN	SYN パケットで TCP ペイロードが送信されると起動します。	—	Deny Packet Inline がディセーブル[26]
1315 ACK Without TCP Stream	ストリームに属していない ACK パケットが送信されると起動します。	—	Produce Alert がディセーブル[27]
1317 Zero Window Probe	ゼロ ウィンドウ プローブ パケットが検出されると起動します。	Modify Packet Inline は、ゼロ ウィンドウ プローブ パケットからデータを削除します。	Modify Packet Inline

表 7-6　TCP ストリーム再構成シグニチャ （続き）

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1330[28] 0 TCP Drop - Bad Checksum	TCP パケットのチェックサムが不正な場合に起動します。	Modify Packet Inline は、チェックサムを訂正します。	Deny Packet Inline
1330 1 TCP Drop - Bad TCP Flags	TCP パケットのフラグの組み合わせが不正な場合に起動します。	—	Deny Packet Inline
1330 2 TCP Drop - Urgent Pointer With No Flag	TCP パケットに URG ポインタが設定されているのに URG フラグがない場合に起動します。	Modify Packet Inline は、ポインタをクリアします。	Modify Packet Inline がディセーブル
1330 3 TCP Drop - Bad Option List	TCP パケットのオプション リストが不正な場合に起動します。	—	Deny Packet Inline
1330 4 TCP Drop - Bad Option Length	TCP パケットのオプションの長さが不正な場合に起動します。	—	Deny Packet Inline
1330 5 TCP Drop - MSS Option Without SYN	SYN フラグが設定されていないパケット内で TCP MSS オプションが検出されると起動します。	Modify Packet Inline は、MSS オプションをクリアします。	Modify Packet Inline
1330 6 TCP Drop - WinScale Option Without SYN	SYN フラグが設定されていないパケット内で TCP ウィンドウ スケール オプションが検出されると起動します。	Modify Packet Inline は、ウィンドウ スケール オプションをクリアします。	Modify Packet Inline
1330 7 TCP Drop - Bad WinScale Option Value	TCP パケットのウィンドウ スケール値が不正な場合に起動します。	Modify Packet Inline は、最も近い制約値に値を設定します。	Modify Packet Inline
1330 8 TCP Drop - SACK Allow Without SYN	SYN フラグが設定されていないパケット内で TCP SACK 許可オプションが検出されると起動します。	Modify Packet Inline は、SACK 許可オプションをクリアします。	Modify Packet Inline
1330 9 TCP Drop - Data in SYN|ACK	SYN フラグと ACK フラグが設定されている TCP パケットにデータも格納されている場合に起動します。	—	Deny Packet Inline
1330 10 TCP Drop - Data Past FIN	FIN の後に TCP データがシーケンスされると起動します。	—	Deny Packet Inline

表 7-6　TCP ストリーム再構成シグニチャ （続き）

シグニチャ ID と名前	説明	パラメータ：デフォルト値（範囲）	デフォルト アクション
1330 11 TCP Drop - Timestamp not Allowed	タイムスタンプ オプションが許可されていないときに、TCP パケットにタイムスタンプ オプションが含まれていると起動します。	—	Deny Packet Inline
1330 12 TCP Drop - Segment Out of Order	TCP セグメントが無効なためキューイングできない場合に起動します。	—	Deny Packet Inline
1330 13 TCP Drop - Invalid TCP Packet	TCP パケットのヘッダーが不正の場合に起動します。	—	Deny Packet Inline
1330 14 TCP Drop - RST or SYN in window	RST フラグまたは SYN フラグを持つ TCP パケットがシーケンス ウィンドウで送信されたが、次のシーケンスではなかった場合に起動します。	—	Deny Packet Inline
1330 15 TCP Drop - Segment Already ACKed	TCP パケット シーケンスがピアによってすでに確認応答されている場合に起動します（キープアライブは除く）。	—	Deny Packet Inline
1330 16 TCP Drop - PAWS Failed	TCP パケットが PAWS チェックに失敗すると起動します。	—	Deny Packet Inline
1330 17 TCP Drop - Segment out of State Order	TCP パケットが TCP セッションの状態に対して適切ではない場合に起動します。	—	Deny Packet Inline
1330 18 TCP Drop - Segment out of Window	TCP パケットのシーケンス番号が許可されているウィンドウの範囲外にある場合に起動します。	—	Deny Packet Inline
3050 Half Open SYN Attack		syn-flood-max-embryonic：5000	
3250 TCP Hijack		max-old-ack：200	
3251 TCP Hijack Simplex Mode		max-old-ack：100	

1. IPS は、TCP セッションの各方向において最後の 256 バイトを保持します。
2. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
3. タイマーは、TCP セッション上をパケットが通過するたびに 0 にリセットされます。デフォルトでは、このシグニチャはアラートを生成しません。必要ならば TCP 接続の期限切れに関するアラートを生成させることもできます。期限の切れたフローの合計数に関する統計情報は、フローが期限切れになるたびに更新されます。
4. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
5. タイマーは最初の SYN パケットで始動し、リセットはされません。セッションの状態はリセットされ、このフローの後続のパケットは無効であると見なされます（SYN の場合を除く）。

6. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
7. タイマーは最初の FIN パケットで始動し、リセットはされません。セッションの状態はリセットされ、このフローの後続のパケットは無効であると見なされます（SYN の場合を除く）。
8. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
9. Modify Packet Inline と Deny Packet Inline はこのシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。
10. Phrak 57 は、URG ポインタを使用してセキュリティ ポリシーを回避する方法を記述します。インライン モードの場合、このシグニチャでパケットを正規化できます。
11. Modify Packet Inline は、そのパケットの URG フラグを取り除き、URG ポインタをゼロにします。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
12. Modify Packet Inline は、選択されたオプションをパケットから取り除きます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
13. Modify Packet Inline は、選択された ACK 許可オプションをパケットから取り除きます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
14. Modify Packet Inline は、選択された ACK 許可オプションをパケットから取り除きます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
15. Modify Packet Inline は、タイムスタンプ オプションをパケットから取り除きます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
16. Modify Packet Inline は、ウィンドウ スケール オプションをパケットから取り除きます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
17. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
18. このシグニチャは、セッション上の各方向に対して TTL を単調減少させるために使用されます。たとえば、TTL 45 が A から B の間で検出される最小の TTL の場合、Modify Packet Inline が設定されていると、それ以降の A から B に向かうすべてのパケットは、最大値が 45 になります。新しい小さい TTL が検出されるたびに、その値がそのセッション上の新しい最大値になります。
19. Modify Packet Inline は、IP TTL が単調減少することを保証します。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
20. Modify Packet Inline は、すべての予約 TCP フラグをクリアします。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
21. このシグニチャは、シグニチャ 1300 のように最後の 256 バイトに制限されることはありません。
22. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
23. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
24. 2.4.21-15.EL.cisco.1 Modify Packet Inline は、MSS 値を TCP Min MSS に引き上げます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline は、パケット 2.4.21-15.EL.cisco.1 をドロップします。
25. Modify Packet Inline は、MSS 値を TCP Max MSS に引き下げます。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline は、パケット 2.4.21-15.EL.cisco.1 をドロップします。
26. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は、現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
27. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。デフォルトでは、このシグニチャでアラートが送信されるパケットは、1330 シグニチャによってドロップされます。
28. これらのサブシグニチャは、ノーマライザが TCP パケットをドロップする理由を表します。デフォルトでは、これらのサブシグニチャはパケットをドロップします。これらのサブシグニチャを使用すると、ノーマライザのチェックに合格しないパケットに対して IPS の通過を許可できるようになります。ドロップ理由は、TCP 統計情報に集計されます。デフォルトでは、これらのサブシグニチャはアラートを生成しません。

詳細情報

ノーマライザ エンジンの詳細については、「ノーマライザ エンジン」（P.B-33）を参照してください。

TCP ストリーム再構成シグニチャの設定

特定のシグニチャの TCP ストリーム再構成を設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　TCP ストリーム再構成シグニチャ ID とサブシグニチャ ID を指定します。

```
ips-ssp(config-sig)# signatures 1313 0
```

ステップ 4　エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine normalizer
```

ステップ 5　デフォルト シグニチャの編集サブモードを開始します。

```
ips-ssp(config-sig-sig-nor)# edit-default-sigs-only default-signatures-only
```

ステップ 6　シグニチャ 1313 の最大 MSS パラメータについて（必要に応じて）デフォルト設定をイネーブルにし、変更します。

```
ips-ssp(config-sig-sig-nor-def)# specify-tcp-max-mss yes
ips-ssp(config-sig-sig-nor-def-yes)# tcp-max-mss 1380
```

（注）　このパラメータをデフォルトの 1460 から 1380 に変更すると、VPN トンネルを通過するトラフィックのフラグメンテーションを防止するのに役立ちます。

ステップ 7　設定を確認できます。

```
ips-ssp(config-sig-sig-nor-def-yes)# show settings
   yes
   -----------------------------------------------
      tcp-max-mss: 1380 default: 1460
   -----------------------------------------------
ips-ssp(config-sig-sig-nor-def-yes)#
```

ステップ 8　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-nor-def-yes)# exit
ips-ssp(config-sig-sig-nor-def)# exit
ips-ssp(config-sig-sig-nor)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

TCP ストリーム再構成のモードの設定

シグニチャ定義サブモードで **stream-reassembly** コマンドを使用して、センサーが TCP セッションの再構成に使用するモードを設定します。

（注） パラメータ **tcp-3-way-handshake-required** と tcp-reassembly-mode only は、無差別モードでトラフィックを検査しているセンサーに影響を与えます。インライン モードでは影響ありません。

オプション

次のオプションが適用されます。

- **tcp-3-way-handshake-required {true | false}**：スリーウェイ ハンドシェイクを完了したセッションのみをセンサーで追跡することを指定します。デフォルトは true です。
- **tcp-reassembly-mode**：センサーが TCP セッションの再構成に使用するモードを指定します。
  - **strict**：シーケンスで次に予測されるものだけを許可します。
  - **loose**：シーケンスのギャップを許容します。
  - **asym**：非対称トラフィックの再構成を許可します。

    デフォルトは strict です。

注意 非対称オプションは、TCP ウィンドウ回避チェックをディセーブルにします。

TCP ストリーム再構成パラメータの設定

TCP ストリーム再構成パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　TCP ストリーム再構成サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
ips-ssp(config-sig)# stream-reassembly
```

ステップ 3　スリーウェイ ハンドシェイクを完了したセッションのみをセンサーで追跡することを指定します。

```
ips-ssp(config-sig-str)# tcp-3-way-handshake-required true
```

ステップ 4　センサーが TCP セッションの再構成に使用するモードを指定します。

```
ips-ssp(config-sig-str)# tcp-reassembly-mode strict
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-sig-str)# show settings
   stream-reassembly
   -----------------------------------------------
      tcp-3-way-handshake-required: true default: true
      tcp-reassembly-mode: strict default: strict
   -----------------------------------------------
ips-ssp(config-sig-str)#
```

ステップ 6　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-str)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

IP ロギングの設定

センサーが攻撃を検出したときに、IP セッション ログを生成するように設定できます。シグニチャの応答アクションとして IP ロギングが設定されているときにシグニチャがトリガーされると、アラートの送信元アドレスとの間で送受信されるすべてのパケットが指定された時間の間ログに記録されます。

シグニチャ定義サブモードで **ip-log** コマンドを使用して、IP ロギングを設定します。

オプション

次のオプションが適用されます。

- **ip-log-bytes**：ログに記録する最大バイト数を指定します。有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。
- **ip-log-packets**：ログに記録するパケットの数を指定します。有効な値は 0 ～ 65535 です。デフォルトは 0 です。
- **ip-log-time**：センサーでログを記録する期間を指定します。有効な値は 30 ～ 300 秒です。デフォルトは 30 秒です。

（注）　センサーは、これらの IP ロギング条件のいずれか 1 つを満たすと、IP ロギングを停止します。

IP ロギング パラメータの設定

IP ロギング パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　IP ログ サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
ips-ssp(config-sig)# ip-log
```

ステップ 3　IP ロギング パラメータを指定します。

a.　ログに記録する最大バイト数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-bytes 200000
```

b.　ログに記録するパケット数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-packets 150
```

c.　センサーでログを記録する時間の長さを指定します。

```
ips-ssp(config-sig-ip)# ip-log-time 60
```

ステップ 4　設定を確認できます。

```
ips-ssp(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 150 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 200000 default: 0
   -----------------------------------------------
ips-ssp(config-sig-ip)#
```

ステップ 5　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-ip)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

カスタム シグニチャの作成

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

ここでは、カスタム シグニチャを作成する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。

- 「カスタム シグニチャの作成手順」（P.7-42）
- 「String TCP エンジン シグニチャの例」（P.7-43）
- 「Service HTTP エンジン シグニチャの例」（P.7-46）
- 「Meta エンジン シグニチャの例」（P.7-49）
- 「Atomic IP Advanced エンジン シグニチャの例」（P.7-53）
- 「String XL エンジンの一致オフセット シグニチャの例」（P.7-54）
- 「String XL エンジンの最小一致長シグニチャの例」（P.7-57）

カスタム シグニチャの作成手順

カスタム シグニチャを作成するには、次の手順を使用します。

ステップ 1　シグニチャ エンジンを選択します。

ステップ 2　シグニチャの識別情報を割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラート ノート（オプション）

- ユーザ コメント（オプション）

ステップ 3　エンジン固有のパラメータを割り当てます。これらのパラメータはシグニチャ エンジンごとに異なりますが、各エンジンに適用される一群のマスター パラメータが存在します。

ステップ 4　アラート応答を割り当てます。

- シグニチャ忠実度レーティング
- アラートの重大度

ステップ 5　アラート動作を割り当てます。

ステップ 6　変更を適用します。

String TCP エンジン シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

（注）　この手順は、String UDP エンジン シグニチャと String ICMP エンジン シグニチャにも適用されます。

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用のパターンマッチング検査エンジンです。String エンジンでは、複数のパターンを 1 つのパターンマッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。String エンジンには、String ICMP、String TCP、および String UDP の 3 種類が存在します。

オプション

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **direction**：トラフィックの方向を指定します。
  - **from-service**：サービス ポートからクライアント ポート宛のトラフィック。
  - **to-service**：クライアント ポートからサービス ポート宛のトラフィック。
- **event-action**：アラートがトリガーされたときに実行するアクションを指定します。
  - **deny-attacker-inline**：（インラインのみ）指定された期間、この攻撃者のアドレスからの現在および将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象ポートがペアになっている現在および将来のパケットを送信しません。
  - **deny-attacker-victim-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象アドレスがペアになっている現在および将来のパケットを送信しません。
  - **deny-connection-inline**：（インラインのみ）この TCP フロー上の現在および将来のパケットを送信しません。
  - **deny-packet-inline**（インラインのみ）現在のパケットを送信しません。
  - **log-attacker-packets**：攻撃者のアドレスが含まれているパケットの IP ロギングを開始します。

  - **log-pair-packets**：攻撃者と攻撃対象のアドレスのペアが含まれているパケットの IP ロギングを開始します。
  - **log-victim-packets**：攻撃対象のアドレスが含まれているパケットの IP ロギングを開始します。
  - **produce-alert**：イベントをアラートとしてイベント ストアに書き込みます。
  - **produce-verbose-alert**：攻撃パケットの符号化されたダンプ（切り詰められる可能性あり）をアラートに含めます。
  - **request-block-connection**：要求を ARC に送信して、この接続をブロックします。
  - **request-block-host**：要求を ARC に送信して、この攻撃者のホストをブロックします。
  - **request-rate-limit**：レート制限要求を ARC に送信して、レート制限を実行します。
  - **request-snmp-trap**：要求をセンサーの通知アプリケーション コンポーネントに送信して、SNMP 通知を実行します。
  - **reset-tcp-connection**：TCP リセットを送信して、TCP フローをハイジャックし、終了します。
  - **modify-packet-inline**：エンド ポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- **no**：エントリまたは選択の設定を削除します。
- **regex-string**：単一の TCP パケット内で検索する正規表現を指定します。
- **service-ports**：ターゲット サービスが常駐する可能性のあるポートまたはポート範囲を指定します。有効な範囲は 0 ～ 65535 です。これは、0 ～ 65535 の範囲内に収まる整数範囲のリストです（a-b[,c-d]）。範囲の 2 番目の数は、最初の数以上である必要があります。
- **specify-exact-match-offset {yes | no}**：（任意）完全一致オフセットをイネーブルにします。
- **specify-min-match-length {yes | no}**：（任意）最小一致長をイネーブルにします。
- **strip-telnet-options**：検索前にデータから Telnet オプション文字を取り除きます。
- **swap-attacker-victim {true | false}**：アラート メッセージ内および実行されるアクションに対し、攻撃者と攻撃対象（送信元と宛先）のアドレスおよびポートを交換します。デフォルトは、交換しないことを意味する false です。

String TCP エンジン シグニチャの作成

String TCP エンジンに基づいてシグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 60025 0
```

ステップ 4　シグニチャ説明サブモードを開始します。

```
ips-ssp(config-sig-sig)# sig-description
```

ステップ 5　新しいシグニチャの名前を指定します。また、**sig-comment** コマンドを使用してシグニチャに関する追加コメントを指定したり、**sig-string-info** コマンドを使用してシグニチャに関する追加情報を指定したりすることもできます。

```
ips-ssp(config-sig-sig-sig)# sig-name This is my new name
```

ステップ 6　シグニチャ説明サブモードを終了します。

```
ips-ssp(config-sig-sig-sig)# exit
```

ステップ 7　String TCP エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine string-tcp
```

ステップ 8　サービス ポートを指定します。

```
ips-ssp(config-sig-sig-str)# service-ports 23
```

ステップ 9　方向を指定します。

```
ips-ssp(config-sig-sig-str)# direction to-service
```

ステップ 10　TCP パケット内で検索する正規表現文字列を指定します。セキュリティ ポリシーに従い、必要ならば **event-action** コマンドを使用してイベント アクションを変更できます。デフォルトのイベント アクションは、**produce-alert** です。

```
ips-ssp(config-sig-sig-str)# regex-string This-is-my-new-Sig-regex
```

ステップ 11　このカスタム String TCP シグニチャに対して、次のオプション パラメータを変更できます。

- **specify-exact-match-offset**
- **specify-min-match-length**
- **strip-telnet-options**
- **swap-attacker-victim**

ステップ 12　設定を確認できます。

```
ips-ssp(config-sig-sig-str)# show settings
   string-tcp
   -----------------------------------------------
      event-action: produce-alert <defaulted>
      strip-telnet-options: false <defaulted>
      specify-min-match-length
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      regex-string: This-is-my-new-Sig-regex
      service-ports: 23
      direction: to-service default: to-service
      specify-exact-match-offset
      -----------------------------------------------
         no
         -----------------------------------------------
            specify-max-match-offset
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-min-match-offset
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
```

```
      swap-attacker-victim: false <defaulted>
   -----------------------------------------------
ips-ssp(config-sig-sig-str)#
```

ステップ 13　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-str)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 14　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

Service HTTP エンジン シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

Service HTTP エンジンは、サービスに特化した文字列ベースのパターンマッチング検査エンジンです。HTTP プロトコルは、今日のネットワークで最も一般的に使用されるプロトコルの 1 つです。また、必要な前処理の時間が非常に長く、検査を必要とするシグニチャも非常に多いため、システムの全体的なパフォーマンスを決める要因になっています。

Service HTTP エンジンでは、複数のパターンを 1 つのパターンマッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現ライブラリが使用されます。このエンジンは、Web サービスに向かう方向のみのトラフィック、または HTTP 要求を検索します。このエンジンでリターン トラフィックを検査することはできません。このエンジンでは、シグニチャごとに対象の Web ポートを別々に指定できます。

HTTP 解読とは、符号化された文字を ASCII 対応文字に正規化することによって、HTTP メッセージをデコードするプロセスです。このプロセスは、ASCII 正規化と呼ばれることもあります。

HTTP パケットを検査するには、あらかじめそのデータを、ターゲット システムでのデータ処理時に表示されるものと同じデータ表現として解読または正規化しておく必要があります。また、ホスト ターゲット タイプごとにカスタマイズされたデコード方式を用意することが推奨されます。そのためには、ターゲット上で動作しているオペレーティング システムおよび Web サーバのバージョンを確認する必要があります。Service HTTP エンジンのデフォルトの解読動作は Microsoft IIS Web サーバを対象としています。

オプション

次のオプションが適用されます。

- **de-obfuscate {true | false}**：検索前に反回避解読を適用します。
- **default**：値をシステムのデフォルト設定に戻します。
- **event-action**：アラートがトリガーされたときに実行するアクションを指定します。
  - **deny-attacker-inline**：（インラインのみ）指定された期間、この攻撃者のアドレスからの現在および将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象ポートがペアになっている現在および将来のパケットを送信しません。

  - **deny-attacker-victim-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象アドレスがペアになっている現在および将来のパケットを送信しません。
  - **deny-connection-inline**：（インラインのみ）この TCP フロー上の現在および将来のパケットを送信しません。
  - **deny-packet-inline**（インラインのみ）現在のパケットを送信しません。
  - **log-attacker-packets**：攻撃者のアドレスが含まれているパケットの IP ロギングを開始します。このアクションによって、**produce-alert** が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
  - **log-pair-packets**：攻撃者と攻撃対象のアドレスのペアが含まれているパケットの IP ロギングを開始します。このアクションによって、**produce-alert** が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
  - **log-victim-packets**：攻撃対象のアドレスが含まれているパケットの IP ロギングを開始します。このアクションによって、**produce-alert** が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
  - **produce-alert**：イベントをアラートとしてイベント ストアに書き込みます。
  - **produce-verbose-alert**：攻撃パケットの符号化されたダンプ（切り詰められる可能性あり）をアラートに含めます。このアクションによって、**produce-alert** が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
  - **request-block-connection**：要求を ARC に送信して、この接続をブロックします。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
  - **request-block-host**：要求を ARC に送信して、この攻撃者のホストをブロックします。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
  - **request-rate-limit**：レート制限要求を ARC に送信して、レート制限を実行します。レート制限デバイスは、このアクションを実行するように設定されている必要があります。
  - **request-snmp-trap**：要求をセンサーの通知アプリケーション コンポーネントに送信して、SNMP 通知を実行します。このアクションによって、**produce-alert** が選択されていない場合でも、アラートがイベント ストアに書き込まれます。このアクションを実装するには、センサーで SNMP を設定する必要があります。
  - **reset-tcp-connection**：TCP リセットを送信して、TCP フローをハイジャックし、終了します。**Reset TCP Connection** は、単一の接続を分析する TCP シグニチャ上でのみ動作します。スイープまたはフラッドに対しては機能しません。
  - **modify-packet-inline**：エンド ポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- **max-field-sizes**：最大フィールド サイズのグループをイネーブルにします。
  - **specify-max-arg-field-length {yes | no}**：max-arg-field-length をイネーブルにします（オプション）。
  - **specify-max-header-field-length {yes | no}**：max-header-field-length をイネーブルにします（オプション）。
  - **specify-max-request-length {yes | no}**：max-request-length をイネーブルにします（オプション）。
  - **specify-max-uri-field-length {yes | no}**：max-uri-field-length をイネーブルにします（オプション）。
- **no**：エントリまたは選択の設定を削除します。
- **regex**：正規表現のグループをイネーブルにします。
  - **specify-arg-name-regex**：arg-name-regex をイネーブルにします（オプション）。

  - **specify-header-regex**：header-regex をイネーブルにします（オプション）。
  - **specify-request-regex**：request-regex をイネーブルにします（オプション）。
  - **specify-uri-regex**：uri-regex をイネーブルにします（オプション）。
- **service-ports**：ターゲット サービスが常駐する可能性のあるポートまたはポート範囲をカンマ区切りのリストで指定します。
- **swap-attacker-victim {true | false}**：アラート メッセージ内および実行されるアクションに対し、攻撃者と攻撃対象（送信元と宛先）のアドレスおよびポートを交換します。デフォルトは、交換しないことを意味する false です。

Service HTTP エンジン シグニチャの作成

Service HTTP エンジンに基づいてカスタム シグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 63000 0
```

ステップ 4　シグニチャ説明モードを開始します。

```
ips-ssp(config-sig-sig)# sig-description
```

ステップ 5　シグニチャ名を指定します。

```
ips-ssp(config-sig-sig-sig)# sig-name myWebSig
```

ステップ 6　アラート特性を指定します。有効な範囲は 0 ～ 65535 です。

```
ips-ssp(config-sig-sig-sig)# alert-traits 2
```

ステップ 7　シグニチャ説明サブモードを終了します。

```
ips-ssp(config-sig-sig-sig)# exit
```

ステップ 8　アラート頻度を指定します。

```
ips-ssp(config-sig-sig)# alert-frequency
ips-ssp(config-sig-sig-ale)# summary-mode fire-all
ips-ssp(config-sig-sig-ale-fir)# summary-key Axxx
ips-ssp(config-sig-sig-ale-fir)# specify-summary-threshold yes
ips-ssp(config-sig-sig-ale-fir-yes)# summary-threshold 200
```

ステップ 9　アラート頻度サブモードを終了します。

```
ips-ssp(config-sig-sig-ale-fir-yes)# exit
ips-ssp(config-sig-sig-ale-fir)# exit
ips-ssp(config-sig-sig-ale)# exit
```

ステップ 10　検索前に反回避解読を適用するようにシグニチャを設定します。

```
ips-ssp(config-sig-sig)# engine service-http
ips-ssp(config-sig-sig-ser)# de-obfuscate true
```

ステップ 11　正規表現パラメータを設定します。

```
ips-ssp(config-sig-sig)# engine service-http
ips-ssp(config-sig-sig-ser)# regex
ips-ssp(config-sig-sig-ser-reg)# specify-uri-regex yes
ips-ssp(config-sig-sig-ser-reg-yes)# uri-regex [Mm][Yy][Ff][Oo][Oo]
```

ステップ 12　正規表現サブモードを終了します。

```
ips-ssp(config-sig-sig-ser-reg-yes)# exit
ips-ssp(config-sig-sig-ser-reg-)# exit
```

ステップ 13　シグニチャ変数 WEBPORTS を使用してサービス ポートを設定します。

```
ips-ssp(config-sig-sig-ser)# service-ports $WEBPORTS
```

ステップ 14　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-ser)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 15　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

シグニチャの正規表現の構文の一覧表については、付録 B「正規表現の構文」を参照してください。

Meta エンジン シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

注意　Meta エンジン シグニチャを大量に使用すると、全体的なセンサー パフォーマンスに悪影響を与える可能性があります。

Meta エンジンでは、スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。シグネチャ イベントが生成されると、Meta エンジンはシグネチャ イベントを検査して、1 つ以上の Meta 定義に一致するかどうかを判定します。Meta エンジンは、すべてのイベント要件が満たされるとシグネチャ イベントを生成します。

すべてのシグネチャ イベントは、シグニチャ イベント アクション プロセッサによって Meta エンジンに渡されます。シグニチャ イベント アクション プロセッサは、最小ヒット数オプションを処理してからイベントを渡します。Meta エンジンがコンポーネント イベントを処理してから、サマライズおよびイベント アクションは処理されます。

（注）　Meta エンジンは、ほとんどのエンジンがパケットを入力としているにもかかわらず、アラートを入力としている点が他のエンジンとは異なります。

オプション

次のオプションが適用されます。

- **component-list**：Meta コンポーネントのリスト。
  - **edit**：リスト内の既存のエントリを編集します。
  - **insert name1**：新しいエントリをリストに挿入します。
  - **move**：リスト内のエントリを移動します。
  - **begin**：エントリをアクティブ リストの先頭に配置します。
  - **end**：エントリをアクティブ リストの末尾に配置します。
  - **inactive**：エントリを非アクティブ リストに配置します。
  - **before**：エントリを指定エントリの前に配置します。
  - **after**：エントリを指定エントリの後に配置します。
- **component-count**：このコンポーネントが満たされるまでにコンポーネントが起動しなければならない回数を指定します。
- **component-sig-id**：このコンポーネントを照合するシグニチャのシグニチャ ID を指定します。
- **component-subsig-id**：このコンポーネントを照合するシグニチャのサブシグニチャ ID を指定します。
- **component-list-in-order {true | false}**：コンポーネント リストの順に起動するかどうか。
- **event-action**：アラートがトリガーされたときに実行するアクションを指定します。
  - **deny-attacker-inline**：（インラインのみ）指定された期間、この攻撃者のアドレスからの現在および将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象ポートがペアになっている現在および将来のパケットを送信しません。
  - **deny-attacker-victim-pair-inline**：（インラインのみ）指定された期間、この攻撃者アドレスと攻撃対象アドレスがペアになっている現在および将来のパケットを送信しません。
  - **deny-connection-inline**：（インラインのみ）この TCP フロー上の現在および将来のパケットを送信しません。
  - **deny-packet-inline**（インラインのみ）現在のパケットを送信しません。
  - **log-attacker-packets**：攻撃者のアドレスが含まれているパケットの IP ロギングを開始します。
  - **log-pair-packets**：攻撃者と攻撃対象のアドレスのペアが含まれているパケットの IP ロギングを開始します。
  - **log-victim-packets**：攻撃対象のアドレスが含まれているパケットの IP ロギングを開始します。
  - **produce-alert**：イベントをアラートとしてイベント ストアに書き込みます。
  - **produce-verbose-alert**：攻撃パケットの符号化されたダンプ（切り詰められる可能性あり）をアラートに含めます。
  - **request-block-connection**：要求を ARC に送信して、この接続をブロックします。
  - **request-block-host**：要求を ARC に送信して、この攻撃者のホストをブロックします。
  - **request-rate-limit**：レート制限要求を ARC に送信して、レート制限を実行します。
  - **request-snmp-trap**：要求をセンサーの通知アプリケーション コンポーネントに送信して、SNMP 通知を実行します。
  - **reset-tcp-connection**：TCP リセットを送信して、TCP フローをハイジャックし、終了します。

  - **modify-packet-inline**：エンド ポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- **meta-key**：Meta シグニチャのストレージ タイプを指定します。
  - **AaBb**：攻撃者と攻撃対象のアドレスおよびポート。
  - **AxBx**：攻撃者と攻撃対象のアドレス。
  - **Axxx**：攻撃者のアドレス。
  - **xxBx**：攻撃対象のアドレス。
- **meta-reset-interval**：Meta シグニチャをリセットする時間を秒数で指定します。有効な値の範囲は 0 ～ 3600 秒です。デフォルトは 60 秒です。

Meta エンジン シグニチャの作成

シグニチャ 64000 のサブシグニチャ 0 は、シグニチャ 2000 のサブシグニチャ 0 からのアラートとシグニチャ 3000 のサブシグニチャ 0 からのアラートを同じ送信元アドレスで検出すると起動します。送信元アドレスが選択されているのは、メタ キーのデフォルト値が Axxx であるためです。この動作は、メタ キーの設定を xxBx（宛先アドレス）などに変更することにより変更できます。

Meta エンジンに基づいてシグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 64000 0
```

ステップ 4　シグニチャ エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine meta
```

ステップ 5　シグニチャ（名前は c1）をリストの先頭に挿入します。

```
ips-ssp(config-sig-sig-met)# component-list insert c1 begin
```

ステップ 6　このコンポーネントを照合するシグニチャのシグニチャ ID を指定します。

```
ips-ssp(config-sig-sig-met-com)# component-sig-id 2000
```

ステップ 7　コンポーネント リスト サブモードを終了します。

```
ips-ssp(config-sig-sig-met-com)# exit
```

ステップ 8　別のシグニチャ（名前は c2）をリストの末尾に挿入します。

```
ips-ssp(config-sig-sig-met)# component-list insert c2 end
```

ステップ 9　このコンポーネントを照合するシグニチャのシグニチャ ID を指定します。

```
ips-ssp(config-sig-sig-met-com)# component-sig-id 3000
```

ステップ 10　設定を確認できます。

```
ips-ssp(config-sig-sig-met-com)# exit
ips-ssp(config-sig-sig-met)# show settings
   meta
   -----------------------------------------------
      event-action: produce-alert <defaulted>
      meta-reset-interval: 60 <defaulted>
      component-list (min: 1, max: 8, current: 2 - 2 active, 0 inactive)
      -----------------------------------------------
      ACTIVE list-contents
      -----------------------------------------------
         NAME: c1
         -----------------------------------------------
            component-sig-id: 2000
            component-subsig-id: 0 <defaulted>
            component-count: 1 <defaulted>
         -----------------------------------------------
         -----------------------------------------------
         NAME: c2
         -----------------------------------------------
            component-sig-id: 3000
            component-subsig-id: 0 <defaulted>
            component-count: 1 <defaulted>
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      meta-key
      -----------------------------------------------
         Axxx
         -----------------------------------------------
            unique-victims: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      component-list-in-order: false <defaulted>
   -----------------------------------------------
ips-ssp(config-sig-sig-met)#
```

ステップ 11　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-met)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- シグニチャ イベント アクション プロセッサの詳細については、「シグニチャ イベント アクション プロセッサ」（P.8-2）を参照してください。
- Meta エンジンの詳細については、「Meta エンジン」（P.B-31）を参照してください。

Atomic IP Advanced エンジン シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

次の Atomic IP Advanced カスタム シグニチャの例は、IPv6 上でプロトコル ID 88 を禁止します。

Atomic IP Advanced シグニチャ エンジンに基づいてシグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 60000 0
```

ステップ 4　シグニチャ エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine atomic-ip-advanced
```

ステップ 5　IP バージョンを指定します。

```
ips-ssp(config-sig-sig-ato)# specify-ip-version yes
```

ステップ 6　IPv6 を指定します。

```
ips-ssp(config-sig-sig-ato-yes)# version ipv6
```

ステップ 7　L4 プロトコルを指定します。

```
ips-ssp(config-sig-sig-ato-yes-ipv)# exit
ips-ssp(config-sig-sig-ato-yes)# exit
ips-ssp(config-sig-sig-ato)# specify-l4-protocol yes
```

ステップ 8　プロトコル ID 88 を指定します。

```
ips-ssp(config-sig-sig-ato-yes)# l4-protocol other-protocol
ips-ssp(config-sig-sig-ato-yes-oth)# other-ip-protocol-id 88
```

ステップ 9　設定を確認できます。

```
ips-ssp(config-sig-sig-ato-yes-oth)# show settings
   other-protocol
   -----------------------------------------------
      other-ip-protocol-id: 88
   -----------------------------------------------
ips-ssp(config-sig-sig-ato-yes-oth)#
```

ステップ 10　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-ato-yes-oth)# exit
ips-ssp(config-sig-sig-ato-yes)# exit
ips-ssp(config-sig-sig-ato)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- Atomic IP Advanced エンジンの詳細およびパラメータのリストについては、「Atomic IP Advanced エンジン」（P.B-14）を参照してください。
- Atomic エンジンの詳細については、「Atomic エンジン」（P.B-12）を参照してください。

String XL エンジンの一致オフセット シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

（注）　この手順は、String XLUDP シグニチャと String XL ICMP シグニチャにも適用されます。ただし、パラメータ **service-ports** は String XL ICMP シグニチャに適用されません。

オプション

次に、完全一致オフセット、最大一致オフセット、または最小一致オフセットを検索するカスタム String XL TCP シグニチャを作成する例を示します。このカスタム String XL TCP シグニチャに対して、次のオプションの一致オフセット パラメータを変更できます。

- **specify-exact-match-offset {yes |no}**：完全一致オフセットをイネーブルにします。
  - **exact-match-offset**：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット（バイト単位）を指定します。値は 0 ～ 65535 です。
- **specify-max-match-offset {yes |no}**：最大一致長をイネーブルにします。
  - **max-match-offset**：一致を有効にするために正規表現文字列がレポートする必要がある最大ストリーム オフセット（バイト単位）を指定します。値は 0 ～ 65535 です。
- **specify-min-match-offset {yes |no}**：最小一致オフセットをイネーブルにします。
- **min-match-offset**：一致を有効にするために正規表現文字列がレポートする必要がある最小ストリーム オフセット（バイト単位）を指定します。値は 0 ～ 65535 です。

String XL TCP エンジン シグニチャの作成

次に、完全一致オフセット、最大一致オフセット、または最小一致オフセットを検索するカスタム String XL TCP シグニチャを作成する例を示します。

String XL TCP エンジンに基づいて一致を検索するカスタム シグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 60003 0
```

ステップ 4　シグニチャ説明サブモードを開始します。

```
ips-ssp(config-sig-sig)# sig-description
```

ステップ 5　新しいシグニチャの名前を指定します。また、**sig-comment** コマンドを使用してシグニチャに関する追加コメントを指定したり、**sig-string-info** コマンドを使用してシグニチャに関する追加情報を指定したりすることもできます。

```
ips-ssp(config-sig-sig-sig)# sig-name This is my new name
```

ステップ 6　シグニチャ説明サブモードを終了します。

```
ips-ssp(config-sig-sig-sig)# exit
```

ステップ 7　String XL TCP エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine string-xl-tcp
```

ステップ 8　サービス ポートを指定します。

```
ips-ssp(config-sig-sig-str)# service-ports 80
```

ステップ 9　方向を指定します。

```
ips-ssp(config-sig-sig-str)# direction to-service
```

ステップ 10　必要ならば、セキュリティ ポリシーに従い、**event-action** コマンドを使用してイベント アクションを変更します。デフォルトのイベント アクションは、**produce-alert** です。

ステップ 11　raw 正規表現をオフにします。

```
ips-ssp(config-sig-sig-str)# specify-raw-regex-string no
```

（注）　raw 正規表現とは、raw モード処理に使用される正規表現の構文です。エキスパート モード専用であり、Cisco IPS シグニチャ開発チーム、あるいはその監視下にある作業者のみによる使用を対象としています。String XL シグニチャは、通常の正規表現と raw 正規表現のいずれでも設定できます。

ステップ 12　TCP パケット内で検索する正規表現文字列を指定します。

```
ips-ssp(config-sig-sig-str-no)# regex-string tcpstring
```

ステップ 13　オプションの String XL TCP パラメータを設定するために、raw 正規表現モードを終了します。

```
ips-ssp(config-sig-sig-str-no)# exit
ips-ssp(config-sig-sig-str)#
```

ステップ 14　このシグニチャの完全一致オフセットを指定します。

```
ips-ssp(config-sig-sig-str)# specify-exact-match-offset yes
ips-ssp(config-sig-sig-str-yes)# exact-match-offset 20
```

（注）　完全一致オフセットが **yes** に設定されている場合、最大一致オフセットと最小一致オフセットは設定できません。完全一致オフセットが **no** に設定されている場合、最大一致オフセットと最小一致オフセットの両方を同時に設定できます。

ステップ 15　完全一致オフセットをオフにし、このシグニチャの最大一致オフセットを指定します。

```
ips-ssp(config-sig-sig-str-yes)# exit
ips-ssp(config-sig-sig-str)# specify-exact-match-offset no
ips-ssp(config-sig-sig-str-no)# specify-max-match-offset yes
ips-ssp(config-sig-sig-str-no-yes)# max-match-offset 30
```

ステップ 16　このシグニチャの最小一致オフセットを指定します。

```
ips-ssp(config-sig-sig-str-no-yes)# exit
ips-ssp(config-sig-sig-str-no)# specify-min-match-offset yes
ips-ssp(config-sig-sig-str-no-yes)# min-match-offset 20
```

ステップ 17　設定を確認できます。

```
ips-ssp(config-sig-sig-str-no-yes)# exit
ips-ssp(config-sig-sig-str-no)# exit
ips-ssp(config-sig-sig-str)# show settings
   string-xl-tcp
   -----------------------------------------------
      event-action: produce-alert <defaulted>
      strip-telnet-options: false <defaulted>
      direction: to-service default: to-service
      service-ports: 80
      specify-max-stream-length
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      specify-raw-regex-string
      -----------------------------------------------
         no
         -----------------------------------------------
            regex-string: tcpstring
            dot-all: false <defaulted>
            end-optional: false <defaulted>
            no-case: false <defaulted>
            stingy: false <defaulted>
            utf8: false <defaulted>
            specify-min-match-length
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
```

```
            swap-attacker-victim: false <defaulted>
            specify-exact-match-offset
            ------------------------------------------------
               no
               ------------------------------------------------
                  specify-max-match-offset
                  ------------------------------------------------
                     yes
                     ------------------------------------------------
                        max-match-offset: 30
                     ------------------------------------------------
                  ------------------------------------------------
                  specify-min-match-offset
                  ------------------------------------------------
                     yes
                     ------------------------------------------------
                        min-match-offset: 20
                     ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
ips-ssp(config-sig-sig-str)#
```

ステップ 18　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-str)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 19　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- すべての String XL パラメータの一覧については、「String XL エンジン」（P.B-59）を参照してください。
- 正規表現の構文の一覧表については、「正規表現の構文」（P.B-10）を参照してください。

String XL エンジンの最小一致長シグニチャの例

注意　カスタム シグニチャは、センサーのパフォーマンスに影響を与える可能性があります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストして、そのシグニチャがネットワーク全体に与える影響を確認してください。

（注）　この手順は、String XL UDP シグニチャと String XL ICMP シグニチャにも適用されます。ただし、パラメータ **service-ports** は String XL ICMP シグニチャに適用されません。

オプション

次のオプション パラメータを変更して、特定の正規表現文字列を操作できます。

- **dot-all true {true | false}**：true に設定すると、\n も含め [\x00-\xFF] と一致します。false に設定すると、\n を除いた範囲 [\x00-\xFF] 内の任意の文字と一致します。デフォルトは false です。

- **specify-min-match-length {yes | no}**：最小一致長をイネーブルにします。
  - **min-match-length**：パターンがヒットしたと見なされるために正規表現文字列が一致しなければならない最大バイト数を指定します。値は 0 ～ 65535 です。
- **stingy {true | false}**：true に設定すると、最初の一致完了後のより長い一致の検索が中止されます。デフォルトは false です。

（注）　stingy は、**min-match-length** でのみ使用できます。それ以外の場合は無視されます。

- **utf8 {true | false}**：true に設定すると、表現内のすべての有効な UTF-8 バイト シーケンスが単一文字として扱われます。デフォルトは false です。

String XL TCP エンジン シグニチャの作成

次に、stingy、dot all、および UTF-8 をオンにして最小一致長を検索するカスタム String XL TCP シグニチャを作成する例を示します。

String XL TCP エンジンに基づいて、stingy、dot all、および UTF-8 をオンにして最小一致長を検索するカスタム シグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig1
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。カスタム シグニチャ ID の範囲は、60000 ～ 65000 です。

```
ips-ssp(config-sig)# signatures 60004 0
```

ステップ 4　シグニチャ説明サブモードを開始します。

```
ips-ssp(config-sig-sig)# sig-description
```

ステップ 5　新しいシグニチャの名前を指定します。また、**sig-comment** コマンドを使用してシグニチャに関する追加コメントを指定したり、**sig-string-info** コマンドを使用してシグニチャに関する追加情報を指定したりすることもできます。

```
ips-ssp(config-sig-sig-sig)# sig-name This is my new name
```

ステップ 6　シグニチャ説明サブモードを終了します。

```
ips-ssp(config-sig-sig-sig)# exit
```

ステップ 7　String XL TCP エンジンを指定します。

```
ips-ssp(config-sig-sig)# engine string-xl-tcp
```

ステップ 8　サービス ポートを指定します。

```
ips-ssp(config-sig-sig-str)# service-ports 80
```

ステップ 9　方向を指定します。

```
ips-ssp(config-sig-sig-str)# direction to-service
```

ステップ 10　必要ならば、セキュリティ ポリシーに従い、**event-action** コマンドを使用してイベント アクションを変更します。デフォルトのイベント アクションは、**produce-alert** です。

ステップ 11　raw 正規表現をオフにします。

```
ips-ssp(config-sig-sig-str)# specify-raw-regex-string no
```

（注）　raw 正規表現とは、raw モード処理に使用される正規表現の構文です。エキスパート モード専用であり、Cisco IPS シグニチャ開発チーム、あるいはその監視下にある作業者のみによる使用を対象としています。String XL シグニチャは、通常の正規表現と raw 正規表現のいずれでも設定できます。

ステップ 12　TCP パケット内で検索する正規表現文字列を指定し、dot all をオンにします。

```
ips-ssp(config-sig-sig-str-no)# regex-string ht+p[\r].
ips-ssp(config-sig-sig-str-no)# dot-all true
```

ステップ 13　このシグニチャの最小一致長を指定します。stingy を設定する場合は、最小一致長のみが使用できます。

```
ips-ssp(config-sig-sig-str-no)# specify-min-match-length yes
ips-ssp(config-sig-sig-str-no-yes)# min-match-length 100
ips-ssp(config-sig-sig-str-no-yes)# exit
ips-ssp(config-sig-sig-str-no)# stingy true
```

ステップ 14　設定を確認できます。

```
ips-ssp(config-sig-sig-str-no)# show settings
   no
   -----------------------------------------------
      regex-string: ht+p[\r\].
      dot-all: true default: false
      end-optional: false <defaulted>
      no-case: false <defaulted>
      stingy: true default: false
      utf8: false <defaulted>
      specify-min-match-length
      -----------------------------------------------
         yes
         -----------------------------------------------
            min-match-length: 100
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-sig-sig-str-no)#
```

ステップ 15　検索する新しい正規表現を指定し、UTF-8 をオンにします。

```
ips-ssp(config-sig-sig-str-no)# regex-string \x5c\x31\x30\x2e\x30[\x00-\xff]+\
x2e\x31\x5c\x74\x65\x6d\x70
ips-ssp(config-sig-sig-str-no)# utf8 true
```

ステップ 16　設定を確認できます。

```
ips-ssp(config-sig-sig-str-no)# show settings
no
   -----------------------------------------------
      regex-string: \x5c\x31\x30\x2e\x30[\x00-\xff]+\x2e\x31\x5c\x74\x65\x6d\x70
      dot-all: true default: false
      end-optional: false <defaulted>
      no-case: false <defaulted>
      stingy: true default: false
      utf8: true default: false
      specify-min-match-length
      -----------------------------------------------
         yes
```

```
                ----------------------------------------------
                   min-match-length: 100
                ----------------------------------------------
             ------------------------------------------------
          ---------------------------------------------
```

ステップ 17　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-str-no)# exit
ips-ssp(config-sig-sig-str)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 18　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- すべての String XL パラメータの一覧については、付録 B「String XL エンジン」を参照してください。
- 正規表現の構文の詳細については、付録 B「正規表現の構文」を参照してください。

CHAPTER 8

イベント アクション規則の設定

（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 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 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、イベント アクション ルール ポリシーの追加方法とイベント アクション ルールの設定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。

- 「セキュリティ ポリシーについて」（P.8-1）
- 「イベント アクション ルールについて」（P.8-2）
- 「イベント アクション ルール ポリシーの使用」（P.8-7）
- 「イベント アクション変数」（P.8-8）
- 「ターゲットの価値レーティングの設定」（P.8-12）
- 「イベント アクション オーバーライドの設定」（P.8-16）
- 「イベント アクション フィルタの設定」（P.8-20）
- 「OS ID の設定」（P.8-26）
- 「一般設定」（P.8-33）
- 「拒否攻撃者リストの設定」（P.8-35）
- 「イベントのモニタリング」（P.8-39）

セキュリティ ポリシーについて

複数のセキュリティ ポリシーを作成し、それらを個々の仮想センサーに適用できます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーから構成されます。Cisco IPS には、sig0 という名前のデフォルトのシグニチャ定義ポリシー、rules0 という名前のデフォルトのイベント アクション規則ポリシー、および ad0 という名前のデフォルトの異常検出ポリシーが用意されています。仮想センサーにこれらのデフォルト ポリシーを割り当てることも、新しいポリシーを作成することもできます。複数のセキュリティ ポリシーを使用すれば、それぞれ異なる要件に基づいたセキュリティ ポリシーを作成し、そうしたカスタマイズされたポリシーを VLAN や物理インターフェイスごとに適用することが可能になります。

イベント アクション ルールについて

イベント アクション ルールは、センサーのイベント アクション処理コンポーネントに対して行う設定のグループです。これらのルールは、イベント発生時にセンサーが実行するアクションを制御します。イベント アクション処理コンポーネントは、次の機能を提供します。

- リスク レーティングの計算
- イベント アクション オーバーライドの追加
- イベント アクションのフィルタリング
- 結果となるイベント アクションの実行
- イベントのサマライズと集約
- 拒否攻撃者リストの保持

（注） IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサは、アラーム チャネル内のシグニチャ イベントから、シグニチャ イベント アクション オーバーライド、シグニチャ イベント アクション フィルタの処理を経由してシグニチャ イベント アクション ハンドラで処理されるまでのデータ フローを調整します。シグニチャ イベント アクション プロセッサは、次のコンポーネントから構成されます。

- アラーム チャネル：sensorApp 検査パスからシグニチャ イベント処理にシグニチャ イベントを伝える領域を表すユニット。
- シグニチャ イベント アクション オーバーライド：リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定済みのリスク レーティングしきい値の範囲内にあるすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立しており、各アクション タイプには別個の値が設定されています。
- シグニチャ イベント アクション フィルタ：シグニチャ ID、アドレス、およびシグニチャ イベントのリスク レーティングに基づいてアクションを削除します。シグニチャ イベント アクション フィルタへ入力するのは、シグニチャ イベント アクション オーバーライドによって追加される可能性のあるアクションを持つシグニチャ イベントです。

  （注） シグニチャ イベント アクション フィルタが実行できるのはアクションの削除だけであり、新しいアクションの追加はできません。

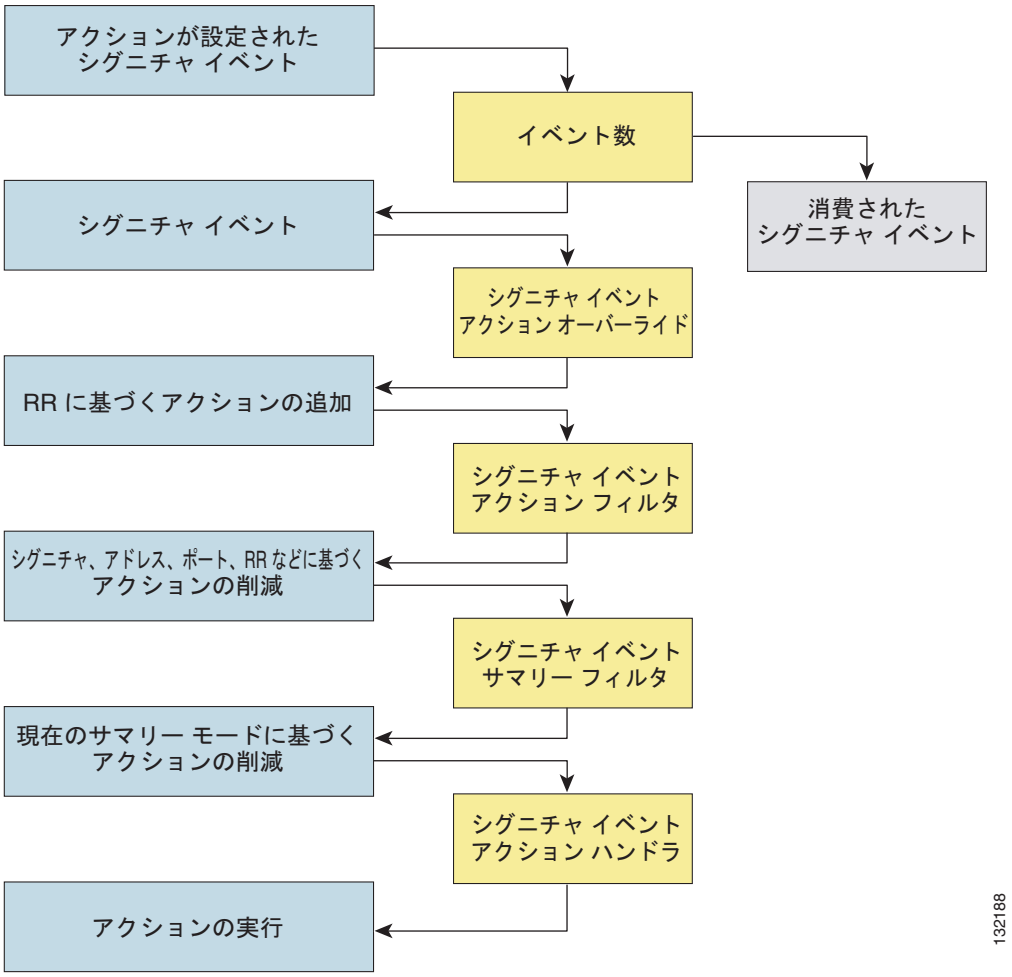
  シグニチャ イベント アクション フィルタには、次のパラメータが適用されます。

  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート
  - 攻撃対象のアドレス

  - 攻撃対象のポート
  - リスク レーティングしきい値の範囲
  - 削除するアクション
  - シーケンス識別子（任意）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット
  - 攻撃対象の OS の関連性または OS の関連性
- シグニチャ イベント アクション ハンドラ：要求されたアクションを実行します。シグニチャ イベント アクション ハンドラから出力されるのは、実行中のアクションだけでなく、イベント ストアに書き込まれる evIdsAlert である可能性があります。

図 8-1 に、シグニチャ イベント アクション プロセッサを通過するシグニチャ イベントの論理的なフローと、このイベントのアクションで実行される操作を示します。これは、アラーム チャネルで受信された、アクションが設定されているシグニチャ イベントで開始され、シグニチャ イベントがシグニチャ イベント アクション プロセッサの機能コンポーネントを通過するときに上から下へ流れます。

図 8-1　シグニチャ イベント アクション プロセッサを通過するシグニチャ イベント



詳細情報

リスク レーティングの詳細については、「リスク レーティングの計算」（P.8-12）を参照してください。

イベント アクション

Cisco IPS は、次のイベント アクションをサポートします。ほとんどのイベント アクションは、その特定のエンジンに対して適切である限り、各シグニチャ エンジンに属します。

アラートおよびログ アクション

- produce-alert：イベントをアラートとしてイベント ストアに書き込みます。

（注）　produce-alert アクションは、シグニチャに対してアラートをイネーブルにした場合に、自動的に実行されません。イベント ストアでアラートを作成するには、produce-alert を選択する必要があります。イベント ストアにアラートを送信する場合は、2 番目のアクションを追加するときに、produce-alert を含める必要があります。また、イベント アクションを設定するたびに、新しいリストが作成され、古いリストと置き換わります。各シグニチャに必要なすべてのイベント アクションを含めてください。

（注）　produce-alert イベント アクションは、グローバル相関によってイベントのリスク レーティングが増加し、deny-packet-inline または deny-attacker-inline のいずれかのイベント アクションが追加されたときに、イベントに追加されます。

- produce-verbose-alert：アラートの不正なパケットの符号化されたダンプを含みます。このアクションによって、produce-alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- log-attacker-packets：攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、produce-alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- log-victim-packets：攻撃対象のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、produce-alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- log-pair-packets：攻撃者と攻撃対象のアドレスのペアが含まれているパケットに対する IP ロギングを開始します。このアクションによって、produce-alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- request-snmp-trap：要求をセンサーの通知アプリケーション コンポーネントに送信して SNMP 通知を実行します。このアクションによって、produce-alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。このアクションを実装するには、センサーで SNMP を設定する必要があります。

拒否アクション

- deny-packet-inline（インラインだけ）：パケットを終了します。

（注）　deny-packet-inline に対するイベント アクション オーバーライドは保護されているため、削除できません。このオーバーライドを使用しない場合は、このエントリに対する override-item-status をディセーブルに設定してください。

- deny-connection-inline（インラインだけ）: この TCP フローで現在と将来のパケットを終了します。
- deny-attacker-victim-pair-inline（インラインだけ）: 指定された期間、攻撃者と攻撃対象のアドレスのペアに対してこのパケットと将来のパケットを送信しません。
- deny-attacker-victim-pair-inline（インラインだけ）: 指定された期間、攻撃者のアドレスと攻撃対象のポートのペアに対してこのパケットと将来のパケットを送信しません。
- deny-attacker-inline（インラインだけ）: 指定された期間、この攻撃者のアドレスからの現在と将来のパケットを終了します。
- センサーによって、システムで拒否される攻撃者のリストは保持されます。拒否攻撃者リストからエントリを削除するために、攻撃者のリストを参照し、リスト全体をクリアしたり、タイマーが期限切れになるのを待ったりすることができます。タイマーは、各エントリのスライディング タイマーです。したがって、攻撃者 A が拒否されても別の攻撃を行う場合、攻撃者 A のタイマーはリセットされ、タイマーの期限が切れるまで攻撃者 A は拒否攻撃者リストに残ります。拒否攻撃者リストがいっぱいになり、新しいエントリを追加できない場合は、パケットは引き続き拒否されます。
- modify-packet-inline（インラインだけ）: エンド ポイントがパケットで行うことを明確にするためにパケット データを変更します。

（注）　イベント アクション フィルタまたはオーバーライドを追加する場合は、modify-packet-inline をアクションとして使用できません。

その他のアクション

- request-block-connection : 要求を ARC に送信してこの接続をブロックします。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

（注）　IPv6 では、request-block-connection はサポートされません。

- request-block-host : 要求を ARC に送信して、この攻撃者ホストをブロックします。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。

（注）　IPv6 では、request-block-host はサポートされません。

- request-rate-limit : レート制限要求を ARC に送信して、レート制限を実行します。レート制限デバイスは、このアクションを実行するように設定されている必要があります。

（注）　request-rate-limit アクションは、特定のシグニチャ セットに適用されます。

（注）　IPv6 では、request-rate-limit はサポートされません。

- reset-tcp-connection：TCP リセットを送信して、TCP フローを乗っ取って終了します。reset-tcp-connection アクションは、単一の接続を分析する TCP シグニチャだけで動作します。スイープまたはフラッドに対しては機能しません。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、または deny-packet-inline をアクションとして追加するイベント アクション オーバーライドの場合、次のアクションが実行される場合があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

deny-packet-inline アクションは、アラート内でドロップ パケット アクションとして表示されます。deny-packet-inline が TCP 接続に対して発生すると、自動的に deny-connection-inline アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

deny-connection-inline が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

詳細情報

- 拒否攻撃者の設定手順については、「拒否攻撃者リストのモニタリングとクリア」（P.8-37）を参照してください。
- 一般設定の手順については、「一般設定」（P.8-34）を参照してください。
- ブロッキング デバイスの設定の手順については、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。
- SNMP の設定の手順については、第 15 章「SNMP の設定」を参照してください。

イベント アクション ルールの設定手順

IPS のイベント アクション ルール コンポーネントを設定する場合は、次の手順を実行します。

1. イベント アクション フィルタで使用する任意の変数を作成します。
2. ターゲットの価値レーティングを作成します。ターゲットの価値レーティングをネットワーク資産に割り当て、リスク レーティングを計算できるようにします。
3. リスク レーティング値に基づいてアクションを追加するオーバーライドを作成します。各イベント アクション タイプにリスク レーティングを割り当てます。
4. フィルタを作成します。ID、IP アドレス、およびシグニチャのリスク レーティングに基づいてアクションを削除するフィルタを割り当てます。

5. OS マッピングを作成します。OS マッピングは、アラートのリスク レーティングの計算で攻撃関連性レーティングに対して使用されます。
6. 一般設定を行います。サマライザまたはメタ イベント ジェネレータを使用するかどうか、あるいは拒否攻撃者パラメータを設定するかどうかを指定します。

イベント アクション ルール ポリシーの使用

サービス イベント アクション ルール サブモードで **service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを作成します。このイベント アクション ルール ポリシーの値は、編集するまでデフォルトのイベント アクション ルールポリシーである rules0 と同じです。

また、特権 EXEC モードで、**copy event-action-rules** *source_destination* コマンドを使用して、既存のポリシーのコピーを作成し、必要に応じて新しいポリシーの値を編集することもできます。

特権 EXEC モードで **list event-action-rules-configurations** コマンドを使用して、イベント アクション ルール ポリシーをリストします。

グローバル コンフィギュレーション モードで **no service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを削除します。グローバル コンフィギュレーション モードで **default service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを工場出荷時の設定にリセットします。

イベント アクション ルール ポリシーを作成、コピー、表示、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール ポリシーを作成します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules MyRules
ips-ssp(config-eve)# exit
Apply Changes?[yes]: yes
ips-ssp(config)# exit
ips-ssp#
```

ステップ 3　既存のイベント アクション ルール ポリシーを新しいイベント アクション ルール ポリシーにコピーします。

```
ips-ssp# copy event-action-rules rules0 rules1
ips-ssp#
```

（注）　ポリシーがすでに存在しているか、新しいポリシーに必要な容量が不足していると、エラーが表示されます。

ステップ 4　デフォルトのイベント アクション ルール ポリシー値を受け入れるか、次のパラメータを編集します。

a. イベント アクション ルール変数を追加します。
b. イベント アクション ルール オーバーライドを設定します。
c. イベント アクション ルール フィルタを設定します。
d. イベント アクション ルールの一般設定を行います。
e. イベント アクション ルールを設定します。
f. イベント アクション ルール OS ID の設定を行います。

ステップ 5　イベント アクション ルール ポリシーのリストをセンサーに表示します。

```
ips-ssp# list event-action-rules-configurations
Event Action Rules
   Instance    Size    Virtual sensor
   rules0      255     vs0
   temp        707     N/A
   MyRules     255     N/A
   rules1      141     vs1
ips-ssp#
```

ステップ 6　イベント アクション ルール ポリシーを削除します。

```
ips-ssp(config)# no service event-action-rules MyRules
ips-ssp(config)#
```

（注）　デフォルトのイベント アクション ルール ポリシーである rules0 を削除することはできません。

ステップ 7　イベント アクション ルール インスタンスが削除されたことを確認します。

```
ips-ssp# list event-action-rules-configurations
Event Action Rules
   Instance    Size    Virtual sensor
   rules0      112     vs0
   rules1      142     N/A
ips-ssp#
```

ステップ 8　イベント アクション ルール ポリシーを工場出荷時の設定にリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# default service event-action-rules rules1
ips-ssp(config)#
```

詳細情報

- イベント アクション ルール変数を追加する手順については、「イベント アクション変数」（P.8-8）を参照してください。
- イベント アクション ルール オーバーライドの設定手順については、「イベント アクション オーバーライドの設定」（P.8-16）を参照してください。
- イベント アクション ルール フィルタの設定手順については、「イベント アクション フィルタの設定」（P.8-20）を参照してください。
- 一般設定の手順については、「一般設定」（P.8-33）を参照してください。
- イベント アクション ルールのターゲットの価値レーティングの設定手順については、「ターゲットの価値レーティングの設定」（P.8-12）を参照してください。
- OS マップの設定手順については、「OS ID の設定」（P.8-26）を参照してください。

イベント アクション変数

ここでは、イベント アクション変数について説明します。次のような構成になっています。

- 「イベント アクション変数について」（P.8-9）
- 「イベント アクション変数の追加、編集、および削除」（P.8-10）

イベント アクション変数について

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

イベント変数を作成し、イベント アクション フィルタでこれらの変数を使用できます。同じ値を複数のフィルタで使用する場合は、変数を使用します。この変数の値を変更すると、この変数を使用するすべてのフィルタが新しい値で更新されます。

（注）　文字列でなく変数を使っていることを示すために、変数をドル記号（$）で始める必要があります。

一部の変数は、シグニチャ システムに対して必須であるため、削除することはできません。変数が保護されている場合は、その変数を選択して編集することはできません。保護されている変数を削除しようとすると、エラー メッセージが表示されます。一度に編集できる変数は 1 つだけです。

IPv4 アドレス

IPv4 アドレスを設定する場合は、次のように完全な IP アドレス、範囲、または範囲のセットを指定します。

- 192.0.2.3-192.0.2.26
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 192.0.2.3-192.0.2.26

IPv6 アドレス

IPv6 アドレスを設定する場合は、次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは 128 ビットであり、16 進数で表現され、8 個の 16 ビット グループにコロンで区切られます。先頭のゼロを省略することができ、間のゼロのグループを二重コロン（::）で表すことができます。アドレスを 2001:db8 プレフィクスで始める必要があります。

ワンポイントアドバイス　エンジニアリング グループに適用される IP アドレス空間があり、そのグループに Windows システムが存在せず、そのグループに対する Windows ベースの攻撃について心配する必要がない場合は、そのエンジニアリング グループの IP アドレス空間に変数を設定できます。次に、この変数を使用して、このグループに対するすべての Windows ベースの攻撃を無視するフィルタを設定できます。

イベント アクション変数の追加、編集、および削除

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

サービス イベント アクション ルール サブモードで **variables** *variable_name* **address** *ip_address* コマンドを使用して、IPv4 イベント アクション変数を作成します。IPv4 アドレスは、1 つのアドレス、1 つの範囲、またはカンマで区切られた複数の範囲のいずれかです。

サービス イベント アクション ルール サブモードで **variables** *variable_name* **ipv6-address** *ip_address* コマンドを使用して、IPv6 イベント アクション変数を作成します。IPv6 アドレスは 128 ビットであり、16 進数で表現され、8 個の 16 ビット グループにコロンで区切られます。先頭のゼロを省略することができ、間のゼロのグループを二重コロン（::）で表すことができます。アドレスを 2001:db8 プレフィクスで始める必要があります。

サービス イベント アクション ルール サブモードで **no variables** *variable_name* コマンドを使用して、イベント アクション変数を削除します。

イベント アクション変数を追加、削除、および編集するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
```

ステップ 3　IPv4 イベント アクション ルール変数を追加します。**address** の有効な値は A.B.C.D-A.B.C.D [,A.B.C.D-A.B.C.D] です。

```
ips-ssp(config-eve)# variables variable-ipv4 address 192.0.2.3
```

ステップ 4　IPv6 イベント アクション ルール変数を追加します。**ipv6-address** の有効な形式は、<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>] です。

```
ips-ssp(config-eve)# variables variable-ipv6 ipv6-address
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

ステップ 5　イベント アクション ルール変数が追加されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variableName: variable-ipv6
      -----------------------------------------------
         ipv6-address: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 default: ::0-FFFF
:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      -----------------------------------------------
      variableName: variable-ipv4
      -----------------------------------------------
         address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 6　イベント アクション ルール変数を編集するには、IPv6 アドレスを範囲に変更します。

```
ips-ssp(config-eve)# variables variable-ipv6 ipv6-address
::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

ステップ 7　イベント アクション ルール変数が編集されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variableName: variable-ipv6
      -----------------------------------------------
         ipv6-address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF default: ::0
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      -----------------------------------------------
```

ステップ 8　イベント アクション ルール変数を削除します。

```
ips-ssp(config-eve)# no variables variable-ipv6
```

ステップ 9　イベント アクション ルール変数が削除されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 1)
   -----------------------------------------------
      variableName: variableipv4
      -----------------------------------------------
         address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 10　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ターゲットの価値レーティングの設定

ここでは、リスク レーティングと、リスク レーティングを使用してターゲットの価値レーティングを設定する方法について説明します。ここでは、次の項目について説明します。

- 「リスク レーティングの計算」（P.8-12）
- 「脅威レーティングについて」（P.8-13）
- 「ターゲットの価値レーティングの追加、編集、および削除」（P.8-14）

リスク レーティングの計算

リスク レーティング（RR）は、ネットワークでの特定のイベントに関連するリスクの数値化を表す、0 ～ 100 の値です。この計算では、攻撃されるネットワーク資産（特定のサーバなど）の値が考慮され、攻撃の重大度レーティングを使用してシグニチャごと、およびターゲットの価値レーティングを使用してサーバごとに設定が行われます。リスク レーティングは、複数のコンポーネントから計算されます。これらのコンポーネントの一部は設定、収集、および派生されます。

（注）　リスク レーティングは、シグニチャではなくアラートに関連します。

リスク レーティングを使用すると、注意が必要なアラートの優先順位を決定できます。リスク レーティングでは、攻撃の重大度（攻撃に成功した場合）、シグニチャの忠実度、グローバル相関データから得られた攻撃者の評価スコア、およびターゲット ホストの全体的な値が考慮されます。リスク レーティングは、evIdsAlert で報告されます。

次の値を使用して、特定のイベントのリスク レーティングが計算されます。

- シグニチャ忠実度レーティング（SFR）：ターゲットに関する具体的な知識がない場合のこのシグニチャのパフォーマンスに関連する重み。シグニチャ忠実度レーティングは、シグニチャごとに設定され、イベントや記述する条件をシグニチャがどの程度正確に検出するかを示します。

  シグニチャ忠実度レーティングは、シグニチャの作成者によってシグニチャごとに計算されます。シグニチャの作成者は、ターゲットに関する適切な情報がない場合のシグニチャの正確性に関する基本的な信頼性ランキングを定義します。これは、分析対象のパケットを送信するのが許可された場合に、検出された動作がターゲット プラットフォームで期待された結果をもたらすことに関する信頼性を表します。たとえば、非常に具体的なルール（特定の正規表現）で記述されたシグニチャは、汎用的なルールで記述されたシグニチャよりも高いシグニチャ忠実度レーティングとなります。

  （注）　シグニチャ忠実度レーティングは、検出されたイベントがどれだけ悪いかを示しません。

- 攻撃の重大度レーティング（ASR）：成功した脆弱性攻撃の重大度に関連する重み。攻撃の重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）からの派生値です。攻撃の重大度レーティングは、シグニチャごとに設定され、検出されたイベントの危険度を示します。

  （注）　攻撃の重大度レーティングは、イベントがどれだけ正確に検出されたかを示しません。

- ターゲットの価値レーティング（TVR）：ターゲットの認識された値に関連する重み。

  ターゲットの価値レーティングは、ユーザ設定可能な値（zero、low、medium、high、または mission critical）で、ネットワーク資産（IP アドレスを使用）の重要性を示します。価値の高い企業リソースにはより厳しく、あまり重要でないリソースにはより緩やかなセキュリティ ポリシーを開発できます。たとえば、デスクトップ ノードに割り当てるターゲットの価値レーティングよりも高いターゲットの価値レーティングを会社の Web サーバに割り当てることができます。この場合、会社の Web サーバに対する攻撃には、デスクトップ ノードに対する攻撃よりも高いリスク レーティングが付与されます。ターゲットの価値レーティングは、イベント アクション ルール ポリシーで設定されます。

- 攻撃関連性レーティング（ARR）：ターゲット オペレーティング システムの重要度に関連する重み。攻撃関連性レーティングは、アラート時に決定される派生値（relevant、unknown、または relevant）です。関連するオペレーティング システムは、シグニチャごとに設定されます。

- 無差別デルタ（PD）：無差別モードで全体のリスク レーティングから削除できる無差別デルタに関連する重み。無差別デルタは 0 ～ 30 の範囲にあり、シグニチャごとに設定されます。

  （注）　トリガー パケットがインラインでない場合は、無差別デルタがレーティングから削除されます。

- ウォッチ リスト レーティング（WLR）：0 ～ 100（CSA MC は範囲 0 ～ 35 だけを使用）の範囲の、CSA MC ウォッチ リストに関連する重み。アラートの攻撃者がウォッチ リストで見つかると、その攻撃者のウォッチ リスト レーティングがこのレーティングに追加されます。

図 8-2 に、リスク レーティングの計算式を図示します。

図 8-2　　リスク レーティングの計算式

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

脅威レーティングについて

脅威レーティングは、実行されたイベント アクションにより下がったリスク レーティングです。非ロギング イベント アクションでは、脅威レーティングが調整されます。実行されたすべてのイベント アクションからの最大脅威レーティングは、リスク レーティングから削除されます。

イベント アクションの脅威レーティングは、次のとおりです。

- deny-attacker-inline：45
- deny-attacker-victim-pair-inline：40
- deny-attacker-service-pair-inline：40
- deny-connection-inline：35
- deny-packet-inline：35
- modify-packet-inline：35
- request-block-host：20
- request-block-connection：20
- reset-tcp-connection：20
- request-rate-limit：20

ターゲットの価値レーティングの追加、編集、および削除

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

IPv4 アドレスの場合は、サービス イベント アクション ルール サブモードで、**target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} **target-address** *ip_address* コマンドを使用してネットワーク資産のターゲットの価値レーティングを追加します。デフォルトは [medium] です。サービス イベント アクション ルール サブモードで **no target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} コマンドを使用して、ターゲットの価値レーティングを削除します。

IPv6 アドレスの場合は、サービス イベント アクション ルール サブモードで **ipv6-target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} **ipv6-target-address** *ip_address* コマンドを使用して、ネットワーク資産のターゲットの価値レーティングを追加します。デフォルトは [medium] です。サービス イベント アクション ルール サブモードで **no ipv6-target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} コマンドを使用して、ターゲットの価値レーティングを削除します。

オプション

次のオプションが適用されます。

- **target-value**：IPv4 ターゲットの価値レーティングを指定します。
  - **zerovalue**：このターゲットの値なし。
  - **low**：このターゲットの低い値。
  - **medium**：このターゲットの通常の値（デフォルト値）。
  - **high**：このターゲットの高い値。
  - **mission-critical**：このターゲットの異常な値。
- **no target-value**：IPv4 ターゲットの価値レーティングを削除します。
- **target-address** *ip_address*：<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] という形式で IPv4 アドレス用 IP アドレスの範囲セットを指定します。
- **ipv6-target-value**：IPv6 ターゲットの価値レーティングを指定します。
  - **zerovalue**：このターゲットの値なし。
  - **low**：このターゲットの低い値。
  - **medium**：このターゲットの通常の値（デフォルト値）。
  - **high**：このターゲットの高い値。

  - **mission-critical**：このターゲットの異常な値。
- **no ipv6-target-value**：IPv6 ターゲットの価値レーティングを削除します。
- **ipv6-target-address** *ip_address*：次の形式で IPv6 アドレス用 IP アドレスの範囲セットを指定します。
  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

ターゲットの価値レーティングの追加、編集、および削除

ネットワーク資産のターゲットの価値レーティングを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules1
```

ステップ 3　ネットワーク資産に IPv4 ターゲットの価値レーティングを割り当てます。

```
sensor(config-eve)# target-value mission-critical target-address 192.0.2.3
```

ステップ 4　ネットワーク資産に IPv6 ターゲットの価値レーティングを割り当てます。

```
sensor(config-eve)# ipv6-target-value mission-critical ipv6-target-address
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

ステップ 5　ターゲットの価値レーティングが追加されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
   target-value (min: 0, max: 5, current: 1)
   -----------------------------------------------
      target-value-setting: mission-critical
      target-address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
   -----------------------------------------------
   ipv6-target-value (min: 0, max: 5, current: 2)
   -----------------------------------------------
      ipv6-target-value-setting: mission-critical
      ipv6-target-address: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 default: ::0-
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
   -----------------------------------------------
sensor(config-eve)#
```

ステップ 6　ターゲットの価値レーティングを編集するには、資産のターゲットの価値レーティング設定を変更します。

```
sensor(config-eve)# target-value low target-address 192.0.2.3
```

ステップ 7　ターゲットの価値レーティングが編集されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
 target-value (min: 0, max: 5, current: 1)
 -----------------------------------------------
    target-value-setting: low
    target-address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
 -----------------------------------------------
```

ステップ 8　ターゲットの価値レーティングを削除します。

```
sensor(config-eve)# no ipv6-target-value mission-critical
```

ステップ 9　ターゲットの価値レーティングが削除されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
 ipv6-target-value (min: 0, max: 5, current: 0)
 -----------------------------------------------
 -----------------------------------------------
```

ステップ 10　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

イベント アクション オーバーライドの設定

ここでは、イベント アクション オーバーライドについて説明します。次のような構成になっています。

- 「イベント アクション オーバーライドについて」（P.8-16）
- 「パケットのインライン拒否について」（P.8-16）
- 「イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化」（P.8-17）

イベント アクション オーバーライドについて

イベント アクション オーバーライドを追加すると、イベントのリスク レーティングに基づいて、そのイベントに関連付けられているアクションを変更できます。イベント アクション オーバーライドは、各シグニチャを個別に設定しないで、グローバルにイベント アクションを追加する方法です。各イベント アクションには、関連付けられたリスク レーティング範囲があります。シグニチャ イベントが発生し、そのイベントのリスク レーティングがイベント アクションの範囲内に入っていた場合、そのアクションがイベントに追加されます。たとえば、リスク レーティングが 85 以上のイベントによって SNMP トラップを生成する場合は、request-snmp-trap のリスク レーティング範囲を 85-100 に設定できます。アクション オーバーライドを使用しない場合は、イベント アクション オーバーライド コンポーネント全体をディセーブルにできます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、または deny-packet-inline をアクションとして追加するイベント アクション オーバーライドの場合、次のアクションが実行される場合があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

deny-packet-inline アクションは、アラート内でドロップ パケット アクションとして表示されます。deny-packet-inline が TCP 接続に対して発生すると、自動的に deny-connection-inline アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

deny-connection-inline が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化

サービス イベント アクション ルール サブモードで **overrides** {**request-block-connection** | **request-block-host** | **deny-attacker-inline** | **deny-packet-inline** | **deny-attacker-service-pair-inline** | **deny-attacker-victim-pair-inline** | **deny-connection-inline** | **log-attacker-packets** | **log-victim-packets** | **log-pair-packets** | **reset-tcp-connection** | **produce-alert** | **produce-verbose-alert** | **request-rate-limit** | **request-snmp-trap**} コマンドを使用して、イベント アクション オーバーライドのパラメータを設定します。サービス イベント アクション ルール サブモードで **no overrides** コマンドを使用して、イベント アクション オーバーライドのパラメータを削除します。

オーバーライド イベント アクション、次にリスク レーティング範囲を設定し、オーバーライドをイネーブルまたはディセーブルにします。

（注） deny-packet-inline に対するイベント アクション オーバーライドは保護されているため、削除できません。このオーバーライドを使用しない場合は、このエントリに対する override-item-status をディセーブルに設定してください。

オプション

次のオプションが適用されます。

- **no overrides**：エントリまたは選択設定を削除します。
- **override-item-status** {**enabled** | **disabled**}：このオーバーライド アイテムの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **risk-rating-range**：このオーバーライド アイテムのリスク レーティング値の範囲を指定します。デフォルトは 0 ～ 100 です。
- **show**：システム設定または履歴情報を表示します。

イベント アクション オーバーライドの設定

イベント アクション オーバーライドを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
ips-ssp(config-eve)#
```

ステップ 3　オーバーライドのアクションを割り当てます。

- 攻撃者の送信元 IP アドレスからのパケットを拒否します。

```
ips-ssp(config-eve)# overrides deny-attacker-inline
ips-ssp(config-eve-ove)#
```

- アラートを引き起こす単一パケットを送信しません。

```
ips-ssp(config-eve)# overrides deny-packet-inline
ips-ssp(config-eve-ove)#
```

- 指定された TCP 接続でパケットを送信しません。

```
ips-ssp(config-eve)# overrides deny-connection-inline
ips-ssp(config-eve-ove)#
```

- 接続を終了するために TCP RST パケットを送信します。

```
ips-ssp(config-eve)# overrides reset-tcp-connection
ips-ssp(config-eve-ove)#
```

- 接続のブロックを要求します。

```
ips-ssp(config-eve)# overrides request-block-connection
ips-ssp(config-eve-ove)#
```

- 攻撃者のホストのブロックを要求します。

```
ips-ssp(config-eve)# overrides request-block-host
ips-ssp(config-eve-ove)#
```

- 攻撃者の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-attacker-packets
ips-ssp(config-eve-ove)#
```

- 攻撃対象の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-victim-packets
ips-ssp(config-eve-ove)#
```

- 攻撃者と攻撃対象の両方の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-pair-packets
ips-ssp(config-eve-ove)#
```

- アラートをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides produce-alert
ips-ssp(config-eve-ove)#
```

- 冗長なアラートをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides produce-verbose-alert
ips-ssp(config-eve-ove)#
```

- SNMP トラップを要求するイベントをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides request-snmp-trap
ips-ssp(config-eve-ove)#
```

ステップ 4　このオーバーライド アイテムのリスク レーティングを設定します。デフォルトのリスク レーティング範囲は 0 ～ 100 です。これを 85 ～ 100 などの異なる値に設定します。

```
ips-ssp(config-eve-ove)# risk-rating-range 85-100
```

ステップ 5　このオーバーライド アイテムの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-ove)# override-item-status {enabled | disabled}
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
   action-to-add: deny-attacker-inline
   -----------------------------------------------
      override-item-status: Enabled default: Enabled
      risk-rating-range: 85-100 default: 0-100
   -----------------------------------------------
```

ステップ 7　イベント アクション オーバーライドのリスク レーティングを編集します。

```
ips-ssp(config-eve)# overrides deny-attacker-inline
ips-ssp(config-eve-ove)# risk-rating 95-100
```

ステップ 8　イベント アクション オーバーライドが編集されたことを確認します。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
-----------------------------------------------
 overrides (min: 0, max: 14, current: 1)
 -----------------------------------------------

       override-item-status: Enabled <defaulted>
       risk-rating-range: 95-100 default: 0-100
    -----------------------------------------------
```

ステップ 9　イベント アクション オーバーライドを削除します。

```
ips-ssp(config-eve)# no overrides deny-attacker-inline
ips-ssp(config-eve-ove)#
```

ステップ 10　イベント アクション オーバーライドが削除されたことを確認します。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
overrides (min: 0, max: 14, current: 1)
-----------------------------------------------
   action-to-add: deny-attacker-inline
   -----------------------------------------------
      override-item-status: Enabled <defaulted>
      risk-rating-range: 95 default: 0-100
   -----------------------------------------------
      override-item-status: Enabled <defaulted>
      risk-rating-range: 90-100 <defaulted>
   -----------------------------------------------
-----------------------------------------------
```

ステップ 11　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

すべてのイベント アクションについては、「イベント アクション」（P.8-4）を参照してください。

イベント アクション フィルタの設定

ここでは、イベント アクション フィルタについて説明します。次のような構成になっています。

- 「イベント アクション フィルタについて」（P.8-20）
- 「イベント アクション フィルタの設定」（P.8-21）

イベント アクション フィルタについて

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

注意　送信元 IP アドレスおよび宛先 IP アドレスに基づくイベント アクション フィルタは、正規のシグニチャとしてフィルタリングしないので、Sweep エンジンには機能しません。スイープ アラートで送信元 IP アドレスと宛先 IP アドレスをフィルタリングするには、Sweep エンジン シグニチャで送信元 IP アドレスおよび宛先 IP アドレス フィルタ パラメータを使用します。

（注）　スイープ シグニチャをフィルタリングする場合は、宛先アドレスをフィルタリングしないことを推奨します。複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

イベント アクション フィルタの設定

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

特定のアクションをイベントから削除するか、または、イベント全体を破棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。フィルタに対するアドレスをグループ化するために定義したイベント アクション変数を使用できます。

（注）　文字列ではなく変数を使用することを示すために、変数の先頭にはドル記号（$）を付ける必要があります。「$」を付けないと、`Bad source and destination` エラーが生じます。

サービス イベント アクション ルール サブモードで **filters {edit | insert | move] name1 [begin | end | inactive | before | after}** コマンドを使用して、イベント アクション フィルタを設定します。

オプション

次のオプションが適用されます。

- **actions-to-remove**：このフィルタ アイテムに対して削除するイベント アクションを指定します。
- **attacker-address-range**：このアイテムに対して IPv4 の攻撃者アドレスの範囲セット（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）を指定します。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。攻撃者のアドレス範囲を指定しない場合は、すべての IPv4 の攻撃者アドレスに一致します。

- **attacker-port-range**：このアイテムに対する攻撃者のポートの範囲セット（たとえば、147-147,8000-10000）を指定します。
- **default**：値をシステムのデフォルト設定に戻します。
- **deny-attacker-percentage**：攻撃者拒否機能で拒否するパケットの割合を指定します。有効な範囲は 0 ～ 100 です。デフォルトは 100 です。
- **filter-item-status {enabled | disabled}**：このフィルタ アイテムの使用をイネーブルまたはディセーブルにします。
- **ipv6-attacker-address-range**：このアイテムに対する IPv6 の攻撃者アドレスの範囲セットを指定します（たとえば、<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]）。

（注）　範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。IPv6 の攻撃者アドレス範囲を指定しない場合は、すべての IPv6 攻撃者アドレスに一致します。

- **ipv6-victim-address-range**：このアイテムに対する攻撃対象のアドレスの範囲セットを指定します（たとえば、<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]）。

（注）　範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。IPv6 の攻撃対象アドレス範囲を指定しない場合は、すべての IPv6 の攻撃対象アドレスに一致します。

- **no**：エントリまたは選択の設定を削除します。
- **os-relevance**：このフィルタに対するイベント OS 関連性を指定します。
  - **relevant**：イベントはターゲット OS に関連します。
  - **not-relevant**：イベントはターゲット OS に関連しません。
  - **unknown**：イベントがターゲット OS に関連するかどうかわかりません。
- **risk-rating-range**：このフィルタ アイテムのリスク レーティング値の範囲を指定します。
- **signature-id-range**：このアイテムのシグニチャ ID の範囲セット（たとえば、1000-2000,3000-3000）を指定します。
- **stop-on-match {true | false}**：このフィルタ アイテムに一致した場合に、フィルタの評価を続行するか、停止します。
- **subsignature-id-range**：このアイテムのサブシグニチャ ID の範囲セット（たとえば、0-2,5-5）を指定します。
- **user-comment**：このフィルタ アイテムに関するコメントを追加できます。
- **victim-address-range**：このアイテムに対して攻撃対象のアドレスの範囲セット（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）を指定します。

（注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。攻撃対象のアドレス範囲を指定しない場合は、すべての IPv4 の攻撃者アドレスに一致します。

- **victim-port-range**：このアイテムに対する攻撃対象のポートの範囲セット（たとえば、147-147,8000-10000）を指定します。

イベント アクション フィルタの設定

イベント アクション フィルタを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules1
ips-ssp(config-eve)#
```

ステップ 3　フィルタ名を作成します。**name1**、**name2** などを使用して、イベント アクション フィルタの名前を指定します。**begin | end | inactive | before | after** キーワードを使用して、フィルタを挿入する場所を指定します。

```
ips-ssp(config-eve)# filters insert name1 begin
```

ステップ 4　このフィルタの値を指定します。デフォルトは 900 ～ 65535 です。

a. シグニチャ ID 範囲を指定します。

```
ips-ssp(config-eve-fil)# signature-id-range 1000-1005
```

b. サブシグニチャ ID 範囲を指定します。デフォルトは 0 ～ 255 です。

```
ips-ssp(config-eve-fil)# subsignature-id-range 1-5
```

c. IPv4 または IPv6 の攻撃者アドレス範囲を指定します。

```
ips-ssp(config-eve-fil)# attacker-address-range 192.0.2.3-192.0.2.26
ips-ssp(config-eve-fil)# ipv6-attacker-address-range
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

d. IPv4 または IPv6 の攻撃対象アドレス範囲を指定します。

```
ips-ssp(config-eve-fil)# victim-address-range 192.56.10.1-192.56.10.255
ips-ssp(config-eve-fil)# ipv6-victim-address-range ::0-FFFF:FFFF:FFFF:FFFF:FFFF:
FFFF:FFFF:FFFF
```

e. 攻撃対象ポート範囲を指定します。デフォルトは 0 ～ 65535 です。

```
ips-ssp(config-eve-fil)# victim-port-range 0-434
```

f. OS 関連性を指定します。デフォルトは 0 ～ 100 です。

```
ips-ssp(config-eve-fil)# os-relevance relevant
```

g. リスク レーティング範囲を指定します。デフォルトは 0 ～ 100 です。

```
ips-ssp(config-eve-fil)# risk-rating-range 85-100
```

h. 削除するアクションを指定します。

```
ips-ssp(config-eve-fil)# actions-to-remove reset-tcp-connection
```

i. 拒否アクションをフィルタリングする場合は、必要な拒否アクションの割合を設定します。デフォルトは 100 です。

```
ips-ssp(config-eve-fil)# deny-attacker-percentage 90
```

j. フィルタのステータスをディセーブルまたはイネーブルのいずれかに指定します。デフォルトはイネーブルです。

```
ips-ssp(config-eve-fil)# filter-item-status {enabled | disabled}
```

k. 一致パラメータで停止を指定します。**true** を指定すると、このアイテムが一致する場合にセンサーがフィルタの処理を停止します。**false** を指定すると、このアイテムが一致する場合であってもセンサーはフィルタの処理を続行します。

```
ips-ssp(config-eve-fil)# stop-on-match {true | false}
```

l. このフィルタを説明するために使用するコメントを追加します。

```
ips-ssp(config-eve-fil)# user-comment NEW FILTER
```

ステップ 5　フィルタの設定を確認します。

```
ips-ssp(config-eve-fil)# show settings
NAME: name1
   ------------------------------------------------
      signature-id-range: 1000-10005 default: 900-65535
      subsignature-id-range: 1-5 default: 0-255
      attacker-address-range: 192.0.2.3-192.0.2.26 default: 0.0.0.0-255.255.255.255
      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255
           ipv6-attacker-address-range: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 defau
lt: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      ipv6-victim-address-range: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF def
ault: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 1-343 default: 0-65535
      risk-rating-range: 85-100 default: 0-100
      actions-to-remove: reset-tcp-connection default:
      deny-attacker-percentage: 90 default: 100
      filter-item-status: Enabled default: Enabled
      stop-on-match: True default: False
      user-comment: NEW FILTER default:
      os-relevance: relevant default: relevant|not-relevant|unknown
   ------------------------------------------------
senor(config-eve-fil)#
```

ステップ 6　既存のフィルタを編集します。

```
ips-ssp(config-eve)# filters edit name1
```

ステップ 7　パラメータを編集します（ステップ 4a ～ 4l を参照）。

ステップ 8　フィルタ リストでフィルタを上下に移動します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# filters move name5 before name1
```

ステップ 9　フィルタが移動されたことを確認します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# show settings
   ------------------------------------------------
   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)
   ------------------------------------------------
   ACTIVE list-contents
   ------------------------------------------------
      NAME: name5
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
      NAME: name1
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
```

```
            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            attacker-port-range: 0-65535 <defaulted>
            victim-port-range: 0-65535 <defaulted>
            risk-rating-range: 0-100 <defaulted>
            actions-to-remove: <defaulted>
            filter-item-status: Enabled <defaulted>
            stop-on-match: False <defaulted>
            user-comment: <defaulted>
         ------------------------------------------------
         ------------------------------------------------
         NAME: name2
         ------------------------------------------------
            signature-id-range: 900-65535 <defaulted>
            subsignature-id-range: 0-255 <defaulted>
            attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            attacker-port-range: 0-65535 <defaulted>
            victim-port-range: 0-65535 <defaulted>
            risk-rating-range: 0-100 <defaulted>
            actions-to-remove: <defaulted>
            filter-item-status: Enabled <defaulted>
            stop-on-match: False <defaulted>
            user-comment: <defaulted>
         ------------------------------------------------
         ------------------------------------------------
      ---------------------------------------------
      INACTIVE list-contents
      ---------------------------------------------
   -----------------------------------------------
   ips-ssp(config-eve)#
```

ステップ 10　フィルタを非アクティブ リストに移動します。

```
ips-ssp(config-eve)# filters move name1 inactive
```

ステップ 11　フィルタが非アクティブ リストに移動されたことを確認します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# show settings
   ---------------------------------------------
   INACTIVE list-contents
   ---------------------------------------------
      ------------------------------------------------
      NAME: name1
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
ips-ssp(config-eve)#
```

ステップ 12　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

イベント アクション変数の設定手順については、「イベント アクション変数の追加、編集、および削除」（P.8-10）を参照してください。

OS ID の設定

ここでは、OS ID と、OS マップの設定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。

- 「パッシブ OS フィンガープリントについて」（P.8-26）
- 「パッシブ OS フィンガープリントの設定に関する留意事項」（P.8-27）
- 「設定された OS マップの追加、編集、削除、および移動」（P.8-28）
- 「OS ID の表示とクリア」（P.8-32）

パッシブ OS フィンガープリントについて

パッシブ OS フィンガープリントにより、センサーはホストが稼動している OS を特定できます。センサーはホスト間のネットワーク トラフィックを分析して、これらのホストの OS をその IP アドレスとともに格納します。センサーはネットワーク上で交換される TCP SYN および SYNACK パケットを検査して、OS タイプを特定します。

次に、センサーはターゲット ホスト OS の OS を使用し、リスク レーティングの攻撃関連性レーティング コンポーネントを計算することによって、攻撃対象への攻撃の関連性を決定します。センサーは、攻撃の関連性に基づいて、攻撃に対するアラートのリスク レーティングを変更したり、攻撃のアラートをフィルタリングしたりできます。ここで、リスク レーティングを使用すると、偽陽性アラートの数を減らしたり（IDS モードの利点）、疑わしいパケットを明確にドロップしたり（IPS モードの利点）できます。また、パッシブ OS フィンガープリントでは、攻撃対象 OS、OS ID のソース、および攻撃対象 OS との関連性をアラート内にレポートすることによって、アラート出力が拡張されます。

パッシブ OS フィンガープリントは、次の 3 つのコンポーネントで構成されます。

- パッシブ OS ラーニング：パッシブ OS ラーニングは、センサーがネットワーク上のトラフィックを監視しているときに行われます。TCP SYN および SYNACK パケットの特性に基づいて、センサーは送信元 IP アドレスのホスト上で稼動している OS を特定します。
- ユーザ設定可能な OS ID：学習された OS マップよりも優先される OS ホスト マップを設定できます。
- 攻撃関連性レーティングおよびリスク レーティングの計算：センサーは OS 情報を使用して、ターゲット ホストに対する攻撃シグニチャの関連性を決定します。攻撃の関連性は、攻撃アラートのリスク レーティング値を構成する攻撃関連性レーティング コンポーネントです。センサーは、CSA MC からインポートされたホストのポスチャ情報で報告された OS タイプを使用して、攻撃関連性レーティングを計算します。

OS 情報には 3 つのソースがあります。センサーは OS 情報のソースを次の順序でランク付けします。

1. 設定された OS マップ : 入力する OS マップ。設定された OS マップは、イベント アクション ルール ポリシーに存在し、1 つまたは多くの仮想センサーに適用できます。

   （注）　同じ IP アドレスに複数のオペレーティング システムを指定できます。リストの最後のものは、一致したオペレーティング システムです。

2. インポートされた OS マップ : 外部のデータ ソースからインポートされた OS マップ。インポートされた OS マップはグローバルであり、すべての仮想センサーに適用されます。

   （注）　現在、CSA MC は唯一の外部データ ソースです。

3. 学習された OS マップ : SYN 制御ビットが設定された TCP パケットのフィンガープリントを介してセンサーが検知した OS マップ。学習された OS マップは、トラフィックを監視する仮想センサーに対してローカルです。

センサーは、ターゲット IP アドレスの OS を特定する必要がある場合に、設定された OS マップを調べます。ターゲット IP アドレスが、設定された OS マップにない場合、センサーはインポートされた OS マップを調べます。ターゲット IP アドレスが、インポートされた OS マップにない場合、センサーはインポートされた OS マップを調べます。そこでも見つからなかった場合、センサーはターゲット IP の OS を不明として処理します。

（注）　パッシブ OS フィンガープリントはデフォルトでイネーブルになり、IPS には各シグニチャのデフォルトの脆弱な OS リストが含まれます。

パッシブ OS フィンガープリントの設定に関する留意事項

パッシブ OS フィンガープリントは機能するよう設定する必要はありません。IPS は、各シグニチャに対してデフォルトの脆弱な OS リストを提供し、パッシブ分析がデフォルトでイネーブルになります。

パッシブ OS フィンガープリントの次の側面を設定できます。

- OS マップを定義 : 重要なシステムで稼動している OS の ID を定義するよう OS マップを設定することが推奨されます。重要なシステムの OS および IP アドレスが変更される可能性が少ない場合は、OS マップを設定することが推奨されます。
- 攻撃関連性レーティングの計算を特定の IP アドレス範囲に制限 : これにより、攻撃関連性レーティングの計算が、保護されたネットワークの IP アドレスに制限されます。
- OS マップをインポート : OS マップをインポートすると、パッシブ分析で取得された OS ID の学習レートと忠実度を向上させることができます。CSA MC などの外部の製品インターフェイスがある場合は、そのインターフェイスから OS ID をインポートできます。
- ターゲットの OS 関連性の値を使用してイベント アクション ルール フィルタを定義 : これにより、OS 関連性だけに基づいてアラートをフィルタリングできるようになります。
- パッシブ分析をディセーブル化 : センサーが新しい OS マップを学習しないようにします。
- シグニチャ脆弱 OS リストを編集 : 脆弱な OS リストは、各シグニチャに対して脆弱な OS タイプを指定します。デフォルト値である general-os は、脆弱な OS リストを指定しないすべてのシグニチャに適用されます。

設定された OS マップの追加、編集、削除、および移動

サービス イベント アクション ルール サブモードで **os-identifications** コマンドを使用して、学習された OS マッピングよりも優先される OS ホスト マッピングを設定します。設定された OS マップは、追加、編集、および削除できます。リスト内で OS マップを上下に移動すると、特定の IP アドレスと OS タイプの組み合わせに対する攻撃関連性レーティングおよびリスク レーティングの計算をセンサーが行う順序を変更できます。

また、リスト内で OS マップを上下に移動すると、特定の IP アドレスに関連付けられている OS をセンサーが解決する順序を変更できます。設定された OS マッピングでは、範囲を設定できます。したがって、ネットワーク 192.168.1.0/24 の場合、管理者は次のように定義できます（表 8-1）。

表 8-1　設定された OS マッピングの例

IP アドレス範囲の設定	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10,192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

より特定的なマッピングをリストの先頭に配置する必要があります。IP アドレス範囲設定では重複は許可されませんが、最もリストの先頭に近いエントリが優先されます。

オプション

次のオプションが適用されます。

- **calc-arr-for-ip-range**：この範囲内の攻撃対象に対する攻撃関連性レーティングを計算します。この値は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）のようになります。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **configured-os-map {edit | insert | move] name1[begin | end | inactive | before | after}**：管理者が定義した IP アドレスと OS ID のマッピングのコレクションを指定します（設定された OS マッピングは、インポートおよび学習された OS マッピングよりも優先されます）。
- **ip**：指定された OS を稼動している 1 つまたは複数のホスト IP アドレスを指定します。この値は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）のようになります。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **os**：1 つまたは複数のホストが稼動している OS のタイプを指定します。
  - **general-os**：すべての OS タイプ
  - **ios**：各種 Cisco IOS
  - **mac-os**：OS X 以前の各種 Apple System OS
  - **netware**：Netware
  - **other**：その他すべての OS
  - **unix**：各種 UNIX

- **aix**：各種 AIX
- **bsd**：各種 BSD
- **hp-ux**：各種 HP-UX
- **irix**：各種 IRIX
- **linux**：各種 Linux
- **solaris**：各種 Solaris
- **windows**：各種 Microsoft Windows
- **windows-nt-2k-xp**：各種 NT、2000、および XP
- **win-nt**：特定の種類の Windows NT
- **unknown**：未知の OS

- **default**：値をシステムのデフォルト設定に戻します。
- **no**：エントリまたは選択の設定を削除します。
- **passive-traffic-analysis {enabled | disabled}**：パッシブ OS フィンガープリント分析をイネーブルまたはディセーブルにします。

OS マップの設定

OS マップを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules1
ips-ssp(config-eve)#
```

ステップ 3　OS マップを作成します。**name1**、**name2** などを使用して、OS マップの名前を指定します。**begin | end | inactive | before | after** キーワードを使用して、フィルタを挿入する場所を指定します。

```
ips-ssp(config-eve)# os-identification
ips-ssp(config-eve-os)# configured-os-map insert name1 begin
ips-ssp(config-eve-os-con)#
```

ステップ 4　この OS マップの値を指定します。

a. ホスト IP アドレスを指定します。

```
ips-ssp(config-eve-os-con)# ip 192.0.2.0-192.0.2.255
```

b. ホスト OS タイプを指定します。

```
ips-ssp(config-eve-os-con)# os unix
```

注意　同じ IP アドレスに複数のオペレーティング システムを指定できます。リストの最後のものは、一致したオペレーティング システムです。

ステップ 5　OS マップの設定を確認します。

```
ips-ssp(config-eve-os-con)# show settings
   NAME: name1
   -----------------------------------------------
      ip: 192.0.2.0-192.0.2.255 default:
      os: unix
   -----------------------------------------------
ips-ssp(config-eve-os-con)#
```

ステップ 6　IP アドレスに対して攻撃関連性レーティング範囲を指定します。

```
ips-ssp(config-eve-os-con)# exit
ips-ssp(config-eve-os)# calc-arr-for-ip-range 192.0.2.1-192.0.2.25
```

ステップ 7　パッシブ OS フィンガープリントをイネーブルにします。

```
ips-ssp(config-eve-os)# passive-traffic-analysis enabled
```

ステップ 8　既存の OS マップを編集します。

```
ips-ssp(config-eve-os)# configured-os-map edit name1
ips-ssp(config-eve-os-con)#
```

ステップ 9　パラメータを編集します（手順 4 ～ 7 を参照）。

ステップ 10　OS マップ リストで OS マップを上下に移動します。

```
ips-ssp(config-eve-os-con)# exit
ips-ssp(config-eve-os)# configured-os-map move name5 before name1
```

ステップ 11　OS マップが移動されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
   -----------------------------------------------
      calc-arr-for-ip-range: 192.0.2.1-192.0.2.25 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 2 - 2 active, 0 inactive)
      ---------------------------------------------
      ACTIVE list-contents
      ---------------------------------------------
         NAME: name2
         ---------------------------------------------
            ip: 192.0.2.33 default:
            os: aix
         ---------------------------------------------
         ---------------------------------------------
         NAME: name1
         ---------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
   -----------------------------------------------
ips-ssp(config-eve-os)#
```

ステップ 12　OS マップを非アクティブ リストに移動します。

```
ips-ssp(config-eve-os)# configured-os-map move name1 inactive
```

ステップ 13　フィルタが非アクティブ リストに移動されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
```

```
   ------------------------------------------------
      calc-arr-for-ip-range: 192.0.2.33 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 2 - 1 active, 1 inactive)
      ------------------------------------------------
      ACTIVE list-contents
      ------------------------------------------------
         NAME: name2
         ------------------------------------------------
            ip: 192.0.2.33 default:
            os: aix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      INACTIVE list-contents
      ------------------------------------------------
         NAME: name1
         ------------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
--MORE--#
```

ステップ 14　OS マップを削除します。

```
ips-ssp(config-eve-os)# no configured-os-map name2
```

ステップ 15　OS マップが削除されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
   ------------------------------------------------
      calc-arr-for-ip-range: 192.0.2.33 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 1 - 0 active, 1 inactive)
      ------------------------------------------------
      INACTIVE list-contents
      ------------------------------------------------
         NAME: name1
         ------------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
   ------------------------------------------------
ips-ssp(config-eve-os)#
```

ステップ 16　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve-os)# exit
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 17　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

OS ID の表示とクリア

EXEC モードで **show os-identification** [*virtual-sensor*] **learned** [*ip-address*] コマンドを使用して、パッシブ分析によりセンサーが学習した IP アドレスに関連する OS ID を表示します。

EXEC モードで **clear os-identification** [*virtual-sensor*] **learned** [*ip-address*] コマンドを使用して、パッシブ分析によりセンサーが学習した IP アドレスに関連する OS ID を削除します。

IP アドレスを指定する場合は、指定された IP アドレスの OS ID だけが表示またはクリアされます。仮想センサーを指定する場合は、指定されたセンサーの OS ID だけが表示またはクリアされます。仮想センサーなしで IP アドレスを指定する場合、IP アドレスはすべての仮想センサーで表示またはクリアされます。

オプション

次のオプションが適用されます。

- *virtual-sensor*：（任意）表示またはクリアする仮想センサーの学習されたアドレスを指定します。
- *ip-address*：（任意）問い合わせる、またはクリアする IP アドレスを指定します。センサーは、指定された IP アドレスにマッピングされた OS ID を表示または削除します。

OS ID の表示とクリア

OS ID を表示またはクリアするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

（注）　ビューア権限を持つアカウントは OS ID を表示できます。

ステップ 2　特定の IP アドレスに関連する学習された OS ID を表示します。

```
ips-ssp# show os-identification learned 192.0.2.1
Virtual sensor vs0:
   10.1.1.12 windows
ips-ssp# show os-identification learned
Virtual sensor vs0:
   10.1.1.12 windows
Virtual sensor vs1:
   10.1.0.1   unix
   10.1.0.2   windows
   10.1.0.3   windows
ips-ssp#
```

ステップ 3　すべての仮想センサーで特定の IP アドレスに対する学習された OS ID をクリアします。

```
ips-ssp# clear os-identification learned 192.0.2.1
```

ステップ 4　OS ID がクリアされたことを確認します。

```
ips-ssp# show statistics os-identification
Statistics for Virtual sensor vs0
   OS Identification
      Configured
      Imported
      Learned
Statistics for Virtual sensor vs1
   OS Identification
      Configured
      Imported
      Learned
ips-ssp#
```

一般設定

ここでは、一般設定について説明します。次のような構成になっています。

- 「イベント アクション サマライズについて」（P.8-33）
- 「イベント アクション集約について」（P.8-33）
- 「一般設定」（P.8-34）

イベント アクション サマライズについて

サマライズでは、複数のイベントを単一のアラートに単純に集約することによって、センサーから送信されるアラートの量が減少します。また、シグニチャごとに特別なパラメータを指定することにより、アラートの処理方法を変更できます。各シグニチャは、推奨される通常の動作を反映するデフォルト値で作成されます。ただし、各シグニチャを調整して、エンジンのタイプごとに定められた制約の範囲内でこのデフォルトの動作を変更できます。

アラートを生成しないアクション（拒否、ブロック、TCP リセット）は、サマライズされていない各シグニチャ イベントに対するフィルタを通過します。アラートを生成するアクションは、サマライズされたこれらのアラートで実行されません。代わりに、これらのアクションは、1 つのサマリー アラートに適用され、フィルタを通過します。

アラートを生成する他のいずれかのアクションを選択し、フィルタで除外しない場合は、produce-alert を選択しない場合でもアラートが作成されます。アラートが作成されないようにするには、アラートを生成するすべてのアクションをフィルタで除外する必要があります。

サマライズおよびイベント アクションは、メタ エンジンがコンポーネント イベントを処理した後に処理されます。これにより、センサーは一連のイベントで発生する疑わしいアクティビティを監視できます。

イベント アクション集約について

基本的な集約は 2 つの動作モードを提供します。単純モードでは、アラートが送信される前に一致する必要があるシグニチャのヒット数しきい値を設定します。高度なモードは、間隔によるカウントです。このモードでは、センサーは 1 秒間ごとのヒット数を追跡し、そのしきい値が満たされた場合のみアラートを送信します。この例では、ヒットはイベントを説明するために使用される用語であり、基本的にアラートですが、ヒット数のしきい値を超えるまでアラートとしてセンサーから送信されません。

次のサマライズ オプションから選択できます。

- fire-all：シグニチャがトリガーされるたびにアラートを起動します。サマライズにこのしきい値が設定された場合は、サマライズが行われるまで各実行に対してアラートが起動されます。サマライズが始まると、各アドレス セットに対してサマリー間隔ごとにアラートが 1 つだけ起動されます。他のアドレス セットのアラートは、すべて表示されるか、個別にサマライズされます。シグニチャに対してアラートが一定時間存在しないと、シグニチャはすべてのモードを起動します。
- summary：シグニチャが初めてトリガーされた場合にアラートを起動し、そのシグニチャの追加アラートがサマリー間隔の間サマライズされます。各アドレス セットに対して各サマリー間隔でアラートを 1 つだけ起動する必要があります。グローバル サマリーしきい値に到達した場合、シグニチャはグローバル サマライズ モードに切り替わります。
- global-summarization：各サマリー間隔に対してアラートを起動します。シグニチャは、グローバル サマライズに対して事前に設定できます。
- fire-once：各アドレス セットに対してアラートを起動します。このモードをグローバル サマライズ モードにアップグレードできます。

一般設定

一般的なイベント アクション ルール設定を行うには、サービス イベント アクション ルール サブモードで、次のコマンドを使用します。

- **global-block-timeout**：ホストまたは接続をブロックする時間（分単位）。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 分です。
- **global-deny-timeout**：攻撃者インラインを拒否する時間（秒単位）。有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
- **global-filters-status** {**enabled | disabled**}：フィルタの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-metaevent-status** {**enabled | disabled**}：メタ イベント ジェネレータの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-overrides-status** {**enabled | disabled**}：オーバーライドの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-summarization-status** {**enabled | disabled**}：サマライザの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **max-denied-attackers**：一度にシステム内で許容できる拒否攻撃者の数を制限します。有効な範囲は 0 ～ 100000000 です。デフォルトは 10000 です。

イベント アクションの一般設定

イベント アクションの一般設定を行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config)# general
```

ステップ 4　メタ イベント ジェネレータをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-metaevent-status {enabled | disabled}
```

ステップ 5　サマライザを有効または無効にします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-summarization-status {enabled | disabled}
```

ステップ 6　拒否攻撃者インライン イベント アクションを設定します。

a. 一度にシステム内で許容できる拒否攻撃者の数を制限します。デフォルトは 1000 です。

```
ips-ssp(config-eve-gen)# max-denied-attackers 100
```

b. システムで攻撃者を拒否する時間（秒単位）を設定します。デフォルトは 3600 秒です。

```
ips-ssp(config-eve-gen)# global-deny-timeout 1000
```

ステップ 7　ホストまたは接続をブロックする時間（分単位）を設定します。デフォルトは 30 分です。

```
ips-ssp(config-eve-gen)# global-block-timeout 20
```

ステップ 8　設定したオーバーライドをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-overrides-status {enabled | disabled}
```

ステップ 9　設定したフィルタをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-filters-status {enabled | disabled}
```

ステップ 10　一般サブモードの設定を確認します。

```
ips-ssp(config-eve-gen)# show settings
   general
   ------------------------------------------------
      global-overrides-status: Enabled default: Enabled
      global-filters-status: Enabled default: Enabled
      global-summarization-status: Enabled default: Enabled
      global-metaevent-status: Enabled default: Enabled
      global-deny-timeout: 1000 default: 3600
      global-block-timeout: 20 default: 30
      max-denied-attackers: 100 default: 10000
   ------------------------------------------------
ips-ssp(config-eve-gen)#
```

ステップ 11　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve-gen)# exit
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

拒否攻撃者リストの設定

ここでは、拒否攻撃者リストと、リストを追加、クリア、およびモニタする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。

- 「拒否攻撃者リストへの拒否攻撃者エントリの追加」（P.8-36）
- 「拒否攻撃者リストのモニタリングとクリア」（P.8-37）

拒否攻撃者リストへの拒否攻撃者エントリの追加

deny attacker [**virtual-sensor** *name*] [**ip-address** *attacker-ip-address*] | **victim** *victim-ip-address* | **port** *port-number*] コマンドを使用して、拒否攻撃者リストに拒否攻撃者エントリを 1 つ追加します。リストから拒否攻撃者エントリを削除するには、このコマンドの **no** 形式を使用します。

オプション

次のオプションが適用されます。

- *name*：（任意）拒否攻撃者エントリを追加する仮想センサーの名前を指定します。
- *attacker-ip-address*：攻撃者の IP アドレスを指定します。
- *victim-ip-address*：（任意）攻撃対象の IP アドレスを指定します。
- *port-number*：（任意）攻撃対象のポート番号を指定します。有効な範囲は 0 ～ 65535 です。

拒否攻撃者リストへのエントリの追加

拒否攻撃者リストに拒否攻撃者エントリを追加するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　IP アドレスが 192.0.2.1 の拒否攻撃者エントリを追加します。

```
ips-ssp# deny attacker ip-address 192.0.2.1
Warning: Executing this command will add deny attacker address on all virtual sensors.
Continue? [yes]:
```

ステップ 3　**yes** を入力して、すべての仮想センサーに対してこの拒否攻撃者エントリを追加します。

ステップ 4　特定の仮想センサーに拒否攻撃者エントリを追加します。

```
ips-ssp# deny attacker virtual-sensor vs0 ip-address 192.0.2.1
```

ステップ 5　リストから拒否攻撃者エントリを削除します。

```
ips-ssp# no deny attacker ip-address 192.0.2.1
Warning: Executing this command will delete this address from the list of attackers being
denied by all virtual sensors.
Continue? [yes]:
```

ステップ 6　**yes** を入力して、リストから拒否攻撃者エントリを削除します。

（注）　攻撃者の拒否をすぐに止めるには、**clear denied-attackers** コマンドを使用して、拒否攻撃者リストをクリアする必要があります。

詳細情報

拒否攻撃者リストから拒否攻撃者を永久的に削除する手順については、「拒否攻撃者リストのモニタリングとクリア」（P.8-37）を参照してください。

拒否攻撃者リストのモニタリングとクリア

show statistics denied-attackers コマンドを使用して、拒否攻撃者リストを表示します。**clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] コマンドを使用して、拒否攻撃者リストを削除し、仮想センサー統計情報をクリアします。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。インライン モードでは、パケット、接続、および攻撃者を拒否するようシグニチャを設定できます。この結果、センサーが単一のパケット、接続、および特定の攻撃者を検出した場合に、これらは拒否されます（つまり、送信されません）。

シグニチャが起動されると、攻撃者は拒否され、リストに追加されます。センサー管理の一部として、リストの削除、またはリスト内の統計情報のクリアが必要な場合があります。

オプション

次のオプションが適用されます。

- *virtual_sensor*：（任意）拒否攻撃者リストをクリアする必要がある仮想センサーを指定します。
- *ip_address*：（任意）クリアする IP アドレスを指定します。

拒否攻撃者の表示と削除

拒否攻撃者リストの表示、リストの削除、統計情報のクリアを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　拒否された IP アドレスのリストを表示します。統計情報は、この時点で 2 つの IP アドレスが拒否されていることを示します。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

ステップ 3　拒否攻撃者リストを削除します。

```
ips-ssp# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力して、リストをクリアします。

ステップ 5　特定の仮想センサーの拒否攻撃者リストを削除します。

```
ips-ssp# clear denied-attackers vs0
Warning: Executing this command will delete all addresses from the list of attackers being
denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 6　**yes** を入力して、リストをクリアします。

ステップ 7　特定の仮想センサーの拒否攻撃者リストから、特定の IP アドレスを削除します。

```
ips-ssp# clear denied-attackers vs0 ip-address 192.0.2.1
Warning: Executing this command will delete ip address 10.1.1.1 from the list of attackers
being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 8　**yes** を入力して、リストをクリアします。

ステップ 9　リストをクリアしたことを確認します。**show statistics denied-attackers** または **show statistics virtual-sensor** コマンドを使用できます。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.
ips-ssp#

ips-ssp# show statistics virtual-sensor
Virtual sensor Statistics
   Statistics for Virtual sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

ステップ 10　統計情報のみをクリアします。

```
ips-ssp# show statistics virtual-sensor clear
```

ステップ 11　統計情報をクリアしたことを確認します。Number of Active Denied Attackers および Number of exec Clear commands during uptime カテゴリ以外の統計情報がすべてクリアされました。リストがクリアされたかどうかを認識することが重要です。

```
ips-ssp# show statistics virtual-sensor
Virtual sensor Statistics
   Statistics for Virtual sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

イベントのモニタリング

ここでは、イベント ストアからイベントを表示したりクリアしたりする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。

- 「イベントの表示」（P.8-39）
- 「イベント ストアからのイベントのクリア」（P.8-42）

イベントの表示

show events [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用して、イベント ストアのイベントを表示します。

開始時刻に開始されているイベントが表示されます。開始時刻を指定しない場合、現時点で開始されているイベントが表示されます。イベント タイプを指定しないと、すべてのイベントが表示されます。

（注）　イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

オプション

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であるか、試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。シグニチャがネットワーク アクティブによってトリガーされると常に、分析エンジンによってアラート イベントが生成されます。レベルが選択されていない場合（informational、low、medium、または high）、すべてのアラート イベントが表示されます。
- **include-traits**：指定された特徴を持つアラートを表示します。
- **exclude-traits**：指定された特徴を持つアラートを表示しません。
- **traits**：特徴ビット位置を 10 進数で指定します（0 ～ 15）。
- **min-threat-rating**：脅威レーティングがこの値以上であるイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：脅威レーティングがこの値以下であるイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。
- **error**：エラー イベントを表示します。エラーの条件が検出されると、サービスによってエラー イベントが生成されます。レベルが選択されていない場合（warning、error、または fatal）、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

  （注）　ARC は、以前は NAC と呼ばれていました。この名前の変更は、Cisco IPS 7.1 の IDM、IME、および CLI に完全には実装されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定した過去の時、分、および秒から開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注）　**show events** コマンドは、指定したイベントが使用可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベントの表示

イベント ストアのイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始しているイベントをすべて表示します。Ctrl キーを押した状態で C キーを押すまで、フィードはすべてのイベントを表示し続けます。

```
ips-ssp# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 351
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

ステップ 3　2011 年 2 月 9 日 10:00 a.m に開始されたブロック要求を表示します。

```
ips-ssp# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: sensor
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
ips-ssp#
```

ステップ 4　2011 年 2 月 9 日 10:00 a.m. に開始された警告レベルのエラーを表示します。

```
ips-ssp# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
ips-ssp# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　30 秒前に開始されたイベントを表示します。

```
ips-ssp# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアからのイベントのクリア

clear events コマンドを使用して、イベント ストアをクリアします。

イベント ストアのイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
ips-ssp# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力して、イベントをクリアします。

CHAPTER 9

異常検出の設定

（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、異常検出（AD）およびその機能と、機能の設定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。

- 「セキュリティ ポリシー」（P.9-2）
- 「異常検出について」（P.9-2）
- 「ワーム」（P.9-2）
- 「異常検出モード」（P.9-3）
- 「異常検出ゾーン」（P.9-4）
- 「異常検出の設定手順」（P.9-5）
- 「異常検出シグニチャ」（P.9-6）
- 「異常検出ポリシーの使用」（P.9-8）
- 「異常検出動作の設定」（P.9-10）
- 「内部ゾーンの設定」（P.9-11）
- 「不正ゾーンの設定」（P.9-20）
- 「外部ゾーンの設定」（P.9-28）
- 「学習受け入れモードの設定」（P.9-37）
- 「KB ファイルの操作」（P.9-40）
- 「異常検出の統計情報の表示」（P.9-47）
- 「異常検出の無効」（P.9-49）

セキュリティ ポリシー

複数のセキュリティ ポリシーを作成し、それらを個々の仮想センサーに適用できます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーから構成されます。Cisco IPS には、sig0 という名前のデフォルトのシグニチャ定義ポリシー、rules0 という名前のデフォルトのイベント アクション規則ポリシー、および ad0 という名前のデフォルトの異常検出ポリシーが用意されています。仮想センサーにこれらのデフォルト ポリシーを割り当てることも、新しいポリシーを作成することもできます。複数のセキュリティ ポリシーを使用すれば、それぞれ異なる要件に基づいたセキュリティ ポリシーを作成し、そうしたカスタマイズされたポリシーを VLAN や物理インターフェイスごとに適用することが可能になります。

異常検出について

注意　異常検出では、両方向からトラフィックが取得されることを前提とします。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

センサーの異常検出コンポーネントは、ワームに感染したホストを検出します。これにより、センサーでは、Code Red や SQL Slammer などのワームとスキャナからの保護に際してシグニチャ アップデートへの依存度が低くなります。異常検出コンポーネントでは、センサーが正常なアクティビティを学習し、正常な動作として学習した動作から逸脱する動作に対してアラートを送信するか、または動的応答アクションを実行します。

（注）　異常検出は、Nimda などの電子メール ベースのワームを検出しません。

異常検出では、次の 2 つの状況が検出されます。

- ワーム トラフィックによって輻輳し始めたパスでネットワークが起動した場合。
- ワームに感染した単一のソースがネットワークに入り、他の脆弱なホストのスキャンを開始した場合。

詳細情報

- 異常検出を無効にする手順については、「異常検出の無効」（P.9-49）を参照してください。
- ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）を参照してください。

ワーム

注意　異常検出では、両方向からトラフィックが取得されることを前提とします。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

ワームは、自身のコピーを作成してその拡散を促進する自動化された自己伝播型侵入エージェントです。ワームは脆弱なホストを攻撃して感染させ、そのホストをベースとして使用して他の脆弱なホストを攻撃します。ネットワーク インスペクションの 1 つの形式（通常はスキャン）を使用して他のホストを検索し、次のターゲットに伝播します。スキャニング ワームは、プローブする IP アドレスのリストを生成することによって脆弱なホストを特定し、そのホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームは、この方法で広がるワームの例です。

異常検出では、スキャナとしての動作によって、ワームに感染したホストを識別します。ワームは、拡散するために新しいホストを見つける必要があります。ワームは、TCP、UDP、およびその他のプロトコルを使用してインターネットまたはネットワークをスキャンし、さまざまな宛先 IP アドレスへの不成功なアクセス試行を生成することによりこれらのホストを見つけます。スキャナは、非常に多くの宛先 IP アドレスに対して（TCP および UDP で）同じ宛先ポートにイベントを生成する送信元 IP アドレスとして定義されます。

TCP プロトコルにとって重要なイベントは、特定の時間内に SYN-ACK 応答のない SYN パケットなどの未確立の接続です。TCP プロトコルを使用してスキャンする、ワームに感染したホストは、異常な数の IP アドレスに対して同じ宛先ポートに未確立の接続を生成します。

UDP プロトコルにとって重要なイベントは、すべてのパケットが単一方向に伝送する UDP 接続などの単一方向接続です。ワームに感染したホストは、UDP プロトコルを使用してスキャンを行い、UDP パケットを生成しますが、複数の宛先 IP アドレスに対して同じ宛先ポートと同じクアッド上でタイムアウト期間内に UDP パケットを受信しません。

ICMP などの他のプロトコルにとって重要なイベントは、送信元 IP アドレスからさまざまな宛先 IP アドレスに送信されます（つまり、単一方向で受信されるパケット）。

注意　ワームが感染する IP アドレスのリストを持ち、スキャニングを使用してワーム自体を拡散する必要がない場合（たとえば、アクティブ スキャニングとは異なり、パッシブ マッピングを使用してネットワークをリッスンする）、ワームは異常検出ワーム ポリシーによって検出されません。また、感染したホスト内のファイルをプローブすることによりメーリング リストを取得し、このリストを電子メールで送信するワームも検出されません。これは、レイヤ 3 またはレイヤ 4 の異常が生成されないためです。

詳細情報

異常検出を無効にする手順については、「異常検出の無効」（P.9-49）を参照してください。

異常検出モード

異常検出は、最初に、ネットワークの最も通常の状態を反映する「平時」学習プロセスを実行します。次に、異常検出は、通常のネットワークに最適なポリシーしきい値セットを派生します。

異常検出には、次のモードがあります。

- 学習受け入れモード：異常検出は、デフォルトで検出モードにありますが、デフォルトの期間である 24 時間、初期学習受け入れモードを実施します。このフェーズ中は攻撃が行われないことを前提とします。異常検出では、ナレッジ ベース（KB）と呼ばれるネットワーク トラフィックの初期ベースラインが作成されます。周期スケジュールのデフォルトの間隔値は 24 時間であり、デフォルトのアクションは循環です。つまり、新しい KB が保存およびロードされ、24 時間後に初期 KB が置き換えられます。

（注）　異常検出では、空の初期 KB を処理するときに攻撃は検出されません。デフォルトの 24 時間後、KB は保存およびロードされ、異常検出によって攻撃が検出されるようになります。

（注）　ネットワークの複雑さに応じて、異常検出をデフォルトの 24 時間以上、学習受け入れモードのままにすることができます。

- 検出モード：操作の進行中は、センサーを検出モードのままにする必要があります。これは 1 日 24 時間、週 7 日間実行します。KB が作成され、初期 KB が置換されたあとで、異常検出は KB に基づいて攻撃を検出します。異常検出は、KB のしきい値に違反するネットワーク トラフィック フローを見つけると、アラートを送信します。異常検出は異常を探すときに、しきい値に違反しない KB の段階的な変更を記録し、新しい KB を作成します。新しい KB は定期的に保存され、古い KB を置き換えるため、最新の KB が保持されます。
- 非アクティブ モード：異常検出は、非アクティブ モードにすることで無効にできます。ある状況では、異常検出を非アクティブ モードにする必要があります（センサーが非対称環境で動作している場合など）。異常検出では、トラフィックが両方向から来ることを前提とするため、センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出によってすべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

例

次の例で、デフォルトの異常検出設定についてまとめます。仮想センサーを 11:00 pm に追加し、デフォルトの異常検出設定を変更しない場合、異常検出は初期 KB の処理を開始し、学習だけを実行します。これは検出モードですが、情報を 24 時間収集して初期 KB を置換するまで、攻撃は検出されません。最初の開始時刻（デフォルトでは 10:00 am）および最初の間隔（デフォルトでは 24 時間）に、学習結果が新しい KB に保存され、この KB がロードされて初期 KB を置換します。異常検出はデフォルトで検出モードであり、異常検出には新しい KB があるため、攻撃の検出が開始されます。

詳細情報

- 異常検出をさまざまなモードにする手順については、「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）を参照してください。
- ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）を参照してください。

異常検出ゾーン

ネットワークをゾーンに分割することで、偽陰性の率を低下させることができます。ゾーンは、宛先 IP アドレスのセットです。内部、不正、および外部の 3 つのゾーンが存在し、それぞれに独自のしきい値があります。

外部ゾーンは、デフォルトのインターネット範囲が 0.0.0.0 ～ 255.255.255.255 のデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンには IP アドレスは含まれません。内部ゾーンまたは不正ゾーンの IP アドレス セットに一致しないパケットは、外部ゾーンで処理されます。

内部ネットワークの IP アドレス範囲を使用して内部ゾーンを設定することを推奨します。このように設定した場合、内部ゾーンは使用している IP アドレス範囲に送信されるすべてのトラフィックであり、外部ゾーンはインターネットに送信されるすべてのトラフィックです。

不正ゾーンは、通常のトラフィックでは決して見られない IP アドレス範囲（割り当てられていない IP アドレスや使用されていない内部 IP アドレス範囲の一部など）で設定できます。不正ゾーンには適正なトラフィックが到達しないと想定されるため、このゾーンは正確な検出に非常に役立ちます。これにより、非常に迅速なワーム ウイルス検出を可能にする非常に低いしきい値を設定できます。

詳細情報

ゾーンの設定手順については、「内部ゾーンの設定」（P.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）を参照してください。

異常検出の設定手順

異常検出の検出部分を設定できます。KB 学習しきい値を上書きするしきい値セットを設定できます。ただし、異常検出は、検出をどのように設定するかに関係なく学習を続行します。また、KB をインポート、エクスポート、およびロードし、KB のデータを参照することもできます。

異常検出の設定時は、次の手順を実行します。

1. 仮想センサーに追加する異常検出ポリシーを作成します。

   または、デフォルトの異常検出ポリシーである ad0 を使用します。

2. 仮想センサーに異常検出ポリシーを追加します。
3. 異常検出ゾーンおよびプロトコルを設定します。
4. デフォルトでは、動作モードは検出に設定されます。ただし、最初の 24 時間は、データが入力された KB を作成するために学習が実行されます。初期 KB は空であるため、デフォルトの 24 時間、異常検出は KB に入力するために使用するデータを収集します。学習期間をデフォルトの 24 時間以上にする場合は、手動でモードを学習受け入れに設定する必要があります。
5. センサーが少なくとも 24 時間（デフォルト値）学習受け入れモードで動作するようにします。

   初期 KB に対してネットワークの通常の状態に関する情報を収集できるよう、センサーを少なくとも 24 時間、学習受け入れモードで動作させる必要があります。ただし、ネットワークの複雑さに応じて、学習受け入れモードの時間を変更する必要があります。この時間の経過後に、センサーは、ネットワークの通常のアクティビティのベースラインとして初期 KB を保存します。

   （注） センサーを少なくとも 24 時間、学習受け入れモードのままにすることが推奨されます。ただし、さらに長い時間（最大 1 週間）センサーを学習受け入れモードで動作させることが理想的です。

6. 異常検出を手動で学習受け入れモードに設定する場合は、再び検出モードに切り替えます。
7. 次のように、異常検出パラメータを設定します。
   - ワーム タイムアウトと、異常検出でバイパスする必要がある送信元および宛先 IP アドレスを設定します。
   - このタイムアウトの経過後、スキャナしきい値が設定された値に戻ります。
   - 異常検出が検出モードにある場合に、自動 KB 更新をイネーブルにするかどうかを決定します。
   - デフォルトの produce-alert 以外のイベント アクションを持つよう 18 個の異常検出ワーム シグニチャを設定します。たとえば、deny-attacker イベント アクションを持つようシグニチャを設定します。

詳細情報

- 異常検出をさまざまなモードにする手順については、「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）を参照してください。
- 新しい異常検出ポリシーの設定手順については、「異常検出ポリシーの使用」（P.9-8）を参照してください。

- ゾーンの設定の詳細については、「内部ゾーンの設定」（P.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）を参照してください。
- 異常検出モードの詳細については、「異常検出モード」（P.9-3）を参照してください。
- 学習受け入れモードの設定の詳細については、「学習受け入れモードの設定」（P.9-37）を参照してください。
- 異常検出シグニチャの設定の詳細については、「異常検出シグニチャ」（P.9-6）を参照してください。
- 拒否攻撃者イベント アクションの詳細については、「イベント アクション」（P.8-4）を参照してください。

異常検出シグニチャ

トラフィック異常エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出で異常が見つかると、これらのシグニチャに関するアラートがトリガーされます。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。アラートの詳細は、ヒストグラムがトリガーされたため、ワーム検出に使用されるしきい値を示します。その時点から、すべてのスキャナはワームに感染したホストとして検出されます。

次の異常検出イベント アクションが可能です。

- produce-alert：イベントをイベント ストアに書き込みます。
- deny-attacker-inline：（インラインのみ）指定された期間、この攻撃者のアドレスから送信されたこのパケットおよび将来のパケットを送信しません。
- log-attacker-packets：攻撃者のアドレスが含まれるパケットに対する IP ロギングを開始します。
- deny-attacker-service-pair-inline：送信元 IP アドレスと宛先ポートをブロックします。
- request-snmp-trapRequest：NotificationApp に要求を送信して SNMP 通知を実行します。
- request-block-host：このホスト（攻撃者）をブロックするよう、ARC に要求を送信します。

表 9-1 に、異常検出ワーム シグニチャのリストを示します。

表 9-1　異常検出ワーム シグニチャ

シグニチャ ID	サブシグニチャ ID	名前	説明
13000	0	Internal TCP Scanner	内部ゾーンで TCP プロトコルを介して単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	0	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。

表 9-1　異常検出ワーム シグニチャ （続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13002	0	Internal Other Scanner	内部ゾーンでほかのプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでほかのプロトコル上にワーム攻撃を識別しました。ほかのヒストグラムのしきい値を超え、ほかのプロトコル上にスキャナが識別されました。
13003	0	External TCP Scanner	外部ゾーンで TCP プロトコルを介して単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	0	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	0	External Other Scanner	外部ゾーンで他のプロトコルを介して単一スキャナを識別しました。
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13006	0	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコルを介してワーム攻撃を識別しました。TCP ヒストグラムのしきい値が超え、TCP プロトコルを介してスキャナが識別されました。
13007	0	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。

表 9-1　異常検出ワーム シグニチャ （続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
13008	0	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介して単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介してワーム攻撃を識別しました。他のヒストグラムのしきい値を超え、他のプロトコルを介してスキャナが識別されました。

詳細情報

アクションをシグニチャに割り当てる手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。

異常検出ポリシーの使用

サービス異常検出サブモードで **service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを作成します。この異常検出ポリシーの値は、編集するまでデフォルトの異常検出ポリシーである ad0 と同じです。

また、特権 EXEC モードで、**copy anomaly-detection** *source_destination* コマンドを使用して、既存のポリシーのコピーを作成し、必要に応じて新しいポリシーの値を編集することもできます。

特権 EXEC モードで **list anomaly-detection-configurations** コマンドを使用して、異常検出ポリシーをリストします。

グローバル コンフィギュレーション モードで **no service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを削除します。グローバル コンフィギュレーション モードで **default service anomaly-detection** *name* コマンドを使用して、異常検出ポリシーを工場出荷時の設定にリセットします。

異常検出ポリシーを作成、コピー、表示、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出ポリシーを作成します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection MyAnomaly Detection
Editing new instance MyAnomaly Detection.
ips-ssp(config-ano)# exit
Apply Changes?[yes]: yes
ips-ssp(config)# exit
ips-ssp#
```

ステップ 3　または、既存の異常検出ポリシーを新しい異常検出ポリシーにコピーします。

```
ips-ssp# copy anomaly-detection ad0 ad1
ips-ssp#
```

（注）　ポリシーがすでに存在しているか、新しいポリシーに必要な容量が不足していると、エラーが表示されます。

ステップ 4　デフォルトの異常検出ポリシー値を受け入れるか、次のようなパラメータの編集を行います。

a. 動作の設定を行います。

b. ゾーンを設定します。

c. 学習受け入れモードを設定します。

d. KB の操作方法を学習します。

ステップ 5　センサーに異常検出ポリシーのリストを表示します。

```
ips-ssp# list anomaly-detection-configurations
Anomaly Detection
   Instance    Size    Virtual Sensor
   ad0         255     vs0
   temp        707     N/A
   MyAnomaly Detection        255     N/A
   ad1         141     vs1
ips-ssp#
```

ステップ 6　異常検出ポリシーを削除します。

```
ips-ssp# configure terminal
ips-ssp(config)# no service anomaly-detection MyAnomaly Detection
ips-ssp(config)# exit
ips-ssp#
```

（注）　デフォルトの異常検出ポリシーである ad0 を削除することはできません。

ステップ 7　異常検出インスタンスが削除されたことを確認します。

```
ips-ssp# list anomaly-detection-configurations
Anomaly Detection
   Instance    Size    Virtual Sensor
   ad0         204     vs0
   ad1         141     N/A
ips-ssp#
```

ステップ 8　異常検出ポリシーを工場出荷時の設定にリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# default service anomaly-detection ad1
ips-ssp(config)#
```

詳細情報

- 動作の設定手順については、「異常検出動作の設定」（P.9-10）を参照してください。
- 異常検出ゾーンの設定手順については、「内部ゾーンの設定」（P.9-11）、「不正ゾーンの設定」（P.9-20）、および「外部ゾーンの設定」（P.9-28）を参照してください。
- 学習受け入れモードの設定手順については、「学習受け入れモードの設定」（P.9-38）を参照してください。
- KB を操作する手順については、「KB ファイルの操作」（P.9-40）を参照してください。

異常検出動作の設定

サービス異常検出サブモードで **worm-timeout** コマンドを使用して、ワーム検出タイムアウトを設定します。このタイムアウトの経過後、スキャナしきい値が設定された値に戻ります。サービス異常検出サブモードで **ignore** コマンドを使用して、異常検出が KB のために情報を収集するときにセンサーが無視する送信元および宛先 IP アドレスを設定します。異常検出はこれらの送信元および宛先 IP アドレスを追跡せず、KB しきい値はこれらの IP アドレスの影響を受けません。

オプション

次のオプションが適用されます。

- **worm-timeout**：ワーム終了タイムアウトの時間（秒単位）を指定します。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。
- **ignore**：異常検出の処理中に無視する IP アドレスを指定します。
  - **enabled [true | false]**：無視される IP アドレスのリストをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
  - **source-ip-address-range**：処理中に異常検出が無視する送信元 IP アドレスを指定します。
  - **dest-ip-address-range**：処理中に異常検出が無視する宛先 IP アドレスを指定します。

（注）　IP アドレスの形式は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] のようになります。

異常検出動作設定の指定

異常検出動作設定を指定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad1
```

ステップ 3　ワーム タイムアウトを指定します。

```
ips-ssp(config-ano)# worm-timeout 800
```

ステップ 4　設定を確認します。

```
ips-ssp(config-ano)# show settings
   worm-timeout: 800 seconds default: 600
```

ステップ 5　異常検出の処理中に無視する宛先 IP アドレスを指定します。

```
ips-ssp(config-ano)# ignore
ips-ssp(config-ano-ign)# dest-ip-address-range 10.10.5.5,10.10.2.1-10.10.2.30
```

ステップ 6　異常検出の処理中に無視する送信元 IP アドレスを指定します。

```
ips-ssp(config-ano-ign)# source-ip-address-range 10.20.30.108-10.20.30.191
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-ano-ign)# show settings
   ignore
   -----------------------------------------------
      enabled: true default: true
      source-ip-address-range: 10.20.30.108-10.20.30.191 default: 0.0.0.0
      dest-ip-address-range: 10.10.5.5,10.10.2.1-10.10.2.30 default: 0.0.0.0
   -----------------------------------------------
ips-ssp(config-ano-ign)#
```

ステップ 8　異常検出サブモードを終了します。

```
ips-ssp(config-ano-ign)# exit
ips-ssp(config-ano)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

内部ゾーンの設定

ここでは、内部ゾーンの設定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。

- 「内部ゾーンについて」（P.9-11）
- 「内部ゾーンの設定」（P.9-11）
- 「内部ゾーンに対する TCP プロトコルの設定」（P.9-13）
- 「内部ゾーンに対する UDP プロトコルの設定」（P.9-15）
- 「内部ゾーンに対する他のプロトコルの設定」（P.9-18）

内部ゾーンについて

内部ゾーンは、使用している内部ネットワークを表す必要があります。また、使用している IP アドレス範囲に送信されるすべてのトラフィックを受信する必要があります。ゾーンがディセーブルな場合は、このゾーンに対するパケットが無視されます。デフォルトでは、ゾーンはイネーブルになります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに対して IP アドレスを設定しない場合は、すべてのパケットがデフォルトのゾーンである外部ゾーンに送信されます。

内部ゾーンに対して TCP、UDP、およびその他のプロトコルをイネーブルまたはディセーブルにできます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

内部ゾーンの設定

サービス異常検出サブモードで **internal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** |**other**} コマンドを使用して、内部ゾーンをイネーブルにし、IP アドレスを内部ゾーンに追加し、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **ip-address-range**：ゾーンのサブネットの IP アドレスを指定します。有効な値は <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] です。

（注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

内部ゾーンの設定

内部ゾーンを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　内部ゾーンをイネーブルにします。

```
ips-ssp(config-ano-int)# enabled true
```

ステップ 4　内部ゾーンに含める IP アドレスを設定します。

```
ips-ssp(config-ano-int)# ip-address-range 192.0.2.72-192.0.2.108
```

ステップ 5　TCP プロトコルを設定します。

ステップ 6　UDP プロトコルを設定します。

ステップ 7　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「内部ゾーンに対する TCP プロトコルの設定」（P.9-13）を参照してください。
- UDP プロトコルの設定手順については、「内部ゾーンに対する UDP プロトコルの設定」（P.9-15）を参照してください。
- その他のプロトコルの設定手順については、「内部ゾーンに対する他のプロトコルの設定」（P.9-18）を参照してください。

内部ゾーンに対する TCP プロトコルの設定

サービス異常検出内部ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：TCP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーン TCP プロトコルの設定

内部ゾーンに対して TCP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# tcp
ips-ssp(config-ano-int-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-int-tcp)# dst-port 20
ips-ssp(config-ano-int-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-int-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-int-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-tcp-dst-yes)# exit
ips-ssp(config-ano-int-tcp-dst)# exit
ips-ssp(config-ano-int-tcp)# exit
ips-ssp(config-ano-int-tcp)# default-thresholds
ips-ssp(config-ano-int-tcp-def)# default-thresholds
ips-ssp(config-ano-int-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-int-tcp)# show settings
   tcp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ----------------------------------------------
         number: 20
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 120 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ----------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true default: true
         ----------------------------------------------
         number: 23
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
         number: 113
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
         number: 567
         ----------------------------------------------
            override-scanner-settings
```

```
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ---------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ---------------------------------------------
ips-ssp(config-ano-int-tcp)#
```

内部ゾーンに対する UDP プロトコルの設定

サービス異常検出内部ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：UDP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# udp
ips-ssp(config-ano-int-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-int-udp)# dst-port 20
ips-ssp(config-ano-int-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-int-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-int-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-udp-dst-yes)# exit
ips-ssp(config-ano-int-udp-dst)# exit
ips-ssp(config-ano-int-udp)# default-thresholds
ips-ssp(config-ano-int-udp-def)# default-thresholds
ips-ssp(config-ano-int-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-int-udp)# show settings
   udp
   -----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      -----------------------------------------------
         number: 20
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
```

```
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            enabled: true default: true
         ---------------------------------------------
         number: 23
         ---------------------------------------------
            override-scanner-settings
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
         number: 113
         ---------------------------------------------
            override-scanner-settings
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
         number: 567
         ---------------------------------------------
            override-scanner-settings
            ---------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
      ---------------------------------------------
      default-thresholds
      ---------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ---------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ---------------------------------------------
      ---------------------------------------------
      enabled: true <defaulted>
   ---------------------------------------------
ips-ssp(config-ano-int-udp)#
```

内部ゾーンに対する他のプロトコルの設定

サービス異常検出内部ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true | false** }：他のプロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

内部ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出内部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# internal-zone
ips-ssp(config-ano-int)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-int)# other
ips-ssp(config-ano-int-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-int-oth)# protocol-number 5
ips-ssp(config-ano-int-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-int-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-int-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-int-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-int-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-int-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-int-oth-pro-yes)# exit
ips-ssp(config-ano-int-oth-pro)# exit
ips-ssp(config-ano-int-oth)# default-thresholds
ips-ssp(config-ano-int-oth-def)# default-thresholds
ips-ssp(config-ano-int-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-int-oth-def)# scanner-threshold 120
```

ステップ 10　他の設定を確認します。

```
ips-ssp(config-ano-int-oth)# show settings
   other
   -----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      -----------------------------------------------
         number: 5
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  -----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            enabled: true default: true
         -----------------------------------------------
      -----------------------------------------------
      default-thresholds
      -----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         -----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      enabled: true default: true
   -----------------------------------------------
ips-ssp(config-ano-int-oth)#
```

不正ゾーンの設定

ここでは、不正ゾーンの設定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。

- 「不正ゾーンについて」（P.9-20）
- 「不正ゾーンの設定」（P.9-20）
- 「不正ゾーンに対する TCP プロトコルの設定」（P.9-21）
- 「不正ゾーンに対する UDP プロトコルの設定」（P.9-24）
- 「不正ゾーンに対する他のプロトコルの設定」（P.9-26）

不正ゾーンについて

不正ゾーンは、正常なトラフィックでは決して見られない IP アドレス範囲（割り当てられていない IP アドレスや使用されていない内部 IP アドレス範囲の一部など）を表す必要があります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに対して IP アドレスを設定しない場合は、すべてのパケットがデフォルトのゾーンである外部ゾーンに送信されます。

内部ゾーンに対して TCP、UDP、およびその他のプロトコルをイネーブルまたはディセーブルにできます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

不正ゾーンの設定

サービス異常検出サブモードで **illegal-zone** {**enabled** | **ip-address-range** | **tcp** | **udp** |**other**} コマンドを使用して、不正ゾーンをイネーブルにし、IP アドレスを不正ゾーンに追加し、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **ip-address-range**：ゾーンのサブネットの IP アドレスを指定します。有効な値は <A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] です。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

不正ゾーンの設定

不正ゾーンを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　不正ゾーンをイネーブルにします。

```
ips-ssp(config-ano-ill)# enabled true
```

ステップ 4　不正ゾーンに含める IP アドレスを設定します。

```
ips-ssp(config-ano-ill)# ip-address-range 192.0.2.72-192.0.2.108
```

ステップ 5　TCP プロトコルを設定します。

ステップ 6　UDP プロトコルを設定します。

ステップ 7　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「不正ゾーンに対する TCP プロトコルの設定」（P.9-21）を参照してください。
- UDP プロトコルの設定手順については、「不正ゾーンに対する UDP プロトコルの設定」（P.9-24）を参照してください。
- その他のプロトコルの設定手順については、「不正ゾーンに対する他のプロトコルの設定」（P.9-26）を参照してください。

不正ゾーンに対する TCP プロトコルの設定

サービス異常検出不正ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：TCP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。

- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーン TCP プロトコルの設定

不正ゾーンに対して TCP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# tcp
ips-ssp(config-ano-ill-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-ill-tcp)# dst-port 20
ips-ssp(config-ano-ill-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ill-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-tcp-dst-yes)# exit
ips-ssp(config-ano-ill-tcp-dst)# exit
ips-ssp(config-ano-ill-tcp)# exit
ips-ssp(config-ano-ill-tcp)# default-thresholds
ips-ssp(config-ano-ill-tcp-def)# default-thresholds
ips-ssp(config-ano-ill-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-ill-tcp)# show settings
   tcp
   ------------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ------------------------------------------------
         number: 20
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               yes
               ------------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ------------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true default: true
         ------------------------------------------------
         number: 23
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 113
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
         number: 567
         ------------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
```

```
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
          ------------------------------------------------
        ------------------------------------------------
        enabled: true <defaulted>
      ------------------------------------------------
ips-ssp(config-ano-ill-tcp)#
```

不正ゾーンに対する UDP プロトコルの設定

サービス異常検出不正ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true | false** }：UDP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# udp
ips-ssp(config-ano-ill-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-ill-udp)# dst-port 20
ips-ssp(config-ano-ill-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ill-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ill-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-udp-dst-yes)# exit
ips-ssp(config-ano-ill-udp-dst)# exit
ips-ssp(config-ano-ill-udp)# exit
ips-ssp(config-ano-ill-udp)# default-thresholds
ips-ssp(config-ano-ill-udp-def)# default-thresholds
ips-ssp(config-ano-ill-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-ill-udp)# show settings
   udp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ----------------------------------------------
         number: 20
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ----------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                  ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true default: true
         ----------------------------------------------
         number: 23
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
```

```
            enabled: true <defaulted>
         ----------------------------------------------
         number: 113
         ----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
         number: 567
         ----------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ---------------------------------------------
               ---------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ----------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
ips-ssp(config-ano-ill-udp)#
```

不正ゾーンに対する他のプロトコルの設定

サービス異常検出不正ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true | false** }：他のプロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。

  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

不正ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出不正ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# illegal-zone
ips-ssp(config-ano-ill)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-ill)# other
ips-ssp(config-ano-ill-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-ill-oth)# protocol-number 5
ips-ssp(config-ano-ill-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ill-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ill-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-ill-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ill-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ill-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ill-oth-pro-yes)# exit
ips-ssp(config-ano-ill-oth-pro)# exit
ips-ssp(config-ano-ill-oth)# default-thresholds
ips-ssp(config-ano-ill-oth-def)# default-thresholds
ips-ssp(config-ano-ill-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ill-oth-def)# scanner-threshold 120
```

ステップ 10　その他のプロトコルの設定を確認します。

```
ips-ssp(config-ano-ill-oth)# show settings
   other
   -----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      -----------------------------------------------
         number: 5
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
               -----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  -----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            enabled: true default: true
         -----------------------------------------------
      -----------------------------------------------
      default-thresholds
      -----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         -----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      enabled: true default: true
   -----------------------------------------------
ips-ssp(config-ano-ill-oth)#
```

外部ゾーンの設定

ここでは、外部ゾーンの設定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。

- 「外部ゾーンについて」（P.9-29）
- 「外部ゾーンの設定」（P.9-29）
- 「外部ゾーンに対する TCP プロトコルの設定」（P.9-30）
- 「外部ゾーンに対する UDP プロトコルの設定」（P.9-32）
- 「外部ゾーンに対するその他のプロトコルの設定」（P.9-35）

外部ゾーンについて

外部ゾーンは、デフォルトのインターネット範囲が 0.0.0.0 ～ 255.255.255.255 のデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンには IP アドレスは含まれません。内部ゾーンまたは不正ゾーンの IP アドレス セットに一致しないパケットは、外部ゾーンで処理されます。

外部ゾーンに対して TCP、UDP、およびその他のプロトコルをイネーブルまたはディセーブルにできます。TCP および UDP プロトコルに対して宛先ポートを設定したり、その他のプロトコルに対してプロトコル番号を設定したりできます。デフォルトしきい値を使用するか、あるいはスキャナ設定を上書きして、独自のしきい値とヒストグラムを追加できます。

外部ゾーンの設定

サービス異常検出サブモードで **external-zone** {**enabled** | **tcp** | **udp** |**other**} コマンドを使用して、外部ゾーンをイネーブルにし、プロトコルを指定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：ゾーンをイネーブルまたはディセーブルにします。
- **tcp**：TCP プロトコルを設定できます。
- **udp**：UDP プロトコルを設定できます。
- **other**：TCP と UDP 以外の他のプロトコルを設定できます。

外部ゾーンの設定

外部ゾーンを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　外部ゾーンをイネーブルにします。

```
ips-ssp(config-ano-ext)# enabled true
```

ステップ 4　TCP プロトコルを設定します。

ステップ 5　UDP プロトコルを設定します。

ステップ 6　その他のプロトコルを設定します。

詳細情報

- TCP プロトコルの設定手順については、「外部ゾーンに対する TCP プロトコルの設定」（P.9-30）を参照してください。
- UDP プロトコルの設定手順については、「外部ゾーンに対する UDP プロトコルの設定」（P.9-32）を参照してください。

- その他のプロトコルの設定手順については、「外部ゾーンに対するその他のプロトコルの設定」（P.9-35）を参照してください。

外部ゾーンに対する TCP プロトコルの設定

サービス異常検出外部ゾーン サブモードで **tcp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、TCP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：TCP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram** {**low** | **medium** | **high**} **num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーン TCP プロトコルの設定

外部ゾーンに対して TCP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　TCP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# tcp
ips-ssp(config-ano-ext-tcp)# enabled true
```

ステップ 4　特定のポートを TCP プロトコルに関連付けます。

```
ips-ssp(config-ano-ext-tcp)# dst-port 20
ips-ssp(config-ano-ext-tcp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-tcp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-tcp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ext-tcp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-tcp-dst-yes)# exit
ips-ssp(config-ano-ext-tcp-dst)# exit
ips-ssp(config-ano-ext-tcp)# exit
ips-ssp(config-ano-ext-tcp)# default-thresholds
ips-ssp(config-ano-ext-tcp-def)# default-thresholds
ips-ssp(config-ano-ext-tcp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-tcp-def)# scanner-threshold 120
```

ステップ 10　TCP 設定を確認します。

```
ips-ssp(config-ano-ext-tcp)# show settings
   tcp
   ----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      ----------------------------------------------
         number: 20
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 100 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ----------------------------------------------
                     dest-ip-bin: low
                     num-source-ips: 100
                     ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true default: true
         ----------------------------------------------
         number: 23
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true <defaulted>
         ----------------------------------------------
         number: 113
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
```

```
            ------------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
         number: 567
         ---------------------------------------------
            override-scanner-settings
            ------------------------------------------------
               no
               ------------------------------------------------
               ------------------------------------------------
            ------------------------------------------------
            enabled: true <defaulted>
         ---------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 120 default: 200
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium
            num-source-ips: 120 default: 1
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
ips-ssp(config-ano-ext-tcp)#
```

外部ゾーンに対する UDP プロトコルの設定

サービス異常検出外部ゾーン サブモードで **udp** {**enabled** | **dst-port** *number* | **default-thresholds**} コマンドを使用して、UDP サービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true | false** }：UDP プロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **dst-port** *number*：特定の宛先ポートに対してしきい値を定義します。有効な値は 0 ～ 65535 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。

– **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーン UDP プロトコルの設定

ゾーンに対して UDP プロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　UDP プロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# udp
ips-ssp(config-ano-ext-udp)# enabled true
```

ステップ 4　特定のポートを UDP プロトコルに関連付けます。

```
ips-ssp(config-ano-ext-udp)# dst-port 20
ips-ssp(config-ano-ext-udp-dst)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-udp-dst)# enabled true
```

ステップ 6　そのポートのスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-udp-dst)# override-scanner-settings yes
ips-ssp(config-ano-ext-udp-dst-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ext-udp-dst-yes)# threshold-histogram low num-source-ips 100
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-udp-dst-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-udp-dst-yes)# exit
ips-ssp(config-ano-ext-udp-dst)# exit
ips-ssp(config-ano-ext-udp)# default-thresholds
ips-ssp(config-ano-ext-udp-def)# default-thresholds
ips-ssp(config-ano-ext-udp-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-udp-def)# scanner-threshold 120
```

ステップ 10　UDP 設定を確認します。

```
ips-ssp(config-ano-ext-udp)# show settings
   udp
   -----------------------------------------------
      dst-port (min: 0, max: 65535, current: 4)
      -----------------------------------------------
         number: 20
         -----------------------------------------------
            override-scanner-settings
            -----------------------------------------------
               yes
```

```
                  ------------------------------------------------
                     scanner-threshold: 100 default: 200
                     threshold-histogram (min: 0, max: 3, current: 1)
                     ------------------------------------------------
                        dest-ip-bin: low
                        num-source-ips: 100
                     ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true default: true
            ------------------------------------------------
            number: 23
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
            number: 113
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
            number: 567
            ------------------------------------------------
               override-scanner-settings
               ------------------------------------------------
                  no
                  ------------------------------------------------
                  ------------------------------------------------
               ------------------------------------------------
               enabled: true <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 120 default: 200
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium
               num-source-ips: 120 default: 1
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
ips-ssp(config-ano-ext-udp)#
```

外部ゾーンに対するその他のプロトコルの設定

サービス異常検出外部ゾーン サブモードで **other** {**enabled** | **protocol** *number* | **default-thresholds**} コマンドを使用して、その他のサービスをイネーブルにし、設定します。

オプション

次のオプションが適用されます。

- **enabled** {**true** | **false** }：他のプロトコルをイネーブルまたはディセーブルにします。
- **default-thresholds**：宛先ポート マップで指定されないすべてのポートに使用されるしきい値を定義します。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。
- **protocol-number** *number*：特定のプロトコルに対するしきい値を定義します。有効な値は 0 ～ 255 です。
- **enabled** {**true** | **false**}：サービスをイネーブルまたはディセーブルにします。
- **override-scanner-settings** {**yes** | **no**}：スキャナ値を上書きできます。
  - **threshold-histogram {low | medium | high} num-source-ips** *number*：しきい値ヒストグラムの値を設定します。
  - **scanner-threshold**：スキャナしきい値を設定します。デフォルトは 200 です。

外部ゾーンの他のプロトコルの設定

ゾーンに対して他のプロトコルを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出外部ゾーン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# external-zone
ips-ssp(config-ano-ext)#
```

ステップ 3　他のプロトコルをイネーブルにします。

```
ips-ssp(config-ano-ext)# other
ips-ssp(config-ano-ext-oth)# enabled true
```

ステップ 4　他のプロトコルに対して特定の番号を関連付けます。

```
ips-ssp(config-ano-ext-oth)# protocol-number 5
ips-ssp(config-ano-ext-oth-pro)#
```

ステップ 5　そのポートのサービスをイネーブルにします。

```
ips-ssp(config-ano-ext-oth-pro)# enabled true
```

ステップ 6　そのプロトコルに対するスキャナ値を上書きします。デフォルトのスキャナ値を使用するか、あるいはそれらの値を上書きし、独自のスキャナ値を設定できます。

```
ips-ssp(config-ano-ext-oth-pro)# override-scanner-settings yes
ips-ssp(config-ano-ext-oth-pro-yes)#
```

ステップ 7　新しいスキャナ設定に対してヒストグラムを追加します。宛先 IP アドレスの数（low、medium、または high）と、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。

```
ips-ssp(config-ano-ext-oth-pro-yes)# threshold-histogram high num-source-ips 75
```

ステップ 8　スキャナしきい値を設定します。

```
ips-ssp(config-ano-ext-oth-pro-yes)# scanner-threshold 100
```

ステップ 9　他のすべての未指定ポートに対してデフォルトしきい値を設定します。

```
ips-ssp(config-ano-ext-oth-pro-yes)# exit
ips-ssp(config-ano-ext-oth-pro)# exit
ips-ssp(config-ano-ext-oth)# default-thresholds
ips-ssp(config-ano-ext-oth-def)# default-thresholds
ips-ssp(config-ano-ext-oth-def)# threshold-histogram medium num-source-ips 120
ips-ssp(config-ano-ext-oth-def)# scanner-threshold 120
```

ステップ 10　その他のプロトコルの設定を確認します。

```
ips-ssp(config-ano-ext-oth)# show settings
   other
   ----------------------------------------------
      protocol-number (min: 0, max: 255, current: 1)
      ----------------------------------------------
         number: 5
         ----------------------------------------------
            override-scanner-settings
            ----------------------------------------------
               yes
               ----------------------------------------------
                  scanner-threshold: 95 default: 200
                  threshold-histogram (min: 0, max: 3, current: 1)
                  ----------------------------------------------
                     dest-ip-bin: high
                     num-source-ips: 75
                  ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            enabled: true default: true
         ----------------------------------------------
      ----------------------------------------------
      default-thresholds
      ----------------------------------------------
         scanner-threshold: 200 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         ----------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      enabled: true default: true
   ----------------------------------------------
ips-ssp(config-ano-ext-oth)#
```

学習受け入れモードの設定

ここでは、KB およびヒストグラムと、学習受け入れモードの設定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。

- 「KB およびヒストグラム」（P.9-37）
- 「学習受け入れモードの設定」（P.9-38）

KB およびヒストグラム

KB にはツリー構造があり、次の情報を含みます。

- KB 名
- ゾーン名
- プロトコル
- サービス

スキャナしきい値と各サービスのヒストグラムは、KB に保存されます。学習受け入れモードを自動に設定し、アクションを循環に設定した場合、新しい KB は 24 時間ごとに作成され、次の 24 時間使用されます。学習受け入れモードを自動に設定し、アクションを保存だけに設定した場合は、新しい KB が作成されますが、現在の KB が使用されます。学習受け入れモードを自動に設定しない場合、KB は作成されません。

（注）　学習受け入れモードは、センサーの現地時間を使用します。

スキャナしきい値は、単一の送信元 IP アドレスがスキャンできるゾーン IP アドレスの最大数を定義します。ヒストグラムしきい値は、ゾーン IP アドレスの指定された数よりも多くをスキャンできる送信元 IP アドレスの最大数を定義します。

異常検出では、攻撃が進行中でないときに学習したヒストグラムから逸脱した場合（つまり、定義されたゾーン宛先 IP アドレスよりも多くを同時にスキャンする送信元 IP アドレスの数を超えた場合）にワーム攻撃が識別されます。たとえば、スキャニングしきい値が 300 であり、ポートのヒストグラムが 445 である場合は、異常検出で 350 個のゾーン宛先 IP アドレスをスキャンするスキャナが識別されると、マス スキャナが検出されたことを示すアクションが生成されます。ただし、このスキャナは、ワーム攻撃が進行中であることを確認しません。表 9-2 に、この例を示します。

表 9-2　ヒストグラム例

送信元 IP アドレスの数	10	5	2
宛先 IP アドレスの数	5	20	100

異常検出が、ポート 445 で 50 個を超えるゾーン宛先 IP アドレスをスキャンする 6 個の同時送信元 IP アドレスを識別した場合は、異常検出がポート 445 でワーム攻撃を識別したことを示す、未指定の送信元 IP アドレスを持つアクションが生成されます。ダイナミック フィルタしきい値である 50 により、新しい内部スキャニングしきい値が指定され、新しいスキャニングしきい値（50）よりも多くをスキャンする各送信元 IP アドレスに対して追加のダイナミック フィルタを生成するよう異常検出がスキャナのしきい値定義を小さくします。

KB が異常検出ポリシーとゾーンごとに学習したことを上書きできます。使用しているネットワーク トラフィックを理解している場合は、オーバーライドを使用して偽陽性を制限できます。

学習受け入れモードの設定

サービス異常検出サブモードで **learning-accept-mode** コマンドを使用して、センサーが長い時間ごとに新しい KB を作成するかどうかを設定します。KB を作成およびロード（循環）するか、保存（保存だけ）するかを設定できます。KB がロードまたは保存される頻度とタイミングをスケジュールできます。

更新された新しい KB ファイルの名前は、現在の日時である *YYYY-Mon-dd-hh_mm_ss* になります。ここで、*Mon* は 3 文字で構成される月の略語です。

（注） 異常検出学習受け入れモードは、センサーの現地時間を使用します。

オプション

次のオプションが適用されます。

- **learning-accept-mode**：KB を保存およびロードするかどうかと、いつ KB を保存およびロードするかを指定します。
  - **auto**：KB を自動的に受け入れるようセンサーを設定します。
  - **manual**：KB を保存しません。

    （注） KB は、**anomaly-detection** [**load** | **save**] コマンドを使用して保存およびロードできます。

- **action**：KB を循環または保存するかどうかを指定できます。
  - **save-only**：新しい KB を保存します。この KB を調べて、異常検出にロードするかどうかを決定できます。

    （注） KB は、**anomaly-detection load** コマンドを使用してロードできます。

  - **rotate**：定義したスケジュールに基づいて、新しい KB を保存し、現在の KB としてロードします。
- **schedule**：KB を受け入れるスケジュールを設定します。
  - **calendar-schedule [days-of-week] [times-of-day]**：特定の日時に学習受け入れモードを開始します。
  - **periodic-schedule [interval] [start-time]**：特定の周期間隔で学習受け入れモードを開始します。

学習受け入れモードの設定

最初の保存は、設定時刻と開始時刻間の完全な間隔後に開始されます。たとえば、時刻が現在 16:00 であり、1 時間の間隔で開始時刻を 16:30 に設定した場合、16:00 と 16:30 の間には 1 時間の間隔がないため、最初の KB は 17:30 に保存されます。

学習受け入れモードを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　異常検出サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service anomaly-detection ad1
```

ステップ 3　KB をどのように保存およびロードするかを指定します。

a. KB が自動的に保存およびロードされることを指定します。ステップ 4 に進みます。

```
ips-ssp(config-ano)# learning-accept-mode auto
ips-ssp(config-ano-auto)#
```

b. KB を手動で保存およびロードすることを指定します。ステップ 6 に進みます。

```
ips-ssp(config-ano)# learning-accept-mode manual
ips-ssp(config-ano-man)#
```

ステップ 4　KB をどのように自動的に受け入れるかを指定します。

a. KB を検査し、ロードするかどうかを決定するために KB を保存します。ステップ 6 に進みます。

```
ips-ssp(config-ano-aut)# action save-only
```

b. 定義したスケジュールに基づいて、KB を保存し、現在の KB としてロードします。ステップ 5 に進みます。

```
ips-ssp(config-ano-aut)# action rotate
```

ステップ 5　自動的な KB の保存およびロードをスケジュールします。

- カレンダー スケジュール：このスケジュールでは、KB が毎月曜日の夜 12 時に保存およびロードされます。

```
ips-ssp(config-ano-aut)# schedule calendar-schedule
ips-ssp(config-ano-aut-cal)# days-of-week monday
ips-ssp(config-ano-aut-cal)# times-of-day time 24:00:00
```

- 周期スケジュール：このスケジュールでは、KB が毎日夜 12 時に保存およびロードされます。

```
ips-ssp(config-ano-aut)# schedule periodic-schedule
ips-ssp(config-ano-aut-per)# start-time 24:00:00
ips-ssp(config-ano-aut-per)# interval 24
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-ano-aut-per)# exit
ips-ssp(config-ano-aut)# show settings
   auto
   -----------------------------------------------
      action: rotate default: rotate
      schedule
      -----------------------------------------------
         periodic-schedule
         -----------------------------------------------
            start-time: 12:00:00 default: 10:00:00
            interval: 24 hours default: 24
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 7　異常検出サブモードを終了します。

```
ips-ssp(config-ano-aut)# exit
ips-ssp(config-ano)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

異常検出 KB を手動で保存およびロードする手順については、「手動による KB の保存およびロード」（P.9-41）を参照してください。

KB ファイルの操作

ここでは、KB ファイルの表示、ロード、保存、コピー、名前変更、および削除を行う方法について説明します。また、2 つの KB ファイルを比較し、KB ファイルのしきい値を表示する手順についても説明します。次のような構成になっています。

- 「KB ファイルの表示」（P.9-40）
- 「手動による KB の保存およびロード」（P.9-41）
- 「KB のコピー、名前変更、および消去」（P.9-42）
- 「2 つの KB 間の違いの表示」（P.9-44）
- 「KB のしきい値の表示」（P.9-45）

KB ファイルの表示

特権 EXEC モードで **show ad-knowledge-base** [*virtual-sensor*] **files** コマンドを使用して、仮想センサーに利用可能な KB ファイルを表示します。

（注）　ファイル名の前の * は、この KB ファイルが現在ロードされている KB ファイルであることを示します。

KB ファイルを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　すべての仮想センサーに対して KB ファイルを表示します。

```
ips-ssp# show ad-knowledge-base files
Virtual Sensor vs0
    Filename                Size    Created
    initial                 84      04:27:07 CDT Wed Jan 29 2010
*   2010-Jan-28-10_00_01    84      04:27:07 CDT Wed Jan 29 2010
Virtual Sensor vs1
    Filename                Size    Created
    initial                 84      14:35:38 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00    84      10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00    84      10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00    84      10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00    84      10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00    84      10:00:00 CDT Mon Mar 20 2011
    2011-Mar-21-10_00_00    84      10:00:00 CDT Tue Mar 21 2011
    2011-Mar-22-10_00_00    84      10:00:00 CDT Wed Mar 22 2011
    2011-Mar-23-10_00_00    84      10:00:00 CDT Thu Mar 23 2011
    2011-Mar-24-10_00_00    84      10:00:00 CDT Fri Mar 24 2011
    2011-Mar-25-10_00_00    84      10:00:00 CDT Sat Mar 25 2011
    2011-Mar-26-10_00_00    84      10:00:00 CDT Sun Mar 26 2011
    2011-Mar-27-10_00_00    84      10:00:00 CDT Mon Mar 27 2011
    2010-Jan-02-10_00_00    84      10:00:00 CDT Thu Jan 02 2010
    2010-Jan-03-10_00_00    84      10:00:00 CDT Fri Jan 03 2010
    2010-Jan-04-10_00_00    84      10:00:00 CDT Sat Jan 04 2010
```

```
    2010-Jan-05-10_00_00   84     10:00:00 CDT Sun Jan 05 2010
    2010-Jan-06-10_00_00   84     10:00:00 CDT Mon Jan 06 2010
ips-ssp#
```

ステップ 3　特定の仮想センサーに対して KB ファイルを表示します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

手動による KB の保存およびロード

特権 EXEC モードで以下のコマンドを使用して、手動で KB を保存およびロードします。

オプション

次のオプションが適用されます。

- **show ad-knowledge-base** *virtual-sensor* **files**：仮想センサーごとに利用可能な KB ファイルを表示します。
- **anomaly-detection** *virtual-sensor* **load** {**initial** | **file** *name*}：指定された仮想センサーに対して KB ファイルを現在の KB として設定します。AD がアクティブな場合、ファイルは現在の KB としてロードされます。
- **anomaly-detection** *virtual-sensor* **save** [*new-name*]：現在の KB ファイルを取得し、ローカルで保存します。

手動による KB の保存およびロード

手動で KB を保存およびロードするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ロードする KB を特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

ステップ 3　特定の仮想センサーに対して KB ファイルを現在の KB ファイルとしてロードします。

```
ips-ssp# anomaly-detection vs0 load file 2011-Mar-16-10_00_00
ips-ssp#
```

ステップ 4　現在の KB ファイルを保存し、新しい名前で保管します。

```
ips-ssp# anomaly-detection vs0 save my-KB
ips-ssp#
```

（注）　このコマンドを入力したときに異常検出がアクティブでない場合は、エラーが生成されます。初期ファイルを上書きすることはできません。

KB のコピー、名前変更、および消去

KB ファイルのコピー、名前変更、および消去を手動で行うには、特権 EXEC モードで以下のコマンドを使用します。

オプション

次のオプションが適用されます。

- **copy ad-knowledge-base** *virtual-sensor* {**current** | **initial** | **file** *name*} *destination-url* : 指定された宛先 URL に KB ファイル（現在、初期、または入力したファイル名）をコピーします。

  （注）　既存の名前にファイルをコピーすると、上書きされます。

- **copy ad-knowledge-base** *virtual-sensor source-url new-name* : 新しいファイル名を持つ KB を、指定した送信元 URL にコピーします。

  （注）　**current** キーワードを *new-name* として使用することはできません。新しい現在の KB ファイルは、**load** コマンドで作成されます。

- **rename ad-knowledge-base** *virtual-sensor* {**current** | **file** ***name***} *new-name* : 既存の KB ファイルの名前を変更します。
- **erase ad-knowledge-base** [*virtual-sensor* [*name*]] : 仮想センサーからすべての KB ファイル、または 1 つの KB ファイル（*name* オプションを使用する場合）を削除します。

初期 KB ファイル、または現在の KB としてロードされた KB ファイルを消去することはできません。送信元および宛先 URL の実際の形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp: : FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp: : SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加する必要があります。

- http: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  http:[[/[username@]location]/directory]/filename
- https: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  https:[[/[username@]location]/directory]/filename

（注）　HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

KB ファイルのコピー、名前変更、および削除

KB ファイルのコピー、名前変更、および削除を行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コピーする KB ファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-20-10_00_00   84     10:00:00 CDT Mon Mar 20 2011
```

ステップ 3　KB ファイルを、IP アドレス 10.1.1.1 を持つコンピュータ上のユーザにコピーします。

```
ips-ssp# copy ad-knowledge-base vs0 file 2011-Mar-16-10_00_00
scp://cidsuser@10.1.1.1/AD/my-KB
password: ********
ips-ssp#
```

ステップ 4　KB ファイルの名前を変更します。

```
ips-ssp# rename ad-knowledge-base vs0 2011-Mar-16-10_00_00 My-KB
ips-ssp#
```

ステップ 5　特定の仮想センサーから KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base vs0 2011-Mar-16-10_00_00
ips-ssp#
```

ステップ 6　1 つの仮想センサーから、現在および初期の KB ファイルとしてロードされたファイルを除くすべての KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base vs0
Warning: Executing this command will delete all virtual sensor 'vs0' knowledge bases
except the file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
ips-ssp#
```

ステップ 7　すべての仮想センサーから、現在および初期の KB ファイルとしてロードされたファイルを除くすべての KB ファイルを削除します。

```
ips-ssp# erase ad-knowledge-base
Warning: Executing this command will delete all virtual sensor knowledge bases except the
file loaded as current and the initial knowledge base.
Continue with erase? [yes]: yes
sensor#
```

詳細情報

- **load** コマンドを使用して新しい KB を作成する手順については、「手動による KB の保存およびロード」（P.9-41）を参照してください。
- SSH 既知ホスト リストにホストを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- TLS の信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

2 つの KB 間の違いの表示

特権 EXEC モードで **show ad-knowledge-base** *virtual-sensor* **diff** {**current** | **initial** | **file** *name1*}{**current** | **initial** | **file** *name2*} [*diff-percentage*] コマンドを使用して、2 つの KB 間の違いを表示します。

オプション

次のオプションが適用されます。

- *virtual-sensor*：比較する KB ファイルを含む仮想センサーの名前を指定します。
- *name1*：比較する最初の既存の KB ファイルの名前を指定します。
- *name2*：比較する 2 番目の既存の KB ファイルの名前を指定します。
- **current**：現在ロードされている KB を指定します。
- **initial**：初期 KB を指定します。
- **file**：既存の KB ファイルの名前を指定します。
- *diff-percentage*：（任意）しきい値が指定された割合よりも異なるサービスを表示します。有効な値は 1 ～ 100 です。デフォルトは 10% です。

2 つの KB の比較

2 つの KB を比較するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　比較するファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs0 files
Virtual Sensor vs0
    Filename              Size   Created
    initial               84     04:27:07 CDT Wed Jan 29 2010
*   2011-Jun-28-10_00_01  84     04:27:07 CDT Thu Jun 29 2011
ips-ssp#
```

ステップ 3　現在ロードされているファイル（* が付いたファイル）を仮想センサー vs0 の初期 KB と比較します。

```
ips-ssp# show ad-knowledge-base vs0 diff initial file 2011-Jun-28-10_00_01
Initial Only Services/Protocols
   External Zone
      TCP Services
         Service = 30
         Service = 20
      UDP Services
         None
      Other Protocols
         Protocol = 1
   Illegal Zone
      None
   Internal Zone
      None
2011-Jun-28-10_00_01 Only Services/Protocols
   External Zone
      None
   Illegal Zone
      None
   Internal Zone
      None
Thresholds differ more than 10%
   External Zone
      None
   Illegal Zone
      TCP Services
         Service = 31
         Service = 22
      UDP Services
         None
      Other Protocols
         Protocol = 3
   Internal Zone
      None
ips-ssp#
```

KB のしきい値の表示

特権 EXEC モードで **show ad-knowledge-base** *virtual-sensor* **thresholds** {**current** | **initial** | **file** *name*} [**zone** {**external** | **illegal** | **internal**]} {[**protocol** {**tcp** | **udp**}] [**dst-port** *port*] | [**protocol other**] [**number** *protocol-number*]} コマンドを表示して、KB のしきい値を表示します。

オプション

次のオプションが適用されます。

- *virtual-sensor*：比較する KB ファイルを含む仮想センサーの名前を指定します。
- *name*：既存の KB ファイルの名前を指定します。
- **current**：現在ロードされている KB を指定します。
- **initial**：初期 KB を指定します。
- **file**：既存の KB ファイルの名前を指定します。
- **zone**：（任意）指定されたゾーンのしきい値を表示します。デフォルトでは、すべてのゾーンの情報が表示されます。

- **external**：外部ゾーンのしきい値を表示します。
- **illegal**：不正ゾーンのしきい値を表示します。
- **internal**：内部ゾーンのしきい値を表示します。
- **protocol**：（任意）指定されたプロトコルのしきい値を表示します。デフォルトでは、すべてのプロトコルに関する情報が表示されます。
- **tcp**：TCP プロトコルのしきい値を表示します。
- **udp**：UDP プロトコルのしきい値を表示します。
- **other**：TCP または UDP 以外の他のプロトコルのしきい値を表示します。
- **dst-port**：（任意）指定されたポートのしきい値を表示します。デフォルトでは、すべての TCP ポートまたは UDP ポートに関する情報が表示されます。
- *port*：ポート番号を指定します。有効な値は 0 ～ 65535 です。
- **number**：（任意）指定された他のプロトコル番号のしきい値を表示します。デフォルトでは、他のすべてのプロトコルに関する情報が表示されます。
- *protocol-number*：プロトコル番号を指定します。有効な値は 0 ～ 255 です。

KB しきい値の表示

KB しきい値を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　しきい値を表示するファイルを特定します。

```
ips-ssp# show ad-knowledge-base vs1 files
Virtual Sensor vs1
    Filename               Size   Created
    initial                84     10:24:58 CDT Tue Mar 14 2011
    2011-Mar-16-10_00_00   84     10:00:00 CDT Thu Mar 16 2011
    2011-Mar-17-10_00_00   84     10:00:00 CDT Fri Mar 17 2011
    2011-Mar-18-10_00_00   84     10:00:00 CDT Sat Mar 18 2011
    2011-Mar-19-10_00_00   84     10:00:00 CDT Sun Mar 19 2011
    2011-Mar-27-10_00_00   84     10:00:00 CDT Mon Mar 27 2011
    2011-Apr-24-05_00_00   88     05:00:00 CDT Mon Apr 24 2011
*   2011-Apr-25-05_00_00   88     05:00:00 CDT Tue Apr 25 2011
```

ステップ 3　不正ゾーンに対する特定のファイルに含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds file 2011-Nov-11-10_00_00 zone illegal

   AD Thresholds
      Creation Date = 2011-Nov-11-10_00_00
      KB = 2011-Nov-11-10_00_00
      Illegal Zone
         TCP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
         UDP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
```

```
                  Low = 10
                  Medium = 3
                  High = 1
            Other Services
               Default
                  Scanner Threshold
                     User Configuration = 200
                  Threshold Histogram - User Configuration
                     Low = 10
                     Medium = 3
                     High = 1
ips-ssp#
```

ステップ 4　現在の KB 不正ゾーン、プロトコル TCP、および宛先ポート 20 に含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds current zone illegal protocol tcp dst-port
20

   AD Thresholds
      Creation Date = 2011-Nov-14-10_00_00
      KB = 2011-Nov-14-10_00_00
      Illegal Zone
         TCP Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
ips-ssp#
```

ステップ 5　現在の KB 不正ゾーンと他のプロトコルに含まれるしきい値を表示します。

```
ips-ssp# show ad-knowledge-base vs0 thresholds current zone illegal protocol other

   AD Thresholds
      Creation Date = 2011-Nov-14-10_00_00
      KB = 2011-Nov-14-10_00_00
      Illegal Zone
         Other Services
            Default
               Scanner Threshold
                  User Configuration = 200
               Threshold Histogram - User Configuration
                  Low = 10
                  Medium = 3
                  High = 1
ips-ssp#
```

異常検出の統計情報の表示

特権 EXEC モードで **show statistics anomaly-detection** [*virtual-sensor-name*] コマンドを使用して、異常検出の統計情報を表示します。攻撃が進行中かどうかを確認できます（`Attack in progress` または *`No attack`*）。また、次の KB がいつ保存されるかを確認することもできます（`Next KB rotation at 10:00:00 UTC Wed Apr 26 2011`）。

（注）　**clear** コマンドは、異常検出統計情報には利用できません。

異常検出統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　特定の仮想センサーに対して異常検出統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection vs0
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Wed Apr 26 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

ステップ 3　すべての仮想センサーに対して統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Wed Jun 29 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Wed Jul 29 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

異常検出の無効

一方向のトラフィックだけを検出するようにセンサーを設定している場合は、異常検出をディセーブルにする必要があります。そうしないと、異常検出がワーム スキャナのように、非対称トラフィックを不完全接続と見なし、アラートを起動するので、多数のアラートを受信することになります。

異常検出をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　分析エンジン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)#
```

ステップ 3　ディセーブルにする異常検出ポリシーを含む仮想センサー名を入力します。

```
ips-ssp(config-ana)# virtual-sensor vs0
ips-ssp(config-ana-vir)#
```

ステップ 4　異常検出動作モードをディセーブルにします。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# operational-mode inactive
ips-ssp(config-ana-vir-ano)#
```

ステップ 5　分析エンジン サブモードを終了します。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(config-ana-vir)# exit
ips-ssp(config-ana-)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

ワームがどのように動作するかの詳細については、「ワーム」（P.9-2）を参照してください。

CHAPTER 10

グローバル相関の設定

（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、グローバル相関の設定について説明します。次のような構成になっています。

- 「グローバル相関について」（P.10-1）
- 「SensorBase ネットワークへの参加」（P.10-2）
- 「レピュテーションについて」（P.10-3）
- 「ネットワーク参加について」（P.10-4）
- 「有効性について」（P.10-5）
- 「レピュテーションとリスク レーティング」（P.10-5）
- 「グローバル相関の機能と目的」（P.10-6）
- 「グローバル相関の要件」（P.10-6）
- 「グローバル相関のセンサー ヘルス メトリックについて」（P.10-7）
- 「グローバル相関インスペクションおよびレピュテーション フィルタリングの設定」（P.10-8）
- 「ネットワーク参加の設定」（P.10-11）
- 「グローバル相関のトラブルシューティング」（P.10-13）
- 「グローバル相関のディセーブル化」（P.10-13）

グローバル相関について

センサーが悪意のあるアクティビティのレピュテーションを持つネットワーク デバイスを認識し、それらのアクティビティに対処できるようにグローバル相関を設定できます。シスコの中央脅威データベースである SensorBase ネットワークに IPS デバイスを加えることにより、グローバル相関更新を受信して取り込むことができます。グローバル相関更新に含まれているレピュテーション情報は、ネットワーク トラフィックの分析に組み込まれます。これにより、送信元 IP アドレスのレピュテーションに

基づいてトラフィックが拒否または許可されるため、IPS の有効性が高まります。参加している IPS デバイスは、Cisco SensorBase ネットワークにデータを送り返します。これによってフィードバック ループが発生し、最新かつグローバルな更新が維持されます。

グローバル相関更新またはテレメトリ データ送信に参加するようセンサーを設定することも、これら両方のサービスをオフにすることもできます。イベントでレピュテーション スコアを表示して、攻撃者のレピュテーション スコアを確認できます。レピュテーション フィルタから統計を表示することもできます。

SensorBase ネットワークへの参加

Cisco IPS のセキュリティ機能である Cisco グローバル相関では、シスコが数年にわたって蓄積した膨大なセキュリティ情報が使用されます。Cisco IPS は、Cisco SensorBase ネットワークから脅威に関する更新情報を定期的に受け取ります。これには、連続攻撃者、ボットネット利用者、マルウェアの出現、ダークネットなど、インターネット上の既知の脅威に関する詳細な情報が含まれています。IPS はこの情報を使用して、重要な資産に攻撃が加えられる前に、最悪の攻撃者をフィルタリングして排除します。次に、グローバルな脅威データをシステムに取り込み、悪意あるアクティビティを事前に検知して阻止します。

ユーザが SensorBase ネットワークへの参加に同意すると、シスコはそのユーザの IPS に送信されたトラフィックの集約的統計情報を収集します。これには Cisco IPS ネットワーク トラフィック プロパティの概要データと、このトラフィックが Cisco アプリケーションによってどのように処理されたかが含まれます。シスコがトラフィックのデータ コンテンツ、企業秘密、または個人情報を収集することはありません。すべてのデータは集約され、セキュア HTTP によって Cisco SensorBase ネットワーク サーバへ定期的に送信されます。シスコと共有されるすべてのデータは匿名であり、厳重な機密事項として扱われます。

表 10-1 に、データがどのように利用されるかを示します。

表 10-1　シスコ ネットワーク参加データの利用方法

参加レベル	データのタイプ	目的
Partial	プロトコル属性 (TCP 最大セグメント サイズ、オプション ストリングなど)	潜在的脅威を追跡し、脅威による影響の把握に役立てます
	攻撃のタイプ (シグニチャの起動、リスク レーティングなど)	現在の攻撃および攻撃の重大度を理解するために使用されます
	接続している IP アドレスおよびポート	攻撃元を特定します
	サマリー IPS パフォーマンス (CPU 使用率、メモリ使用率、インライン対 無差別など)	製品の有効性を追跡します
Full	攻撃対象の IP アドレスおよびポート	脅威の動作パターンを検知します

Partial または Full ネットワーク参加をイネーブルにすると、ネットワーク参加の免責条項が表示されます。参加するには yes を入力する必要があります。ライセンスをインストールしていない場合は警告が表示され、センサーがライセンスされない限り、グローバル相関インスペクションとレピュテーション フィルタリングはディセーブルであることが通知されます。ライセンスは http://www.cisco.com/go/licens で取得できます。

詳細情報

センサー ライセンスの取得とインストールの方法については、「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。

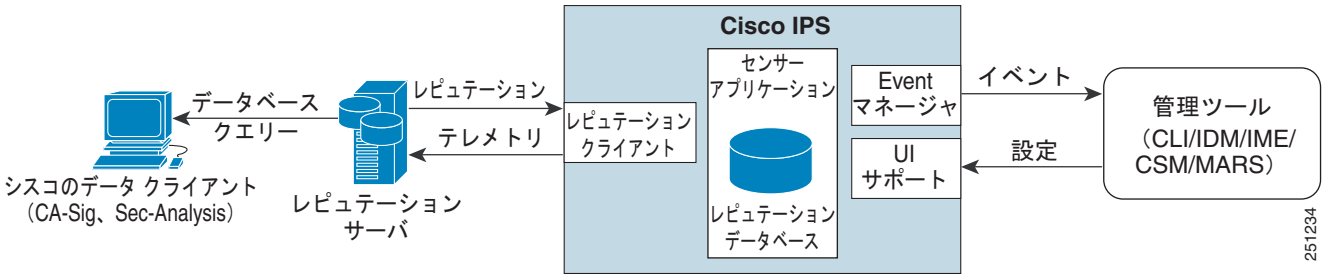
レピュテーションについて

レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに対する評価のことです。これにより、現場にインストールされた IPS センサーは、既存のネットワーク インフラストラクチャを使用して協力することが可能になります。多くの場合、レピュテーションを持つネットワーク デバイスは悪意があるか、感染しています。レピュテーションの情報と統計は CLI で確認できます。

IPS センサーはグローバル相関サーバ（レピュテーション サーバとも呼ばれる）と協力して、センサーの有効性を改善します。

図 10-1 にセンサーとグローバル相関サーバの役割を示します。

図 10-1　　IPS の管理とグローバル相関サーバの対話



グローバル相関サーバは、悪意がある、または感染しているホストとして識別される可能性がある特定の IP アドレスについて、センサーに情報を提供します。センサーはこの情報を使用して、既知のレピュテーションを持つホストから潜在的に有害なトラフィックを受信した場合に実行すべきアクション（ある場合）を判断します。グローバル相関データベースはすばやく変更されるので、センサーは定期的にグローバル相関のアップデートをグローバル相関サーバからダウンロードする必要があります。

注意　センサーがシグニチャまたはグローバル相関のアップデートを適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関アップデートのサイズによって決まります。バイパス モードをオフにすると、インライン センサーはアップデートの適用中にトラフィックの送信を停止します。

詳細情報

グローバル相関統計情報の表示については、「統計情報の表示」（P.17-20）を参照してください。

ネットワーク参加について

ネットワーク参加によって、シスコは世界中のセンサーからほぼリアルタイムでデータを収集できます。カスタマー サイトにインストールされたセンサーは、SensorBase ネットワークにデータを送信できます。これらのデータがグローバル相関データベースに提供されることで、レピュテーションの正確性が向上します。センサーと SensorBase ネットワーク間の通信には、TCP/IP を介した HTTPS 要求および応答が使用されます。ネットワーク参加では、インターネットへのネットワーク接続が必要です。

ネットワーク参加によって次のデータが収集されます。

- シグニチャ ID
- 攻撃者の IP アドレス
- 攻撃者のポート
- 最大セグメント サイズ
- 攻撃対象の IP アドレス
- 攻撃対象のポート
- シグニチャのバージョン
- TCP オプション ストリング
- レピュテーション スコア
- リスク レーティング

ネットワーク参加に関する統計情報には、アラートのヒット数とミス数、レピュテーション アクション、拒否されたパケットのカウンタが示されます。

ネットワーク参加には次の 3 つのモードがあります。

- オフ：ネットワーク参加サーバは、データの収集、統計情報の追跡、または Cisco SensorBase ネットワークへの接続試行は行いません。
- 部分的参加：ネットワーク参加サーバは、データ収集、統計情報の追跡、SensorBase ネットワークとの通信を行います。潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。
- 完全参加：ネットワーク参加サーバは、データ収集、統計情報の追跡、SensorBase ネットワークとの通信を行います。ネットワーク参加データから除外された IP アドレスを除き、収集されたデータはすべて送信されます。

注意　シグニチャ アップデートの場合と同様に、センサーがグローバル相関のアップデートを適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関アップデートのサイズによって決まります。バイパス モードをオフにすると、インライン センサーはアップデートの適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

詳細情報

ネットワーク参加の詳細については、「ネットワーク参加の設定」（P.10-11）を参照してください。

有効性について

参加している IPS クライアントからデータを取得し、それを既知の脅威に関する既存の資料とともに使用すると、IPS の有効性が向上します。有効性は以下に基づいて測定されます。

- 実行可能なイベントの偽陽性（パーセンテージ）
- 実行可能なイベントにはならない脅威の偽陰性（パーセンテージ）
- すべてのイベントのうち実行可能なイベント（パーセンテージ）

このデータを使用して、IPS シグニチャ チームはシグニチャの正確性を高め、IPS エンジニアリング チームはセンサーのさまざまな配置タイプを把握します。

詳細情報

レピュテーションとリスク レーティングの詳細については、「レピュテーションとリスク レーティング」（P.10-5）を参照してください。

レピュテーションとリスク レーティング

リスク レーティングとは、ネットワーク イベントに悪意がある確立に関する概念のことです。ユーザは、ネットワーク上の特定のイベントに関連付けられたリスクについて、定量化された数値を指定できます。デフォルトでは、極端なリスク レーティングを持つアラートがあると、トラフィックがシャットダウンされます。レピュテーションは、既知のアクティビティに基づいて、特定の攻撃者の IP アドレスから悪意のある動作が開始される可能性を示します。アラーム チャネルによってこのレピュテーションに対する特定のスコアが計算され、リスク レーティングに追加されることで、IPS の有効性が向上します。攻撃者のレピュテーション スコアが悪い場合は、差分リスクがリスク レーティングに追加され、攻撃性がさらに高くなります。

アラーム チャネルは、データ パスからのシグニチャ イベントを処理します。アラート処理ユニットは、複数の集約技術、アクション オーバーライド、アクション フィルタ、攻撃者レピュテーション、アクション別のカスタム処理方式を備えています。シスコはレピュテーション参加クライアントからの大量のレピュテーション データを使用して、アラーム チャネルで攻撃者のスコアを計算し、このスコアを使用してリスク レーティングとアラートのアクションを調整します。

詳細情報

- リスク レーティングの詳細については、「リスク レーティングの計算」（P.8-12）を参照してください。
- 脅威レーティングの詳細については、「脅威レーティングについて」（P.8-13）を参照してください。
- イベント アクション フィルタの詳細については、「イベント アクション フィルタの設定」（P.8-20）を参照してください。
- アラーム チャネルの詳細については、「SensorApp について」（P.A-22）を参照してください。
- イベント アクション集約の詳細については、「イベント アクション集約について」（P.8-33）を参照してください。

グローバル相関の機能と目的

グローバル相関には、主として次の 3 つの機能があります。

- グローバル相関インスペクション：攻撃者に対する既知のグローバル相関レピュテーションを使用してアラート処理を調整し、悪いスコアを持つ攻撃者がセンサーで検知された場合にアクションを拒否します。
- レピュテーション フィルタリング：悪意のある既知のサイトからのパケットに対して自動拒否アクションを適用します。
- ネットワーク レピュテーション：センサーがアラートと TCP フィンガープリントを SensorBase ネットワークに送信します。

グローバル相関の目的は次のとおりです。

- アラートをインテリジェントに処理することにより、有効性を高める。
- 悪意のある既知のサイトに対する保護を強化する。
- テレメトリ データを SensorBase ネットワークと共有し、アラートおよびセンサー アクションの可視性をグローバル規模で向上させる。
- 設定を簡素化する。
- 情報のアップロードおよびダウンロードを自動的に処理する。

グローバル相関の要件

グローバル相関には次の要件があります。

- 有効なライセンス

  グローバル相関機能が動作するには、有効なセンサー ライセンスを所有している必要があります。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、アップデートは試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

- ネットワーク参加免責条項への同意
- センサーおよび DNS サーバ用の外部接続

  Cisco IPS のグローバル相関機能では、センサーを Cisco SensorBase ネットワークに接続する必要があります。これらの機能が動作するには、ドメイン名解決も必要となります。DNS クライアントが稼動している HTTP プロキシ サーバを介して接続するようにセンサーを設定するか、またはセンサーの管理インターフェイスにルーティング可能なインターネット アドレスを割り当て、DNS サーバを使用するようにセンサーを設定できます。Cisco IPS では、HTTP プロキシおよび DNS サーバはグローバル相関機能でのみ使用されます。

注意　低速コマンドとコントロール コネクションを使用する環境に配置されたセンサーは、グローバル相関更新を低速でダウンロードします。

- IPv6 アドレスのサポートなし

  グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

- インライン モードのセンサー

  インライン拒否アクションを使用することでグローバル相関機能の有効性を高めることができるよう、センサーはインライン モードで動作する必要があります。

- グローバル相関機能をサポートするセンサー
- グローバル相関機能をサポートする IPS バージョン

詳細情報

- センサー ライセンスの取得とインストールの方法については、「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。
- ネットワーク参加の免責条項については、「SensorBase ネットワークへの参加」（P.10-2）を参照してください。
- グローバル相関をサポートする HTTP プロキシまたは DNS サーバの設定については、「グローバル相関用の DNS サーバとプロキシ サーバの設定」（P.4-10）を参照してください。

グローバル相関のセンサー ヘルス メトリックについて

グローバル相関では、次のメトリックがセンサー ヘルス モニタリングに追加されます。

- 緑色は前回の更新が正しく行われたことを示します。
- 黄色は、過去 1 日（86,400 秒）以内に成功した更新がないことを示します。
- 赤色は、過去 3 日（259,200 秒）以内に成功した更新がないことを示します。

ネットワーク参加では、次のメトリックがセンサー ヘルス モニタリングに追加されます。

- 緑色は前回の接続が正しく行われたことを示します。
- 黄色は、6 回未満の接続が連続して失敗したことを示します。
- 赤色は、6 回を超える接続が連続して失敗したことを示します。

センサーのヘルス統計情報を設定するには、サービス サブモードで **health-monitor** コマンドを使用します。**health-monitor** コマンドの結果を表示するには、**show health** コマンドを使用します。

注意　グローバル相関のヘルス ステータスは、デフォルトで赤に設定され、グローバル相関が正しくアップデートされると緑に変わります。グローバル相関の正常なアップデートには、DNS サーバまたは HTTP プロキシ サーバが必要です。DNS および HTTP プロキシ サーバ設定機能は IPS 7.0(1)E3 以降に装備されているため、6.*x* から 7.0(1)E3 以上にアップグレードした場合は未設定になっています。その結果、センサーに DNS または HTTP プロキシ サーバが設定されるまで、グローバル相関ヘルスおよび全体センサー ヘルス ステータスは赤になっています。DNS または HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合、グローバル相関をディセーブルにし、グローバル相関ヘルス ステータスを除外するようにセンサー ヘルス ステータスを設定すると、赤色のグローバル相関ヘルスおよび全体センサー ヘルス ステータスに対処できます。

詳細情報

- センサー ヘルス メトリックの詳細およびグローバル相関ヘルス ステータスをイネーブルまたはディセーブルにする方法については、「ヘルス ステータス情報の設定」（P.17-5）を参照してください。
- センサー ヘルス メトリックの表示手順については、「センサーの全体的なヘルス ステータスの表示」（P.17-10）を参照してください。
- グローバル相関をサポートする HTTP プロキシまたは DNS サーバの設定については、「グローバル相関用の DNS サーバとプロキシ サーバの設定」（P.4-10）を参照してください。
- グローバル相関をディセーブルにする手順については、「グローバル相関インスペクションおよびレピュテーション フィルタリングの設定」（P.10-9）を参照してください。

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定

ここでは、グローバル相関インスペクションとレピュテーション フィルタリング、およびそれらの設定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。

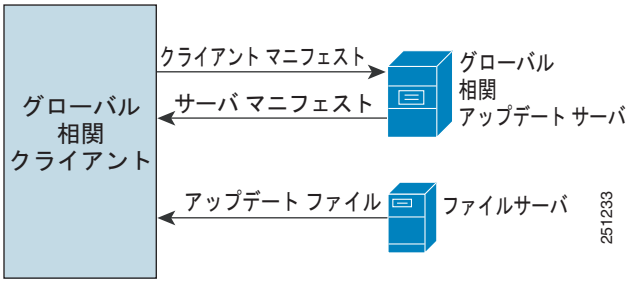
- 「グローバル相関インスペクションおよびレピュテーション フィルタリングについて」（P.10-8）
- 「グローバル相関インスペクションおよびレピュテーション フィルタリングの設定」（P.10-9）

グローバル相関インスペクションおよびレピュテーション フィルタリングについて

ユーザは、SensorBase ネットワークからのアップデートを使用してリスク レーティングを調整できるよう、センサーを設定することができます。クライアントはグローバル相関更新サーバおよびファイル サーバと通信することで、使用可能なアップデートとセンサーに適用可能なアップデートを判断します。グローバル相関更新サーバは、センサーにサーバ マニフェスト ドキュメントを提供します。このドキュメントには、使用可能なアップデート、およびファイル サーバからそれらを取得する方法が指定されています。センサーは、サーバ マニフェストの情報を使用して、ファイル サーバからアップデート ファイルをダウンロードします。

図 10-2 に、グローバル相関アップデート クライアントがファイルを取得する方法を示します。

図 10-2　グローバル相関アップデート クライアント



注意　グローバル相関機能が動作するには、有効なセンサー ライセンスを所有している必要があります。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、アップデートは試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

グローバル相関を設定すると、定期的な間隔で自動アップデートが実行されます。デフォルトの間隔は約 5 分ですが、この間隔はグローバル相関サーバで変更できます。センサーは完全なアップデートを取得した後、定期的に差分アップデートを適用します。

HTTP プロキシまたは DNS サーバの設定は、サービス ネットワーク設定サブモードで行います。グローバル相関をオンにしている場合は、悪意のあるホストに対してどれだけ積極的に拒否アクションを実施するかを選択できます。次に、悪意のある既知のホストへのアクセスを拒否するために、レピュテーション フィルタリングをイネーブルにします。発生する可能性があった内容に関するレポートだけが必要な場合は、test-global-correlation をイネーブルにします。これにより、センサーは監査モードに設定され、センサーが実行したと想定されるアクションがイベント内に生成されます。

特権 EXEC モードで **show health** コマンドを使用して、センサーの全体的なヘルス ステータス情報を表示します。ヘルス ステータス カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

注意　シグニチャ アップデートの場合と同様に、センサーがグローバル相関のアップデートを適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関アップデートのサイズによって決まります。バイパス モードをオフにすると、インライン センサーはアップデートの適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

詳細情報

- グローバル相関機能の設定手順については、「グローバル相関インスペクションおよびレピュテーション フィルタリングの設定」（P.10-9）を参照してください。
- センサー ヘルス メトリックの表示手順については、「センサーの全体的なヘルス ステータスの表示」（P.17-10）を参照してください。
- CollaborationApp の詳細については、「CollaborationApp」（P.A-27）を参照してください。

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定

グローバル相関が動作するには、DNS サーバまたは HTTP プロキシ サーバが常時設定されている必要があります。

オプション

次のオプションが適用されます。

- **global-correlation-inspection {off | on}**：グローバル相関インスペクションのオン / オフを切り替えます。オンの場合、センサーは、SensorBase ネットワークからの更新を使用して、リスク レーティングを調整します。デフォルトは on です。
- **global-correlation-inspection-influence {permissive | standard | aggressive}**：グローバル相関インスペクションのレベルを選択できます。デフォルトは standard です。
  - **permissive**：トラフィック拒否の決定にグローバル相関データはほとんど影響しません。
  - **standard**：グローバル相関は、トラフィック拒否の決定に一定の影響を与えます。
  - **aggressive**：グローバル相関データは、トラフィック拒否の決定に大きく影響します。
- **reputation-filtering {on | off}**：レピュテーション フィルタリングのオン / オフを切り替えます。オンの場合、センサーは、グローバル相関データベースにリストされている悪意のあるホストへのアクセスを拒否します。デフォルトは on です。
- **test-global-correlation {on | off}**：グローバル相関の影響を受けた拒否アクションのレポートをイネーブルにします。実際にホストを拒否しなくても、グローバル相関機能をテストすることができます。デフォルトは off です。

グローバル相関の設定

グローバル相関機能を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル相関サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service global-correlation
ips-ssp(config-glo)#
```

ステップ 3　グローバル相関インスペクションをオンにします。

```
ips-ssp(config-glo)# global-correlation-inspection on
ips-ssp(config-glo)#
```

ステップ 4　グローバル相関インスペクションのレベルを指定します。

```
ips-ssp(config-glo)# global-correlation-inspection-influence aggressive
ips-ssp(config-glo)#
```

ステップ 5　レピュテーション フィルタリングをオンにします。

```
ips-ssp(config-glo)# reputation-filtering on
ips-ssp(config-glo)#
```

ステップ 6　グローバル相関データをテストします。ただし、実際にはトラフィックを拒否しません。

```
ips-ssp(config-glo)# test-global-correlation on
ips-ssp(config-glo)#
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-glo)# show settings
   global-correlation-inspection: on default: on
   global-correlation-inspection-influence: aggressive default: standard
   reputation-filtering: on default: on
   test-global-correlation: on default: off
ips-ssp(config-glo)#
```

ステップ 8　グローバル相関サブモードを終了します。

```
ips-ssp(config-glo)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- グローバル相関をサポートするプロキシまたは DNS サーバの設定については、「グローバル相関用の DNS サーバとプロキシ サーバの設定」（P.4-10）を参照してください。
- センサー ライセンスの取得とインストールの方法については、「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。
- センサー ヘルス メトリックの詳細については、「センサーの全体的なヘルス ステータスの表示」（P.17-10）を参照してください。

ネットワーク参加の設定

ユーザは、SensorBase ネットワークにデータを送信するようにセンサーを設定できます。センサーが完全に参加して、すべてのデータを SensorBase ネットワークに送信するように設定することができます。あるいは、データは収集するが、潜在的に機密性の高いデータ（トリガー パケットの宛先 IP アドレスなど）は除外するようにセンサーを設定することもできます。

（注）　センサーを部分的ネットワーク参加用に設定すると、第三者がグローバル相関データベースから内部ネットワークに関する調査情報を抽出するときに制限が課されます。

オプション

次のオプションが適用されます。

- **network-participation**：ネットワーク参加のレベルを設定します。デフォルトは off です。
  - **off**：SensorBase ネットワークにデータは提供されません。
  - **partial**：データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除外されます。
  - **full**：すべてのデータが SensorBase ネットワークに提供されます。

    （注）　ネットワーク参加をオンにするには、ネットワーク参加の免責条項に同意する必要があります。

ネットワーク参加の開始

ネットワーク参加をオンにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル相関サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service global-correlation
ips-ssp(config-glo)#
```

ステップ 3　ネットワーク参加をオンにします。

```
ips-ssp(config-glo)# network-participation [full | partial]
ips-ssp(config-glo)# exit
```

ステップ 4　**yes** を入力して SensorBase ネットワークへの参加に同意します。

```
If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS
network traffic properties and how this traffic was handled by the Cisco appliances. We do
not collect the data content of traffic or other sensitive business or personal
information. All data is aggregated and sent via secure HTTP to the Cisco SensorBase
Network servers in periodic intervals. All data shared with Cisco will be anonymous and
treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-glo)# show settings
   network-participation: full default: off
   global-correlation-inspection: on default: on
   global-correlation-inspection-influence: aggressive default: standard
   reputation-filtering: on default: on
   test-global-correlation: on default: off
ips-ssp(config-glo)#
```

ステップ 6　グローバル相関サブモードを終了します。

```
ips-ssp(config-glo)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

SensorBase ネットワークへの参加の詳細については、「SensorBase ネットワークへの参加」（P.10-2）を参照してください。

グローバル相関のトラブルシューティング

グローバル相関を設定する場合は、以下が順守されていることを確認してください。

- グローバル相関の更新はセンサー管理インターフェイスを介して行われるので、ファイアウォールでポート 443/80 トラフィックが許可されている必要があります。
- グローバル相関機能が動作するには、HTTP プロキシ サーバまたは DNS サーバが設定されていなければなりません。
- グローバル相関機能が動作するには有効な IPS ライセンスが必要です。
- グローバル相関機能には外部 IP アドレスのみが含まれるため、センサーを社内ラボに配置するとグローバル相関情報を受信できません。
- お使いのセンサーがグローバル相関機能をサポートしていることを確認してください。
- お使いの IPS バージョンがグローバル相関機能をサポートしていることを確認してください。

詳細情報

- DNS または HTTP プロキシ サーバの設定手順については、「グローバル相関用の DNS サーバとプロキシ サーバの設定」（P.4-10）を参照してください。
- IPS ライセンスの取得手順については、「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。

グローバル相関のディセーブル化

DNS サーバまたは HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合は、グローバル相関をディセーブルにすると、全体センサー ヘルス内で、グローバル相関ヘルスが問題を通知する赤色で表示されなくなります。グローバル相関ステータスを除外するようセンサー ヘルスを設定することもできます。

オプション

次のオプションが適用されます。

- **global-correlation-inspection {off | on}**：グローバル相関インスペクションのオン / オフを切り替えます。オンの場合、センサーは、SensorBase ネットワークからの更新を使用して、リスク レーティングを調整します。デフォルトは on です。
- **reputation-filtering {on | off}**：レピュテーション フィルタリングのオン / オフを切り替えます。オンの場合、センサーは、グローバル相関データベースにリストされている悪意のあるホストへのアクセスを拒否します。デフォルトは on です。
- **network-participation**：ネットワーク参加のレベルを設定します。デフォルトは off です。
  - **off**：SensorBase ネットワークにデータは提供されません。
  - **partial**：データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除外されます。
  - **full**：すべてのデータが SensorBase ネットワークに提供されます。

グローバル相関のディセーブル化

グローバル相関をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル相関サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service global-correlation
ips-ssp(config-glo)#
```

ステップ 3　グローバル相関インスペクションをオフにします。

```
ips-ssp(config-glo)# global-correlation-inspection off
ips-ssp(config-glo)#
```

ステップ 4　レピュテーション フィルタリングをオフにします。

```
ips-ssp(config-glo)# reputation-filtering off
ips-ssp(config-glo)#
```

ステップ 5　ネットワーク参加をオフにします。

```
ips-ssp(config-glo)# network-participation off
ips-ssp(config-glo)# exit
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-glo)# show settings
   network-participation: full default: off
   global-correlation-inspection: on default: off
   reputation-filtering: on default: off
ips-ssp(config-glo)#
```

ステップ 7　グローバル相関サブモードを終了します。

```
ips-ssp(config-glo)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

CHAPTER 11

外部製品インターフェイスの設定

（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、外部製品インターフェイスの設定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。

- 「外部製品インターフェイスについて」（P.11-1）
- 「CSA MC について」（P.11-2）
- 「外部製品インターフェイスの問題」（P.11-3）
- 「IPS インターフェイスをサポートする CSA MC の設定」（P.11-4）
- 「外部製品インターフェイスとポスチャ ACL の追加」（P.11-5）
- 「外部製品インターフェイスのトラブルシューティング」（P.11-9）

外部製品インターフェイスについて

外部製品インターフェイスは、外部のセキュリティおよび管理製品から情報を受信して処理するように設計されています。これらの外部セキュリティおよび管理製品は、センサー設定情報を自動的に拡張するために使用できる情報を収集します。たとえば、外部製品から受信できる情報のタイプには、ホストのプロファイル（ホスト OS の設定、アプリケーションの設定、セキュリティ ポスチャ）や、悪意のあるネットワーク アクティビティの原因と特定された IP アドレスなどがあります。

（注） Cisco IPS では、CSA MC だけにインターフェイスを追加できます。

CSA MC について

CSA MC は、ネットワーク ホストにセキュリティ ポリシーを適用します。これには 2 つのコンポーネントがあります。

- ネットワーク ホスト上に存在し、そのホストを保護するエージェント。
- Management Console（MC）：エージェントを管理するアプリケーション。セキュリティ ポリシーの更新をエージェントにダウンロードし、エージェントから操作情報をアップロードします。

CSA MC は、管理対象の CSA エージェントからホスト ポスチャ情報を受信します。また、ネットワークからの隔離が必要と判断された IP アドレスのウォッチ リストを保守します。CSA MC は、ホスト ポスチャ イベントと隔離 IP アドレス イベントの 2 種類のイベントをセンサーに送信します。

ホスト ポスチャ イベント（IPS ではインポートされた OS 識別と呼ばれる）には次の情報が含まれます。

- CSA MC によって割り当てられた一意のホスト ID
- CSA エージェント ステータス
- ホスト システムのホスト名
- ホスト上でイネーブルになっている IP アドレスのセット
- CSA ソフトウェア バージョン
- CSA ポーリング ステータス
- CSA テスト モード ステータス
- NAC ポスチャ

たとえば、OS 固有のシグニチャが起動され、ターゲットがその OS を実行している場合、攻撃の関連性が高いため、対応の重要度は大きくなります。ターゲット OS が異なる場合、攻撃の関連性は低く、対応はそれほど重要でない場合があります。シグニチャ攻撃関連性レーティングは、このホストに合わせて調整されます。

隔離ホスト イベント（IPS ではウォッチ リストと呼ばれる）には、次の情報が含まれます。

- IP アドレス
- 隔離の理由
- ルール違反に関連付けられたプロトコル（TCP、UDP、または ICMP）
- ルールベースの違反が、確立されたセッションまたは UDP パケットのいずれに関連付けられているかを示すインジケータ。

たとえば、ホストのいずれかが攻撃者としてリストされているシグニチャが起動された場合、非常に深刻な事態が予想されます。このホストには、リスク レーティングが加算されます。加算の度合いは、ホストが隔離された原因によって異なります。

センサーはこれらのイベントからの情報を使用して、イベント内の情報と、ホスト ポスチャおよび隔離 IP アドレスのリスク レーティングの設定に基づき、リスク レーティングの加算値を決定します。

（注） ホスト ポスチャおよびウォッチ リスト IP アドレス情報は、仮想センサーには関連付けらず、グローバル情報として扱われます。

CSA MC と IPS センサー間の通信は、SSL/TLS によってセキュアな状態で維持されます。センサーは、CSA MC との SSL/TLS 通信を開始します。この通信は相互に認証されます。CSA MC は、X.509 証明書を提出して認証を行います。センサーは、ユーザ名 / パスワード認証を使用します。

（注）　イネーブルにできる CSA MC インターフェイスは 2 つだけです。

注意　センサーとの通信ができるよう、CSA MC は信頼できるホストとして追加する必要があります。

詳細情報

信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

外部製品インターフェイスの問題

外部製品インターフェイスがホスト ポスチャと隔離イベントを受信した場合、次のような問題が生じる可能性があります。

- センサーは、一定数のホスト レコードしか保存できません。
  - レコード数が 10,000 を超えると、後続のレコードはドロップされます。
  - レコードが 10,000 の制限値に達し、その後 9900 を下回ると新しいレコードはドロップされなくなります。
- ホストが IP アドレスを変更できる、あるいは別のホストの IP アドレスを使用しているように見えます（DHCP リースの期限満了やワイヤレス ネットワーク内での移動などによる）。

  IP アドレスが競合すると、センサーは最新のホスト ポスチャ イベントを最も正確なものと見なします。
- ネットワークでは、異なる VLAN に重複する IP アドレス範囲を含めることができるが、ホスト ポスチャには VLAN ID 情報を加えることはできません。

  指定されたアドレス範囲を無視するように、センサーを設定できます。
- ホストがファイアウォールの背後にあるため、CSA MC がホストに到達できません。

  到達不能ホストは除外できます。
- CSA MC イベント サーバでは、デフォルトで最大 10 個のサブスクリプションを開くことができます。この値は変更できます。

  サブスクリプションを開くには、管理アカウントとパスワードが必要です。
- CSA データが仮想化されず、センサーでグローバルに処理されます。
- ホスト ポスチャ OS と IP アドレスがパッシブ OS フィンガープリント ストレージに統合されます。これらはインポートされた OS プロファイルとして表示できます。
- 隔離されたホストを表示できません。
- センサーが各 CSA MC ホストの X.509 証明書を認識しなければなりません。これらを信頼できるホストとして追加する必要があります。
- 最大 2 台の外部製品デバイスを設定できます。

詳細情報

- OS マップおよび識別情報の使用の詳細については、「設定された OS マップの追加、編集、削除、および移動」（P.8-28）および「OS ID の表示とクリア」（P.8-32）を参照してください。
- 信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

IPS インターフェイスをサポートする CSA MC の設定

（注）　ホスト ポスチャ イベントと隔離 IP アドレス イベントの詳細については、『*Using Management Center for Cisco Security Agents 5.1*』を参照してください。

ホスト ポスチャ イベントと隔離 IP アドレス イベントがセンサーに送信されるよう、CSA MC を設定する必要があります。

IPS インターフェイスをサポートする CSA MC を設定するには、次の手順を実行します。

ステップ 1　[Events] > [Status SummaryChoose] を選択します。

ステップ 2　[Network Status] セクションで、[Host history collection enabled] の横にある [No] をクリックし、ポップアップ ウィンドウで [Enable] をクリックします。

（注）　システムのホスト履歴収集がグローバルにイネーブル化されます。この機能をオンにすると MC ログ ファイルがすぐにいっぱいになる可能性があるので、デフォルトではディセーブルになっています。

ステップ 3　[Systems] > [Groups] を選択し、次に作成する管理者アカウントと一緒に使用する新しいグループ（ホストなし）を作成します。

ステップ 4　[Maintenance] > [Administrators] > [Account Management] を選択し、IPS が MC システムにアクセスするための新しい CSA MC 管理者アカウントを作成します。

ステップ 5　**モニタ**のロールを持つ新しい管理者アカウントを作成します。

この新しいアカウントには設定特権が許可されていないので、MC のセキュリティを維持することができます。

この管理者アカウントのユーザ名とパスワードを覚えておいてください。センサーで外部製品インターフェイスを設定するとき必要になります。

ステップ 6　[Maintenance] > [Administrators] > [Access Control] を選択し、この管理者アカウントに制限を追加します。

ステップ 7　[Access Control] ウィンドウで、作成した管理者を選択し、作成したグループを選択します。

（注）　この設定を保存すると、この新しい管理者アカウントの MS アクセスがさらに制限され、CSA MC のセキュリティを維持することができます。

外部製品インターフェイスとポスチャ ACL の追加

注意 Cisco IPS で追加できる外部製品インターフェイスは CSA MC インターフェイスだけです。Cisco IPS は 2 つの CSA MC インターフェイスをサポートしています。

サービス外部製品インターフェイス サブモードで **cisco-security-agents-mc-settings** *ip-address* を使用して、CSA MC を外部製品インターフェイスとして追加します。

オプション

次のオプションが適用されます。

- **enabled {yes | no}**：CSA MC からの情報の受信をイネーブルまたはディセーブルにします。
- **host-posture-settings**：CSA MC から受信したホスト ポスチャの処理方法を指定します。
  - **allow-unreachable-postures {yes | no}**：CSA MC から到達不能なホストのポスチャを許可します。

    CSA MC がホスト ポスチャ内のどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IPS が IP アドレスを認識できない場合、あるいはネットワーク上で IP アドレスが重複している場合に、そのポスチャをフィルタリングするのに役立ちます。このフィルタは、CSA MC だけでなく IPS からもホストに到達できないネットワーク トポロジに最適です。たとえば、IPS と CSA MC が同じネットワーク セグメントにある場合などです。
  - **enabled** {**yes** | **no**}：CSA MC からのホスト ポスチャの受信をイネーブルまたはディセーブルにします。
  - **posture-acls** {**edit** | **insert** | **move**} **name1 {begin | end | inactive | before | after}**：許可または拒否されたポスチャ アドレスのリスト。

    このコマンドを使用すると、IPS が IP アドレスを認識できない場合、あるいはネットワーク上で IP アドレスが重複している場合に、そのポスチャをフィルタリングすることができます。
  - **action {permit | deny}**：指定されたネットワーク アドレスと一致するポスチャを許可または拒否します。
  - **network-address** *address*：許可または拒否するポスチャのネットワーク アドレスを x.x.x.x/nn 形式で指定します。
- **password**：CSA MC へのログインに使用するパスワード。
- **port**：CSA MC に接続するための TCP ポート。有効な範囲は 1 ～ 65535 です。デフォルトは 443 です。
- **username**：CSA MC へのログインに使用するユーザ名。
- **watchlist-address-settings**：CSA MC から受信したウォッチ リストのアドレスの処理方法を指定します。
  - **enabled {yes | no}**：CSA MC からのウォッチ リスト アドレスの受信をイネーブルまたはディセーブルにします。
  - **manual-rr-increase**：攻撃者が CSA MC によって手動でウォッチ リストに記載されたためにイベント RR に加算される数値。有効な範囲は 0 ～ 35 です。デフォルトは 25 です。
  - **packet-rr-increase**：セッションレス パケットベースのポリシー違反を理由に攻撃者が CSA MC によってウォッチ リストに記載されたため、イベント リスク レーティングに加算される数値。有効な範囲は 0 ～ 35 です。デフォルトは 10 です。

– **session-rr-increase**：セッションベースのポリシー違反を理由に攻撃者が CSA MC によってウォッチ リストに記載されたため、イベント リスク レーティングに加算される数値。有効な範囲は 0 ～ 35 です。デフォルトは 25 です。

外部製品インターフェイスの追加

外部製品を追加する場合は、センサーとの通信ができるよう、必ず信頼できるホストとして追加してください。

外部製品インターフェイスを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　外部製品インターフェイス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service external-product-interface
```

ステップ 3　CSA MC インターフェイスを追加します。

```
ips-ssp(config-ext)# cisco-security-agents-mc-settings 209.165.200.225

ips-ssp(config-ext-cis)#
```

ステップ 4　CSA MC からの情報の受信をイネーブルにします。

```
ips-ssp(config-ext-cis)# enabled yes
```

ステップ 5　デフォルト ポートの設定を変更します。

```
ips-ssp(config-ext-cis)# port 80
```

ステップ 6　ログインの設定を変更します。

a. ユーザ名を入力します。

```
ips-ssp(config-ext-cis)# username jsmith
```

b. パスワードを入力して確認します。

```
ips-ssp(config-ext-cis)# password
Enter password[]: *******
Re-enter password: *******
ips-ssp(config-ext-cis)#
```

（注）　手順 7 ～ 10 は省略できます。手順 7 ～ 10 を実行しない場合、フィルタは適用されず、すべての CSA MC 情報はデフォルト値を使用して受信されます。

ステップ 7　（任意）ウォッチ リストの設定を構成します。

a. ウォッチ リスト情報を外部製品からセンサーに渡せるようにします。

```
ips-ssp(config-ext-cis-wat)# enabled yes
```

（注）　ウォッチ リストをイネーブルにしていない場合、CSA MC から受信したウォッチ リスト情報は削除されます。

b. 手動ウォッチ リスト RR の比率をデフォルトの 25 から変更します。

```
ips-ssp(config-ext-cis-wat)# manual-rr-increase 30
```

c. セッションベースのウォッチ リスト RR の比率をデフォルトの 25 から変更します。

```
ips-ssp(config-ext-cis-wat)# session-rr-increase 30
```

d. パケットベースのウォッチ リスト RR の比率をデフォルトの 10 から変更します。

```
ips-ssp(config-ext-cis-wat)# packet-rr-increase 20
```

ステップ 8　（任意）ホスト ポスチャ情報を外部製品からセンサーに渡せるようにします。

```
ips-ssp(config-ext-cis)# host-posture-settings
ips-ssp(config-ext-cis-hos)# enabled yes
```

（注）　ホスト ポスチャ情報をイネーブルにしていない場合、CSA MC から受信したホスト ポスチャ情報は削除されます。

ステップ 9　（任意）到達不能ホストからのホスト ポスチャ情報を、外部製品からセンサーに渡せるようにします。

```
ips-ssp(config-ext-cis-hos)# allow-unreachable-postures yes
```

（注）　CSA MC がホスト ポスチャ内のどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IPS が IP アドレスを認識できない場合、あるいはネットワーク上で IP アドレスが重複している場合に、そのポスチャをフィルタリングするのに役立ちます。このフィルタは、CSA MC だけでなく IPS からもホストに到達できないネットワーク トポロジに最適です。たとえば、IPS と CSA MC が同じネットワーク セグメントにある場合などです。

ステップ 10　ポスチャ ACL を設定します。

a. ポスチャ ACL を ACL リストに追加します。

```
ips-ssp(config-ext-cis-hos)# posture-acls insert name1 begin
ips-ssp(config-ext-cis-hos-pos)#
```

（注）　ポスチャ ACL とはネットワーク アドレスの範囲のことで、この範囲に対してホスト ポスチャが許可または拒否されます。IPS が IP アドレスを認識できない場合、または IP アドレスがネットワーク上で重複している場合、ポスチャ ACL を使用してそのポスチャをフィルタリングします。

b. ポスチャ ACL が使用するネットワーク アドレスを入力します。

```
ips-ssp(config-ext-cis-hos-pos)# network-address 192.0.2.0/24
```

c. ポスチャ ACL が実行するアクション（拒否または許可）を選択します。

```
ips-ssp(config-ext-cis-hos-pos)# action permit
```

ステップ 11　設定を確認できます。

```
ips-ssp(config-ext-cis-hos-pos)# exit
ips-ssp(config-ext-cis-hos)# exit
ips-ssp(config-ext-cis)# exit
ips-ssp(config-ext)# show settings
   cisco-security-agents-mc-settings (min: 0, max: 2, current: 1)
   -----------------------------------------------
      ip-address: 209.165.200.225
      -----------------------------------------------
         interface-type: extended-sdee <protected>
```

```
            enabled: yes default: yes
            url: /csamc50/sdee-server <protected>
            port: 80 default: 443
            use-ssl
            ------------------------------------------------
               always-yes: yes <protected>
            ------------------------------------------------
            username: jsmith
            password: <hidden>
            host-posture-settings
            ------------------------------------------------
               enabled: yes default: yes
               allow-unreachable-postures: yes default: yes
               posture-acls (ordered min: 0, max: 10, current: 1 - 1 active, 0 inactive)
               ---------------------------------------------
               ACTIVE list-contents
               ---------------------------------------------
                  NAME: name1
                  ------------------------------------------
                     network-address: 192.0.2.0/24
                     action: permit
                  ------------------------------------------
                  ------------------------------------------
               ---------------------------------------------
            ------------------------------------------------
            watchlist-address-settings
            ------------------------------------------------
               enabled: yes default: yes
               manual-rr-increase: 30 default: 25
               session-rr-increase: 30 default: 25
               packet-rr-increase: 20 default: 10
            ------------------------------------------------
         ---------------------------------------------
      ------------------------------------------
ips-ssp(config-ext)#
```

ステップ 12　外部製品インターフェイス サブモードを終了します。

```
ips-ssp(config-ext)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

外部製品インターフェイスのトラブルシューティング

外部製品インターフェイスのトラブルシューティングを行う場合は、次の点を確認します。

- インターフェイスがアクティブかどうかを確認するには、CLI で **show statistics external-product-interface** コマンドの出力を確認します。または、IDM で [Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答のインターフェイス状態の行を確認します。あるいは、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答のインターフェイス状態の行を確認します。
- CSA MC の IP アドレスが信頼できるホストに追加されていることを確認してください。追加していない場合は追加し、数分待ってから再度確認します。
- ブラウザを使用して CSA MC でサブスクリプションを開いてから閉じ、サブスクリプション ログイン情報を確認します。
- イベント ストアで CSA MC サブスクリプション エラーがないか確認します。

詳細情報

- 信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。
- イベントの表示手順については、「イベント ストアからのイベントのクリア」（P.8-42）を参照してください。

CHAPTER 12

IP ロギングの設定

（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、センサーで IP ロギングを設定する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。

- 「IP ロギングについて」（P.12-1）
- 「自動 IP ロギングの設定」（P.12-2）
- 「特定の IP アドレスに対する手動 IP ロギングの設定」（P.12-4）
- 「IP ログの内容の表示」（P.12-5）
- 「動作している IP ログの停止」（P.12-6）
- 「表示する IP ログ ファイルのコピー」（P.12-8）

IP ロギングについて

IP アドレスで指定したホストに関連するすべての IP トラフィックをキャプチャするように、手動でセンサーを設定できます。IP トラフィックをログに記録する期間、および記録するパケット数とバイト数を指定できます。指定したパラメータが 1 つでも該当した時点で、センサーは IP トラフィックのロギングを停止します。

また、特定のシグニチャが起動するたびに IP パケットを記録するように、センサーを設定することもできます。センサーが IP トラフィックをログに記録する期間、および記録するパケット数とバイト数を指定できます。

注意 IP ロギングをイネーブルにすると、システム パフォーマンスは低下します。

（注）　IP ログ ファイルを削除したり管理することはできません。**no iplog** コマンドでは、IP ログは削除されません。その IP ログへのパケットの記録が停止されるだけです。IP ログは循環バッファに格納されます。古い IP ログは新しい IP ログによって上書きされるので、循環バッファがいっぱいになることはありません。

センサーから IP ログをコピーし、libpcap 形式のパケット ファイルを読み取りできる Wireshark や TCPDUMP などのツールでそれらのログを解析できます。

（注）　各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

自動 IP ロギングの設定

ip-log-packets *number*、**ip-log-time** *number*、および **ip-log-bytes** *number* コマンドを使用して、センサーに自動 IP ロギング パラメータを設定します。

オプション

次のオプションが適用されます。

- **ip-log-packets**：ログに記録するパケットの数を指定します。有効な値は 0 ～ 65535 です。デフォルトは 0 です。
- **ip-log-time**：センサーでパケットを記録する期間を指定します。有効な値は 0 ～ 65535 分です。デフォルトは 30 分です。
- **ip-log-bytes**：ログに記録する最大バイト数を指定します。有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。
- **default**：パラメータをリセットします。

（注）　自動 IP ログは、これらいずれかのパラメータに達するまでパケットのキャプチャを継続します。

自動 IP ロギングはシグニチャ単位で、またはイベント アクション オーバーライドとして設定されます。自動 IP ロギングをトリガーするアクションは次のとおりです。

- log-attacker-packets
- log-victim-packets
- log-pair-packets

自動 IP ロギングの設定

自動 IP ロギング パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　シグニチャ定義 IP ログ コンフィギュレーション サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)# ip-log
```

ステップ 3　センサーがログに記録するパケットの数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-packets 200
```

ステップ 4　センサーがパケットを記録する期間を指定します。

```
ips-ssp(config-sig-ip)# ip-log-time 60
```

ステップ 5　記録するバイト数を指定します。

```
ips-ssp(config-sig-ip)# ip-log-bytes 5024
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 200 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 5024 default: 0
   -----------------------------------------------
ips-ssp(config-sig-ip)#
```

ステップ 7　IP ロギング サブモードを終了します。

```
ips-ssp(config-sig-ip)# exit
ips-ssp(config-sig)# exit
Apply Changes?:[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- IP ログ ファイルをコピーおよび表示するには、「表示する IP ログ ファイルのコピー」（P.12-8）を参照してください。
- イベント アクションの詳細については、「シグニチャへのアクションの割り当て」（P.7-16）および「イベント アクション オーバーライドの設定」（P.8-16）を参照してください。

特定の IP アドレスに対する手動 IP ロギングの設定

iplog *name ip_address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*] コマンドを使用して、仮想センサーで特定の IP アドレスの IP パケットを手動で記録します。

オプション

次のオプションが適用されます。

- *name*：ロギングを開始および終了する仮想センサーを指定します。
- *ip_address*：指定された送信元 IP アドレスまたは宛て先 IP アドレス（あるいはその両方）が含まれたパケットをログに記録します。
- *minutes*：ロギングが動作する期間を指定します。有効な範囲は 1 ～ 60 分です。デフォルトは 10 分です。
- *numPackets*：記録するパケットの最大数を指定します。有効な範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。
- *numBytes*：記録する最大バイト数を指定します。有効な範囲は 0 ～ 4294967295 です。0 の値はバイト数が無制限であることを示します。

（注） *minutes*、n*umPackets*、*numBytes* パラメータは省略可能です。3 つすべてを指定する必要はありません。しかし、複数のパラメータを指定した場合、センサーは最初のしきい値に到達するまでロギングを続行します。たとえば、時間を 5 分に設定し、パケット数を 1000 に設定すると、センサーは 1000 番目のパケットがキャプチャされると、2 分しか経過していなくてもロギングを停止します。

手動 IP ロギングの設定

仮想センサーで特定の IP アドレスのパケットを手動で記録するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　特定の IP アドレスに対する IP ロギングを開始します。

```
ips-ssp# iplog vs0 192.0.2.1 duration 5
Logging started for virtual sensor vs0, IP address 192.0.2.1, Log ID 1
Warning: IP Logging will affect system performance.
ips-ssp#
```

この例で、センサーは IP アドレス 192.0.2.1 との間で送受信されるすべての IP パケットを 5 分間ログに記録しています。

（注） 後で参照するときのために、ログ ID はメモしておいてください。

ステップ 3　**iplog-status** コマンドを使用して IP ログのステータスをモニタします。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

（注）　各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

詳細情報

- 特定の IP アドレスに関する IP パケットのロギングを停止するには、「動作している IP ログの停止」（P.12-6）を参照してください。
- IP パケットをシグニチャに関連付けられたイベントとしてログに記録するには、「自動 IP ロギングの設定」（P.12-2）を参照してください。
- IP ログ ファイルをコピーおよび表示するには、「表示する IP ログ ファイルのコピー」（P.12-8）を参照してください。

IP ログの内容の表示

iplog-status [**log-id** *log_id*] [**brief**] [**reverse**] [| {**begin** *regular_expression* | **exclude** *regular_expression* | **include** *regular_expression* }] コマンドを使用して、使用可能な IP ログの内容を表示します。

ログが作成されると、ステータスは `added` になります。最初のエントリがログに挿入されると、ステータスは `started` に変わります。パケット数の制限に達するなどしてログが完了すると、ステータスは `completed` に変わります。

オプション

次のオプションが適用されます。

- *log_id*：（任意）ステータスを表示したいファイルのログ ID を指定します。
- **brief**：（任意）各ログの IP ログ ステータス情報のサマリーを表示します。
- **reverse**：（任意）リストを逆の日付順で（最新のログから順に）表示します。
- |：（任意）この後に出力処理の指定が続くことを示します。
- *regular_expression*：IP ログ ステータスの出力に含まれる正規表現。
- **begin**：**more** コマンドの出力を検索し、指定された文字列の最初のインスタンスからの出力を表示します。
- **exclude**：IP ログ ステータスの出力をフィルタリングし、特定の正規表現が含まれた行を除外します。
- **include**：IP ログ ステータスの出力をフィルタリングし、特定の正規表現が含まれた行を挿入します。

IP ログの表示

IP のログの内容を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　すべての IP ログのステータスを表示します。

```
ips-ssp# iplog-status
Log ID:                 2425
```

```
IP Address 1:           192.0.2.1
Virtual Sensor:         vs0
Status:                 started
Start Time:             2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:       1039438


Log ID:                 2342
IP Address 1:           192.0.2.10
IP Address 2:           192.0.2.20
Virtual Sensor:         vs0
Status:                 completed
Event ID:               209348
Start Time:             2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:               2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

ステップ 3　すべての IP ログの簡単なリストを表示します。

```
ips-ssp# iplog-status brief
Log ID   VS    IP Address1   Status      Event ID   Start Date
2425     vs0   192.0.2.10    started     N/A        2003/07/30
2342     vs0   192.0.2.20    completed   209348     2003/07/30
ips-ssp#
```

動作している IP ログの停止

no iplog [**log-id** *log_id* | **name** *name*] コマンドを使用して、`started` 状態のログの記録を停止し、`added` 状態のログを削除します。

（注）　added 状態の IP ログで **no iplog** コマンドを使用すると、IP ログが停止します。added 状態は、IP ログがまだ空である（パケットがない）ことを示しています。パケットがない状態での停止は、空の IP ログを停止することを意味します。空の IP ログは、停止の際に削除されます。

（注）　**no iplog** コマンドでは、IP ログは削除されません。このコマンドは、その IP ログでそれ以上パケットをキャプチャしないようセンサーに通知するだけです。

オプション

次のオプションが適用されます。

- *log_id* : 停止するロギング セッションのログ ID。ログ ID を検索するには **iplog-status** コマンドを使用します。
- *name* : ロギングを開始または終了する仮想センサー。

IP ロギング セッションのディセーブル化

1 つまたはすべての IP ロギング セッションをディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　特定の IP ロギング セッションを停止します。

a. 停止するセッションのログ ID を検索します。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

（注）　各アラートは、そのアラートが原因となって作成された IP ログを参照します。複数のアラートによって同一の IP アドレスに関する IP ログが作成された場合は、それらすべてのアラートに対して IP ログが 1 つだけ作成されます。各アラートは同じ IP ログを参照します。ただし IP ログ ステータスの出力には、その IP ログをトリガーした最初のアラートのイベント ID だけが表示されます。

b. IP ログ セッションを停止します。

```
ips-ssp# no iplog log-id 137857512
```

ステップ 3　仮想センサーでのすべての IP ロギング セッションを停止します。

```
ips-ssp# no iplog name vs0
```

ステップ 4　IP ロギングが停止されたことを確認します。ログが停止されると、completed ステータスが表示されます。

```
ips-ssp# iplog-status
Log ID:              1
IP Address 1:        192.0.2.1
Virtual Sensor:      vs0
Status:              completed
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
ips-ssp#
```

表示する IP ログ ファイルのコピー

copy iplog *log_id destination_url* コマンドを使用して、IP ログを FTP または SCP サーバにコピーし、Ethereal や tcpdump などのスニフィング ツールで表示できるようにします。

オプション

次のオプションが適用されます。

- *log_id*：ロギング セッションのログ ID を指定します。ログ ID は **iplog-status** コマンドを使用して検索できます。
- *destination_url*：コピー先ファイルの場所を指定します。URL またはキーワードを使用できます。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

FTP または SCP プロトコルを使用すると、パスワードの入力を求められます。

IP ログ ファイルのコピー

IP ログ ファイルを FTP または SCP サーバにコピーするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コピーするログ ファイルのログ ID のステータスが completed になるまで、**iplog-status** コマンドを使用して IP ログ ステータスをモニタします。

```
ips-ssp# iplog-status
Log ID:              2425
IP Address:          192.0.2.1
Virtual Sensor:      vs0
Status:              started
Start Time:          2010/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:    1039438

Log ID:              2342
IP Address:          192.0.2.2
Virtual Sensor:      vs0
Status:              completed
Event ID:            209348
Start Time:          2010/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:            2010/07/30 18:34:18 2002/07/30 12:34:18 CST
ips-ssp#
```

ステップ 3　IP ログを FTP または SCP サーバにコピーします。

```
ips-ssp# copy iplog 2342 ftp://root@209.165.200.225/user/iplog1
Password: ******** Connected to 209.165.200.225 (209.165.200.225). 220 linux.machine.com
FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30 :36 EST 2000) ready. ftp> user (username)
root 331 Password required for root. Password:230 User root logged in. ftp> 200 Type set
to I. ftp> put iplog.8518.tmp iplog1 local: iplog.8518.tmp remote: iplog1 227 Entering
Passive Mode (2,4,6,8,179,125) 150 Opening BINARY mode data connection for iplog1. 226
Transfer complete. 30650 bytes sent in 0.00246 secs (1.2e+04 Kbytes/sec) ftp>
```

ステップ 4　Wireshark や TCPDUMP などのスニファ プログラムを使用して IP ログを開きます。Wireshark の詳細については、http://www.wireshark.org を参照してください。TCPDUMP の詳細については、http://www.tcpdump.org/ 参照してください。

CHAPTER 13

インターフェイスのライブ トラフィックの表示とキャプチャ

（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、パケット ファイルを表示、キャプチャ、コピー、消去する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。

- 「パケットの表示とキャプチャについて」（P.13-1）
- 「インターフェイスのライブ トラフィックの表示」（P.13-2）
- 「インターフェイスのライブ トラフィックのキャプチャ」（P.13-4）
- 「パケット ファイルのコピー」（P.13-7）
- 「パケット ファイルの消去」（P.13-8）

パケットの表示とキャプチャについて

インターフェイスのライブ トラフィックを表示またはキャプチャし、そのライブ トラフィックや以前にキャプチャされたファイルを画面に直接表示することができます。ストレージは 1 つのローカル ファイルのみに使用でき、後続のキャプチャ要求によって既存のファイルは上書きされます。ストレージ ファイルのサイズはプラットフォームによって異なります。要求された数のパケットがキャプチャされる前に最大ファイル サイズに達すると、メッセージが表示される場合があります。

（注） インターフェイスからライブ トラフィックをキャプチャしても、センサーの機能は中断されません。

注意 インターフェイスの設定を変更すると、そのインターフェイスで実行されている **packet** コマンドが異常終了します。

注意　**packet display** または **capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックの表示

packet display *interface_name* [**snaplen** *length*] [**count** *count*] [**verbose**] [**expression** *expression*] コマンドを使用して、インターフェイスのライブ トラフィックを画面に直接表示します。

（注）　ライブ表示を終了するには、Ctrl キーを押した状態で C キーを押します。

オプション

次のオプションが適用されます。

- *interface_name*：インターフェイス名、インターフェイス タイプ（GigabitEthernet、FastEthernet、Management）、スロット / ポートの順に指定します。システムに存在するインターフェイス名だけを使用できます。
- **snaplen**：（任意）キャプチャする各パケットの最大バイト数を指定します。有効な範囲は 68 ～ 1600 です。デフォルトは 0 です。0 の値は、パケット全体をキャプチャするために必要な長さを使用することを意味します。
- **count**：（任意）キャプチャするパケットの最大数を指定します。有効な範囲は 1 ～ 10000 です。

  （注）　このオプションを指定しない場合、最大ファイル サイズまでキャプチャされるとキャプチャは停止します。

- **verbose**：（任意）1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します。
- **expression**：パケット表示フィルタの式を指定します。この式は TCPDUMP に直接渡されるので、TCPDUMP 式の構文に従う必要があります。

  （注）　式の構文については、TCPDUMP の man ページで説明されています。

- **file-info**：保存されたパケット ファイルに関する情報を表示します。

  file-info で表示される情報は次のとおりです。

  Captured by: *user:id*, Cmd: *cliCmd*

  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress

  ここで

  user = キャプチャを開始するユーザのユーザ名

  id = ユーザの CLI ID

  cliCmd = キャプチャを実行するために入力されたコマンド

注意　**packet display** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックの表示

インターフェイスのライブ トラフィックを画面に表示するようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用してセンサーにログインします。

ステップ 2　PortChannel0/0 など、目的のインターフェイスのライブ トラフィックを表示します。

```
ips-ssp# packet display PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:43:05.691883 IP (tos 0x10, ttl  64, id 55460, offset 0, flags [DF], length: 100)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 4233955485:4233955533(48) ack
1495691730 win 8576 <nop,nop,timestamp 44085169 226014949>
03:43:05.691975 IP (tos 0x10, ttl  64, id 55461, offset 0, flags [DF], length: 164)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 48:160(112) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.691998 IP (tos 0x10, ttl  64, id 53735, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 48 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693165 IP (tos 0x10, ttl  64, id 53736, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693351 IP (tos 0x10, ttl  64, id 55462, offset 0, flags [DF], length: 316)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 160:424(264) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693493 IP (tos 0x10, ttl  64, id 55463, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 424:664(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693612 IP (tos 0x10, ttl  64, id 55464, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 664:904(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693628 IP (tos 0x10, ttl  64, id 53737, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 424 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693654 IP (tos 0x10, ttl  64, id 53738, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 664 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693926 IP (tos 0x10, ttl  64, id 55465, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 904:1144(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694043 IP (tos 0x10, ttl  64, id 55466, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1144:1384(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694163 IP (tos 0x10, ttl  64, id 55467, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1384:1624(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694209 IP (tos 0x10, ttl  64, id 53739, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 1384 win 11704
<nop,nop,timestamp 226014950 44085169>
03:43:05.694283 IP (tos 0x10, ttl  64, id 55468, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1624:1864(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694402 IP (tos 0x10, ttl  64, id 55469, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1864:2104(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694521 IP (tos 0x10, ttl  64, id 55470, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2104:2344(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694690 IP (tos 0x10, ttl  64, id 53740, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 2344 win 11704
<nop,nop,timestamp 226014950 44085169>
```

```
03:43:05.694808 IP (tos 0x10, ttl  64, id 55471, offset 0, flags [DF], length: 300)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2344:2592(248) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
```

ステップ 3　**expression** オプションを使用すると、表示内容を制限できます。たとえば、TCP パケットだけを表示することができます。

（注）　TCPDUMP の man ページで説明されているとおり、プロトコル識別子 tcp、udp、および icmp はキーワードでもあるため、2 つのバック スラッシュ（\\）を使用してエスケープする必要があります。

```
ips-ssp# packet display PortChannel0/1 verbose expression ip proto \\tcp
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:42:02.509738 IP (tos 0x10, ttl  64, id 27743, offset 0, flags [DF], length: 88)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 3449098782:3449098830(48) ack
3009767154 win 8704
03:42:02.509834 IP (tos 0x10, ttl  64, id 27744, offset 0, flags [DF], length: 152)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 48:160(112) ack 1 win 8704
03:42:02.510248 IP (tos 0x0, ttl 252, id 55922, offset 0, flags [none], length: 40)
64.101.182.54.47039 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 8760
03:42:02.511262 IP (tos 0x10, ttl  64, id 27745, offset 0, flags [DF], length: 264)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 160:384(224) ack 1 win 8704
03:42:02.511408 IP (tos 0x10, ttl  64, id 27746, offset 0, flags [DF], length: 248)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 384:592(208) ack 1 win 8704
03:42:02.511545 IP (tos 0x10, ttl  64, id 27747, offset 0, flags [DF], length: 240)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 592:792(200) ack 1 win 8704
```

ステップ 4　パケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:25579, Cmd: packet capture PortChannel0/1
Start: 2010/02/03 02:56:48 UTC, End: 2010/02/03 02:56:51 UTC
ips-ssp#
```

インターフェイスのライブ トラフィックのキャプチャ

packet capture *interface_name* [**snaplen** *length*] [**count** *count*] [**expression** *expression*] コマンドを使用して、インターフェイスのライブ トラフィックをキャプチャします。**packet capture** コマンドを使用できるのは、一度に 1 ユーザだけです。2 番めのユーザ要求が発行されるとエラー メッセージが表示され、現在キャプチャを実行しているユーザに関する情報が示されます。

注意　**packet capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

packet capture コマンドでは、libpcap 出力をローカル ファイルにキャプチャします。**packet display packet-file** [**verbose**] [**expression** *expression*] コマンドを使用して、このローカル ファイルを表示します。ローカル ファイルに関する情報がある場合は、**packet display file-info** を使用して表示できます。

オプション

次のオプションが適用されます。

- *interface_name*：論理インターフェイス名を指定します。システムに存在するインターフェイス名だけを使用できます。
- **snaplen**：キャプチャする各パケットの最大バイト数を指定します（任意）。有効な範囲は 68 ～ 1600 です。デフォルトは 0 です。
- **count**：キャプチャするパケットの最大数を指定します（任意）。有効な範囲は 1 ～ 10000 です。

（注） このオプションを指定しない場合、最大ファイル サイズまでキャプチャされるとキャプチャは停止します。

- **expression**—パケット キャプチャ フィルタの式を指定します。この式は TCPDUMP に直接渡されるので、TCPDUMP 式の構文に従う必要があります。
- **file-info**：保存されたパケット ファイルに関する情報を表示します。

  file-info で表示される情報は次のとおりです。

  Captured by: *user:id*, Cmd: *cliCmd*

  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress

  ここで

  user = キャプチャを開始するユーザのユーザ名

  id = ユーザの CLI ID

  cliCmd = キャプチャを実行するために入力されたコマンド
- **verbose**：1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します。このパラメータはオプションです。

インターフェイスのライブ トラフィックのキャプチャ

インターフェイスのライブ トラフィックをキャプチャするようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用してセンサーにログインします。

ステップ 2　PortChannel0/0 など、目的のインターフェイスのライブ トラフィックをキャプチャします。

```
ips-ssp# packet capture PortChannel0/0
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
125 packets captured
126 packets received by filter
0 packets dropped by kernel
```

ステップ 3　キャプチャされたパケット ファイルを表示します。

```
ips-ssp# packet display packet-file
reading from file /usr/cids/idsRoot/var/packet-file, link-type EN10MB (Ethernet)
03:03:13.216768 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:13.232881 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 3266153791 win
64328
03:03:13.232895 IP 192.0.2.3.23 > 64.101.182.244.1978: P 1:157(156) ack 0 wi
n 5840
```

```
03:03:13.433136 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 157 win 65535
03:03:13.518335 IP 10.89.130.134.42342 > 255.255.255.255.42342: UDP, length: 76
03:03:15.218814 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:15.546866 IP 64.101.182.244.1978 > 192.0.2.3.23: P 0:2(2) ack 157 win
65535
03:03:15.546923 IP 192.0.2.3.23 > 64.101.182.244.1978: P 157:159(2) ack 2 wi
n 5840
03:03:15.736377 IP 64.101.182.244.1978 > 192.0.2.3.23: . ack 159 win 65533
03:03:17.219612 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.218535 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.843658 IP 64.101.182.143.3262 > 10.89.130.23.445: P 3749577803:37495778
56(53) ack 3040953472 win 64407
03:03:20.174835 IP 161.44.55.250.1720 > 10.89.130.60.445: S 3147454533:314745453
3(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:21.219958 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:21.508907 IP 161.44.55.250.1809 > 10.89.130.61.445: S 3152179859:315217985
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:23.221004 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:23.688099 IP 161.44.55.250.1975 > 10.89.130.63.445: S 3160484670:316048467
0(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:25.219054 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:25.846552 IP 172.20.12.10.2984 > 10.89.130.127.445: S 1345848756:134584875
6(0) win 64240 <mss 1460,nop,nop,sackOK>
03:03:26.195342 IP 161.44.55.250.2178 > 10.89.130.65.445: S 3170518052:317051805
2(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.222725 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:27.299178 IP 161.44.55.250.2269 > 10.89.130.66.445: S 3174717959:317471795
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.308798 arp who-has 161.44.55.250 tell 10.89.130.66
03:03:28.383028 IP 161.44.55.250.2349 > 10.89.130.67.445: S 3178636061:317863606
1(0) win 65520 <mss 1260,nop,nop,sackOK>
--MORE--
```

ステップ 4　パケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:8874, Cmd: packet capture PortChannel0/0
Start: 2010/01/07 00:12:50 UTC, End: 2010/01/07 00:15:30 UTC
ips-ssp#
```

パケット ファイルのコピー

copy packet-file *destination_url* コマンドを使用してパケット ファイルを FTP または SCP サーバにコピーし、そのファイルを保存したり Wireshark や TCPDUMP など他のツールを使って解析したりします。

オプション

次のオプションが適用されます。

- **packet-file**：**packet capture** コマンドを使用してキャプチャし、ローカルに保存された libpcap ファイルを指定します。
- *destination_url*：コピー先ファイルの場所を指定します。URL またはキーワードを使用できます。

（注）　コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。

  - ftp:：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。
    ftp:[//[username@] location]/relativeDirectory]/filename
    ftp:[//[username@]location]//absoluteDirectory]/filename
  - scp:：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。
    scp:[//[username@] location]/relativeDirectory]/filename
    scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用すると、パスワードの入力を求められます。

パケット ファイルのコピー

パケット ファイルを FTP または SCP サーバにコピーするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　パケット ファイルを FTP または SCP サーバにコピーします。

```
ips-ssp# copy packet-file scp://jbrown@209.165.200.225/work/
Password: *********
packet-file               100% 1670     0.0KB/s   00:00
ips-ssp#
```

ステップ 3　Wireshark または TCPDUMP を使用してパケット ファイルを表示します。

パケット ファイルの消去

erase packet-file コマンドを使用してパケット ファイルを消去します。パケット ファイルは 1 つしかありません。サイズは 16 MB で、**packet capture** コマンドが実行されるたびに上書きされます。

パケット ファイルを消去するには、次の手順を実行します。

ステップ 1　現在キャプチャされているパケット ファイルに関する情報を表示します。

```
ips-ssp# packet display file-info
Captured by: cisco:1514, Cmd: packet capture GigabitEthernet0/1
Start: 2005/02/15 03:55:00 CST, End: 2005/02/15 03:55:05 CST
ips-ssp#
```

ステップ 2　パケット ファイルを消去します。

```
ips-ssp# erase packet-file
ips-ssp#
```

ステップ 3　パケット ファイルが消去されたことを確認します。

```
ips-ssp# packet display file-info
No packet-file available.
ips-ssp#
```

CHAPTER 14

Attack Response Controller でのブロッキングおよびレート制限の設定

（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。

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IDM、IME、および CLI には Network Access Controller、**nac**、および **network-access** などの記述が含まれています。

この章では、センサーでブロッキングおよびレート制限を実行するための ARC の設定について説明します。次のような構成になっています。

- 「ブロッキングについて」（P.14-2）
- 「レート制限について」（P.14-4）
- 「レート制限のサービス ポリシーについて」（P.14-5）
- 「ARC を設定する前に」（P.14-5）
- 「サポートされるデバイス数」（P.14-6）
- 「ブロッキング プロパティの設定」（P.14-7）
- 「ユーザ プロファイルの設定」（P.14-21）
- 「ブロッキングおよびレート制限デバイスの設定」（P.14-22）
- 「センサーをマスター ブロッキング センサーにする設定」（P.14-29）
- 「ホスト ブロッキングの設定」（P.14-32）
- 「ネットワーク ブロッキングの設定」（P.14-33）
- 「接続ブロッキングの設定」（P.14-34）
- 「ブロックされているホストおよび接続のリストの取得」（P.14-35）

ブロッキングについて

（注）　ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IDM、IME、および CLI には Network Access Controller、**nac**、および **network-access** などの記述が含まれています。

ARC は、攻撃側のホストおよびネットワークからのアクセスをブロックすることで、疑わしいイベントに対応し、ネットワーク デバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のマスター ブロッキング センサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

ARC は、新しいブロックでのアクション応答を 7 秒以内に完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキング デバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は 250 以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス / 方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えると、ARC がブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりする場合があります。

注意　マルチモード管理コンテキストの FWSM では、ブロッキングはサポートされません。

セキュリティ アプライアンスがマルチモードで設定されている場合、Cisco IPS はブロック要求に VLAN 情報を挿入しません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタし、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを指している可能性があります。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。
- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホスト ブロックにブロックが自動的に切り替えられます。
- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。ホスト ブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

注意　ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

自動ブロックの場合は、特定のシグニチャに対するイベント アクションとして [request-block-host] または [request-block-connection] チェック ボックスをオンにし、それらのアクションを設定済みの任意のイベント アクション オーバーライドに追加する必要があります。これによって、そのシグニチャがトリガーされたとき、SensorApp は ARC にブロック要求を送信することができます。SensorApp からブロック要求を受信すると、ARC はホストまたは接続をブロックするようにデバイス コンフィギュレーションを更新します。

Cisco ルータおよび Catalyst 6500 シリーズ スイッチでは、ARC は ACL または VACL を適用してブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティ アプライアンスでは、ACL または VACL は使用されません。組み込みの **shun** および **no shun** コマンドが使用されます。

注意　ARC が作成する ACL を、ユーザまたは他のシステムが変更してはいけません。これらの ACL は一時的なものであり、センサーによって新しい ACL が絶えず作成されています。Pre-Block ACL および Post-Block ACL にのみ変更を加えることができます。

ARC でデバイスを管理するには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）。
- ログイン パスワード。
- イネーブル パスワード（イネーブル特権を持つユーザは不要）。
- 管理対象のインターフェイス（ethernet0、vlan100 など）。
- 作成される ACL または VACL の先頭（Pre-Block ACL または VACL）または末尾（Post-Block ACL または VACL）に適用する既存の ACL または VACL 情報。セキュリティ アプライアンスはブロッキングに ACL を使用しないため、この情報はセキュリティ アプライアンスには適用されません。
- デバイスとの通信に Telnet と SSH のどちらを使用しているか。
- ブロックしない IP アドレス（ホストまたはホストの範囲）。
- ブロックの継続時間。

ヒント　ARC のステータスを確認するには、`sensor#` に **show statistics network-access** と入力します。管理下にあるデバイス、アクティブなブロックとレート制限、すべてのデバイスのステータスが出力に表示されます。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

詳細情報

- request-block-host または request-block-connection イベント アクションをシグニチャに追加する手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。
- 特定のリスク レーティングのアラートに request-block-host または request-block-connection イベント アクションを追加するオーバーライドの設定手順については、「イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化」（P.8-17）を参照してください。
- Pre-Block ACL および Post-Block ACL の詳細については、「センサーによるデバイスの管理方法」（P.14-22）を参照してください。

レート制限について

ARC は、保護されているネットワーク内のトラフィックに対してレート制限を行います。レート制限により、センサーはネットワーク デバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

レート制限を追加するには以下を指定します。

- レート制限の送信元アドレスまたは宛先アドレス（あるいはその両方）
- TCP または UDP プロトコルを使用するレート制限の送信元ポートまたは宛先ポート（あるいはその両方）

レート制限シグニチャをチューニングすることもできます。また、アクションを request-rate-limit に設定し、これらのシグニチャの比率を設定する必要があります。

（注）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

表 14-1 に、サポートされるレート制限シグニチャとパラメータを示します。

表 14-1　レート制限シグニチャ

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	なし
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	なし
6910	Net Flood UDP	UDP	No	なし
6920	Net Flood TCP	TCP	No	なし
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

ヒント　ARC のステータスを確認するには、sensor# に **show statistics network-access** と入力します。管理下にあるデバイス、アクティブなブロックとレート制限、すべてのデバイスのステータスが出力に表示されます。

詳細情報

- ルータにレート制限を設定する手順については、「ブロッキングおよびレート制限デバイスの設定」（P.14-22）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

レート制限のサービス ポリシーについて

レート制限が設定されているインターフェイス/方向にはサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、**acls** および **class-map** エントリを使用してトラフィックを識別し、**policy-map** および **service-policy** エントリを使用してトラフィックをポリシングします。

ARC を設定する前に

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをデバイス管理用のマスター ブロッキング センサーとして設定すると、もう一方のセンサーからマスター ブロッキング センサーに要求を転送できます。

（注）　マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のセキュリティ アプライアンスと 10 台のルータでブロッキングを行う場合、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ARC でブロッキングまたはレート制限を設定する前に、必ず次の作業を実行してください。

- ネットワーク トポロジを解析し、どのデバイスをどのセンサーによってブロックするか、ブロックしてはならないアドレスはどれかを確認します。
- 各デバイスへのログインに必要なユーザ名、デバイスのパスワード、イネーブル パスワード、および接続タイプ（Telnet または SSH）の情報を収集します。
- デバイスのインターフェイス名を確認します。
- Pre-Block ACL または VACL、および Post-Block ACL または VACL が必要な場合は、その名前を確認します。

- ブロックするインターフェイス、ブロックしないインターフェイス、およびそれらの方向（インまたはアウト）を確認します。誤ってネットワーク全体をシャットダウンすることは避けなければなりません。

詳細情報

マスター ブロッキング センサーの設定手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

サポートされるデバイス数

注意　推奨される制限を超えると、ARC がブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりする場合があります。

デフォルトでは、ARC は任意の組み合わせで 250 までのデバイスをサポートします。ARC によるブロッキングでは、次のデバイスがサポートされます。

- Cisco IOS 11.2 以降（ACL）を使用する Cisco シリーズ ルータ
  - Cisco 1600 シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ
- Catalyst 5000 スイッチ、RSM 搭載、IOS 11.2(9)P 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、IOS 12.1(13)E 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、Catalyst ソフトウェア バージョン 7.5(1) 以降（VACL）
  - Supervisor Engine 1A（PFC 搭載）
  - Supervisor Engine 1A（MSFC1 搭載）
  - Supervisor Engine 1A（MFSC2 搭載）
  - Supervisor Engine 2（MSFC2 搭載）
  - Supervisor Engine 720（MSFC3 搭載）

（注）　Supervisor Engine での VACL ブロッキングと MSFC での ACL ブロッキングがサポートされます。

- PIX Firewall、バージョン 6.0 以降（**shun** コマンド）
  - 501
  - 506E
  - 515E
  - 525
  - 535
- ASA バージョン 7.0 以降（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ブロッキングを設定するには、ACL、VACLS、または **shun** コマンドのいずれかを使用します。すべてのファイアウォールおよび ASA モデルで **shun** コマンドがサポートされます。

ARC によるレート制限では、次のデバイスがサポートされます。

- Cisco IOS 12.3 以降を使用する Cisco シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ

注意　ARC は、VIP を使用する 7500 ルータでのレート制限はできません。ARC はエラーを報告しますが、レート制限は実行できません。

ブロッキング プロパティの設定

デフォルトのブロッキング プロパティは変更可能です。デフォルトのプロパティを使用することを推奨しますが、変更する必要がある場合は、次の手順を使用します。

- 「センサー自体のブロックの許可」（P.14-8）
- 「ブロッキングのディセーブル」（P.14-9）
- 「最大ブロックエントリ数の指定」（P.14-11）
- 「ブロック時間の指定」（P.14-13）
- 「ACL ロギングのイネーブル化」（P.14-14）
- 「NVRAM への書き込みのイネーブル化」（P.14-15）
- 「すべてのブロッキング イベントおよびエラーのロギング」（P.14-17）

- 「ブロッキング インターフェイスの最大数の設定」（P.14-18）
- 「絶対にブロックしないアドレスの設定」（P.14-19）

センサー自体のブロックの許可

サービス ネットワーク アクセス サブモードで **allow-sensor-block {true | false}** コマンドを使用して、センサーがそれ自体をブロックするように設定します。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、推奨しません。センサーでそれ自体の IP アドレスをブロックするルールが作成されても、センサーからブロッキング デバイスへのアクセスが妨げられないことが確認された場合は、このオプションを設定できます。

センサーがそれ自体をブロックすることを許可するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　センサーがそれ自体をブロックするように設定します。デフォルトでは、この値は false です。

```
ips-ssp(config-net-gen)# allow-sensor-block true
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: true default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 192.0.2.1
         ---------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 209.165.200.224/27
         ---------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
--MORE--
```

ステップ 6　センサーがそれ自体をブロックしないように設定します。

```
ips-ssp(config-net-gen)# allow-sensor-block false
```

ステップ 7　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 192.0.2.1
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 209.165.200.224/27
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキングのディセーブル

サービス ネットワーク アクセス サブモードで **block-enable {true | false}** コマンドを使用して、センサーでのブロッキングをイネーブルまたはディセーブルにします。

（注）　ブロッキングが機能するには、デバイスがブロッキングを実行するように設定する必要があります。

デフォルトでは、センサーのブロッキングはイネーブルになっています。デバイスが ARC によって管理されており、そのデバイスを手動で設定する必要がある場合、まずブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。デバイスや ARC がクラッシュする可能性があるためです。

注意　デバイスのメンテナンスを目的としてブロッキングをディセーブルにする場合は、メンテナンスの完了後、必ずブロッキングをイネーブルにしてください。そうでないと、本来ブロック可能な攻撃に対してネットワークが脆弱になります。

（注）　ブロッキングがディセーブルの間も、ARC は引き続きブロックを受信し、アクティブなブロックの時間を追跡します。ただし、管理下にあるデバイスで新しいブロックの追加や削除は行いません。ブロッキングが再度イネーブルになると、デバイスのブロックは更新されます。

ブロッキングまたはレート制限をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　センサーでブロッキングをディセーブルにします。デフォルトでは、この値は true に設定されています。

```
ips-ssp(config-net-gen)# block-enable false
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: false default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 192.0.2.1
         ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 209.165.200.224/27
         ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
--MORE--
```

ステップ 6　センサーでブロッキングをイネーブルにします。

```
ips-ssp(config-net-gen)# block-enable true
```

ステップ 7　設定がデフォルトに戻ったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 192.0.2.1
         ---------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 209.165.200.224/27
         ---------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- センサーで Cisco ルータの管理を設定する手順については、「センサーで Cisco ルータを管理するための設定」（P.14-23）を参照してください。
- センサーで Cisco ルータおよびスイッチの管理を設定する手順については、「センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定」（P.14-26）を参照してください。

最大ブロックエントリ数の指定

サービス ネットワーク アクセス サブモードで **block-max-entries** コマンドを使用して、最大ブロックエントリ数を設定します。同時に維持するブロックの数を指定できます（1 ～ 65535）。デフォルト値は 250 です。

注意　250 を超える最大ブロック エントリ数を設定することは推奨できません。ACL または shun エントリ数が多いと、一部のデバイスで問題が発生する場合があります。エントリ数を増やす前に、各デバイスのマニュアルでその制限を確認してください。

（注）　ブロック数が最大ブロック エントリ数を超えることはありません。最大数に達すると、既存のブロックがタイムアウトするか削除されるまで新しいブロックは発生しません。

最大ブロック エントリ数を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロック エントリの最大数を変更します。

```
ips-ssp(config-net-gen)# block-max-entries 100
```

ステップ 5　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
         -------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
--MORE--
```

ステップ 6　ブロック数をデフォルト値の 250 に戻します。

```
ips-ssp(config-net-gen)# default block-max-entries
```

ステップ 7　設定を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
```

```
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0
      ---------------------------------------------
      ---------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ---------------------------------------------
         ip-address: 192.0.2.1
         -----------------------------------------
      ---------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ---------------------------------------------
         ip-address: 209.165.200.224/27
         -----------------------------------------
      ---------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ---------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロック時間の指定

サービス イベント アクション ルール サブモードで **global-block-timeout** コマンドを使用して、自動ブロックが継続される時間を変更します。デフォルトは 30 分です。

（注）　デフォルトのブロック時間の変更は、すべてのシグニチャに影響するシグニチャ パラメータを変更することによって行います。

（注）　手動ブロックの時間は、そのブロックの要求時に設定されます。

デフォルトのブロック時間を変更するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

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

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-rul)# general
```

ステップ 4　ブロック時間を指定します。この値は、ブロック イベントの継続時間を分単位で示しています（0 ～ 10000000）。

```
ips-ssp(config-rul-gen)# global-block-timeout 60
```

ステップ 5　設定を確認します。

```
ips-ssp(config-rul-gen)# show settings
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 60 default: 30
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
ips-ssp(config-rul-gen)#
```

ステップ 6　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-rul-gen)# exit
ips-ssp(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

（注）　シグニチャがアップデートされるまで、少し時間がかかります。

ACL ロギングのイネーブル化

サービス ネットワーク アクセス サブモードで **enable-acl-logging {true | false}** コマンドを使用します。ACL ロギングをイネーブルにすると、ARC はログ パラメータを ACL または VACL のブロック エントリに追加します。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。ACL ロギングのイネーブル化は、ルータとスイッチだけに適用されます。デフォルトではディセーブルになっています。

ACL ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ACL ロギングをイネーブルにします。

```
ips-ssp(config-net-gen)# enable-acl-logging true
```

ステップ 5　ACL ロギングがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: true default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 6　**false** キーワードを使用して ACL ロギングをディセーブルにします。

```
ips-ssp(config-net-gen)# enable-acl-logging false
```

ステップ 7　ACL ログングがディセーブルに設定されたことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

NVRAM への書き込みのイネーブル化

enable-nvram-write {true | false} コマンドを使用して、ARC が最初に接続したときにルータが NVRAM に書き込みを実行するようにセンサーを設定します。enable-nvram-write をイネーブルにすると、ACL が更新されるたびに NVRAM への書き込みが実行されます。デフォルトではディセーブルになっています。

NVRAM 書き込みをイネーブルにすると、ブロッキングに関するすべての変更が NVRAM に書き込まれます。ルータが再起動されても、適切なブロックがアクティブな状態で維持されます。NVRAM 書き込みをディセーブルにすると、ルータの再起動後、ブロッキングが実行されない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合は、NVRAM の寿命が長くなり、新しいブロックを設定する時間が短縮されます。

NVRAM 書き込みをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　NVRAM への書き込みをイネーブルにします。

```
ips-ssp(config-net-gen)# enable-nvram-write true
```

ステップ 5　NVRAM への書き込みがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: true default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
```

ステップ 6　NVRAM への書き込みをディセーブルにします。

```
ips-ssp(config-net-gen)# enable-nvram-write false
```

ステップ 7　NVRAM への書き込みがディセーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

すべてのブロッキング イベントおよびエラーのロギング

サービス ネットワーク アクセス サブモードで **log-all-block-events-and-errors {true | false}** コマンドを使用して、ブロックの後に続くイベントを最初から最後までログに記録するようにセンサーを設定します。たとえば、ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。**log-all-block-events-and-errors** をディセーブルにすると、新しいイベントとエラーは抑止されます。デフォルトはイネーブルです。

ブロッキング イベントとエラーのロギングをディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロッキング イベントとエラーのロギングをディセーブルにします。

```
ips-ssp(config-net-gen)# log-all-block-events-and-errors false
```

ステップ 5　ロギングがディセーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: false default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　ブロッキング イベントとエラーのロギングをイネーブルにします。

```
ips-ssp(config-net-gen)# log-all-block-events-and-errors true
```

ステップ 7　ロギングがイネーブルになったことを確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキング インターフェイスの最大数の設定

max-interfaces コマンドを使用して、ブロックを実行するためのインターフェイスの最大数を設定します。たとえば、PIX Firewall は 1 つのインターフェイスとしてカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。1 つのルータ、スイッチ、またはファイアウォールに、最大 250 のブロッキング インターフェイスを設定できます。最大 250 の Catalyst 6K スイッチ、ルータ、およびファイアウォールを設定できます。

max-interfaces コマンドでは、すべてのインターフェイスとデバイスの合計数の制限を設定します。インターフェイスとデバイスの合計数の制限を設定できる一方、デバイス単位で設定できるブロッキング インターフェイスには、固定の制限値があります。ネットワーク アクセス モードで **show settings** コマンドを使用すると、デバイスごとに固有の最大制限値が表示されます。

ブロッキング インターフェイスの最大数を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　インターフェイスの最大数を指定します。

```
ips-ssp(config-net-gen)# max-interfaces 50
```

ステップ 5　インターフェイスの最大数を確認します。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 50 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　設定をデフォルトの 250 に戻します。

```
ips-ssp(config-net-gen)# default max-interfaces
```

ステップ 7　デフォルト設定を確認します。

```
ips-ssp(config-net-gen)# show settings

   general
   ------------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

絶対にブロックしないアドレスの設定

サービス ネットワーク アクセス サブモードで **never-block-hosts** および **never-block-networks** コマンドを使用して、ブロックしないホストとネットワークを設定します。

オプション

次のオプションが適用されます。

- *ip_address*：ブロックしないデバイスの IP アドレス。
- *ip_address/netmask*：ブロックしないネットワークの IP アドレス。形式は A.B.C.D/nn です。

信頼できるネットワーク デバイスによる通常の予期可能な動作が攻撃と見なされることも考えられるため、手動でも絶対にブロックしてはならないホストおよびネットワークをセンサーが識別するように調整する必要があります。そのようなデバイスは絶対にブロックしてはなりません。また、信頼できる内部のネットワークも絶対にブロックしてはなりません。単一のホストを指定することも、ネットワーク全体を指定することもできます。

（注）　**never-block-hosts** および **never-block-networks** コマンドは、Request Block Host および Request Block Connection イベント アクションだけに適用されます。Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップ対象から除外するホストをフィルタリングするには、イベント アクション ルールを使用します。

ブロックしないアドレスの設定

アドレスがブロッキング デバイスでブロックされないように設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 4　ブロックしないアドレスを指定します。

- シングル ホスト

```
ips-ssp(config-net-gen)# never-block-hosts 192.0.2.1
```

- ネットワーク

```
ips-ssp(config-net-gen)# never-block-networks 209.165.200.224/27
```

ステップ 5　設定を確認できます。

```
ips-ssp(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 192.0.2.1
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 2)
      -----------------------------------------------
         ip-address: 209.165.200.224/27
--MORE--
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

イベント アクション フィルタの設定手順については、「イベント アクション フィルタの設定」（P.8-21）を参照してください。

ユーザ プロファイルの設定

サービス ネットワーク アクセス サブモードで **user-profiles** *profile_name* コマンドを使用して、センサーが管理する他のデバイスにユーザ プロファイルを設定します。ユーザ プロファイルには、ユーザ ID、パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同一のパスワードとユーザ名を共有するすべてのルータを、1 つのユーザ プロファイルにまとめることができます。

（注） デバイスへのログインにユーザ名またはパスワードが必要ない場合は、その値を設定しないでください。

（注） ユーザ プロファイルは、ブロッキング デバイスを設定する前に作成する必要があります。

ユーザ プロファイルを作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ユーザ プロファイル名を作成します。

```
ips-ssp(config-net)# user-profiles PROFILE1
```

ステップ 4　そのユーザ プロファイルに対応するユーザ名を入力します。

```
ips-ssp(config-net-use)# username username
```

ステップ 5　このユーザのパスワードを指定します。

```
ips-ssp(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

ステップ 6　このユーザのイネーブル パスワードを指定します。

```
ips-ssp(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

ステップ 7　設定を確認できます。

```
ips-ssp(config-net-use)# show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
ips-ssp(config-net-use)#
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-use)# exit
ips-ssp(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ブロッキングおよびレート制限デバイスの設定

ここでは、センサーがブロッキングまたはレート制限の実行に使用するデバイスの設定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。

- 「センサーによるデバイスの管理方法」（P.14-22）
- 「センサーで Cisco ルータを管理するための設定」（P.14-23）
- 「センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定」（P.14-26）
- 「センサーで Cisco ファイアウォールを管理するための設定」（P.14-28）

センサーによるデバイスの管理方法

（注）　ACL はレート制限デバイスには適用されません。

ARC は Cisco ルータおよびスイッチ上の ACL を使用して、これらのデバイスを管理します。ACL は、次のように作成されます。

1. センサーの IP アドレスまたは NAT アドレス（指定されている場合）が記述された **permit** 行

   （注）　センサーのブロックを許可している場合、この行は ACL に含まれません。

2. Pre-Block ACL（指定されている場合）

   この ACL は、すでにデバイスに存在している必要があります。

   （注）　ARC は ACL 内の行を読み取り、それらの行を ACL の先頭にコピーします。

3. アクティブなブロックがある場合、そのブロック
4. 次のいずれか
   - Post-Block ACL（指定されている場合）

     この ACL は、すでにデバイスに存在している必要があります。

     （注）　ARC は ACL 内の行を読み取り、それらの行を ACL の末尾にコピーします。

（注）　一致しないすべてのパケットを許可するには、ACL の最終行を **permit ip any any** にしてください。

- **permit ip any any**（Post-Block ACL を指定した場合は使用されません）

ARC は 2 つの ACL を使用してデバイスを管理します。アクティブな ACL は一度に 1 つだけです。オフラインの ACL 名を使用して新しい ACL が作成され、それがインターフェイスに適用されます。次のサイクルでは、ARC はこのプロセスを逆順で実行します。

注意　ARC が作成する ACL を、ユーザまたは他のシステムが変更してはいけません。これらの ACL は一時的なものであり、センサーによって新しい ACL が絶えず作成されています。Pre-Block ACL および Post-Block ACL にのみ変更を加えることができます。

Pre-Block ACL または Post-Block ACL を修正する必要がある場合は、次の手順を実行します。

1. センサーでブロッキングをディセーブルにします。
2. デバイスの設定に変更を加えます。
3. センサーでブロッキングを再びイネーブルにします。

ブロッキングが再度イネーブルになると、センサーは新しいデバイス コンフィギュレーションを読み取ります。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。その場合は、マスター ブロッキング センサーを使用してください。

詳細情報

- ブロッキングをイネーブルにする手順については、「ブロッキング プロパティの設定」（P.14-7）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

センサーで Cisco ルータを管理するための設定

ここでは、Cisco ルータを管理できるようにセンサーを設定する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。

- 「ルータと ACL」（P.14-23）
- 「センサーで Cisco ルータを管理するための設定」（P.14-24）

ルータと ACL

（注）　Pre-Block ACL と Post-Block ACLS は、レート制限には適用されません。

Pre-Block ACL と Post-Block ACL は、ルータのコンフィギュレーション内に作成し、保存します。これらの ACL は名前付きまたは番号付きの拡張 IP ACL にする必要があります。ACL の作成の詳細については、ルータのマニュアルを参照してください。[Pre-Block ACL] と [Post-Block ACL] の各フィールドに、ルータですでに設定されているこれら ACL の名前を入力します。

Pre-Block ACL は、主にブロック対象外のものを許可するために使用されます。この ACL を使用してパケットがチェックされるとき、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block ACL の許可の行である場合、ACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block ACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block ACL は、同じインターフェイスまたは方向に対して、追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合、その ACL を Post-Block ACL として使用できます。Post-Block ACL がない場合、センサーは新しい ACL の末尾に **permit ip any any** を挿入します。

センサーが起動すると、2 つの ACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の ACL が作成されます。

- センサーの IP アドレスに対応する **permit** 行
- Pre-Block ACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block ACL のすべての設定行のコピー

センサーは新しい ACL を、指定したインターフェイスと方向に適用します。

（注） 新しい ACL がルータのインターフェイスまたは方向に適用されると、そのインターフェイスまたは方向に対する他の ACL が適用されなくなります。

センサーで Cisco ルータを管理するための設定

Cisco ルータを管理できるようにセンサーを設定し、ブロッキングおよびレート制限を実行するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるルータの IP アドレスを設定します。

```
ips-ssp(config-net)# router-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成した論理デバイス名を入力します。

```
ips-ssp(config-net-rou)# profile-name user_profile_name
```

ARC はどのような入力内容も受け入れます。そのユーザ プロファイルが存在するかどうかは確認されません。

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-rou)# communication {telnet | ssh-3des}
```

（注）　3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-rou)# nat-address nat_address
```

（注）　これによって ACL の 1 行目の IP アドレスが、センサーのアドレスから NAT アドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　ルータがブロッキングまたはレート制限、あるいはその両方を実行するかどうかを指定します。

（注）　デフォルトはブロッキングです。ルータでブロッキングだけを実行する場合、応答機能を設定する必要はありません。

a.　レート制限のみの場合

```
ips-ssp(config-net-rou)# response-capabilities rate-limit
```

b.　ブロッキングとレート制限の場合

```
ips-ssp(config-net-rou)# response-capabilities block|rate-limit
```

ステップ 8　インターフェイス名と方向を指定します。

```
ips-ssp(config-net-rou)# block-interfaces interface_name {in | out}
```

注意　インターフェイス名はインターフェイスの完全な名前か、ルータが **interface** コマンドを使用して認識できる省略名のいずれかでなければなりません。

ステップ 9　（任意）pre-ACL 名を追加します（ブロッキングのみ）。

```
ips-ssp(config-net-rou-blo)# pre-acl-name pre_acl_name
```

ステップ 10　（任意）post-ACL 名を追加します（ブロッキングのみ）。

```
ips-ssp(config-net-rou-blo)# post-acl-name post_acl_name
```

ステップ 11　設定を確認できます。

```
ips-ssp(config-net-rou-blo)# exit
ips-ssp(config-net-rou)# show settings
   ip-address: 192.0.2.1
   -----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      -----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         -----------------------------------------------
            pre-acl-name: <defaulted>
```

```
            post-acl-name: <defaulted>
          ------------------------------------------------
        ----------------------------------------------
        response-capabilities: block|rate-limit default: block
      ------------------------------------------
ips-ssp(config-net-rou)#
```

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-rou)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定

ここでは、Cisco スイッチを管理できるようにセンサーを設定する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。

- 「スイッチと VACL」（P.14-26）
- 「センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定」（P.14-27）

スイッチと VACL

ARC を設定して、Cisco Catalyst ソフトウェアの実行時にスイッチ自体の VACL を使用してブロッキングするか、あるいは Cisco IOS ソフトウェアの実行時に MSFC またはスイッチ自体のルータ ACL を使用してブロッキングすることができます。ここでは、VACL を使用したブロッキングについて説明します。VACL を使用するスイッチがレート制限を実行するように設定することはできません。Catalyst 6500 シリーズ スイッチでブロッキング インターフェイスを設定し、ブロックするトラフィックの VLAN を指定する必要があります。

スイッチのコンフィギュレーション内に Pre-Block VACL と Post-Block VACL を作成し、保存します。これらの VACL は、名前付きまたは番号付きの拡張 IP VACL にする必要があります。VACL の作成の詳細については、スイッチのマニュアルを参照してください。[Pre-Block VACL] と [Post-Block VACL] の各フィールドに、スイッチですでに設定されている VACL の名前を入力します。

Pre-Block VACL は、主としてセンサーでブロックの対象外とするものを許可するために使用されます。VACL でパケットが確認されると、最初に一致した行によってアクションが決定されます。最初に一致した行が Pre-Block VACL の permit 行の場合、VACL の後の部分に（自動ブロックの）deny 行があっても、そのパケットは許可されます。Pre-Block VACL は、ブロックによって生じる deny 行をオーバーライドできます。

Post-Block VACL は、同じ LAN 上で追加のブロッキングまたは許可を行う場合に最適です。センサーが管理する VLAN 上に既存の VACL がある場合、その既存 VACL を Post-Block VACL として使用することができます。Post-Block VACL がない場合、センサーは新しい VACL の末尾に **permit ip any any** を挿入します。

センサーは、起動すると 2 つの VACL の内容を読み込みます。そして、次のエントリが含まれた 3 つ目の VACL を作成します。

- センサーの IP アドレスに対応する **permit** 行
- Pre-Block VACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block VACL のすべての設定行のコピー

センサーは、指定された VLAN に新しい VACL を適用します。

（注）　新しい VACL がスイッチの VLAN に適用されると、その VLAN に対して他の VACL は適用されなくなります。

詳細情報

ルータ ACL を使用したブロッキングの設定手順については、「ブロッキングおよびレート制限デバイスの設定」（P.14-22）を参照してください。

センサーで Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータを管理するための設定

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理できるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるルータの IP アドレスを設定します。

```
ips-ssp(config-net)# cat6k-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成したユーザ プロファイル名を入力します。

```
ips-ssp(config-net-cat)# profile-name user_profile_name
```

（注）　ARC はどのような入力内容も受け入れます。論理デバイスが存在するかどうかのチェックは行いません。

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-cat)# communication {telnet | ssh-3des}
```

（注）　3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-cat)# nat-address nat_address
```

（注）　これによって ACL の 1 行目の IP アドレスが、センサーの IP アドレスから NAT のアドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　VLAN 番号を指定します。

```
ips-ssp(config-net-cat)# block-vlans vlan_number
```

ステップ 8　（任意）pre-VACL 名を追加します。

```
ips-ssp(config-net-cat-blo)# pre-vacl-name pre_vacl_name
```

ステップ 9　（任意）post-VACL 名を追加します。

```
ips-ssp(config-net-cat-blo)# post-vacl-name post_vacl_name
```

ステップ 10　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-cat-blo)# exit
ips-ssp(config-net-cat)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーで Cisco ファイアウォールを管理するための設定

Cisco ファイアウォールを管理できるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)#
```

ステップ 3　ARC によって制御されるファイアウォールの IP アドレスを指定します。

```
ips-ssp(config-net)# firewall-devices ip_address
```

ステップ 4　ユーザ プロファイルの設定時に作成したユーザ プロファイル名を入力します。ARC はどのような入力内容も受け入れます。ARC は入力を受け入れず、論理デバイスが存在するかどうか確認します。

```
ips-ssp(config-net-fir)# profile-name user_profile_name
```

ステップ 5　センサーへのアクセスに使用する方法を指定します。指定しないと、SSH 3DES が使用されます。

```
ips-ssp(config-net-fir)# communication {telnet | ssh-3des}
```

（注）　3DES を使用している場合は、**ssh host-key** *ip_address* コマンドを使用してキーを受け入れる必要があります。そうでないと、ARC はデバイスに接続できません。

ステップ 6　センサーの NAT アドレスを指定します。

```
ips-ssp(config-net-fir)# nat-address nat_address
```

（注）　これによって ACL の 1 行目の IP アドレスが、センサーの IP アドレスから NAT のアドレスに変更されます。このアドレスは、管理対象のデバイスに設定された NAT アドレスではありません。これはセンサーが中間デバイスによって変換されたアドレス、つまり、センサーと管理対象デバイスの間にあるアドレスです。

ステップ 7　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-fir)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- ユーザ プロファイルの設定手順については、「ユーザ プロファイルの設定」（P.14-21）を参照してください。
- 既知のホスト リストにデバイスを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。

センサーをマスター ブロッキング センサーにする設定

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したマスター ブロッキング センサーに、ブロッキング要求を転送できます。マスター ブロッキング センサーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。マスター ブロッキング センサーの ARC は、他のセンサーで動作している ARC の要求に応じてデバイスでのブロッキングを制御します。マスター ブロッキング センサーは、レート制限を転送することもできます。

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをデバイス管理用のマスター ブロッキング センサーとして設定すると、もう一方のセンサーからマスター ブロッキング センサーに要求を転送できます。

マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス / 方向を持つ 10 個のファイアウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキング転送センサーで、マスター ブロッキング センサーとして機能するリモート ホストを特定します。マスター ブロッキング センサーでは、ブロッキング転送センサーをアクセス リストに追加する必要があります。

マスター ブロッキング センサーが Web 接続に TLS を必要とする場合は、マスター ブロッキング センサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。

（注）　通常、マスター ブロッキング センサーはネットワーク デバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。

ブロッキングまたはレート制限用に設定されたデバイスがなくても、ブロッキングまたはレート制限用に設定されたセンサーは、ブロッキングおよびレート制限要求をマスター ブロッキング センサーに転送することができます。ブロッキングまたはレート制限要求がイベント アクションとして設定されているシグニチャが起動した場合、センサーはブロック要求またはレート制限要求をマスター ブロッキング センサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

注意　1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

サービス ネットワーク アクセス サブモードで **master-blocking-sensors** *mbs_ip_address* コマンドを使用して、マスター ブロッキング センサーを設定します。

オプション

次のオプションが適用されます。

- *master_blocking_sensor_ip_address*：ブロック要求を転送するセンサーの IP アドレスを指定します。
- **password**：ブロック要求を転送するセンサーのアカウント パスワードを指定します。
- **port**：ブロック要求を転送するセンサーのポートを指定します。
- **tls {true | false}**：リモート センサーに TLS が必要な場合は true、それ以外の場合は false に設定します。
- **password**：ブロック要求を転送するセンサーのアカウント名を指定します。

マスター ブロッキング センサーの設定

センサーの ARC がマスター ブロッキング センサーにブロックを転送するように設定するには、次の手順を実行します。

ステップ 1　マスター ブロッキング センサーとブロッキング転送センサーの両方で、管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　両方のセンサーでコンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　必要に応じて TLS を設定します。

a. マスター ブロッキング センサーで TLS が必要かどうかと、使用されるポート番号を確認します。enable-tls が true の場合はステップ b に進みます。

```
ips-ssp(config)# service web-server
ips-ssp(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
ips-ssp(config-web)#
```

b. ブロッキング転送センサーで、マスター ブロッキング センサーの X.509 証明書を受け入れるように設定します。

```
ips-ssp(config-web)# exit
ips-ssp(config)# tls trusted-host ip-address master_blocking_sensor_ip_address port
port_number
```

例

```
ips-ssp(config)# tls trusted-host ip-address 192.0.2.1 port 8080

Certificate MD5 fingerprint is
F4:4A:14:BA:84:F4:51:D0:A4:E2:15:38:7E:77:96:D8Certificate SHA1 fingerprint is
84:09:B6:85:C5:43:60:5B:37:1E:6D:31:6A:30:5F:7E:4D:4D:E8:B2

Would you like to add this to the trusted certificate table for this host?[yes]:
```

（注）　証明書のフィンガープリントに基づいて証明書を受け入れるよう求めるプロンプトが表示されます。センサーが提供するのは、自己署名証明書（認識された認証局の署名がある証明書ではなく）だけです。マスター ブロッキング センサーのホスト センサーの証明書を確認するには、そのホスト センサーにログインし、**show tls fingerprint** コマンドを入力して、ホスト証明書のフィンガープリントと一致することを確認します。

ステップ 4　**yes** を入力して、マスター ブロッキング センサーの証明書を受け入れます。

ステップ 5　ネットワーク アクセス モードを開始します。

```
ips-ssp(config)# service network-access
```

ステップ 6　一般サブモードを開始します。

```
ips-ssp(config-net)# general
```

ステップ 7　マスター ブロッキング センサーのエントリを追加します。

```
ips-ssp(config-net-gen)# master-blocking-sensors master_blocking_sensor_ip_address
```

ステップ 8　マスター ブロッキング センサー ホストの管理アカウントのユーザ名を指定します。

```
ips-ssp(config-net-gen-mas)# username username
```

ステップ 9　このユーザのパスワードを指定します。

```
ips-ssp(config-net-gen-mas)# password
Enter password []: *****
Re-enter mbs-password []: *****
ips-ssp(config-net-gen-mas)#
```

ステップ 10　ホストの HTTP 通信用のポート番号を指定します。

```
ips-ssp(config-net-gen-mas)# port port_number
```

指定しない場合のデフォルトは 80/443 です。

ステップ 11　ホストが TLS/SSL を使用するかどうかを指定します。

```
ips-ssp(config-net-gen-mas)# tls {true | false}
ips-ssp(config-net-gen-mas)
```

（注）　値を true に設定する場合は、**tls trusted-host ip-address** *master_blocking_sens0r_ip_address* コマンドを使用する必要があります。

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
ips-ssp(config-net-gen-mas)# exit
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
ips-ssp(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ステップ 14　マスター ブロッキング センサーで、ブロック転送センサーの IP アドレスをアクセス リストに追加します。

詳細情報

ブロッキング転送センサーの IP アドレスをアクセス リストに追加する手順については、「アクセス リストの変更」（P.4-5）を参照してください。

ホスト ブロッキングの設定

特権 EXEC モードで **block host** *ip-address* [**timeout** *minutes*] コマンドを使用して、ホストをブロックします。ホストのブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、ホスト ブロックの設定前に行う必要があります。ブロックされているホストのリストを表示することもできます。

（注）　ホスト ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *ip-address*：ブロックするホストの IP アドレスを指定します。
- *minutes*：（任意）ホスト ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

ホストのブロッキング

ホストをブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、15 分間のホスト ブロックを設定します。このホスト ブロックは 15 分で終了します。

```
ips-ssp# block host 192.0.2.1 timeout 15
```

ステップ 3　ホスト ブロックを開始します。このホスト ブロックは削除されるまで継続されます。

```
ips-ssp# block host 192.0.2.1
```

ステップ 4　ホスト ブロックを終了します。

```
ips-ssp# no block host 192.0.2.1
ips-ssp#
```

ネットワーク ブロッキングの設定

特権 EXEC モードで **block network** *ip-address/netmask* [**timeout** *minutes*] コマンドを使用して、ネットワークをブロックします。ネットワークのブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、ネットワーク ブロックの設定前に行う必要があります。ブロックされているネットワークのリストを表示することもできます。

（注）　ネットワーク ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *ip-address/netmask*：ブロックするネットワークのサブネットを *X.X.X.X/nn* 形式で指定します。*X.X.X.X* はセンサーの IP アドレスで、ピリオドで区切られた 4 オクテットで記述される 32 ビット アドレスです。*X* は 0 ～ 255、*nn* はネットマスクのビット数（1032）を示します。
- *minutes*：（任意）ネットワーク ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

ネットワークのブロッキング

ネットワークをブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、15 分間のネットワーク ブロックを設定します。このネットワーク ブロックは 15 分で終了します。

```
ips-ssp# block network 192.0.2.0/24 timeout 15
```

ステップ 3　ネットワーク ブロックを開始します。このネットワーク ブロックは削除されるまで継続されます。

```
ips-ssp# block network 192.0.2.0/24
```

ステップ 4　ネットワーク ブロックを終了します。

```
ips-ssp# no block network 192.0.2.0/24
ips-ssp#
```

接続ブロッキングの設定

特権 EXEC モードで **block connection** *source-ip-address destination-ip-address* [**port** *port-number*] [**protocol** *type*] [**timeout** *minutes*] コマンドを使用して、2 つの IP アドレス間の接続をブロックします。接続ブロックを削除するには、このコマンドの **no** 形式を使用します。ブロッキングの設定は、接続ブロックの設定前に行う必要があります。ブロックされている接続のリストを表示することもできます。

（注）　接続ブロックの時間を設定しない場合、そのブロックは永続的に実行されます。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロックはサポートされません。適応型セキュリティ アプライアンスでは、接続情報が追加されたホスト ブロックだけがサポートされます。

オプション

次のオプションが適用されます。

- *source-ip-address*：接続ブロックでの送信元 IP アドレスを指定します。
- *destination-ip-address*：接続ブロックでの宛先 IP アドレスを指定します。
- *port-number*：（任意）宛先ポート番号を指定します。有効な範囲は 0 ～ 65535 です。
- *type*：（任意）プロトコル タイプを指定します。有効なタイプは **tcp** または **udp** です。
- *minutes*：（任意）接続ブロックの時間を分単位で指定します。指定できる範囲は 0 ～ 70560 分です。

接続のブロッキング

接続をブロックするには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、ポート、プロトコル、時間を指定して、送信元 IP アドレスと宛先 IP アドレス間の接続ブロックを設定します。この接続ブロックは 30 分で終了します。

```
ips-ssp# block connection 10.0.0.0 172.16.0.0 port 80 protocol tcp timeout 30
```

ステップ 3　接続ブロックを開始します。この接続ブロックは削除されるまで継続されます。

```
ips-ssp# block connection 10.0.0.0 172.16.0.0
```

ステップ 4　接続ブロックを終了します。

```
ips-ssp# no block connection 10.0.0.0
ips-ssp#
```

ブロックされているホストおよび接続のリストの取得

show statistics コマンドを使用して、ブロックされているホストと接続のリストを取得します。

ブロックされているホストおよび接続のリストを取得するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を確認します。`Host` エントリは、ブロックされているホストと、ブロックの時間を示しています。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.1.1.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
```

```
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.1.1.1
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   BlockedAddr
      Host
         IP = 192.168.1.1
         Vlan =
         ActualIp =
         BlockMinutes = 80
         MinutesRemaining = 76
```

CHAPTER 15

SNMP の設定

（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、SNMP を設定する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。

- 「SNMP について」（P.15-1）
- 「SNMP の設定」（P.15-2）
- 「SNMP トラップの設定」（P.15-4）
- 「サポート対象 MIB」（P.15-6）

注意 センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

SNMP について

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

SNMP は、簡易な要求および応答プロトコルです。ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。この動作は、4 つのプロトコル動作、Get、GetNext、Set、および Trap の 1 つを使用することにより実現されます。

SNMP によるモニタ用にセンサーを設定できます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、マネージャは、エージェントを直接ポーリングするか、他の関連デバイス エージェントをポーリングしてイベントについて理解を深められます。

（注） トラップで指示される通知は、重要でない SNMP 要求を除外することによって、ネットワーク リソースおよびエージェント リソースの大幅な節約をもたらします。ただし、SNMP ポーリングを完全には排除できません。SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

SNMP の設定

注意 センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

サービス通知サブモードで一般的な SNMP パラメータを設定します。

オプション

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **enable-set-get {true | false}**：オブジェクト ID（OID）の **get** および **set** をイネーブルにします。
- **no**：エントリまたは選択の設定を削除します。
- **read-only-community**：SNMP エージェントに読み取り専用のコミュニティ名を指定します。デフォルトは public です。
- **read-write-community**：SNMP エージェントに読み書き可能なコミュニティ名を指定します。デフォルトは private です。
- **snmp-agent-port**：SNMP エージェントがリッスンするポートを指定します。デフォルトの SNMP ポート番号は 161 です。
- **snmp-agent-protocol**：SNMP エージェントが通信に使用するプロトコルを指定します。デフォルト プロトコルは UDP です。
- **system-contact**：このセンサーの連絡先情報を指定します。system-contact オプションは、SNMPv2-MIB::sysContact.0 値を変更します。
- **system-location**：センサーの場所を指定します。system-location オプションは、SNMPv2-MIB::sysLocation.0 値を変更します。

SNMP の一般的なパラメータの設定

SNMP の一般的なパラメータを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　通知サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(config-not)#
```

ステップ 3　SNMP 管理ワークステーションがセンサー SNMP エージェントに要求を発行できるように、SNMP をイネーブルにします。

```
ips-ssp(config-not)# enable-set-get true
```

ステップ 4　SNMP エージェントパラメータを指定します。これらの値はセンサー SNMP エージェントのコミュニティ名を設定します。コミュニティ名は、SNMP 照会の強力でない認証に使用されるプレーン テキストのパスワード メカニズムです。

a. 読み取り専用のコミュニティ ストリングを割り当てます。読み取り専用のコミュニティ名には、SNMP エージェントに対する照会用のパスワードを指定します。

```
ips-ssp(config-not)# read-only-community PUBLIC1
```

b. 読み書き可能なコミュニティ ストリングを割り当てます。読み書き可能なコミュニティ名には、SNMP エージェントに対する **set** 用のパスワードを指定します。

```
ips-ssp(config-not)# read-write-community PRIVATE1
```

（注）　管理ワークステーションは、センサーにある、センサー SNMP エージェントに対して SNMP 要求を送信します。管理ワークステーションが要求を発行して、コミュニティ ストリングがセンサーのものと一致しない場合、センサーは要求を拒否します。

c. センサーの連絡先ユーザ ID を割り当てます。

```
ips-ssp(config-not)# system-contact BUSINESS
```

d. センサーの場所を入力します。

```
ips-ssp(config-not)# system-location AUSTIN
```

e. センサー SNMP エージェントのポートを入力します。

```
ips-ssp(config-not)# snmp-agent-port 161
```

（注）　ポートまたはプロトコルを変更する場合は、センサーをリブートする必要があります。

f. センサー SNMP エージェントが使用するプロトコルを指定します。

```
ips-ssp(config-not)# snmp-agent-protocol udp
```

（注）　ポートまたはプロトコルを変更する場合は、センサーをリブートする必要があります。

ステップ 5　設定を確認できます。

```
ips-ssp(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: public <defaulted>
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
ips-ssp(config-not)#
```

ステップ 6　通知サブモードを終了します。

```
ips-ssp(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 7　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

アクションをシグニチャに割り当てる手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。

SNMP トラップの設定

注意　センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして **request-snmp-trap** も選択する必要があります。

サービス通知サブモードで SNMP トラップを設定します。

オプション

次のオプションが適用されます。

- **enable-detail-traps {true | false}**：サイズの制限がない詳細トラップの送信をイネーブルにします。他のトラップはスパース モード（484 バイト未満）で送信されます。
- **enable-notifications {true | false}**：イベント通知をイネーブルにします。
- **error-filter {warning | error | fatal}**：SNMP トラップを生成するエラーを決定します。SNMP トラップは、フィルタに一致するすべての evError イベントについて生成されます。デフォルトはエラーおよび重大です。
- **trap-community-name**：トラップの宛先を定義する際に名前を指定しない場合は、トラップを送信する際に使用されるコミュニティ名を指定します。

- **trap-destinations**：シグニチャ アクションから生成されたエラー イベントおよびアラート イベントを送信する宛先を定義します。
  - **trap-community-name**：トラップを送信する際に使用されるコミュニティ名を指定します。コミュニティ名を指定しない場合は、一般トラップのコミュニティ名が使用されます。
  - **trap-port**：SNMP トラップを送信するポート番号を指定します。

SNMP トラップの設定

SNMP トラップを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　通知サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(config-not)#
```

ステップ 3　SNMP トラップをイネーブルにします。

```
ips-ssp(config-not)# enable-notifications true
```

ステップ 4　SNMP トラップ用に次のパラメータを指定します。

a. SNMP トラップを介して通知するエラー イベントを指定します。

```
ips-ssp(config-not)# error-filter {error | warning | fatal}
```

（注） **error-filter [error | warning | fatal]** コマンドには、エラー、警告、および重大トラップが含まれます。このコマンドは重大度に基づいてトラップをフィルタ処理します（除去しません）。

b. 詳細 SNMP トラップが必要かどうかを指定します。

```
ips-ssp(config-not)# enable-detail-traps true
```

c. 詳細トラップに含めるコミュニティ ストリングを入力します。

```
ips-ssp(config-not)# trap-community-name TRAP1
```

ステップ 5　センサーがこれらのトラップを送信する管理ワークステーションを認識するように、SNMP トラップ宛先のパラメータを指定します。

a. SNMP 管理ステーションの IP アドレスを入力します。

```
ips-ssp(config-not)# trap-destinations 10.0.0.0
```

b. SNMP 管理ステーションの UDP ポートを入力します。デフォルトは 162 です。

```
ips-ssp(config-not-tra)# trap-port 162
```

c. トラップ コミュニティ ストリングを入力します。

```
ips-ssp(config-not-tra)# trap-community-name AUSTIN_PUBLI
```

（注） コミュニティ ストリングはトラップに含まれていて、複数のエージェントから複数のトラップ タイプを受信する場合に役立ちます。たとえば、ルータまたはセンサーはトラップを送信できるので、コミュニティ ストリング内にルータまたはセンサーを特別に識別するものを入れておくと、コミュニティ ストリングに基づいてトラップをフィルタ処理できます。

ステップ 6　設定を確認できます。

```
ips-ssp(config-not-tra)# exit
ips-ssp(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 1)
   -----------------------------------------------
      ip-address: 10.1.1.1
      -------------------------------------------
         trap-community-name: AUSTIN_PUBLIC default:
         trap-port: 161 default: 162
      -------------------------------------------
   -----------------------------------------------
   error-filter: warning|error|fatal default: error|fatal
   enable-detail-traps: true default: false
   enable-notifications: true default: false
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: PUBLIC1 default: public
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
ips-ssp(config-not)#
```

ステップ 7　通知サブモードを終了します。

```
ips-ssp(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 8　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

アクションをシグニチャに割り当てる手順については、「シグニチャへのアクションの割り当て」（P.7-16）を参照してください。

サポート対象 MIB

センサーでは、次のプライベート MIB がサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注） MIB II はセンサーで使用できますが、シスコではサポートしていません。一部の要素が正確でないことがわかっています（たとえば、センシング インターフェイスの IF MIB からのパケット カウントなど）。MIB II の要素を使用できますが、シスコでは、それらがすべて正確な情報を提供することを保証していません。シスコは、リストにあるその他の MIB を完全サポートしていますし、それらの出力も正確です。

これらのプライベートの Cisco MIB は、次の URL の [SNMP v2 MIBs] という見出しの下で確認できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 16

コンフィギュレーション ファイルの操作

（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、コンフィギュレーション ファイルの表示、コピー、および消去を実行するコマンド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。

- 「現在の設定の表示」（P.16-1）
- 「現在のサブモード コンフィギュレーションの表示」（P.16-3）
- 「現在の設定の出力のフィルタ処理」（P.16-16）
- 「現在のサブモード コンフィギュレーションの出力のフィルタ処理」（P.16-18）
- 「論理ファイルの内容の表示」（P.16-19）
- 「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.16-22）
- 「バックアップ コンフィギュレーション ファイルの作成と使用」（P.16-24）
- 「コンフィギュレーション ファイルの消去」（P.16-25）

現在の設定の表示

show configuration または **more current-config** コマンドを使用して、現在の設定の内容を表示します。

現在の設定の内容を表示する手順は、次のとおりです。

ステップ 1 CLI にログインします。

ステップ 2 現在の設定を表示します。

```
ips-ssp# show configuration
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
```

```
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
```

```
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
ips-ssp#
```

現在のサブモード コンフィギュレーションの表示

サブモードで **show settings** コマンドを使用して、そのサブモードの現在の設定を表示します。

サブモードの現在の設定を表示する手順は、次のとおりです。

ステップ 1　CLI にログインします。

ステップ 2　サービス分析エンジン サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -------------------------------------------
         max-open-iplog-files: 20 <defaulted>
```

```
      ------------------------------------------------
   ------------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   ------------------------------------------------
      <protected entry>
      name: vs0 <defaulted>
      ------------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         physical-interface (min: 0, max: 999999999, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         logical-interface (min: 0, max: 999999999, current: 0)
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
ips-ssp(config-ana)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 3　サービス異常検出サブモードの現在の設定を表示します。

```
ips-ssp(config)# service anomaly-detection ad0
ips-ssp(config-ano)# show settings
   worm-timeout: 600 seconds <defaulted>
   learning-accept-mode
   ------------------------------------------------
      auto
      ------------------------------------------------
         action: rotate <defaulted>
         schedule
         ------------------------------------------------
            periodic-schedule
            ------------------------------------------------
               start-time: 10:00:00 <defaulted>
               interval: 24 hours <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   internal-zone
   ------------------------------------------------
      enabled: true <defaulted>
      ip-address-range: 0.0.0.0 <defaulted>
      tcp
      ------------------------------------------------
         dst-port (min: 0, max: 65535, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
```

```
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
   udp
   ------------------------------------------------
      dst-port (min: 0, max: 65535, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 100 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
   other
   ------------------------------------------------
      protocol-number (min: 0, max: 255, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 100 <defaulted>
         threshold-histogram (min: 0, max: 3, current: 3)
         ------------------------------------------------
            <protected entry>
            dest-ip-bin: low <defaulted>
            num-source-ips: 10 <defaulted>
            <protected entry>
            dest-ip-bin: medium <defaulted>
            num-source-ips: 1 <defaulted>
            <protected entry>
            dest-ip-bin: high <defaulted>
            num-source-ips: 1 <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      enabled: true <defaulted>
   ------------------------------------------------
------------------------------------------------
illegal-zone
------------------------------------------------
   enabled: true <defaulted>
   ip-address-range: 0.0.0.0 <defaulted>
   tcp
   ------------------------------------------------
      dst-port (min: 0, max: 65535, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      default-thresholds
      ------------------------------------------------
         scanner-threshold: 100 <defaulted>
```

```
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
      udp
      ------------------------------------------------
         dst-port (min: 0, max: 65535, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
      other
      ------------------------------------------------
         protocol-number (min: 0, max: 255, current: 0)
         ------------------------------------------------
         ------------------------------------------------
         default-thresholds
         ------------------------------------------------
            scanner-threshold: 100 <defaulted>
            threshold-histogram (min: 0, max: 3, current: 3)
            ------------------------------------------------
               <protected entry>
               dest-ip-bin: low <defaulted>
               num-source-ips: 10 <defaulted>
               <protected entry>
               dest-ip-bin: medium <defaulted>
               num-source-ips: 1 <defaulted>
               <protected entry>
               dest-ip-bin: high <defaulted>
               num-source-ips: 1 <defaulted>
            ------------------------------------------------
         ------------------------------------------------
         enabled: true <defaulted>
      ------------------------------------------------
   ------------------------------------------------
   external-zone
   ------------------------------------------------
```

```
enabled: true <defaulted>
tcp
-----------------------------------------------
   dst-port (min: 0, max: 65535, current: 0)
   -------------------------------------------
   -------------------------------------------
   default-thresholds
   -------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      -----------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
         dest-ip-bin: high <defaulted>
         num-source-ips: 1 <defaulted>
      -----------------------------------------
   -------------------------------------------
   enabled: true <defaulted>
-----------------------------------------------
udp
-----------------------------------------------
   dst-port (min: 0, max: 65535, current: 0)
   -------------------------------------------
   -------------------------------------------
   default-thresholds
   -------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      -----------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
         dest-ip-bin: high <defaulted>
         num-source-ips: 1 <defaulted>
      -----------------------------------------
   -------------------------------------------
   enabled: true <defaulted>
-----------------------------------------------
other
-----------------------------------------------
   protocol-number (min: 0, max: 255, current: 0)
   -------------------------------------------
   -------------------------------------------
   default-thresholds
   -------------------------------------------
      scanner-threshold: 100 <defaulted>
      threshold-histogram (min: 0, max: 3, current: 3)
      -----------------------------------------
         <protected entry>
         dest-ip-bin: low <defaulted>
         num-source-ips: 10 <defaulted>
         <protected entry>
         dest-ip-bin: medium <defaulted>
         num-source-ips: 1 <defaulted>
         <protected entry>
```

```
                dest-ip-bin: high <defaulted>
                num-source-ips: 1 <defaulted>
             -----------------------------------------------
          -------------------------------------------------
          enabled: true <defaulted>
       -----------------------------------------------
    -------------------------------------------------
    ignore
    -------------------------------------------------
       enabled: true <defaulted>
       source-ip-address-range: 0.0.0.0 <defaulted>
       dest-ip-address-range: 0.0.0.0 <defaulted>
    -------------------------------------------------
ips-ssp(config-ano)# exit
ips-ssp(config)# exit
ips-ssp# exit
```

ステップ 4　サービス認証サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service authentication
ips-ssp(config-aut)# show settings
   attemptLimit: 0 <defaulted>
   password-strength
   -----------------------------------------------
      size: 8-64 <defaulted>
      digits-min: 0 <defaulted>
      uppercase-min: 0 <defaulted>
      lowercase-min: 0 <defaulted>
      other-min: 0 <defaulted>
      number-old-passwords: 0 <defaulted>
   -----------------------------------------------
ips-ssp(config-aut)#
```

ステップ 5　サービス イベント アクション規則サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
ips-ssp(config-rul)# show settings
   variables (min: 0, max: 256, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   overrides (min: 0, max: 12, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
   -----------------------------------------------
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 30 <defaulted>
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
   target-value (min: 0, max: 5, current: 0)
   -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-rul)# exit
ips-ssp(config)# exit
ips-ssp# exit
```

ステップ 6　外部製品インターフェイス サブモードの現在の設定を表示します。

```
ips-ssp(config)# service external-product-interface
ips-ssp(config-ext)# show settings
   cisco-security-agents-mc-settings (min: 0, max: 2, current: 0)
   -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ext)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 7　サービス グローバル相関サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service global-correlation
ips-ssp(config-glo)# show settings
   network-participation: off <defaulted>
   global-correlation-inspection: on <defaulted>
   global-correlation-inspection-influence: standard <defaulted>
   reputation-filtering: on <defaulted>
   test-global-correlation: off <defaulted>
ips-ssp(config-glo)# exit
ips-ssp(config)# exit
ips-ssp# exit
```

ステップ 8　サービス ヘルスモニタリング サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service health-monitor
ips-ssp(config-hea)# show settings
   enable-monitoring: true <defaulted>
   persist-security-status: 5 minutes <defaulted>
   heartbeat-events
   -----------------------------------------------
      enable: 300 seconds <defaulted>
   -----------------------------------------------
   application-failure-policy
   -----------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   -----------------------------------------------
   bypass-policy
   -----------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   -----------------------------------------------
   interface-down-policy
   -----------------------------------------------
      enable: true <defaulted>
      status: red <defaulted>
   -----------------------------------------------
   inspection-load-policy
   -----------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 80 percent <defaulted>
      red-threshold: 91 percent <defaulted>
   -----------------------------------------------
   missed-packet-policy
   -----------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 1 percent <defaulted>
      red-threshold: 6 percent <defaulted>
   -----------------------------------------------
   memory-usage-policy
   -----------------------------------------------
```

```
      enable: false <defaulted>
      yellow-threshold: 80 percent <defaulted>
      red-threshold: 91 percent <defaulted>
   ------------------------------------------------
   signature-update-policy
   ------------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 30 days <defaulted>
      red-threshold: 60 days <defaulted>
   ------------------------------------------------
   license-expiration-policy
   ------------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 30 days <defaulted>
      red-threshold: 0 days <defaulted>
   ------------------------------------------------
   event-retrieval-policy
   ------------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 300 seconds <defaulted>
      red-threshold: 600 seconds <defaulted>
   ------------------------------------------------
   global-correlation-policy
   ------------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 86400 seconds <protected>
      red-threshold: 259200 seconds <protected>
   ------------------------------------------------
   network-participation-policy
   ------------------------------------------------
      enable: false <defaulted>
      yellow-threshold: 1 connection failures <protected>
      red-threshold: 6 connection failures <protected>
   ------------------------------------------------
ips-ssp(config-hea)# exit
ips-ssp(config)# exit
ips-ssp# exit
```

ステップ 9　サービス ホスト サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      ------------------------------------------------
         network-address: 10.0.0.0/8
         ------------------------------------------------
         network-address: 64.0.0.0/8
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
   time-zone-settings
   ------------------------------------------------
      offset: 0 minutes default: 0
      standard-time-zone-name: UTC default: UTC
   ------------------------------------------------
   ntp-option
```

```
   ------------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
   ------------------------------------------------
   summertime-option
   ------------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
   ------------------------------------------------
   auto-upgrade-option
   ------------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
   ------------------------------------------------
   crypto
   ------------------------------------------------
      key (min: 0, max: 10, current: 2)
      ---------------------------------------------
         <protected entry>
         name: realm-cisco.pub <defaulted>
         type
         ------------------------------------------
            rsa-pubkey
            ---------------------------------------
               length: 2048 <defaulted>
               exponent: 65537 <defaulted>
               modulus: 24442189989357747083874855335232628843599968934198559648
630199473878411519325039111726689401947545491553904076580203933306118912925083008
859403040311860144996325688124280680580895816141963373996230606249900570491030559
901539559350860600086797768080736401860634357232523755752931263045580687043018638
056211443743928906945667092207499582739028476161059151575200840514024367308318977
822469964934598367010389389888297490802884118543730076293589703535912161993319470
931302986888300125472155726463496235946883864106491531394780685290408235195513217
273138099965383039716130153270715220046567107828128924197692417332033911704 <defaulted>
            ---------------------------------------
         ---------------------------------------
         <protected entry>
         name: realm-trend.pub <defaulted>
         type
         ------------------------------------------
            rsa-pubkey
            ---------------------------------------
               length: 2048 <defaulted>
               exponent: 65537 <defaulted>
               modulus: 21765561422573021314159855351418723031625093380777053696
638172895270605709325510654898181907137456721482605270300606672083666066038026793043906672414339062649547930055010161817958463728705293646569214657261265137596920354521585644221602944203520804404212975401970895119903756769601133853673296766452897957779734919840565870452145148201133669507313464000443084915946264347069994760866882281401483006339953420464706950905244343952536370652725522451077112223580181150460544783251498481432705991010069844368525754878413669427639752950801767999053092352324562955800867242032979140959842243284443915822231384237991008381919 <defaulted>
            ---------------------------------------
         ---------------------------------------
      ---------------------------------------------
   ------------------------------------------------
ips-ssp(config-hos)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 10　サービス インターフェイス サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service interface
ips-ssp(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   -----------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      -----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      <protected entry>
      name: PortChannel0/0 <defaulted>
      -----------------------------------------------
         media-type: backplane <protected>
         description: <defaulted>
         admin-state: enabled <protected>
         duplex: full <protected>
         speed: 10000 <protected>
         alt-tcp-reset-interface
         -----------------------------------------------
            none
            -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   command-control: Management0/0 <protected>
   interface-notifications
   -----------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   -----------------------------------------------
ips-ssp(config-int)#
```

ステップ 11　サービス ロガー サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service logger
ips-ssp(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: false <defaulted>
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   -----------------------------------------------
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
```

```
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
   ------------------------------------------------
ips-ssp(config-log)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 12　サービス ネットワーク アクセス サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      rate-limit-max-entries: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
```

```
      never-block-networks (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   ---------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ---------------------------------------------
      profile-name: test
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: <defaulted>
      -----------------------------------------------
   ---------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   router-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
ips-ssp(config-net)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 13　通知サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service notification
ips-ssp(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: false <defaulted>
   snmp-agent-port: 161 <defaulted>
   snmp-agent-protocol: udp <defaulted>
   read-only-community: public <defaulted>
   read-write-community: private <defaulted>
   trap-community-name: public <defaulted>
   system-location: Unknown <defaulted>
   system-contact: Unknown <defaulted>
ips-ssp(config-not)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 14　シグニチャ定義サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)# show settings
   variables (min: 0, max: 256, current: 1)
   -----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
```

```
      ------------------------------------------------
         web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,2432
6-24326 <defaulted>
      ------------------------------------------------
   ------------------------------------------------
   application-policy
   ------------------------------------------------
      http-policy
      ------------------------------------------------
         http-enable: false <defaulted>
         max-outstanding-http-requests-per-connection: 10 <defaulted>
         aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
      ------------------------------------------------
      ftp-enable: false <defaulted>
   ------------------------------------------------
   fragment-reassembly
   ------------------------------------------------
      ip-reassemble-mode: nt <defaulted>
   ------------------------------------------------
   stream-reassembly
   ------------------------------------------------
--MORE--
```

ステップ 15　SSH 既知ホスト サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service ssh-known-hosts
ips-ssp(config-ssh)# show settings
   rsa1-keys (min: 0, max: 500, current: 0)
   ------------------------------------------------
   ------------------------------------------------
ips-ssp(config-ssh)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 16　信頼できる証明書サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service trusted-certificate
ips-ssp(config-tru)# show settings
   trusted-certificates (min: 0, max: 500, current: 1)
   ------------------------------------------------
      common-name: 192.0.2.3
      certificate: MIICJDCCAY0CCPbSkgXUchJIMA0GCSqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTA
lVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlTU00tSVBTMjAxFjAUBgNVB
AMTDTEwLjg5LjEzMC4xMDgwHhcNMDMwMTAzMDE1MjEwWhcNMDUwMTAzMDE1MjEwWjBXMQswCQYDVQQGE
wJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAGA1UECxMJU1NNLUlQUzIwMRYwFAYDV
QQDEw0xMC44OS4xMzAuMTA4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzldqLFG4MT4bfgh3mJ
fP/DCilnnaLfzHK9FdnhmWI4FY+9MVvAI7MOhAcuV6HYfyp6n6cYvH+Eswzl9uv7H5nouID9St9GI3Yr
SUtlIQAJ4QVL2DwWP230x6KdHrYqcj+Nmhc7AnnPypjidwGSfF+VetIJLEeRFh/mI2JcmwF2QIDAQABM
A0GCSqGSIb3DQEBBQUAA4GBAAUI2PLANTOehxvCfwd6UAFXvy8uifbjqKMC1jrrF+f9KGkxmR+XZvUaG
OS83FYDXlXJvB5Xyxms+Y01wGjzKKpxegBoan8OB8o193Ueszdpvz2xYmiEgywCDyVJRsw3hAFMXWMS5
XsBUiHtw0btHH0j7ElFZxUjZv12fGz8hlnY
   ------------------------------------------------
ips-ssp(config-tru)# exit
ips-ssp(config)# exit
ips-ssp#
```

ステップ 17　Web サーバ サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp(config)# service web-server
ips-ssp(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
ips-ssp(config-web)# exit
ips-ssp(config)# exit
ips-ssp#
```

現在の設定の出力のフィルタ処理

more *keyword* | [**begin** | **exclude** | **include**] *regular-expression* コマンドを使用して、コマンドの出力をさらに検索します。

オプション

次のオプションが適用されます。

- *keyword*：current-config または backup-config を指定します。
  - **current-config**：現在の実行コンフィギュレーションを指定します。コマンドが入力されると、この設定が維持されます。
  - **backup-config**：コンフィギュレーション バックアップ ファイル用の保管場所を指定します。
- |：パイプ記号は、そのあとに出力処理の指定が続くことを示します。
- **begin**：**more** コマンドのフィルタリングされていない出力を、指定された正規表現が含まれる最初の行から開始します。
- **exclude**：**more** コマンドの出力で、特定の正規表現が含まれる行を除外します。
- **include**：**more** コマンドの出力で、指定する正規表現が含まれる行のみを含めます。
- *regular-expression*：**more** コマンドの出力で、検出される正規表現を指定します。

（注）　*regular-expression* オプションは、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。

More コマンドの使用によるフィルタ処理

more コマンドをフィルタ処理するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば、正規表現「ip」で始まる current-config の出力をフィルタ処理します。

```
ips-ssp# more current-config | begin ip
generating current config:
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
```

```
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
service logger
master-control
enable-debug true
exit
exit
! ------------------------------
service network-access
general
log-all-block-events-and-errors true
--MORE--
```

（注）　Ctrl キーを押した状態で C キーを押して出力を停止して CLI プロンプトに戻ります。

ステップ 3　current-config の出力から正規表現「ip」を除外します。

```
ips-ssp# more current-config | exclude ip
generating current config:
! ------------------------------
! Version 7.1(1)
! Current configuration last modified Fri Aug 11 15:10:57 2010
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface FastEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-name ips-ssp
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
--MORE--
```

（注）　Ctrl キーを押した状態で C キーを押して出力を停止して CLI プロンプトに戻ります。

ステップ 4　current-config の出力に正規表現「ip」を含めます。

```
ips-ssp# more current-config | include ip
generating current config:
host-ip 192.0.2.0/24,192.0.2.17
engine atomic-ip
```

現在のサブモード コンフィギュレーションの出力のフィルタ処理

目的のサブモードで **show settings | [begin | exclude | include]** *regular_expression* コマンドを使用して、サブモード コンフィギュレーションの内容の出力の検索またはフィルタ処理を行います。

オプション

次のオプションが適用されます。

- **|** : パイプ記号は、そのあとに出力処理の指定が続くことを示します。
- **begin** : **show settings** コマンドのフィルタリングされていない出力を、指定された正規表現が含まれる最初の行から開始します。
- **exclude** : **show settings** コマンドの出力で、特定の正規表現が含まれる行を除外します。
- **include** : **show settings** コマンドの出力で、指定する正規表現が含まれる行のみを含めます。
- *regular_expression* : **show settings** コマンドの出力で検出される任意の正規表現を指定します。

（注）　*regular_expression* オプションは、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。

サブモードの出力のフィルタ処理

サブモード コンフィギュレーションの内容の出力の検索またはフィルタ処理をするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　たとえば正規表現「filters」についてイベント アクション規則設定の出力を検索します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules
ips-ssp(config-rul)# show settings | begin filters
filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
 ---------------------------------------------
 general
 ---------------------------------------------
    global-overrides-status: Enabled <defaulted>
    global-filters-status: Enabled <defaulted>
    global-summarization-status: Enabled <defaulted>
    global-metaevent-status: Enabled <defaulted>
    global-deny-timeout: 3600 <defaulted>
    global-block-timeout: 15 default: 30
    max-denied-attackers: 10000 <defaulted>
 ---------------------------------------------
 target-value (min: 0, max: 5, current: 0)
```

```
 -----------------------------------------------
 -----------------------------------------------
ips-ssp(config-rul)#
```

ステップ 3　ネットワーク アクセス設定の出力をフィルタ処理して正規表現を除外します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)# show settings | exclude false
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      block-enable: true default: true
      block-max-entries: 11 default: 250
      max-interfaces: 13 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 1)
      -----------------------------------------------
         ipaddress: 192.0.2.1
         -----------------------------------------------
            password: <hidden>
            port: 443 default: 443
            tls: true default: true
            username: cisco default:
         -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 10.89.146.112
         -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      -----------------------------------------------
         ip-address: 88.88.88.0/24
--MORE--
```

ステップ 4　ホスト設定の出力をフィルタ処理して正規表現「ip.」を含めます。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# show settings | include ip
      host-ip: 192.0.2.0/24,192.0.2.17 default: 192.168.1.2/24,192.168.1.1
ips-ssp(config-hos)#
```

論理ファイルの内容の表示

more *keyword* コマンドを使用して、現在のシステム設定または保存されたバックアップのシステム設定など、論理ファイルの内容を表示します。

オプション

次のオプションが適用されます。

- *keyword*：current-config または backup-config を指定します。
  - **current-config**：現在の実行コンフィギュレーションを指定します。コマンドが入力されると、この設定が維持されます。
  - **backup-config**：コンフィギュレーション バックアップ ファイル用の保管場所を指定します。

（注）　オペレータとビューアは、現在の設定のみ表示できます。管理者のみがパスワードなどの非表示フィールドを表示できます。

terminal length 0 コマンドを使用してターミナル長をゼロに設定することにより、**more current-config** または **more backup-config** で more prompt をディセーブルにできます。その結果、**more** コマンドは、ファイルの内容全体を一時停止せずに表示します。

論理ファイルの内容の表示

論理ファイルの内容を表示するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在のコンフィギュレーション ファイルの内容を表示します。

```
ips-ssp# more current-config
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,192.0.2.17
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
```

```
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
```

```
ips-ssp#
```

詳細情報

terminal コマンドを使用する手順については、「ターミナル プロパティの変更」（P.17-12）を参照してください。

リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元

（注）　アップグレードする前に現在のコンフィギュレーション ファイルをリモート サーバにコピーすることを推奨します。

copy [**/erase**] *source_url destination_url keyword* コマンドを使用して、コンフィギュレーション ファイルをリモート サーバにコピーします。その後、リモート サーバから現在の設定を復元できます。まず現在の設定をバックアップするプロンプトが表示されます。

オプション

次のオプションが適用されます。

- **/erase**：コピーする前にコピー先ファイルを消去します。

  このキーワードは、current-config だけに適用されます。backup-config は、常に上書きされます。このキーワードがコピー先の current-config に対して指定されている場合、コピー元の設定がシステムのデフォルト設定に適用されます。このキーワードがコピー先の current-config に対して指定されていない場合、コピー元の設定がその current-config にマージされます。

- *source_url*：コピー元のファイルの場所です。URL またはキーワードを使用できます。
- *destination_url*：コピー先のファイルの場所です。URL またはキーワードを使用できます。
- **current-config**：現在の実行コンフィギュレーションです。コマンドが入力されると、設定が維持されます。
- **backup-config**：コンフィギュレーション バックアップの保管場所です。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加することも必要です。

- http: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  http:[[/[username@]location]/directory]/filename
- https: : Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。
  https:[[/[username@]location]/directory]/filename

（注）　Web サイトにアクセスするのにユーザ名が必要な場合、HTTP および HTTPS によってパスワードが要求されます。HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

注意　センシング インターフェイスおよび仮想センサーが同じ設定になっていない場合、別のセンサーからのコンフィギュレーション ファイルのコピーは、エラーになる可能性があります。

現在の設定のリモート サーバへのバックアップ

現在の設定をリモート サーバにバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** を入力して、現在の設定をバックアップの設定にコピーします。

```
cfg            100% |*********************************************| 36124       00:00
```

バックアップ ファイルからの現在の設定の復元

バックアップ ファイルから現在の設定を復元するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** を入力して、現在の設定をバックアップの設定にコピーします。

```
cfg            100% |***********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

ステップ 4　現在設定されているホスト名、IP アドレス、サブネット マスク、管理インターフェイス、およびアクセス リストを保持するには、**no** を入力します。残りの設定が復元された後、センサーへのアクセスを確保するために、この情報を保持することを推奨します。

詳細情報

- リモート ホストを SSH 既知ホスト リストに追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- リモート ホストを TLS の信頼できるホストのリストに追加する手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

バックアップ コンフィギュレーション ファイルの作成と使用

設定を保護するために、現在の設定のバックアップを作成し、表示することによってそれが保存したい設定であることを確認できます。この設定を復元する必要があるときは、バックアップ コンフィギュレーション ファイルを現在の設定とマージするか、現在のコンフィギュレーション ファイルにバックアップ コンフィギュレーション ファイルを上書きします。

現在の設定をバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定を保存します。現在の設定がバックアップ ファイルに保存されます。

```
ips-ssp# copy current-config backup-config
```

ステップ 3　バックアップ コンフィギュレーション ファイルを表示します。バックアップ コンフィギュレーション ファイルが表示されます。

```
ips-ssp# more backup-config
```

ステップ 4　バックアップの設定を現在の設定とマージしたり、現在の設定を上書きしたりすることができます。

- バックアップの設定を現在の設定とマージします。

  ```
  ips-ssp# copy backup-config current-config
  ```

- バックアップの設定で現在の設定を上書きします。

  ```
  ips-ssp# copy /erase backup-config current-config
  ```

コンフィギュレーション ファイルの消去

erase {**backup-config** | **current-config**} コマンドを使用して、論理ファイルを削除します。

次のオプションが適用されます。

- **current-config**：現在の実行コンフィギュレーションです。コマンドが入力されると、設定が維持されます。
- **backup-config**：コンフィギュレーション バックアップの保管場所です。

現在の設定を消去して、すべての設定をデフォルトに戻すには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

```
ips-ssp# erase current-config
Warning: Removing the current-config file will result in all configuration being reset to
default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no username"
command.
Continue? []:
```

ステップ 2　Enter を押して、続行するか、**no** を入力して停止します。

CHAPTER 17

管理タスク

（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、センサーの管理面で役立つ手順について説明します。次のような構成になっています。

- 「IPS SSP パスワードの回復」（P.17-2）
- 「センサー データベースのクリア」（P.17-4）
- 「ヘルス ステータス情報の設定」（P.17-5）
- 「センサーの全体的なヘルス ステータスの表示」（P.17-10）
- 「バナー ログインの作成」（P.17-10）
- 「CLI セッションの終了」（P.17-11）
- 「ターミナル プロパティの変更」（P.17-12）
- 「イベントの設定」（P.17-13）
- 「システム クロックの表示」（P.17-16）
- 「拒否攻撃者リストのクリア」（P.17-17）
- 「ポリシー リストの表示」（P.17-19）
- 「統計情報の表示」（P.17-20）
- 「技術サポート情報の表示」（P.17-30）
- 「バージョン情報の表示」（P.17-31）
- 「ネットワークの接続性の診断」（P.17-34）
- 「コマンド履歴の表示」（P.17-34）
- 「IP パケットのルートのトレース」（P.17-35）
- 「サブモード設定の表示」（P.17-36）

IPS SSP パスワードの回復

ここでは、IPS SSP のパスワードを回復する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。

- 「IPS SSP パスワードの回復」（P.17-2）
- 「パスワード回復のディセーブル化」（P.17-3）
- 「パスワード回復の状態の確認」（P.17-3）
- 「パスワード回復のトラブルシューティング」（P.17-4）

IPS SSP パスワードの回復

（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。

CLI または ASDM を使用して IPS SSP のデフォルト（**cisco**）にパスワードをリセットできます。パスワードをリセットすると、IPS SSP がリブートします。リブート中は、IPS サービスを使用できません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、ROMMON confreg ビットを 0x7 に設定してから、IPS SSP をリブートします。この ROMMON ビットにより、GRUB メニューがデフォルトでオプション 2（**パスワードのリセット**）になります。

指定したスロット内の IPS SSP に搭載されている IPS のバージョンがパスワード回復をサポートしていない場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーから、[Tools] > [IPS Password Reset] を選択します。

（注）　このオプションは、IPS モジュールがインストールされていなければ表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで、[OK] をクリックしてパスワードをデフォルト（**cisco**）にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットに失敗した場合は、適応型セキュリティ アプライアンスに正しい ASA ソフトウェアが搭載されていること、および IPS SSP に IPS 7.1 以降が搭載されていることを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。IPS SSP がリブートします。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブル化されたセンサーでパスワードを回復しようとすると、プロセスはエラーや警告なしに進行しますが、パスワードはリセットされません。パスワードを忘れたためにセンサーにログインできず、パスワード回復がディセーブルに設定されている場合は、センサーのイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。CLI、IDM、または IME を使用してパスワード回復をディセーブルにできます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
ips-ssp# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
ips-ssp(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
ips-ssp(config-hos)# password-recovery disallowed
```

IDM または IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用し、IDM または IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復の状態の確認

show settings | **include password** コマンドを使用して、パスワード回復がイネーブルかどうかを確認します。

パスワード回復がイネーブルかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp (config)# service host
ips-ssp (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタリングされた出力で設定を表示することにより、パスワード回復の状態を確認します。

```
ips-ssp(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
ips-ssp(config-hos)#
```

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行うときは、次の点に注意します。

- ROMMON プロンプト、GRUB メニュー、スイッチ CLI、またはルータ CLI からは、センサー設定内でパスワード回復がディセーブルになっているかどうかを判別できません。パスワード回復を試みると、常に成功しているように見えます。ディセーブルになっていた場合、パスワードは **cisco** にリセットされません。この場合、センサーのイメージを再作成するしか方法はありません。
- パスワード回復は、ホスト設定でディセーブルにできます。外部メカニズムを使用するプラットフォームの場合、コマンドを実行してパスワードをクリアすることができますが、IPS でパスワード回復がディセーブルになっていると、IPS は、パスワード回復が許可されていないことを検出し、外部からの要求を拒否します。
- パスワード回復の状態を確認するには、**show settings | include password** コマンドを使用します。

センサー データベースのクリア

特権 EXEC モードで **clear database** [*virtual-sensor*] **all | nodes | alerts | inspectors** コマンドを使用して、センサー データベースの特定の部分をクリアします。**clear database** コマンドはトラブルシューティングとテストに有用です。

注意　TAC の指示に基づく場合、あるいは蓄積した状態情報をクリアしてクリーンなデータベースで起動する必要がある条件のテストの場合を除き、このコマンドの使用を推奨しません。

オプション

次のオプションが適用されます。

- *virtual-sensor*：センサー上に設定された仮想センサーの名前を指定します。
- **all**：すべてのノード、インスペクタ、アラート データベースをクリアします。

注意　このコマンドによって、サマリー アラートが破棄されます。

- **nodes**：パケット ノード、TCP セッション情報、およびインスペクタ リストを含む、パケット データベースの要素全体をクリアします。
- **alerts**：アラート ノード、メタ インスペクタ情報、サマリー状態、およびイベント カウント構造を含む、アラート データベースをクリアします。
- **inspectors**：ノードのインスペクタ リストをクリアします。インスペクタ リストは、センサーが実行している間に収集されたパケットの動作と監視結果を示します。

センサー データベースのクリア

センサー データベースのクリアには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　センサー データベース全体をクリアします。

```
ips-ssp# clear database all
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 3　**yes** を入力してセンサー上のすべてのデータベースをクリアします。

ステップ 4　パケット ノードをクリアします。

```
ips-ssp# clear database nodes
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 5　**yes** を入力してパケット ノード データベースをクリアします。

ステップ 6　特定の仮想センサー上のアラート データベースをクリアします。

```
ips-ssp# clear database vs0 alerts
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 7　**yes** を入力してアラート データベースをクリアします。

ステップ 8　センサー上のインスペクタ リストをクリアします。

```
ips-ssp# clear database inspectors
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 9　**yes** を入力してインスペクタ データベースをクリアします。

ヘルス ステータス情報の設定

センサーのヘルス統計情報を設定するには、サービス サブモードで **health-monitor** コマンドを使用します。**health-monitor** コマンドの結果を表示するには、**show health** コマンドを使用します。ヘルス ステータス カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

オプション

次のオプションが適用されます。

- **application-failure-policy {enable | disable} {true | false} status {green | yellow | red}**：アプリケーション障害を全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。
- **bypass-policy {enable | disable} {true | false} status {green | yellow | red}**：バイパス モードがアクティブかどうかを確認して、それを全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

- **enable-monitoring** {**true | false**}：センサーのヘルスとセキュリティをモニタするかどうか選択できます。
- **event-retrieval-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：いつ最後のイベントを取得したか、しきい値を設定して、それを全体的なセンサーのヘルス レーティングに適用できます。しきい値に達すると、ヘルス ステータスは赤または黄色に低下します。しきい値の範囲は 0 ～ 4294967295 秒です。

（注）　イベント取得メトリックは、IME など外部のモニタリング アプリケーションによって最後のイベントが取得された時刻を記録します。外部のイベント モニタリングを実行しない場合は、event retrieval policy をディセーブルにします。

- **global-correlation-policy {enable | disable} {true | false}**：このメトリックを全体的なセンサーのヘルス レーティングに適用できます。
- **heartbeat-events {enable | disable}** *seconds*：指定した秒単位の間隔でハートビート イベントを送信できるようにして、それを全体的なセンサーのヘルス レーティングに適用できます。間隔の範囲は、15 ～ 86400 秒です。
- **inspection-load-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：インスペクション ロードのしきい値を設定できます。しきい値に達すると、ヘルス ステータスは赤または黄色に低下します。範囲は 0 ～ 100 です。
- **interface-down-policy {enable | disable} {true | false} status {green | yellow | red}**：イネーブルになっているインターフェイスが 1 つ以上ダウンしているかどうかを確認して、それを全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。
- **license-expiration-policy {enable | disable} {true | false} red-threshold yellow-threshold**：ライセンスが期限切れになる時点にしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。
- **memory-usage-policy {enable | disable} {true | false} red-threshold yellow-threshold**：メモリ使用状況のパーセンテージしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。範囲は 0 ～ 100 です。
- **missed-packet-policy {enable | disable} {true | false} red-threshold yellow-threshold**：欠落パケットのパーセンテージしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。
- **network-participation-policy {enable | disable} {true | false}**：このメトリックを全体的なセンサーのヘルス レーティングに適用できます。
- **persist-security-status**：セキュリティ ステータスを下げる最新のイベントの発生後に、低セキュリティが続く期間を分単位で設定できます。
- **signature-update-policy {enable | disable} {true | false} red-threshold yellow-threshold**：最後にシグニチャがアップデートされてから経過した日数のしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。

ヘルス統計情報の設定

センサーにヘルス統計情報を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス ヘルス モニタ サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service health-monitor
ips-ssp(config-hea)#
```

ステップ 3　アプリケーション障害ステータスに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# application-failure-policy
ips-ssp(config-hea-app)# enable true
ips-ssp(config-hea-app)# status red
ips-ssp(config-hea-app)# exit
ips-ssp(config-hea)#
```

ステップ 4　バイパス ポリシーに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# bypass-policy
ips-ssp(config-hea-byp)# enable true
ips-ssp(config-hea-byp)# status yellow
ips-ssp(config-hea-byp)# exit
ips-ssp(config-hea)#
```

ステップ 5　IPS-SSP ヘルスおよびセキュリティ モニタリングに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# enable-monitoring true
ips-ssp(config-hea)#
```

ステップ 6　イベント取得メトリックに対してイベント取得のしきい値を設定します。

```
ips-ssp(config-hea)# event-retrieval-policy
ips-ssp(config-hea-eve)# enable true
ips-ssp(config-hea-eve)# red-threshold 100000
ips-ssp(config-hea-eve)# yellow-threshold 100
ips-ssp(config-hea-eve)# exit
ips-ssp(config-hea)#
```

ステップ 7　グローバル相関に対してヘルス メトリックをイネーブルにします。

```
ips-ssp(config-hea)# global-correlation-policy
ips-ssp(config-hea-glo)# enable true
ips-ssp(config-hea-glo)# exit
ips-ssp(config-hea)#
```

ステップ 8　指定した秒単位の間隔で送信されるハートビート イベントに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# heartbeat-events enable 20000
ips-ssp(config-hea)#
```

ステップ 9　インスペクション ロードのしきい値を設定します。

```
ips-ssp(config-hea)# inspection-load-policy
ips-ssp(config-hea-ins)# enable true
ips-ssp(config-hea-ins)# red-threshold 100
ips-ssp(config-hea-ins)# yellow-threshold 50
ips-ssp(config-hea-ins)# exit
ips-ssp(config-hea)#
```

ステップ 10　インターフェイス ダウン ポリシーをイネーブルにします。

```
ips-ssp(config-hea)# interface-down-policy
ips-ssp(config-hea-int)# enable true
ips-ssp(config-hea-int)# status yellow
ips-ssp(config-hea-int)# exit
ips-ssp(config-hea)#
```

ステップ 11　ライセンスの期限が切れるまでの日数を設定します。

```
ips-ssp(config-hea)# license-expiration-policy
ips-ssp(config-hea-lic)# enable true
ips-ssp(config-hea-lic)# red-threshold 400000
ips-ssp(config-hea-lic)# yellow-threshold 200000
ips-ssp(config-hea-lic)# exit
ips-ssp(config-hea)#
```

ステップ 12　メモリ使用状況のしきい値を設定します。

```
ips-ssp(config-hea)# memory-usage-policy
ips-ssp(config-hea-mem)# enable true
ips-ssp(config-hea-mem)# red-threshold 100
ips-ssp(config-hea-mem)# yellow-threshold 50
ips-ssp(config-hea-mem)# exit
ips-ssp(config-hea)#
```

ステップ 13　欠落パケットのしきい値を設定します。

```
ips-ssp(config-hea)# missed-packet-policy
ips-ssp(config-hea-mis)# enable true
ips-ssp(config-hea-mis)# red-threshold 50
ips-ssp(config-hea-mis)# yellow-threshold 20
ips-ssp(config-hea-mis)# exit
ips-ssp(config-hea)#
```

ステップ 14　セキュリティ ステータスを下げる最新のイベントの発生後に、低セキュリティが続く期間を分単位で設定します。

```
ips-ssp(config-hea)# persist-security-status 10
ips-ssp(config-hea)#
```

ステップ 15　最後にシグニチャがアップデートされてからの日数を設定します。

```
ips-ssp(config-hea)# signature-update-policy
ips-ssp(config-hea-sig)# enable true
ips-ssp(config-hea-sig)# red-threshold 30000
ips-ssp(config-hea-sig)# yellow-threshold 10000
ips-ssp(config-hea-sig)# exit
ips-ssp(config-hea)#
```

ステップ 16　設定値を確認します。

```
ips-ssp(config-hea)# show settings
   enable-monitoring: true default: true
   persist-security-status: 10 minutes default: 5
   heartbeat-events
   -----------------------------------------------
      enable: 20000 seconds default: 300
   -----------------------------------------------
   application-failure-policy
   -----------------------------------------------
      enable: true default: true
      status: red default: red
   -----------------------------------------------
   bypass-policy
   -----------------------------------------------
```

```
      enable: true default: true
      status: yellow default: red
   ------------------------------------------------
   interface-down-policy
   ------------------------------------------------
      enable: true default: true
      status: yellow default: red
   ------------------------------------------------
   inspection-load-policy
   ------------------------------------------------
      enable: true default: true
      yellow-threshold: 50 percent default: 80
      red-threshold: 100 percent default: 91
   ------------------------------------------------
   missed-packet-policy
   ------------------------------------------------
      enable: true default: true
      yellow-threshold: 20 percent default: 1
      red-threshold: 50 percent default: 6
   ------------------------------------------------
   memory-usage-policy
   ------------------------------------------------
      enable: true default: false
      yellow-threshold: 50 percent default: 80
      red-threshold: 100 percent default: 91
   ------------------------------------------------
   signature-update-policy
   ------------------------------------------------
      enable: true default: true
      yellow-threshold: 10000 days default: 30
      red-threshold: 30000 days default: 60
   ------------------------------------------------
   license-expiration-policy
   ------------------------------------------------
      enable: true default: true
      yellow-threshold: 200000 days default: 30
      red-threshold: 400000 days default: 0
   ------------------------------------------------
   event-retrieval-policy
   ------------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 100000 seconds default: 300
      red-threshold: 100 seconds default: 600
   ------------------------------------------------
ips-ssp(config-hea)#
```

ステップ 17　ヘルス モニタリング サブモードを終了します。

```
ips-ssp(config-hea)# exit
Apply Changes:?[yes]:
```

ステップ 18　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

センサーの全体的なヘルス ステータスの表示

特権 EXEC モードで **show health** コマンドを使用して、センサーの全体的なヘルス ステータス情報を表示します。ヘルス ステータス カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

注意　センサーを初めて起動するときは、センサーが完全に起動して動作するまで、特定のヘルス メトリック ステータスが赤色になりますが、これは正常な状態です。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

センサーの全体的なヘルス ステータスを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　センサーのヘルスおよびセキュリティ ステータスを表示します。

```
ips-ssp# show health
Overall Health Status                                 Red
Health Status for Failed Applications                 Green
Health Status for Signature Updates                   Green
Health Status for License Key Expiration              Red
Health Status for Running in Bypass Mode              Green
Health Status for Interfaces Being Down               Red
Health Status for the Inspection Load                 Green
Health Status for the Time Since Last Event Retrieval Green
Health Status for the Number of Missed Packets        Green
Health Status for the Memory Usage                    Not Enabled
Health Status for Global Correlation                  Red
Health Status for Network Participation               Not Enabled

Security Status for Virtual Sensor vs0   Green
ips-ssp#
```

バナー ログインの作成

banner login コマンドを使用して、ユーザおよびパスワードのログイン プロンプトの前に表示されるバナー ログインを作成します。メッセージの最大長は 2500 文字です。バナーを削除するには、**no banner login** コマンドを使用します。

バナー ログインを作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
ips-ssp# configure terminal
```

ステップ 3　バナー ログインを作成します。

```
ips-ssp(config)# banner login
Banner[]:
```

ステップ 4　メッセージを入力します。

```
Banner[]: This message will be displayed on banner login. ^M Thank you
ips-ssp(config)#
```

（注）　メッセージ内で？または復帰を使用するには、Ctrl キーを押した状態で V キーと？ キーを押すか、Ctrl キーを押した状態で V キーと Enter を押します。これらは ^M と表現されます。

例

```
This message will be displayed on login.
Thank you
login: cisco
Password:****
```

ステップ 5　バナー ログインを削除します。ログイン時にバナーが表示されなくなります。

```
ips-ssp(config)# no banner login
```

CLI セッションの終了

clear line *cli_id* [**message**] コマンドを使用して、別の CLI セッションを終了します。**message** キーワードを使用すると、受信ユーザに対して終了要求とともにメッセージを送信できます。メッセージの最大長は 2500 文字です。

オプション

次のオプションが適用されます。

- *cli_id* : ログイン セッションに関連付けられた CLI ID 番号を指定します。**show users** コマンドを使用して、CLI ID 番号を確認します。
- **message** : 受信ユーザに送信するメッセージを指定します。

注意　**clear line** コマンドでは、CLI ログイン セッションのクリアしかできません。このコマンドでは、サービス ログインをクリアできません。

最大セッション数に達した場合に、管理者がログインしようとすると、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, would you like to terminate
one of the open sessions? [no]
```

最大セッション数が開かれている場合に、オペレータまたはビューアがログインしようとすると、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

CLI セッションの終了

CLI セッションを終了するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

（注）　オペレータおよびビューアは、現在のログインと同じユーザ名のある行しかクリアできません。

ステップ 2　ログイン セッションに関連付けられた CLI ID 番号を確認します。

```
ips-ssp# show users
    CLI ID   User    Privilege
*   13533    jtaylor administrator
    15689    jsmith  operator
    20098    viewer  viewer
```

ステップ 3　jsmith の CLI セッションを終了します。

```
ips-ssp# clear line cli_id message
Message[]:
```

例

```
ips-ssp# clear line 15689 message
Message{}: Sorry! I need to terminate your session.
ips-ssp#
```

ユーザ jsmith は、管理者 jtaylor から次のメッセージを受信します。

```
ips-ssp#
***
***
*** Termination request from jtaylor
***
Sorry! I need to terminate your session.
```

ターミナル プロパティの変更

terminal [length] *screen _length* コマンドを使用して、ログイン セッションのターミナル プロパティを変更します。*screen_ length* オプションによって、--more-- プロンプトが表示される前に、画面上に表示される行数を設定できます。値をゼロにすると、出力は一時停止しなくなります。デフォルト値は 24 行です。

（注）　ターミナル セッションの一部のタイプは画面長を指定する必要がありません。これは、一部のリモート ホストで、指定した画面長を取得できるためです。

ターミナル プロパティを変更するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　複数画面の出力間で一時停止しないようにするには、screen length の値に 0 を使用します。

```
ips-ssp# terminal length 0
```

（注）　screen length の値は、ログイン セッション間で保存されません。

ステップ 3　10 行ごとに CLI を一時停止して、--more-- プロンプトを表示するには、*screen length* の値に 10 を使用します。

```
ips-ssp# terminal length 10
```

イベントの設定

ここでは、イベント ストアからイベントを表示したりクリアしたりする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。

- 「イベントの表示」（P.17-13）
- 「イベント ストアからのイベントのクリア」（P.17-16）

イベントの表示

show events [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用して、イベント ストアのイベントを表示します。

開始時刻に開始されているイベントが表示されます。開始時刻を指定しない場合、現時点で開始されているイベントが表示されます。イベント タイプを指定しないと、すべてのイベントが表示されます。

（注）　イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

オプション

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であるか、試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。シグニチャがネットワーク アクティブによってトリガーされると常に、分析エンジンによってアラート イベントが生成されます。レベルが選択されていない場合（informational、low、medium、または high）、すべてのアラート イベントが表示されます。
- **include-traits**：指定された特徴を持つアラートを表示します。
- **exclude-traits**：指定された特徴を持つアラートを表示しません。
- **traits**：特徴ビット位置を 10 進数で指定します（0 ～ 15）。
- **min-threat-rating**：脅威レーティングがこの値以上であるイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：脅威レーティングがこの値以下であるイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。

- **error**：エラー イベントを表示します。エラーの条件が検出されると、サービスによってエラー イベントが生成されます。レベルが選択されていない場合（warning、error、または fatal）、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

（注）　ARC は、以前は NAC と呼ばれていました。この名前の変更は、Cisco IPS 7.1 の IDM、IME、および CLI に完全には実装されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定した過去の時、分、および秒から開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注）　**show events** コマンドは、指定したイベントが使用可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベントの表示

イベント ストアのイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始しているイベントをすべて表示します。

```
ips-ssp# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

Ctrl キーを押した状態で C キーを押すまで、フィードはすべてのイベントを表示し続けます。

ステップ 3　2011 年 2 月 9 日 10:00 a.m に開始されたブロック要求を表示します。

```
ips-ssp# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
```

```
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
ips-ssp#
```

ステップ 4　2011 年 2 月 9 日 10:00 a.m. に開始された警告レベルのエラーを表示します。

```
ips-ssp# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
ips-ssp# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　30 秒前に開始されたイベントを表示します。

```
ips-ssp# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316
```

```
evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアからのイベントのクリア

clear events コマンドを使用して、イベント ストアをクリアします。

イベント ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
ips-ssp# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力して、イベントをクリアします。

システム クロックの表示

show clock [**detail**] コマンドを使用して、システム クロックを表示します。**detail** オプションを使用すると、クロック ソース（NTP またはシステム）と現在のサマータイム設定（設定されている場合）を表示できます。

システム クロックは、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックがタイミング ソース（NTP など）によって設定されている場合は、このフラグが設定されます。

表 17-1 に、システム クロック フラグを示します。

表 17-1　システム クロック フラグ

記号	説明
*	時刻は信頼できません。
（空白）	時刻は信頼できます。
.	時刻は信頼できますが、NTP と同期していません。

システム クロックを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
ips-ssp# show clock
22:57:43 UTC Fri Aug 13 2010
```

ステップ 3　システム クロックを詳細表示します。これは、センサーが時刻を適応型セキュリティ アプライアンスから取得していることを示します。

```
ips-ssp# show clock detail
22:58:08 UTC Fri Aug 13 2010
Time source is chassis
Summer time starts 03:00:00 UTC Sun Mar 14 2010
Summer time stops 01:00:00 UTC Sun Nov 07 2010
```

ステップ 4　システム クロックを詳細表示します。これは、時刻源が設定されていないことを示しています。

```
ips-ssp# show clock detail
*20:09:43 UTC Thu Apr 03 2010
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2010
Summer time stops 01:00:00 UTC Sun Nov 02 2010
```

拒否攻撃者リストのクリア

show statistics denied-attackers コマンドを使用して、拒否攻撃者リストを表示します。**clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] コマンドを使用して、拒否攻撃者リストを削除し、仮想センサー統計情報をクリアします。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。インライン モードでは、パケット、接続、および攻撃者を拒否するようシグニチャを設定できます。この結果、センサーが単一のパケット、接続、および特定の攻撃者を検出した場合に、これらは拒否されます（つまり、送信されません）。

シグニチャが起動されると、攻撃者は拒否され、リストに追加されます。センサー管理の一部として、リストの削除、またはリスト内の統計情報のクリアが必要な場合があります。

オプション

次のオプションが適用されます。

- *virtual_sensor*：（任意）拒否攻撃者リストをクリアする必要がある仮想センサーを指定します。
- *ip_address*：（任意）クリアする IP アドレスを指定します。

拒否攻撃者リストの表示、削除、およびクリア

拒否攻撃者リストの表示、リストの削除、統計情報のクリアを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　拒否された IP アドレスのリストを表示します。統計情報は、この時点で 2 つの IP アドレスが拒否されていることを示します。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

ステップ 3　拒否攻撃者リストを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力して、リストをクリアします。

ステップ 5　特定の仮想センサーの拒否攻撃者リストを削除します。

```
ips-ssp# clear denied-attackers vs0
Warning: Executing this command will delete all addresses from the list of attackers being
denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 6　**yes** を入力して、リストをクリアします。

ステップ 7　特定の仮想センサーの拒否攻撃者リストから、特定の IP アドレスを削除します。

```
ips-ssp# clear denied-attackers vs0 ip-address 192.0.2.1
Warning: Executing this command will delete ip address 192.0.2.1 from the list of
attackers being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 8　**yes** を入力して、リストをクリアします。

ステップ 9　リストをクリアしたことを確認します。**show statistics denied-attackers** または **show statistics virtual-sensor** コマンドを使用できます。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.
ips-ssp#

ips-ssp# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
```

```
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

ステップ 10　統計情報のみをクリアします。

```
ips-ssp# show statistics virtual-sensor clear
```

ステップ 11　統計情報をクリアしたことを確認します。Number of Active Denied Attackers および Number of exec Clear commands during uptime カテゴリ以外の統計情報がすべてクリアされました。リストがクリアされたかどうかを認識することが重要です。

```
ips-ssp# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

ポリシー リストの表示

EXEC モードで **list {anomaly-detection-configurations | event-action-rules-configurations | signature-definition-configurations}** を使用して、これらのコンポーネントのポリシーのリストを表示します。ファイル サイズはバイト単位です。N/A の状態の仮想センサーは、ポリシーが仮想センサーに割り当てられていないことを示します。

センサー上のポリシーのリストを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　異常検出のポリシーのリストを表示します。

```
ips-ssp# list anomaly-detection-configurations
Anomaly Detection
   Instance   Size   Virtual Sensor
   ad0        255    vs0
   temp       707    N/A
   MyAD       255    N/A
   ad1        141    vs1
ips-ssp#
```

ステップ 3　イベント アクション規則のポリシーのリストを表示します。

```
ips-ssp# list event-action-rules-configurations
Event Action Rules
   Instance   Size   Virtual Sensor
   rules0     112    vs0
   rules1     141    vs1
ips-ssp#
```

ステップ 4　シグニチャ定義のポリシーのリストを表示します。

```
ips-ssp# list signature-definition-configurations
Signature Definition
   Instance   Size   Virtual Sensor
   sig0       336    vs0
   sig1       141    vs1
   sig2       141    N/A
ips-ssp#
```

統計情報の表示

show statistics [analysis-engine | anomaly-detection | authentication | denied-attackers | event-server | event-store | external-product-interface | global-correlation | host | logger | network-access | notification | os-identification | sdee-server | transaction-server | virtual-sensor | web-server] [clear] コマンドを使用して、各センサー アプリケーションの統計情報を表示します。

show statistics {**anomaly-detection** | **denied-attackers** | **os-identification** | **virtual-sensor**} [***name*** | **clear**] を使用して、すべての仮想センサーについてこれらのコンポーネントの統計情報を表示します。仮想センサー名を指定すると、その仮想センサーの統計情報のみが表示されます。

（注）　分析エンジン、異常検出、ホスト、ネットワーク アクセス、または OS 識別アプリケーションには、**clear** オプションを使用できません。

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジンの統計情報を表示します。

```
ips-ssp# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
```

```
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
ips-ssp#
```

ステップ 3　異常検出の統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

ステップ 4　認証の統計情報を表示します。

```
ips-ssp# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
ips-ssp#
```

ステップ 5　システムの拒否攻撃者の統計情報を表示します。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


ips-ssp#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
ips-ssp# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
ips-ssp#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
ips-ssp# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
ips-ssp#
```

ステップ 8　グローバル相関の統計情報を表示します。

```
ips-ssp# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
```

```
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
ips-ssp#
```

ステップ 9　ホストの統計情報を表示します。

```
ips-ssp# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2011
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2011
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2011
    =   Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
    =   Error: httpResponse status returned:  Unauthorized
   lastInstallAttempt = N/A
   nextAttempt = 16:26:30 CDT Tue Jun 17 2011

ips-ssp#
```

ステップ 10　ロギング アプリケーションの統計情報を表示します。

```
ips-ssp# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
ips-ssp#
```

ステップ 11　ARC の統計情報を表示します。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 192.0.2.1
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.3
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.4
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 192.0.2.5
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 192.0.2.6
      NATAddr = 0.0.0.0
      Communications = telnet
```

```
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 192.0.2.7
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 192.0.2.8
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 192.0.2.9
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 192.0.2.10
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 192.0.2.11
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 203.0.113.1
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.24
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 209.165.201.30
         Mask = 255.255.255.224
         BlockMinutes =
ips-ssp#
```

ステップ 12　通知アプリケーションの統計情報を表示します。

```
ips-ssp# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
ips-ssp#
```

ステップ 13　OS 識別の統計情報を表示します。

```
ips-ssp# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
ips-ssp#
```

ステップ 14　SDEE サーバの統計情報を表示します。

```
ips-ssp# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
ips-ssp#
```

ステップ 15　トランザクション サーバの統計情報を表示します。

```
ips-ssp# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
ips-ssp#
```

ステップ 16　仮想センサーの統計情報を表示します。

```
ips-ssp# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 0
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 0
         The average bytes per packet since reset = 0
```

```
        Denied Address Information
           Number of Active Denied Attackers = 0
           Number of Denied Attackers Inserted = 0
           Number of Denied Attacker Victim Pairs Inserted = 0
           Number of Denied Attacker Service Pairs Inserted = 0
           Number of Denied Attackers Total Hits = 0
           Number of times max-denied-attackers limited creation of new entry = 0
           Number of exec Clear commands during uptime = 0
        Denied Attackers and hit count for each.
        Denied Attackers with percent denied and hit count for each.


        The Signature Database Statistics.
           The Number of each type of node active in the system (can not be reset
              Total nodes active = 0
              TCP nodes keyed on both IP addresses and both ports = 0
              UDP nodes keyed on both IP addresses and both ports = 0
              IP nodes keyed on both IP addresses = 0
           The number of each type of node inserted since reset
              Total nodes inserted = 0
              TCP nodes keyed on both IP addresses and both ports = 0
              UDP nodes keyed on both IP addresses and both ports = 0
              IP nodes keyed on both IP addresses = 0
           The rate of nodes per second for each time since reset
              Nodes per second = 0
              TCP nodes keyed on both IP addresses and both ports per second = 0
              UDP nodes keyed on both IP addresses and both ports per second = 0
              IP nodes keyed on both IP addresses per second = 0
           The number of root nodes forced to expire because of memory constraint
              TCP nodes keyed on both IP addresses and both ports = 0
           Packets dropped because they would exceed Database insertion rate limit
s = 0
        Fragment Reassembly Unit Statistics for this Virtual Sensor
           Number of fragments currently in FRU = 0
           Number of datagrams currently in FRU = 0
           Number of fragments received since reset = 0
           Number of fragments forwarded since reset = 0
           Number of fragments dropped since last reset = 0
           Number of fragments modified since last reset = 0
           Number of complete datagrams reassembled since last reset = 0
           Fragments hitting too many fragments condition since last reset = 0
           Number of overlapping fragments since last reset = 0
           Number of Datagrams too big since last reset = 0
           Number of overwriting fragments since last reset = 0
           Number of Initial fragment missing since last reset = 0
           Fragments hitting the max partial dgrams limit since last reset = 0
           Fragments too small since last reset = 0
           Too many fragments per dgram limit since last reset = 0
           Number of datagram reassembly timeout since last reset = 0
           Too many fragments claiming to be the last since last reset = 0
           Fragments with bad fragment flags since last reset = 0
        TCP Normalizer stage statistics
           Packets Input = 0
           Packets Modified = 0
           Dropped packets from queue = 0
           Dropped packets due to deny-connection = 0
           Current Streams = 0
           Current Streams Closed = 0
           Current Streams Closing = 0
           Current Streams Embryonic = 0
           Current Streams Established = 0
           Current Streams Denied = 0
        Statistics for the TCP Stream Reassembly Unit
           Current Statistics for the TCP Stream Reassembly Unit
```

```
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   Cumulative Statistics for the TCP Stream Reassembly Unit since reset
      TCP streams that have been tracked since last reset = 0
      TCP streams that had a gap in the sequence jumped = 0
      TCP streams that was abandoned due to a gap in the sequence = 0
      TCP packets that arrived out of sequence order for their stream = 0
      TCP packets that arrived out of state order for their stream = 0
      The rate of TCP connections tracked per second since reset = 0
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 0
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 0
   Number of FireOnce Intermediate Alerts = 0
   Number of Summary First Alerts = 0
   Number of Summary Intermediate Alerts = 0
   Number of Regular Summary Final Alerts = 0
   Number of Global Summary Final Alerts = 0
   Number of Active SigEventDataNodes = 0
   Number of Alerts Output for further processing = 0
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
      request-rate-limit = 0
SigEvent Action Filter Stage Statistics
   Number of Alerts received to Action Filter Processor = 0
   Number of Alerts where an action was filtered = 0
   Number of Filter Line matches = 0
   Number of Filter Line matches causing decreased DenyPercentage = 0
   Actions Filtered
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
```

```
            reset-tcp-connection = 0
            request-rate-limit = 0
      SigEvent Action Handling Stage Statistics.
         Number of Alerts received to Action Handling Processor = 0
         Number of Alerts where produceAlert was forced = 0
         Number of Alerts where produceAlert was off = 0
         Actions Performed
            deny-attacker-inline = 0
            deny-attacker-victim-pair-inline = 0
            deny-attacker-service-pair-inline = 0
            deny-connection-inline = 0
            deny-packet-inline = 0
            modify-packet-inline = 0
            log-attacker-packets = 0
            log-pair-packets = 0
            log-victim-packets = 0
            produce-alert = 0
            produce-verbose-alert = 0
--MORE--
```

ステップ 17　Web サーバの統計情報を表示します。

```
ips-ssp# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
ips-ssp#
```

ステップ 18　ロギング アプリケーションなどのアプリケーションの統計情報をクリアします。統計情報が取得され、クリアされます。

```
ips-ssp# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

ステップ 19　統計情報がクリアされたことを確認します。これによって統計情報はすべて 0 から始まります。

```
ips-ssp# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
```

```
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
ips-ssp#
```

技術サポート情報の表示

show tech-support [**page**] [**destination-url** *destination_url*] コマンドを使用して、画面にシステム情報を表示するか、その情報を特定の URL に送信します。この情報は、TAC とのトラブルシューティング ツールとして使用できます。

オプション

次のパラメータはオプションです。

- **page**：一度に 1 ページの情報として出力を表示します。

  Enter を押して出力の次の行を表示するか、Space を使用して次のページの情報を表示します。
- **destination-url**：HTML としてフォーマットし、このコマンドに続く宛先に送信する必要がある情報を示します。このキーワードを使用すると、出力は画面に表示されません。
- *destination_url*：HTML としてフォーマットする必要がある情報を示します。URL は、情報を送信する宛先を示します。このキーワードを使用しないと、画面に情報が表示されます。

技術サポート情報の表示

技術サポート情報を表示するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　画面上に出力を表示します。システム情報が画面上に一度に 1 ページずつ表示されます。次のページを表示するには Space を押します。プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

```
ips-ssp# show tech-support page
```

ステップ 3　出力（HTML フォーマット）をファイルに送信するには、次の手順を実行します。

a. 次のコマンドを入力し、その後に有効な宛先を指定します。`password:` プロンプトが表示されます。

```
ips-ssp# show tech-support destination-url destination_url
```

次に示す種類の宛先を指定できます。

- **ftp:**：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`ftp:[[//username@location]/relativeDirectory]/filename` または `ftp:[[//username@location]//absoluteDirectory]/filename` です。
- **scp:**：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`scp:[[//username@]location]/relativeDirectory]/filename` または `scp:[[//username@]location]//absoluteDirectory]/filename` です。

たとえば、技術サポート出力をファイル `/absolute/reports/sensor1Report.html` に送信するには、

```
ips-ssp# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

b. このユーザ アカウントのパスワードを入力します。Generating report: メッセージが表示されます。

バージョン情報の表示

インストールされているすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の設定を表示するには、**more current-config** コマンドを使用します。

バージョンおよび設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　バージョン情報を表示します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

ips-ssp#
#
```

（注）　--MORE-- というプロンプトが表示された場合、Space を押して詳細な情報を表示するか、Ctrl キーを押した状態で C キーを押して出力をキャンセルし、CLI プロンプトに戻ります。

ステップ 3　設定情報を表示します。

（注）　**more current-config** または **show configuration** コマンドを使用できます。

```
ips-ssp# more current-config
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
```

```
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
ips-ssp#
```

ネットワークの接続性の診断

ping *ip_address* [**count**] コマンドを使用して、基本的なネットワークの接続性を診断します。

注意　このコマンドには、コマンド割り込みは使用できません。完了まで実行する必要があります。

基本的なネットワークの接続性を診断するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　目的のアドレスを ping します。count は、送信するエコー要求の数です。数を指定しない場合、4 回の要求が送信されます。範囲は 1 ～ 10,000 です。

```
ips-ssp# ping ip_address count
```

正常な ping の例

```
ips-ssp# ping 192.0.2.1 6
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 192.0.2.1: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=5 ttl=61 time=0.2 ms

--- 192.0.2.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

失敗した ping の例

```
ips-ssp# ping 172.16.0.0 3
PING 172.16.0.0 (172.16.0.0): 56 data bytes

--- 172.16.0.0 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
ips-ssp#
```

コマンド履歴の表示

show history コマンドを使用して、現在のメニューで入力したコマンドのリストを取得します。リスト内のコマンドの最大数は 50 です。

最近使用したコマンドのリストを取得するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　EXEC モードで使用したコマンドの履歴を表示します。

```
ips-ssp# show history
clear line
configure terminal
show history
```

ステップ 3　ネットワーク アクセス モードで使用したコマンドの履歴を表示します。

```
ips-ssp# configure terminal
ips-ssp (config)# service network-access
ips-ssp (config-net)# show history
show settings
show settings terse
show settings | include profile-name|ip-address
exit
show history
ips-ssp (config-net)#
```

IP パケットのルートのトレース

trace *ip_address count* コマンドを使用して、IP パケットが宛先まで送られるルートを表示します。*ip_address* オプションはルートをトレースする先のシステムのアドレスです。*count* オプションで、実行するホップ数を定義できます。デフォルトは 4 です。有効な値は 1 ～ 256 です。

注意　このコマンドに対して使用できる、コマンド割り込みはありません。完了まで実行する必要があります。

IP パケットのルートをトレースするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　目的の IP パケットのルートを表示します。

```
ips-ssp# trace 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 4 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.267 ms  0.262 ms  0.236 ms
 2  192.0.2.12 (192.0.2.12)  0.24 ms *  0.399 ms
 3  * 192.0.2.12 (192.0.2.12)  0.424 ms *
 4  192.0.2.12 (192.0.2.12)  0.408 ms *  0.406 ms
ips-ssp#
```

ステップ 3　デフォルトの 4 より多くのホップを実行するルートを設定します。*count* オプションを使用します。

```
ips-ssp# trace 10.0.0.1 8
traceroute to 10.0.0.1 (10.0.0.1), 8 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.35 ms  0.261 ms  0.238 ms
 2  192.0.2.12 (192.0.2.12)  0.36 ms *  0.344 ms
 3  * 192.0.2.12 (192.0.2.12)  0.465 ms *
 4  192.0.2.12 (192.0.2.12)  0.319 ms *  0.442 ms
 5  * 192.0.2.12 (192.0.2.12)  0.304 ms *
 6  192.0.2.12 (192.0.2.12)  0.527 ms *  0.402 ms
 7  * 192.0.2.12 (192.0.2.12)  0.39 ms *
 8  192.0.2.12 (192.0.2.12)  0.37 ms *  0.486 ms
ips-ssp#
```

サブモード設定の表示

任意のサブモードで **show settings** [**terse**] コマンドを使用して、現在の設定の内容を表示します。

サブモードの現在の設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp (config)# service network-access
ips-ssp (config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ------------------------------------------------
      profile-name: 2admin
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
      profile-name: insidePix
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: <defaulted>
      ------------------------------------------------
      profile-name: qatest
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
```

```
      username: <defaulted>
   ------------------------------------------------
   profile-name: fwsm
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: outsidePix
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: cat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: <defaulted>
   ------------------------------------------------
   profile-name: rcat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
   profile-name: nopass
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: <defaulted>
   ------------------------------------------------
   profile-name: test
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: sshswitch
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
-----------------------------------------------
cat6k-devices (min: 0, max: 250, current: 1)
-----------------------------------------------
   ip-address: 10.89.147.61
   ------------------------------------------------
      communication: telnet default: ssh-3des
      nat-address: 0.0.0.0 <defaulted>
      profile-name: cat
      block-vlans (min: 0, max: 100, current: 1)
      ------------------------------------------------
         vlan: 1
         ------------------------------------------------
            pre-vacl-name: <defaulted>
            post-vacl-name: <defaulted>
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
-----------------------------------------------
router-devices (min: 0, max: 250, current: 1)
-----------------------------------------------
```

```
      ip-address: 10.89.147.54
      ---------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ---------------------------------------------
            interface-name: fa0/0
            direction: in
            ---------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ---------------------------------------------
      ip-address: 10.89.147.10
      ---------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: insidePix
      ---------------------------------------------
      ip-address: 10.89.147.82
      ---------------------------------------------
         communication: ssh-3des <defaulted>
         nat-address: 0.0.0.0 <defaulted>
         profile-name: f1
      ---------------------------------------------
   ---------------------------------------------
ips-ssp (config-net)#
```

ステップ 3　簡単なモードで ARC 設定を表示します。

```
ips-ssp(config-net)# show settings terse
   general
   ---------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ---------------------------------------------
      profile-name: 2admin
```

```
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
   ------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.61
   ------------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.54
   ------------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ------------------------------------------------
      ip-address: 10.89.147.10
      ip-address: 10.89.147.82
   ------------------------------------------------
ips-ssp(config-net)#
```

ステップ 4　**include** キーワードを使用して、フィルタ処理された出力に設定を表示できます。たとえば、ARC 設定のプロファイル名と IP アドレスだけを表示できます。

```
ips-ssp(config-net)# show settings | include profile-name|ip-address
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
      ip-address: 10.89.147.61
         profile-name: cat
      ip-address: 10.89.147.54
         profile-name: r7200
      ip-address: 10.89.147.10
         profile-name: insidePix
      ip-address: 10.89.147.82
         profile-name: test
ips-ssp(config-net)#
```

CHAPTER 18

IPS SSP の設定

（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。

（注） すべての IPS プラットフォームは 10 の同時 CLI セッションを許可します。

この章では、IPS SSP の設定に固有の手順について説明します。次のような構成になっています。

- 「IPS SSP の設定手順」（P.18-1）
- 「IPS SSP の初期化の確認」（P.18-2）
- 「IPS SSP の仮想センサーの作成」（P.18-3）
- 「IPS SSP のリロード、シャットダウン、リセット、および復旧」（P.18-9）
- 「ヘルスおよびステータス情報」（P.18-10）
- 「IPS スイッチポートで停止したトラフィック フロー」（P.18-13）
- 「フェールオーバー シナリオ」（P.18-14）

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. モジュール ソフトウェアが最新でない場合は、現在の IPS ソフトウェアを入手してインストールします。
2. ライセンス キーを入手してインストールします。
3. IPS SSP にログ（セッション）インします。
4. 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。
5. IPS SSP の初期化を確認します。
6. 仮想センサーを設定します。

7. ユーザの追加、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。
8. 侵入防御を設定します。
9. グローバル相関を設定します。
10. IPS SSP 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。
11. 入手可能になった新しいシグニチャ 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。
12. 必要に応じて、IPS SSP 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** コマンドを実行する手順については、「IPS SSP の高度なセットアップ」（P.3-7）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。
- 仮想センサーの作成手順については、「IPS SSP の仮想センサーの作成」（P.18-3）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。
- 侵入防御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」、第 7 章「シグニチャの定義」、第 9 章「異常検出の設定」、および第 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。
- 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。
- IPS SSP をスムーズに実行し続ける手順については、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。
- IPS SSP のイメージを再作成する手順については、「IPS SSP システム イメージのインストール」（P.20-1）を参照してください。

IPS SSP の初期化の確認

show module *slot* **details** コマンドを使用して、IPS SSP を初期化したこと、およびソフトウェアのバージョンが正しいことを確認できます。

初期化を確認するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　IPS SSP の詳細を入手します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS10
Hardware version:   1.0
Serial Number:      JAF1350ABSL
Firmware version:   2.0(1)3
Software version:   7.1(0.326)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App.name:           IPS
App.Status:         Up
```

```
App.Status Desc:   Normal Operation
App.version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

ステップ 3　情報を確認します。

IPS SSP の仮想センサーの作成

ここでは、IPS SSP 上で仮想センサーを作成する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。

- 「IPS SSP と仮想化」（P.18-3）
- 「IPS SSP 仮想センサーの設定手順」（P.18-4）
- 「仮想センサーの作成」（P.18-4）
- 「適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て」（P.18-6）

IPS SSP と仮想化

注意　IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

IPS SSP には、1 つのセンシング インターフェイス、PortChannel 0/0 があります。複数の仮想センサーを作成する場合は、このインターフェイスを 1 つの仮想センサーにだけ割り当てる必要があります。残りの仮想センサーには、インターフェイスを指定する必要はありません。

仮想センサーを作成した後、**allocate-ips** コマンドを使用して、それらを適応型セキュリティ アプライアンス上のセキュリティ コンテキストにマッピングする必要があります。複数のセキュリティ コンテキストを複数の仮想センサーにマッピングできます。

（注）　**allocate-ips** コマンドは、シングル モードには適用されません。このモードでは、**policy-map** コマンドで名前が指定されているすべての仮想センサーが適応型セキュリティ アプライアンスで受け入れられます。

allocate-ips コマンドは、新しいエントリをセキュリティ コンテキスト データベースに追加します。指定した仮想センサーが存在しないと、警告が出力されます。ただし、設定は受け入れられます。**service-policy** コマンドが処理されるとき、設定が再びチェックされます。仮想センサーが有効でなければ、**fail-open** ポリシーが適用されます。

IPS SSP 仮想センサーの設定手順

次の手順に従って、IPS SSP 上に仮想センサーを作成し、それらを適応型セキュリティ アプライアンスのコンテキストに割り当てます。

1. IPS SSP 上で最大 4 つの仮想センサーを設定します。
2. IPS SSP センシング インターフェイス（PortChannel 0/0）を仮想センサーの 1 つに割り当てます。
3. 仮想センサーを適応型セキュリティ アプライアンス上の異なるコンテキストに割り当てます。
4. MPF を使用してトラフィックをターゲットの仮想センサーに誘導します。

仮想センサーの作成

（注） 4 つの仮想センサーを作成できます。

サービス分析エンジン サブモードで **virtual-sensor** *name* コマンドを使用して、IPS SSP 上の仮想センサーを作成します。仮想センサーにポリシー（異常検出、イベント アクション規則、およびシグニチャ定義）を割り当てます。デフォルトのポリシーである ad0、rules0、または sig0 を使用できます。あるいは、新しいポリシーを作成することもできます。その後、IPS SSP のセンシング インターフェイス PortChannel0/0 を 1 つの仮想センサーに割り当てます。

オプション

次のオプションが適用されます。

- **anomaly-detection**：異常検出パラメータを指定します。
  - **anomaly-detection-name** *name*：異常検出ポリシーの名前を指定します。
  - **operational-mode**：異常検出モード（**inactive**、**learn**、**detect**）を指定します。
- **description**：仮想センサーの説明。
- **event-action-rules**：イベント アクション規則ポリシーの名前を指定します。
- **signature-definition**：シグニチャ定義ポリシーの名前を指定します。
- **physical-interfaces**：物理インターフェイスの名前を指定します。
- **no**：エントリまたは選択を削除します。

仮想センサーの作成

IPS SSP 上で仮想センサーを作成するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス分析モードを開始します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

ステップ 3　仮想センサーを追加します。

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

ステップ 4　この仮想センサーの説明を追加します。

```
sensor(config-ana-vir)# description virtual sensor 1
```

ステップ 5　異常検出ポリシーと動作モードをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad1
sensor(config-ana-vir-ano)# operational-mode learn
```

ステップ 6　イベント アクション規則ポリシーをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules1
```

ステップ 7　シグニチャ定義ポリシーをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# signature-definition sig1
```

ステップ 8　インターフェイスを 1 つの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# physical-interface PortChannel0/0
```

ステップ 9　仮想センサー設定を確認します。

```
sensor(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: PortChannel0/0
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

ステップ 10　分析エンジン モードを終了します。

```
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes:?[yes]:
sensor(config)#
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

- 異常検出ポリシーの作成および設定の手順については、「異常検出ポリシーの使用」（P.9-8）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作成および設定の手順については、「イベント アクション ルール ポリシーの使用」（P.8-7）を参照してください。
- シグニチャ定義の作成および設定の手順については、「シグニチャ定義ポリシーの操作」（P.7-1）を参照してください。

適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て

IPS SSP で仮想センサーを作成してから、適応型セキュリティ アプライアンス上のセキュリティ コンテキストに仮想センサーを割り当てる必要があります。

オプション

次のオプションが適用されます。

- **[no] allocate-ips** *sensor_name* [*mapped_name*] [**default**]：仮想センサーをセキュリティ コンテキストに割り当てます。サポートされているモードは、マルチ モード、システム コンテキスト、およびコンテキスト サブモードです。

  （注）　1 つのコンテキストには、同じ IPS SSP を 2 回割り当てられません。

  - *sensor_name*：IPS SSP で設定した IPS SSP の名前を指定します。名前が有効でない場合、警告メッセージが表示されます。
  - *mapped_name*：セキュリティ コンテキストが IPS SSP を認識する名前を指定します。

    （注）　マッピング名は、コンテキストから IPS SSP の実際の名前を隠すのに使用されます。通常、セキュリティまたは便宜上の理由で使用され、コンテキスト設定をより一般的にします。マッピング名が使用されない場合、実際の IPS SSP 名が使用されます。1 つのコンテキスト内で 2 つの異なる IPS SSP に 1 つのマッピング名を再利用できません。

  - **no**：センサーの割り当てを解除し、ポリシー マップ設定を検索し、そのセンサーを参照しているすべての IPS サブコマンドを削除します。
  - **default**：この IPS SSP をデフォルトに指定します。仮想センサーを指定しないすべてのレガシー IPS 設定は、この IPS SSP にマッピングされます。

注意　コンテキストごとに設定できるデフォルト IPS SSP は 1 つのみです。別の IPS SSP をデフォルトに指定する場合は、その前に既存のデフォルト IPS SSP のデフォルト フラグをオフにする必要があります。

  - **clear configure allocate-ips**：設定を削除します。
  - **allocate-ips?**：設定済みの IPS SSP のリストを表示します。
- **show ips [detail]**：使用可能な仮想センサーをすべて表示します。サポートされるモードは、EXEC モード、シングルまたはマルチ モード、システムまたはユーザ モードです。
  - **detail**：仮想センサー ID 番号を追加します。

（注）　シングル モードでは、コマンドは使用可能な仮想センサーすべての名前を表示します。マルチ モード ユーザ コンテキストでは、コマンドはこのコンテキストに割り当てられた仮想センサーすべてのマッピング名を表示します。マルチ モード システム コンテキストでは、コマンドは仮想センサーすべての名前を表示します。また detail キーワードを使用すると、センサー ID 番号、割り当てられたコンテキスト、およびマッピング名が表示されます。

- **show context [detail]**：仮想センサーに関する情報を表示するように更新されます。ユーザ コンテキスト モードでは、このコンテキストに割り当てられているすべての仮想センサーのマッピングされた名前を表示するために、新しい行が 1 つ追加されます。システム モードでは、このコンテキストに割り当てられた仮想センサーの本当の名前とマッピングされた名前を表示するために、新しい行が 2 つ追加されます。

複数の仮想センサーを 1 つのコンテキストに割り当てることができます。1 つの仮想センサーは複数のコンテキストで共有することができます。共有した場合、それらのコンテキストは、同じ仮想センサーに対してそれぞれ異なるマッピングされた名前（エイリアス）を使用できます。次の手順では、マルチ モードで 3 つのセキュリティ コンテキストを追加する方法とそれらのセキュリティ コンテキストに仮想センサーを割り当てる方法を示します。

仮想センサーのコンテキストへの割り当て

マルチ モードで IPS SSP の仮想センサーを、適応型セキュリティ アプライアンスコンテキストに割り当てるには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　使用可能な仮想センサーのリストを表示します。

```
asa# show ips detail
Sensor Name      Sensor ID
-----------      ---------
vs0              1
vs1              2
asa#
```

ステップ 3　コンフィギュレーション モードを開始します。

```
asa# configure terminal
asa(config)#
```

ステップ 4　マルチ モードを開始します。

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

ステップ 5　3 つのコンテキスト モードをマルチ モードに追加します。

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.101
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.102
asa(config-ctx)#   allocate-interface Management0/0
asa(config-ctx)#   config-url disk0:/admin.cfg
Cryptochecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up .... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.103
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.104
asa(config-ctx)#   config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
asa(config-ctx)#   config-url disk0:/c3.cfg

WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

ステップ 6　仮想センサーをセキュリティ コンテキストに割り当てます。

```
asa(config)# context admin
asa(config-ctx)#   allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)#   allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

ステップ 7　各コンテキストに MPF を設定します。

（注）　次に、コンテキスト 3（c3）の例を示します。

```
asa(config)# context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
```

```
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

ステップ 8　設定を確認します。

```
asa/c3(config)# exit
asa(config)# changeto system
asa(config)# show ips detail
Sensor Name       Sensor ID        Allocated To     Mapped Name
-----------       ---------        ------------     -----------
vs0               1                admin            adminvs0
                                   c3               c3vs0
vs1               2                c2               c2vs1
                                   c3               c3vs1
asa(config)#
```

詳細情報

ASA 5585-X のフェールオーバーの詳細なシナリオについては、「フェールオーバー シナリオ」（P.C-48）を参照してください。

IPS SSP のリロード、シャットダウン、リセット、および復旧

（注）　特権 EXEC モードまたはグローバル コンフィギュレーション モードから、**hw-module** コマンドを入力できます。シングル ルーテッド モードおよびシングル トランスペアレント モードでコマンドを入力できます。マルチ モード（ルーテッドまたはトランスペアレント マルチ モード）での適応型セキュリティ アプライアンスの動作に対して、システム コンテキスト（管理者またはユーザ コンテキストからでなく）からは **hw-module** コマンドの実行しかできません。

次のコマンドを使用して、リロード、シャットダウン、リセット、パスワードの回復、および IPS SSP を適応型セキュリティ アプライアンスから直接回復します。

- **hw-module module** *slot_number* **reload**

  このコマンドは、ハードウェアをリセットすることなく IPS SSP 上のソフトウェアをリロードします。IPS SSP がアップ状態の場合にのみ有効です。

- **hw-module module** *slot_number* **shutdown**

  このコマンドは、IPS SSP 上のソフトウェアをシャットダウンします。IPS SSP がアップ状態の場合にのみ有効です。

- **hw-module module** *slot_number* **reset**

  このコマンドは、IPS SSP のハードウェア リセットを実行します。IPS SSP がアップ、ダウン、無応答、復旧状態のいずれかにある場合に適用できます。

- **hw-module module** *slot_number* **password-reset**

  このコマンドは、IPS SSP の cisco という CLI アカウントのパスワードをデフォルトの **cisco** に戻します。

- **hw-module module** *slot_number* **recover** [**boot** | **stop** | **configure**]

  recover コマンドは、リカバリ パラメータの設定または変更のためのインタラクティブ オプションのセットを表示します。パラメータを変更、または既存の設定を保持するには、Enter を押します。

  - **hw-module module** *slot_number* **recover boot**

    このコマンドは、IPS SSP のリカバリを開始します。IPS SSP がアップ状態の場合にのみ適用できます。

  - **hw-module module** *slot_number* **recover stop**

    このコマンドは、IPS SSP のリカバリを終了します。IPS SSP が復旧状態の場合にのみ適用できます。

注意　IPS SSP のリカバリを停止する必要がある場合、IPS SSP のリカバリを開始してから 30 ～ 45 秒以内に **hw-module module 1 recover stop** コマンドを発行する必要があります。これ以上待つと、予期しない結果を招く場合があります。たとえば、IPS SSP が無応答状態になる可能性があります。

  - **hw-module module 1 recover configure**

    このコマンドを使用して、IPS SSP のリカバリのためのパラメータを設定します。必須パラメータは、IP アドレスおよびリカバリ イメージの TFTP URL の場所です。

    例

```
ips-ssp# hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

詳細情報

IPS SSP システム イメージの復旧の手順については、「IPS SSP システム イメージのインストール」（P.20-1）を参照してください。

ヘルスおよびステータス情報

IPS SSP の一般的なヘルス情報を表示するには、**show module 1 details** コマンドを使用します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.1(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
```

```
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

出力には、IPS SSP がアップ状態であることが表示されます。ステータスが Down を示している場合は、**hw-module module 1 reset** コマンドを使用してリセットできます。

```
asa# hw-module module 1 reset

The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
Data plane Status:  Not Applicable
Status:             Shutting Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
Data plane Status:  Not Applicable
Status:             Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
```

```
Data plane Status:  Not Applicable
Status:             Init
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Reload
App. Status Desc:   Starting up
App. version:       7.1(1)E4
Data plane Status:  Down
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

IPS SSP の復旧に問題がある場合は、**debug module-boot** コマンドを使用して、ブート時に出力を表示します。TFTP サーバに適切な IP アドレスを使用しており、TFTP サーバに適切なファイルがあることを確認します。その後、再び **hw-module module 1 recover** コマンドを使用してモジュールを復元します。

```
ips-ssp# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.10.10.10//IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img
Port IP Address [0.0.0.0]: 10.10.10.11
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.10.10.254

asa(config)# debug module-boot
debug module-boot enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
```

```
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2010
Slot-1 141> Platform ASA5585-SSP-IPS20
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=192.0.2.3
Slot-1 147>   SERVER=192.0.2.15
Slot-1 148>   GATEWAY=192.0.2.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSP-K9-sys-1.1-a-7.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img@192.0.2.15 via 192.0.2.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2010
Slot-1 161> Platform ASA5585-SSP-IPS20
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=192.0.2.3
Slot-1 167>   SERVER=192.0.2.15
Slot-1 168>   GATEWAY=192.0.2.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img@192.0.2.15 via 192.0.2.254
```

IPS スイッチポートで停止したトラフィック フロー

問題　IPS SSP がリセットされるか、シャットダウンされると、IPS SSP (1/x) にあるポート上のトラフィックは適応型セキュリティを通過しなくなります。このことは、トラフィックが IPS にモニタされているかどうかに関係なく、これらのポートを通過するすべてのトラフィックに影響します。IPS SSP がリセットまたはシャットダウンされると、ポート上のリンクがダウンします。

考えられる原因　IPS SSP (1/x) にあるポートを使用し、何らかのメカニズムで IPS SSP をリセットまたはシャットダウンしました。

ソリューション　適応型セキュリティ アプライアンス (0/x) 上のポートは、IPS SSP がリセットまたはシャットダウンされてもリンクを失わないので、代わりにこれらのポートを使用してください。

フェールオーバー シナリオ

設定変更、シグニチャおよびシグニチャ エンジンのアップデート、サービス パック、IPS SSP での SensorApp のクラッシュの場合は、次のフェールオーバー シナリオを ASA 5585-X に適用します。

フェールオープン モードの単一の ASA 5585-X

- ASA が IPS SSP でフェールオープン モードに設定されていて、IPS SSP で設定変更、またはシグニチャおよびシグニチャ エンジンのアップデートが発生する場合、トラフィックは検査されずに ASA を通過します。
- ASA が IPS SSP でフェールオープン モードに設定されていて、IPS SSP で SensorApp のクラッシュ、またはサービス パックのアップグレードが発生する場合、トラフィックは検査されずに ASA を通過します。

フェールクローズ モードの単一の ASA 5585-X

- ASA が IPS SSP でフェールクローズ モードに設定されていて、IPS SSP で設定変更、またはシグニチャおよびシグニチャ エンジンのアップデートが発生する場合、ASA を通過するトラフィックは停止されます。
- ASA が IPS SSP でフェールクローズ モードに設定されていて、IPS SSP で SensorApp のクラッシュ、またはサービス パックのアップグレードが発生する場合、ASA を通過するトラフィックは停止されます。

フェールオープン モードでの 2 台の ASA 5585-X

- ASA がフェールオープン モードに設定されていて、アクティブな ASA 上の IPS SSP で設定変更、またはシグニチャおよびシグニチャ エンジンのアップデートが発生する場合、トラフィックは引き続き、検査されずにアクティブな ASA を通過します。フェールオーバーはトリガーされません。
- ASA がフェールオープン モードに設定されていて、アクティブな ASA 上の IPS SSP で SensorApp のクラッシュ、またはサービス パックのアップグレードが発生する場合、フェールオーバーがトリガーされ、トラフィックはこれまでスタンバイ IPS SSP であった IPS SSP を通過します。

フェールクローズ モードでの 2 台の ASA 5585-X

- ASA がフェールクローズ モードに設定されていて、アクティブな ASA 上の IPS SSP で設定変更、またはシグニチャおよびシグニチャ エンジンのアップデートが発生する場合、アクティブな ASA を通過するトラフィックは停止されます。フェールオーバーはトリガーされません。
- ASA がフェールクローズ モードに設定されていて、アクティブな ASA 上の IPS SSP で SensorApp のクラッシュ、またはサービス パックのアップグレードが発生する場合、フェールオーバーがトリガーされ、トラフィックはこれまでスタンバイ IPS SSP であった IPS SSP を通過します。

設定例

プライマリ ASA 用に次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

セカンダリ ASA 用に次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

CHAPTER 19

Cisco IPS ソフトウェアの概要

（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、最新の Cisco IPS ソフトウェアの入手方法に関する情報を示します。次のような構成になっています。

- 「IPS 7.1(1)E4 のファイル」（P.19-1）
- 「Cisco IPS ソフトウェアの入手方法」（P.19-2）
- 「IPS ソフトウェアのバージョン管理」（P.19-3）
- 「IPS ソフトウェア リリースの例」（P.19-6）
- 「アップグレードの注意事項と警告」（P.19-8）
- 「IPS マニュアルへのアクセス」（P.19-9）
- 「Cisco Security Intelligence Operations」（P.19-10）
- 「Cisco.com からのライセンス キーの取得」（P.19-10）

IPS 7.1(1)E4 のファイル

（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。

次のファイルは、Cisco IPS 7.1(1)E4 の一部です。

- Readme
  - IPS-7-1-1-E4.readme.txt
- システム イメージ ファイル
  - IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img

  - IPS-SSP_40-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-1-E4.img
- リカバリ イメージ ファイル
  - IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-1-E4.pkg

Cisco IPS ソフトウェアの入手方法

メジャーおよびマイナー アップデート、サービス パック、シグニチャおよびシグニチャ エンジンのアップデート、システム ファイルおよびリカバリ ファイル、ファームウェア アップグレード、および Readme は、Cisco.com の Download Software サイトにあります。シグニチャのアップデートは、約 1 週間ごとに、また必要に応じて頻繁に Cisco.com に掲示されます。サービス パックは必要に応じて Cisco.com に掲示されます。メジャーおよびマイナー アップデートも定期的に掲示されます。最新の IPS ソフトウェアがないかどうか、定期的に Cisco.com を確認してください。

ソフトウェアをダウンロードする前に、暗号化アクセス用のアカウントが必要です。Download Software サイトから IPS ソフトウェアを初めてダウンロードするときに、このアカウントを設定します。最新のソフトウェア リリースに関する情報を受信するように IPS Alert Bulletins に申し込めます。

（注） ソフトウェアをダウンロードするには、Cisco.com にログインする必要があります。ソフトウェアのダウンロードには、有効な IPS メンテナンス契約と Cisco.com のパスワードが必要です。シグニチャ アップデートの適用にはセンサー ライセンスが必要です。

IPS ソフトウェアのダウンロード

Cisco.com のソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　[Support] ドロップダウン メニューから、[Download Software] を選択します。

ステップ 3　[Select a Software Product Category] で [Security Software] を選択します。

ステップ 4　[Intrusion Prevention System (IPS)] を選択します。

ステップ 5　ユーザ名とパスワードを入力します。

ステップ 6　[Download Software] ウィンドウで、[IPS Appliances] > [Cisco Intrusion Prevention System] を選択し、ダウンロードするバージョンをクリックします。

（注） ソフトウェアのダウンロードには、IPS サブスクリプション サービス ライセンスが必要です。

ステップ 7　必要なソフトウェア ファイルのタイプをクリックします。ウィンドウの右側のリストに使用可能なファイルが表示されます。ファイル名、ファイル サイズ、メモリおよびリリース日でソートできます。リリース ノートおよびその他の製品マニュアルにアクセスできます。

ステップ 8　ダウンロードするファイルをクリックします。ファイルの詳細が表示されます。

ステップ 9　ファイルが正しいことを確認して、[Download] をクリックします。

ステップ 10　[Agree] をクリックして、ソフトウェア ダウンロード規則に同意します。Cisco.com から初めてファイルをダウンロードする場合は、先に [Encryption Software Export Distribution Authorization] フォームに必要事項を入力する必要があります。

- フォームに入力し、[Submit] をクリックします。

  Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy が表示されます。
- ポリシーを読み、[I Accept] をクリックします。

  [Encryption Software Export/Distribution] フォームが表示されます。

すでに [Encryption Software Export Distribution Authorization] フォームに記入し、Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy を読んで承諾した場合、これらのフォームは表示されません。[File Download] ダイアログボックスが表示されます。

ステップ 11　ファイルを開くか、コンピュータに保存します。

ステップ 12　Readme またはこれらのリリース ノートの手順に従い、アップデートをインストールします。

詳細情報

- 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、「Cisco.com からのライセンス キーの取得」（P.19-10）を参照してください。
- IPS ファイルのバージョン管理方式の説明については、「IPS ソフトウェアのバージョン管理」（P.19-3）を参照してください。

IPS ソフトウェアのバージョン管理

Cisco.com から IPS ソフトウェア イメージをダウンロードするときは、そのバージョン管理方式を理解して、ファイルがそれぞれ、ベース ファイル、累積ファイル、あるいは差分ファイルのどれであるかを知っておく必要があります。

メジャー アップデート

メジャー アップデートには、製品の新しい機能やアーキテクチャの変更などが含まれます。たとえば、Cisco IPS 7.1 ベース バージョンには、その前のメジャー リリース以降の内容（マイナー アップデート機能、サービス パックのフィックス、およびシグニチャ アップデート）すべて（廃止された機能を除く）に加えて、新しい変更が組み込まれます。メジャー アップデート 7.1(1) には、5.1(6) 以降が必要です。各メジャー アップデートには、対応するシステムおよびリカバリ パッケージがあります。

（注）　7.1(1) メジャー アップデートは、5.1(6) 以降のセンサーを 7.1(1) にアップグレードするのに使用されます。すでに 7.1(1) がインストールされたセンサーに 7.1(1) を再インストールする場合は、メジャー アップデートではなくシステム イメージまたはリカバリ手順を使用します。

マイナー アップデート

マイナー アップデートは、メジャー バージョンに対する差分です。マイナー アップデートは、サービス パックのベース バージョンでもあります。7.1 の最初のマイナー アップデートは 7.2 です。マイナー アップデートは、製品のマイナーな拡張を行うためにリリースされます。マイナー アップデートには、前回のメジャー バージョン以降に発生したすべてのマイナー機能（廃止された機能を除く）、サービス パックのフィックス、シグニチャ アップデートに加えて、新しいマイナー機能のリリースが組み込まれます。前のメジャー バージョンまたはマイナー バージョンにマイナー アップデートをインストールできます（多くの場合、それ以前のバージョンでもインストールできます）。最新のマイナー

バージョンにアップグレードする必要がある最小サポート バージョンは、マイナー アップデートに付属する Readme に示されています。各マイナー アップデートには、対応するシステムおよびリカバリ パッケージがあります。

サービス パック

サービス パックは、ベース バージョンのリリース後の累積です（マイナーまたはメジャー）。サービス パックは、障害フィックスのリリースとして使用され、新しい機能強化は行われません。サービス パックには、前回のベース バージョン（マイナーまたはメジャー）以降に発生したすべてのサービス パックのフィックスに加えて、新しい障害フィックスのリリースが組み込まれます。サービス パックには、マイナー バージョンが必要です。最新のサービス パックにアップグレードする必要がある最小サポート バージョンは、サービス パックに付属する Readme に示されています。サービス パックには最新のエンジン アップデートも含まれています。たとえば、サービス パック 7.1(3) がリリースされて、E4 が最新のエンジン レベルである場合、サービス パックは 7.1(3)E4 としてリリースされます。

パッチ リリース

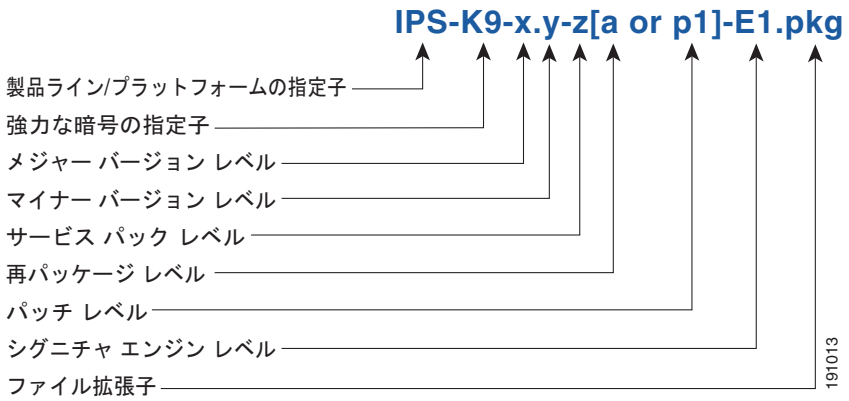
パッチ リリースは、ソフトウェア リリース後にアップグレード バイナリで確認された障害に対処するために使用されます。これらの障害に対処する、次のメジャー アップデートやマイナー アップデート、またはサービス パックを待たずに、パッチが公開されることがあります。パッチは、関連するサービス パック レベルにそれ以前のすべてのパッチ リリースを含みます。パッチは、次の正式なメジャー アップデートやマイナー アップデート、またはサービス パックにまとめられます。

パッチ リリースをインストールする前に、最新のメジャー アップデートやマイナー アップデート、またはサービス パックをインストールする必要があります。たとえば、パッチ リリース 7.1(1p1) には 7.1(1) が必要です。

（注） 新しいパッチへのアップグレードに、古いパッチのアンインストールは必要ありません。たとえば、パッチ 7.1(1p1) から 7.1(1p2) へのアップグレードは、最初に 7.1(1p1) をアンインストールすることなく実行できます。

図 19-1 は、IPS ソフトウェア ファイルの各部分がメジャー アップデートとマイナー アップデート、サービス パック、およびパッチ リリースの何を表すかを図示したものです。

図 19-1　メジャー アップデートとマイナー アップデート、サービス パック、およびパッチ リリースに対応する IPS ソフトウェア ファイル名

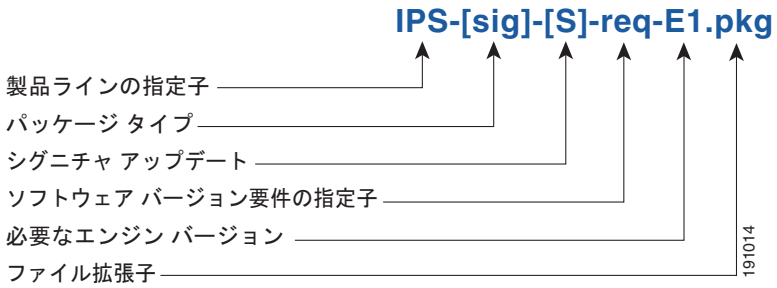


シグニチャ アップデート

シグニチャ アップデートは、悪意のあるネットワーク アクティビティを認識するように設計された規則セットを含むパッケージ ファイルです。シグニチャ アップデートは、他のソフトウェア アップデートとは別にリリースされます。メジャー アップデートまたはマイナー アップデートがリリースされるたびに、少なくとも 6 ヵ月間は新しいバージョンおよび次に古いバージョンに、シグニチャ アップデートをインストールできます。シグニチャ アップデートは、必要なシグニチャ エンジンのバージョンによって異なります。このため、*req* 指定子では、特定のシグニチャ アップデートのサポートに必要なシグニチャ エンジンを示します。

図 19-3 は、IPS ソフトウェア ファイルの各部分がシグニチャ アップデートの何を表すかを図示したものです。

図 19-2　シグニチャ アップデートに対応する IPS ソフトウェア ファイル名

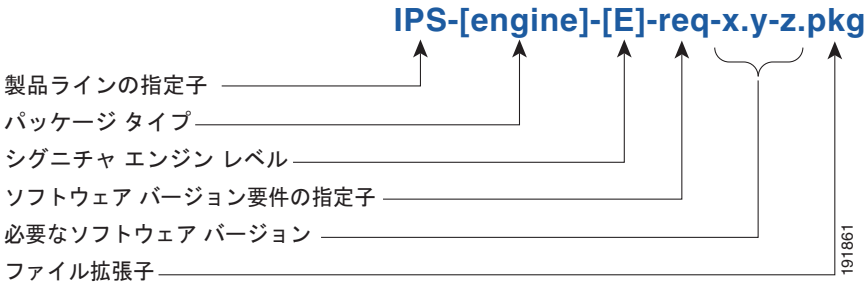


シグニチャ エンジン アップデート

シグニチャ エンジン アップデートは、新しいシグニチャ アップデートをサポートするバイナリ コードを含む実行可能ファイルです。シグニチャ エンジン ファイルには特定のサービス パックが必要です。これは、*req* 指定子でも指定されます。

図 19-3 は、IPS ソフトウェア ファイルの各部分がシグニチャ エンジン アップデートの何を表すかを図示したものです。

図 19-3　シグニチャ エンジン アップデートに対応する IPS ソフトウェア ファイル名



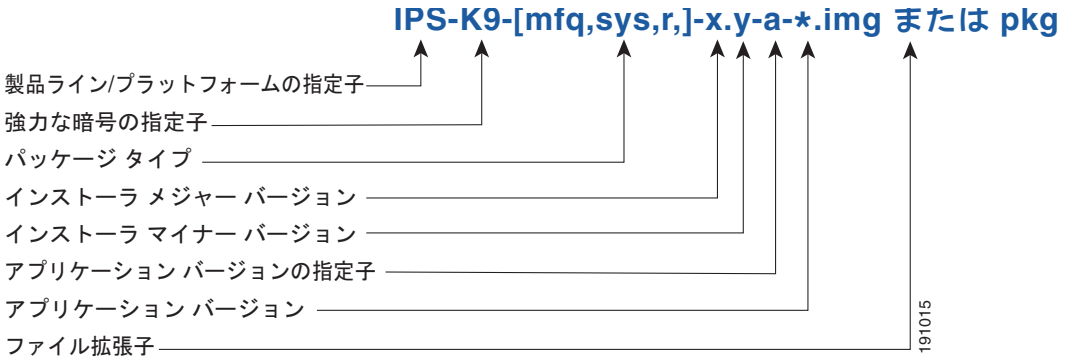
リカバリ イメージおよびシステム イメージのファイル

リカバリ イメージおよびシステム イメージのファイルには、インストーラと基盤アプリケーションで別個のバージョンが含まれています。インストーラのバージョンには、メジャー バージョン フィールドとマイナー バージョン フィールドが含まれています。メジャー バージョンは、イメージ インストーラへの大きな変更が 1 つあるたびに増加します。たとえば、.tar から rpm への切り替えやカーネルの変更などがあります。マイナー バージョンは、次のいずれかによって増加します。

- インストーラへの小さな変更、たとえばユーザ プロンプトの追加などがあった場合。
- イメージ ファイルを再パッケージしてインストーラの障害や問題に対処する必要がある場合、再パッケージはインストーラのマイナー バージョンを 1 つ増加させる必要があります。

図 19-4 は、IPS ソフトウェア ファイルの各部分がリカバリ イメージおよびシステム イメージ ファイルの何を表すかを図示したものです。

図 19-4　リカバリ イメージおよびシステム イメージのファイルに対応する IPS ソフトウェア ファイル名



IPS ソフトウェア リリースの例

（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。

表 19-1 は、プラットフォームに依存しない Cisco IPS ソフトウェア リリースの例を示します。

表 19-1　プラットフォームに依存しないリリースの例

リリース	目標頻度	ID	バージョンの例	ファイル名の例
シグニチャ アップデート[1]	毎週	sig	S369	IPS-sig-S369-req-E4.pkg
シグニチャ エンジン アップデート[2]	必要に応じて	engine	E4	IPS-engine-E4-req-7.1-1.pkg
サービス パック[3]	半年ごと または必要に応じて	—	7.1(3)	IPS-K9-7.1-3-E4.pkg
マイナー バージョン アップデート[4]	毎年	—	7.2(1)	IPS-K9-7.2-1-E4.pkg **（注）** IPS-AIM-K9-7.2-1-E4.pkg は、AIM-IPS のマイナー バージョン アップデートです。IPS-NME-K-9-7.2-1-E4.pkg は、NME-IPS のマイナー バージョン アップデートです。

表 19-1　プラットフォームに依存しないリリースの例 （続き）

リリース	目標頻度	ID	バージョンの例	ファイル名の例
メジャー バージョン アップデート[5]	毎年	—	8.0(1)	IPS-K9-8.0-1-E4.pkg
パッチ リリース[6]	必要に応じて	patch	7.1(1p1)	IPS-K9-patch-7.1-1pl-E4.pkg
リカバリ パッケージ[7]	毎年または必要に応じて	r	1.1-7.1(1)	IPS-K9-r-1.1-a-7.1-1-E4.pkg

1. シグニチャ アップデートには、最新の累積 IPS シグニチャが含まれます。
2. シグニチャ エンジン アップデートは、以降のシグニチャ アップデートで新しいシグニチャによって使用される、新しいエンジンまたはエンジン パラメータを追加します。
3. サービス パックには、障害のフィックスが含まれます。
4. マイナー バージョンには、新しいマイナー バージョンの特性または機能、もしくはその両方が含まれます。
5. メジャー バージョンには、新しいメジャー バージョンの機能やアーキテクチャが含まれます。
6. パッチ リリースは暫定フィックスです。
7. 同じ基盤アプリケーション イメージを含む新しいリカバリ パッケージをリリースする必要がある場合は、r 1.1 を r 1.2 に変更できます。たとえば、インストーラの障害フィックスがある場合、基盤アプリケーション バージョンがまだ 7.0(4) であっても、リカバリ パーティション イメージは r 1.2 になります。

表 19-2 に、プラットフォームに依存するソフトウェア リリースの例を示します。

表 19-2　プラットフォームに依存するリリースの例

リリース	目標頻度	ID	サポートされるプラットフォーム	ファイル名の例
システム イメージ[1]	毎年	sys	各センサー プラットフォームに対して個別のファイル	IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
メンテナンス パーティション イメージ[2]	毎年	mp	IDSM2	c6svc-mp.2-1-2.bin.gz
ブートローダ	必要に応じて	bl	AIM IPS NME IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin （x、y、z はリリース番号）
ミニカーネル	必要に応じて	mini-kernel	AIM IPS NME IPS	pse_mini_kernel_1.1.10.64.bz2

1. システム イメージには、センサー全体のイメージの再作成に使用される、リカバリとアプリケーションを組み合わせたイメージが含まれます。
2. メンテナンス パーティション イメージには、IDSM2 メンテナンス パーティションの完全なイメージが含まれます。ファイルは、IDSM2 アプリケーション パーティションからインストールされますが、IDSM2 アプリケーション パーティションには影響しません。

表 19-3 に、プラットフォーム固有名で使用されるプラットフォーム ID を示します。

表 19-3　プラットフォーム ID

センサー ファミリ	ID
IPS 4240 シリーズ	4240
IPS 4255 シリーズ	4255
IPS 4260 シリーズ	4260
IPS 4270-20 シリーズ	4270_20
Catalyst 6K 用 IDS モジュール	IDSM2
IPS ネットワーク モジュール	AIM NME
適応型セキュリティ アプライアンスモジュール	SSC_5 SSM_10 SSM_20 SSM_40 SSP_10 SSP_20 SSP_40 SSP_60

詳細情報

Cisco.com でこれらのファイルにアクセスする方法については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

アップグレードの注意事項と警告

次のアップグレードの注意事項と警告は、IPS SSP のアップグレードに適用されます。

- IPS 7.1(1)E4 は、IPS SSP をインストールした ASA 5585-X 適応型セキュリティ アプライアンスだけに適用されます。
- IPS 7.1(1)E4 をアンインストールできません。システム イメージ ファイルを使用して、センサーのイメージを再作成する必要があります。これによって、すべての設定が失われます。
- Cisco.com からソフトウェア アップグレードを受信し、使用するには、センサーごとに有効な Cisco Service for IPS メンテナンス契約が必要です。
- グローバル相関のヘルス ステータスは、デフォルトで赤に設定され、グローバル相関が正しくアップデートされると緑に変わります。グローバル相関の正常なアップデートには、DNS サーバまたは HTTP プロキシ サーバが必要です。グローバル相関のヘルス ステータスおよびセンサーの全体的なヘルス ステータスは、センサーで DNS または HTTP プロキシ サーバが設定されるまで赤になります。DNS または HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合、グローバル相関をディセーブルにし、グローバル相関ヘルス ステータスを除外するようにセンサー ヘルス ステータスを設定すると、赤色のグローバル相関ヘルスおよび全体センサー ヘルス ステータスに対処できます。

- センサーにアップデートをインストールし、そのセンサーがリブート後に使用できなくなった場合は、センサーのイメージを再作成する必要があります。センサーのイメージを次の方法で再作成できます。
  - **hw-module module 1 recover configure/boot** コマンドを使用して、適応型セキュリティ アプライアンスからイメージを再作成します。
  - ROMMON を使用して、適応型セキュリティ アプライアンスからイメージを再作成します。

注意　センサーのシステム イメージをインストールすると、アカウントはすべて削除され、デフォルトのアカウントとパスワードが **cisco** にリセットされます。

詳細情報

- Cisco.com のダウンロードにアクセスする手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。
- IPS SSP のイメージを再作成するために **hw-module module 1 recover configure/boot** コマンドを使用する手順については、「hw-module コマンドを使用したシステム イメージのインストール」（P.20-4）を参照してください。
- IPS SSP のイメージを再作成するために ROMMON を使用する手順については、「ROMMON を使用したシステム イメージのインストール」（P.20-6）を参照してください。

IPS マニュアルへのアクセス

IPS のマニュアルは次の URL にあります。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

または、Cisco.com から IPS マニュアルへアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　[Support] をクリックします。

ステップ 3　[Support and Documentation] で、[Security] をクリックします。

ステップ 4　[Products] > [Security] > [Intrusion Prevention System (IPS)] > [IPS Appliances] > [Cisco IPS 4200 Series Sensors] をクリックします。

[Cisco IPS 4200 Series Sensors] ウィンドウが表示されます。

ステップ 5　次のカテゴリの 1 つをクリックして、Cisco IPS のマニュアルにアクセスします。

- **Download Software**：Download Software サイトに移動します。

（注）　ソフトウェア ダウンロード サイトにアクセスするには、Cisco.com にログインする必要があります。

- **Release and General Information**：ドキュメント ロードマップとリリース ノートがあります。
- **Reference Guides**：コマンド リファレンスとテクニカル リファレンスがあります。
- **Design**：デザイン ガイドとデザイン テクニカル ノートがあります。
- **Install and Upgrade**：ハードウェア インストレーション ガイドと規制ガイドがあります。

- **Configure**：IPS CLI、IDM、および IME 用のコンフィギュレーション ガイドがあります。
- **Troubleshoot and Alerts**：TAC テクニカル ノートとフィールド ノートがあります。

Cisco Security Intelligence Operations

Cisco.com の Cisco Security Intelligence Operations サイトは、現在の脆弱性とセキュリティの脅威に関するインテリジェンス レポートを提供しています。また、ネットワークを保護し、組織のリスクを減らすようにセキュリティ システムを展開するために役立つその他のセキュリティ項目についてもレポートしています。

最も効果的にネットワークの保護および管理を実行できるように、最新のセキュリティの脅威に注意する必要があります。Cisco Security Intelligence Operations には、日付、重大度、緊急度別に掲載されている上位 10 のインテリジェンス レポートがあり、また脅威に対応できる新しいシグニチャの有無も含まれています。

Cisco Security Intelligence Operations には、興味深いセキュリティの記事が記載された Security News セクションがあります。関連するセキュリティ ツールおよびリンクがあります。

Cisco Security Intelligence Operations には次の URL からアクセスできます。

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations は、シグニチャ ID、タイプ、構造、および説明などの個別のシグニチャ情報のリポジトリでもあります。

セキュリティ アラートおよびシグニチャを次の URL で検索できます。

http://tools.cisco.com/security/center/search.x

Cisco.com からのライセンス キーの取得

ここでは、Cisco.com からライセンス キーを取得する方法、および CLI、IDM、または IME を使用してライセンス キーをインストールする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。

- 「ライセンスについて」（P.19-10）
- 「IPS 製品用のサービス プログラム」（P.19-11）
- 「IDM または IME を使用したライセンス キーの取得とインストール」（P.19-12）

ライセンスについて

ライセンス キーなしでもセンサーは動作しますが、シグニチャ アップデートの取得およびグローバル相関機能の使用にはライセンス キーが必要です。ライセンス キーを取得するには、次のものを用意する必要があります。

- Cisco Service for IPS サービス契約

  契約を購入するには、リセラー、シスコのサービスまたは製品の営業担当者にお問い合わせください。

- IPS デバイス シリアル番号

  IPS デバイス シリアル番号を IDM または IME で確認するには、IDM で、[Configuration] > [Sensor Management] > [Licensing] を選択し、IME の場合は [Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。または、CLI で **show version** コマンドを使用します。

- 有効な Cisco.com ユーザ名およびパスワード

試用ライセンス キーも利用できます。契約の問題により、センサーにライセンスを設定できない場合は、ライセンスの必要なシグニチャ アップデートをサポートする 60 日間の試用ライセンスを取得できます。

ライセンス キーは、Cisco.com ライセンス サーバから取得できます。取得したライセンス キーは、センサーに配信されます。あるいは、ローカル ファイルで提供されるライセンス キーでライセンス キーを更新することもできます。http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックしてライセンス キーを要求します。

次の場所でライセンス キーのステータスを確認できます。

- [IDM Home] ウィンドウの [Health] タブ上の [Licensing] セクション
- [IDM Licensing] ペイン（[Configuration] > [Licensing]）
- [Licensing] タブ上の [Device Details] セクション内の [IME Home] ページ
- CLI ログイン時のライセンス通知

IDM、IME、または CLI を開始するとき、ライセンス ステータスが必ず通知されます（ライセンス キーが試用かどうか、無効かどうか、有効期限切れかどうか）。ライセンス キーがない、無効、または期限切れの場合、IDM、IME、および CLI を引き続き使用できますが、シグニチャ アップデートをダウンロードすることはできません。

センサー上にすでに有効なライセンスがある場合は、[License] ペイン上の [Download] をクリックすることで、IDM または IME を実行しているコンピュータに自分のライセンス キーのコピーをダウンロードし、ローカル ファイルに保存できます。その後、紛失または破損したライセンスと置き換えることができます。あるいは、センサーのイメージを再作成した後にライセンスを再インストールできます。

IPS 製品用のサービス プログラム

ライセンス キーをダウンロードしたり、最新の IPS シグニチャ アップデートを取得したりするには、IPS 製品用の Cisco Services for IPS サービス契約が必要です。シスコと直接取り引きしている場合は、担当のアカウント マネージャまたはサービス アカウント マネージャに連絡して、Cisco Services for IPS サービス契約を購入します。シスコと直接取り引きしていない場合は、1 ティアまたは 2 ティア パートナーからサービス アカウントを購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS

- IDSM2
- NME IPS

IPS を搭載していない ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合は、SMARTnet 契約を購入する必要があります。

（注） SMARTnet は、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトの NBD ハードウェア交換を提供します。

IPS SSP を搭載して出荷される ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合、あるいは IPS SSP を購入して ASA 5500 シリーズ適応型セキュリティ アプライアンス製品に追加する場合は、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS は、IPS シグニチャ アップデート、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトの NBD ハードウェア交換を提供します。

たとえば、ASA 5585-X を購入した後、IPS の追加が必要になり、ASA-IPS10-K9 を購入する場合は、Cisco Services for IPS サービス契約の購入が必要になります。Cisco Services for IPS サービス契約を結んだ後は、製品シリアル番号を用意して、ライセンス キーを要求する必要があります。

注意 製品を RMA に出したことがある場合、シリアル番号は変更されています。その場合は、新しいシリアル番号用に新しいライセンス キーを取得する必要があります。

IDM または IME を使用したライセンス キーの取得とインストール

（注） ライセンス キーを要求するには、有効な Cisco.com ユーザ名とパスワードに加え、Cisco Services for IPS サービス契約も必要です。

ライセンス キーを取得およびインストールするには、次の手順を実行してください。

ステップ 1　管理者権限を持つアカウントを使用して IDM または IME にログインします。

ステップ 2　IDM で [Configuration] > [Sensor Management] > [Licensing] を選択します。IME で [Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。

[Licensing] ペインに現在のライセンスのステータスが表示されます。すでにライセンスをインストールしている場合は、必要に応じて [Download] をクリックしてライセンスを保存できます。

ステップ 3　次のいずれかを実行してライセンス キーを取得します。

- [Cisco.com] オプション ボタンをクリックして、Cisco.com からライセンスを取得します。IDM または IME は、Cisco.com のライセンス サーバにアクセスし、サーバにシリアル番号を送信してライセンス キーを取得します。これがデフォルトの方式です。ステップ 4 に進みます。

- [License File] オプション ボタンをクリックして、ライセンス ファイルを使用します。このオプションを使用するには、www.cisco.com/go/license でライセンス キーを申請する必要があります。ライセンス キーは、電子メールで送信されてきます。IDM または IME がアクセスできるドライブにそのライセンス キーを保存します。このオプションは、ご使用のコンピュータが Cisco.com にアクセスできない場合に役立ちます。ステップ 7 に進みます。

ステップ 4　[Update License] をクリックし、[Licensing] ダイアログボックスで [Yes] をクリックして続行します。[Status] ダイアログボックスは、センサーが Cisco.com への接続を試行していることを示します。[Information] ダイアログボックスで、ライセンス キーがアップデートされたことを確認します。

ステップ 5　[OK] をクリックします。

ステップ 6　www.cisco.com/go/license にアクセスします。

ステップ 7　必要なフィールドに入力します。ライセンス キーは、指定した電子メール アドレスに送信されます。

注意　ライセンス キーは、指定されたシリアル番号を持つ IPS デバイス上でしか動作しないため、正確なシリアル番号を用意する必要があります。

ステップ 8　IDM または IME を実行中のクライアントがアクセスできるハードディスク ドライブまたはネットワーク ドライブにライセンス キーを保存します。

ステップ 9　IDM または IME にログインします。

ステップ 10　IDM で [Configuration] > [Sensor Management] > [Licensing] を選択します。IME で [Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。

ステップ 11　[Update License] で、[License File] オプション ボタンをクリックします。

ステップ 12　[Local File Path] フィールドに、ライセンス ファイルへのパスを指定するか、[Browse Local] をクリックしてファイルを参照します。

ステップ 13　ライセンス ファイルを参照し、[Open] をクリックします。

ステップ 14　[Update License] をクリックします。

詳細情報

Cisco Services for IPS サービス契約の取得の詳細については、「IPS 製品用のサービス プログラム」（P.19-11）を参照してください。

CLI を使用したライセンス キーの取得とインストール

（注）　新しいライセンス キーの上に古いライセンス キーをインストールすることはできません。

copy *source-url license_file_name* **license-key** コマンドを使用して、ライセンス キーをセンサーにコピーします。

オプション

次のオプションが適用されます。

- *source-url*：コピー元のファイルの場所です。URL またはキーワードを使用できます。
- *destination-url*：コピー先ファイルの場所です。URL またはキーワードを使用できます。

- **license-key**：サブスクリプション ライセンス ファイルです。
- *license_file_name*：受信するライセンス ファイルの名前です。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加する必要があります。

- http:：Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。

  http:[[/[username@]location]/directory]/filename

- https:：Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。

  https:[[/[username@]location]/directory]/filename

（注）　HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

ライセンス キーのインストール

ライセンス キーをインストールするには、次の手順を実行します。

ステップ 1　www.cisco.com/go/license にアクセスしてライセンス キーを要求します。

（注）　ライセンス キーを要求するには、有効な Cisco.com ユーザ名とパスワードに加え、Cisco Services for IPS サービス契約も必要です。

ステップ 2　必要なフィールドに入力します。Cisco IPS シグニチャ サブスクリプション サービス ライセンス キーは、指定した電子メール アドレスに電子メールで送信されます。

（注）　ライセンス キーは、指定されたシリアル番号を持つ IPS デバイス上でしか動作しないため、正確なシリアル番号を用意する必要があります。

ステップ 3　Web サーバ、FTP サーバ、または SCP サーバが存在するシステムにライセンス キーを保存します。

ステップ 4　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 5　ライセンス キーをセンサーにコピーします。

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

ステップ 6　センサーがライセンスされていることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor#
```

詳細情報

- リモート ホストを SSH 既知ホスト リストに追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- リモート ホストを信頼できるホストのリストに追加する手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。
- Cisco Services for IPS サービス契約の取得の詳細については、「IPS 製品用のサービス プログラム」（P.19-11）を参照してください。

CHAPTER 20

IPS SSP システム イメージのインストール

（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 SSP システム イメージをインストールする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。

- 「IPS 7.1(1)E4 のファイル」（P.20-1）
- 「サポートされる FTP および HTTP/HTTPS サーバ」（P.20-2）
- 「ROMMON について」（P.20-2）
- 「TFTP サーバ」（P.20-3）
- 「シリアル ポートへの接続」（P.20-3）
- 「IPS SSP システム イメージのインストール」（P.20-4）
- 「リカバリ パーティションのアップグレード」（P.20-9）
- 「アプリケーション パーティションの復旧」（P.20-10）

IPS 7.1(1)E4 のファイル

（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。

次のファイルは、Cisco IPS 7.1(1)E4 の一部です。

- Readme
  - IPS-7-1-1-E4.readme.txt
- システム イメージ ファイル
  - IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img

  - IPS-SSP_40-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-1-E4.img
- リカバリ イメージ ファイル
  - IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-1-E4.pkg

詳細情報

Cisco.com から IPS ソフトウェア ファイルをダウンロードする手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

サポートされる FTP および HTTP/HTTPS サーバ

次の FTP サーバで IPS ソフトウェアのアップデートがサポートされています。

- WU-FTPD 2.6.2（Linux）
- Solaris 2.8
- Sambar 6.0（Windows 2000）
- Serv-U 5.0（Windows 2000）
- MS IIS 5.0（Windows 2000）

次の HTTP/HTTPS サーバで IPS ソフトウェアのアップデートがサポートされています。

- CSM - Apache サーバ（Tomcat）
- CSM - Apache サーバ（JRun）

ROMMON について

適応型セキュリティ アプライアンスには ROMMON と呼ばれるプリブート CLI が含まれています。これにより、プライマリ デバイスのイメージが紛失、破損、またはその他の理由で通常のアプリケーションをブートできない場合に、適応型セキュリティ アプライアンス上のイメージをブートすることができます。ROMMON は、リモートの適応型セキュリティ アプライアンスの復旧に特に役立ちます（シリアル コンソール ポートが利用可能な場合）。

ROMMON へのアクセスは、適応型セキュリティ アプライアンス シャーシの RJ-45F コネクタで利用可能なシスコ標準の非同期 RS-232C DTE であるシリアル コンソール ポートを介してのみ可能です。シリアル ポートは、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、フロー制御なしに設定されています。

詳細情報

ターミナル サーバを使用する手順については、「シリアル ポートへの接続」（P.20-3）を参照してください。

TFTP サーバ

ROMMON は、TFTP を使用してイメージをダウンロードし、起動します。TFTP は、遅延やエラー回復などのネットワークの問題は処理しません。TFTP は限定的なパケットの整合性チェックを実装するので、正しい整合性値を持つパケットが順番に到着し、エラーが発生する可能性はきわめて低くなります。ただし、TFTP はパイプラインを提供しないので、転送の合計時間は、転送するパケットの数にネットワークの平均 RTT を掛けた値と等しくなります。この制限があるため、TFTP サーバはセンサーと同じ LAN セグメントに配置することを推奨します。RTT が 100 ミリ秒未満のネットワークでは、イメージを確実に伝送する必要があります。一部の TFTP サーバでは、転送可能な最大ファイル サイズが約 32 MB に制限されていることに注意してください。

シリアル ポートへの接続

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を使用するターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで回線およびポートを設定します。イネーブル モードでは、次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。

ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

IPS SSP システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定は失われます。システム イメージをインストールしてセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用する方法や、センサーのブート時にリカバリ パーティションを選択する方法で復旧を試みてください。

ここでは、**hw-module** コマンドまたは ROMMON を使用して IPS SSP のシステム イメージをインストールする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。

- 「hw-module コマンドを使用したシステム イメージのインストール」（P.20-4）
- 「ROMMON を使用したシステム イメージのインストール」（P.20-6）

hw-module コマンドを使用したシステム イメージのインストール

システム イメージをインストールするには、適応型セキュリティ アプライアンスの CLI を使用して TFTP サーバから IPS SSP にソフトウェア イメージを転送します。適応型セキュリティ アプライアンスは IPS SSP の ROMMON アプリケーションと通信してイメージを転送できます。

（注）　指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。

（注）　ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

IPS SSP のソフトウェア イメージをインストールするには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　イネーブル モードを開始します。

```
asa# enable
```

ステップ 3　IPS SSP のリカバリ設定を行います。

```
asa (enable)# hw-module module 1 recover configure
```

（注）　リカバリ設定を誤った場合は、**hw-module module 1 recover stop** コマンドを使用してシステム イメージの再作成を停止すると、設定を修正できます。

ステップ 4　ソフトウェア イメージの TFTP URL を指定します。

```
Image URL [tftp://0.0.0.0/]:
```

例

```
Image URL [tftp://0.0.0.0/]: tftp://192.0.2.5/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

ステップ 5　IPS SSP のコマンドおよびコントロール インターフェイスを指定します。

（注）　ポート IP アドレスは、IPS SSP の管理 IP アドレスです。

```
Port IP Address [0.0.0.0]:
```

例

```
Port IP Address [0.0.0.0]: 192.0.2.22
```

ステップ 6　VLAN ID を 0 のままにしておきます。

```
VLAN ID [0]:
```

ステップ 7　IPS SSP のデフォルト ゲートウェイを指定します。

```
Gateway IP Address [0.0.0.0]:
```

例

```
Gateway IP Address [0.0.0.0]: 192.0.2.254
```

ステップ 8　リカバリを実行します。

```
asa# hw-module module 1 recover boot
```

これにより、TFTP サーバから IPS SSP にソフトウェア イメージが転送され、再起動されます。

ステップ 9　リカバリが完了するまで、定期的に確認します。

（注）　ステータスは、リカバリ中は `Recovery` となり、インストールが完了すると `Up` になります。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS10
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.1(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.11
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
```

```
Mgmt TLS enabled    true
asa#
```

（注）　出力の [Status] フィールドは IPS SSP の動作ステータスを示します。IPS SSP の動作ステータスは、通常は「Up」と表示されます。適応型セキュリティ アプライアンスはソフトウェア イメージを IPS SSP に転送しますが、出力の [Status] フィールドには「Recover」と表示されます。適応型セキュリティ アプライアンスがソフトウェア イメージの転送を完了し、IPS SSP を再起動すると、新たに転送されたイメージが実行されます。

（注）　このプロセス中に発生する可能性のあるエラーをデバッグするには、**debug module-boot** コマンドを使用して、ソフトウェア インストール プロセスのデバッグをイネーブルにします。

ステップ 10　IPS SSP に対してセッションを開始します。

ステップ 11　**cisco** を 3 度と新しいパスワードを 2 度入力します。

ステップ 12　**setup** コマンドを使用して IPS SSP を初期化します。

詳細情報

- IPS SSP アプリケーション パーティションの復旧手順については、「アプリケーション パーティションの復旧」（P.20-10）を参照してください。
- IPS ソフトウェアの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

ROMMON を使用したシステム イメージのインストール

適応型セキュリティ アプライアンスで ROMMON を使用して、システム イメージを IPS SSP に TFTP でダウンロードすることにより、IPS SSP のシステム イメージをインストールできます。

IPS SSP のシステム イメージをインストールするには、次の手順を実行します。

ステップ 1　IPS SSP のシステム イメージ ファイル（IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img など）を、適応型セキュリティ アプライアンスからアクセスできる TFTP サーバの TFTP ルート ディレクトリにダウンロードします。

（注）　適応型セキュリティ アプライアンスのイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS SSP をブートします。

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit
```

```
Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr  8 00:12:33 CDT 2010

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

ステップ 3　システムのブート中に、次のプロンプトで Break または Esc キーを押してブートを中断します。ブートをただちに開始するには、Space を押します。

（注）　Break または Esc キーは 10 秒以内に押してください。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

システムが ROMMON モードに入ります。rommon> プロンプトが表示されます。

ステップ 4　現在のネットワーク設定を確認します。

```
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

変数の定義は次のとおりです。

- Address：IPS SSP のローカル IP アドレス
- Server：アプリケーション イメージが格納されている TFTP サーバの IP アドレス
- Gateway：IPS SSP が使用するゲートウェイの IP アドレス
- Port：IPS SSP 管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのままにしておきます）
- Image：システム イメージ ファイル / パス名
- Config：これらのプラットフォームでは未使用

（注）　ネットワーク接続を確立するために、すべての値が必要なわけではありません。address、server、gateway、および image の値は必要です。ローカル環境を設定するために必要な設定がわからない場合は、システム管理者に連絡してください。

ステップ 5　必要に応じて、TFTP ダウンロードに使用するインターフェイスを変更します。

```
rommon> PORT=interface_name
```

（注）　TFTP ダウンロードに使用するデフォルト インターフェイスは PortChannel0/0 です。これは IPS SSP の管理インターフェイスに相当します。

ステップ 6　必要に応じて、IPS SSP 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注）　IPS SSP に割り当てられているのと同じ IP アドレスを使用します。

ステップ 7　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 8　必要に応じて、ゲートウェイの IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 9　次のいずれかのコマンドを使用して、ローカルのイーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスとファイル名を定義します。

```
rommon> IMAGE=path/file_name
```

注意　**IMAGE** コマンドをすべて大文字で入力していることを確認してください。他の ROMMON コマンドは小文字または大文字で入力できますが、**IMAGE** コマンドは、特にすべて大文字で入力する必要があります。

UNIX の例

```
rommon> IMAGE=/system_images/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

（注）　パスは UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルト tftpboot ディレクトリにあるイメージには、IMAGE 指定のディレクトリ名もスラッシュも含まれていません。

Windows の例

```
rommon> IMAGE=¥system_images¥IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

ステップ 11　**set** を入力して Enter を押し、ネットワークの設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定がブート後も保持されるように NVRAM に設定を保存できます。そうしない場合は、ROMMON からイメージをブートするたびにこの情報を入力する必要があります。

ステップ 12　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を防ぐため、システム イメージのインストール中は IPS SSP の電源を切らないでください。

（注）　ネットワーク設定が正しければ、システムは指定されたイメージを IPS SSP にダウンロードし、ブートします。必ず IPS SSP のイメージを使用してください。

詳細情報

- IPS SSP アプリケーション パーティションの復旧手順については、「アプリケーション パーティションの復旧」（P.20-10）を参照してください。
- IPS ソフトウェアの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

リカバリ パーティションのアップグレード

リカバリ パーティションを最新バージョンでアップグレードするには、**upgrade** コマンドを使用します。これにより、センサーのアプリケーション パーティションを復旧する必要がある場合の準備ができます。

（注）　リカバリ パーティション イメージはメジャーおよびマイナー アップデートのために生成されます。サービス パックまたはシグニチャ アップデートのために生成されるという状況はごくまれにしかありません。

センサーのリカバリ パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg など）を、センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバにダウンロードします。

注意　一部のブラウザでは、ファイル名に拡張子が付加されます。保存されたファイルのファイル名は、ダウンロード ページに表示されているファイル名と一致する必要があります。一致しないと、そのファイルはリカバリ パーティションのアップグレードに使用できません。

ステップ 2　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 3　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 4　リカバリ パーティションをアップグレードします。

```
ips-ssp(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg

ips-ssp(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
```

ステップ 5　サーバ パスワードを入力します。アップグレードのプロセスが開始されます。

（注）　この手順では、リカバリ パーティションのイメージだけが再作成されます。アプリケーション パーティションは、このアップグレードでは変更されません。リカバリ パーティションの後にアプリケーション パーティションのイメージを再作成するには、**recover application-partition** コマンドを使用します。

アプリケーション パーティションの復旧

ここでは、アプリケーション パーティションの復旧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。

- 「アプリケーション パーティションについて」（P.20-10）
- 「IPS SSP アプリケーション パーティション イメージの復旧」（P.20-11）

アプリケーション パーティションについて

センサーのアプリケーション パーティション イメージが使用できなくなった場合は、復旧することができます。この方法を使用すると一部のネットワーク設定情報が保持されるので、復旧の実行後、ネットワークにアクセスできます。

recover application-partition コマンドを使用してリカバリ パーティションをブートすると、センサーのアプリケーション パーティションが自動的に復旧されます。

（注）　アプリケーション パーティション イメージを復旧する前にリカバリ パーティションを最新のバージョンにアップグレードしてある場合は、その最新のソフトウェア イメージをインストールできます。

recover application-partition コマンドは Telnet または SSH 接続によって実行できるので、リモートの場所に設置されているセンサーを復旧するにはこのコマンドを使用することを推奨します。

（注）　復旧後にセンサーに再接続するときは、デフォルトのユーザ名とパスワードの **cisco** でログインする必要があります。

詳細情報

リカバリ パーティションを最新バージョンにアップグレードする手順については、「リカバリ パーティションのアップグレード」（P.20-9）を参照してください。

IPS SSP アプリケーション パーティション イメージの復旧

アプリケーション パーティション イメージを復旧するには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg など）を、センサーからアクセスできる FTP、HTTP、または HTTPS サーバにダウンロードします。

ステップ 2　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 3　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

（注）　リカバリ パーティションをアップグレードするには、センサーがすでに IPS 7.1(1) を実行している必要があります。

ステップ 4　アプリケーション パーティション イメージを復旧します。

```
ips-ssp(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 7.1(1)E4. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

ステップ 5　**yes** を入力して続行します。

recover コマンドを実行すると、すぐにシャットダウンが開始されます。シャットダウンには少し時間がかかることがあり、この間にも CLI にアクセスできますが、アクセスは警告なしに終了されます。

アプリケーション パーティションのイメージは、リカバリ パーティションに保存されているイメージを使用して再作成されます。ここで、**setup** コマンドを使用してセンサーを初期化する必要があります。IP アドレス、ネットマスク、アクセス リスト、時間帯、およびオフセットが保存され、イメージが再作成されたアプリケーション パーティションに適用されます。**recover application-partition** コマンドをリモートで実行した場合は、デフォルトのユーザ名とパスワード（**cisco**/**cisco**）を使用してセンサーに SSH で接続して、**setup** コマンドによって再度センサーを初期化します。Telnet は、デフォルトでディセーブルになっているので、センサーを初期化するまで Telnet は使用できません。

詳細情報

- **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。
- リカバリ パーティションを最新バージョンにアップグレードする手順については、「リカバリ パーティションのアップグレード」（P.20-9）を参照してください。

APPENDIX A

システム アーキテクチャについて

（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。

この付録では、Cisco IPS のシステム アーキテクチャについて説明します。次のような構成になっています。

- 「Cisco IPS の目的」（P.A-1）
- 「システム設計」（P.A-2）
- 「システム アプリケーション」（P.A-3）
- 「ユーザ対話」（P.A-4）
- 「セキュリティ機能」（P.A-4）
- 「MainApp」（P.A-5）
- 「SensorApp」（P.A-22）
- 「CollaborationApp」（P.A-27）
- 「CLI」（P.A-29）
- 「通信」（P.A-31）
- 「Cisco IPS のファイル構造」（P.A-34）
- 「Cisco IPS アプリケーションの概要」（P.A-35）

Cisco IPS の目的

Cisco IPS の目的は、悪意のあるネットワーク アクティビティを検出して防止することにあります。Cisco IPS ソフトウェアは、アプライアンスとモジュールの 2 つのプラットフォームにインストールできます。Cisco IPS には、管理アプリケーションとモニタリング アプリケーションが含まれています。IDM は、IPS の管理およびモニタリングに使用できるネットワーク管理 JAVA アプリケーションです。

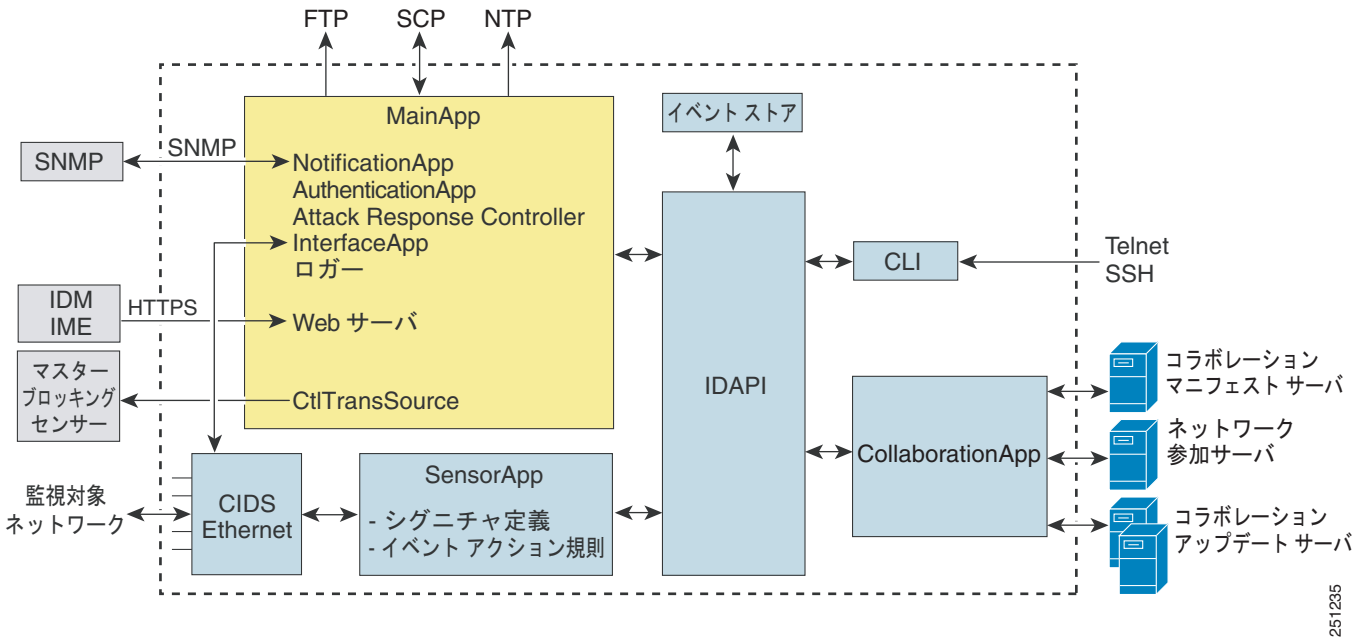
IME は、IPS イベントの表示に使用できる IPS ネットワーク モニタリング JAVA アプリケーションです。IME には、IDM 設定コンポーネントも含まれています。IDM および IME は、HTTP または HTTPS を使用して IPS と通信し、ユーザのコンピュータ上で実行されます。

システム設計

Cisco IPS ソフトウェアは、Linux オペレーティング システム上で動作します。Linux OS を強化するために、不要なパッケージの削除、使用しないサービスの無効化、ネットワーク アクセスの制限、およびシェルへのアクセスの停止を行いました。

図 A-1 に、IPS ソフトウェアのシステム設計を示します。

図 A-1　システム設計



詳細情報

- MainApp の詳細については、「MainApp」（P.A-5）を参照してください。
- SensorApp の詳細については、「SensorApp」（P.A-22）を参照してください。
- CollaborationApp の詳細については、「CollaborationApp」（P.A-27）を参照してください。
- CLI の詳細については、「CLI」（P.A-29）を参照してください。

システム アプリケーション

（注）　各アプリケーションには、それぞれ独自の XML 形式の構成ファイルがあります。

Cisco IPS ソフトウェアには、次のアプリケーションが含まれています。

- MainApp：システムの初期化、他のアプリケーションの起動および停止、OS の設定、およびアップグレードの実行を行います。これには、次のコンポーネントが含まれます。
  - ctlTransSource（Control Transaction Server）：センサーによる制御トランザクションの送信を可能にします。これは、Attack Response Controller（旧称 Network Access Controller）のマスター ブロッキング センサー機能をイネーブルにするために使用します。
  - イベント ストア：IPS イベント（エラー、ステータス、アラートの各システム メッセージ）を格納するために使用され、CLI、IDM、IME、ASDM、または SDEE からアクセスできるインデックス付きストア。
  - InterfaceApp：バイパスおよび物理設定を処理し、ペアになっているインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。
  - ロガー：アプリケーションのすべてのログ メッセージをログ ファイルに書き出し、アプリケーションのエラー メッセージをイベント ストアに書き出します。
  - Attack Response Controller（旧称 Network Access Controller）：リモート ネットワーク デバイス（ファイアウォール、ルータ、およびスイッチ）を管理し、アラート イベントの発生時にブロッキング機能を提供します。ARC は、制御対象のネットワーク デバイスで ACL を作成して適用するか、または **shun** コマンドを使用します（ファイアウォール）。
  - NotificationApp：アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp はパブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的なヘルスに関する情報を提供します。
  - Web サーバ（HTTP SDEE サーバ）：いくつかのサーブレットを使用して IPS サービスを提供することにより、SDEE プロトコルを介した Web インターフェイスおよび他の IPS デバイスとの通信を提供します。
  - AuthenticationApp：ユーザが CLI、IDM、IME、ASDM、または SDEE アクションを実行できることを確認します。
- SensorApp（分析エンジン）：パケットのキャプチャと分析を行います。
- CollaborationApp：IDAPI 制御トランザクション、セマフォ、共有メモリ、ファイル交換などのさまざまなプロセス間通信テクノロジーを使用して、MainApp および SensorApp とのインターフェイスをとります。
- CLI：Telnet または SSH を通じてセンサーに正しくログインすると実行されるインターフェイス。CLI で作成されたすべてのアカウントは、CLI をアカウントのシェルとして使用します（サービス アカウントは例外。許可されるサービス アカウントは 1 つだけです）。使用できる CLI コマンドは、ユーザの権限に依存します。

すべての Cisco IPS アプリケーションは、IDAPI と呼ばれる共通 API を通じて相互に通信します。リモート アプリケーション（他のセンサー、管理アプリケーション、およびサードパーティ ソフトウェア）は、SDEE プロトコルを通じてセンサーと通信します。

センサーには、次のパーティションがあります。

- アプリケーション パーティション：完全な IPS システム イメージ。
- メンテナンス パーティション：IDSM2 のアプリケーション パーティションのイメージを再作成するために使用される、特殊な目的の IPS イメージ。メンテナンス パーティションのイメージを再作成すると、すべての設定が失われます。
- リカバリ パーティション：センサーのリカバリに使用される、特殊な目的のイメージ。リカバリ パーティションで起動すると、アプリケーション パーティションを完全に再作成することができます。ネットワーク設定は保存されますが、それ以外のすべての設定は失われます。

ユーザ対話

ユーザは、次の方法で Cisco IPS と対話します。

- デバイスのパラメータ設定

  システムとその機能の初期設定を生成します。これは頻繁に実行する作業ではなく、通常は一度だけ実行します。システムには妥当なデフォルト値が設定され、ユーザができるだけ変更を加えずに済むようになっています。Cisco IPS は CLI、IDM、IME、CSM、ASDM を使用して設定できるほか、別のアプリケーションで SDEE を使用して設定できます。

- 調整

  主に分析エンジンに対して、わずかな設定変更を加えます。分析エンジンはアプリケーションでネットワーク トラフィックをモニタする部分です。ネットワークに最初にシステムをインストールした後、システムが効率的に動作し、有用と考えられる情報だけを生成するようになるまで何度も調整を加えることができます。カスタム シグニチャの作成、機能のイネーブル化、サービス パックまたはシグニチャ アップデートの適用が可能です。Cisco IPS は CLI、IDM、IME、CSM、ASDM を使用して調整できるほか、別のアプリケーションで SDEE を使用して調整できます。

- アップデート

  自動アップデートをスケジュールしたり、アプリケーションやシグニチャ データ ファイルに今すぐアップデートを適用したりすることができます。Cisco IPS は CLI、IDM、IME、CSM、ASDM を使用して調整できるほか、別のアプリケーションで SDEE を使用してアップデートできます。

- 情報の取得

  CLI、IDM、IME、CSM、ASDM、CS MARS を使用して、または、別のアプリケーションで SDEE を使用して、システムからデータ（ステータス メッセージ、エラー、およびアラート）を取得できます。

詳細情報

SDEE の詳細については、「SDEE」（P.A-33）を参照してください。

セキュリティ機能

Cisco IPS には次のセキュリティ機能があります。

- ネットワーク アクセスは、アクセスを許可された特定のホストに限定されます。
- Web サーバ、SSH と SCP または Telnet を使用して接続を試みるリモート ホストには、すべて認証が実行されます。

- デフォルトでは、Telnet アクセスはディセーブルになっています。Telnet をイネーブルにするように選択できます。
- デフォルトでは、SSH アクセスはイネーブルになっています。
- FTP サーバはセンサー上では実行されません。SCP を使用して、ファイルをリモートでコピーできます。
- デフォルトでは、Web サーバでは TLS または SSL が使用されます。TLS と SSL をディセーブルにするように選択できます。
- 不要なサービスはディセーブルになっています。
- CISCO-CIDS-MIB 内では、Cisco MIB Police で必要とされる SNMP セットのみが許可されます。パブリック ドメイン SNMP エージェントによって実装される OID は、MIB によって指定される場合は書き込み可能になります。

MainApp

ここでは MainApp について説明します。次のような構成になっています。

- 「MainApp について」（P.A-5）
- 「MainApp の役割」（P.A-6）
- 「イベント ストア」（P.A-6）
- 「NotificationApp」（P.A-9）
- 「CtlTransSource」（P.A-11）
- 「Attack Response Controller」（P.A-12）
- 「ロガー」（P.A-19）
- 「AuthenticationApp」（P.A-19）
- 「Web サーバ」（P.A-22）

MainApp について

MainApp には、SensorApp と CLI を除くすべての IPS コンポーネントが含まれています。起動時にオペレーティング システムによってロードされ、SensorApp をロードします。その後、MainApp は次のサブシステム コンポーネントを起動します。

- 認証
- ロガー
- ARC
- Web サーバ
- 通知（SNMP）
- 外部製品インターフェイス
- インターフェイス マネージャ
- イベント ストア
- ヘルスおよびセキュリティ モニタリング

MainApp の役割

MainApp には、次の役割があります。

- シスコがサポートするハードウェア プラットフォームの検証
- ソフトウェアのバージョンおよび PEP 情報の報告
- IPS コンポーネントの起動、停止、およびバージョンの報告
- ホスト システムの設定
- システム クロックの管理
- イベント ストアの管理
- ソフトウェア アップグレードのインストールおよびアンインストール

（注） Cisco IPS では、MainApp はシグニチャおよびシグニチャ エンジンのアップデートを Cisco.com から自動的にダウンロードできます。

- オペレーティング システムのシャットダウンおよびリブート

MainApp は、**show version** コマンドへの応答として次の情報を表示します。

- センサーのビルド バージョン
- MainApp のバージョン
- 実行中の各アプリケーションのバージョン
- インストールされている各アップグレードのバージョンおよびタイムスタンプ
- インストールされている各アップグレードの次のダウングレード バージョン
- プラットフォームのバージョン
- 他のパーティションにあるセンサーのビルドのバージョン

MainApp は、ホスト統計情報の収集や、ヘルスおよびセキュリティ モニタリングのステータスの報告も行います。

イベント ストア

ここではイベント ストアについて説明します。次のような構成になっています。

- 「イベント ストアについて」（P.A-6）
- 「イベントのデータ構造」（P.A-7）
- 「IPS イベント」（P.A-8）

イベント ストアについて

各 IPS イベントは、タイム スタンプと一意の単調な昇順 ID とともにイベント ストアに保存されます。このタイム スタンプは、固定サイズのインデックス付きイベント ストア内でイベントにインデックスを付ける際のプライマリ キーとして使用されます。循環式のイベント ストアが設定されたサイズに達すると、最も古い 1 つまたは複数のイベントが新しく保存されるイベントで上書きされます。イベント ストアにアラート イベントを書き込むアプリケーションは SensorApp だけです。ログ、ステータス、およびエラー イベントは、すべてのアプリケーションがイベント ストアに書き込みます。

固定サイズのインデックス付きイベント ストアでは、時刻、タイプ、プライオリティ、および限られた数のユーザ定義属性に基づいて、シンプルなイベントのクエリーを実行できます。各イベントに low、medium、または high のプライオリティが割り当てられている場合は、1 回のイベント クエリーで目的のイベント タイプ、侵入イベントのプライオリティ、および時間範囲のリストを指定できます。

表 A-1 に、いくつかの例を示します。

表 A-1　IPS イベントの例

IPS イベント タイプ	intrusion イベントのプライオリティ	開始タイムスタンプ値	停止タイムスタンプ値	意味
status	—	0	最大値	格納されているすべての status イベントを取得します。
error status	—	0	65743	時刻 65743 よりも前に格納されたすべての error および status イベントを取得します。
status	—	65743	最大値	時刻 65743 以降に格納された status イベントを取得します。
intrusion attack response	low	0	最大値	プライオリティ low で格納されているすべての侵入および攻撃応答イベントを取得します。
attack response error status intrusion	medium high	4123000000	4123987256	時刻が 4123000000 から 4123987256 の間に格納された、プライオリティが medium または high の攻撃応答、エラー、ステータス、および侵入イベントを取得します。

イベント ストアのサイズは、センサーが IPS イベント コンシューマに接続されていないときに IPS イベントをバッファリングするのに十分な大きさです。バッファリングが十分であるかどうかは、ユーザの要件と、使用するノードの能力に依存します。循環バッファ内の最も古いイベントは、最新のイベントによって置き換えられます。

イベントのデータ構造

さまざまな機能ユニットが、次の 7 種類のデータをやり取りします。

- intrusion イベント：SensorApp によって生成されます。intrusion イベントはセンサーが検出します。
- error イベント：ハードウェアまたはソフトウェアの不具合によって発生します。
- ステータス イベント：設定がアップデートされたなどの、アプリケーションのステータスの変更を報告します。
- control transaction log イベント：センサーが制御トランザクションの結果を記録します。
- 攻撃応答イベント：ブロック要求などの ARC 向けアクション。
- デバッグ イベント：アプリケーションのステータスの変更に関するきわめて詳細なレポートで、デバッグに使用されます。
- 制御トランザクション データ：制御トランザクションに関連するデータ。たとえば、アプリケーションの診断データ、セッション ログ、およびアプリケーションとやり取りされる設定データ。

これら 7 種類のデータを *IPS* データと総称します。6 つのイベント タイプ（侵入、エラー、ステータス、制御トランザクション ログ、ネットワーク アクセス、およびデバッグ）は特徴が似ており、*IPS イベント*と総称されます。IPS イベントは、IPS を構成する数種類のアプリケーションによって生成され、他の IPS アプリケーションによってサブスクライブされます。IPS イベントには、次のような特徴があります。

- IDS イベントを生成するように設定されているアプリケーション インスタンスによって、自然発生的に生成されます。特定のイベントを生成するように他のアプリケーション インスタンスから要求されることはありません。
- 特定の宛先はありません。1 つまたは複数のアプリケーションによって格納され、その後、取得されます。

制御トランザクションは、次のタイプの要求に関係します。

- アプリケーション インスタンスの設定データをアップデートする要求
- アプリケーション インスタンスの診断データの要求
- アプリケーション インスタンスの診断データをリセットする要求
- アプリケーション インスタンスを再起動する要求
- ブロック要求などの ARC 向け要求

制御トランザクションには、次のような特徴があります。

- 常に、1 つの応答を伴う 1 つの要求によって構成されます。

  要求と応答には、任意の量のデータが関連付けられる可能性があります。すべての応答には、少なくとも肯定応答または否定応答が含まれます。
- ポイントツーポイントのトランザクションです。

  制御トランザクションは 1 つのアプリケーション インスタンス（発信側）からもう 1 つのアプリケーション インスタンス（応答側）に送信されます。

IPS データは、XML 形式で XML ドキュメントとして表されます。システムでは、ユーザ設定可能なパラメータがいくつかの XML ファイルに格納されます。

IPS イベント

IPS アプリケーションは、ある種のできごとが発生したことを報告するために IPS イベントを生成します。イベントは、SensorApp が生成するアラートやアプリケーションが生成するエラーなどのデータです。イベントは、イベント ストアというローカル データベースに格納されます。

5 種類のイベントがあります。

- evAlert：ネットワーク アクティビティによってシグニチャがトリガーされたことを報告する alert イベント メッセージ
- evStatus：IPS アプリケーションのステータスとアクションを報告するステータス イベント メッセージ
- evError：応答アクションの試行中に発生したエラーを報告する error イベント メッセージ
- evLogTransaction：各センサー アプリケーションによって生成された制御トランザクションを報告する log transaction メッセージ
- evShunRqst：ARC がいつブロック要求を発行したかを報告するブロック要求メッセージ。

ステータス メッセージおよびエラー メッセージは、CLI、IME、および ASDM を使用して表示できます。

SensorApp および ARC は、応答アクション（TCP リセット、IP ロギングの開始と停止、ブロッキングの開始と停止、トリガー パケット）をステータス メッセージとしてログに記録します。

NotificationApp

NotificationApp は、センサーがアラートおよびシステム エラー メッセージを SNMP トラップとして送信できるようにします。イベント ストアのイベントをサブスクライブし、それらのイベントを SNMP MIB に変換して、パブリック ドメイン SNMP エージェントを使用して宛先に送信します。NotificationApp は、set および get の送信をサポートします。SNMP GET により、センサーの基本的なヘルス情報を提供できます。

スパース モードでは、NotificationApp は evAlert イベントから次の情報を送信します。

- 発信者情報
- イベント ID
- イベントの重大度
- 時刻（UTC および現地時間）
- シグニチャ名
- シグニチャ ID
- サブシグニチャ ID
- 参加者情報
- アラーム特性

詳細モードでは、NotificationApp は evAlert イベントから次の情報を送信します。

- 発信者情報
- イベント ID
- イベントの重大度
- 時刻（UTC および現地時間）
- シグニチャ名
- シグニチャ ID
- サブシグニチャ ID
- バージョン
- サマリー
- インターフェイス グループ
- VLAN
- 参加者情報
- アクション
- アラーム特性
- シグニチャ
- IP ログ ID

NotificationApp は、ユーザが定義したフィルタに従って、どの evError イベントをトラップとして送信するかを決定します。エラーの重大度（error、fatal、および warning）に基づいてフィルタリングできます。NotificationApp は、evError イベントから次の情報を送信します。

- 発信者情報
- イベント ID
- イベントの重大度

- 時刻（UTC および現地時間）
- エラー メッセージ

NotificationApp は、センサーからの次の全般的なヘルスおよびシステム情報の GET をサポートします。

- パケット損失
- パケット拒否
- 生成されたアラーム
- FRP 内のフラグメント
- FRP 内のデータグラム
- 初期状態の TCP ストリーム
- 確立状態の TCP ストリーム
- 終了状態の TCP ストリーム
- システム内の TCP ストリーム
- 再構成用のキューに入れられた TCP パケット
- アクティブなノードの合計
- 両方の IP アドレスと両方のポートでキー付けされた TCP ノード
- 両方の IP アドレスと両方のポートでキー付けされた UDP ノード
- 両方の IP アドレスでキー付けされた IP ノード
- センサーのメモリの重要なステージ
- インターフェイスのステータス
- コマンドおよび制御パケットの統計情報
- フェールオーバーの状態
- システムの稼働時間
- CPU 使用率
- システムのメモリ使用状況
- PEP

（注） すべての IPS プラットフォームが PEP をサポートしているわけではありません。

NotificationApp は次の統計情報を提供します。

- エラー トラップ数
- イベント アクション トラップ数
- SNMP GET 要求の数
- SNMP SET 要求の数

CtlTransSource

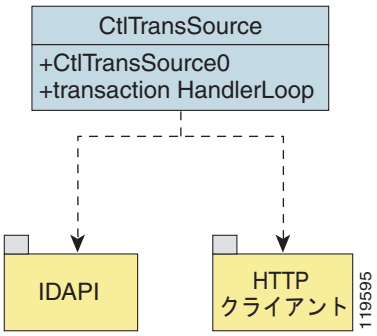
CtlTransSource は、ローカルで開始されたリモート制御トランザクションを HTTP プロトコルを使用してリモートの宛先に転送するアプリケーションです。CtlTransSource は、TLS または非 TLS 接続を開始し、その接続を使用してリモート制御トランザクションを HTTP サーバに伝えます。

CtlTransSource は、リモート HTTP サーバでリモート制御トランザクションを実行するために必要なクレデンシャルを確立する必要があります。リモート ノード上の HTTP サーバにユーザ名とパスワードの形式で ID を提示することによってクレデンシャルを確立します（基本認証）。認証が成功すると、要求者には、その接続の各要求で提示する必要のあるユーザ認証を格納したクッキーが割り当てられます。

CtlTransSource サーバ内の transactionHandlerLoop メソッドは、リモート制御トランザクションに対するプロキシとして機能します。ローカル アプリケーションがリモート制御トランザクションを起動すると、IDAPI は最初にトランザクションを CtlTransSource に送信します。transactionHandlerLoop メソッドは、CtlTransSource に送信されたリモート制御トランザクションを待機するループです。

図 A-2 に、CtlTransSource 内の transactionHandlerLoop メソッドを示します。

図 A-2　CtlTransSource



transactionHandlerLoop は、リモート アドレッシングされたトランザクションを受信すると、そのリモート制御トランザクションをリモートの宛先に転送するように試みます。transactionHandlerLoop は、トランザクションを制御トランザクション メッセージの形式にします。transactionHandlerLoop は、HttpClient クラスを使用して、リモート ノード上の HTTP サーバに対して制御トランザクション要求を発行します。リモート HTTP サーバは、リモート制御トランザクションを処理し、適切な応答メッセージを HTTP 応答として返します。リモート HTTP サーバが IPS Web サーバである場合、Web サーバは CtlTransSource サーブレットを使用してリモート制御トランザクションを処理します。

transactionHandlerLoop は、制御トランザクションの応答として、応答か障害応答のいずれかをリモート制御トランザクションの発信側に返します。HTTP サーバが許可されていないステータス応答（HTTP クライアントが HTTP サーバに対する十分なクレデンシャルを持っていないことを示す）を返す場合、transactionHandlerLoop は CtlTransSource 専用のユーザ名とパスワードを使用して要求者の ID を認証して、トランザクション要求を再発行します。transactionHandlerLoop は、終了を指示する制御トランザクションを受信するか終了イベントが発生するまでループします。

Attack Response Controller

ここでは ARC について説明します。次のような構成になっています。

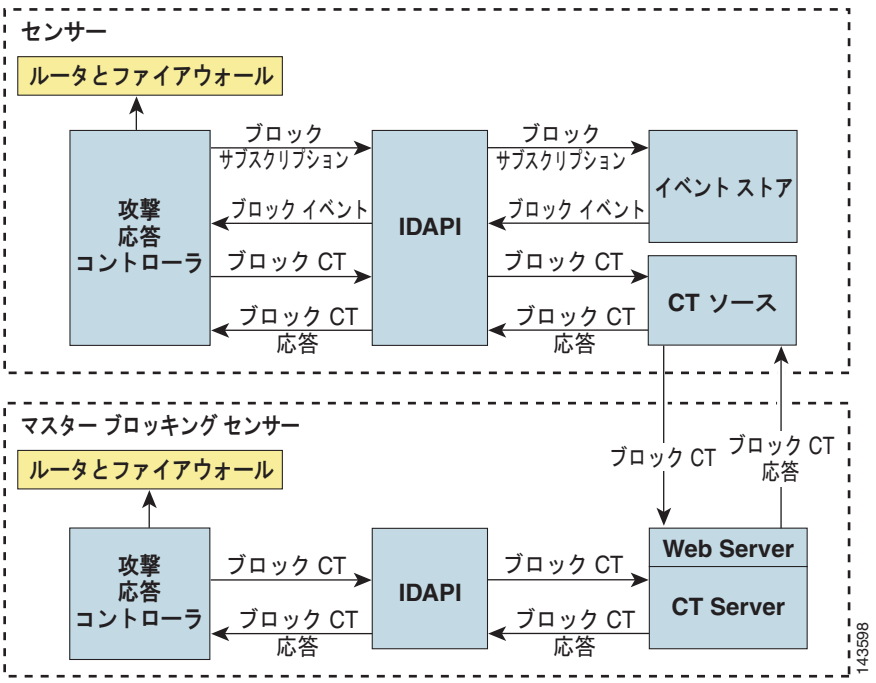
- 「ARC について」（P.A-12）
- 「ARC の機能」（P.A-13）
- 「サポートされているブロッキング デバイス」（P.A-15）
- 「ACL と VACL」（P.A-15）
- 「再起動時の状態の維持」（P.A-16）
- 「接続ベースおよび無条件のブロッキング」（P.A-17）
- 「シスコのファイアウォールによるブロッキング」（P.A-17）
- 「Catalyst スイッチによるブロッキング」（P.A-18）

ARC について

ARC の主な役割は、イベントをブロックすることです。NAC アプリケーションはブロックに対応するとき、管理対象のデバイスと直接対話してブロックを有効化するか、Control Transaction Server を通じてマスター ブロッキング センサーにブロック要求を送信します。マスター ブロッキング センサー上の Web サーバは、制御トランザクションを受け取るとそれを Control Transaction Server に渡し、Control Transaction Server は ARC に渡します。次に、マスター ブロッキング センサー上の ARC は、管理対象のデバイスと対話してブロックをイネーブルにします。

図 A-3 は ARC を図示したものです。

図 A-3　　ARC



（注） ARC のインスタンスは、ネットワーク デバイスを制御できない場合、1 つだけ制御できる場合、多数を制御できる場合があります。ARC は、他の ARC アプリケーション、IPS 管理ソフトウェア、他のネットワーク管理ソフトウェア、システム管理者との間でネットワーク デバイスの制御を一切共有しません。1 つのセンサー上で実行できる ARC インスタンスは 1 つだけです。

ARC は、次のいずれかに対応してブロックを開始します。

- ブロック アクションが設定されたシグニチャから生成された alert イベント
- CLI、IDM、IME、または ASDM から手動で設定されたブロック
- ホストまたはネットワーク アドレスに対して永続的に設定されたブロック

デバイスをブロックするように ARC を設定すると、ARC はそのデバイスと Telnet または SSH 接続を開始します。ARC は、デバイスごとに接続を維持します。ブロックが開始されると、ARC は制御対象の各デバイスに新しい設定または ACL のセットを（インターフェイス方向ごとに 1 つずつ）プッシュします。ブロックが完了すると、すべての設定または ACL はブロックを削除するようにアップデートされます。

ARC の機能

ARC には、次の機能があります。

- 3DES を使用した Telnet および SSH 1.5 による通信

  そのデバイスの ARC 設定で指定されたプロトコルのみが試行されます。何らかの理由で接続が失われると、ARC は再確立を試みます。

- ルータ上の既存 ACL およびスイッチ上の既存 VACL。

  ARC によって制御されるルータのインターフェイスまたは方向に既存の ACL がある場合は、その ACL を ARC によって生成された設定にマージするように指定できます。これは、preblock ACL を指定するとすべてのブロックの前に、postblock ACL を指定するとブロックの後に行われます。Catalyst 6000 VACL デバイス タイプには、ARC が制御するインターフェイスごとに preblock および postblock VACL を指定できます。ファイアウォール デバイス タイプでは、ブロックを実行するために別の API が使用され、ARC はファイアウォール上の既存の ACL には影響を与えません。

  （注） Catalyst 5000 RSM および Catalyst 6000 MSFC2 ネットワーク デバイスは、Cisco ルータとして同じようにサポートされます。

- リモート センサーのリストに対するブロックの転送

  ARC は、リモート センサーのリストにブロックを転送できます。そのため、複数のセンサーが実質的に共同で 1 つのネットワーク デバイスを制御することができます。このようなリモート センサーをマスター ブロッキング センサーと言います。

- ネットワーク デバイスのインターフェイスに対するブロッキングの指定

  ルータの ARC 設定で、ブロッキングが実行されるインターフェイスと方向を指定できます。VACL 設定では、ブロッキングが実行されるインターフェイスを指定できます。

  （注） シスコのファイアウォールでは、インターフェイスまたは方向に基づくブロックは行わないため、この設定が指定されることはありません。

ARC は、同時に 250 までのインターフェイスを制御できます。

- ホストまたはネットワークに対する指定された時間のブロッキング

  ARC は、分単位で指定された時間だけ、または永続的にホストまたはネットワークをブロックできます。ARC は、ブロックの期限がいつ切れたかを判断し、その時点でホストまたはネットワークのブロックを解除します。

- 重要なイベントのロギング

  ARC は、ブロックまたはブロック解除アクションが正常に完了するか何らかのエラーが発生すると、確認イベントを書き込みます。また、ARC は、ネットワーク デバイスの通信セッションの切断と回復、設定エラー、ネットワーク デバイスから報告されるエラーなどの重要なイベントも記録します。

- ARC 再起動時におけるブロッキング状態の維持

  シャットダウンまたは再起動が発生したとき、ARC は期限が切れていないブロックを再適用します。シャットダウン中に期限が切れたブロックは削除されます。

  （注） ARC がブロッキング状態を正しく維持するためには、アプリケーションのシャットダウン中にシステムの時刻が変更されないことが条件です。

- ネットワーク デバイス再起動時におけるブロッキング状態の維持

  ネットワーク デバイスがシャットダウンされ、再起動されると、ARC は必要に応じてブロックを再適用し、期限が切れたブロックを削除します。ARC は、ARC のシャットダウンおよび再起動が同時に、または重複して発生しても影響を受けません。

- 認証と認可

  ARC は、リモート TACACS+ サーバの使用を含め、AAA 認証および認可を使用するネットワーク デバイスとの間で通信セッションを確立できます。

- 2 種類のブロッキング

  ARC は、ホスト ブロックとネットワーク ブロックをサポートしています。ホスト ブロックは、接続ベースまたは無条件です。ネットワーク ブロックは、常に無条件です。

- NAT アドレス指定

  ARC は、センサーに対して NAT アドレスを使用するネットワーク デバイスを制御できます。ネットワーク デバイスを設定する際に NAT アドレスを指定すると、そのデバイスに対するブロックからセンサーのアドレスがフィルタ処理されるときに、ローカル IP アドレスの代わりにそのアドレスが使用されます。

- シングル ポイント制御

  ARC はネットワーク デバイスの制御を管理者や他のソフトウェアとの間で共有しません。設定をアップデートする必要がある場合は、変更が完了するまで ARC をシャットダウンしておきます。ARC は、CLI または任意の Cisco IPS マネージャからイネーブルまたはディセーブルにすることができます。ARC は、再イネーブルされると、自身を完全に初期化し直します。これには、制御対象のネットワーク デバイスごとに現在の設定を再読み込みすることも含まれます。

  （注） ファイアウォールを含むすべてのネットワーク デバイスを設定する際は、ARC によるブロッキングをディセーブルにすることを推奨します。

- 常に最大 250 のアクティブなブロックを維持

  ARC は、同時に 250 までのアクティブなブロックを維持できます。ARC は 65535 までのブロックをサポートしていますが、許可は 250 までにすることを推奨します。

（注）　ブロックの数は、インターフェイスおよび方向の数とは異なります。

サポートされているブロッキング デバイス

ARC は、次のデバイスを制御できます。

- Cisco IOS 11.2 以降を実行する Cisco ルータ

（注）　レート制限を実行するためには、ルータで Cisco IOS 12.3 以降を実行している必要があります。

- スーパーバイザ エンジン上で実行される Supervisor Engine ソフトウェア 5.3(1) 以降、および RSM 上で実行される IOS 11.2(9)P 以降を使用する Catalyst 5000 シリーズ スイッチ

（注）　ブロッキングは RSM 上で実行されるため、RSM が必要です。

- PFC がインストールされ、Catalyst ソフトウェア 5.3 以降が実行される Catalyst 6000 シリーズ スイッチ
- Catalyst ソフトウェア 5.4(3) 以降、および MSFC2 上の Cisco IOS 12.1(2)E 以降を使用する Catalyst 6000 MSFC2
- Cisco ASA 500 シリーズのモデル ASA 5510、ASA 5520、および ASA 5540
- FWSM

（注）　FWSM はマルチモードの管理コンテキストではブロックを実行できません。

ACL と VACL

ARC が制御するインターフェイスまたは方向のパケットをフィルタ処理する場合は、すべてのブロックの前に ACL を適用したり（preblock ACL）、すべてのブロックの後に ACL を適用する（postblock ACL）ように ARC を設定できます。これらの ACL は、ネットワーク デバイス上で非アクティブな ACL として設定されます。preblock および postblock ACL は、インターフェイスおよび方向ごとに定義できます。ARC は、ネットワーク デバイス上のアクティブな ACL をアップデートする際、リストを取得してキャッシュしてから、ブロッキングを行う ACE にマージします。ほとんどの場合は、ブロックの効果を妨げないように、既存 ACL を postblock ACL として指定します。ACL はパケットを、最初に検索された ACE と照合することにより機能します。この最初の ACE でパケットが許可された場合、その後の deny ステートメントは検索されません。

インターフェイスおよび方向ごとに異なる preblock および postblock ACL を指定することも、同じ ACL を複数のインターフェイスおよび方向に再利用することもできます。preblock リストを適用しない場合は、ホストやネットワークに対して never block オプションを使用したり、既存の設定ステートメントを使用して常にブロックしたりすることができます。forever block は、normal block でタイムアウト値を -1 にした場合と同じです。

ARC は、所有する ACL のみを変更します。ユーザによって定義された ACL は変更しません。ARC が維持する ACL は、ユーザ定義の ACL では使用が禁じられている特殊な形式になっています。命名規則は、**IPS_**<interface_name>**_[in | out]_[0 | 1]** です。<interface_name> は、ブロッキング インターフェイスに対して ARC 設定で指定された名前に対応します。

Catalyst スイッチでは、これは、ブロッキング インターフェイスの VLAN 番号です。これらの名前は、preblock および postblock ACL では使用しないでください。

Catalyst 6000 VACL では、preblock および postblock VACL を指定できます。また、インターフェイスのみが指定可能です（VLAN では方向は使用されません）。

ファイアウォールでは、ブロッキングに異なる API が使用されるため、preblock または postblock ACL は使用できません。代わりに、ファイアウォールでは ACL を直接作成する必要があります。

再起動時の状態の維持

センサーがシャットダウンされると、ARC はすべてのブロックとレート制限を（開始タイムスタンプとともに）ARC によって維持されるローカル ファイル（nac.shun.txt）に書き込みます。ARC が起動すると、このファイルを使用して、制御対象のネットワーク デバイスにブロックのアップデートが必要かどうかが判断されます。ファイル内に期限が切れていないブロックが見つかると、ネットワーク デバイスの起動時に適用されます。ARC がシャットダウンされるときは、未処理の有効なブロックが存在していても ACL に対して特別なアクションは行われません。nac.shun.txt ファイルが正確であるためには、ARC が実行されていない間にシステムの時刻が変更されないことが必要です。

注意　nac.shun.txt ファイルには手動による変更を加えないでください。

次のシナリオに、ARC が再起動時にどのように状態を維持するかを示します。

シナリオ 1

ARC が停止したときには 2 つのブロックが有効で、そのうちの 1 つは ARC が再起動する前に期限が切れます。再起動した ARC は、最初に nac.shun.txt ファイルを読み取ります。次に、preblock および postblock ACL または VACL を読み取ります。アクティブな ACL または VACL は、次の順序で構築されます。

1. **allow** *sensor_ ip_address* コマンド（**allow sensor shun** コマンドが設定されていない場合）
2. preblock ACL
3. 設定にある **always block** コマンドのエントリ
4. nac.shun.txt にある期限が切れていないブロック
5. postblock ACL

ARC 設定でホストが never block と指定されている場合、ACL の permit ステートメントには変換されません。代わりに、ARC にキャッシュされて、着信 addShunEvent イベントおよび addShunEntry 制御トランザクションをフィルタ処理するために使用されます。

シナリオ 2

preblock ACL および postblock ACL は指定されていませんが、アクティブな ACL が存在しています。新しい ACL は、次の順序で構築されます。

1. **allow** *sensor_ ip_address* コマンド（**allow sensor shun** コマンドが設定されていない場合）
2. 設定にある **always block** コマンドのエントリ
3. nac.shun.txt にある期限が切れていないブロック
4. **permit IP any any** コマンド

接続ベースおよび無条件のブロッキング

ARC は、ホストに関しては 2 種類、ネットワークに関しては 1 種類のブロッキングをサポートしています。ホスト ブロックは、接続ベースまたは無条件です。ネットワーク ブロックは、常に無条件です。

ホスト ブロックを受信すると、ARC はホスト ブロックの connectionShun 属性を調べます。connectionShun が true に設定されていると、ARC は接続ブロッキングを実行します。すべてのホスト ブロックは、宛先 IP アドレス、ソース ポート、宛先ポート、プロトコルといったオプションのパラメータを含むことができます。接続ブロックが実行されるためには、少なくとも送信元および宛先 IP アドレスが存在している必要があります。接続ブロックに送信元ポートが存在する場合、その送信元ポートは無視され、ブロックには含まれません。

次の条件のとき、ARC は必要に応じて接続タイプからブロックを変換して、ブロックを無条件にします。

- 指定されたソース IP アドレスに対して、いずれかのタイプのブロックがアクティブである。
- そのソース IP アドレスに対して、いずれかのタイプの新しいブロックが受信された。
- 新しいブロックのいずれかのオプション パラメータ（ソース ポートを除く）が以前のブロックと異なる。

ブロックがアップデートされると（既存のブロックがすでに有効になっている送信元 IP アドレスまたはネットワークに関して新しいブロックが受信された場合など）、既存のブロックの残り時間（分）が決定されます。新しいブロックの時間がこの残り時間以下の場合、アクションは何も発生しません。そうでない場合は、新しいブロックのタイムアウトによって既存のブロックのタイムアウトが置き換えられます。

注意　シスコのファイアウォールは、ホストの接続ブロッキングをサポートしません。接続ブロックが適用されると、ファイアウォールはそれを無条件ブロックのように扱います。シスコのファイアウォールは、ネットワーク ブロッキングもサポートしません。ARC がシスコのファイアウォールに対してネットワーク ブロックの適用を試みることはありません。

シスコのファイアウォールによるブロッキング

ARC は、**shun** コマンドを使用して、ファイアウォールでのブロックを実行します。**shun** コマンドの形式は次のとおりです。

- IP アドレスをブロックする。

  shun srcip [*destination_ip_address source_port destination_port* [*port*]]

- IP アドレスのブロックを解除する。

  no shun ip

- すべてのブロックをクリアする。

  clear shun

- アクティブなブロック、または実際にブロックされているグローバル アドレスを表示する。

  show shun [*ip_address*]

ARC は、**show shun** コマンドに対する応答を使用して、ブロックが実行されたかどうかを判断します。

shun コマンドは既存の ACL、コンジット、outbound コマンドを置き換えるものではないので、既存のファイアウォール設定をキャッシュしたり、ブロックをファイアウォール設定にマージしたりする必要はありません。

注意　ARC の実行中は、手動でブロックを実行したり既存のファイアウォール設定を変更したりしないでください。

block コマンドでソース IP アドレスのみを指定すると、既存のアクティブな TCP 接続は維持されますが、ブロックされたホストからの着信パケットはすべてドロップされます。

ARC が最初に起動したとき、ファイアウォール内のアクティブなブロックが内部のブロッキング リストと比較されます。内部のリストに対応するエントリがないブロックは削除されます。

ARC は、ローカル ユーザ名または TACACS+ サーバを使用して、ファイアウォールでの認証をサポートします。ファイアウォールで認証に AAA を使用して TACACS+ サーバは使用しないように設定すると、ARC は予約済みのユーザ名 *pix* を使用してファイアウォールと通信します。

ファイアウォールで認証に TACACS+ サーバを使用する場合は、TACACS+ ユーザ名を使用します。AAA ログインを使用する一部のファイアウォール設定では、3 つのパスワード プロンプトが表示されます。初期ファイアウォール パスワード、AAA パスワード、およびイネーブル パスワードです。ARC では、初期ファイアウォール パスワードと AAA パスワードを同じにすることが要求されます。

NAT または PAT を使用するようにファイアウォールを設定し、ファイアウォール外部のネットワークのパケットをセンサーが確認する場合、ファイアウォール内部のネットワークから開始されたホスト攻撃が検出されると、センサーはファイアウォールから提供された変換アドレスをブロックしようとします。ダイナミック NAT アドレッシングを使用している場合は、ブロックが効果を発揮しなかったり、無害なホストがブロックされることがあります。PAT アドレッシングを使用している場合は、ファイアウォールが内部ネットワーク全体をブロックする可能性があります。これらの状況を回避するには、センサーを内部インターフェイスに配置するか、センサーがブロックを行わないように設定します。

Catalyst スイッチによるブロッキング

PFC を搭載した Catalyst スイッチは、VACL を使用してパケットをフィルタ処理します。VACL は、VLAN 間および VLAN 内のすべてのパケットをフィルタ処理します。

WAN カードが取り付けられている場合は MSFC ルータ ACL がサポートされ、MSFC2 を通じてセンサーがインターフェイスを制御するようにすることができます。

（注）　MSFC2 カードは、Catalyst スイッチで VACL によるブロッキングを行うための設定の一部として必要なわけではありません。

注意　Catalyst スイッチで ARC を設定する場合は、制御対象のインターフェイスで方向を指定しないでください。インターフェイス名は VLAN 番号です。preblock および postblock のリストは、VACL である必要があります。

Catalyst の VACL には、次のコマンドを使用できます。

- 既存の VACL を表示する。

  show security acl info *acl_name*

- アドレスをブロックする（*address_spec* は、ルータの ACL で使用されるものと同じです）。

  set security acl ip *acl_name* **deny** *address_spec*

- リストの構築後に VACL をアクティブにする。

  commit security acl all

- 1 つの VACL をクリアする。
  clear security acl map *acl_name*
- すべての VACL をクリアする。
  clear security acl map all
- VACL を VLAN にマップする。
  set sec acl *acl_name vlans*

ロガー

センサーは、すべてのイベント（alert、error、status、debug の各メッセージ）を永続的な循環バッファに記録します。また、センサーは IP ログも生成します。このメッセージと IP ログには、CLI、IDM、ASDM、および SDEE クライアントからアクセスできます。

IPS アプリケーションは、ロガーを使用してメッセージをログに記録します。ロガーは、ログ メッセージを debug、timing、warning、error、fatal の 5 段階の重大度のいずれかで送信します。ロガーは、ログ メッセージを、循環式のテキスト ファイルである /usr/cids/idsRoot/log/main.log に書き込みます。ファイルがサイズの上限に達すると、古いメッセージは新しいメッセージによって上書きされます。したがって、main.log では、最後に書き込まれたメッセージが末尾にあるとは限りません。main.log に書き込まれた最新の行を見つけるには、「= END OF FILE =」を検索してください。

main.log は、**show tech-support** コマンドの出力に含まれます。メッセージが warning またはそれよりも上（error または fatal）のレベルで記録されると、ロガーはメッセージを evError イベントに変換して（対応するエラーの重大度で）、イベント ストアに挿入します。

ロガーは、informational 以上のレベルで cron メッセージ以外のすべての syslog メッセージ（*.info;cron.none）を受信し、エラーの重大度を Warning に設定してから evErrors としてイベント ストアに挿入します。ロガーおよびアプリケーションのロギングは、service logger コマンドによって制御されます。

ロガーは、ロギング ゾーンごとにロギング重大度を制御することにより、各アプリケーションが生成するログ メッセージを制御できます。ユーザは、TAC のエンジニアまたは開発者の依頼および指示の下で、ロガー サービスの individual-zone-control にのみアクセスします。トラブルシューティングのために、TAC はデバッグ ロギングを依頼することがあります。

AuthenticationApp

ここでは AuthenticationApp について説明します。次のような構成になっています。

- 「AuthenticationApp について」（P.A-19）
- 「ユーザの認証」（P.A-20）
- 「センサーにおける認証の設定」（P.A-20）
- 「TLS および SSH 信頼関係の管理」（P.A-20）

AuthenticationApp について

AuthenticationApp には、次の役割があります。

- ユーザの ID の認証
- ユーザのアカウント、権限、キー、および証明書の管理
- AuthenticationApp、およびセンサー上の他のアクセス サービスで使用する認証方法を設定する。

ユーザの認証

ユーザ アクセスに適切なセキュリティを確立するために、センサーで認証を設定する必要があります。センサーをインストールすると、初期アカウントとして、パスワードの期限が切れている cisco というアカウントが作成されます。センサーに対する管理アクセス権を持ったユーザは、デフォルトの管理アカウント（cisco）を使用してセンサーにログインすることにより、CLI または IDM や ASDM などの IPS マネージャを通じてセンサーにアクセスします。CLI で、管理者はパスワードの変更を要求されます。IPS マネージャは、setEnableAuthenticationTokenStatus 制御トランザクションを開始することによってアカウントのパスワードを変更します。

CLI または IPS マネージャを通じて、管理者は使用する認証方法（ユーザ名とパスワード、SSH 認証キーなど）を設定します。管理者用のアプリケーションは、認証設定を確立するために setAuthenticationConfig 制御トランザクションを起動します。

認証設定には、アカウント ロッキングの処理方法を指定するログイン試行の上限値が含まれています。アカウント ロッキングは、ログインの試みが連続して失敗した回数が、指定されたログイン試行の上限値を超えると起動されます。アカウントがロックされると、その後のログインの試行はすべて拒否されます。アカウントのロックを解除するには、setEnableAuthenticationTokenStatus 制御トランザクションを使用してアカウントの認証トークンをリセットします。アカウント ロッキング機能は、ログイン試行の上限値を 0 に設定すると無効になります。

管理者は、CLI または IPS マネージャから新しいユーザ アカウントを追加できます。

センサーにおける認証の設定

ユーザが Web サーバや CLI などのサービスを通じてセンサーにアクセスしようとするときは、ユーザの ID が認証され、ユーザの権限が確立される必要があります。ユーザにアクセスを提供するサービスは、ユーザの ID を認証するために、AuthenticationApp に対して execAuthenticateUser 制御トランザクション要求を開始します。通常、制御トランザクション要求にはユーザ名とパスワードが含まれています。または、SSH 認証キーを使用してユーザの ID を認証することもできます。

AuthenticationApp は、execAuthenticateUser 制御トランザクション要求に対して、ユーザの ID の認証を試みることによって応答します。AuthenticationApp は、ユーザの認証ステータスおよび権限を含む制御トランザクション応答を返します。ユーザの ID を認証できない場合、AuthenticationApp は、非認証ステータスと匿名ユーザ権限を制御トランザクション応答として返します。制御トランザクション応答では、アカウントのパスワードが期限切れであるかどうかも示されます。execAuthenticateUser 制御トランザクションを開始することによってユーザを認証するユーザ インターフェイス アプリケーションは、ユーザにパスワードの変更を要求します。

AuthenticationApp は、基盤となるオペレーティング システムを使用してユーザの ID を確認します。すべての IPS アプリケーションは、AuthenticationApp に制御トランザクションを送信します。AuthenticationApp は、オペレーティング システムを使用してその応答を作成します。

リモート シェル サービスである Telnet と SSH は、IPS アプリケーションではありません。これらは、オペレーティング システムを直接呼び出します。ユーザが認証されていれば、オペレーティング システムは IPS CLI を起動します。この場合、CLI は特殊な形式の execAuthenticateUser 制御トランザクションを送信することにより、ログイン ユーザの権限レベルを判断します。次に CLI は、この権限レベルに応じて、使用可能にするコマンドを用意します。

TLS および SSH 信頼関係の管理

IP ネットワーク上の暗号化通信は、パケット内のデータを復号化するために必要な秘密キーを、交換されるパケットだけから受動的攻撃者が発見できないようにすることで、データ プライバシーを実現します。

しかし、同じような危険性を持つ攻撃ベクトルとして、接続のサーバ側であるように装う詐称があります。すべての暗号化プロトコルには、クライアントがこの種の攻撃から身を守るための手段が用意されています。IPS は、SSH と TLS という 2 つの暗号化プロトコルをサポートしています。また、AuthenticationApp は、センサーが暗号化通信のクライアントまたはサーバになる場合の信頼を管理するのに役立ちます。

IPS Web サーバおよび SSH サーバは、暗号化通信のサーバ エンドポイントです。これらは、秘密キーによって ID を保護し、接続してくるクライアントに公開キーを提供します。TLS では、この公開キーは X.509 証明書の中に含まれています。X.509 証明書には他の情報も格納されています。センサーに接続するリモート システムは、接続確立時に受け取った公開キーが、目的のものであることを確認する必要があります。

クライアントは、中間者攻撃を防御するため、信頼できる公開キーのリストを維持する必要があります。この信頼性を確立するための詳細な手順は、プロトコルおよびクライアント ソフトウェアによって異なります。一般的に、クライアントは 16 ～ 20 バイトのフィンガープリントを表示します。クライアントが信頼を確立するように設定する人間のオペレータは、信頼の確立を試行する前に、アウトオブバンド方式を使用してサーバのキー フィンガープリントを取得する必要があります。フィンガープリントが一致すると信頼関係が確立され、その後、クライアントは自動的にそのサーバに接続でき、リモート サーバが詐称者でないことを確信できます。

show ssh server-key および **show tls fingerprint** を使用して、センサーのキー フィンガープリントを表示できます。センサー コンソールに直接接続したときにこれらのコマンドの出力を記録しておくと、後から信頼関係を確立する際、その情報を使用することにより、ネットワークを通じてセンサーの ID を確認できます。

たとえば、Microsoft Internet Explorer Web ブラウザを使用して最初にセンサーに接続したときには、セキュリティ警告ダイアログボックスで、証明書が信頼されていないことが示されます。Internet Explorer のユーザ インターフェイスを使用して証明書のサムプリントを調べることができます。この値は、**show tls fingerprint** コマンドによって表示される SHA1 フィンガープリントと正確に一致する必要があります。確認が終わったら、この証明書をブラウザの信頼済み CA のリストに追加して、永続的な信頼を確立します。

この信頼性を確立するための手順は、TLS クライアントごとに異なります。センサー自体に TLS クライアントが含まれており、制御トランザクションを他のセンサーに送信したり、アップグレードおよびコンフィギュレーション ファイルを TLS Web サーバからダウンロードするために使用されます。センサーの通信相手となる TLS サーバの信頼性を確立するには、**tls trusted-host** コマンドを使用します。

同様に、センサーには SSH クライアントが含まれており、管理対象ネットワーク デバイスとの通信、アップグレードのダウンロード、リモート ホストへのコンフィギュレーション ファイルおよびサポート ファイルのコピーに使用されます。センサーが接続する SSH サーバとの信頼関係を確立するには、**ssh host-key** コマンドを使用します。

TLS 信頼済み証明書および SSH 既知ホストのリストは、**service trusted-certificates** コマンドおよび **service ssh-known-hosts** コマンドで管理できます。

X.509 証明書には、信頼関係のセキュリティを向上させる追加情報が含まれていますが、これは混乱を招く場合があります。たとえば、X.509 証明書には、その証明書を信頼できる有効期間が含まれています。通常、この期間は証明書が作成された時点から始まる年数です。使用時点で X.509 証明書が有効であることを厳密に確認するには、クライアント システムで正確なクロックを維持する必要があります。

また、X.509 証明書は、特定のネットワーク アドレスと結び付けられています。センサーはこのフィールドに、センサーのコマンドおよびコントロール インターフェイスの IP アドレスを挿入します。そのため、センサーのコマンドおよびコントロール IP アドレスを変更すると、サーバの X.509 証明書は再生成されます。新しい IP アドレスでこのセンサーを見つけ、新しい証明書を信頼するには、以前の証明書を信頼していた、ネットワーク上のすべてのクライアントを再設定しなければなりません。

AuthenticationApp の SSH 既知ホストおよび TLS 信頼済み証明書サービスを使用することにより、センサーを高いセキュリティ レベルで運用することができます。

Web サーバ

Web サーバは SDEE サポートを提供します。これによってセンサーは、セキュリティ イベントの報告、IDIOM トランザクションの受信、および IP ログの提供が可能になります。

Web サーバは HTTP 1.0 および 1.1 をサポートします。Web サーバとの通信には、パスワードなどの機密情報が関係することがよくあります。これらを攻撃者が盗聴することが可能になると、システムの安全性が大きく損なわれます。そのため、センサーは TLS がイネーブルな状態で出荷されます。TLS プロトコルは、SSL と互換性のある暗号化プロトコルです。

（注）　RDEP イベント サーバ サービスは、IPS 6.1 では非推奨であり、現在の IPS システム アーキテクチャから削除されました。Web サーバでは、現在は SDEE イベント サーバが使用されます。

SensorApp

ここでは SensorApp について説明します。次のような構成になっています。

- 「SensorApp について」（P.A-22）
- 「インライン、正規化、およびイベント リスク レーティング機能」（P.A-24）
- 「SensorApp の新機能」（P.A-25）
- 「パケット フロー」（P.A-25）
- 「シグニチャ イベント アクション プロセッサ」（P.A-26）

SensorApp について

SensorApp は、パケットの取り込みと分析を実行します。SensorApp では、シグニチャを使用してポリシー違反が検出され、違反に関する情報がアラートの形式でイベント ストアに転送されます。

パケットは、センサー上のネットワーク インターフェイスからパケットを収集するように設計されたプロデューサが提供する、プロセッサのパイプラインを通過します。

SensorApp では、次のプロセッサがサポートされています。

- タイム プロセッサ

  このプロセッサは、タイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、失効したデータベース エントリを期限切れにし、時間に依存する統計を計算することです。

- 拒否フィルタ プロセッサ

  このプロセッサは、攻撃者拒否機能を処理します。拒否された送信元 IP アドレスのリストを管理します。リスト内の各エントリは、グローバルな拒否タイマーに基づいて有効期限切れになります。拒否タイマーは、仮想センサー設定内で設定できます。

- シグニチャ イベント アクション プロセッサ

  このプロセッサは、イベント アクションを処理します。次のイベント アクションがサポートされます。

  - TCP フローのリセット
  - IP ログ
  - パケットの拒否

- フローの拒否
- 攻撃者の拒否
- アラート
- ホストのブロック
- 接続のブロック
- SNMP トラップの生成
- トリガー パケットのキャプチャ

イベント アクションは、イベント リスク レーティングしきい値と関連付けできます。アクションが実行されるには、このしきい値を超える必要があります。

- 統計情報プロセッサ

  このプロセッサは、パケット カウントやパケットの到着レートなど、システム統計情報を継続して追跡します。

- レイヤ 2 プロセッサ

  このプロセッサは、レイヤ 2 関連イベントを処理します。また、不正な形式のパケットを識別し、処理パスから削除します。アラート、パケットのキャプチャ、パケットの拒否など、不正な形式のパケットの検出に対して実行可能なイベントを設定することができます。レイヤ 2 プロセッサは、ユーザが設定したポリシーのために拒否されたパケットに関する統計情報をアップデートします。

- データベース プロセッサ

  このプロセッサは、シグニチャの状態とフロー データベースを管理します。

- フラグメント再構成プロセッサ

  このプロセッサは、フラグメント化された IP データグラムを再構成します。センサーがインライン モードの場合、IP フラグメントの正規化も処理します。

- ストリーム再構成プロセッサ

  このプロセッサは、さまざまなストリームベース インスペクタでパケットが適切な順序で到着するよう、TCP ストリームを並べ替えます。また、TCP ストリームの正規化も行います。ノーマライザ エンジンを使用すると、アラートおよび拒否アクションをイネーブルまたはディセーブルにできます。

  TCP ストリーム再構成プロセッサのノーマライザはホールドダウン タイマーを備え、これによって再構成イベントの後でストリームの状態を再構築することができます。このタイマーは設定できません。ホールドダウン間隔の間、システムは、ストリームの状態を、システムを通過するストリーム内の最初のパケットと同期化します。ホールドダウンの有効期限が切れると、SensorApp は設定されたポリシーを実施します。このポリシーで、スリーウェイ ハンドシェイクを使用して開かれていないストリームの拒否が要求される場合、ホールドダウン期間中に休止していた確立済みストリームは転送されず、タイムアウトが許可されます。ホールドダウン期間中に同期化されたストリームは、続行を許可されます。

- シグニチャ分析プロセッサ

  このプロセッサは、ストリームベースでなく、処理中のパケット用に設定されているインスペクタにパケットをディスパッチします。

- スレーブ ディスパッチ プロセッサ

  デュアル CPU システムにのみ存在するプロセスです。

一部のプロセッサは、シグニチャ分析を実行するためにインスペクタを呼び出します。すべてのインスペクタは、アラーム チャネルを呼び出して、必要に応じてアラートを生成することができます。

SensorApp は次のユニットもサポートします。

- 分析エンジン

  分析エンジンは、センサーの設定を処理します。インターフェイスをマッピングし、またシグニチャおよびアラーム チャネル ポリシーを設定済みインターフェイスにマッピングします。

- アラーム チャネル

  アラーム チャネルは、インスペクタによって生成されたすべてのシグニチャ イベントを処理します。主な機能は、渡された各イベントのアラートを生成することです。

インライン、正規化、およびイベント リスク レーティング機能

（注）　Cisco ASA 5585-X（IPS SSP 搭載）は正規化をサポートしません。

SensorApp には、次のインライン、正規化、およびイベント リスク レーティング機能が含まれています。

- パケットのインライン処理

  センサーがデータ パスのパケットを処理するときには、ポリシー設定で明示的に拒否されていない限り、すべてのパケットは変更されずに転送されます。TCP の正規化により、一部のパケットが適切なカバレッジを確保するために遅延することがあります。ポリシー違反が発生すると、SensorApp はアクションの設定を許可します。パケットの拒否、フローの拒否、攻撃者の拒否など、追加のアクションがインライン モードで使用できるようになります。

  IPS にとって不明であるか、対象でないすべてのパケットは、分析されずにペアのインターフェイスに転送されます。すべてのブリッジングおよびルーティング プロトコルは、ポリシー違反が原因で発生する可能性のある拒否の場合のみ、転送されます。インライン（または無差別）のデータ処理に使用されるインターフェイスには、IP スタックは関連付けられません。無差別モードにおける 802.1q パケットの現在のサポートが、インライン モードにまで拡張されます。

- IP の正規化

  意図的または意図しない IP データグラムのフラグメンテーションによって、不正利用が隠され、それらの検出が困難または不可能になることがあります。フラグメンテーションは、ファイア ウォールやルータにあるようなアクセス コントロール ポリシーを回避するために使用される場合もあります。また、さまざまなオペレーティング システムがさまざまな方法を使用して、フラグメント化されたデータグラムをキューに入れたりディスパッチしたりします。エンド ホストがデータグラムを再構成する際に使用可能なすべての方法をセンサーで確認する必要がある場合、センサーはサービス拒否攻撃に対して脆弱になります。フラグメント化したすべてのデータグラムをインラインで再構成して、完成したデータグラムのみを転送し、必要に応じてデータグラムを再度フラグメント化することが、この問題の解決策です。IP フラグメンテーションの正規化の装置は、この機能を実行します。

- TCP の正規化

  意図的または意図しない TCP セッション セグメンテーションによって、いくつかの攻撃クラスが隠されることがあります。ポリシーが偽陽性や偽陰性なしに実施されるようにするには、2 つの TCP エンドポイントの状態が追跡され、実際のホスト エンドポイントによって処理されたデータだけが渡される必要があります。TCP ストリームで重複が発生する可能性がありますが、TCP セグメントの再転送以外は、非常にまれです。TCP セッションでの上書きは発生してはならないものです。上書きが発生する場合は、誰かがセキュリティ ポリシーを意図的に回避しようとしているか、TCP スタックの実装が壊れています。センサーが TCP プロキシとして動作していない限り、両方のエンドポイントの状態について完全な情報を保持することはできません。センサーが TCP プロキシとして動作する代わりに、セグメントが適切に並べられ、ノーマライザによって回避や攻撃に関係する異常なパケットが検索されます。

- イベント リスク レーティング

  イベント リスク レーティングには、潜在的に悪意のあるアクションの検出だけでなく、次の追加情報が組み込まれています。

  - 攻撃が成功した場合の攻撃の重大度
  - シグニチャの忠実度
  - ターゲット ホストに関する潜在的な攻撃の関連性
  - ターゲット ホストの全体的な価値

  イベント リスク レーティングはシステムからの偽陽性の減少に役立ち、アラート発生原因のより適切な制御を可能にします。

SensorApp の新機能

SensorApp には、次の新機能が含まれます。

- ポリシー テーブル：リスク カテゴリの設定（high、medium、および low）のリストを提供します。
- 回避保護：ノーマライザのインライン インターフェイス モード センサーをストリクト モードから非対称モードに切り換えます。
- センサー ヘルス メーター：センサー全体のヘルスの統計情報を提供します。
- トップ サービス：TCP、UDP、ICMP、および IP プロトコルの上位 10 個のインスタンスを提供します。
- セキュリティ メーター：脅威のカテゴリに入るアラートのプロファイルを設定し、この情報を赤、黄、および緑のバケットで報告します。これらのバケットの移行ポイントを設定できます。
- フロー状態のクリア：データベースをクリアできます。データベースをクリアすると、センサーが再起動時と同様に初期状態で起動します。
- 再起動ステータス：センサーの現在の起動段階および再起動段階を定期的に報告します。

パケット フロー

パケットは、NIC によって受信され、IPS 共有ドライバにより、ユーザによってマッピングされたカーネル内のメモリ スペースに配置されます。パケットの前には、IPS ヘッダーが付加されます。また、各パケットには、パケットがシグニチャ イベント アクション プロセッサに到達したときにそのパケットを通過させるか拒否するかを示すフィールドも含まれます。

プロデューサは、ユーザによってマッピングされた共有カーネルのパケット バッファからパケットを取り出し、センサーのモデルに適したプロセッサを実装する処理機能を呼び出します。順序は、次のようになります。

- シングル プロセッサの実行

  タイム プロセッサ --> レイヤ 2 プロセッサ --> 拒否フィルタ プロセッサ --> フラグメント再構成プロセッサ --> 統計情報プロセッサ --> データベース プロセッサ --> シグニチャ分析プロセッサ --> ストリーム再構成プロセッサ --> シグニチャ イベント アクション プロセッサ

- デュアル プロセッサの実行

  実行スレッド 1 タイム プロセッサ --> レイヤ 2 プロセッサ --> 拒否フィルタ プロセッサ --> フラグメント再構成プロセッサ --> 統計情報プロセッサ --> データベース プロセッサ --> シグニチャ分析プロセッサ --> スレーブ ディスパッチ プロセッサ --> | 実行スレッド 2 データベース プロセッサ --> ストリーム再構成プロセッサ --> シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサは、アラーム チャネル内のシグニチャ イベントから、シグニチャ イベント アクション オーバーライド、シグニチャ イベント アクション フィルタの処理を経由してシグニチャ イベント アクション ハンドラで処理されるまでのデータ フローを調整します。シグニチャ イベント アクション プロセッサは、次のコンポーネントから構成されます。

- アラーム チャネル

  SensorApp 検査パスからシグニチャ イベント処理にシグニチャ イベントを伝達するための領域となるユニット。

- シグニチャ イベント アクション オーバーライド

  リスク レーティング値に基づいて、アクションを追加します。シグニチャ イベント アクション オーバーライドは、設定済みのリスク レーティングしきい値の範囲内にあるすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立しており、各アクション タイプには別個の値が設定されています。

- シグニチャ イベント アクション フィルタ

  シグニチャ イベントのシグニチャ ID、アドレス、およびリスク レーティングに基づいてアクションを削除します。シグニチャ イベント アクション フィルタへ入力するのは、シグニチャ イベント アクション オーバーライドによって追加される可能性のあるアクションを持つシグニチャ イベントです。

  （注） シグニチャ イベント アクション フィルタが実行できるのはアクションの削除だけであり、新しいアクションの追加はできません。

  シグニチャ イベント アクション フィルタには、次のパラメータが適用されます。

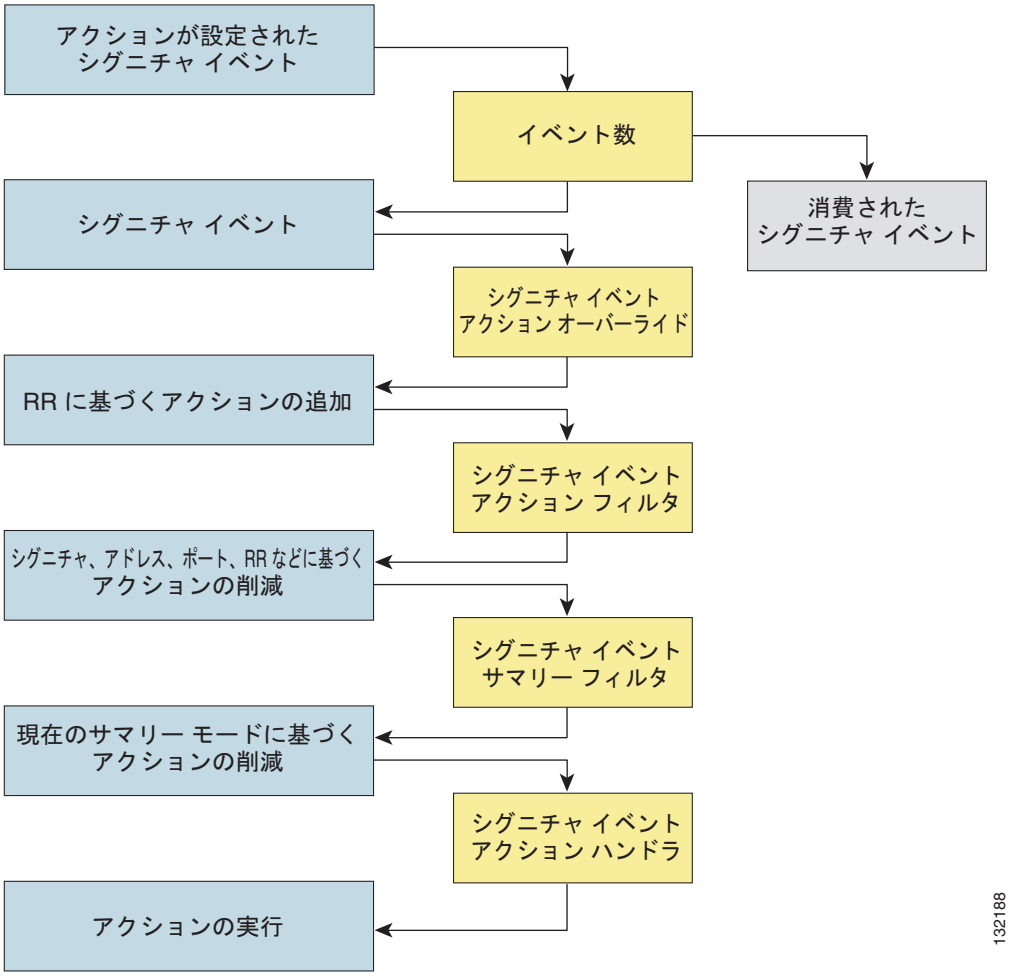
  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート
  - 攻撃対象のアドレス
  - 攻撃対象のポート
  - リスク レーティングしきい値の範囲
  - 削除するアクション
  - シーケンス識別子（任意）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット
  - 攻撃対象の OS の関連性または OS の関連性

- シグニチャ イベント アクション ハンドラ

  要求されたアクションを実行します。シグニチャ イベント アクション ハンドラから出力されるのは、実行中のアクションだけでなく、イベント ストアに書き込まれる evIdsAlert である可能性があります。

図 A-4（P.A-27）に、シグニチャ イベント アクション プロセッサを通過するシグニチャ イベントの論理的なフローと、このイベントのアクションで実行される操作を示します。これは、アラーム チャネルで受信された、アクションが設定されているシグニチャ イベントで開始され、シグニチャ イベントがシグニチャ イベント アクション プロセッサの機能コンポーネントを通過するときに上から下へ流れます。

図 A-4　シグニチャ イベント アクション プロセッサを通過するシグニチャ イベント



CollaborationApp

ここでは、CollaborationApp について説明します。次のような構成になっています。

- 「CollaborationApp について」（P.A-28）
- 「アップデート コンポーネント」（P.A-28）
- 「error イベント」（P.A-29）

CollaborationApp について

CollaborationApp は、MainApp および SensorApp のピアです。IDAPI 制御トランザクション、セマフォ、共有メモリ、ファイル交換などのさまざまなプロセス間通信テクノロジーを使用して、それらとのインターフェイスをとります。

グローバル相関サーバと CollaborationApp の間で、レピュテーション アップデートが交換されます。CollaborationApp は、4 つのアップデート コンポーネントを使用してセンサーと通信します。

- スコアの重みに関する一連の規則
- 一連の IP アドレスおよびアドレス範囲（規則およびアラートとともに、レピュテーション スコアの計算に必要な情報を提供します）
- トラフィックを常に拒否する必要のある、IP アドレスおよびアドレス範囲のリスト
- ネットワーク参加の設定（これにより、サーバは、センサーがテレメトリ データをサーバに送信するレートを制御できるようになります）

センサーは、コラボレーション情報をネットワーク参加サーバに送信します。センサーはグローバル相関サーバに対し、使用可能なコラボレーションの更新、およびグローバル相関サーバによる更新ファイルのダウンロード元のリストを照会します。

（注）　SensorApp は CollaborationApp よりも先に開始しますが、これらは非同期で初期化されます。したがって、レピュテーション更新サーバは、SensorApp でアップデートを受け入れる準備ができる前に、1 つ以上のグローバル相関の更新をダウンロードして適用を試みる可能性があります。更新サーバはアップデートをダウンロードして部分的に処理することもありますが、アップデートをコミットできるようになるには、SensorApp の準備完了まで待つ必要があります。

詳細情報

グローバル相関の詳細および設定方法については、第 10 章「グローバル相関の設定」を参照してください。

アップデート コンポーネント

グローバル相関アップデート クライアントは、グローバル相関更新サーバとマニフェストを交換します。サーバ マニフェストを解析して、ダウンロード可能な新しいアップデートとそれらが存在する場所を判別した後、インストールされるアップデートのリストを作成します。すべてのアップデートが正常に適用されると、グローバル相関アップデート クライアントは、適用された各コンポーネントのアップデートをコミットし、新しいアップデートが使用可能になったことを SensorApp に通知し、クライアント マニフェストをアップデートして、コミットされた各コンポーネントの最新のアップデートを反映します。

クライアント マニフェストには、センサーの UDI が含まれています。これには、センサーのシリアル番号と、センサーが真正な Cisco IPS センサーであることを確認するためにサーバが使用する暗号化された共有秘密が含まれます。サーバ マニフェストには、各コンポーネントが使用できるアップデート ファイルのリストが含まれています。リスト内の各アップデート ファイルについて、サーバ マニフェストにはアップデートのバージョン、タイプ、順序、場所、ファイル転送プロトコルなどのデータが含まれています。

アップデート ファイルには 2 種類あります。コンポーネントのデータベースにある既存のデータをすべて置き換える完全なアップデート ファイルと、情報の追加、削除、または置換によって既存のレピュテーション データを変更する差分アップデートです。すべてのコンポーネントにすべてのアップデート ファイルが適用されると、作業データベースを置き換えることによって一時データベースがコミットされます。

認証と許可は、秘密暗号化メカニズムと復号キー管理によって実現されます。グローバル相関更新サーバは、クライアント マニフェストに含まれている共有秘密暗号化メカニズムを使用して、センサーを認証します。グローバル相関アップデート クライアントは、復号キー管理を使用してセンサーを許可します。グローバル相関更新サーバによって認証されたセンサーには、アップデート ファイルを復号化できるように、サーバ マニフェスト内の有効なキーが送信されます。

注意　グローバル相関をイネーブルにしているけれども DNS または HTTP プロキシ サーバを設定していない場合は、警告メッセージを受け取ります。この警告は、グローバル相関をディセーブルにするか、DNS または HTTP プロキシ サーバを追加するように通知するものです。

詳細情報

DNS またはプロキシ サーバを追加してグローバル相関をサポートする手順については、「ネットワーク設定値の変更」（P.4-1）を参照してください。

error イベント

グローバル相関のアップデートが失敗した場合は、evError イベントが生成されます。エラー メッセージはセンサー統計情報に含まれています。次の条件が発生すると、重大度が Error のステータス メッセージになります。

- センサーがライセンスされていない
- DNS または HTTP プロキシ サーバが設定されていない
- マニフェストの交換が失敗した
- アップデート ファイルのダウンロードが失敗した
- アップデートの適用またはコミットが失敗した

グローバル相関がイネーブルになるようにホストまたはグローバル相関設定を編集して保存したけれども、DNS または HTTP プロキシ サーバが設定されていない場合、重大度レベルが Warning の evError イベントが生成されます。

詳細情報

センサー統計情報を表示する手順については、「統計情報の表示」（P.17-20）を参照してください。

CLI

ここでは、IPS CLI について説明します。次のような構成になっています。

- 「CLI について」（P.A-30）
- 「ユーザ ロール」（P.A-30）
- 「サービス アカウント」（P.A-31）

CLI について

CLI は、Telnet、SSH、シリアル インターフェイスなどのすべての直接ノード アクセスについて、センサーのユーザ インターフェイスを提供します。センサー アプリケーションは CLI で設定します。基盤となる OS への直接接続は、サービス ロールを通じて許可されます。

ユーザ ロール

ユーザ ロールには次の 4 つがあります。

- ビューア（Viewer）：設定およびイベントを表示できますが、自分のユーザ パスワード以外の設定データは修正できません。
- オペレータ（Operator）：すべてのデータを表示できるほか、次のオプションを修正できます。
  - シグニチャ チューニング（優先順位、無効/有効）
  - 仮想センサーの定義
  - 管理対象ルータ
  - 自分のユーザ パスワード
- 管理者（Administrator）：すべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、次のオプションを修正できます。
  - センサーのアドレス設定
  - 設定エージェントまたはビュー エージェントとして接続が許可されたホストのリスト
  - 物理的なセンシング インターフェイスの割り当て
  - 物理インターフェイスの制御のイネーブル化またはディセーブル化
  - ユーザとパスワードの追加および削除
  - 新しい SSH ホスト キーおよびサーバ証明書の生成
- サービス（Service）：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。サービス ユーザは、IDM または IME にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。

  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。許可されるサービス アカウントは 1 つだけです。サービス ロールを持つアカウントは、トラブルシューティングの目的でのみ作成してください。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、慎重に検討してください。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。

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.
*********************************************************************************
```

サービス アカウント

サービス アカウントは、サポートとトラブルシューティングのツールです。これによって TAC は、CLI シェルではなくネイティブ オペレーティング システムのシェルにログインすることができます。これは、デフォルトではセンサーには存在しません。TAC がセンサーのトラブルシューティングのために使用できるように、ユーザがこれを作成する必要があります。

1 つのセンサーで使用できるサービス アカウントは 1 つだけです。また、1 つのサービス ロールで使用できるアカウントも 1 つだけです。サービス アカウントのパスワードが設定またはリセットされると、root アカウントのパスワードが同じパスワードに設定されます。そのため、サービス アカウントのユーザはこの同じパスワードを使用して、root に su できます。サービス アカウントが削除されると、root アカウントのパスワードはロックされます。

サービス アカウントは、設定の目的で使用されることを想定していません。TAC の指示に基づき、サービス アカウントからセンサーに対して加えられた変更だけがサポートされます。サービス アカウントからオペレーティング システムに追加のサービスを加えること、およびそれを実行することは、他の IPS サービスの適切な実行に影響するため、シスコはこれをサポートしません。TAC は、追加のサービスが加えられたセンサーをサポートしません。

サービス アカウントへのログインは、ログ ファイル /var/log/.tac を確認することによって追跡できます。このファイルは、サービス アカウントによるログインの記録でアップデートされます。

（注）　Cisco IPS には、CLI、IDM、または IME から使用可能ないくつかのトラブルシューティング機能が組み込まれています。ほとんどのトラブルシューティングの状況で、サービス アカウントは不要です。TAC の指示の下にサービス アカウントを作成してトラブルシューティングを実行しなければならない、きわめてまれな問題もあります。サービス アカウントを使用すると、CLI に組み込まれた保護をバイパスし、root 権限でセンサーにアクセスすることができます。これは他の場合はディセーブルになっています。特別な理由で必要となる場合を除いては、サービス アカウントを作成しないことを推奨します。サービス アカウントは、不要になったら削除する必要があります。

通信

ここでは、Cisco IPS で使用される通信プロトコルについて説明します。次のような構成になっています。

- 「IDIOM」（P.A-32）
- 「IDCONF」（P.A-32）
- 「SDEE」（P.A-33）
- 「CIDEE」（P.A-33）
- 「IDAPI」（P.A-34）

IDIOM

IDIOM は、IPS によって報告されるイベント メッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の標準です。これらのメッセージは、IDIOM XML スキーマに準拠した XML ドキュメントで構成されています。

IDIOM は、イベントと制御トランザクションという 2 種類のインタラクションをサポートしています。イベント インタラクションは、アラートなどの IPS イベントを交換するために使用されます。IDIOM は、イベント インタラクションにイベント メッセージとエラー メッセージという 2 種類のメッセージを使用します。制御トランザクションは、ホストが別のホストでアクションを開始したり、別のホストの状態を変更または読み取るための手段です。制御トランザクションでは、要求、応答、設定、エラーの 4 種類の IDIOM メッセージが使用されます。1 つのホスト内のアプリケーション インスタンス間で通信されるイベントおよび制御トランザクションは、ローカル イベントまたはローカル制御トランザクションと呼ばれ、ローカル IDIOM メッセージと総称されます。異なるホスト間で通信されるイベントおよび制御トランザクションは、リモート イベントおよびリモート制御トランザクションと呼ばれ、リモート IDIOM メッセージと総称されます。

（注）　IDIOM の大部分は、IDCONF、SDEE、および CIDEE によって置き換えられています。

IDCONF

Cisco IPS は、XML ドキュメントを使用して自身の設定を管理します。IDCONF は、Cisco IPS 制御トランザクションを含めた XML スキーマを指定します。IDCONF スキーマは、設定ドキュメントの内容を指定するのではなく、設定ドキュメント作成の基になるフレームワークと構成単位を指定します。これは、特定の機能でサポートされる属性を使用することにより、それを設定することができないプラットフォームや機能の場合は IPS マネージャおよび CLI がその機能を無視できるメカニズムを提供します。

IDCONF メッセージは IDIOM の要求および応答メッセージ内にラップされます。

次に、IDCONF の例を示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<request xmlns="http://www.cisco.com/cids/idiom" schemaVersion="2.00">
  <editConfigDelta xmlns="http://www.cisco.com/cids/idconf">
    <component name="userAccount">
      <config typedefsVersion="2004-03-01" xmlns="http://www.cisco.com/cids/idconf">
        <struct>
           <map name="user-accounts‟ editOp=‟merge”>
             <mapEntry>
               <key>
                <var name="name">cisco</var>
              </key>
               <struct>
                <struct name="credentials">
                  <var name="role">administrator</var>
                </struct>
               </struct>
            </mapEntry>
          </map>
        </struct>
      </config>
    </component>
  </editDefaultConfig>
</request>
```

SDEE

IPS は、侵入アラートやステータス イベントなどのさまざまなタイプのイベントを生成します。IPS は、IPS 業界最先端の独自プロトコル、SDEE を使用して、管理アプリケーションなどのクライアントにイベントを伝達します。SDEE は、セキュリティ デバイスのイベントを伝達するための製品に依存しない標準です。SDEE には、各種のセキュリティ デバイスによって生成されるイベントの伝達に必要な拡張機能が追加されています。

SDEE を使用してクライアントにイベントを伝達するシステムは、SDEE プロバイダーと呼ばれます。SDEE では、HTTP または HTTP over SSL および TLS プロトコルを使用してイベントが転送されるように指定します。HTTP または HTTPS を使用する場合は、SDEE クライアントが HTTP 要求の発信側となり、SDEE プロバイダーは HTTP サーバとして動作します。

IPS には、HTTP または HTTPS 要求を処理する Web サーバが含まれています。Web サーバは、実行時にロード可能なサーブレットを使用して、各種の HTTP 要求を処理します。各サーブレットは、そのサーブレットに関連付けられた URL に送られる HTTP 要求を処理します。SDEE サーバは、Web サーバ サーブレットとして実装されます。

SDEE サーバは、許可された要求のみを処理します。要求は、クライアントの ID を認証し、クライアントの権限レベルを確認するために Web サーバから発信されている場合に許可されます。

CIDEE

CIDEE は、Cisco IPS が使用する SDEE への拡張を指定します。CIDEE 標準は、Cisco IPS がサポートする可能性のあるすべての拡張を指定しています。特定のシステムでは、CIDEE の拡張のサブセットを実装する場合もあります。ただし、必須と指定された拡張は、すべてのシステムでサポートする必要があります。

CIDEE は、Cisco IPS 固有のセキュリティ デバイス イベント、および SDEE の evIdsAlert 要素に対する IPS の拡張を指定します。

CIDEE は次のイベントをサポートします。

- evError：エラー イベント

  CIDEE プロバイダーがエラーまたは警告状態を検出したときに、CIDEE プロバイダーによって生成されます。evError イベントには、エラー コードとテキストによるエラーの説明が含まれます。

- evStatus：ステータス メッセージ イベント

  ホストで潜在的に注意が必要な何らかの状態が発生したことを示すために、CIDEE プロバイダーによって生成されます。ステータス イベントでは、異なるタイプのステータス メッセージが報告される可能性があります（イベントごとに 1 つのメッセージ）。各タイプのステータス メッセージには、そのステータス メッセージで説明されている発生タイプに固有のデータ要素のセットが含まれます。ステータス メッセージの多くに含まれる情報は、監査の目的で役立ちます。エラーと警告はステータス情報とは見なされず、evStatus ではなく evError を使用して報告されます。

- evShunRqst：ブロック要求イベント

  ネットワークのブロッキングを処理するサービスがブロック アクションを開始することを示すために生成されます。

次に、CDIEE 拡張イベントの例を示します。

```
<sd:events xmlns:cid="http://www.cisco.com/cids/2004/04/cidee"
xmlns:sd="http://example.org/2010/08/sdee">
 <sd:evIdsAlert eventId="1042648730045587005" vendor="Cisco" severity="medium">
  <sd:originator>
    <sd:hostId>Beta4Sensor1</sd:hostId>
    <cid:appName>sensorApp</cid:appName>
```

```
  <cid:appInstanceId>8971</cid:appInstanceId>
</sd:originator>
<sd:time offset="0" timeZone="UTC">1043238671706378000</sd:time>
<sd:signature description="IOS Udp Bomb" id="4600" cid:version="S37">
  <cid:subsigId>0</cid:subsigId>
</sd:signature> …
```

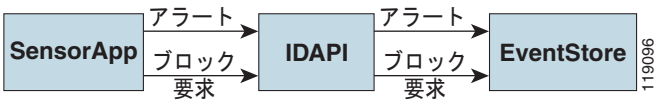
IDAPI

IPS アプリケーションは、IDAPI というプロセス間通信 API を使用して内部的な通信を処理します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。IDAPI は、すべてのアプリケーションが通信の際に使用するインターフェイスです。

SensorApp は、そのインターフェイス上のネットワーク トラフィックをキャプチャし、分析します。シグニチャが一致すると、SensorApp はアラートを生成します。このアラートはイベント ストアに格納されます。シグニチャがブロッキング応答アクションを実行するように設定されていると、SensorApp はブロック イベントを生成します。このイベントもイベント ストアに格納されます。

図 A-5 に、IDAPI インターフェイスを示します。

図 A-5　　IDAPI



各アプリケーションは、イベントおよび制御トランザクションを送受信するように IDAPI に登録します。IDAPI は次のサービスを提供します。

- 制御トランザクション
  - 制御トランザクションを開始する。
  - インバウンド制御トランザクションを待機する。
  - 制御トランザクションに応答する。
- IPS イベント
  - リモート IPS イベントをサブスクライブする。受信したリモート IPS イベントは、イベント ストアに格納されます。
  - イベント ストアから IPS イベントを読み取る。
  - イベント ストアに IPS イベントを書き込む。

IDAPI は、アトミックなデータ アクセスを実現するために必要な同期メカニズムを備えています。

Cisco IPS のファイル構造

Cisco IPS のディレクトリ構造は次のとおりです。

- /usr/cids/idsRoot：メインのインストール ディレクトリ。
- /usr/cids/idsRoot/shared：システムのリカバリ中に使用されるファイルが格納されます。
- /usr/cids/idsRoot/var：センサーの実行中に動的に作成されたファイルが格納されます。
- /usr/cids/idsRoot/var/updates：アップデート インストレーション用のファイルとログが格納されます。

- /usr/cids/idsRoot/var/virtualSensor：SensorApp が正規表現を分析するために使用するファイルが格納されます。
- /usr/cids/idsRoot/var/eventStore：イベント ストア アプリケーションが含まれます。
- /usr/cids/idsRoot/var/core：システムのクラッシュ時に作成される重要なファイルが格納されます。
- /usr/cids/idsRoot/var/iplogs：iplog ファイルのデータが格納されます。
- /usr/cids/idsRoot/bin：バイナリ実行可能ファイルが含まれます。
- /usr/cids/idsRoot/bin/authentication：認証アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/cidDump：技術サポート向けのデータを収集するスクリプトが含まれます。
- /usr/cids/idsRoot/bin/cidwebserver：Web サーバ アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/cidcli：CLI アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/nac：ARC アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/logApp：ロガー アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/mainApp：メイン アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/sensorApp：センサー アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/collaborationApp：コラボレーション アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/falcondump：IDSM2 のセンシング ポートでパケット ダンプを取得するアプリケーションが含まれます。
- /usr/cids/idsRoot/etc：センサーのコンフィギュレーション ファイルが含まれます。
- /usr/cids/idsRoot/htdocs：Web サーバの IDM ファイルが含まれます。
- /usr/cids/idsRoot/lib：センサー アプリケーションのライブラリ ファイルが含まれます。
- /usr/cids/idsRoot/log：デバッグ用のログ ファイルが含まれます。
- /usr/cids/idsRoot/tmp：センサーの実行中に作成される一時ファイルが格納されます。

Cisco IPS アプリケーションの概要

表 A-2 に、IPS を構成するアプリケーションの概要を示します。

表 A-2　アプリケーションの概要

アプリケーション	説明
AuthenticationApp	IP アドレス、パスワード、およびデジタル証明書に基づいてユーザを許可および認証します。
Attack Response Controller	ARC は、各センサー上で実行されます。各 ARC は、ローカル イベント ストアのネットワーク アクセス イベントをサブスクライブします。ARC の設定には、センサー、およびそのローカル ARC が制御するネットワーク アクセス デバイスのリストが含まれます。ネットワーク アクセス イベントをマスター ブロッキング センサーに送信するように設定されている場合、ARC は、デバイスを制御するリモート ARC に対してネットワーク アクセス コントロール トランザクションを開始します。これらのネットワーク アクセス アクション制御トランザクションは、IPS マネージャがネットワーク アクセス アクションを発行するときにも使用されます。

表 A-2　アプリケーションの概要 （続き）

アプリケーション	説明
CLI	コマンドライン入力を受け付け、IDAPI を使用してローカル設定を変更します。
CollaborationApp	グローバル相関データベースを通じて他のデバイスと情報を共有することにより、すべてのデバイスの総合的効果を高めます。
Control Transaction Server[1]	リモート クライアントからの制御トランザクションを受け付け、ローカル制御トランザクションを開始して、リモート クライアントに応答を返します。
Control Transaction Source[2]	リモート アプリケーションに向けられた制御トランザクションを待機し、制御トランザクションをリモート ノードに転送し、応答を発信側に返します。
IDM	HTML IPS 管理インターフェイスを提供する Java アプレットです。
IME	イベントを表示およびアーカイブするためのインターフェイスを提供する Java アプレットです。
InterfaceApp	バイパスおよび物理設定を処理し、ペアになっているインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。
ロガー	アプリケーションのすべてのログ メッセージをログ ファイルに書き出し、アプリケーションのエラー メッセージをイベント ストアに書き出します。
MainApp	設定を読み取ってアプリケーションを起動し、アプリケーションの開始および終了とノードの再起動を扱い、ソフトウェアのアップグレードを処理します。
NotificationApp	アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp はパブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的なヘルスに関する情報を提供します。
SDEE サーバ[3]	リモート クライアントからイベントの要求を受け付けます。
SensorApp	モニタされているネットワーク上のトラフィックをキャプチャして分析し、intrusion および network access イベントを生成します。ロギングをオン/オフする IP ロギング制御トランザクション、および IP ログ ファイルを送信および削除する IP ロギング制御トランザクションに応答します。
Web サーバ	リモート HTTP クライアント要求を待機し、適切なサーブレット アプリケーションを呼び出します。

1. これは Web サーバ サーブレットです。
2. これは、リモート制御トランザクション プロキシです。
3. これは Web サーバ サーブレットです。

APPENDIX B

シグニチャ エンジンの概要

（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。

この付録では、IPS シグニチャ エンジンについて説明します。次のような構成になっています。

- 「シグニチャ エンジンの概要」（P.B-2）
- 「Master エンジン」（P.B-4）
- 「正規表現の構文」（P.B-10）
- 「AIC エンジン」（P.B-11）
- 「Atomic エンジン」（P.B-12）
- 「Fixed エンジン」（P.B-27）
- 「Flood エンジン」（P.B-30）
- 「Meta エンジン」（P.B-31）
- 「Multi String エンジン」（P.B-32）
- 「ノーマライザ エンジン」（P.B-33）
- 「Service エンジン」（P.B-36）
- 「State エンジン」（P.B-54）
- 「String エンジン」（P.B-56）
- 「String XL エンジン」（P.B-59）
- 「Sweep エンジン」（P.B-62）
- 「Traffic Anomaly エンジン」（P.B-65）
- 「Traffic ICMP エンジン」（P.B-67）
- 「Trojan エンジン」（P.B-68）

シグニチャ エンジンの概要

シグニチャ エンジンは、特定のカテゴリで多数のシグニチャをサポートすることを目的とした Cisco IPS のコンポーネントです。エンジンは、パーサーとインスペクタで構成されています。各エンジンにはパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。

（注）　Cisco IPS エンジンは、標準化された 正規表現をサポートします。

Cisco IPS には、次のシグニチャ エンジンが含まれます。

- AIC：Web トラフィックの綿密な分析を行います。AIC エンジンは、HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの不正利用を防ぎます。また、指定されたポート上でトンネルを作成しようとするインスタント メッセージングや gotomypc などのアプリケーションを管理制御できます。また、AIC を使用して、FTP トラフィックを検査し、発行されるコマンドを制御することもできます。AIC エンジンには、AIC FTP と AIC HTTP の 2 つがあります。
- Atomic：Atomic エンジンは、マルチレベルの選択肢を持つ 4 つのエンジンに結合されます。IP + TCP など、レイヤ 3 属性とレイヤ 4 属性を 1 つのシグニチャ内で結合できます。Atomic エンジンでは、標準化された正規表現のサポートが使用されます。Atomic エンジンは、次のタイプで構成されます。
  - Atomic ARP：レイヤ 2 ARP プロトコルを検査します。Atomic ARP エンジンが異なるのは、大半のエンジンはレイヤ 3 IP プロトコルに基づいているためです。
  - Atomic IP Advanced：IPv6 レイヤ 3 および ICMPv6 レイヤ 4 トラフィックを検査します。
  - Atomic IP：IP プロトコル パケット、および関連付けられているレイヤ 4 トランスポート プロトコルを検査します。

    このエンジンを使用することで、IP ヘッダーおよびレイヤ 4 ヘッダー内のフィールドに照合する値を指定でき、正規表現を使用したレイヤ 4 ペイロードの検査が可能になります。

    （注）　すべての IP パケットは、Atomic IP エンジンよって検査されます。このエンジンは、4.x Atomic ICMP、Atomic IP Options、Atomic L3 IP、Atomic TCP、および Atomic UDP の各エンジンに取って代わりました。

  - Atomic IPv6：不正な形式の IPv6 トラフィックによって誘導される 2 つの IOS 脆弱性を検出します。
- Fixed：固定レベルまで並列正規表現照合を実行してから、1 つの正規表現テーブルを使用する検査を停止します。Fixed エンジンには、ICMP、TCP、および UDP の 3 つがあります。
- Flood：ホストおよびネットワークに向けられた ICMP および UDP フラッドを検出します。Flood エンジンには、Flood Host と Flood Net の 2 つがあります。
- Meta：スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。
- Multi String：1 つのシグニチャに対する複数の文字列を照合することにより、レイヤ 4 トランスポート プロトコルおよびペイロードを検査します。このエンジンは、ストリームベースの TCP と単一の UDP、および ICMP パケットを検査します。
- Normalizer：IP および TCP ノーマライザが機能する方法を設定し、IP および TCP ノーマライザに関連するシグニチャ イベントに設定を提供します。RFC 準拠を強制できます。

- Service：特定のプロトコルを処理します。Service エンジンは、次のプロトコル タイプに分けられます。
  - DNS：DNS（TCP および UDP）トラフィックを検査します。
  - FTP：FTP トラフィックを検査します。
  - FTP V2：IOS IPS をサポートします。

    このシグニチャ エンジンは、IOS IPS 向けにチューニング済みのプロトコル デコード エンジンを提供します。このエンジンを使用しようとすると、エラー メッセージを受け取ります。
  - Generic：カスタム サービスおよびペイロードをデコードし、ネットワーク プロトコルを一般的に分析します。
  - H225：VoIP トラフィックを検査します。VoIP ネットワークに到達する SETUP メッセージが有効であり、ポリシーで定義されている範囲内にあることを、ネットワーク管理者が確認するのに役立ちます。また、アドレスや、url-id、email-id、および表示情報などの Q.931 文字列フィールドが特定の長さに従っており、そこに潜在的な攻撃パターンが含まれていないことを確認するのにも役立ちます。
  - HTTP：HTTP トラフィックを検査します。WEBPORTS 変数では、HTTP トラフィックの検査ポートを定義します。
  - HTTP V2：IOS IPS をサポートします。

    このシグニチャ エンジンは、IOS IPS 向けにチューニング済みのプロトコル デコード エンジンを提供します。このエンジンを使用しようとすると、エラー メッセージを受け取ります。
  - IDENT：IDENT（クライアントおよびサーバ）トラフィックを検査します。
  - MSRPC：MSRPC トラフィックを検査します。
  - MSSQL：Microsoft SQL トラフィックを検査します。
  - NTP：NTP トラフィックを検査します。
  - P2P：P2P トラフィックを検査します。
  - RPC：RPC トラフィックを検査します。
  - SMB Advanced：Microsoft SMB パケットと Microsoft DCE/RPC（MSRPC）over SMB パケットを処理します。

    （注） SMB エンジンは、SMB Advanced エンジンに置き換えられました。SMB エンジンがまだ IDM、IME、および CLI に表示される場合でも、このシグニチャは廃止されています。つまり、新規のシグニチャには、対応する古いシグニチャの ID を持つ obsoletes パラメータ セットがあります。新規の SMB Advanced エンジンを使用して、SMB エンジンにあったカスタム シグニチャを書き換えてください。
  - SMPT V1：IOS IPS をサポートします。

    このシグニチャ エンジンは、IOS IPS 向けにチューニング済みのプロトコル デコード エンジンを提供します。このエンジンを使用しようとすると、エラー メッセージを受け取ります。
  - SNMP：SNMP トラフィックを検査します。
  - SSH：SSH トラフィックを検査します。
  - TNS：TNS トラフィックを検査します。
- State：SMTP などのプロトコル内の文字列のステートフル検索を実施します。State エンジンには非表示のコンフィギュレーション ファイルがあります。このファイルは、新規の状態定義をシグニチャ アップデートに配信できるよう、状態の移行を定義するために使用されます。

- String：ICMP、TCP、または UDP プロトコルに基づいた正規表現文字列を検索します。String エンジンには、String ICMP、String TCP、および String UDP の 3 つがあります。
- String XL：ICMP、TCP、または UDP プロトコルに基づいた正規表現文字列を検索します。String XL エンジンは、正規表現アクセラレータ カードの最適な動作を実現します。String エンジンには、String ICMP XL、String TCP XL、および String UDP XL の 3 つがあります。

（注）　現時点で、String XL エンジンと正規表現アクセラレータ カードをサポートしているのは、Cisco ASA 5585-X のみです。

（注）　正規表現アクセラレータ カードは、標準の String エンジンと新規の String XL エンジンの両方に使用されます。ほとんどの標準 String エンジン シグニチャは、変更することなく、正規表現アクセラレータ カードによってコンパイルおよび分析できます。ただし、標準の String エンジン シグニチャを正規表現アクセラレータ カード用にコンパイルできない特別な状況もあります。そのような状況では、正規表現アクセラレータ カードでコンパイルする String XL エンジンの特定のパラメータを使用して、String XL エンジンに新規のシグニチャが作成されます。String XL エンジンの新規シグニチャは、標準の String エンジンにある元のシグニチャに代わるものです。

- Sweep：1 つのホスト（ICMP と TCP）、宛先ポート（TCP と UDP）、および 2 つのノード間で RPC 要求を送受信する複数のポートからのスイープを分析します。Sweep エンジンには、Sweep と Sweep Other TCP の 2 つがあります。
- Traffic Anomaly：ワームについて TCP、UDP、およびその他のトラフィックを検査します。
- Traffic ICMP：TFN2K、LOKI、DDOS などの非標準プロトコルを分析します。パラメータを設定できるのは 2 つのシグニチャだけです。
- Trojan：BO2K および TFN2K など、非標準プロトコルからのトラフィックを分析します。Trojan エンジンには、Bo2k、Tfn2k、および UDP の 3 つがあります。これらのエンジンには、ユーザが設定できるパラメータはありません。

詳細情報

シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Master エンジン

Master エンジンは、他のエンジンに構造体およびメソッドを提供し、コンフィギュレーションからの入力とアラート出力を処理します。ここでは、Master エンジンについて説明します。次のような構成になっています。

- 「一般的なパラメータ」（P.B-5）
- 「アラート頻度」（P.B-7）
- 「イベント アクション」（P.B-8）

一般的なパラメータ

次のパラメータは、Master エンジンの一部であり、すべてのシグニチャに適用されます（そのシグニチャ エンジンにとって意味がある場合）。

表 B-1 に、一般的な Master エンジンのパラメータを示します。

表 B-1　MASTER エンジンのパラメータ

パラメータ	説明	値
signature-id	このシグニチャの ID を指定します。	*number*
sub-signature-id	このシグニチャのサブ ID を指定します。	*number*
alert-severity	次に示すアラートの重大度を指定します。 • 危険アラート • 中間レベル アラート • 低レベル アラート • 情報アラート	• high • medium • low • informational（デフォルト）
sig-fidelity-rating	このシグニチャの忠実度レーティングを指定します。	0 ～ 100 （デフォルト = 100）
promisc-delta	アラートの重大度の決定に使用するデルタ値を指定します。	0 ～ 30 （デフォルト = 5）
sig-name	シグニチャの名前を指定します。	*sig-name*
alert-notes	アラート メッセージに含まれる、このシグニチャに関する追加情報を示します。	*alert-notes*
user-comments	このシグニチャに関するコメントを示します。	*comments*
alert-traits	このシグニチャについて文書化する特性を指定します。	0 ～ 65335
release	シグニチャが最後に更新されたリリースを示します。	*release*
signature-creation-date	シグニチャが作成された日付を指定します。	—
signature-type	シグニチャのカテゴリを指定します。	• anomaly • component • exploit • other vulnerability
engine	シグニチャが属するエンジンを指定します。 **（注）** エンジン固有のパラメータは、engine カテゴリの下に表示されます。	—
event-count	アラートを生成するまでのイベントの発生回数を指定します。	1 ～ 65535 （デフォルト = 1）

表 B-1　MASTER エンジンのパラメータ （続き）

パラメータ	説明	値
event-count-key	このシグニチャに関するイベントをカウントするストレージ タイプを指定します。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃者のアドレスと攻撃対象のポート • 攻撃対象のアドレス • 攻撃者と攻撃対象のアドレスおよびポート	• Axxx • AxBx • Axxb • xxBx • AaBb
specify-alert-interval {yes | no}	アラート間隔をイネーブルにします。 • alert-interval：イベント カウントがリセットされるまでの秒数を指定します。	2 ～ 1000
status	シグニチャが、イネーブルとディセーブルのどちらであるか、アクティブと廃棄のどちらであるかを指定します。	enabled | retired {yes | no}
obsoletes	新しいシグニチャによって古いシグニチャがディセーブルになったことを示します。	—
vulnerable-os-list	パッシブ OS フィンガープリントと組み合わせると、IPS は、所定の攻撃がターゲット システムに関連している可能性があるかどうかを判断できるようになります。	aix bsd general-os hp-ux ios irix linus mac-os netware other solaris unix windows windows-ut windows-nt-2k-xp
mars-category {yes | no}	MARS 攻撃カテゴリにシグニチャをマッピングします。[1]	—

1. これは、コンフィギュレーションに設定でき、アラートに表示できる静的情報カテゴリです。詳細については、MARS のマニュアルを参照してください。

Promiscuous Delta

無差別デルタによって、無差別モードでの特定のアラートのリスク レーティングが下がります。センサーはターゲット システムの属性を認識せず、無差別モードではパケットを拒否できないため、管理者がリスク レーティングの高いアラートの調査に集中できるよう、（リスク レーティングの低さに基づいて）無差別アラートの優先順位を下げるのに役立ちます。インライン モードでは、攻撃パケットがターゲット ホストに到達することのないよう、センサーがそれらのパケットを拒否できるので、ターゲットが脆弱であるかどうかは問題になりません。ネットワーク上で攻撃は拒否されるので、IPS はリスク レーティング値を下げません。サービス、OS、またはアプリケーションに固有ではないシグニチャは、無差別デルタが 0 になります。シグニチャが OS、サービス、またはアプリケーションに固有の場合は、カテゴリごとに 5 つのポイントで 5、10、または 15 の無差別デルタが計算されます。

注意　シグニチャの promisc-delta 設定は変更しないことを推奨します。

Obsoletes

シスコのシグニチャ チームでは、改善された最新のシグニチャに置き換えられた古い廃止シグニチャを示すため、また、エンジンでより適切なインスタンスを使用できる場合にそのエンジンでディセーブル化されたシグニチャを示すために、obsoletes フィールドを使用します。たとえば、現在、いくつかの String XL ハードウェア高速化シグニチャが、String エンジンに定義された同等のシグニチャに取って代わりました。

Vulnerable OS List

シグニチャの脆弱な OS の設定とパッシブ OS フィンガープリントを組み合わせると、IPS は、特定の攻撃がターゲット システムに関連している可能性があるかどうかを判断できます。攻撃が関連していることがわかると、表示されるアラートのリスク レーティング値が増大します。関連性が不明である場合は、通常、パッシブ OS フィンガープリント リストにエントリが存在しないため、リスク レーティングに対する変更は行われません。パッシブ OS フィンガープリントのエントリが存在し、シグニチャの脆弱な OS の設定に一致しない場合、リスク レーティング値は減少します。リスク レーティングは、デフォルトで +/- 10 ポイント単位で増減されます。

詳細情報

- 無差別モードの詳細については、「無差別モード」（P.5-3）を参照してください。
- パッシブ OS フィンガープリントの詳細については、「OS ID の設定」（P.8-26）を参照してください。

アラート頻度

アラート頻度のパラメータの目的は、stick などの IDS DoS ツールに対抗するために、イベント ストアに書き込まれるアラートの量を削減することです。fire-all、fire-once、summarize、および global-summarize という 4 つのモードがあります。サマリー モードは、現在のアラート量に応じて動的に変わります。たとえば、シグニチャを fire-all に設定できますが、一定のしきい値に達するとサマライズが開始されます。

表 B-2 に、アラート頻度のパラメータを示します。

表 B-2　Master エンジンのアラート頻度のパラメータ

パラメータ	説明	値
alert-frequency	アラートをグループ化するためのサマリー オプション。	—
summary-mode	サマライズに使用されるモード。	—
fire-all	すべてのイベントについてアラートを起動します。	—
fire-once	1 回だけアラートを起動します。	—
global-summarize	攻撃者や攻撃対象の数に関係なく 1 回だけアラートが起動されるようにアラートをサマライズします。	—
summarize	アラートをサマライズします。	—
summary-threshold	アラート数のしきい値。この値を超えるとシグニチャはサマリー モードに送られます。	0 ～ 65535
global-summary-threshold	イベント数のしきい値。この値を超えるとアラートはグローバル サマリーにサマライズされます。	1 ～ 65535

表 B-2　Master エンジンのアラート頻度のパラメータ （続き）

パラメータ	説明	値
summary-interval	各サマリー アラートで使用される時間（秒数）。	1 ～ 1000
summary-key	シグニチャをサマライズするストレージ タイプ：	Axxx
	• 攻撃者のアドレス	AxBx
	• 攻撃者と攻撃対象のアドレス	Axxb
	• 攻撃者のアドレスと攻撃対象のポート	xxBx
	• 攻撃対象のアドレス	AaBb
	• 攻撃者と攻撃対象のアドレスおよびポート	

イベント アクション

（注）　次のイベント アクションのほとんどは、その特定のエンジンに適していない場合を除き、各シグニチャ エンジンに属しています。

次のイベント アクション パラメータは、各シグニチャ エンジンに属しています（そのシグニチャ エンジンにとって意味がある場合）。

- アラートおよびログ アクション
  - produce-alert：evIdsAlert をイベント ストアに書き込みます。
  - produce-verbose-alert：evIdsAlert に、違反パケットの符号化ダンプ（切り捨てられている可能性あり）を組み込みます。
  - log-attacker-packets：攻撃者のアドレスを含むパケットの IP ロギングを開始し、アラートを送信します。
  - log-victim-packets：攻撃対象のアドレスを含むパケットの IP ロギングを開始し、アラートを送信します。
  - log-pair-packets：（インライン モードのみ）攻撃者のアドレスと攻撃対象のアドレスのペアを含むパケットの IP ロギングを開始します。
  - request-snmp-trap：SNMP 通知を実行する要求を NotificationApp に送信します。
- 拒否アクション
  - deny-packet-inline：（インライン モードのみ）このパケットを送信しません。

    （注）　deny-packet-inline に対するイベント アクション オーバーライドは保護されているため、削除できません。このオーバーライドを使用しない場合は、このエントリに対する override-item-status をディセーブルに設定してください。

  - deny-connection-inline：（インライン モードのみ）TCP フローでこのパケットおよび将来のパケットを送信しません。
  - deny-attacker-victim-pair-inline：（インライン モードのみ）指定された期間、この攻撃者と攻撃対象のアドレスのペアについては、このパケットおよび将来のパケットを送信しません。
  - deny-attacker-service-pair-inline：（インライン モードのみ）指定された期間、攻撃者のアドレスと攻撃対象のポートのペアについては、このパケットと将来のパケットを送信しません。

- deny-attacker-inline：（インライン モードのみ）指定された期間、この攻撃者のアドレスから発生したこのパケットおよび将来のパケットを送信しません。

（注）　これは最も厳しい拒否アクションです。単一の攻撃者アドレスからの現在および将来のパケットが拒否されます。各拒否アドレスは、拒否が開始された最初のイベントから *X* 秒でタイムアウトになります。X は、設定した秒数です。ネットワーク上でアドレスを再び許可する **clear denied-attackers** コマンドを使用して、拒否されたすべての攻撃者エントリをクリアできます。

- modify-packet-inline：（インライン モードのみ）エンド ポイントにおけるパケットの使用目的についてあいまいさを取り除くため、パケット データを変更します。

（注）　modify-packet-inline は、ノーマライザ エンジンの一部です。このパラメータは、パケットを停止し、不良チェックサム、範囲外の値、その他の RFC 違反などの不規則な問題を修正します。

- その他のアクション

（注）　IPv6 は、request-block-host、request-block-connection、または request-rate-limit の各イベント アクションをサポートしません。

  - request-block-connection：この接続をブロックするよう、ARC に要求します。
  - request-block-host：この攻撃者ホストをブロックするよう、ARC に要求します。
  - request-rate-limit：レート制限を実行するよう、ARC に要求します。
  - reset-tcp-connection：TCP リセットを送信して、TCP フローを乗っ取って終了します。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、または deny-packet-inline をアクションとして追加するイベント アクション オーバーライドの場合、次のアクションが実行される場合があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

パケットのインライン拒否アクションは、アラート内でドロップ パケット アクションとして表示されます。パケットのインライン拒否が TCP 接続に対して発生すると、自動的に接続のインライン拒否アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

接続のインライン拒否が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

正規表現の構文

正規表現（Regex）は、テキストを記述する手段として、強力で柔軟性のある表記言語です。パターンマッチングでは、正規表現によりあらゆる任意のパターンを簡潔に表記できます。

表 B-3 に、IPS シグニチャの正規表現の構文を示します。

表 B-3　シグニチャの正規表現の構文

メタ文字	名前	説明
?	疑問符	0 回または 1 回の繰り返し。
*	星印（アスタリスク）	0 回以上の繰り返し。
+	プラス	1 回以上の繰り返し。
{x}	量指定子	ちょうど *X* 回の繰り返し。
{x,}	最小量指定子	少なくとも *X* 回の繰り返し。
.	ドット	改行（0x0A）以外の任意の 1 文字。
[abc]	文字クラス	リスト内の任意の 1 文字。
[^abc]	否定文字クラス	リストにない任意の 1 文字。
[a-z]	文字範囲クラス	範囲内（両端も含む）の任意の 1 文字。
( )	カッコ	他のメタ文字の適用範囲を制限する際に使用する。
|	論理和（OR）	このメタ文字によって区切られている複数の表現のいずれかと一致します。
^	キャレット	行の先頭。
char	エスケープ文字。	*char* がメタ文字である場合も含めて、*char* そのものと一致する。
char	文字	char がメタ文字でない場合は、char そのものと一致する。
\r	復帰	復帰文字（0x0D）と一致する。
\n	改行	改行文字（0x0A）と一致する。
\t	Tab	タブ文字（0x09）と一致する。
\f	フォーム フィード	フォーム フィード文字（0x0C）と一致する。
\xNN	エスケープされた 16 進数文字	16 進コード 0xNN（0<=N<=F）を持つ文字と一致する。
\NNN	エスケープされた 8 進数文字	8 進コード NNN（0<=N<=8）を持つ文字と一致する。

繰り返し演算子ではいずれの場合も、該当する文字列のうち最も短いものが一致対象となります。一方、それ以外の演算子では、その適用範囲に最大限多くの文字が取り込まれるため、該当する文字列のうち最も長いものが一致対象となります。

表 B-4 は、正規表現のパターンの例を示したものです。

表 B-4　正規表現のパターン

一致対象	正規表現
Hacker	Hacker
Hacker または hacker	[Hh]acker
bananas、bananananas、banananananas など、一定の規則で構成されたすべての文字列	ba(na)+s
同じ行の中にある foo と bar の間に改行以外の文字が 0 個以上ある文字列	foo.*bar
foo または bar	foo|bar
moon または soon	(m|s)oon

AIC エンジン

Application Inspection and Control（AIC）エンジンは、HTTP Web トラフィックを検査し、FTP コマンドを施行します。ここでは、AIC エンジンとそのパラメータについて説明します。次のような構成になっています。

- 「AIC エンジンについて」（P.B-11）
- 「AIC エンジンとセンサーのパフォーマンス」（P.B-11）
- 「AIC エンジンのパラメータ」（P.B-12）

AIC エンジンについて

AIC は、Web トラフィックを徹底的に分析できます。HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。また、指定されたポート上でトンネルを作成しようとするインスタント メッセージングや gotomypc などのアプリケーションを管理制御できます。P2P およびインスタント メッセージングが HTTP で動作している場合は、それらのアプリケーションの検査チェックおよびポリシー チェックが可能です。AIC は、FTP トラフィックを検査し、実行されているコマンドを制御する方法も提供します。事前に定義されているシグニチャをイネーブルまたはディセーブルにしたり、カスタム シグニチャによってポリシーを作成したりできます。

（注）　AIC エンジンは、HTTP トラフィックが AIC Web ポート上で受信されたときに動作します。トラフィックが Web トラフィックでも、AIC Web ポート上で受信されなければ、Service HTTP エンジンが実行されます。AIC 検査は、AIC Web ポートとして設定されたポートで、検査対象のトラフィックが HTTP トラフィックであれば、任意のポート上に存在できます。

AIC エンジンとセンサーのパフォーマンス

アプリケーション ポリシーの適用は、独自のセンサー機能です。AIC ポリシーの適用は、悪用、脆弱性、および異常を検査する従来の IPS テクノロジーをベースにしたものではなく、HTTP サービス ポリシーと FTP サービス ポリシーを適用するように設計されています。このポリシー適用に必要な検査動作は、従来の IPS 検査動作と比べて負荷が非常に高くなります。この機能の使用には、パフォーマンスの大幅な低下が伴います。AIC がイネーブルの場合、センサーの全体的な帯域幅キャパシティが減少します。

AIC ポリシーの適用は、IPS デフォルト設定ではディセーブルになっています。AIC ポリシーの適用を有効にする場合は、必要なポリシーだけを慎重に選択し、必要のないポリシーはディセーブルにすることを強く推奨します。また、センサーの検査負荷が最大容量に近くなっている場合は、センサーがオーバーサブスクライブされる可能性があるので、この機能の使用は推奨されません。このタイプのポリシー適用を処理する場合は、適応型セキュリティ アプライアンス ファイアウォールを使用することを推奨します。

AIC エンジンのパラメータ

AIC エンジンは、Web トラフィックのディープ インスペクション用のシグニチャを定義します。また、FTP コマンドを許可し、強制するシグニチャを定義します。AIC エンジンには、AIC HTTP と AIC FTP の 2 つがあります。

AIC エンジンには、次の機能があります。

- Web トラフィック：
  - RFC コンプライアンスの強制
  - HTTP 要求メソッドの許可と強制
  - 応答メッセージの検証
  - MIME タイプの強制
  - 転送符号化タイプの検証
  - 転送されるメッセージ コンテンツとデータ タイプに基づいたコンテンツ制御
  - URI の長さの強制
  - 設定されているポリシーとヘッダーに応じたメッセージ サイズの強制
  - トンネリング、P2P、およびインスタント メッセージングの強制

    この強制は、正規表現を使用して実行されます。事前定義されたシグニチャが存在しますが、リストを拡張できます。
- FTP トラフィック：
  - FTP コマンドの許可と強制

詳細情報

- AIC エンジン シグニチャの設定手順については、「AIC シグニチャの設定」（P.7-18）を参照してください。
- カスタム AIC シグニチャの例については、「AIC シグニチャの作成」（P.7-27）を参照してください。

Atomic エンジン

Atomic エンジンには、アラートの起動原因となる単純な単一パケットの条件に関するシグニチャが含まれます。ここでは、Atomic エンジンについて説明します。次のような構成になっています。

- 「Atomic ARP エンジン」（P.B-13）
- 「Atomic IP Advanced エンジン」（P.B-14）
- 「Atomic IP エンジン」（P.B-23）
- 「Atomic IPv6 エンジン」（P.B-26）

Atomic ARP エンジン

Atomic ARP エンジンは、レイヤ 2 の基本的な ARP シグニチャを定義し、ARP スプーフィング ツールである dsniff と ettercap に対して高度な検出を実行します。

表 B-5 に、Atomic ARP エンジンに固有のパラメータを示します。

表 B-5　Atomic ARP エンジンのパラメータ

パラメータ	説明	値
specify-arp-operation	（任意）ARP 動作をイネーブルにします。 • arp-operation：検査する ARP 動作のタイプ。	0 ～ 65535
specify-mac-flip	（任意）MAC アドレスの置換回数をイネーブルにします。 • mac-flip：アラート内の MAC アドレスを置換する回数を指定します。	0 ～ 65535
specify-request-inbalance	（任意）要求のアンバランスをイネーブルにします。 • request-inbalance：特定の IP アドレスに対して応答よりも要求の方が多い場合に、アラートを起動します。	0 ～ 65535
specify-type-of-arp-sig	（任意）ARP シグニチャのタイプをイネーブルにします。 • type-of-arp-sig：起動する ARP シグニチャのタイプを指定します。 – 宛先ブロードキャスト：255.255.255.255 の ARP 宛先アドレスを検出した場合に、このシグニチャのアラートを起動します。 – 同一の送信元と宛先：送信元と宛先の MAC アドレスが同じである ARP 宛先アドレスを検出した場合に、このシグニチャのアラートを起動します。 – 送信元ブロードキャスト（デフォルト）：255.255.255.255 の ARP 送信元アドレスを検出した場合に、このシグニチャのアラートを起動します。 – 送信元マルチキャスト：ARP 送信元 MAC アドレス 01:00:5e:（00-7f）を検出した場合に、このシグニチャのアラートを起動します。	dst-broadcast same-src-dst src-broadcast src-multicast
storage-key	固定データを保存するために使用するアドレス キーのタイプ。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃対象のアドレス • グローバル	Axxx AxBx xxBx xxxx

Atomic IP Advanced エンジン

ここでは、Atomic IP Advanced エンジンについて説明します。次のような構成になっています。

- 「Atomic IP Advanced エンジンの概要」（P.B-14）
- 「Atomic IP Advanced エンジンに関する制約事項」（P.B-15）
- 「Atomic IP Advanced エンジンのパラメータ」（P.B-15）

Atomic IP Advanced エンジンの概要

Atomic IP Advanced エンジンは、IPv6 ヘッダーとその拡張、IPv4 ヘッダーとそのオプション、ICMP、ICMPv6、TCP、および UDP の解析および解釈を行い、異常なアクティビティを探し出します。

Atomic IP Advanced エンジン シグニチャは、次のことを行います。

- 偽造されたアドレスなど、IP アドレスの異常を検査します。
- パケットの長さフィールドに不良情報が含まれていないか検査します。
- パケットに関する情報アラートを起動します。
- 限定された既知の脆弱性に対して、重大度の高いアラートを起動します。
- IPv6 にも適用できる Engine Atomic IP 内の IPv6 固有のシグニチャを複製します。
- パケット データからの IP アドレス、ポート、プロトコル、および制限付きの情報に基づいてトンネル化されたトラフィックを識別する、デフォルトのシグニチャを提供します。

一番外側の IP トンネルだけが識別されます。IPv6 トンネル、または IPv4 トンネル内の IPv6 トラフィックが検出されると、シグニチャはアラートを起動します。埋め込まれたトンネル内のその他の IPv6 トラフィックがすべて検査されるわけではありません。次のトンネリング メソッドがサポートされていますが、個別に検出されません。たとえば、ISATAP、6to4、および手動 IPv6 RFC 4213 トンネルはすべて IPv4 内の IPv6 として表示され、シグニチャ 1007 によって検出されます。

- ISATAP
- 6to4（RFC 3056）
- 手動で設定されたトンネル（RFC 4213）
- IPv6 over GRE
- UDP 内の Teredo（IPv6）
- MPLS（非暗号化）
- IPv6 over IPv6

IPv6 は次の動作をサポートしています。

- 送信元 IP アドレス、宛先 IP アドレス、または IP アドレス ペアによる拒否
- アラート
- TCP 接続のリセット
- ロギング

Atomic IP Advanced エンジンに関する制約事項

Atomic IP Advanced エンジンには、次の制限事項があります。

- レイヤ 4 識別子が最初のパケットに表示されないようにパケットがフラグメント化されている場合、パケットのレイヤ 4 フィールドは検出できません。
- フラグメントの再構成は存在しないため、IPv6 によってフラグメント化されたパケットのフローから、レイヤ 4 の攻撃は検出できません。
- トンネル化されたフローを使用した攻撃は検出できません。
- フラグメンテーション ヘッダーに対する確認は制限されています。
- IPv6 機能は、ASA 8.2(4) が導入されている場合に IPS SSP でサポートされます。
- 不正な重複ヘッダーが存在する場合、シグニチャは起動しますが、各ヘッダーを個別に検査することはできません。
- 異常検出は、IPv6 トラフィックをサポートしません。IPv4 トラフィックのみが異常検出プロセッサに送信されます。
- IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、アラートは生成されますがアクションは実行されません。

Atomic IP Advanced エンジンのパラメータ

（注）　範囲内の 2 番目の数は、最初の数以上である必要があります。

表 B-6 に、Atomic IP Advanced エンジンに固有のパラメータを示します。

表 B-6　Atomic IP Advanced エンジンのパラメータ

パラメータ	説明	値
グローバル		
fragment-status	フラグメントが必要かどうかを指定します。	any | no-fragments | want-fragments
specify-encapsulation	（任意）パケットの L3 の始まりの前にあるカプセル化を指定します。[1] • encapsulation：検査するカプセル化のタイプ。	none | mpls | gre | ipv4-in-ipv6 | ipip| any
specify-ip-version	（任意）IP プロトコル バージョンを指定します。 • version：IPv4 または IPv6。	ipv4 | ipv6
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]
Regex		
specify-regex-inspection	（任意）正規表現の検査をイネーブルにします。	[yes] | [no]

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
regex-scope	検索の開始ポイントと終了ポイントを指定します。	• ipv6-doh-only • ipv6-doh-plus • ipv6-hoh-only • ipv6-hoh-plus • ipv6-rh-only • ipv6-rh-plus • layer3-only • layer3-plus • layer4
regex-string	単一の TCP パケット内で検索する正規表現を指定します。	string
specify-exact-match-offset	完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために regex-string が報告する必要のある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	最小一致長をイネーブルにします。 • min-match-length：regex-string が一致する必要のある最小バイト数を指定します。	0 ～ 65535
specify-min-match-offset	最小一致オフセットをイネーブルにします。 • min-match-offset：一致を有効にするために regex-string が報告する必要のある最小ストリーム オフセットを指定します。	0 ～ 65535
specify-max-match-offset	最大一致オフセットをイネーブルにします。 • max-match-offset：一致を有効にするために regex-string が報告する必要のある最大ストリーム オフセットを指定します。	0 ～ 65535
IPv6		
specify-authentication-header	（任意）認証ヘッダーの検査をイネーブルにします。 • ah-present：認証ヘッダーが存在することを指定します。 – ah-length：認証ヘッダーの長さを指定します。 – ah-next-header：認証ヘッダーの値を指定します。	have-ah | no-ah 0 ～ 1028 0 ～ 255

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-dest-options-header	（任意）宛先オプション ヘッダーの検査をイネーブルにします。 • doh-present：宛先オプション ヘッダーが存在することを指定します。 – doh-count：検査する宛先オプション ヘッダーの数を指定します。 – doh-length：検査する宛先オプション ヘッダーの長さを指定します。 – doh-next-header：検査する次の宛先オプション ヘッダーの数を指定します。 – doh-option-type：検査する宛先オプション ヘッダーのタイプを指定します。 – doh-option-length：検査する宛先オプション ヘッダーの長さを指定します。	have-doh | no-doh 0 ～ 2 8 ～ 2048 0 ～ 255 0 ～ 255 0 ～ 255
specify-esp-header	（任意）ESP ヘッダーの検査をイネーブルにします。 • esp-present ：ESP ヘッダーが存在することを指定します。	have-esp | no-esp
specify-first-next-header	（任意）最初のネクスト ヘッダーの検査をイネーブルにします。 • first-next-header : 検査する最初のネクスト ヘッダーの値を指定します。	0 ～ 255
specify-flow-label	（任意）フロー ラベルの検査をイネーブルにします。 • flow-label：検査するフロー ラベルの値を指定します。	0 ～ 1048575
specify-headers-out-of-order	（任意）順序が不正なヘッダーの検査をイネーブルにします。 • headers-out-of-order：検査するヘッダー順序を指定します。	[true] | [false]
specify-headers-repeated	（任意）繰り返されたヘッダーの検査をイネーブルにします。 • headers-repeated：検査するヘッダーの繰り返しを指定します。	[true] | [false]
specify-hop-limit	（任意）ホップ制限をイネーブルにします。 • hop-limit：検査するホップ制限の値を指定します。	0 ～ 255
specify-hop-options-header	（任意）ホップバイホップ オプション ヘッダーの検査をイネーブルにします。 • hoh-present : ホップバイホップ オプション ヘッダーが存在することを指定します。	have-hoh | no-hoh

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-ipv6-addr-options	（任意）IPv6 アドレス オプションをイネーブルにします。 • ipv6-addr-options : IPv6 アドレス オプションを指定します。 – address-with-localhostt : ::1 を持つ IP アドレス。 – documentation-address : 2001:db8::/32 プレフィクスを持つ IP アドレス。 – ipv6-addr : IP アドレス。 – link-local-address : IPv6 リンク ローカル アドレスを検査します。 – multicast-dst : 宛先マルチキャスト アドレスを検査します。 – multicast-src : 送信元マルチキャスト アドレスを検査します。 – not-link-local-address : リンクローカルではないアドレスを検査します。 – not-valid-address : リンクローカル、グローバル、またはマルチキャストに予約されていないアドレスを検査します。 – src-ip-eq-dst-ip : 送信元アドレスと宛先アドレスは同じです。	
specify-ipv6-data-length	（任意）IPv6 データ長の検査をイネーブルにします。 • ipv6-data-length : 検査する IPv6 データ長を指定します。	0 ～ 65535
specify-ipv6-header-length	（任意）IPv6 ヘッダー長の検査をイネーブルにします。 • ipv6-header-length : 検査する IPv6 ヘッダー長を指定します。	0 ～ 65535
specify-ipv6-total-length	（任意）IPv6 の合計長の検査をイネーブルにします。 • ipv6-total-length : 検査する IPv6 の合計長を指定します。	0 ～ 65535
specify-ipv6-payload-length	（任意）IPv6 ペイロード長の検査をイネーブルにします。 • ipv6-payload-length : 検査する IPv6 ペイロード長を指定します。	0 ～ 65535
specify-routing-header	（任意）ルーティング ヘッダーの検査をイネーブルにします。 • rh-present : ルーティング ヘッダーが存在することを指定します。	have-rh | no-rh

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-traffic-class	（任意）トラフィック クラスの検査をイネーブルにします。 • traffic-class：検査するトラフィック クラスの値を指定します。	0 ～ 255
IPv4		
specify-ip-addr-options	（任意）IP アドレス オプションをイネーブルにします。 • ip-addr-options：IP アドレス オプションを指定します。	address-with-localhost ip-addr rfc-1918-address src-ip-eq-dst-ip
specify-ip-header-length	（任意）IP ヘッダー長の検査をイネーブルにします。 • ip-header-length 検査する IP ヘッダー長を指定します。	0 ～ 16
specify-ip-id	（任意）IP 識別子の検査をイネーブルにします。 • ip-id：検査する IP ID を指定します。	0 ～ 255
specify-ip-option-inspection	（任意）IP オプションの検査をイネーブルにします。 • ip-option-inspection：IP オプションの値を指定します。 – ip-option：照合する IP OPTION コード。 – ip-option-abnormal：オプションのリストに誤りがあります。	0 ～ 65535 [true] | [false]
specify-ip-payload-length	（任意）IP ペイロード長の検査をイネーブルにします。 • ip-payload-length：検査する IP ペイロード長を指定します。	0 ～ 65535
specify-ip-tos	（任意）サービスの IP タイプを指定します。 • ip-tos：検査するサービスの IP タイプを指定します。	0 ～ 255
specify-ip-total-length	（任意）IP 合計長の検査をイネーブルにします。 • ip-total-length：検査する IP パケットの合計長を指定します。	0 ～ 65535
specify-ip-ttl	（任意）IP 存続可能時間の検査をイネーブルにします。 • ip-ttl：IP TTL の検査を指定します。	0 ～ 255
specify-ip-version	（任意）IP バージョンの検査をイネーブルにします。 • ip-version：検査する IP バージョンを指定します。	0 ～ 16

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
L4 プロトコル		
specify-l4-protocol	（任意）L4 プロトコルの検査をイネーブルにします。 • l4-protocol：検査する L4 プロトコルを指定します。	icmp icmpv6 tcp udp other
その他の L4 プロトコル		
other-ip-protocol-id	（任意）その他の L4 プロトコルの検査をイネーブルにします。 • other-ip-protocol-id：アラートを送信する単一 IP プロトコル番号を指定します。	0 ～ 256
L4 プロトコル ICMP		
specify-icmp-code	（任意）L4 ICMP コードの検査をイネーブルにします。 • icmp-code：ICMP ヘッダーの CODE 値を指定します。	0 ～ 65535
specify-icmp-id	（任意）L4 ICMP ID の検査をイネーブルにします。 • icmp-id：ICMP ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
specify-icmp-seq	（任意）L4 ICMP シーケンスの検査をイネーブルにします。 • icmp-seq：検査する ICMP シーケンスを指定します。	0 ～ 65535
specify-icmp-type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • icmp-type：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
L4 プロトコル ICMPv6		
specify-icmpv6-code	（任意）L4 ICMPv6 コードの検査をイネーブルにします。 • icmpv6-code：ICMPv6 ヘッダーの CODE 値を指定します。	0 ～ 255
specify-icmpv6-id	（任意）L4 ICMPv6 識別子の検査をイネーブルにします。 • icmpv6-id：ICMPv6 ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
specify-icmpv6-length	（任意）L4 ICMPv6 長の検査をイネーブルにします。 • icmpv6-length：ICMPv6 ヘッダーの LENGTH 値。	0 ～ 65535

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-icmpv6-mtu-field	（任意）L4 ICMPv6 MTU フィールドの検査をイネーブルにします。 • icmpv6-mtu-field：ICMPv6 ヘッダーの MTU フィールド値。	4,294,967,295
specify-icmpv6-option-type	（任意）L4 ICMPv6 タイプの検査をイネーブルにします。 • icmpv6-option-type：検査する ICMPv6 オプション タイプを指定します	0 ～ 255
icmpv6-option-length	（任意）L4 ICMPv6 オプション タイプの検査をイネーブルにします。 • icmpv6-option-length：検査する ICMPv6 オプション タイプを指定します	0 ～ 255
specify-icmpv6-seq	（任意）L4 ICMPv6 シーケンスの検査をイネーブルにします。 • icmpv6-seq：ICMPv6 ヘッダーの SEQUENCE 値。	0 ～ 65535
specify-icmpv6-type	（任意）L4 ICMPv6 タイプの検査をイネーブルにします。 • icmpv6-type : ICMPv6 ヘッダーの TYPE 値。	0 ～ 255
L4 プロトコル TCP および UDP		
specify-dst-port	（任意）使用する宛先ポートをイネーブルにします。 • dst-port：このシグニチャの該当宛先ポート。	0 ～ 65535
specify-src-port	（任意）使用する送信元ポートをイネーブルにします。 • src-port : このシグニチャの該当送信元ポート。	0 ～ 65535
specify-tcp-mask	（任意）使用する TCP マスクをイネーブルにします。 • tcp-mask：TCP フラグの比較に使用するマスク。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• urg • ack • psh • rst • syn • fin

表 B-6　Atomic IP Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-tcp-flags	（任意）使用する TCP フラグをイネーブルにします。 • tcp-flags：マスクによってマスクされた場合に照合する TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• urg • ack • psh • rst • syn • fin
specify-tcp-reserved	（任意）使用のために予約されている TCP をイネーブルにします。 • tcp-reserved：予約されている TCP。	0 ～ 63
specify-tcp-header-length	（任意）L4 TCP ヘッダー長の検査をイネーブルにします。 • tcp-header-length：検査に使用する TCP ヘッダーの長さを指定します。	0 ～ 60
specify-tcp-payload-length	（任意）L4 TCP ペイロード長の検査をイネーブルにします。 • tcp-payload-length：TCP ペイロードの長さを指定します。	0 ～ 65535
specify-tcp-urg-pointer	（任意）L4 TCP URG ポインタの検査をイネーブルにします。 • tcp-urg-pointer：TCP URG フラグ検査を指定します。	0 ～ 65535
specify-tcp-window-size	（任意）L4 TCP ウィンドウ サイズの検査をイネーブルにします。 • tcp-window-size：TCP パケットのウィンドウ サイズを指定します。	0 ～ 65535
specify-udp-valid-length	（任意）L4 UDP の有効な長さの検査をイネーブルにします。 • udp-valid-length：有効と見なされ、検査の必要のない UDP パケット長を指定します。	0 ～ 65535
specify-udp-length-mismatch	（任意）L4 UDP 長の不一致の検査をイネーブルにします。 • udp-length-mismatch：IP データ長が UDP ヘッダー長よりも短い場合はアラートを起動します。	[true] | [false]

1. パケットが GRE、IPIP、IPv4inIPv6、または MPL の場合、センサーは L3 カプセル化ヘッダーおよびカプセル化ヘッダーをスキップし、すべての検査は 2 番目の L3 から開始されます。カプセル化の列挙型によって、エンジンは当該の L3 の前にカプセル化ヘッダーが存在するかどうかを確認できます。

詳細情報

- カスタム IPv6 シグニチャの例については、「Atomic IP Advanced エンジン シグニチャの例」（P.7-53）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Atomic IP エンジン

Atomic IP エンジンは、IP プロトコル ヘッダーと、関連するレイヤ 4 トランスポート プロトコル（TCP、UDP、および ICMP）およびペイロードを検査するシグニチャを定義します。Atomic エンジンでは、複数のパケットにまたがる固定データは保存されません。その代わりに、1 つのパケットの分析を基にしてアラームを起動できます。

表 B-7 に、Atomic IP エンジンに固有のパラメータを示します。

表 B-7　Atomic IP エンジンのパラメータ

パラメータ	説明	値
specify-ip-addr-options	（任意）IP アドレス オプションをイネーブルにします。 • ip-addr-options：IP アドレス オプションを指定します。	address-with-localhost ip-addr rfc-1918-address src-ip-eq-dst-ip
specify-ip-header-length	（任意）IP ヘッダー長の検査をイネーブルにします。 • ip-header-length：検査する IP ヘッダー長を指定します。	0 ～ 16
specify-ip-id	（任意）IP 識別子の検査をイネーブルにします。 • ip-id：検査する IP ID を指定します。	0 ～ 255
specify-ip-option-inspection	（任意）IP オプションの検査をイネーブルにします。 • ip-option-inspection：IP オプションの値を指定します。 – ip-option：照合する IP OPTION コード。 – ip-option-abnormal：オプションのリストに誤りがあります。	0 ～ 65535 [true] | [false]
specify-ip-payload-length	（任意）IP ペイロード長の検査をイネーブルにします。 • ip-payload-length：検査する IP ペイロード長を指定します。	0 ～ 65535
specify-ip-tos	（任意）サービスの IP タイプを指定します。 • ip-tos：検査するサービスの IP タイプを指定します。	0 ～ 6 255

表 B-7　Atomic IP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-ip-total-length	（任意）IP 合計長の検査をイネーブルにします。 • ip-total-length：検査する IP パケットの合計長を指定します。	0 ～ 65535
specify-ip-ttl	（任意）IP 存続可能時間の検査をイネーブルにします。 • ip-ttl：IP TTL の検査を指定します。	0 ～ 255
specify-ip-version	（任意）IP バージョンの検査をイネーブルにします。 • ip-version：検査する IP バージョンを指定します。	0 ～ 16
specify-l4-protocol	（任意）L4 プロトコルの検査をイネーブルにします。 • l4-protocol：検査する L4 プロトコルを指定します。	icmp tcp udp other-protocol
specify-icmp-code	（任意）L4 ICMP コードの検査をイネーブルにします。 • icmp-code：ICMP ヘッダーの CODE 値を指定します。	0 ～ 65535
specify-icmp-id	（任意）L4 ICMP ID の検査をイネーブルにします。 • icmp-id：ICMP ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
specify-icmp-seq	（任意）L4 ICMP シーケンスの検査をイネーブルにします。 • icmp-seq：検査する ICMP シーケンスを指定します。	0 ～ 65535
specify-icmp-type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • icmp-type：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
specify-icmp-total-length	（任意）L4 ICMP 合計ヘッダー長の検査をイネーブルにします。 • icmp-total-length：検査する ICMP 合計長の値を指定します。	0 ～ 65535
other-ip-protocol-id	（任意）その他の L4 プロトコルの検査をイネーブルにします。 • other-ip-protocol-id：アラートを送信する単一 IP プロトコル番号を指定します。	0 ～ 256

表 B-7　Atomic IP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-dst-port	（任意）使用する宛先ポートをイネーブルにします。 • dst-port：このシグニチャの該当宛先ポート。	0 ～ 65535
specify-src-port	（任意）使用する送信元ポートをイネーブルにします。 • src-port：このシグニチャの該当送信元ポート。	0 ～ 65535
specify-tcp-mask	（任意）使用する TCP マスクをイネーブルにします。 • tcp-mask：TCP フラグの比較に使用するマスク。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• urg • ack • psh • rst • syn • fin
specify-tcp-flags	（任意）使用する TCP フラグをイネーブルにします。 • tcp-flags：マスクによってマスクされた場合に照合する TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• urg • ack • psh • rst • syn • fin
specify-tcp-reserved	（任意）使用のために予約されている TCP をイネーブルにします。 • tcp-reserved：予約されている TCP。	0 ～ 63
specify-tcp-header-length	（任意）L4 TCP ヘッダー長の検査をイネーブルにします。 • tcp-header-length：検査に使用する TCP ヘッダーの長さを指定します。	0 ～ 60

表 B-7　Atomic IP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-tcp-payload-length	（任意）L4 TCP ペイロード長の検査をイネーブルにします。 • tcp-payload-length：TCP ペイロードの長さを指定します。	0 ～ 65535
specify-tcp-urg-pointer	（任意）L4 TCP URG ポインタの検査をイネーブルにします。 • tcp-urg-pointer：TCP URG フラグ検査を指定します。	0 ～ 65535
specify-tcp-window-size	（任意）L4 TCP ウィンドウ サイズの検査をイネーブルにします。 • tcp-window-size：TCP パケットのウィンドウ サイズを指定します。	0 ～ 65535
specify-udp-length	（任意）L4 UDP 長の検査をイネーブルにします。 • udp-length：IP データ長が UDP ヘッダー長よりも短い場合はアラートを起動します。	0 ～ 65535
specify-udp-valid-length	（任意）L4 UDP の有効な長さの検査をイネーブルにします。 • udp-valid-length：有効と見なされ、検査の必要のない UDP パケット長を指定します。	0 ～ 65535
specify-udp-length-mismatch	（任意）L4 UDP 長の不一致の検査をイネーブルにします。 • udp-length-mismatch：IP データ長が UDP ヘッダー長よりも短い場合はアラートを起動します。	[true] | [false]

Atomic IPv6 エンジン

Atomic IPv6 エンジンは、異常のある IPv6 トラフィックによって誘導される 2 つの IOS 脆弱性を検出します。これらの脆弱性は、ルータ クラッシュやその他のセキュリティ問題を引き起こすおそれがあります。IOS 脆弱性の 1 つは、最初のフラグメントを複数処理し、バッファ オーバーフローを引き起こします。もう 1 つは、不正な ICMPv6 ネイバー探索オプションを処理し、同様にバッファ オーバーフローを引き起こします。

（注）　IPv6 は、IP アドレスを 32 ビットから 128 ビットに拡大し、より多くのアドレッシング階層レベルとアドレス指定可能ノード、およびアドレスの自動設定をサポートします。

8 つの Atomic IPv6 シグニチャがあります。Atomic IPv6 は、次のタイプのネイバー探索プロトコルを検査します。

- タイプ 133：ルータ送信要求
- タイプ 134：ルータ アドバタイズメント

- タイプ 135：ネイバー送信要求
- タイプ 136：ネイバー アドバタイズメント
- タイプ 137：リダイレクト

（注）　ホストおよびルータはネイバー探索を使用して、添付されたリンクに常駐し、無効になったキャッシュ値を素早くパージすることがわかっているネイバーのリンク層アドレスを判断します。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送する隣接ルータを検出します。

各ネイバー探索タイプには、1 つまたは複数のネイバー探索オプションを設定することができます。Atomic IPv6 エンジンは、各オプションの長さに対して RFC 2461 に明記されている有効値への準拠性を検査します。オプションの長さに違反があると、その長さが検出されたオプション タイプに対応するアラートが生成されます（シグニチャ 1601 ～ 1605）。

（注）　Atomic IPv6 シグニチャには、特に設定が必要なパラメータはありません。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Fixed エンジン

Fixed エンジンは、複数の正規表現パターンを 1 つのパターン マッチング テーブルにまとめ、データ内の検索を一度に実行できるようにします。このエンジンは、ICMP、TCP、および UDP プロトコルをサポートします。最小の検査深さに達すると（1 ～ 100 バイト）、検査は停止します。Fixed エンジンには、Fixed ICMP、Fixed TCP、および Fixed UDP の 3 つがあります。

（注）　Fixed TCP および Fixed UDP は、除外ポートとして service-ports パラメータを使用します。Fixed ICMP は、除外される ICMP タイプとして service-ports パラメータを使用します。

表 B-8 に、Fixed ICMP エンジンに固有のパラメータを示します。

表 B-8　Fixed ICMP エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
max-payload-inspect-length	シグニチャの最大検査深さを指定します。	1 ～ 250
regex-string	単一のパケット内で検索する正規表現を指定します。	string

表 B-8　Fixed ICMP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために regex-string が報告する必要のある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：regex-string が一致する必要のある最小バイト数を指定します。	0 ～ 65535
specify-icmp-type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • icmp-type：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

表 B-9 に、Fixed TCP エンジンに固有のパラメータを示します。

表 B-9　Fixed TCP エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
max-payload-inspect-length	シグニチャの最大検査深さを指定します。	1 ～ 250
regex-string	単一のパケット内で検索する正規表現を指定します。	string
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために regex-string が報告する必要のある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：regex-string が一致する必要のある最小バイト数を指定します。	0 ～ 65535

表 B-9　Fixed TCP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-service-ports	使用するサービス ポートをイネーブルにします。 • service-ports：ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-10 に、Fixed UDP エンジンに固有のパラメータを示します。

表 B-10　Fixed UDP エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
max-payload-inspect-length	シグニチャの最大検査深さを指定します。	1 ～ 250
regex-string	単一のパケット内で検索する正規表現を指定します。	string
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために regex-string が報告する必要のある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：regex-string が一致する必要のある最小バイト数を指定します。	0 ～ 65535
specify-service-ports	使用するサービス ポートをイネーブルにします。 • service-ports：ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Flood エンジン

Flood エンジンは、複数のパケットを単一のホストまたはネットワークに送信しているホストまたはネットワークをモニタするシグニチャを定義します。たとえば、攻撃対象ホストに送信される（特定のタイプの）パケットが 1 秒あたり 150 以上検出されると起動するシグニチャを作成できます。Flood エンジンには、Flood Host と Flood Net の 2 つのタイプがあります。

表 B-11 に、Flood Host エンジンに固有のパラメータを示します。

表 B-11　Flood Host エンジンのパラメータ

パラメータ	説明	値
protocol	検査するトラフィックの種類。	ICMP UDP
rate	1 秒あたりのパケット数のしきい値。	0 ～ 65535[1]
icmp-type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535
dst-ports	UDP プロトコルを選択した場合の宛先ポートを指定します。	0 ～ 65535[2] a-b[,c-d]
src-ports	UDP プロトコルを選択する場合の送信元ポートを指定します。	0 ～ 65535[3] a-b[,c-d]

1. レートが 1 秒あたりのパケット数よりも大きい場合はアラートが起動します。
2. 範囲の 2 番目の数は、最初の数以上である必要があります。
3. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-12 に、Flood Net エンジンに固有のパラメータを示します。

表 B-12　Flood Net エンジンのパラメータ

パラメータ	説明	値
gap	フラッディング シグニチャに許可された時間の差（秒単位）。	0 ～ 65535
peaks	許可されたフラッディング トラフィックのピークの数。	0 ～ 65535
protocol	検査するトラフィックの種類。	ICMP TCP UDP
rate	1 秒あたりのパケット数のしきい値。	0 ～ 65535[1]
sampling-interval	トラフィックをサンプリングする間隔。	1 ～ 3600
icmp-type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535

1. レートが 1 秒あたりのパケット数よりも大きい場合はアラートが起動します。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Meta エンジン

注意　Meta エンジン シグニチャを大量に使用すると、全体的なセンサー パフォーマンスに悪影響を与える可能性があります。

Meta エンジンでは、スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。シグネチャ イベントが生成されると、Meta エンジンはシグネチャ イベントを検査して、1 つ以上の Meta 定義に一致するかどうかを判定します。Meta エンジンは、すべてのイベント要件が満たされるとシグネチャ イベントを生成します。

すべてのシグネチャ イベントは、シグニチャ イベント アクション プロセッサによって Meta エンジンに渡されます。シグニチャ イベント アクション プロセッサは、最小ヒット数オプションを処理してからイベントを渡します。Meta エンジンがコンポーネント イベントを処理してから、サマライズおよびイベント アクションは処理されます。

表 B-13 に、Meta エンジンに固有のパラメータを示します。

表 B-13　Meta エンジン パラメータ

パラメータ	説明	値
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]
meta-reset-interval	Meta シグニチャをリセットする時間（秒単位）。	0 ～ 3600
component-list	Meta コンポーネントのリスト。 • edit：既存のエントリを編集します。 • insert：新しいエントリをリストに挿入します。 – begin：エントリをアクティブ リストの先頭に配置します。 – end：エントリをアクティブ リストの末尾に配置します。 – inactive：エントリを非アクティブ リストに配置します。 – before:エントリを指定エントリの前に配置します。 – after：エントリを指定エントリの後に配置します。 • move：リスト内のエントリを移動します。	*name1*

表 B-13　Meta エンジン パラメータ （続き）

パラメータ	説明	値
meta-key	Meta シグニチャのストレージ タイプ。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃者と攻撃対象のアドレスおよびポート • 攻撃対象のアドレス	AaBb AxBx Axxx xxBx
unique-victim-ports	Meta シグニチャごとに一意の必須攻撃対象ポートの番号。	1 ～ 256
component-list-in-order	コンポーネント リストが順番に起動するかどうか。	[true] | [false]

詳細情報

- カスタム Meta エンジン シグニチャの例については、「Meta エンジン シグニチャの例」（P.7-49）を参照してください。
- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Multi String エンジン

注意　Multi String エンジンは、メモリの使用状況に大きく影響することがあります。

Multi String エンジンでは、レイヤ 4 トランスポート プロトコル（ICMP、TCP、および UDP）のペイロードを検査するシグニチャを定義します。この検査は、1 つのシグニチャに対して複数の文字列を照合して行います。シグニチャを起動するために一致する必要がある一連の正規表現パターンを指定できます。たとえば、UDP サービスで regex 1 とそれに続く regex 2 を検索するシグニチャを定義できます。UDP および TCP の場合は、ポート番号と方向を指定できます。単一の送信元ポート、単一の宛先ポート、または両方のポートを指定できます。文字列の照合は両方向で実行されます。

複数の正規表現パターンを指定する必要がある場合は、Multi String エンジンを使用してください。それ以外の場合は、String ICMP、String TCP、または String UDP エンジンを使用して、これらのプロトコルのいずれかに対応した単一の正規表現パターンを指定できます。

表 B-14 に、Multi String エンジンに固有のパラメータを示します。

表 B-14　Multi String エンジンのパラメータ

パラメータ	説明	値
inspect-length	起動するシグニチャに対して違反するすべての文字列を含める必要があるストリームまたはパケットの長さ。	0 ～ 4294967295
protocol	レイヤ 4 プロトコルの選択。	icmp tcp udp

表 B-14　Multi String エンジンのパラメータ （続き）

パラメータ	説明	値
regex-component	regex コンポーネントのリスト。 • regex-string：検索する文字列。 • spacing-type：前回の一致箇所から、またはそれが一致結果からリストの最初のエントリの場合はストリームまたはパケットの先頭から空ける必要のある間隔のタイプ。	list（1 ～ 16 項目） exact minimum
port-selection	検査する TCP または UDP ポートのタイプ。 • both-ports：送信元ポートと宛先ポートの両方を指定します。 • dest-ports：宛先ポートの範囲を指定します。 • source-ports：送信元ポートの範囲を指定します。[1]	0 ～ 65535 [2]
exact-spacing	この正規表現文字列と直前の正規表現文字列との間、またはそれがリスト内の最初のエントリである場合にはストリームまたはパケットの先頭から空ける必要のある正確なバイト数。	0 ～ 4294967296
min-spacing	この正規表現文字列と直前の正規表現文字列との間、またはストリームやパケットの先頭から（リスト内の最初のエントリである場合）、空ける必要のある最小バイト数。	0 ～ 4294967296
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. ポートの照合は、クライアントからサーバへ、およびサーバからクライアントへ向かうトラフィック フローの両方の方向で実行されます。たとえば、送信元ポート値が 80 である場合、クライアントからサーバへのトラフィック フローの方向では、クライアント ポートがポート 80 の場合に検査が実行されます。サーバからクライアントへのトラフィック フローの方向では、サーバ ポートがポート 80 の場合に検査が実行されます。
2. 有効な値は、a-b[,c-d] 形式で指定された 0 ～ 65535 の範囲内の整数から成るカンマ区切りのリストです。範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

ノーマライザ エンジン

ノーマライザ エンジンは、IP フラグメンテーションと TCP 正規化を処理します。ここでは、ノーマライザ エンジンについて説明します。次のような構成になっています。

- 「ノーマライザ エンジンの概要」（P.B-34）
- 「ノーマライザ エンジンのパラメータ」（P.B-35）

ノーマライザ エンジンの概要

（注）　ノーマライザ エンジンには、カスタム シグニチャは追加できません。既存のシグニチャの調整は可能です。

ノーマライザ エンジンは、IP フラグメント再構成と TCP ストリーム再構成を処理します。ノーマライザ エンジンを使用すると、センサーが同時に追跡しようとするフラグメントの最大数など、システム リソースの使用に対する制限を設定できます。無差別モードのセンサーは、違反に対するアラートを報告します。インライン モードのセンサーは、produce-alert、deny-packet-inline、および modify-packet-inline など、イベント アクション パラメータで指定されたアクションを実行します。

注意　シグニチャ 3050 Half Open SYN Attack でアクションとして modify-packet-inline を選択している場合、保護がアクティブである間は 20 ～ 30 % ほどパフォーマンスが低下する可能性があります。保護は、実際の SYN フラッドの間だけアクティブになります。

IP フラグメンテーションの正規化

IP データグラムの意図した、または意図しないフラグメンテーションによってエクスプロイトが隠れる可能性があるので、検出が困難または不可能になります。フラグメンテーションは、ファイアウォールやルータにあるようなアクセス コントロール ポリシーを回避するために使用される場合もあります。また、さまざまなオペレーティング システムがさまざまな方法を使用して、フラグメント化されたデータグラムをキューに入れたりディスパッチしたりします。センサーがエンド ホストでデータグラムを再構成するために考えられるすべての方法を確認する必要がある場合は、センサーが DoS 攻撃を受ける可能性があります。フラグメント化されたデータグラムをすべてインラインで再構成し、完全なデータグラムだけを転送し、必要に応じてそのデータグラムを再度フラグメント化すれば、これを防ぐことができます。IP フラグメンテーションの正規化の装置は、この機能を実行します。

TCP の正規化

意図的または意図しない TCP セッション セグメンテーションによって、いくつかの攻撃クラスが隠されることがあります。ポリシーが偽陽性や偽陰性なしに実施されるようにするには、2 つの TCP エンドポイントの状態が追跡され、実際のホスト エンドポイントによって処理されたデータだけが渡される必要があります。TCP ストリームで重複が発生する可能性がありますが、TCP セグメントの再転送以外は、非常にまれです。TCP セッションでの上書きは発生してはならないものです。上書きが発生する場合は、誰かがセキュリティ ポリシーを意図的に回避しようとしているか、TCP スタックの実装が壊れています。センサーが TCP プロキシとして動作していない限り、両方のエンドポイントの状態について完全な情報を保持することはできません。センターが TCP プロキシとして動作する代わりに、セグメントが適切に並べられ、ノーマライザ エンジンによって回避および攻撃に関連する異常なパケットが検索されます。

IPv6 フラグメント

ノーマライザ エンジンは IPv6 フラグメントを再構成し、その他のエンジンやプロセッサによる検査およびアクション用に再構成されたバッファを転送できます。IPv4 と IPv6 の相違点は、次のとおりです。

- ノーマライザ エンジン シグニチャの modify-packet-inline は、IPv6 データグラムには効果がありません。
- シグニチャ 1206（IP Fragment Too Small）は、IPv6 データグラムに対して起動しません。Atomic IP Advanced エンジンのシグニチャ 1741 は、小さすぎる IPv6 フラグメントに対して起動します。
- シグニチャ 1202 は IPv6 ヘッダー フィールドが長いため、IPv6 の max-datagram-size を超えてさらに 48 バイトを追加できます。

詳細情報

- ノーマライザ エンジンに IP フラグメントの再構成シグニチャを設定する手順については、「IP フラグメント再構成の設定」（P.7-29）を参照してください。
- ノーマライザ エンジンに TCP ストリームの再構成シグニチャを設定する手順については、「TCP ストリーム再構成の設定」（P.7-33）を参照してください。

ノーマライザ エンジンのパラメータ

表 B-15 に、ノーマライザ エンジンに固有のパラメータを示します。

表 B-15　ノーマライザ エンジンのパラメータ

パラメータ	説明
edit-default-sigs-only	編集可能なシグニチャ。
specify-fragment-reassembly-timeout	（任意）フラグメント再構築タイムアウトをイネーブルにします。
specify-hijack-max-old-ack	（任意）hijack-max-old-ack をイネーブルにします。
specify-max-dgram-size	（任意）最大データグラム サイズをイネーブルにします。
specify-max-fragments	（任意）最大フラグメントをイネーブルにします。
specify-max-fragments-per-dgram	（任意）データグラムあたりの最大フラグメントをイネーブルにします。
specify-max-last-fragments	（任意）直前の最大フラグメントをイネーブルにします。
specify-max-partial-dgrams	（任意）最大部分データグラムをイネーブルにします。
specify-max-small-fragss	（任意）最大スモール フラグメントをイネーブルにします。
specify-min-fragment-size	（任意）最小フラグメント サイズをイネーブルにします。
specify-service-ports	（任意）サービス ポートをイネーブルにします。
specify-syn-flood-max-embryonic	（任意）SYN フラッドの最大初期接続をイネーブルにします。
specify-tcp-closed-timeout	（任意）TCP クローズド タイムアウトをイネーブルにします。
specify-tcp-embryonic-timeout	（任意）TCP 初期接続タイムアウトをイネーブルにします。
specify-tcp-idle-timeout	（任意）TCP アイドル タイムアウトをイネーブルにします。
specify-tcp-max-mss	（任意）TCP 最大 mss（最大セグメント サイズ）をイネーブルにします。
specify-tcp-max-queue	（任意）TCP 最大キューをイネーブルにします。
specify-tcp-min-mss	（任意）TCP 最小 mss をイネーブルにします。
specify-tcp-option-number	（任意）TCP オプション番号をイネーブルにします。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service エンジン

ここでは、Service エンジンについて説明します。次のような構成になっています。

- 「Service エンジンの概要」（P.B-36）
- 「Service DNS エンジン」（P.B-36）
- 「Service FTP エンジン」（P.B-38）
- 「Service Generic エンジン」（P.B-38）
- 「Service H225 エンジン」（P.B-40）
- 「Service HTTP エンジン」（P.B-42）
- 「Service IDENT エンジン」（P.B-44）
- 「Service MSRPC エンジン」（P.B-45）
- 「Service MSSQL エンジン」（P.B-46）
- 「Service NTP エンジン」（P.B-47）
- 「Service P2P エンジン」（P.B-47）
- 「Service RPC エンジン」（P.B-48）
- 「Service SMB Advanced エンジン」（P.B-49）
- 「Service SNMP エンジン」（P.B-51）
- 「Service SSH エンジン」（P.B-52）
- 「Service TNS エンジン」（P.B-53）

Service エンジンの概要

Service エンジンは、2 つのホスト間のレイヤ 5+ トラフィックを分析します。これらは、固定データを追跡する 1 対 1 シグニチャです。エンジンは、ライブ サービスに似た方法でレイヤ 5+ ペイロードを分析します。

Service エンジンには共通した特性がありますが、個々のエンジンには、検査対象のサービスに関する固有の情報が保持されます。文字列エンジンの使用が不適切または望ましくない場合には、Service エンジンによって、アルゴリズムに特化した汎用文字列エンジンの機能が補完されます。

Service DNS エンジン

表 B-16 に、Service DNS エンジンに固有のパラメータを示します。

表 B-16　Service DNS エンジンのパラメータ

パラメータ	説明	値
protocol	このインスペクタの該当プロトコル。	tcp udp
specify-query-chaos-string	（任意）DNS クエリー クラスのカオス文字列をイネーブルにします。	*query-chaos-string*

表 B-16　Service DNS エンジンのパラメータ （続き）

パラメータ	説明	値
specify-query-class	（任意）クエリー クラスをイネーブルにします。 • query-class：DNS クエリー クラスの 2 バイト値	0 ～ 65535
specify-query-invalid-domain-name	（任意）無効なドメイン名のクエリーをイネーブルにします。 • query-invalid-domain-name：255 を超える DNS クエリーの長さ	[true] | [false]
specify-query-jump-count-exceeded	（任意）しきい値を超えたジャンプ カウントのクエリーをイネーブルにします。 • query-jump-count-exceeded：DNS 圧縮カウンタ	[true] | [false]
specify-query-opcode	（任意）クエリー命令コードをイネーブルにします。 • query-opcode：DNS クエリー命令コードの 1 バイト値	0 ～ 65535
specify-query-record-data-invalid	（任意）無効なレコード データのクエリーをイネーブルにします。 • query-record-data-invalid：不完全な DNS レコード データ	[true] | [false]
specify-query-record-data-len	（任意）クエリー レコード データ長をイネーブルにします。 • query-record-data-len：DNS 応答レコードのデータ長	0 ～ 65535
specify-query-src-port-53	（任意）クエリー送信元ポート 53 をイネーブルにします。 • query-src-port-53：DNS パケット送信元ポート 53	[true] | [false]
specify-query-stream-len	（任意）クエリー ストリーム長をイネーブルにします。 • query-stream-len：DNS パケット長	0 ～ 65535
specify-query-type	（任意）クエリー タイプをイネーブルにします。 • query-type：DNS クエリー タイプの 2 バイト値	0 ～ 65535
specify-query-value	（任意）クエリー値をイネーブルにします。 • query-value：クエリー 0 応答 1	[true] | [false]

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service FTP エンジン

Service FTP エンジンは、FTP ポートのコマンド デコード専用です。無効な **port** コマンドや PASV ポート スプーフィングをトラップします。これは、String エンジンが検出に適さない場合のギャップを埋めます。パラメータはブール値であり、**port** コマンドのデコードにおけるさまざまなエラー トラップ条件にマッピングされます。Service FTP エンジンは、TCP ポート 20 および 21 で稼動します。ポート 20 はデータ用であり、Service FTP エンジンはこのポートに対する検査を行いません。Service FTP エンジンは、ポート 21 の制御トランザクションを検査します。

表 B-17 に、Service FTP エンジンに固有のパラメータを示します。

表 B-17　Service FTP エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
ftp-inspection-type	実行する検査のタイプ： • FTP ポート コマンド内の無効なアドレスを検索します。 • FTP ポート コマンド内の無効なポートを検索します。 • PASV ポート スプーフィングを検索します。	bad-port-cmd-address bad-port-cmd-port pasvI
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service Generic エンジン

Service Generic エンジンを使用すると、コンフィギュレーション ファイルでシグニチャを更新するだけで、プログラム シグニチャを発行できます。このエンジンには、コンフィギュレーション ファイルで定義されている簡易マシンおよびアセンブリ言語が含まれています。このエンジンは、仮想マシンを介して（アセンブリ言語から導出された）マシン コードを実行します。仮想マシンは、命令を処理し、パケットから重要な情報を引き出して、マシン コードに指定されている比較および演算を実行します。このエンジンは、String エンジンと State エンジンを補足する迅速なシグニチャ応答エンジンとして設計されています。

新しい機能は、正規表現パラメータを Service Generic エンジンと拡張命令に追加します。Service Generic エンジンは、パケットを解析するために作成されたミニプログラムに基づいてトラフィックを分析できます。これらのミニプログラムは、パケットを分析し、特定の条件を検索するコマンドで構成されます。

（注）　カスタム シグニチャを作成するために、Service Generic エンジンを使用することはできません。

注意　この複雑な言語に特有の性質上、重大度およびイベント アクション以外に Service Generic エンジンのシグニチャ パラメータを編集することは推奨しません。

表 B-18 に、Service Generic エンジンに固有のパラメータを示します。

表 B-18　Service Generic エンジンのパラメータ

パラメータ	説明	値
specify-dst-port	（任意）宛先ポートをイネーブルにします。 • dst-port：このシグニチャの該当宛先ポート。	0 ～ 65535
specify-ip-protocol	（任意）IP プロトコルをイネーブルにします。 • ip-protocol：このインスペクタが検査する IP プロトコル。	0 ～ 255
specify-payload-source	（任意）ペイロード送信元検査をイネーブルにします。 • payload-source：次のタイプのペイロード送信元検査。 – ICMP データの検査 – レイヤ 2 ヘッダーの検査 – レイヤ 3 ヘッダーの検査 – レイヤ 4 ヘッダーの検査 – TCP データの検査 – UDP データの検査	icmp-data l2-header l3-header l4-header tcp-data udp-dataI
specify-src-port	（任意）送信元ポートをイネーブルにします。 • src-port：このシグニチャの該当送信元ポート。	0 ～ 65535
specify-regex-string	ポリシー タイプが regex の場合に検索する正規表現。 • 単独の TCP パケット内での検索に使用する正規表現。 • （任意）使用する最小一致長をイネーブルにします。 一致と見なされるために必要な正規表現の最小一致長です。	regex-string specify-min -match-leng th
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service H225 エンジン

Service H225 エンジンは、H225.0 プロトコルを分析します。このプロトコルは、多数のサブプロトコルで構成され、H.323 スイートの一部です。H.323 は、パケットベースのネットワーク上での会議開催を実現するために連携して動作する、複数のプロトコルとその他の標準の集まりです。

H.225.0 コール シグナリングおよびステータス メッセージは、H.323 コール セットアップの一部です。ゲートキーパーやエンドポイント端末など、ネットワーク内のさまざまな H.323 エンティティが、H.225.0 プロトコル スタックの実装を実行します。Service H225 エンジンは、H.225.0 プロトコルを分析して、複数の H.323 ゲートキーパー、VoIP ゲートウェイ、およびエンドポイント端末に対する攻撃を検出します。また、TCP PDU を介して交換されるコール シグナリング メッセージについて、ディープ パケット インスペクションを提供します。さらに、Service H225 エンジンは、H.225.0 プロトコルを分析することで無効な H.255.0 メッセージ、およびこれらのメッセージのさまざまなプロトコル フィールドの悪用やそれらに対するオーバーフロー攻撃を検出します。

H.225.0 コール シグナリング メッセージは、Q.931 プロトコルに基づいています。発信側エンドポイントは、Q.931 SETUP メッセージを着信側となるエンドポイントに送信します。着信側エンドポイントのアドレスは、許可手順またはいくつかのルックアップ手法を通じて取得します。着信側のエンドポイントは、Q.931 CONNECT メッセージを送信して接続を受け入れるか、または接続を拒否します。H.225.0 接続が確立されると、発信側エンドポイントまたは着信側エンドポイントのどちらかが H.245 アドレスを提供します。このアドレスを使用して、制御プロトコル（H.245）チャネルが確立されます。

SETUP コール シグナリング メッセージは、コール セットアップの一部として H.323 エンティティ間で交換される最初のメッセージであるため、特に重要です。SETUP メッセージはコール シグナリング メッセージでよく見られるフィールドの多くを使用しており、攻撃に晒される可能性のある実装ではほとんど SETUP メッセージのセキュリティ チェックに失敗します。そのため、H.225.0 SETUP メッセージの妥当性を確認し、ネットワーク境界に対してもチェックを実施することが非常に重要となります。

Service H225 エンジンには、H225 SETUP メッセージの TPKT 検証、Q.931 プロトコル検証、および ASN.1PER 検証を実行するためのシグニチャが組み込まれています。ASN.1 は、データ構造を記述するための表記です。PER は、異なる形式の符号化を使用します。PER は、データ タイプに基づいて符号化し、よりコンパクトな表現を生成することに特化しています。

Q.931 および TPKT 長さシグニチャを調整し、より細分化されたシグニチャを特定の H.225 プロトコル フィールドに追加および適用し、Q.931 または H.225 プロトコルの単一のフィールドに複数のパターン検索シグニチャを適用できます。

Service H225 エンジンは、次の機能をサポートします。

- TPKT 検証および長さチェック
- Q.931 情報要素の検証
- Q.931 情報要素内のテキスト フィールドの正規表現シグニチャ
- Q.931 情報要素の長さチェック
- SETUP メッセージの検証
- ASN.1 PER 符号化エラー チェック
- ULR-ID、E-mail-ID、h323-id などのフィールドの正規表現と長さの両方に対応する設定シグニチャ

TPKT および SAN.1 シグニチャの数は決まっています。これらのタイプのカスタム シグニチャは作成できません。TPKT シグニチャの場合は、長さシグニチャの値範囲だけを変更する必要があります。ASN.1 の場合、パラメータは変更しないでください。Q.931 シグニチャについては、テキスト フィールドの新規の正規表現シグニチャを追加できます。SETUP シグニチャについては、各種の SETUP メッセージ フィールドの長さおよび正規表現を確認するためのシグニチャを追加できます。

表 B-19 に、Service H225 エンジンに固有のパラメータを示します。

表 B-19　Service H.225 エンジンのパラメータ

パラメータ	説明	値
message-type	シグニチャを適用する H225 メッセージのタイプ。 • SETUP • ASN.1-PER • Q.931 • TPKT	asn.1-per q.931 setup tpkt
policy-type	シグニチャを適用する H225 ポリシーのタイプ: • フィールド長を検査する。 • 存在を検査する。 特定のフィールドがメッセージ内に存在する場合は、アラートが送信されます。 • 正規表現を検査する。 • フィールドの妥当性を検査する。 • 値を検査する。 TPKT シグニチャの場合、[regex] と [presence] は有効な値ではありません。	length presence regex validate value
specify-field-name	（任意）使用するフィールド名をイネーブルにします。SETUP および Q.931 メッセージ タイプにのみ有効です。このシグニチャを適用するフィールド名のドット付き表記を指定します。 • field-name：検査するフィールドの名前。	1 ～ 512
specify-invalid-packet-index	（任意）ASN と TPKT 固有のエラー、および固定マッピングを持つその他のエラーで使用する無効なパケット インデックスをイネーブルにします。 • invalid-packet-index：無効なパケット インデックスを検査します。	0 ～ 255
specify-regex-string	ポリシー タイプが [regex] の場合に検索する正規表現。TPKT シグニチャには設定しないでください。 • 単独の TCP パケット内での検索に使用する正規表現。 • （任意）使用する最小一致長をイネーブルにします。 一致と見なされるために必要な正規表現の最小一致長です。TPKT シグニチャには設定しないでください。	regex-string specify-min-match-length

表 B-19　Service H.225 エンジンのパラメータ （続き）

パラメータ	説明	値
specify-value-range	長さまたは値ポリシー タイプに有効です（0x00 ～ 6535）。その他のポリシー タイプの場合は無効です。 • value-range：値の範囲。	0 ～ 65535[1] a-b
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service HTTP エンジン

Service HTTP エンジンは、サービスに特化した文字列ベースのパターンマッチング検査エンジンです。HTTP プロトコルは、今日のネットワークで最も一般的に使用されるプロトコルの 1 つです。また、必要な前処理の時間が非常に長く、検査を必要とするシグニチャも非常に多いため、システムの全体的なパフォーマンスを決める要因になっています。

Service HTTP エンジンでは、複数のパターンを 1 つのパターンマッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現ライブラリが使用されます。このエンジンは、Web サービスに向かう方向のみのトラフィック、または HTTP 要求を検索します。このエンジンでリターン トラフィックを検査することはできません。このエンジンでは、シグニチャごとに対象の Web ポートを別々に指定できます。

HTTP 解読とは、符号化された文字を ASCII 対応文字に正規化することによって、HTTP メッセージをデコードするプロセスです。このプロセスは、ASCII 正規化と呼ばれることもあります。

HTTP パケットを検査するには、あらかじめそのデータを、ターゲット システムでのデータ処理時に表示されるものと同じデータ表現として解読または正規化しておく必要があります。また、ホスト ターゲット タイプごとにカスタマイズされたデコード方式を用意することが推奨されます。そのためには、ターゲット上で動作しているオペレーティング システムおよび Web サーバのバージョンを確認する必要があります。Service HTTP エンジンのデフォルトの解読動作は Microsoft IIS Web サーバを対象としています。

表 B-20 に、Service HTTP エンジンに固有のパラメータを示します。

表 B-20　Service HTTP エンジンのパラメータ

パラメータ	説明	値
de-obfuscate	検索の前に反回避解読を適用します。	[true] | [false]
max-field-sizes	最大フィールド サイズ グループ。	—

表 B-20　Service HTTP エンジンのパラメータ （続き）

パラメータ	説明	値
specify-max-arg-field-length	（任意）引数フィールドの最大長をイネーブルにします。 • max-arg-field-length：引数フィールドの最大長。	0 ～ 65535
specify-max-header-field-length	（任意）ヘッダー フィールドの最大長をイネーブルにします。 • max-header-field-length：ヘッダー フィールドの最大長。	0 ～ 65535
specify-max-request-length	（任意）要求フィールドの最大長をイネーブルにします。 • max-request-length : 要求フィールドの最大長。	0 ～ 65535
specify-max-uri-field-length	（任意）URI フィールドの最大長をイネーブルにします。 • max-uri-field-length：URI フィールドの最大長。	0 ～ 65535
regex	正規表現グループ。	—
specify-arg-name-regex	（任意）特定の正規表現の引数フィールドの検索をイネーブルにします。 • arg-name-regex：HTTP 引数フィールド（コンテンツ長で定義されているとおりのエンティティ本体の中で、? の後ろ）で検索する正規表現。	—
specify-header-regex	（任意）特定の正規表現のヘッダー フィールドの検索をイネーブルにします。 • header-regexHTTP ヘッダー フィールドで検索する正規表現。 ヘッダーは、最初の CRLF の後ろから定義され、CRLFCRLF まで続きます。	—
specify-request-regex	（任意）特定の正規表現の要求フィールドの検索をイネーブルにします。 • request-regexHTTP URI フィールドと HTTP 引数フィールドの両方で検索する正規表現。 • specify-min-request-match-length：要求の最小一致長の設定をイネーブルにします。	0 ～ 65535
specify-uri-regex	（任意）HTTP URI フィールドで検索する正規表現。URI フィールドは、HTTP メソッド（たとえば、GET）の後ろで、最初の CRLF の前まで定義されます。正規表現は保護されています。つまり、値は変更できません。	[/\\][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][.]jpeg

表 B-20　Service HTTP エンジンのパラメータ （続き）

パラメータ	説明	値
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- Service HTTP カスタム シグニチャの例については、「Service HTTP エンジン シグニチャの例」（P.7-46）を参照してください。
- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service IDENT エンジン

Service IDENT エンジンは、TCP ポート 113 のトラフィックを検査します。基本デコードと、長さのオーバーフローを指定するパラメータが用意されています。たとえば、コンピュータ A のユーザまたはプログラムからコンピュータ B の ident 要求が実行された場合は、A と B 間の接続のユーザ ID のみが求められている可能性があります。B の ident サーバは、TCP ポート 113 の接続を受信します。A のクライアントは接続を確立し、その接続で使用している A と B のポートの番号を送信して、ID が必要な接続を指定します。B のサーバは、その接続を使用しているユーザを判断し、そのユーザの名前を示す文字列を A に返します。Service IDENT エンジンは、TCP ポート 113 での ident の不正利用を検査します。

表 B-21 に、Service IDENT エンジンに固有のパラメータを示します。

表 B-21　Service IDENT エンジンのパラメータ

パラメータ	説明	値
inspection-type	実行する検査のタイプ： • has-newline：ペイロードで非終端改行文字を検査します。 • has-bad-port：ペイロードで不良ポートを検査します。 • size：これよりも長いペイロード長を検査します。	—
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
direction	トラフィックの方向： • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service MSRPC エンジン

Service MSRPC エンジンは、MSRPC パケットを検査します。MSRPC によって、ネットワーク環境内の複数のコンピュータとそれらのアプリケーション ソフトウェアとの間の連携処理が可能になります。これは、トランザクションベースのプロトコルです。つまり、チャネルを確立し、処理要求と応答を渡す一連の通信が行われます。

MSRPC は、ISO レイヤ 5 ～ 6 プロトコルで、UDP、TCP、および SMB などのその他のトランスポート プロトコルの上層にあたります。MSRPC エンジンには、MSRPC PDU のフラグメンテーションと再構成を可能にする機能が組み込まれています。

この通信チャネルが、最近の Windows NT、Windows 2000、および Window XP セキュリティの脆弱性の原因です。Service MSRPC エンジンは、最も一般的なトランザクション タイプに対応する DCE および RPC プロトコルだけをデコードします。

表 B-22 に、Service MSRPC エンジンに固有のパラメータを示します。

表 B-22　Service MSRPC エンジンのパラメータ

パラメータ	説明	値
protocol	このインスペクタの該当プロトコル。 • type：UDP または TCP	tcp udp
specify-flags	設定するフラグ。 • msrpc-flags • msrpc-tcp-flags-mask	concurrent-execution did-not-execute first-fragment last-fragment maybe-semantics object-uuid reserved
specify-operation	（任意）MSRPC 動作の使用をイネーブルにします。 • operation：要求する MSRPC 動作。 SMB_COM_TRANSACTION コマンドに必要です。完全一致。	0 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

表 B-22　Service MSRPC エンジンのパラメータ （続き）

パラメータ	説明	値
specify-regex-string	（任意）正規表現文字列の使用をイネーブルにします。 • specify-exact-match-offset：完全一致オフセットをイネーブルにします。 – exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。 • specify-min-match-length：最小一致長をイネーブルにします。 – min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
specify-uuid	（任意）UUID をイネーブルにします。 • uuid：MSRPC UUID フィールド。	000001a000000000c000000000000046

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service MSSQL エンジン

Service MSSQL エンジンは、Microsoft SQL サーバによって使用されるプロトコルを検査します。このエンジンには 1 つの MSSQL シグニチャが含まれています。このエンジンは、デフォルトの sa アカウントを使用した MSSQL サーバへのログイン試行を検出すると、アラートを起動します。ログイン ユーザ名や、パスワードが使用されたかどうかなど、MSSQL プロトコル値に基づいてカスタム シグニチャを追加できます。

表 B-23 に、Service MSSQL エンジンに固有のパラメータを示します。

表 B-23　Service MSSQL エンジンのパラメータ

パラメータ	説明	値
password-present	MS SQL ログインでパスワードが使用されたかどうか。	[true] | [false]
specify-sql-username	（任意）SQL ユーザ名の使用をイネーブルにします。 • sql-username：MS SQL サービスにログインするユーザのユーザ名（完全一致）。	sa

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service NTP エンジン

Service NTP エンジンは、NTP プロトコルを検査します。このエンジンには、1 つの NTP シグニチャ（NTP readvar オーバーフロー シグニチャ）が含まれます。このシグニチャは、サイズが大きいため NTP サービスでキャプチャできない NTP データが、readvar コマンドに指定されていることを検出した場合に、アラートを起動します。NTP プロトコルの値（モードや制御パケットのサイズなど）に基づいて、シグニチャを調整したり、カスタム シグニチャを作成したりできます。

表 B-24 に、Service NTP エンジンに固有のパラメータを示します。

表 B-24　Service NTP エンジンのパラメータ

パラメータ	説明	値
inspection-type	実行する検査のタイプ。	
inspect-ntp-packets	NTP パケットを検査します。 • control-opcode：RFC1305 の付録 B に基づく NTP 制御パケットの命令コード番号。 • max-control-data-size：制御パケットで送信されるデータの最大許容量。 • mode：RFC 1305 に基づく NTP パケットの動作モード。	0 ～ 65535
is-invalid-data-packet	無効な NTP データ パケットを検索します。NTP データ パケットの構造を調べ、サイズが正しいことを確認します。	[true] | [false]
is-non-ntp-traffic	NTP ポートの非 NTP パケットをチェックします。	[true] | [false]

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service P2P エンジン

P2P ネットワークでは、ファイル共有のためにクライアントとサーバの両方として同時に機能できるノードを使用します。P2P ネットワークには著作物が含まれていることが多く、企業ネットワークでそれらを使用することは会社のポリシーに違反する可能性があります。Service P2P エンジンはそのようなネットワークをモニタし、最適化された TCP および UDP P2P プロトコル ID を提供します。Service P2P エンジンには、次の特性があります。

- すべての TCP ポートおよび UDP ポートで受信します。
- 正規表現ではなく、ハードコード化されたシグニチャの使用によってパフォーマンスを向上します。
- P2P プロトコルが識別されるか、P2P プロトコルは識別されずに 10 パケットを確認した後、トラフィックを無視します。

P2P シグニチャはハード コード化されているので、編集できるパラメータは Master エンジンのパラメータのみになります。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service RPC エンジン

Service RPC エンジンは、RPC プロトコルに特化しており、反回避の方式として完全なデコードが行われます。これにより、フラグメント化されたメッセージ（複数パケット内の 1 つのメッセージ）およびバッチ メッセージ（1 つのパケット内の複数メッセージ）を処理できます。

RPC ポートマッパーは、ポート 111 上で動作します。通常の RPC メッセージは、550 より上位であれば任意のポートで送受信できます。RPC スイープは、TCP ポート スイープとほぼ同じものです。異なるのは、有効な RPC メッセージが送信された場合に一意のポートだけをカウントするという点です。RPC は、UDP 上でも実行されます。

表 B-25 に、Service RPC エンジンに固有のパラメータを示します。

表 B-25　Service RPC エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
protocol	該当プロトコル。	tcp udp
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
specify-regex-string	（任意）正規表現文字列の使用をイネーブルにします。 • specify-exact-match-offset：完全一致オフセットをイネーブルにします。 – exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。 • specify-min-match-length：最小一致長をイネーブルにします。 – min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
specify-is-spoof-src	（任意）スプーフィングの送信元アドレスをイネーブルにします。 • is-spoof-src：送信元アドレスが 127.0.0.1 の場合にアラートを起動します。	[true] | [false]
specify-port-map-program	（任意）ポートマッパー プログラムをイネーブルにします。 • port-map-program：このシグニチャのポートマッパーに送信されたプログラム番号。	0 ～ 9999999999
specify-rpc-max-length	（任意）RPC 最大長をイネーブルにします。 • rpc-max-length：RPC メッセージ全体の最大許容長。長さが指定した値より長いとアラートを起動します。	0 ～ 65535

表 B-25　Service RPC エンジンのパラメータ （続き）

パラメータ	説明	値
specify-rpc-procedure	（任意）RPC プロシージャをイネーブルにします。 • rpc-procedure：このシグニチャの RPC プロシージャ番号。	0 ～ 1000000
specify-rpc-program	（任意）RPC プログラムをイネーブルにします。 • rpc-program：このシグニチャの RPC プログラム番号。	0 ～ 1000000
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service SMB Advanced エンジン

（注）　SMB エンジンは、SMB Advanced エンジンに置き換えられました。SMB エンジンがまだ IDM、IME、および CLI に表示される場合でも、このシグニチャは廃止されています。つまり、新規のシグニチャには、対応する古いシグニチャの ID を持つ obsoletes パラメータ セットがあります。新規の SMB Advanced エンジンを使用して、SMB エンジンにあったカスタム シグニチャを書き換えてください。

Service SMB Advanced エンジンは、SMB パケットを介して Microsoft SMB および Microsoft RPC を処理します。Service SMB Advanced エンジンは、コネクション型 MSRPC に同じデコード メソッドを使用します。これは、MSRPC エンジンに、MSRPC パケットは SMB プロトコルを経由する必要があるという要件があるためです。Service SMB Advanced エンジンは、TCP ポート 139 および 445 での SMB を経由した MSRPC をサポートしています。また、MSRPC エンジンからのコネクション型 DCS/RPC コードのコピーを使用します。

表 B-26 に、Service SMB Advanced エンジンに固有のパラメータを示します。

表 B-26　Service SMB Advanced エンジンのパラメータ

パラメータ	説明	値
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535 a-b[,c-d] [1]
specify-command	（任意）SMB コマンドをイネーブルにします。 • command：SMB コマンドの値。完全に一致する必要があります。SMB パケットのタイプを定義します。[2]	0 ～ 255

表 B-26　Service SMB Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-direction	（任意）トラフィック方向をイネーブルにします。 • direction：トラフィックの方向を指定できます。 – from-service：サービス ポートからクライアント ポート宛のトラフィック。 – to-service：クライアント ポートからサービス ポート宛のトラフィック。	from service to service
specify-operation	（任意）MSRPC over SMB をイネーブルにします。 • msrpc-over-smb-operation：SMB_COM_TRANSACTION コマンドに使用します。完全に一致する必要があります。	0 ～ 65535
specify-regex-string	（任意）正規表現文字列の検索をイネーブルにします。 • regex-string：単一の TCP パケット内で検索する正規表現。	
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：正規表現文字列が一致する必要がある最小バイト数。	
specify-payload-source	（任意）ペイロード送信元をイネーブルにします。 • payload-source：ペイロード送信元の検査。[3]	
specify-scan-interval	（任意）スキャン間隔をイネーブルにします。 • scan-interval：アラート率の計算に使用される間隔（秒単位）。	1 ～ 131071
specify-tcp-flags	（任意）TCP フラグをイネーブルにします。 • msrpc-tcp-flags • msrpc-tcp-flags-mask	• concurrent execution • did not execute • first fragment • last fragment • maybe • object UUID • pending cancel • reserved

表 B-26　Service SMB Advanced エンジンのパラメータ （続き）

パラメータ	説明	値
specify-type	（任意）MSRPC over SMB パケットのタイプをイネーブルにします。 • type：SMB パケットを介した MSRPC の Type フィールド。	• [0] = 要求 • [2] = 応答 • [11] = バインド • [12] = バインド応答
specify-uuid	（任意）UUID を経由した MSRPC をイネーブルにします。 • uuid：MSRPC UUID フィールド。	16 進数の 0 ～ 9、a ～ f、A ～ F で構成される 32 文字の文字列。
specify-hit-count	（任意）ヒット カウントをイネーブルにします。 • hit-count：scan-interval 内の発生回数のしきい値。この値を超えるとアラートが起動されます。	1 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	[true] | [false]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. 現在、37 (0x25) SMB_COM_TRANSACTION コマンド \x26amp および 162 (0xA2) SMB COM NT CREATE ANDX コマンドをサポートしています。
3. TCP_Data は、パケット全体に対して正規表現を実行します。SMB_Data は、SMB ペイロードでのみ正規表現を実行します。Resource_DATA は、SMB_Resource に対して正規表現を実行します。

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service SNMP エンジン

Service SNMP エンジンは、ポート 161 宛のすべての SNMP パケットを検査します。特定のコミュニティ名とオブジェクト ID に基づいて、SNMP シグニチャを調整したり、カスタム SNMP シグニチャを作成したりできます。

コミュニティ名とオブジェクト ID を照合するために、文字列比較や正規表現演算を使用する代わりに、整数を使用してすべての比較を実行し、プロトコル デコードを高速化しストレージ要件を削減します。

表 B-27 に、Service SNMP エンジンに固有のパラメータを示します。

表 B-27　Service SNMP エンジンのパラメータ

パラメータ	説明	値
inspection-typeI	実行する検査のタイプ。	—
brute-force-inspection	総当たり攻撃の試行を検査します。 • brute-force-count：総当たり攻撃と見なされる一意の SNMP コミュニティ名の数。	0 ～ 65535
invalid-packet-inspection	SNMP プロトコル違反を検査します。	—
non-snmp-traffic-inspection	UDP ポート 161 宛の非 SNMP トラフィックを検査します。	—
snmp-inspection	SNMP トラフィックを検査します。 • specify-community-name [yes | no] – community-name：SNMP コミュニティ名（SNMP パスワード）を検索します。 • specify-object-id [yes | no] – object-id：SNMP オブジェクト ID を検索します。	*community-name* *object-id*

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service SSH エンジン

Service SSH エンジンは、ポート 22 の SSH トラフィックに対して使用します。SSH セッションのセットアップを除いてすべてが暗号化されるため、Service SSH エンジンはセットアップのフィールドだけをモニタします。SSH には 2 つのデフォルト シグニチャがあります。これらのシグニチャを調整することはできますが、カスタム シグニチャは作成できません。

表 B-28 に、Service SSH エンジンに固有のパラメータを示します。

表 B-28　Service SSH エンジンのパラメータ

パラメータ	説明	値
length-type	次の SSH 長さタイプのいずれかを検査します。 • key-length：検査対象の SSH キーの長さ。 – length：キーがこれよりも長い場合は、RSAREF オーバーフローが発生します。 • user-length：ユーザ長の SSH 検査。 – length：キーがこれよりも長い場合は、RSAREF オーバーフローが発生します。	0 ～ 65535

表 B-28　Service SSH エンジンのパラメータ （続き）

パラメータ	説明	値
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
specify-packet-depth	（任意）パケット数をイネーブルにします。 • packet-depth：セッション キーが失われたと判断するまでにモニタするパケット数。	0 ～ 65535

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service TNS エンジン

Service TNS エンジンは、TNS プロトコルを検査します。TNS は、業界標準のすべてのネットワーク プロトコルに単一の共通インターフェイスを備えたデータベース アプリケーションを提供します。TNS を使用すると、アプリケーションは異なるプロトコルを使用しているネットワークを経由して他のデータベース アプリケーションに接続することができます。デフォルトの TNS 受信ポートは TCP 1521 です。TNS は、クライアントを別のホストまたは他の TCP ポート（またはその両方）にリダイレクトする REDIRECT フレームもサポートしています。REDIRECT パケットをサポートするため、TNS エンジンはすべての TCP ポートで受信します。また、TNS 以外のストリームを無視するための簡単な TNS フレーム ヘッダー検証ルーチンを備えています。

表 B-29 に、Service TNS エンジンに固有のパラメータを示します。

表 B-29　Service TNS エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
type	TNS フレーム値のタイプを指定します。 • [1]：接続 • [2]：受け入れ • [4]：拒否 • [5]：リダイレクト • [6]：データ • [11]：再送信 • [12]：マーカー	1 2 4 5 6 11 12

表 B-29　Service TNS エンジンのパラメータ （続き）

パラメータ	説明	値
specify-regex-string	（任意）正規表現文字列の使用をイネーブルにします。 • specify-exact-match-offset：完全一致オフセットをイネーブルにします。 – exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。 • specify-min-match-length：最小一致長をイネーブルにします。 – min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
specify-regex-payload-src	検査するプロトコルを指定します。 • payload-src： – tcp-data：TCP パケットのデータ部分に対して正規表現を実行します。 – tns-data：すべての空白が削除されている TNS データに対してだけ正規表現を実行します。	tcp tns

詳細情報

- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

State エンジン

State エンジンは、TCP ストリームに対して状態ベースで、正規表現ベースのパターン検査を行います。State エンジンとは、何らかの状態を保存するデバイスで、特定の時に入力に基づいて 1 つの状態から別の状態に移行したり、処理または出力を発生させたりすることができます。ステート マシンは、出力やアラートの原因となる特定のイベントを記述するために使用します。State エンジンには、SMTP、Cisco Login、および LPR Format String の 3 つのステート マシンがあります。

表 B-30 に、State エンジンに固有のパラメータを示します。

表 B-30　State エンジンのパラメータ

パラメータ	説明	値
state-machine	ステート マシン グループ。	• smpt • lpr-format-string • cisco-login
cisco-login	Cisco ログインのステート マシンを指定します。 • state-name：状態の名前。この状態になると、シグニチャはアラートを起動します。 – シスコ デバイスの状態 – Control-C 状態 – パスワード プロンプト状態 – 開始状態	• cisco-device • control-c • pass-prompt • start
lpr-format-string	LPR フォーマット ストリングの脆弱性を検査するステート マシンを指定します。 • state-name：状態の名前。この状態になると、シグニチャはアラートを起動します。 – LPR フォーマット ストリング検査を終了する中断状態 – フォーマット文字の状態 – 開始状態	• abort • format-char • start
state-name	SMTP プロトコルのステート マシンを指定します。 • state-name：状態の名前。この状態になると、シグニチャはアラートを起動します。 – LPR フォーマット ストリング検査を終了する中断状態 – メール本文の状態 – メール ヘッダーの状態 – SMTP コマンドの状態 – 開始状態	• abort • mail-body • mail-header • smtp-commands • start
direction	トラフィックの方向： • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]

表 B-30　State エンジンのパラメータ （続き）

パラメータ	説明	値
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
specify-max-match-offset	（任意）最大一致オフセットをイネーブルにします。 • max-match-offset：一致を有効にするために正規表現文字列が報告する必要がある最大ストリーム オフセット。	0 ～ 65535
specify-min-match-offset	（任意）最小一致オフセットをイネーブルにします。 • min-match-offset：一致を有効にするために正規表現文字列が報告する必要がある最小ストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

String エンジン

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用のパターンマッチング検査エンジンです。String エンジンでは、複数のパターンを 1 つのパターンマッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。String エンジンには、String ICMP、String TCP、および String UDP の 3 種類が存在します。

表 B-31 に、String ICMP エンジンに固有のパラメータを示します。

表 B-31　String ICMP エンジンのパラメータ

パラメータ	説明	値
direction	トラフィックの方向： • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
icmp-type	ICMP ヘッダーの TYPE 値。	0 ～ 18[1] a-b[,c-d]
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-32 に、String TCP エンジンに固有のパラメータを示します。

表 B-32　String TCP エンジン

パラメータ	説明	値
direction	トラフィックの方向： • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535

表 B-32　String TCP エンジン （続き）

パラメータ	説明	値
strip-telnet-options	パターンを検索する前に、データから Telnet オプション文字を削除します。[2]	[true] | [false]
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. このパラメータは、主に、IPS 反回避ツールとして使用します。

表 B-33 に、String UDP エンジンに固有のパラメータを示します。

表 B-33　String UDP エンジン

パラメータ	説明	値
direction	トラフィックの方向： • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
service-ports	ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。	0 ～ 65535[1] a-b[,c-d]
specify-exact-match-offset	（任意）完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
specify-min-match-length	（任意）最小一致長をイネーブルにします。 • min-match-length：正規表現文字列が一致する必要がある最小バイト数。	0 ～ 65535
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- カスタム String エンジン シグニチャの例については、「String TCP エンジン シグニチャの例」（P.7-43）を参照してください。
- すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

String XL エンジン

String XL エンジンは、その他の String エンジンと同じことを行います（つまり、1 つのシグニチャあたりに 1 つの文字列のマッチング機能を提供します）が、使用する正規表現構文が異なります。String TCP XL エンジンはストリームベースであり、Cross-Packet Inspection（XPI）を使用します。パケットは、順番に並んでいる必要があります。UDP と ICMP はどちらもステートレスであるので、String UDP XL および String ICMP XL シグニチャ エンジンはセッション ステートを割り当てる必要がなく、各パケットは別個の検索になります。

正規表現アクセラレータ カードは、標準の String エンジンと新規の String XL エンジンの両方に使用されます。ほとんどの標準 String エンジン シグニチャは、変更することなく、正規表現アクセラレータ カードによってコンパイルおよび分析できます。ただし、標準の String エンジン シグニチャを正規表現アクセラレータ カード用にコンパイルできない特別な状況もあります。そのような状況では、正規表現アクセラレータ カードでコンパイルする String XL エンジンの特定のパラメータを使用して、String XL エンジンに新規のシグニチャが作成されます。String XL エンジンの新規シグニチャは、標準の String エンジンにある元のシグニチャに代わるものです。

正規表現構文または raw 表現構文を使用できますが、raw 表現構文はエキスパート ユーザ専用です。String XL シグニチャを設定するときは、raw 表現構文を使用していない限り、regex-string パラメータが必要です。

（注）　raw 正規表現とは、raw モード処理に使用される正規表現の構文です。エキスパート モード専用であり、Cisco IPS シグニチャ開発チーム、あるいはその監視下にある作業者のみによる使用を対象としています。String XL シグニチャは、通常の正規表現と raw 正規表現のいずれでも設定できます。

表 B-34 に、String XL エンジン（TCP、ICMP、および UDP）に固有のパラメータを示します。

表 B-34　String XL エンジンのパラメータ

パラメータ	説明	値
direction	（必須）検査するトラフィックの方向。 • サービス ポートからクライアント ポート宛のトラフィック。 • クライアント ポートからサービス ポート宛のトラフィック。	from-service to-service
dot-all	true に設定すると、\n を含む [\x00-\xFF] と一致し、false に設定すると、\n を除く範囲 [\x00-\xFF] 内のすべてと一致します。	true | false（デフォルト）
end-optional	パケットの最後で、その他すべての条件が満たされても最後が表示されない場合、最小限度を超えていれば一致結果が報告されます。	true | false（デフォルト）
icmp-type	ICMP メッセージ ヘッダーのタイプ。シグニチャ エンジンが string-icmp である場合は必須です。	0 ～ 18[1] a-b[,c-d]
no-case	表現内のすべてのアルファベット文字の大文字と小文字を区別します。	true | false（デフォルト）

表 B-34　String XL エンジンのパラメータ （続き）

パラメータ	説明	値
raw-regex	true に設定すると、min-match-length、max-match-length、min-whole-length、max-whole-length、dot-all、utf8、no-case、stingy、および end-optional は正規表現文字列の再フォーマットに使用されません。 **（注）** raw-regex を使用すると、正規表現文字列を変換せずに raw 構文に入力できます。	true | false（デフォルト）
regex-string	（必須）検索に使用する正規表現パターン。 **（注）** max-stream-length が設定されていない限り、このパラメータは必須です。max-stream-length が設定されている場合は、regex-string を設定しないでください。	string
service-ports	（必須）ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲。 **（注）** このパラメータは、String XL TCP シグニチャ エンジンおよび String XL UDP シグニチャ エンジンに必須です。String XL ICMP シグニチャ エンジンには、使用できません。	0 ～ 65535[2] a-b[,c-d]
specify-exact-match-offset	完全一致オフセットをイネーブルにします。 • exact-match-offset：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット（バイト単位）。	[yes] | [no] 0 ～ 65535
specify-max-match-offset	最大一致オフセットをイネーブルにします。 • maximum-match-offset：一致を有効にするために正規表現文字列が報告する必要がある最大ストリーム オフセット。	yes | no 0 ～ 65535
specify-min-match-offset	最小一致オフセットをイネーブルにします。 • min-match-offset：一致を有効にするために正規表現文字列が報告する必要がある最小ストリーム オフセット（バイト単位）。	yes | no 0 ～ 65535
specify-max-match-length	最大一致長をイネーブルにします。 • max-match-length：パターンがヒットと見なされるために正規表現文字列が一致する必要のある最大バイト数。	yes | no 0 ～ 65535
specify-min-match-length	最小一致長をイネーブルにします。 • min-match-length：パターンがヒットと見なされるために正規表現文字列が一致する必要のある最小バイト数。	yes | no 0 ～ 65535

表 B-34　String XL エンジンのパラメータ （続き）

パラメータ	説明	値
specify-max-stream-length	最大ストリーム長をイネーブルにします。 • max-stream-length：最初に設定されたバイト数に検索を制限します。ストリームの長さが、この値でチェックされます。ストリームのバイト数がこの値よりも多い場合は、アラートがトリガーされます。 （注）　このパラメータを指定すると、raw-regex または regex-string を設定できません。	[yes] | [no] 0 ～ 65535
specify-max-whole-length	最大全長をイネーブルにします。 • max-whole-length：フラグメント化されないパターンの最大長。	[yes] | [no] 0 ～ 65535
specify-min-whole-length	最小全長をイネーブルにします。 • min-whole-length：フラグメント化されないパターンの最小長。	yes | no 0 ～ 65535
stingy	最初に完全に一致した後は、それより大きい一致検索を停止します。 （注）　stingy は、min-match-length を指定した場合のみ使用できます。それ以外では、無視されます。	true | false（デフォルト）
strip-telnet-options	パターンを検索する前に、データから Telnet オプション文字を削除します。[3]	true | false（デフォルト）
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true | false（デフォルト）
utf8	表現内のすべての公正な UTF-8 バイト シーケンスを 1 文字として処理します。	true | false（デフォルト）

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. 範囲の 2 番目の数は、最初の数以上である必要があります。
3. このパラメータは、主に、IPS 反回避ツールとして使用します。

サポートされないパラメータ

end-optional パラメータと specify-max-stream-length パラメータは、String XL エンジンに表示されますが、IPS 7.1(1)E4 では無効です。これらのパラメータを設定しようとすると、エラー メッセージを受け取ります。たとえば、specify-max-stream-length を使用してシグニチャを作成し、保存しようとすると、次のエラー メッセージが表示されます。

```
Apply Changes?[yes]: yes
Error: string-xl-tcp 60003.0 : Maximum Stream Length is currently not supported.
Please don't use this option.

The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]:
```

Sweep エンジン

ここでは、Sweep エンジンについて説明します。次のような構成になっています。

- 「Sweep エンジン」（P.B-62）
- 「Sweep Other TCP エンジン」（P.B-64）

Sweep エンジン

Sweep エンジンは、2 つのホスト間または 1 つのホストから多数のホストへのトラフィックを分析します。既存のシグニチャを調整することも、カスタム シグニチャを作成することもできます。Sweep エンジンには、ICMP、UDP、および TCP 用のプロトコル固有のパラメータがあります。

Sweep エンジンのアラート条件は、根本的に一意のパラメータのカウントに基づいています。一意のパラメータとは、スイープのタイプに応じて明確に特定されたホスト数またはポート数のしきい値です。一意のパラメータは、一定時間内にアドレス セット上で一意の数を超えるポートまたはホストが検出された場合に、アラームをトリガーします。一意のポートおよびホストのトラッキング処理をカウンティングと言います。

注意　送信元 IP アドレスおよび宛先 IP アドレスに基づくイベント アクション フィルタは、正規のシグニチャとしてフィルタリングしないので、Sweep エンジンには機能しません。スイープ アラートで送信元 IP アドレスと宛先 IP アドレスをフィルタリングするには、Sweep エンジン シグニチャで送信元 IP アドレスおよび宛先 IP アドレス フィルタ パラメータを使用します。

Sweep エンジン内のすべてのシグニチャに、一意のパラメータを指定する必要があります。2 ～ 40 の制限がスイープに対して適用されます。2 は、スイープの絶対最小値であり、それに満たない場合は（1 つのホストまたはポートの）スイープではありません。40 は実際の最大値で、スイープが過剰にメモリを消費しないように適用する必要があります。さらに現実的な一意の範囲の値は 5 ～ 15 です。

TCP スイープには、どのスイープ インスペクタ スロットで特定の接続をカウントするかを決定するために、TCP フラグとマスクを指定する必要があります。ICMP スイープには、さまざまなタイプの ICMP パケットを識別するために、ICMP タイプを指定する必要があります。

DataNode

Sweep エンジン シグニチャに関連するアクティビティが検出されると、IPS は DataNode を使用して、特定のホストに対するモニタリングを停止するタイミングを決定します。DataNode には、ストリームのクロスパケット再構成用に、また、ストリーム単位、送信元単位、および宛先単位の検査状態を追跡するために必要とされる、さまざまな固定カウンタおよび変数が含まれます。スイープを含む DataNode は、スイープの期限を決定します。DataNode は、*x* 秒間（プロトコルによる）トラフィックが検出されなかった場合に、スイープを停止します。

DataNode には、いくつかの適応型タイムアウトがあります。DataNode は、包含されるオブジェクトがすべて削除されてから、アドレス セットに対して 30 秒のアイドル時間経過後に期限切れとなります。包含されている各オブジェクトにはさまざまなタイムアウトが設定されています。たとえば、TCP ストリームには確立された接続に対する 1 時間のタイムアウトがあります。その他のほとんどのオブジェクトに設定されている期限は、5 ～ 60 秒など、はるかに短い時間になります。

表 B-35 に、Sweep エンジンに固有のパラメータを示します。

表 B-35　Sweep エンジンのパラメータ

パラメータ	説明	値
dst-addr-filter	スイープ カウント アルゴリズムから除外する宛先 IP アドレス。	<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]
src-addr-filter	スイープ カウント アルゴリズムから除外する送信元 IP アドレス。	<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]
protocol	このインスペクタの該当プロトコル。	• icmp • udp • tcp
specify-icmp-type	(任意) ICMP ヘッダー タイプの検査をイネーブルにします。 • icmp-type：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 255
specify-port-range	(任意) 検査でのポート範囲の使用をイネーブルにします。 • port-range：検査で使用する UDP ポート範囲。	0 ～ 65535 a-b[,c-d]
fragment-status	フラグメントが必要かどうかを指定します。 • 任意のフラグメント ステータス。 • フラグメントを検査しない。 • フラグメントを検査する。	• any • no-fragments • want-fragments
inverted-sweep	一意のカウントの対象として宛先ポートではなく送信元ポートを使用します。	[true] | [false]
mask	TCP フラグの比較に使用するマスク： • URG ビット • ACK ビット • PSH ビット • RST ビット • SYN ビット • FIN ビット	• urg • ack • psh • rst • syn • fin
storage-key	固定データを保存するために使用するアドレス キーのタイプ。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃者のアドレスと攻撃対象のポート	Axxx AxBx Axxb
suppress-reverse	このアドレス セットで反対方向にスイープが実行されている場合、アラートを起動しません。	true| false
swap-attacker-victim	アラート メッセージおよびアクションで攻撃者および攻撃対象のアドレスとポート（送信元および宛先）がスワップする場合は、true。スワップしない場合は false（デフォルト）。	true| false

表 B-35　Sweep エンジンのパラメータ （続き）

パラメータ	説明	値
tcp-flags	マスクによってマスクされた場合に照合する TCP フラグ。 • URG ビット • ACK ビット • PSH ビット • RST ビット • SYN ビット • FIN ビット	• urg • ack • psh • rst • syn • fin
unique	2 つのホスト間の一意のポート接続数のしきい値。	0 ～ 65535

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Sweep Other TCP エンジン

Sweep Other TCP エンジンは、2 つのホスト間のトラフィックを分析して、一般に攻撃対象のフィンガープリントに使用される異常パケットを検索します。既存のシグニチャを調整することも、カスタム シグニチャを作成することもできます。

TCP スイープには、TCP フラグとマスクを指定する必要があります。TCP フラグのセットに複数のエントリを指定できます。また、オプションのポート範囲を指定して、特定のパケットを除外することもできます。

表 B-36 に、Sweep Other TCP エンジンに固有のパラメータを示します。

表 B-36　Sweep Other TCP エンジンのパラメータ

パラメータ	説明	値
specify-port-range	（任意）検査でのポート範囲の使用をイネーブルにします。 • port-range：検査で使用する UDP ポート範囲。	0 ～ 65535 a-b[,c-d]
set-tcp-flags	照合する TCP フラグを設定します。 • tcp-flags：この検査で使用される TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• urg • ack • psh • rst • syn • fin

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Traffic Anomaly エンジン

（注）　異常検出シグニチャを編集または調整することはできますが、カスタムの異常検出シグニチャを作成することはできません。

Traffic Anomaly エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出で異常が見つかると、これらのシグニチャに関するアラートがトリガーされます。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。アラートの詳細は、ヒストグラムがトリガーされたため、ワーム検出に使用されるしきい値を示します。その時点から、すべてのスキャナはワームに感染したホストとして検出されます。

次の異常検出イベント アクションが可能です。

- produce-alert：イベントをイベント ストアに書き込みます。
- deny-attacker-inline：指定された期間、この攻撃者のアドレスから発生したこのパケットおよび将来のパケットを送信しません。
- log-attacker-packets：攻撃者のアドレスが含まれるパケットに対する IP ロギングを開始します。
- log-pair-packets：攻撃者と攻撃対象のアドレス ペアが含まれているパケットの IP ロギングを開始します。
- deny-attacker-service-pair-inline：送信元 IP アドレスと宛先ポートをブロックします。
- request-snmp-trap：SNMP 通知を実行するよう、NotificationApp に要求を送信します。
- request-block-host：このホスト（攻撃者）をブロックするよう、ARC に要求を送信します。

表 B-37 に、異常検出ワーム シグニチャのリストを示します。

表 B-37　異常検出ワーム シグニチャ

シグニチャ ID	サブシグニチャ ID	名前	説明
13000	0	Internal TCP Scanner	内部ゾーンで TCP プロトコルを介して単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	0	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。

表 B-37　異常検出ワーム シグニチャ （続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
13002	0	Internal Other Scanner	内部ゾーンでほかのプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでほかのプロトコル上にワーム攻撃を識別しました。ほかのヒストグラムのしきい値を超え、ほかのプロトコル上にスキャナが識別されました。
13003	0	External TCP Scanner	外部ゾーンで TCP プロトコルを介して単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	0	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	0	External Other Scanner	外部ゾーンで他のプロトコルを介して単一スキャナを識別しました。
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13006	0	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコルを介してワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコルを介してスキャナが識別されました。
13007	0	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13008	0	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介して単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでほかのプロトコルを介してワーム攻撃を識別しました。他のヒストグラムのしきい値を超え、他のプロトコルを介してスキャナが識別されました。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Traffic ICMP エンジン

Traffic ICMP エンジンは、TFN2K、LOKI、DDoS などの非標準プロトコルを分析します。このエンジンには、ユーザが設定可能なパラメータを持つ 2 つのシグニチャ（LOKI プロトコルに基づく）だけが含まれます。

TFN2K は、TFN の新しいバージョンです。TFN2K は DDoS エージェントの一種であり、感染した複数のコンピュータ（ゾンビ）による協調した攻撃（何百または何千もの未知の攻撃ホストから 1 つのコンピュータまたはドメインに向けて偽のトラフィック フラッドを送信する攻撃）を制御します。TFN2K はランダムに抽出されたパケット ヘッダー情報を送信しますが、それにはシグニチャの定義に使用できる 2 つの識別子が付いています。1 つは L3 チェックサムが不正かどうかを示し、もう 1 つはペイロードの末尾に文字 64「A」が検出されたかどうかを示します。TFN2K は、任意のポートで実行可能であり、ICMP、TCP、UDP、またはこれらのプロトコルの組み合わせを使用して通信できます。

LOKI は、バック ドア型トロイの木馬タイプです。コンピュータが感染すると、悪意のあるコードにより ICMP トンネルが作成されます。この ICMP トンネルは、ICMP 応答内での小さなペイロードの送信に使用されるおそれがあります（ICMP をブロックするように設定していないと、ICMP 応答はファイアウォールを通過することがあります）。LOKI シグニチャは、ICMP エコーの要求と応答のアンバランス、簡易 ICMP コード、およびペイロード識別子をモニタします。

（TFN2K を除く）DDOS カテゴリは、ICMP ベースの DDOS エージェントを対象とします。ここで使用する主なツールは、TFN と Stacheldraht です。これらは TFN2K と同様に動作しますが、ICMP だけに依存し、固定コマンド（整数および文字列）を備えています。

表 B-38 に、Traffic ICMP エンジンに固有のパラメータを示します。

表 B-38　Traffic ICMP エンジンのパラメータ

パラメータ	説明	値
parameter-tunable-sig	設定可能なパラメータがシグニチャに存在するかどうか。	[yes] | [no]
inspection-type	実行する検査のタイプ： • 最初の LOKI トラフィックを検査する。 • 変更された LOKI トラフィックを検査する。	is-loki is-mod-loki
reply-ratio	要求と応答のアンバランス。要求と比べて、応答が指定した数より多い場合に、アラートを起動します。	0 ～ 65535
want-request	アラートを起動する前に、ECHO REQUEST の検出が必要となります。	[true] | [false]

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Trojan エンジン

Trojan エンジンは、BO2K および TFN2K などの非標準プロトコルを分析します。Trojan エンジンには、Trojan BO2K、TrojanTFN2K、および Trojan UDP の 3 つがあります。

BO は、UDP 上のみで実行された最初の Windows のバック ドア型トロイの木馬です。これはまもなく、BO2K に更新されました。BO2K は、基本的な XOR で暗号化された UDP と TCP の両方に対応しています。これらには、特定のクロスパケット特性を持つプレーンな BO ヘッダーがあります。

また、BO2K には、BO ヘッダーを暗号化し、ほぼ認識できないクロスパケット パターンを作成するように設計された隠れた TCP モジュールもあります。UDP モードの BO および BO2K は、Trojan UDP エンジンによって処理されます。TCP モードは、Trojan BO2K エンジンによって処理されます。

（注）　Trojan UDP エンジンの swap-attacker-victim を除き、Trojan エンジンに固有のパラメータはありません。

詳細情報

すべてのシグニチャ エンジンに共通するパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

APPENDIX C

トラブルシューティングに関するヒントと手順

（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。

この付録にはトラブルシューティングに関するヒントと、IPS SSP およびソフトウェアに関する手順が含まれています。次のような構成になっています。

- 「Bug Toolkit」（P.C-2）
- 「予防保守」（P.C-2）
- 「ディザスタ リカバリ」（P.C-6）
- 「パスワード回復」（P.C-8）
- 「時刻源」（P.C-10）
- 「仮想化の利点および制約事項」（P.C-12）
- 「サポート対象 MIB」（P.C-13）
- 「グローバル相関のトラブルシューティング」（P.C-13）
- 「異常検出をディセーブルにする場合」（P.C-14）
- 「分析エンジン応答なし」（P.C-15）
- 「外部製品インターフェイスのトラブルシューティング」（P.C-16）
- 「センサーのトラブルシューティング」（P.C-17）
- 「IPS SSP のトラブルシューティング」（P.C-48）
- 「情報の収集」（P.C-52）

Bug Toolkit

Bug Toolkit を使用すると、ソフトウェア バージョン、フィーチャ セット、およびキーワードに基づいて既知のバグを検索できます。各バグが統合されているか、可能な場合は修正されていると、検索結果のマトリクスが表示されます。また、検索結果をバグ グループに保存したり、それらのグループに新しい欠陥アラートを配信できる永続的なアラート エージェントを作成したりすることができます。

（注）　Bug Toolkit にアクセスするには、Cisco.com にログインする必要があります。

Bug Toolkit には、次の URL を使用してアクセスします。

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

予防保守

ここでは、センターの予防保守の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。

- 「予防保守の概要」（P.C-2）
- 「バックアップ コンフィギュレーション ファイルの作成と使用」（P.C-3）
- 「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.C-3）
- 「サービス アカウントの作成」（P.C-5）

予防保守の概要

次の処理は、センサーの維持に役立ちます。

- 適切な設定をバックアップします。現在の設定が使用不可能になっても、それをバックアップ バージョンと交換することができます。
- バックアップ設定をリモート システムに保存します。
- 手動アップグレードは、必ず設定をバックアップしてから行ってください。自動アップグレードが設定されている場合は、定期バックアップを必ず実施してください。
- 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。

注意　サービス アカウントを作成するかどうかは、慎重に検討してください。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。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。

詳細情報

- コンフィギュレーション ファイルのバックアップ手順については、「バックアップ コンフィギュレーション ファイルの作成と使用」（P.C-3）を参照してください。
- リモート サーバを使用してコンフィギュレーション ファイルをコピーおよび復元する手順については、「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.C-3）を参照してください。
- サービス アカウントの詳細については、「サービス アカウントの作成」（P.C-5）を参照してください。

バックアップ コンフィギュレーション ファイルの作成と使用

設定を保護するために、現在の設定のバックアップを作成し、表示することによってそれが保存したい設定であることを確認できます。この設定を復元する必要があるときは、バックアップ コンフィギュレーション ファイルを現在の設定とマージするか、現在のコンフィギュレーション ファイルにバックアップ コンフィギュレーション ファイルを上書きします。

現在の設定をバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定を保存します。現在の設定がバックアップ ファイルに保存されます。

```
ips-ssp# copy current-config backup-config
```

ステップ 3　バックアップ コンフィギュレーション ファイルを表示します。バックアップ コンフィギュレーション ファイルが表示されます。

```
ips-ssp# more backup-config
```

ステップ 4　バックアップの設定を現在の設定とマージしたり、現在の設定を上書きしたりすることができます。

- バックアップの設定を現在の設定とマージします。

  ```
  ips-ssp# copy backup-config current-config
  ```

- バックアップの設定で現在の設定を上書きします。

  ```
  ips-ssp# copy /erase backup-config current-config
  ```

リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元

（注）　アップグレードする前に現在のコンフィギュレーション ファイルをリモート サーバにコピーすることを推奨します。

copy [**/erase**] *source_url destination_url keyword* コマンドを使用して、コンフィギュレーション ファイルをリモート サーバにコピーします。その後、リモート サーバから現在の設定を復元できます。まず現在の設定をバックアップするプロンプトが表示されます。

オプション

次のオプションが適用されます。

- **/erase**：コピーする前にコピー先ファイルを消去します。

  このキーワードは、current-config だけに適用されます。backup-config は、常に上書きされます。このキーワードがコピー先の current-config に対して指定されている場合、コピー元の設定がシステムのデフォルト設定に適用されます。このキーワードがコピー先の current-config に対して指定されていない場合、コピー元の設定がその current-config にマージされます。

- *source_url*：コピー元のファイルの場所です。URL またはキーワードを使用できます。
- *destination_url*：コピー先のファイルの場所です。URL またはキーワードを使用できます。

- **current-config**：現在の実行コンフィギュレーションです。コマンドが入力されると、設定が維持されます。
- **backup-config**：コンフィギュレーション バックアップの保管場所です。

コピー元およびコピー先 URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバの場合のコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、リモート ホストを SSH 既知ホスト リストに追加することも必要です。

- http:：Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。

  http:[[/[username@]location]/directory]/filename

- https:：Web サーバの場合のコピー元 URL。このプレフィクスの構文は、次のとおりです。

  https:[[/[username@]location]/directory]/filename

（注）　Web サイトにアクセスするのにユーザ名が必要な場合、HTTP および HTTPS によってパスワードが要求されます。HTTPS プロトコルを使用する場合は、リモート ホストが TLS の信頼できるホストである必要があります。

注意　センシング インターフェイスおよび仮想センサーが同じ設定になっていない場合、別のセンサーからのコンフィギュレーション ファイルのコピーは、エラーになる可能性があります。

現在の設定のリモート サーバへのバックアップ

現在の設定をリモート サーバにバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** を入力して、現在の設定をバックアップの設定にコピーします。

```
cfg            100% |***********************************************| 36124       00:00
```

バックアップ ファイルからの現在の設定の復元

バックアップ ファイルから現在の設定を復元するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** を入力して、現在の設定をバックアップの設定にコピーします。

```
cfg            100% |***********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

ステップ 4　現在設定されているホスト名、IP アドレス、サブネット マスク、管理インターフェイス、およびアクセス リストを保持するには、**no** を入力します。残りの設定が復元された後、センサーへのアクセスを確保するために、この情報を保持することを推奨します。

詳細情報

サポートされる HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」（P.20-2）を参照してください。

サービス アカウントの作成

トラブルシューティングの際に使用する TAC 用のサービス アカウントを作成できます。センサーには複数のユーザがアクセスできますが、センサーに対するサービス権限を持てるのは 1 人のユーザだけです。サービス アカウントは、サポートの目的のためにのみ使用します。

root ユーザのパスワードは、サービス アカウントが作成されたときにサービス アカウントのパスワードに同期化されます。root アクセス権限を取得するには、サービス アカウントでログインしてから、**su - root** コマンドで root ユーザに切り替わる必要があります。

注意　TAC の指示に基づく場合を除き、サービス アカウントを使用してセンサーに変更を加えないでください。サービス アカウントを使用してセンサーを設定すると、その設定は TAC のサポート対象外になります。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、他の IPS サービスの適切なパフォーマンスと機能に影響を及ぼします。TAC は、追加のサービスが加えられたセンサーをサポートしません。

注意　サービス アカウントを作成するかどうかは、慎重に検討してください。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。

サービス アカウントを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　サービス アカウントのパラメータを指定します。ユーザ名はパターン ^[A-Za-z0-9()+:,_/-]+$ に従います。つまり、ユーザ名は必ず英字または数字から始まり、A ～ Z の任意の英字（大文字または小文字）、0 ～ 9 の任意の数字、および - と _ からなる 1 ～ 64 の文字で構成します。

```
ips-ssp(config)# user username privilege service
```

ステップ 4　入力を要求されたらパスワードを指定します。パスワードは、センサー管理者によって設定された要件を満たす必要があります。このセンサーに対してサービス アカウントがすでに存在する場合は、次のエラー メッセージが表示され、サービス アカウントは作成されません。

```
Error: Only one service account may exist
```

ステップ 5　コンフィギュレーション モードを終了します。

```
ips-ssp(config)# exit
ips-ssp#
```

サービス アカウントを使用して CLI 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 reimaged to guarantee proper operation.
*****************************************************************************************
```

ディザスタ リカバリ

ここでは、推奨事項と、障害発生後にセンサーの復旧が必要な場合に実行すべき手順について説明します。

次に示す推奨事項に従い、障害に備えてください。

- 設定に CLI、IDM、または IME を使用する場合は、変更が行われるたびに現在の設定をセンサーから FTP または SCP サーバへコピーします。
- その設定に対する特定のソフトウェア バージョンをメモします。コピーされた設定は、同じバージョンのセンサーにしか適用できません。
- また、そのセンサー上で使用されているユーザ ID のリストも必要です。ユーザ ID およびパスワードのリストは、設定内に保存されません。

障害が発生したときにセンサーの復旧が必要な場合は、次の作業を行ってみてください。

1. センサーのイメージを再作成します。
2. デフォルトのユーザ ID とパスワード（**cisco**）を使用してセンサーにログインします。

（注）　パスワード **cisco** の変更を促すプロンプトが表示されます。

3. センサーを初期化します。
4. センサーのアップグレードを行い、最後に設定が保存およびコピーされたときにセンサーに搭載されていた IPS ソフトウェア バージョンにします。

警告　**障害発生前にセンサーに搭載されていた IPS ソフトウェア バージョンにセンサーを戻さずに、保存された設定のコピーを試みると、設定エラーを引き起こす場合があります。**

5. 最後に保存された設定をセンサーにコピーします。
6. クライアントを更新して、センサーの新しいキーと証明書を使用します。

   イメージを再作成すると、センサーの SSH キーと HTTPS 証明書が変更されるので、ホストを SSN 既知ホスト リストに追加し直す必要があります。
7. 前のユーザを作成します。

詳細情報

- コンフィギュレーション ファイルのバックアップ手順については、「バックアップ コンフィギュレーション ファイルの作成と使用」（P.C-3）を参照してください。
- センサーの現在のユーザ リストを取得する手順については、「ユーザ ステータスの表示」（P.4-18）を参照してください。
- センサーのイメージを再作成する手順については、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。
- **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「IPS SSP の初期化」を参照してください。
- IPS ソフトウェアの取得とインストール方法の詳細については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。
- リモート サーバを使用してコンフィギュレーション ファイルをコピーおよび復元する手順については、「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.C-3）を参照してください。
- SSH 既知ホスト リストにホストを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- ユーザを追加する手順については、「ユーザの追加と削除」（P.4-14）を参照してください。

パスワード回復

ここでは、IPS SSP のパスワードを回復する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。

- 「IPS SSP パスワードの回復」（P.C-8）
- 「パスワード回復のディセーブル化」（P.C-9）
- 「パスワード回復の状態の確認」（P.C-9）
- 「パスワード回復のトラブルシューティング」（P.C-10）

IPS SSP パスワードの回復

（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。

CLI または ASDM を使用して IPS SSP のデフォルト（**cisco**）にパスワードをリセットできます。パスワードをリセットすると、IPS SSP がリブートします。リブート中は、IPS サービスを使用できません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、ROMMON confreg ビットを 0x7 に設定してから、センサーをリブートします。この ROMMON ビットにより、GRUB メニューがデフォルトでオプション 2（**パスワードのリセット**）になります。

指定したスロット内のモジュールに搭載されている IPS のバージョンがパスワード回復をサポートしていない場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーから、[Tools] > [IPS Password Reset] を選択します。

（注）　このオプションは、IPS モジュールがインストールされていなければ表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで、[OK] をクリックしてパスワードをデフォルト（**cisco**）にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットに失敗した場合は、適応型セキュリティ アプライアンスに適切な ASA ソフトウェア、および IPS SSP に IPS 7.1 以降がインストールされていることを確認します。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。IPS SSP がリブートします。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブル化されたセンサーでパスワードを回復しようとすると、プロセスはエラーや警告なしに進行しますが、パスワードはリセットされません。パスワードを忘れたためにセンサーにログインできず、パスワード回復がディセーブルに設定されている場合は、センサーのイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。CLI、IDM、または IME を使用してパスワード回復をディセーブルにできます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
ips-ssp# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
ips-ssp(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
ips-ssp(config-hos)# password-recovery disallowed
```

IDM または IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用し、IDM または IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復の状態の確認

show settings | **include password** コマンドを使用して、パスワード回復がイネーブルかどうかを確認します。

パスワード回復がイネーブルかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp (config)# service host
ips-ssp (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタリングされた出力で設定を表示することにより、パスワード回復の状態を確認します。

```
ips-ssp(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
ips-ssp(config-hos)#
```

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行うときは、次の点に注意します。

- ROMMON プロンプト、GRUB メニュー、スイッチ CLI、またはルータ CLI からは、センサー設定内でパスワード回復がディセーブルになっているかどうかを判別できません。パスワード回復を試みると、常に成功しているように見えます。ディセーブルになっていた場合、パスワードは **cisco** にリセットされません。この場合、センサーのイメージを再作成するしか方法はありません。
- パスワード回復は、ホスト設定でディセーブルにできます。外部のメカニズムを使用するプラットフォームの場合は、パスワードをクリアするコマンドを実行できますが、IPS でパスワード回復がディセーブルであると、IPS はパスワードの回復が許可されていないことを検知して、外部要求を拒否します。
- パスワード回復の状態を確認するには、**show settings | include password** コマンドを使用します。

時刻源

ここでは、IPS SSP で正確な時間を維持する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。

- 「時刻源と IPS SSP」（P.C-10）
- 「IPS SSP のクロックと適応型セキュリティ デバイスのクロックの同期化」（P.C-11）
- 「IPS SSP が NTP サーバと同期していることを確認する」（P.C-11）
- 「IPS SSP の時刻の修正」（P.C-12）

時刻源と IPS SSP

センサーには、信用できる時刻源が必要です。すべてのイベント（アラート）に、正しい UTC と現地時間のタイムスタンプが必要です。正確なタイムスタンプがないと、攻撃の後でログを正しく分析できません。センサーを初期化するとき、時間帯とサマータイム設定をセットアップします。

IPS SSP 上の時刻を設定する方法は 2 つあります。

- IPS SSP が、自身のクロックを、自身を搭載している適応型セキュリティ アプライアンスのクロックと自動的に同期します。これがデフォルトです。
- 時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように IPS SSP を設定できます。

（注） NTP サーバを使用することを推奨します。認証済みまたは未認証の NTP を使用できます。認証済みの NTP の場合、NTP サーバの IP アドレス、NTP サーバのキー ID、および NTP サーバのキー値が必要です。初期化時に NTP をセットアップすることも、CLI、IDM、IME、または ASDM を使用して NTP を設定することもできます。

詳細情報

NTP の設定手順については、「NTP の設定」（P.4-31）を参照してください。

IPS SSP のクロックと適応型セキュリティ デバイスのクロックの同期化

IPS SSP は、起動するたび、および適応型セキュリティ アプライアンスのクロックが設定されるたびに、システム クロックと適応型セキュリティ アプライアンスのクロックを同期させます。IPS SSP クロックと適応型セキュリティ アプライアンスのクロックは、時間とともにずれていく傾向にあります。この差は、1 日で数秒になることがあります。この問題を回避するため、IPS SSP クロックと適応型セキュリティ アプライアンスのクロックの両方が外部の NTP サーバに同期していることを確認します。IPS SSP のクロックのみ、または適応型セキュリティ アプライアンスのクロックのみが NTP サーバに同期すると、時間のずれが生じます。

IPS SSP が NTP サーバと同期していることを確認する

IPS では、無効な NTP キー値または ID など、誤りのある NTP の設定はセンサーに適用できません。誤りのある設定を適用しようとすると、エラー メッセージを受け取ります。NTP の設定を確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。NTP 統計情報セクションには、NTP サーバとのセンサーの同期に関するフィードバックを含む NTP 統計情報が表示されます。

NTP の設定を確認するには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　ホストの統計情報を生成します。

```
ips-ssp# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
          11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
          LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
         ind assID status  conf reach auth condition  last_event cnt
           1 10372  f014   yes   yes   ok     reject    reachable  1
           2 10373  9014   yes   yes  none    reject    reachable  1
         status = Not Synchronized
     ...
```

ステップ 3　数分後に再び、ホストの統計情報を生成します。

```
ips-ssp# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
          LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
         ind assID status  conf reach auth condition  last_event cnt
           1 10372  f624   yes   yes   ok   sys.peer   reachable  2
           2 10373  9024   yes   yes  none    reject    reachable  2
         status = Synchronized
```

ステップ 4　ステータスが引き続き `Not Synchronized` を示す場合は、NTP サーバ管理者と一緒に NTP サーバの設定が正しいことを確認してください。

IPS SSP の時刻の修正

保存されているイベントには、その作成時刻がタイムスタンプとして記録されるため、時刻の設定に誤りがあると、それらのイベントに対しても誤った時刻が記録されます。イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。元のセンサーのセットアップ時に、8:00 a.m. と指定すべきところを誤って 8:00 p.m. と指定した場合、それを修正すると、修正後の時刻は現在よりさかのぼった時刻に設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中にセンサーを中部時間に設定し、さらにサマータイムを有効にした場合、現地時間が 8:04 p.m. であれば、時刻は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。この場合、時刻を 9:00 a.m. に変更すれば、時計は 09:01:33 CDT と表示されます。ただし、UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。ここにタイムスタンプの問題が生じる原因があります。

イベント レコードのタイムスタンプの整合性を確保するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブをクリアする必要があります。

（注）　イベントは、個別には削除できません。

詳細情報

イベントをクリアする手順については、「イベントのクリア」（P.C-76）を参照してください。

仮想化の利点および制約事項

（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。

センサーの設定に関する問題を回避するため、センサーにおける仮想化の利点と制約事項を理解しておいてください。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。

  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。
- 固定ストアが制限されます。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

サポート対象 MIB

SNMP の設定に関する問題を回避するため、センサーでサポートされている MIB を知っておいてください。

センサーでは、次のプライベート MIB がサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注） MIB II はセンサーで使用できますが、シスコではサポートしていません。一部の要素が正確でないことがわかっています（たとえば、センシング インターフェイスの IF MIB からのパケット カウントなど）。MIB II の要素を使用できますが、シスコでは、それらがすべて正確な情報を提供することを保証していません。シスコは、リストにあるその他の MIB を完全サポートしていますし、それらの出力も正確です。

これらのプライベートの Cisco MIB は、次の URL の [SNMP v2 MIBs] という見出しの下で確認できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

グローバル相関のトラブルシューティング

グローバル相関を設定する場合は、以下が順守されていることを確認してください。

- グローバル相関の更新はセンサー管理インターフェイスを介して行われるので、ファイアウォールでポート 443/80 トラフィックが許可されている必要があります。
- グローバル相関機能が動作するには、HTTP プロキシ サーバまたは DNS サーバが設定されていなければなりません。
- グローバル相関機能が動作するには有効な IPS ライセンスが必要です。
- グローバル相関機能には外部 IP アドレスのみが含まれるため、センサーを社内ラボに配置するとグローバル相関情報を受信できません。

- お使いのセンサーがグローバル相関機能をサポートしていることを確認してください。
- お使いの IPS バージョンがグローバル相関機能をサポートしていることを確認してください。

詳細情報

グローバル相関の詳細については、第 10 章「グローバル相関の設定」を参照してください。

異常検出をディセーブルにする場合

一方向のトラフィックだけを検出するようにセンサーを設定している場合は、異常検出をディセーブルにする必要があります。そうしないと、異常検出がワーム スキャナのように、非対称トラフィックを不完全接続と見なし、アラートを起動するので、多数のアラートを受信することになります。

異常検出をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　分析エンジン サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(config-ana)#
```

ステップ 3　ディセーブルにする異常検出ポリシーを含む仮想センサー名を入力します。

```
ips-ssp(config-ana)# virtual-sensor vs0
ips-ssp(config-ana-vir)#
```

ステップ 4　異常検出動作モードをディセーブルにします。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# operational-mode inactive
ips-ssp(config-ana-vir-ano)#
```

ステップ 5　分析エンジン サブモードを終了します。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(config-ana-vir)# exit
ips-ssp(config-ana-)# exit
Apply Changes:?[yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

ワームの詳細については、「ワーム」（P.9-2）を参照してください。

分析エンジン応答なし

エラー メッセージ　Output from show statistics analysis-engine
Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

エラー メッセージ　Output from show statistics anomaly-detection
Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

エラー メッセージ　Output from show statistics denied-attackers
Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

考えられる原因　これらのエラー メッセージは、**show tech support** コマンドを実行したときに、分析エンジンが実行していないと表示されます。

推奨処置　分析エンジンが実行中であることを確認し、問題が解決されるかどうかをモニタしてください。

分析エンジンが実行中であることを確認し、問題をモニタするには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　分析エンジンが実行していないことを確認します。

```
ips-ssp# show version

-----
MainApp N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
AnalysisEngine N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Not Running
CLI N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500
```

分析エンジンが Not Running を示すかどうかを確認します。

ステップ 3　**show tech-support** を入力し、出力を保存します。

ステップ 4　センサーをリブートします。

ステップ 5　問題が解決されたかどうかを確認するには、センサーが安定してから **show version** を入力します。

ステップ 6　分析エンジンがまだ Not Running を示す場合は、元の **show tech support** コマンド出力を TAC に提出してください。

外部製品インターフェイスのトラブルシューティング

ここでは、外部製品インターフェイスに起こり得る問題と、トラブルシューティングのヒントを示します。外部製品インターフェイスの詳細については、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。次のような構成になっています。

- 「外部製品インターフェイスに関する問題」（P.C-16）
- 「外部製品インターフェイスのトラブルシューティングのヒント」（P.C-17）

外部製品インターフェイスに関する問題

外部製品インターフェイスがホスト ポスチャと隔離イベントを受信した場合、次のような問題が生じる可能性があります。

- センサーは、一定数のホスト レコードしか保存できません。
  - レコード数が 10,000 を超えると、後続のレコードはドロップされます。
  - レコードが 10,000 の制限値に達し、その後 9900 を下回ると新しいレコードはドロップされなくなります。
- ホストが IP アドレスを変更できる、あるいは別のホストの IP アドレスを使用しているように見えます（DHCP リースの期限満了やワイヤレス ネットワーク内での移動などによる）。IP アドレスが競合すると、センサーは最新のホスト ポスチャ イベントを最も正確なものと見なします。
- ネットワークでは、異なる VLAN に重複する IP アドレス範囲を含めることができるが、ホスト ポスチャには VLAN ID 情報を加えることはできません。指定されたアドレス範囲を無視するように、センサーを設定できます。
- ホストがファイアウォールの背後にあるため、CSA MC がホストに到達できません。到達不能ホストは除外できます。
- CSA MC イベント サーバでは、デフォルトで最大 10 個のサブスクリプションを開くことができます。この値は変更できます。サブスクリプションを開くには、管理アカウントとパスワードが必要です。
- CSA データが仮想化されず、センサーでグローバルに処理されます。
- ホスト ポスチャ OS と IP アドレスがパッシブ OS フィンガープリント ストレージに統合されます。これらはインポートされた OS プロファイルとして表示できます。
- 隔離されたホストを表示できません。
- センサーが各 CSA MC ホストの X.509 証明書を認識しなければなりません。これらを信頼できるホストとして追加する必要があります。
- 最大 2 台の外部製品デバイスを設定できます。

詳細情報

- OS マップおよび識別情報の使用の詳細については、「設定された OS マップの追加、編集、削除、および移動」（P.8-28）および「OS ID の表示とクリア」（P.8-32）を参照してください。
- 信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。

外部製品インターフェイスのトラブルシューティングのヒント

外部製品インターフェイスのトラブルシューティングを行う場合は、次の点を確認します。

- インターフェイスがアクティブかどうかを確認するには、CLI で **show statistics external-product-interface** コマンドの出力を確認します。または、IDM で [Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答のインターフェイス状態の行を確認します。あるいは、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答のインターフェイス状態の行を確認します。
- CSA MC の IP アドレスが信頼できるホストに追加されていることを確認してください。追加していない場合は追加し、数分待ってから再度確認します。
- ブラウザを使用して CSA MC でサブスクリプションを開いてから閉じ、サブスクリプション ログイン情報を確認します。
- イベント ストアで CSA MC サブスクリプション エラーがないか確認します。

詳細情報

- 信頼できるホストの追加手順については、「TLS の信頼できるホストの追加」（P.4-40）を参照してください。
- イベントの表示手順については、「イベントの表示」（P.C-73）を参照してください。

センサーのトラブルシューティング

ここでは、センサーのトラブルシューティングについて説明します。次のような構成になっています。

- 「接続不良のトラブルシューティング」（P.C-17）
- 「分析エンジンがビジー状態になる」（P.C-18）
- 「通信の問題」（P.C-18）
- 「SensorApp とアラート」（P.C-23）
- 「ブロッキング」（P.C-30）
- 「ロギング」（P.C-39）
- 「ソフトウェアのアップグレード」（P.C-45）

接続不良のトラブルシューティング

センサーおよび適応型セキュリティ アプライアンスで接続不良のトラブルシューティングを行うには、次の処理を実行します。

- すべての電源コードがしっかり接続されていることを確認します。
- 外部と内部のすべてのコンポーネントのすべてのケーブルが、正しい位置にしっかり接続されていることを確認します。
- すべてのデータ ケーブルおよび電源コードを取り外し、破損がないことを確認します。ケーブルに曲がったピンや破損したコネクタがないことを確認します。
- 各デバイスが適切に設置されていることを確認します。
- デバイスにラッチがある場合は、ラッチが完全に閉められ、ロックされていることを確認します。

- コンポーネントの接続が適切でないことを示すインターロックまたはインターコネクト インジケータをチェックします。
- 問題が続く場合は、各デバイスを取り外し、再び取り付けて、コネクタやソケットに曲がったピンやその他の破損がないことを確認します。

分析エンジンがビジー状態になる

センサーのイメージを再作成した後、分析エンジンは正規表現テーブルの再構築中となり、新しい設定に応答しません。分析エンジンがビジー状態であるかどうかを確認するには、**show statistics virtual-sensor** コマンドを使用します。分析エンジンがビジー状態である場合は、次のエラー メッセージを受け取ります。

```
ips-ssp# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables. This
may take a while.
```

分析エンジンが正規表現テーブルを再構築中であるときに、シグニチャのイネーブル化や廃棄などで設定を更新しようとすると、エラー メッセージを受け取ります。

```
ips-ssp# configure terminal
ips-ssp(config)# service sig sig0
ips-ssp(config-sig)# sig 2000 0
ips-ssp(config-sig-sig)# status enabled
ips-ssp(config-sig-sig)# status
ips-ssp(config-sig-sig-sta)# enabled true
ips-ssp(config-sig-sig-sta)# retired false
ips-ssp(config-sig-sig-sta)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes?[yes]:
Error: editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex
tables. This may take a while.
The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]: no
No changes were made to the configuration.
ips-ssp(config)#
```

センサーの起動後すぐに仮想センサー統計情報を取得しようとすると、エラー メッセージを受け取ります。センサーがキャッシュ ファイルの再構築を終えても、仮想センサーの初期化が終了していません。

```
ips-ssp# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy.
ips-ssp#
```

分析エンジンがビジー状態であることを示すエラーを受け取った場合は、しばらく待ってから設定変更を試みてください。**show statistics virtual-sensor** コマンドを使用すると、分析エンジンが再び使用可能になるときがわかります。

通信の問題

ここでは、センサーの通信に関する問題のトラブルシューティングに役立つ情報を提供します。次のような構成になっています。

- 「Telnet または SSH でセンサーの CLI にアクセスできない」（P.C-19）
- 「設定が誤っているアクセス リストの修正」（P.C-21）
- 「重複している IP アドレスがインターフェイスをシャットダウンする」（P.C-22）

Telnet または SSH でセンサーの CLI にアクセスできない

Telnet（すでにイネーブルにしてある場合）または SSH を利用してセンサーの CLI にアクセスできない場合は、次の手順を実行します。

ステップ 1　コンソール、端末、またはモジュール セッションから、センサーの CLI にログインします。

ステップ 2　センサー管理インターフェイスがイネーブルであることを確認します。

```
ips-ssp# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

管理インターフェイスは、リスト内のステータス行 `Media Type = TX` のインターフェイスです。Link Status が `Down` の場合は、ステップ 3 に進みます。Link Status が `Up` の場合は、ステップ 5 に進みます。

ステップ 3　センサー IP アドレスが一意であることを確認します。

```
ips-ssp# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

管理インターフェイスは、ネットワーク上の別のデバイスに同じ IP アドレスがあることを検出すると、起動しません。

ステップ 4　管理ポートがアクティブなネットワーク接続に接続していることを確認します。管理ポートがアクティブなネットワーク接続に接続していないと、管理インターフェイスは起動しません。

ステップ 5　センサーに接続しようとしているワークステーションの IP アドレスが、センサー アクセス リストで許可されていることを確認します。

```
ips-ssp# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

ワークステーション ネットワーク アドレスがセンサー アクセス リストで許可されている場合は、ステップ 6 に進みます。

ステップ 6　ワークステーション ネットワーク アドレスの許可エントリを追加し、設定を保存してから、接続を再試行します。

ステップ 7　ネットワーク設定でワークステーションからセンサーへの接続が許可されていることを確認します。

センサーがファイアウォールの後ろで保護されており、ワークステーションがファイアウォールの前にある場合、ワークステーションにセンサーへのアクセスを許可するようにファイアウォールが設定されていることを確認します。または、ワークステーションが、ワークステーションの IP アドレスのネットワーク アドレス変換を行っているファイアウォールの後ろにあり、センサーがファイアウォールの前にある場合は、ワークステーションの変換アドレスに対する許可エントリがセンサー アクセス リストに含まれていることを確認します。

詳細情報

- センサーで Telnet をイネーブルおよびディセーブルにする手順については、「Telnet のイネーブル化とディセーブル化」（P.4-4）を参照してください。
- センサーで直接 CLI セッションを開くさまざまな方法については、第 2 章「IPS SSP へのログイン」を参照してください。
- IP アドレスを変更する手順については、「IP アドレス、ネットマスク、およびゲートウェイの変更」（P.4-3）を参照してください。
- アクセス リストを変更する手順については、「設定が誤っているアクセス リストの修正」（P.C-21）を参照してください。

設定が誤っているアクセス リストの修正

設定が誤っているアクセス リストを修正するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　設定を表示して、アクセス リストを確認します。

```
ips-ssp# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ips-ssp#
```

ステップ 3　クライアント IP アドレスが許可されたネットワーク内にリストされているかどうか確認します。リストされていない場合は、その IP アドレスを追加します。

```
ips-ssp# configure terminal
ips-ssp(config)# service host
ips-ssp(config-hos)# network-settings
ips-ssp(config-hos-net)# access-list 171.69.70.0/24
```

ステップ 4　設定を確認できます。

```
ips-ssp(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 192.168.1.2/24,192.168.1.1
      host-name: ips-ssp default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      -----------------------------------------------
         network-address: 10.0.0.0/8
         -----------------------------------------------
         network-address: 64.0.0.0/8
         -----------------------------------------------
         network-address: 171.69.70.0/24
         -----------------------------------------------
```

```
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
ips-ssp(config-hos-net)#
```

重複している IP アドレスがインターフェイスをシャットダウンする

同じ IP アドレスを持つ 2 台のセンサーが新たにイメージ化され、同じネットワーク上で同時にアップ状態になると、インターフェイスはシャットダウンします。Linux では、他のホストとのアドレスの競合を検出した場合、コマンド/コントロール インターフェイスがアクティブになることが防止されます。

問題のセンサーが、ネットワーク上の別のホストと競合する IP アドレスを持っていないことを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態かどうかを判断します。

```
ips-ssp# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
```

```
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

出力に表示されるコマンド/コントロール インターフェイスのリンク ステータスがダウン状態である場合は、ハードウェアの問題か、IP アドレスの競合があります。

ステップ 3　センサーのケーブル接続が正しいことを確認します。

ステップ 4　IP アドレスが正しいことを確認します。

詳細情報

IP アドレスが正しいことを確認する手順については、「ネットワーク設定値の変更」（P.4-1）を参照してください。

SensorApp とアラート

ここでは、SensorApp とアラートに関する問題のトラブルシューティングに役立つ情報を提供します。次のような構成になっています。

- 「SensorApp が実行しない」（P.C-23）
- 「物理的な接続性、SPAN、または VACL ポートの問題」（P.C-25）
- 「アラートを表示できない」（P.C-27）
- 「センサーがパケットを監視しない」（P.C-28）
- 「破損した SensorApp 設定のクリーンアップ」（P.C-29）

SensorApp が実行しない

センシング プロセス SensorApp は、常に動作している必要があります。常に動作していないと、アラートを受信できません。SensorApp は分析エンジンの一部であるので、分析エンジンが実行中であることを確認する必要があります。

分析エンジンが実行中であることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジン サービスのステータスを特定します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S512.0              2010-09-08
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
No license present
Sensor up-time is 21:09.
```

```
Using 10276M out of 11899M bytes of available memory (86% usage)
system is using 28.4M out of 160.0M bytes of available disk space (18% usage)
application-data is using 64.9M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 58.7M out of 71.7M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
AnalysisEngine     S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Not Running
CollaborationApp   S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CLI                S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500

Upgrade History:

  IPS-K9-7.1-1-E4   10:53:07 UTC Mon Sep 27 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 26-Sep-2010 to 26-Sep-2012

ips-ssp#
```

ステップ 3　分析エンジンが実行中でない場合は、それに関係するエラーが発生していないか調べます。

```
ips-ssp# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=10772192586963300O5 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

（注）　最後に再起動した日時が表示されます。この例では、最後の再起動は 2004 年 2 月 19 日 7 時 34 分でした。

ステップ 4　ソフトウェアのアップデートが最新のものであることを確認します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S512.0              2010-09-08
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
No license present
Sensor up-time is 21:09.
Using 10276M out of 11899M bytes of available memory (86% usage)
system is using 28.4M out of 160.0M bytes of available disk space (18% usage)
application-data is using 64.9M out of 171.4M bytes of available disk space (40%
```

```
 usage)
boot is using 58.7M out of 71.7M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
AnalysisEngine     S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CollaborationApp   S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CLI                S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500

Upgrade History:

  IPS-K9-7.1-1-E4   10:53:07 UTC Mon Sep 27 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 26-Sep-2010 to 26-Sep-2012

ips-ssp#
```

最新のものではない場合は、Cisco.com からダウンロードします。

ステップ 5　分析エンジンがまだ実行されない場合は、TAC にお問い合わせください。

詳細情報

- IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャについて」を参照してください
- 最新の Cisco IPS ソフトウェアを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

物理的な接続性、SPAN、または VACL ポートの問題

センサーが正しく接続されていないと、アラートを受信しません。

センサーが正しく接続されていることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態にあり、パケット カウントが増加していることを確認します。

```
ips-ssp# show interfaces
Interface Statistics
   Total Packets Received = 6208415
   Total Bytes Received = 18446744071628877824
   Missed Packet Percentage = 2
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
```

```
   Total Packets Received = 350763
   Total Bytes Received = 21510843
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 79405
   Total Bytes Transmitted = 48931908
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface PortChannel0/0
   Interface function = Sensing interface
   Description =
   Media Type = backplane
   Default Vlan = 0
   InlineMode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Up
   Admin Enabled Status = Enabled
   Link Speed = Auto_10000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 2
   Total Packets Received = 6208415
   Total Bytes Received = 2214293504
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 343056
   Total Undersize Packets Received = 0
   Total Receive Errors = 175751
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 6208415
   Total Bytes Transmitted = 2214293504
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 343056
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/1
   Interface function = Reserved for future use
ips-ssp#
```

ステップ 3　Link Status が Down になっている場合は、センシング ポートが適切に接続されているか確認します。

ステップ 4　インターフェイスの設定を確認します。

ステップ 5　インターフェイスがアップ状態であり、パケット カウントが増加していることを再び確認します。

```
ips-ssp# show interfaces
```

詳細情報

センサーでインターフェイスを設定する手順については、第 5 章「インターフェイスの設定」を参照してください。

アラートを表示できない

アラートが表示されない場合は、次の処理を試みてください。

- シグニチャがイネーブルであることを確認します。
- シグニチャが廃棄されていないことを確認します。
- 製品アラートをアクションとして設定していることを確認します。

（注）　製品アラートを選択しても、後から別のイベント アクションを追加し、その新しい設定に製品アラートを追加していない場合、アラートはイベント ストアに送信されません。シグニチャを設定するたびに、既存の設定が新しい設定に上書きされるので、シグニチャごとに必要なイベント アクションをすべて設定していることを確認してください。

- センサーがパケットを監視していることを確認します。
- アラートが生成されていることを確認します。
- センシング インターフェイスが仮想センサー内にあることを確認します。

アラートが表示されることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　シグニチャが有効であることを確認します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)# signatures 1300 0
ips-ssp(config-sig-sig)# status
ips-ssp(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   -----------------------------------------------
ips-ssp(config-sig-sig-sta)#
```

ステップ 3　製品アラートを設定していることを確認します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)# signatures 1300 0
ips-ssp(config-sig-sig)# engine ?
normalizer     Signature engine
ips-ssp(config-sig-sig)# engine normalizer
ips-ssp(config-sig-sig-nor)# event-action produce-alert
ips-ssp(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
ips-ssp#
```

ステップ 4　センサーがパケットを監視していることを確認します。

```
ips-ssp# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

ステップ 5　アラートが表示されるかどうかを確認します。

```
ips-ssp# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
    Number of Alerts received = 0
    Number of Alerts Consumed by AlertInterval = 0
    Number of Alerts Consumed by Event Count = 0
    Number of FireOnce First Alerts = 0
    Number of FireOnce Intermediate Alerts = 0
    Number of Summary First Alerts  = 0
    Number of Summary Intermediate Alerts  = 0
    Number of Regular Summary Final Alerts  = 0
    Number of Global Summary Final Alerts  = 0
    Number of Alerts Output for further processing = 0alertDetails: Traffic Source: int0 ;
```

センサーがパケットを監視しない

センサーがネットワーク上のパケットを監視していない場合、インターフェイスの設定が正しくないことが考えられます。

センサーがパケットを監視していない場合は、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態であり、パケットを受信していることを確認します。

```
ips-ssp# show interfaces PortChannel0/0
MAC statistics from interface PortChannel0/0
   Interface function = Sensing interface
   Description =
   Media Type = backplane
```

```
   Default Vlan = 0
   InlineMode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Up
   Admin Enabled Status = Enabled
   Link Speed = Auto_10000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 2
   Total Packets Received = 6208912
   Total Bytes Received = 2214357120
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 343056
   Total Undersize Packets Received = 0
   Total Receive Errors = 175751
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 6208912
   Total Bytes Transmitted = 2214357120
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 343056
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

ステップ 3　インターフェイスがアップ状態でない場合は、ケーブル接続をチェックしてください。

詳細情報

IPS SSP を適切にインストールする手順については、『*Installing the Cisco Intrusion Prevention System Security Services Processor 7.1*』を参照してください。

破損した SensorApp 設定のクリーンアップ

SensorApp の設定が破損状態となり、SensorApp を実行できない場合は、SensorApp を完全に削除してから再起動する必要があります。

SensorApp の設定を削除するには、次の手順を実行します。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　root に su します。

ステップ 3　IPS アプリケーションを停止します。

```
/etc/init.d/cids stop
```

ステップ 4　仮想センサー ファイルを交換します。

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

ステップ 5　キャッシュ ファイルを削除します。

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

ステップ 6　サービス アカウントを終了します。

ステップ 7　センサー CLI にログインします。

ステップ 8　IPS サービスを起動します。

```
ips-ssp# cids start
```

ステップ 9　管理者権限でアカウントにログインします。

ステップ 10　センサーをリブートします。

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? [yes]:yes
Request Succeeded.
ips-ssp#
```

詳細情報

IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャについて」を参照してください。

ブロッキング

ここでは、ブロッキングおよび ARC サービスのトラブルシューティングに役立つ情報を提供します。取り上げる項目は次のとおりです。

- 「ブロッキングのトラブルシューティング」（P.C-30）
- 「ARC が実行中であることを確認する」（P.C-31）
- 「ARC 接続がアクティブであることを確認する」（P.C-32）
- 「デバイスのアクセスに関する問題点」（P.C-34）
- 「ネットワーク デバイス上のインターフェイスおよび方向を確認する」（P.C-35）
- 「ネットワーク デバイスへの SSH 接続を有効にする」（P.C-36）
- 「シグニチャに対してブロッキングが発生していない」（P.C-37）
- 「マスター ブロッキング センサーの設定を確認する」（P.C-38）

ブロッキングのトラブルシューティング

ARC の設定を終えた後は、**show version** コマンドを使用して、ARC が正しく実行されているかどうかを確認できます。ネットワーク デバイスに ARC が接続されていることを確認するには、**show statistics network-access** コマンドを使用します。

（注）　ARC は、以前は Network Access Controller と呼ばれていました。この名前は IPS 5.1 から変更されましたが、IDM、IME、および CLI にはまだ Network Access Controller、**nac**、および **network-access** として表示されます。

ARC のトラブルシューティングを行うには、次の手順を実行します。

1. ARC が実行中であることを確認します。
2. ARC がネットワーク デバイスに接続されていることを確認します。
3. 特定のシグニチャのイベント アクションが、ホストのブロックに設定されていることを確認します。

4. マスター ブロッキング センサーが正しく設定されていることを確認します。

詳細情報

- ARC が実行中であることを確認する手順については、「ARC が実行中であることを確認する」（P.C-31）を参照してください。
- ARC が接続されていることを確認する手順については、「ARC 接続がアクティブであることを確認する」（P.C-32）を参照してください。
- イベント アクションがホストのブロックに設定されていることを確認する手順については、「シグニチャに対してブロッキングが発生していない」（P.C-37）を参照してください。
- マスター ブロッキング センサーが正しく設定されていることを確認する手順については、「マスター ブロッキング センサーの設定を確認する」（P.C-38）を参照してください。
- ARC アーキテクチャの詳細については、「Attack Response Controller」（P.A-12）を参照してください。

ARC が実行中であることを確認する

ARC が実行中であることを確認するには、**show version** コマンドを使用します。MainApp が実行されていない場合、ARC を実行できません。ARC は MainApp の一部です。

ARC が実行中であることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　MainApp が実行中であることを確認します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(0.346)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S512.0              2010-09-08
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
No license present
Sensor up-time is 21:09.
Using 10276M out of 11899M bytes of available memory (86% usage)
system is using 28.4M out of 160.0M bytes of available disk space (18% usage)
application-data is using 64.9M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 58.7M out of 71.7M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
AnalysisEngine     S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CollaborationApp   S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CLI                S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500
```

```
Upgrade History:

  IPS-K9-7.1-0.346-E4   10:53:07 UTC Mon Sep 27 2010

Recovery Partition Version 1.1 - 7.1(0.346)E4

Host Certificate Valid from: 26-Sep-2010 to 26-Sep-2012
ips-ssp#
```

ステップ 3　MainApp の表示が `Not Running` である場合、ARC は失敗しています。TAC にお問い合わせください。

詳細情報

IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャについて」を参照してください。

ARC 接続がアクティブであることを確認する

ARC の統計情報で State が `Active` でない場合は、問題が発生しています。

統計情報で State が Active であることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC が接続状態にあることを確認します。

出力の State セクションを調べて、すべてのデバイスが接続状態にあることを確認します。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
ips-ssp#
```

ステップ 3　ARC が接続状態にない場合は、繰り返し発生しているエラーを探します。

```
ips-ssp# show events error hh:mm:ss month day year | include : nac
```

例

```
ips-ssp# show events error 00:00:00 Apr 01 2007 | include : nac
```

ステップ 4　ソフトウェアのアップデートが最新のものであることを確認します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S512.0              2010-09-08
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
No license present
Sensor up-time is 21:09.
Using 10276M out of 11899M bytes of available memory (86% usage)
system is using 28.4M out of 160.0M bytes of available disk space (18% usage)
application-data is using 64.9M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 58.7M out of 71.7M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
AnalysisEngine     S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CollaborationApp   S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CLI                S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500

Upgrade History:

  IPS-K9-7.1-1-E4   10:53:07 UTC Mon Sep 27 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 26-Sep-2010 to 26-Sep-2012
ips-ssp#
```

（注）　最新のものではない場合は、Cisco.com からダウンロードします。

ステップ 5　ARC の既知の DDTS については、ソフトウェア アップグレードに添付の Readme を参照してください。

ステップ 6　デバイスごとに設定（ユーザ名、パスワード、IP アドレス）が正しいことを確認します。

ステップ 7　ネットワーク デバイスごとにインターフェイスと方向が正しいことを確認します。

ステップ 8　ネットワーク デバイスで SSH-3DES が使用されている場合は、デバイスへの SSH 接続をすでにイネーブルにしていることを確認します。

ステップ 9　制御対象の各デバイスで各インターフェイスおよび方向が正しいことを確認します。

詳細情報

- 最新の Cisco IPS ソフトウェアを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。
- デバイスの設定の詳細については、「デバイスのアクセスに関する問題点」（P.C-34）を参照してください。
- 各ネットワーク デバイスのインターフェイスと方向を確認する手順については、「ネットワーク デバイス上のインターフェイスおよび方向を確認する」（P.C-35）を参照してください。
- SSH をイネーブルにする手順については、「ネットワーク デバイスへの SSH 接続を有効にする」（P.C-36）を参照してください。

デバイスのアクセスに関する問題点

ARC は、管理しているデバイスにアクセスできない場合があります。管理対象のデバイスの IP アドレス、ユーザ名、およびパスワードが正しいことと、インターフェイスおよび方向が正しく設定されていることを確認してください。

（注） SSH デバイスが SSH 1.5 をサポートしている必要があります。センサーは、SSH 2.0 をサポートしていません。

デバイスへのアクセスの問題についてトラブルシューティングを行うには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　管理対象デバイスの IP アドレスを確認します。

```
ips-ssp# configure terminal
ips-ssp (config)# service network-access
ips-ssp(config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ------------------------------------------------
      profile-name: r7200
```

```
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
   ------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.54
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ------------------------------------------------
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ------------------------------------------------
   ------------------------------------------------
ips-ssp(config-net)#
```

ステップ 3　デバイスに手動で接続して、正しいユーザ名、正しいパスワード、および有効なパスワードを使用していること、さらにセンサーからデバイスに到達可能であることを確認します。

a. サーバ アカウントにログインします。

b. Telnet または SSH を使用してネットワーク デバイスに接続し、設定を確認します。

c. デバイスに到達できることを確認します。

d. ユーザ名とパスワードを確認します。

ステップ 4　各ネットワーク デバイスの各インターフェイスおよび方向が正しいことを確認します。

詳細情報

各ネットワーク デバイスのインターフェイスと方向を確認する手順については、「ネットワーク デバイス上のインターフェイスおよび方向を確認する」（P.C-35）を参照してください。

ネットワーク デバイス上のインターフェイスおよび方向を確認する

制御対象の各デバイス上で各インターフェイスおよび方向が正しいことを確認するには、手動ブロックを不正なホストに送信し、ルータの ACL 内のブロックされているアドレスについて拒否エントリが存在するかどうかを確認できます。

（注） IDM を使用して手動ブロックを実行するには、[Monitoring] > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] を選択します。IME を使用して手動ブロックを実行するには、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] を選択します。

不正なホストに対する手動ブロックを開始するには、次の手順を実行します。

ステップ 1　ARC 一般サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)# general
```

ステップ 2　不正なホストの IP アドレスの手動ブロックを開始します。

```
ips-ssp(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 3　一般サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 4　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ステップ 5　ルータに Telnet 接続して、ブロックされたアドレスの拒否エントリがルータの ACL 内に存在することを確認します。手順については、ルータのマニュアルを参照してください。

ステップ 6　手動ブロックを削除するにはステップ 1 ～ 4 を繰り返します。ただし、ステップ 2 では、コマンドの前に **no** を配置します。

```
ips-ssp(config-net-gen)# no block-hosts 10.16.0.0
```

ネットワーク デバイスへの SSH 接続を有効にする

ネットワーク デバイスの通信プロトコルとして SSH-3DES を使用している場合は、デバイス上で該当するプロトコルを必ずイネーブルにしておく必要があります。

ネットワーク デバイスへの SSH 接続を有効にするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
ips-ssp# configure terminal
```

ステップ 3　SSH をイネーブルにします。

```
ips-ssp(config)# ssh host blocking_device_ip_address
```

ステップ 4　デバイスを受け入れるよう指示するメッセージが表示されたら、**yes** と入力します。

シグニチャに対してブロッキングが発生していない

特定のシグニチャに対してブロッキングが発生していない場合は、イベント アクションがホストをブロックするように設定されているかどうかチェックします。

特定のシグニチャに対してブロッキングが発生していることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service signature-definition sig0
ips-ssp(config-sig)#
```

ステップ 3　イベント アクションがホストをブロックするように設定されていることを確認します。

（注）　アラートを受信するには、イベント アクションを設定するときに必ず **produce-alert** を追加する必要があります。

```
ips-ssp(config-sig)# signatures 1300 0
ips-ssp(config-sig-sig)# engine normalizer
ips-ssp(config-sig-sig-nor)# event-action produce-alert|request-block-host
ips-ssp(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
         default-signatures-only
         -----------------------------------------------
            specify-service-ports
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-max-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-min-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
--MORE--
```

ステップ 4　シグニチャ定義サブモードを終了します。

```
ips-ssp(config-sig-sig-nor)# exit
ips-ssp(config-sig-sig)# exit
ips-ssp(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 5　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

マスター ブロッキング センサーの設定を確認する

マスター ブロッキング センサーが適切に設定されていることを確認するには、あるいは適切に設定されていないマスター ブロッキング センサーのトラブルシューティングを行うには、**show statistics network-access** コマンドを使用します。リモート マスター ブロッキング センサーが TLS を使用して Web アクセスを行っている場合は、転送センサーが TLS の信頼できるホストとして設定されていることを確認します。

マスター ブロッキング センサーの設定を確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を表示し、マスター ブロッキング センサーのエントリが統計情報にあることを確認します。

```
ips-ssp# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 3　統計情報にマスター ブロッキング センサーが表示されていない場合は、それを追加してください。

ステップ 4　不正なホスト IP アドレスへの手動ブロックを開始し、マスター ブロッキング センサーがブロックを開始していることを確認します。

```
ips-ssp# configure terminal
ips-ssp(config)# service network-access
ips-ssp(config-net)# general
ips-ssp(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 5　ネットワーク アクセス一般サブモードを終了します。

```
ips-ssp(config-net-gen)# exit
ips-ssp(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ステップ 7　ARC の統計情報にブロックが表示されていることを確認します。

```
ips-ssp# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

ステップ 8　マスター ブロッキング センサー ホストの CLI にログインし、**show statistics network-access** コマンドを使用して、マスター ブロッキング センサーの ARC の統計情報にブロックも表示されていることを確認します。

```
ips-ssp# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 9　リモート マスター ブロッキング センサーが TLS を使用して Web アクセスを行っている場合は、転送センサーが TLS ホストとして設定されていることを確認します。

```
ips-ssp# configure terminal
ips-ssp(config)# tls trust ip master_blocking_sensor_ip_address
```

詳細情報

センサーをマスター ブロッキング センサーとして設定する手順については、「センサーをマスター ブロッキング センサーにする設定」（P.14-29）を参照してください。

ロギング

ここでは、ロギングについて説明します。次のような構成になっています。

- 「ロギングの概要」（P.C-39）
- 「デバッグ ロギングをイネーブルにする」（P.C-40）
- 「ゾーン名」（P.C-43）
- 「SysLog に cidLog メッセージを転送する」（P.C-44）

ロギングの概要

TAC では、トラブルシューティングのためにデバッグ ロギングをオンにすることを推奨する場合もあります。ロガーは、さまざまなロギング ゾーンのロギングの重大度を制御することにより、各アプリケーションが生成するログ メッセージの種類を制御します。デフォルトでは、デバッグ ロギングはオンではありません。個別ゾーン制御を有効にすると、各ゾーンでは設定されたロギング レベルを使用します。個別ゾーン制御を有効にしなければ、すべてのゾーンで同じロギング レベルが使用されます。

デバッグ ロギングをイネーブルにする

注意　デバッグ ロギングをイネーブルにすることは、パフォーマンスに重大な影響を与えるので、TAC によって指示された場合にのみ使用する必要があります。

デバッグ ロギングをイネーブルにするには、次の手順を実行できます。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　log.conf ファイルを編集し、追加のログ ステートメントを収容するためにログのサイズを増やします。

```
vi /usr/cids/idsRoot/etc/log.conf
```

ステップ 3　`fileMaxSizeInK=500` を `fileMaxSizeInK=5000` に変更します。

ステップ 4　ファイルのゾーンと CID セクションの位置を特定し、重大度を debug に設定します。

```
severity=debug
```

ステップ 5　ファイルを保存し、vi エディタを終了し、サービス アカウントを終了します。

ステップ 6　CLI に管理者としてログインします。

ステップ 7　マスター コントロール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service logger
ips-ssp(config-log)# master-control
```

ステップ 8　すべてのゾーンに対するデバッグ ロギングをイネーブルにします。

```
ips-ssp(config-log-mas)# enable-debug true
ips-ssp(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   -----------------------------------------------
ips-ssp(config-log-mas)#
```

ステップ 9　個々のゾーン制御をオンにします。

```
ips-ssp(config-log-mas)# individual-zone-control true
ips-ssp(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
ips-ssp(config-log-mas)#
```

ステップ 10　マスター ゾーン制御を終了します。

```
ips-ssp(config-log-mas)# exit
```

ステップ 11　ゾーン名を表示します。

```
ips-ssp(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
   -----------------------------------------------
```

```
   zone-control (min: 0, max: 999999999, current: 14)
   ------------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
ips-ssp(config-log)#
```

ステップ 12　特定のゾーンの重大度レベル（debug、timing、warning、または error）を変更します。

```
ips-ssp(config-log)# zone-control IdsEventStore severity error
ips-ssp(config-log)# show settings
   master-control
   ------------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ------------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ------------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
```

```
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   -----------------------------------------------
ips-ssp(config-log)#
```

ステップ 13　特定のゾーンのデバッグを有効にします。

```
ips-ssp(config-log)# zone-control nac severity debug
ips-ssp(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   -----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
```

```
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: debug default: warning
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
    ------------------------------------------------
ips-ssp(config-log)#
```

ステップ 14　ロガー サブモードを終了します。

```
ips-ssp(config-log)# exit
Apply Changes:?[yes]:
```

ステップ 15　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

それぞれのゾーン名が示す内容に関するリストについては、「ゾーン名」（P.C-43）を参照してください。

ゾーン名

表 C-1 にデバッグ ロガー ゾーン名をリストします。

表 C-1　デバッグ ロガー ゾーン名

ゾーン名	説明
AD	異常検出ゾーン
AuthenticationApp	認証ゾーン
Cid	一般的なロギング ゾーン
Cli	CLI ゾーン
IdapiCtlTrans	すべての制御トランザクション ゾーン
IdsEventStore	イベント ストア ゾーン
MpInstaller	IDSM-2 マスター パーティション インストーラ ゾーン

表 C-1　デバッグ ロガー ゾーン名 （続き）

ゾーン名	説明
cmgr	Card Manager サービス ゾーン[1]
cplane	コントロール プレーン ゾーン[2]
csi	CIDS Servlet インターフェイス[3]
ctlTransSource	発信制御トランザクション ゾーン
intfc	インターフェイス ゾーン
nac	ARC ゾーン
rep	レピュテーション ゾーン
sched	自動更新スケジューラ ゾーン
sensorApp	分析エンジン ゾーン
tls	SSL および TLS ゾーン

1. Card Manager サービスは、シャーシ内のモジュール間で制御と状態の情報を交換するために AIP-SSM で使用されます。
2. コントロール プレーンは、AIP-SSM で Card Manager が使用するトランスポート通信層です。
3. CIDS servlet インターフェイスは、CIDS Web サーバと servlet 間のインターフェイス層です。

詳細情報

IPS ロガー サービスの詳細については、「ロガー」（P.A-19）を参照してください。

SysLog に cidLog メッセージを転送する

cidLog メッセージを syslog に転送することが有用な場合があります。

cidLog メッセージを syslog に転送するには、次の手順を実行します。

ステップ 1　idsRoot/etc/log.conf ファイルに進みます。

ステップ 2　次の変更を加えます。

a. [logApp] `enabled=false` を設定します。

`enabled=true` はコメント化されます。これは `enabled=false` がデフォルトであるためです。

b. [drain/main] `type=syslog` を設定します。

次の例に、ロギング コンフィギュレーション ファイルを示します。

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
```

```
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

syslog の出力が syslog ファシリティ local6 に送信され、syslog メッセージ プロパティとは次の対応関係があります。

```
LOG_DEBUG,          //    デバッグ
LOG_INFO,                //      タイミング
LOG_WARNING,    //      警告
LOG_ERR,                 //      エラー
LOG_CRIT                 //       重大
```

（注） /etc/syslog.conf の該当するファシリティが適切な優先順位で有効になっていることを確認します。

注意 syslog は logApp よりもかなり時間がかかります（1 秒あたり 50 メッセージ程度。logApp は 1 秒あたり 1000 メッセージ程度）。デバッグの重大度は、一度に 1 つのゾーンでのみイネーブルにすることを推奨します。

ソフトウェアのアップグレード

ここでは、ソフトウェア アップグレードのトラブルシューティングに役立つ情報を提供します。次のような構成になっています。

- 「アップグレード エラー」（P.C-45）
- 「適用するアップデートと前提条件」（P.C-46）
- 「自動アップデートに関する問題」（P.C-46）
- 「センサーに格納されたアップデートを使用してセンサーを更新する」（P.C-47）

アップグレード エラー

IPS をアップグレードすると、分析エンジンが実行されていないことを示すエラーを受け取る場合があります。

```
ips-ssp# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.1-1-E4.pkg
Password: ********
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

このエラーを受け取った場合は、アップグレードを再試行する前に分析エンジンを実行する必要があります。このエラーの原因は多くの場合、現在実行中のバージョンの欠陥です。センサーのリブートを試みて、リブートしたら **setup** コマンドを実行し、仮想センサー vs0 からインターフェイスを削除します。トラフィックがモニタされていないと、分析エンジンは通常アップ状態で、実行中となります。この時点でアップグレードが可能です。アップグレードを終えたら、**setup** コマンドを使用して仮想センサー vs0 にインターフェイスを追加し直します。

または、システム イメージ ファイルを使用して、必要なバージョンに直接、センサーのイメージを再作成できます。イメージの再作成処理では分析エンジンが実行中であるかどうかがチェックされないため、センサーのイメージを再作成し、エラーを回避できます。

注意　システム イメージ ファイルを使用してイメージを再作成すると、すべての設定がデフォルトに復元されます。

詳細情報

- **setup** コマンドの詳細については、第 3 章「IPS SSP の初期化」を参照してください。
- センサーのイメージの再作成の詳細については、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。

適用するアップデートと前提条件

ソフトウェアのサービス パックのバージョンとマイナーおよびメジャー バージョンは正しいものを使用する必要があります。新しいソフトウェアの適用に関して問題が発生している場合は、適切なアップデートを適切な前提条件で実行しているかどうかを確認します。

- シグニチャ アップデートには、ファイル名にリストされている最小バージョンおよびエンジン バージョンが必要です。
- エンジン アップデートには、エンジン アップデート ファイル名のメジャーまたはマイナー バージョンが必要です。サービス パックを適用するには、正しいマイナー バージョンが必要です。
- マイナー バージョンを適用するには、正しいメジャー バージョンが必要です。
- メジャー バージョンを適用するには、前のメジャー バージョンが必要です。

詳細情報

IPS ソフトウェア ファイル名を解釈する方法については、「IPS ソフトウェアのバージョン管理」（P.19-3）を参照してください。

自動アップデートに関する問題

次のリストに、自動アップデートのトラブルシューティングに役立つ情報を示します。

- TCPDUMP を実行します。
  - サービス アカウントを作成します。root に **su** して、コマンド/コントロール インターフェイスで TCPDUMP を実行し、センサーと FTP サーバ間のパケットをキャプチャします。
  - **upgrade** コマンドを使用して、センサーを手動でアップグレードします。
  - FTP サーバから返されるエラーの TCPDUMP 出力を調べます。

- センサーが正しいディレクトリ内にあることを確認します。

  ディレクトリを正しく指定する必要があります。これが、Windows FTP サーバにおける問題の原因です。場合によっては、ディレクトリ名の前に余分に「/」を 1 つ、あるいは「/」を 2 つ付ける必要があります。これを確認するには、固有の FTP 接続を介して送信された TCPDUMP 出力に示されているのと同じ FTP コマンドを使用します。

- MS-DOS ファイル構造体ではなく UNIX ファイル構造体をエミュレートするには、Windows FTP サーバ セットアップ オプションを使用する必要があります。
- SCP を使用する場合は、SSH ホスト キーを既知のホスト リストに必ず追加しておきます。

手動による **upgrade** コマンドを試してから、自動アップデートを試みます。**upgrade** コマンドでは動作するが、自動アップデートでは動作しない場合は、次の手順を実行します。

- センサーに搭載された IPS ソフトウェア バージョンを特定します。
- 自動アップデートにパスワードが設定されていることを確認します。自動アップデートのパスワードは、手動アップデートで使用されるパスワードと一致する必要があります。
- FTP サーバ内のファイル名が、Cisco.com の [Downloads] に表示されるものと同じであることを確認します。これには大文字の使用も含まれます。一部の Windows FTP サーバは大文字化されていないファイルへのアクセスを許可しますが、名前が変更されているのでセンサーは最終的にファイルを拒否します。
- 必要であれば、自動アップデートで TCPDUMP を実行します。正常な手動アップデートを異常な自動アップデートと比較し、そこからトラブルシューティングを行うことができます。

詳細情報

- 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。
- センサーのイメージを再作成する手順については、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。
- SSH 既知ホスト リストにホストを追加する手順については、「SSH 既知ホスト リストへのホストの追加」（P.4-35）を参照してください。
- ソフトウェア バージョンを特定する手順については、「バージョン情報の表示」（P.C-57）を参照してください。

センサーに格納されたアップデートを使用してセンサーを更新する

アップデート パッケージをセンサー上の /var ディレクトリに格納し、必要に応じて、そこからセンサーを更新することができます。

センサーに格納されたアップデートを使用してセンサーを更新するには、次の手順を実行します。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　Cisco.com からアップデート パッケージファイルを取得します。

ステップ 3　FTP または SCP を使用して、アップデート ファイルをセンサーの /usr/cids/idsRoot/var ディレクトリに送信します。

ステップ 4　ファイルの権限を設定します。

```
chmod 644 ips_package_file_name
```

ステップ 5　サービス アカウントを終了します。

ステップ 6　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

ステップ 7　センサーのホスト キーを格納します。

```
ips-ssp# configure terminal
ips-ssp(config)# service ssh
ips-ssp(config-ssh)# rsa1-keys sensor_ip_address
```

ステップ 8　センサーをアップグレードします。

```
ips-ssp(config)# upgrade scp://service@Sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

詳細情報

Cisco IPS ソフトウェアを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

IPS SSP のトラブルシューティング

（注）　IPS SSP のソフトウェアのアーキテクチャは、4200 シリーズ センサーのものと同じです。「センサーのトラブルシューティング」（P.C-17）に記載されたトラブルシューティング ツールと同じものを使用できます。

ここでは、IPS SSP に関するトラブルシューティングの情報を示します。次のような構成になっています。

- 「フェールオーバー シナリオ」（P.C-48）
- 「ヘルスおよびステータス情報」（P.C-49）
- 「IPS スイッチポートで停止したトラフィック フロー」（P.C-52）

フェールオーバー シナリオ

シグニチャおよびシグニチャ エンジンのアップデートと、メジャーおよびマイナー アップデートを適用するときには、次のフェールオーバー シナリオが ASA 5585-X に適用されます。

フェールオープン モードの単一の ASA 5585-X

- シグニチャまたはシグニチャ エンジンのアップデート時に ASA 5585-X がフェールオープン モードに設定されている場合は、設定変更があっても、トラフィックは通過します。
- マイナーまたはメジャー アップデート時に ASA 5585-X がフェールオープン モードに設定されている場合は、SensorApp がクラッシュしても、トラフィックは通過します。

フェールクローズ モードの単一の ASA 5585-X

- シグニチャまたはシグニチャ エンジンのアップデート時に ASA 5585-X がフェールクローズ モードに設定されている場合に、設定変更があると、トラフィックは停止します。
- マイナーまたはメジャー アップデート時に ASA 5585-X がフェールクローズ モードに設定されている場合に、SensorApp がクラッシュすると、トラフィックは停止します。

フェールオープン モードでの 2 台の ASA 5585-X

- シグニチャまたはシグニチャ エンジンのアップデート時に ASA 5585-X がフェールオープン モードに設定されている場合は、設定変更があっても、トラフィックは通過します。
- マイナーまたはメジャー アップデート時に ASA 5585-X がフェールオープン モードに設定されている場合に、SensorApp がクラッシュすると、トラフィックはフェールオーバーされます。

フェールクローズ モードでの 2 台の ASA 5585-X

- シグニチャまたはシグニチャ エンジンのアップデート時に ASA 5585-X がフェールクローズ モードに設定されている場合に、設定変更があると、トラフィックは停止します。
- マイナーまたはメジャー アップデート時に ASA 5585-X がフェールクローズ モードに設定されている場合に、SensorApp がクラッシュすると、トラフィックはフェールオーバーされます。

設定例

プライマリ ASA 5585-X には、次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

セカンダリ ASA 5585-X には、次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

ヘルスおよびステータス情報

IPS SSP の一般的なヘルス情報を表示するには、**show module 1 details** コマンドを使用します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.1(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
```

```
Mgmt TLS enabled    true
asa
```

出力には、IPS SSP がアップ状態であることが表示されます。ステータスが Down を示している場合は、**hw-module module 1 reset** コマンドを使用してリセットできます。

```
asa# hw-module module 1 reset

The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
Data plane Status:  Not Applicable
Status:             Shutting Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
Data plane Status:  Not Applicable
Status:             Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.1(1)E4
Data plane Status:  Not Applicable
Status:             Init
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
```

```
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Reload
App. Status Desc:   Starting up
App. version:       7.1(1)E4
Data plane Status:  Down
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.1(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

IPS SSP の復旧に問題がある場合は、**debug module-boot** コマンドを使用して、ブート時に出力を表示します。TFTP サーバに適切な IP アドレスを使用しており、TFTP サーバに適切なファイルがあることを確認します。その後、再び **hw-module module 1 recover** コマンドを使用してモジュールを復元します。

```
ips-ssp# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.10.10.10//IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img
Port IP Address [0.0.0.0]: 10.10.10.11
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.10.10.254

asa(config)# debug module-boot
debug module-boot enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2010
Slot-1 141> Platform ASA5585-SSP-IPS20
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
```

```
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=192.0.2.3
Slot-1 147>   SERVER=192.0.2.15
Slot-1 148>   GATEWAY=192.0.2.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSP-K9-sys-1.1-a-7.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img@192.0.2.15 via 192.0.2.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2010
Slot-1 161> Platform ASA5585-SSP-IPS20
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=192.0.2.3
Slot-1 167>   SERVER=192.0.2.15
Slot-1 168>   GATEWAY=192.0.2.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSP_10-K9-sys-1.1-a-7.1-0.1.img@192.0.2.15 via 192.0.2.254
```

IPS スイッチポートで停止したトラフィック フロー

問題　IPS SSP がリセットされるか、シャットダウンされると、IPS SSP (1/x) にあるポート上のトラフィックは適応型セキュリティを通過しなくなります。このことは、トラフィックが IPS にモニタされているかどうかに関係なく、これらのポートを通過するすべてのトラフィックに影響します。IPS SSP がリセットまたはシャットダウンされると、ポート上のリンクがダウンします。

考えられる原因　IPS SSP (1/x) にあるポートを使用し、何らかのメカニズムで IPS SSP をリセットまたはシャットダウンしました。

ソリューション　適応型セキュリティ アプライアンス (0/x) 上のポートは、IPS SSP がリセットまたはシャットダウンされてもリンクを失わないので、代わりにこれらのポートを使用してください。

情報の収集

次に示す CLI コマンドおよびスクリプトを使用すれば、問題が発生した際にセンサーに関する情報を収集し、センサーの状態を診断することができます。**show tech-support** コマンドを使用してセンサーのすべての情報を収集することも、ここで示す他の個々のコマンドを使用して特定の情報を収集することもできます。ここでは、次の項目について説明します。

- 「ヘルスおよびネットワーク セキュリティ情報」（P.C-53）
- 「技術サポート情報」（P.C-53）

- 「バージョン情報」（P.C-57）
- 「統計情報」（P.C-60）
- 「インターフェイス情報」（P.C-70）
- 「イベント情報」（P.C-72）
- 「cidDump スクリプト」（P.C-76）
- 「Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス」（P.C-77）

ヘルスおよびネットワーク セキュリティ情報

特権 EXEC モードで **show health** コマンドを使用して、センサーの全体的なヘルス ステータス情報を表示します。ヘルス ステータス カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

注意　センサーを初めて起動するときは、センサーが完全に起動して動作するまで、特定のヘルス メトリック ステータスが赤色になりますが、これは正常な状態です。

センサーの全体的なヘルス ステータスを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　センサーのヘルスおよびセキュリティ ステータスを表示します。

```
ips-ssp# show health
Overall Health Status                                  Red
Health Status for Failed Applications                  Green
Health Status for Signature Updates                    Green
Health Status for License Key Expiration               Red
Health Status for Running in Bypass Mode               Green
Health Status for Interfaces Being Down                Red
Health Status for the Inspection Load                  Green
Health Status for the Time Since Last Event Retrieval  Green
Health Status for the Number of Missed Packets         Green
Health Status for the Memory Usage                     Not Enabled
Health Status for Global Correlation                   Red
Health Status for Network Participation                Not Enabled

Security Status for Virtual Sensor vs0   Green
ips-ssp#
```

技術サポート情報

show tech-support コマンドは、センサーのすべてのステータスおよび設定情報をキャプチャするのに有用です。ここでは、**show tech-support** コマンドについて説明します。次のような構成になっています。

- 「show tech-support コマンドの概要」（P.C-54）
- 「技術サポート情報の表示」（P.C-54）
- 「技術サポート コマンドの出力」（P.C-55）

show tech-support コマンドの概要

show tech-support コマンドはセンサーにおけるすべてのステータスと情報をキャプチャし、現在の設定、バージョン情報、cidDump 情報などが含まれます。出力は、大きくなり 1 MB を超えることもあります。出力はリモート システムに転送できます。リモート システムに出力をコピーする手順については、「技術サポート情報の表示」（P.C-54）を参照してください。

（注）　TAC に連絡する前に **show tech-support** コマンドを必ず実行してください。

技術サポート情報の表示

show tech-support [**page**] [**destination-url** *destination_url*] コマンドを使用して、画面にシステム情報を表示するか、その情報を特定の URL に送信します。この情報は、TAC とのトラブルシューティング ツールとして使用できます。

次のパラメータはオプションです。

- **page**：一度に 1 ページの情報として出力を表示します。Enter を押して出力の次の行を表示するか、Space を使用して次のページの情報を表示します。
- **destination-url**：HTML としてフォーマットし、このコマンドに続く宛先に送信する必要がある情報を示します。このキーワードを使用すると、出力は画面に表示されません。
- *destination_url*：HTML としてフォーマットする必要がある情報を示します。URL は、情報を送信する宛先を示します。このキーワードを使用しないと、画面に情報が表示されます。

技術サポート情報を表示するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　画面上に出力を表示します。システム情報が画面上に一度に 1 ページずつ表示されます。次のページを表示するには Space を押します。プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

```
ips-ssp# show tech-support page
```

ステップ 3　出力（HTML フォーマット）をファイルに送信するには、次の手順を実行します。

a.　次のコマンドを入力し、その後に有効な宛先を指定します。

```
ips-ssp# show tech-support destination-url destination_url
```

次に示す種類の宛先を指定できます。

- **ftp:**：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`ftp:[[//username@location]/relativeDirectory]/filename` または `ftp:[[//username@location]//absoluteDirectory]/filename` です。
- **scp:**：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`scp:[[//username@]location]/relativeDirectory]/filename` または `scp:[[//username@]location]//absoluteDirectory]/filename` です。

たとえば、技術サポート出力をファイル `/absolute/reports/sensor1Report.html` に送信するには、

```
ips-ssp# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

`password:` プロンプトが表示されます。

b.　このユーザ アカウントのパスワードを入力します。`Generating report:` メッセージが表示されます。

技術サポート コマンドの出力

show tech-support コマンド出力の例を次に示します。

（注） この出力例では、コマンドの先頭部分を示すと共に、インターフェイス、ARC、およびcidDump サービスに関する情報を一覧表示します。

```
ips-ssp# show tech-support page
System Status Report
This Report was generated on Tue Sep 28 16:15:12 2010.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S512.0              2010-09-08
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
No license present
Sensor up-time is 22:07.
Using 10276M out of 11899M bytes of available memory (86% usage)
system is using 28.4M out of 160.0M bytes of available disk space (18% usage)
application-data is using 64.9M out of 171.4M bytes of available disk space (40% usage)
boot is using 58.7M out of 71.7M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


MainApp            S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
AnalysisEngine     S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CollaborationApp   S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500   Running
CLI                S-SPYKER_2010_SEP_27_10_39_7_1_0_346   (Release)   2010-09-27
T10:41:56-0500

Upgrade History:

  IPS-K9-7.1-0.346-E4   10:53:07 UTC Mon Sep 27 2010

Recovery Partition Version 1.1 - 7.1(0.346)E4

Host Certificate Valid from: 26-Sep-2010 to 26-Sep-2012


Output from show interfaces
Interface Statistics
   Total Packets Received = 6221044
   Total Bytes Received = 18446744071630494336
   Missed Packet Percentage = 2
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_1000
```

```
   Link Duplex = Auto_Full
   Total Packets Received = 363587
   Total Bytes Received = 22281175
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 79511
   Total Bytes Transmitted = 48942270
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface PortChannel0/0
   Interface function = Sensing interface
   Description =
   Media Type = backplane
   Default Vlan = 0
   InlineMode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Up
   Admin Enabled Status = Enabled
   Link Speed = Auto_10000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 2
   Total Packets Received = 6221044
   Total Bytes Received = 2215910016
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 343056
   Total Undersize Packets Received = 0
   Total Receive Errors = 175751
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 6221044
   Total Bytes Transmitted = 2215910016
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 343056
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/1
   Interface function = Reserved for future use

Output from show statistics authentication
General
   totalAuthenticationAttempts = 0
   failedAuthenticationAttempts = 0

Output from show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 79585
   Processing Load Percentage
         Thread    5 sec   1 min   5 min
         0         1       1       1
         1         1       1       1
         2         1       1       1
         3         1       1       1
         Average   1       1       1

   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 136
   The rate of bytes per second = 45157
   Receiver Statistics
      Total number of packets processed since reset = 3347548
```

```
   Total number of IP packets processed since reset = 3347548
Transmitter Statistics
   Total number of packets transmitted = 6221065
   Total number of packets denied = 0
   Total number of packets reset = 0
Fragment Reassembly Unit Statistics
   Number of fragments currently in FRU = 0--MORE--
```

バージョン情報

show version コマンドは、センサー情報を取得するのに有用です。ここでは、**show version** コマンドについて説明します。次のような構成になっています。

- 「show version コマンドの概要」（P.C-57）
- 「バージョン情報の表示」（P.C-57）

show version コマンドの概要

show version コマンドは、センサーの基本的な情報を示します。さらに、障害が発生している場所を示すことができます。次のような情報が提供されます。

- 実行中のアプリケーション
- アプリケーションのバージョン
- ディスクおよびメモリの用途
- アプリケーションのアップグレード履歴

（注）　IDM から同じ情報を取得するには、[Monitoring] > [Sensor Monitoring] > [Support Information] > [Diagnostics Report] を選択します。IME から同じ情報を取得するには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Diagnostics Report] を選択します。

バージョン情報の表示

インストールされているすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の設定を表示するには、**more current-config** コマンドを使用します。

バージョンおよび設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　バージョン情報を表示します。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
```

```
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40% usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

ips-ssp#
```

（注） --MORE-- というプロンプトが表示された場合、Space を押して詳細な情報を表示するか、Ctrl キーを押した状態で C キーを押して出力をキャンセルし、CLI プロンプトに戻ります。

ステップ 3　設定情報を表示します。

（注） **more current-config** または **show configuration** コマンドを使用できます。

```
ips-ssp# more current-config
! ------------------------------
! Current configuration last modified Fri Oct 22 14:04:10 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S518.0   2010-10-04
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.148.15/24,10.89.148.254
```

```
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 64.102.255.40
port 8080
exit
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
signatures 2004 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
```

```
service analysis-engine
virtual-sensor vs0
physical-interface PortChannel0/0
exit
exit
ips-ssp#
```

統計情報

show statistics コマンドは、センサーのサービスの状態を検査するのに有用です。ここでは、**show statistics** コマンドについて説明します。次のような構成になっています。

- 「show statistics コマンドの概要」（P.C-60）
- 「統計情報の表示」（P.C-61）

show statistics コマンドの概要

センサーのサービス状態のスナップショットを表示するには、**show statistics** コマンドを使用します。次のサービスが統計情報を提供します。

- 分析エンジン
- 認証
- 拒否攻撃者
- イベント サーバ
- イベント ストア
- ホスト
- ロガー
- 攻撃応答（旧称ネットワーク アクセス）
- 通知
- SDEE サーバ
- トランザクション サーバ
- トランザクション ソース
- Virtual Sensor
- Web サーバ

（注）　IDM から同じ情報を取得するには、[Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。IME から同じ情報を取得するには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

統計情報の表示

show statistics [analysis-engine | anomaly-detection | authentication | denied-attackers | event-server | event-store | external-product-interface | global-correlation | host | logger | network-access | notification | os-identification | sdee-server | transaction-server | virtual-sensor | web-server] [clear] コマンドを使用して、各センサー アプリケーションの統計情報を表示します。

show statistics {**anomaly-detection** | **denied-attackers** | **os-identification** | **virtual-sensor**} [***name*** | **clear**] を使用して、すべての仮想センサーについてこれらのコンポーネントの統計情報を表示します。仮想センサー名を指定すると、その仮想センサーの統計情報のみが表示されます。

（注） 分析エンジン、異常検出、ホスト、ネットワーク アクセス、または OS 識別アプリケーションには、**clear** オプションを使用できません。

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジンの統計情報を表示します。

```
ips-ssp# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
ips-ssp#
```

ステップ 3　異常検出の統計情報を表示します。

```
ips-ssp# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
```

```
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp-4240#
```

ステップ 4　認証の統計情報を表示します。

```
ips-ssp# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
ips-ssp#
```

ステップ 5　システムの拒否攻撃者の統計情報を表示します。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


ips-ssp#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
ips-ssp# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
ips-ssp#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
ips-ssp# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
ips-ssp#
```

ステップ 8　グローバル相関の統計情報を表示します。

```
ips-ssp# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
ips-ssp#
```

ステップ 9　ホストの統計情報を表示します。

```
ips-ssp# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2011
   Command Control Port Device = FastEthernet0/0
Network Statistics
```

```
   fe0_0     Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2011
    =   Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
    =   Error: httpResponse status returned:  Unauthorized
   lastInstallAttempt = N/A
   nextAttempt = 16:26:30 CDT Tue Jun 17 2011

ips-ssp#
```

ステップ 10　ロギング アプリケーションの統計情報を表示します。

```
ips-ssp# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
ips-ssp#
```

ステップ 11　ARC の統計情報を表示します。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
```

```
      EnableNvramWrite = false
      EnableAclLogging = false
      AllowSensorBlock = false
      BlockMaxEntries = 11
      MaxDeviceInterfaces = 250
      NetDevice
         Type = PIX
         IP = 10.89.150.171
         NATAddr = 0.0.0.0
         Communications = ssh-3des
      NetDevice
         Type = PIX
         IP = 10.89.150.219
         NATAddr = 0.0.0.0
         Communications = ssh-3des
      NetDevice
         Type = PIX
         IP = 10.89.150.250
         NATAddr = 0.0.0.0
         Communications = telnet
      NetDevice
         Type = Cisco
         IP = 10.89.150.158
         NATAddr = 0.0.0.0
         Communications = telnet
         BlockInterface
            InterfaceName = ethernet0/1
            InterfaceDirection = out
            InterfacePostBlock = Post_Acl_Test
         BlockInterface
            InterfaceName = ethernet0/1
            InterfaceDirection = in
            InterfacePreBlock = Pre_Acl_Test
            InterfacePostBlock = Post_Acl_Test
      NetDevice
         Type = CAT6000_VACL
         IP = 10.89.150.138
         NATAddr = 0.0.0.0
         Communications = telnet
         BlockInterface
            InterfaceName = 502
            InterfacePreBlock = Pre_Acl_Test
         BlockInterface
            InterfaceName = 507
            InterfacePostBlock = Post_Acl_Test
   State
      BlockEnable = true
      NetDevice
         IP = 10.89.150.171
         AclSupport = Does not use ACLs
         Version = 6.3
         State = Active
         Firewall-type = PIX
      NetDevice
         IP = 10.89.150.219
         AclSupport = Does not use ACLs
         Version = 7.0
         State = Active
         Firewall-type = ASA
      NetDevice
         IP = 10.89.150.250
         AclSupport = Does not use ACLs
         Version = 2.2
         State = Active
```

```
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
ips-ssp#
```

ステップ 12　通知アプリケーションの統計情報を表示します。

```
ips-ssp# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
ips-ssp#
```

ステップ 13　OS 識別の統計情報を表示します。

```
ips-ssp# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
ips-ssp#
```

ステップ 14　SDEE サーバの統計情報を表示します。

```
ips-ssp# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
ips-ssp#
```

ステップ 15　トランザクション サーバの統計情報を表示します。

```
ips-ssp# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
ips-ssp#
```

ステップ 16　仮想 ips-ssp の統計情報を表示します。

```
ips-ssp# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 0
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 0
         The average bytes per packet since reset = 0
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 0
         Number of Denied Attacker Victim Pairs Inserted = 0
         Number of Denied Attacker Service Pairs Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 0
      Denied Attackers and hit count for each.
      Denied Attackers with percent denied and hit count for each.


      The Signature Database Statistics.
         The Number of each type of node active in the system (can not be reset
            Total nodes active = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The number of each type of node inserted since reset
            Total nodes inserted = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The rate of nodes per second for each time since reset
            Nodes per second = 0
            TCP nodes keyed on both IP addresses and both ports per second = 0
            UDP nodes keyed on both IP addresses and both ports per second = 0
            IP nodes keyed on both IP addresses per second = 0
         The number of root nodes forced to expire because of memory constraint
            TCP nodes keyed on both IP addresses and both ports = 0
```

```
      Packets dropped because they would exceed Database insertion rate limit
s = 0
   Fragment Reassembly Unit Statistics for this Virtual Sensor
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
      Number of fragments received since reset = 0
      Number of fragments forwarded since reset = 0
      Number of fragments dropped since last reset = 0
      Number of fragments modified since last reset = 0
      Number of complete datagrams reassembled since last reset = 0
      Fragments hitting too many fragments condition since last reset = 0
      Number of overlapping fragments since last reset = 0
      Number of Datagrams too big since last reset = 0
      Number of overwriting fragments since last reset = 0
      Number of Initial fragment missing since last reset = 0
      Fragments hitting the max partial dgrams limit since last reset = 0
      Fragments too small since last reset = 0
      Too many fragments per dgram limit since last reset = 0
      Number of datagram reassembly timeout since last reset = 0
      Too many fragments claiming to be the last since last reset = 0
      Fragments with bad fragment flags since last reset = 0
   TCP Normalizer stage statistics
      Packets Input = 0
      Packets Modified = 0
      Dropped packets from queue = 0
      Dropped packets due to deny-connection = 0
      Current Streams = 0
      Current Streams Closed = 0
      Current Streams Closing = 0
      Current Streams Embryonic = 0
      Current Streams Established = 0
      Current Streams Denied = 0
   Statistics for the TCP Stream Reassembly Unit
      Current Statistics for the TCP Stream Reassembly Unit
         TCP streams currently in the embryonic state = 0
         TCP streams currently in the established state = 0
         TCP streams currently in the closing state = 0
         TCP streams currently in the system = 0
         TCP Packets currently queued for reassembly = 0
      Cumulative Statistics for the TCP Stream Reassembly Unit since reset
         TCP streams that have been tracked since last reset = 0
         TCP streams that had a gap in the sequence jumped = 0
         TCP streams that was abandoned due to a gap in the sequence = 0
         TCP packets that arrived out of sequence order for their stream = 0
         TCP packets that arrived out of state order for their stream = 0
         The rate of TCP connections tracked per second since reset = 0
   SigEvent Preliminary Stage Statistics
      Number of Alerts received = 0
      Number of Alerts Consumed by AlertInterval = 0
      Number of Alerts Consumed by Event Count = 0
      Number of FireOnce First Alerts = 0
      Number of FireOnce Intermediate Alerts = 0
      Number of Summary First Alerts = 0
      Number of Summary Intermediate Alerts = 0
      Number of Regular Summary Final Alerts = 0
      Number of Global Summary Final Alerts = 0
      Number of Active SigEventDataNodes = 0
      Number of Alerts Output for further processing = 0
   SigEvent Action Override Stage Statistics
      Number of Alerts received to Action Override Processor = 0
      Number of Alerts where an override was applied = 0
      Actions Added
         deny-attacker-inline = 0
         deny-attacker-victim-pair-inline = 0
```

```
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
                request-rate-limit = 0
          SigEvent Action Filter Stage Statistics
             Number of Alerts received to Action Filter Processor = 0
             Number of Alerts where an action was filtered = 0
             Number of Filter Line matches = 0
             Number of Filter Line matches causing decreased DenyPercentage = 0
             Actions Filtered
                deny-attacker-inline = 0
                deny-attacker-victim-pair-inline = 0
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
                request-rate-limit = 0
          SigEvent Action Handling Stage Statistics.
             Number of Alerts received to Action Handling Processor = 0
             Number of Alerts where produceAlert was forced = 0
             Number of Alerts where produceAlert was off = 0
             Actions Performed
                deny-attacker-inline = 0
                deny-attacker-victim-pair-inline = 0
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
--MORE--
```

ステップ 17　Web サーバの統計情報を表示します。

```
ips-ssp# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
```

```
crypto library version = 6.0.3
ips-ssp#
```

ステップ 18　ロギング アプリケーションなどのアプリケーションの統計情報をクリアします。

```
ips-ssp# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

統計情報が取得され、クリアされます。

ステップ 19　統計情報がクリアされたことを確認します。

```
ips-ssp# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
ips-ssp#
```

統計情報はすべて 0 から始まります。

インターフェイス情報

show interfaces コマンドは、センシング インターフェイスおよびコマンド/コントロール インターフェイスに関する情報を収集するために有用です。ここでは、**show interfaces** コマンドについて説明します。次のような構成になっています。

- 「show interfaces コマンドの概要」（P.C-71）
- 「インターフェイス コマンドの出力」（P.C-71）

show interfaces コマンドの概要

show interfaces コマンドにより次の情報を把握することができます。

- インターフェイスがアップ状態かダウン状態かどうか
- パケットが監視されているかどうか、どのインターフェイスでそれが行われるか
- SensorApp によってパケットがドロップされているかどうか
- パケット ドロップを生じるようなエラーがインターフェイスによってレポートされているかどうか

show interfaces コマンドは、すべてのシステム インターフェイスの統計情報を表示します。または、個々のコマンドを使用してコマンド/コントロール インターフェイス（**show interfaces** *command_control_interface_name*）、センシング インターフェイス（**show interfaces** *interface_name*）の統計情報を表示します。

インターフェイス コマンドの出力

次に、**show interfaces** コマンドの出力例を示します。

```
ips-ssp# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
```

```
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
ips-ssp#
```

イベント情報

show events コマンドを使用すれば、SensorApp によって生成されたアラートおよびアプリケーションによって生成されたエラーを表示できます。ここでは、**show events** コマンドについて説明します。次のような構成になっています。

- 「センサーのイベント」（P.C-72）
- 「show events コマンドの概要」（P.C-72）
- 「イベントの表示」（P.C-73）
- 「イベントのクリア」（P.C-76）

センサーのイベント

5 種類のイベントがあります。

- evAlert：侵入検知アラート
- evError：アプリケーション エラー
- evStatus：ステータスの変更（IP ログの作成など）
- evLogTransaction：各センサー アプリケーションによって処理されるコントロール トランザクションのレコード
- evShunRqst：ブロックの要求

イベントは、新しいイベントによって上書きされるまでイベント ストアにとどまります。

show events コマンドの概要

show events コマンドは、Event Viewer または Security Monitor でイベントを確認できないといった、イベント キャプチャの問題のトラブルシューティングを行う際に有用です。**show events** コマンドを使用すれば、イベントが生成されていることを確認するためにセンサー上でどのイベントが生成されているかを特定し、モニタ側に障害があるかどうかを判定することができます。

イベント ストアからすべてのイベントをクリアするには、**clear events** コマンドを使用します。

ここで、**show events** コマンドのパラメータを示します。

```
ips-ssp# show events
<cr>
alert           Display local system alerts.
error           Display error events.
hh:mm[:ss]      Display start time.
log             Display log events.
nac             Display NAC shun events.
past            Display events starting in the past specified time.
status          Display status events.
|               Output modifiers.
```

イベントの表示

show events [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用して、イベント ストアのイベントを表示します。

開始時刻に開始されているイベントが表示されます。開始時刻を指定しない場合、現時点で開始されているイベントが表示されます。イベント タイプを指定しないと、すべてのイベントが表示されます。

（注） イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であるか、試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。シグニチャがネットワーク アクティブによってトリガーされると常に、分析エンジンによってアラート イベントが生成されます。

  レベルが選択されていない場合（informational、low、medium、または high）、すべてのアラート イベントが表示されます。
- **include-traits**：指定された特徴を持つアラートを表示します。
- **exclude-traits**：指定された特徴を持つアラートを表示しません。
- **traits**：特徴ビット位置（0 ～ 15）（10 進数）。
- **min-threat-rating**：脅威レーティングがこの値以上であるイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：脅威レーティングがこの値以下であるイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。
- **error**：エラー イベントを表示します。エラーの条件が検出されると、サービスによってエラー イベントが生成されます。

  レベルが選択されていない場合（warning、error、または fatal）、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

  （注） ARC は、以前は NAC と呼ばれていました。この名前の変更は、Cisco IPS 7.0 の IDM、IME、および CLI に完全には実装されていません。
- **status**：ステータス イベントを表示します。
- **past**：指定した過去の時、分、および秒から開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注） **show events** コマンドは、指定したイベントが使用可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベント ストアのイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始しているイベントをすべて表示します。

```
ips-ssp#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exception:
handshake incomplete.
```

Ctrl キーを押した状態で C キーを押すまで、フィードはすべてのイベントを表示し続けます。

ステップ 3　2008 年 2 月 9 日 10:00 a.m. 以降のブロック要求を表示します。

```
ips-ssp# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2008/02/09 10:33:31 2008/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
ips-ssp#
```

ステップ 4　2008 年 2 月 9 日 10:00 a.m. 以降の警告レベルのエラーを表示します。

```
ips-ssp# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2008/01/07 04:49:25 2008/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
ips-ssp# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2008/03/02 14:15:59 2008/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　30 秒前に開始されたイベントを表示します。

```
ips-ssp# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベントのクリア

clear events コマンドを使用して、イベント ストアをクリアします。

イベント ストアのイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
ips-ssp# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力して、イベントをクリアします。

cidDump スクリプト

IDM、IME、または CLI にアクセスしなくても、root としてログインし /usr/cids/idsRoot/bin/cidDump を実行することにより、サービス アカウントから基本的なスクリプトである cidDump を実行できます。cidDump ファイルのパスは /usr/cids/idsRoot/htdocs/private/cidDump.html です。

cidDump は大量の情報を取り込むためのスクリプトです。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。

cidDump スクリプトを実行するには、次の手順を実行します。

ステップ 1　センサーのサービス アカウントにログインします。

ステップ 2　サービス アカウント パスワードを使用して **root** に **su** します。

ステップ 3　次のコマンドを入力します。

```
/usr/cids/idsRoot/bin/cidDump
```

ステップ 4　次のコマンドを入力して、結果として生成される /usr/cids/idsRoot/log/cidDump.html ファイルを圧縮します。

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

ステップ 5　問題がある場合は、結果として生成された HTML ファイルを TAC または IPS の開発者に送信します。

詳細情報

Cisco FTP サイトにファイルを送信する手順については、「Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス」（P.C-77）を参照してください。

Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス

大きなファイル（たとえば、cidDump.html、**show tech-support** コマンドの出力、コア ファイル）は、ftp-sj サーバにアップロードできます。

Cisco FTP サイトへのファイルのアップロードおよび Cisco FTP サイトのファイルへのアクセスを行うには、次の手順に従います。

ステップ 1　ftp-sj.cisco.com に匿名でログインします。

ステップ 2　/incoming というディレクトリに変更します。

ステップ 3　**put** コマンドを使用してファイルをアップロードします。必ずバイナリ転送タイプを使用します。

ステップ 4　アップロードされたファイルにアクセスするには、ECS でサポートされたホストにログインします。

ステップ 5　/auto/ftp/incoming ディレクトリに変更します。

APPENDIX D

CLI のエラー メッセージ

（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。

この付録では、CLI のエラー メッセージと CLI の検証エラー メッセージの一覧を示します。次のような構成になっています。

- 「CLI のエラー メッセージ」（P.D-1）
- 「CLI 検証エラー メッセージ」（P.D-5）

CLI のエラー メッセージ

表 D-1 では、CLI のエラー メッセージについて説明します。

表 D-1　CLI のエラー メッセージ

エラー メッセージ	理由	コマンド
`getVirtualSensorStatistics : Analysis Engine is busy`	仮想センサーが初期化を終了していないため、分析エンジンがビジー状態です。	**show statistics virtual-sensor**
`getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables.This may take a while.`	センサーのイメージが作成された直後で、分析エンジンはキャッシュ ファイルを構築中のため、ビジー状態です。	**show statistics virtual-sensor**
`editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex tables.This may take a while.`	センサーのイメージが作成された直後で、分析エンジンはキャッシュ ファイルを構築中のため、ビジー状態です。	**service signature-definition**
`Invalid command received.`	.conf ファイルおよびコードが同期していません。このフィールドでは通常、発生しない状態です。	すべてのコマンド
`Invalid port number was entered.`	URI に範囲外のポート番号が入力されました。	**copy**、**upgrade**、**show tech-support**

表 D-1　CLI のエラー メッセージ （続き）

エラー メッセージ	理由	コマンド
Invalid scheme was entered.	内部テーブルが同期していません。このフィールドでは通常、発生しない状態です。	**copy**、**upgrade**、**show tech-support**
Unknown scheme was entered.	URI に無効なスキームが入力されました。	**copy**、**upgrade**、**show tech-support**
The filename <file> is not a valid upgrade file type.	プラットフォームおよびバージョンに対して誤ったファイルのインストールが試みられました。	**upgrade**
idsPackageMgr: digital signature of the update was not valid	シグニチャ アップデートまたはサービス パックが破損しています。TAC に連絡します。	**upgrade**
Cannot create a new event-action-rules configuration. “rules0 “ is currently the only configuration allowed.	サービス イベント アクション規則に対して無効な論理インスタンス名が入力されました。[1]	**service event-action-rules**
Cannot create a new signature-definition configuration. “sig0 “ is currently the only configuration allowed.	サービス シグニチャ定義に対して無効な論理インスタンス名が入力されました。[2]	**service signature-definition**
Cannot create a new anomaly-detection configuration. “ad0 “ is currently the only configuration allowed.	サービス異常検出に対して無効な論理インスタンス名が入力されました。[3]	**service anomaly-detection**
User does not exist.	管理者が、システムに存在しないユーザ名のパスワードの変更を試みています。	**password**
Incorrect password for user account.	ユーザが、パスワードを変更しようとして無効なパスワードを入力しました。	**password**
Empty user list.	curUserAccountList.xml ファイルにエントリがありません。このフィールドでは通常、発生しない状態です。	**username**
User already exists.	ユーザの作成が試みられましたが、そのユーザはすでにシステムに存在します。	**username**
Cannot communicate with system processes.Please contact your system administrator.	1 つまたは複数の必須アプリケーションが制御トランザクションに応答していません。	すべてのコマンド
Source and Destination are the same.	—	**copy**
Backup config was missing.	ユーザが、バックアップ コンフィギュレーション ファイルのコピーまたは消去を試みましたが、バックアップ コンフィギュレーション ファイルは生成されていません。	**copy** **erase**

表 D-1　CLI のエラー メッセージ （続き）

エラー メッセージ	理由	コマンド
Could not load CLI configuration files, can not complete request.	.conf ファイルが見つかりません。このフィールドでは通常、発生しない状態です。	**copy**
Error writing to <URL>.	コピー先に指定された URL に書き込みできませんでした。	**copy**
Error reading from <URL>.	コピー元に指定された URL を読み取りできませんでした。	**copy**
Packet-file does not exist.	ユーザがパケットファイルのコピーまたは消去を試みましたが、パケットファイルはキャプチャされていません。	**copy** **erase**
No downgrade available.	ユーザが、アップグレードされていないシステムのダウングレードを試みました。	**downgrade**
No packet-file available.	ユーザが、ファイル情報またはパケットファイルの表示を試みましたが、パケットファイルが存在しません。	**packet**
Log file exists but an error occurred during read.	ユーザが表示またはコピーしていた iplog ファイルが上書きされました。ファイルの内容は、一部表示可能です。	**packet**
Another user is currently capturing into the packet-file.Please try again later.	—	**packet capture**
Another CLI client is currently displaying packets from the interface.	この操作を行うには、他の CLI セッションが表示を終了するまで待機する必要があります。複数のユーザがコマンド コントロール インターフェイスを同時に表示する可能性があります。	**packet display**
Log does not exist.	ユーザが、存在しない iplog のコピーまたは表示を試みました。	**copy iplog** **packet display iplog**
The requested IPLOG is not complete.Please try again after the IPLOG status is 'completed.'	ユーザが、完成していない iplog のコピーまたは表示を試みました。	**copy iplog**
Could not create pipe /usr/cids/idsRoot/tmp/ pipe_cliPacket.<pid>.tmp	iplog ファイルを送信するためのパイプを開くことができませんでした。この状態は、スペースまたはリソース上の制限があることを示しています。このフィールドでは通常、発生しない状態です。	**copy iplog**

表 D-1　CLI のエラー メッセージ （続き）

エラー メッセージ	理由	コマンド
The log file was overwritten while the copy was in progress.The copied log file may be viewable but is incomplete.	iplog がセンサーからのコピー中に上書きされました。	**copy iplog**
Could not read license file.	ライセンス ファイルがコピーされましたが、開くことができません。	**copy license-key**
Could not write the temporary license file location used to copy the file off the box.	一時保存場所の /usr/cids/idsRoot/tmp/ips.lic を開くことができませんでした。この状態は、スペース上の制限があることを示しています。このフィールドでは通常、発生しない状態です。	**copy license-key**
Virtual sensor name does not exist.	ユーザが、存在しない仮想センサー上の iplog の開始または停止を試みました。	**iplog**
You do not have permission to terminate the requested CLI session.	オペレータ ユーザまたはビューア ユーザが、別のユーザに属する CLI セッションの終了を試みました。	**clear line**
Invalid CLI ID specified, use the 'show users all' command to view the valid CLI session IDs.	ユーザが、存在しない CLI セッションのキャンセルを試みました。	**clear line**
The maximum allowed CLI sessions are currently open, please try again later.	すでに最大数の CLI セッションが開かれているときに、オペレータ ユーザまたはビューア ユーザがログインを試みました。	initial login
The maximum allowed CLI sessions are currently open, would you like to terminate one of the open sessions?	すでに最大数の CLI セッションが開かれているときに、管理者ユーザがログインを試みました。	initial login
Can not communicate with system processes.Please contact your system administrator.	CLI からセンサー上のアプリケーションにアクセスして起動情報を取得できませんでした。これは通常、発生しない致命的なエラーです。ユーザはサービス アカウントにログインして、手動でセンサーをリブートする必要があります。	initial login
The instance cannot be removed.Instance assigned to virtual sensor name.	ユーザが、仮想センサーに現在割り当てられている設定インスタンスの削除を試みました。設定をデフォルトにリセットするには、**default service** コマンドを使用します。	**no service** *component instance*
Insufficient disk space to complete request.	コンフィギュレーション ファイルの新しいインスタンスを作成するには、ディスクの空き容量が足りません。	**copy instance service** *component instance*

1. このエラーは、仮想ポリシーをサポートしていないプラットフォームでのみ発生します。
2. このエラーは、仮想ポリシーをサポートしていないプラットフォームでのみ発生します。
3. このエラーは、仮想ポリシーをサポートしていないプラットフォームでのみ発生します。

CLI 検証エラー メッセージ

表 D-2 に検証エラー メッセージを示します。

表 D-2　検証エラー メッセージ

エラー メッセージ	理由 / 場所
Interface ‘name’ has not been subdivided.	物理インターフェイスまたはインライン インターフェイス *name* のサブインターフェイス タイプはありません（サービス インターフェイス サブモード）。
Interface ‘name’ subinterface ‘num’ does not exist.	物理インターフェイス *name* がインライン VLAN ペアに分割されましたが、指定されたサブインターフェイス番号が存在しません（サービス インターフェイス サブモード）。
Interface ‘name’ is the command-control interface.	物理インターフェイス *name* は、コマンド / コントロール インターフェイスです（サービス インターフェイス サブモード）。
Interface ‘name’ has been subdivided.	物理インターフェイス *name* のサブインターフェイス タイプは、インライン VLAN ペアまたは VLAN グループです。あるいは、インライン インターフェイス *name* のサブインターフェイス タイプは VLAN グループです（サービス インターフェイス サブモード）。
Interface ‘name’ is assigned to inline-interfaces ‘inlinename.’	物理インターフェイス *name* は、インライン インターフェイス エントリの interface1 または interface2 に割り当てられています（サービス インターフェイス サブモード）。
Vlan ‘vlannum’ is assigned to subinterface ‘subnum.’	VLAN *vlannum* は、すでに別のサブインターフェイス *subnum* エントリの vlan1 または vlan2 に割り当てられています（サービス インターフェイス サブモード）。
Vlan range ‘vlanrange’ overlaps with vlans assigned to subinterface ‘subnum.’	VLAN 範囲 *vlanrange* には、別のサブインターフェイス *subnum* エントリの *vlans range* にすでに使用されている値が含まれています（サービス インターフェイス サブモード）。
Unassigned vlans already assigned to subinterface ‘subnum.’	未割り当ての VLAN は、すでに別のサブインターフェイス *subnum* エントリで選択されています。
Inline-interface ‘inlinename’ does not exist.	インライン インターフェイス *inlinename* が存在しません（サービス インターフェイス サブモード）。
The default-vlans for the selected interfaces do not match.interface1, ‘name’ default-vlan is ‘vlannum,’ interface2, ‘name’ default-vlan is ‘vlannum.’	ユーザがインライン インターフェイスのサブインターフェイス タイプを VLAN グループに変更しようとしましたが、インライン インターフェイスに割り当てられている 2 つのインターフェイスのデフォルト VLAN が一致しません（サービス インターフェイス サブモード）。

表 D-2　検証エラー メッセージ （続き）

エラー メッセージ	理由 / 場所
interface1 and interface2 must be set before the logical interface can be divided into subinterfaces.	ユーザがインライン インターフェイスのサブインターフェイス タイプを VLAN グループに変更しようとしましたが、interface1 および interface2 の両方が設定されていません（サービス インターフェイス サブモード）。
Interface ‘name’ has not been subdivided into inline-vlan-pairs.	物理インターフェイス *name* サブインターフェイス タイプがインライン VLAN ペアではありません（サービス インターフェイス サブモード）。
Interface already assigned to virtual sensor ‘vsname.’	仮想センサー エントリの物理インターフェイス セットに追加しようとしているインターフェイスとオプションのサブインターフェイスは、すでに別の仮想センサー エントリに割り当てられています。
The instance cannot be removed.Instance assigned to virtual sensor ‘vsname.’	ユーザが削除しようとしているシグニチャ定義、イベント アクション ルール、または異常検出のコンフィギュレーション ファイルは、現在仮想センサー *vsname* で使用されています。

APPENDIX E

Cisco IPS 7.1 で使用されるオープン ソース ライセンス ファイル

このマニュアルには、Cisco IPS 7.1 で使用されるオープン ソース ソフトウェアのラインセンスおよび注意事項が記載されています。このマニュアルに記載されるフリー / オープン ソース ソフトウェアに関して質問がある場合、または該当するフリー / オープン ソース ライセンス（GNU Lesser/General Public License など）で権利が認められたソース コードのコピーを希望する場合は、external-opensource-requests@cisco.com にお問い合わせください。

内容

この付録には Cisco IPS 7.1 で使用されるオープン ソース ソフトウェアの一覧を示します。次のような構成になっています。

- 「bash 3.2」（P.E-B）
- 「busybox 1.13.1」（P.E-G）
- 「cracklib 2.8.12」（P.E-L）
- 「curl 7.18.2 1」（P.E-Q）
- 「diffutils 2.8.1」（P.E-R）
- 「e2fsprogs 1.39」（P.E-W）
- 「Expat XML parser 2.0.1」（P.E-AB）
- 「expect 5.4.3」（P.E-AB）
- 「glibc 2.9」（P.E-AB）
- 「gnupg 1.4.5」（P.E-AF）
- 「hotplug 2004_03_29」（P.E-AJ）
- 「i2c-tools 3.0.2」（P.E-AO）
- 「ipmiutil 2.3.3」（P.E-AT）
- 「iptables 1.4.1」（P.E-AT）
- 「kernel 2.6.29.1」（P.E-AY）
- 「libpcap 0.9.8」（P.E-BH）
- 「libtecla 1.4.1」（P.E-BI）
- 「Linux-Pam 1.0.1」（P.E-BI）

- 「lm_sensors 3.0.2」（P.E-BJ）
- 「module-init-tools 3.2.2 1.0.0.0900084」（P.E-BO）
- 「Ncurses 5.6」（P.E-BS）
- 「net-snmp 5.4.1」（P.E-BT）
- 「NTP 4.2.4p5」（P.E-BX）
- 「openssh 5.1p1」（P.E-CA）
- 「openssl 0.9.8j」（P.E-CG）
- 「pciutils 3.0.1」（P.E-CJ）
- 「procps 3.2.7」（P.E-CP）
- 「sysfsutils 2.1.0」（P.E-CT）
- 「sysstat 8.1.3」（P.E-CU）
- 「tcl 8.4.9」（P.E-CY）
- 「tcpdump 3.9.8 1.0.1.0801182」（P.E-CZ）
- 「tipc 1.7.6-bundle」（P.E-CZ）
- 「util-linux 2.12r」（P.E-DB）
- 「zlib 1.2.3」（P.E-DC）

bash 3.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

busybox 1.13.1

Available under license:

A note on GPL versions

BusyBox is distributed under version 2 of the General Public License (included in its entirety, below). Version 2 is the only version of this license which this version of BusyBox (or modified versions derived from this one) may be distributed under.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for

this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is

void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does. Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

The code and graphics on this website (and it's mirror sites, if any) are

Copyright (c) 1999-2004 by Erik Andersen. All rights reserved.

Copyright (c) 2005-2011 Rob Landley.

Documents on this Web site including their graphical elements, design, and layout are protected by trade dress and other laws and MAY BE COPIED OR IMITATED IN WHOLE OR IN PART. THIS WEBSITE IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE WEBSITE TO THE EXTENT PERMITTED BY APPLICABLE LAW.

SHOULD THIS WEBSITE PROVE DEFECTIVE, YOU MAY ASSUME THAT SOMEONE MIGHT GET AROUND TO SERVICING, REPAIRING OR CORRECTING IT SOMETIME WHEN THEY HAVE NOTHING BETTER TO DO. REGARDLESS, YOU GET TO KEEP BOTH PIECES.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THIS WEBSITE AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS WEBSITE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR LOSS OF HAIR, LOSS OF LIFE, LOSS OF MEMORY, LOSS OF YOUR CARKEYS, MISPLACEMENT OF YOUR PAYCHECK, OR COMMANDER DATA BEING RENDERED UNABLE TO ASSIST THE STARFLEET OFFICERS ABORD THE STARSHIP ENTERPRISE TO RECALIBRATE THE MAIN DEFLECTOR ARRAY, LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE WEBSITE TO OPERATE WITH YOUR WEBBROWSER), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You have been warned.

You can contact the webmaster at <rob@landley.net of problem with this.

bzip2 applet in busybox is based on lightly-modified source of bzip2 version 1.0.4. bzip2 source is distributed under the following conditions (copied verbatim from LICENSE file).

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2011 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESSOR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.

jseward@bzip.org

bzip2/libbzip2 version 1.0.4 of 20 December 2011

cracklib 2.8.12

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does. Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

curl 7.18.2 1

Available under license:

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2008, Daniel Stenberg, <daniel@haxx.se

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright (c) 1995, 1996, 1997, 1998, 1999 Kungliga Tekniska Hogskolan

(Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

diffutils 2.8.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

e2fsprogs 1.39

Available under license:

This package, the EXT2 filesystem utilities, are made available under the GNU Public License, with the exception of the lib/uuid directory which is made available under a BSD-style license. Please seelib/uuid/COPYING for more details for the license for the files comprising the libuuid library.

However, I request that if the version string in the file version.h contains the string "pre-", or "WIP" that this version of e2fsprogs be distributed in source form only. Please feel free to give a copy of the e2fsck binary to help a friend recover his or her filesystem, as the need arises. However, "pre" or "WIP" indicates that this release is under development, and available for ALPHA testing. So for your protection as much as mine, I'd prefer that it not appear in a some distribution --- especially not a CD-ROM distribution!

The most recent officially distributed version can be found at http://e2fsprogs.sourceforge.net. If you need to make a distribution, that's the one you should use. If there is some reason why you'd like a more recent version that is still in ALPHA testing for your distribution, please contact me (tytso@mit.edu), and we will very likely be able to work out something that will work for all concerned.

The release schedules for this package are flexible, if you give me enough lead time.

Theodore Ts'o

15-Mar-2010

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Expat XML parser 2.0.1

Available under license:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

expect 5.4.3

Available under license:

Written by: Don Libes, NIST, 90/02/06

Design and implementation of this program was paid for by U.S. tax dollars. Therefore it is public domain. However, the author and NIST would appreciate credit if this program or parts of it are used.

glibc 2.9

Available under license:

GNU GENERAL PUBLIC LICENSE

This file contains the copying permission notices for various files in the GNU C Library distribution that have copyright owners other than the Free Software Foundation. These notices all require that a copy of the notice be included in the accompanying documentation and be distributed with binary distributions of the code, so be sure to include this file along with any binary distributions derived from the GNU C Library.

All code incorporated from 4.4 BSD is distributed under the following license:

Copyright (C) 1991 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. [This condition was removed.]

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The DNS resolver code, taken from BIND 4.9.5, is copyrighted both by UC Berkeley and by Digital Equipment Corporation. The DEC portions are under the following license:

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The Sun RPC support (from rpcsrc-4.0) is covered by the following license:

Copyright (C) 1984, Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

The following CMU license covers some of the support code for Mach, derived from Mach 3.0:

Mach Operating System

Copyright (C) 1991,1990,1989 Carnegie Mellon University

All Rights Reserved.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Carnegie Mellon requests users of this software to return to

Software Distribution Coordinator

School of Computer Science

Carnegie Mellon University

Pittsburgh PA 15213-3890

or Software.Distribution@CS.CMU.EDU any improvements or extensions that they make and grant Carnegie Mellon the rights to redistribute these changes.

The file if_ppp.h is under the following CMU license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY CARNEGIE MELLON UNIVERSITY AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following license covers the files from Intel's "Highly Optimized Mathematical Functions for Itanium" collection:

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The files inet/getnameinfo.c and sysdeps/posix/getaddrinfo.c are copyright (C) by Craig Metz and are distributed under the following license:

The Inner Net License, Version 2.00

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.

1. All terms of the all other applicable copyrights and licenses must be followed.

2. Redistributions of source code must retain the authors' copyright notice(s), this list of conditions, and the following disclaimer.

3. Redistributions in binary form must reproduce the authors' copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

4. [The copyright holder has authorized the removal of this clause.]

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

If these license terms cause you a real problem, contact the author./

GNU LESSER GENERAL PUBLIC LICENSE

Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved.

gnupg 1.4.5

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St., Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St., Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

hotplug 2004_03_29

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least

the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

i2c-tools 3.0.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

ipmiutil 2.3.3

Available under license:

The BSD 2.0 License

Copyright (c) 2002-2008, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

iptables 1.4.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) 19yy <name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

kernel 2.6.29.1

Available under license:

NOTE!This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of "derived work". Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the Linux kernel) is copyrighted by me and others who actually wrote it.

Also note that the only valid version of the GPL as far as the kernel is concerned is _this_ particular version of the license (i.e. v2, not v2.2 or v3.x or whatever), unless explicitly otherwise stated.

Linus Torvalds

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most

of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Copyright (c) 2010-2011 QLogic Corporation

QLogic Linux Networking HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

Copyright (c) 2010-2008 QLogic Corporation

QLogic Linux Networking HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

FlashPoint Driver Developer's Kit

Version 1.0

Copyright 1995-1996 by Mylex Corporation

All Rights Reserved

This program is free software; you may redistribute and/or modify it under the terms of either:

a) the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version,

or

b) the "BSD-style License" included below.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See either the GNU General Public License or the BSD-style License below for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The BSD-style License is as follows:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain this LICENSE. FlashPoint file, without modification, this list of conditions, and the following disclaimer. The following copyright notice must appear immediately at the beginning of all source files:

Copyright 1995-1996 by Mylex Corporation. All Rights Reserved

This file is available under both the GNU General Public License and a BSD-style copyright; see LICENSE. FlashPoint for details.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of Mylex Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY MYLEX CORP."AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2010-2005 QLogic Corporation

QLogic Linux Fibre Channel HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

GNU LIBRARY GENERAL PUBLIC LICENSE

nicstar.c v0.22 Jawaid Bazyar (bazyar@hypermall.com)

nicstar.c, M.Welsh (matt.welsh@cl.cam.ac.uk)

Hacked October, 1997 by Jawaid Bazyar, Interlink Advertising Services Inc.

http://www.hypermall.com/

97/10/01 - commented out CFG_PHYIE bit - we don't care when the PHY interrupts us (except possibly for removal/insertion of the cable?)

97/10/04 - began heavy inline documentation of the code. Corrected typos and spelling mistakes.

97/10/05 - added code to handle PHY interrupts, disable PHY on loss of link, and correctly re-enable PHY when link is re-established.(put back CFG_PHYIE)

Modified to work with the IDT7721 nicstar -- AAL5 (tested) only.

R. D. Rechenmacher <ron@fnal.gov

Linux driver for the IDT77201 NICStAR PCI ATM controller.

PHY component is expected to be 155 Mbps S/UNI-Lite or IDT 77155; see init_nicstar() for PHY initialization to change this. This driver expects the Linux ATM stack to support scatter-gather lists (skb-Implementing minimal-copy of received data:

IDT always receives data into a small buffer, then large buffers as needed. This means that data must always be copied to create the linear buffer needed by most non-ATM protocol stacks (e.g. IP)

Fix is simple: make large buffers large enough to hold entire SDU, and leave <small_buffer_data copy small buffer contents to head of large buffer.

Trick is to avoid fragmenting Linux, due to need for a lot of large buffers. This is done by 2 things:

1) skb-combined, allow nicstar_free_rx_skb to be called to recycle large data buffers

2) skb_clone of received buffers

See nicstar_free_rx_skb and linearize_buffer for implementation details.

Copyright (c) 1996 University of Cambridge Computer Laboratory

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. M. Welsh, 6 July 1996

linux-2.6.29.1/drivers/net/LICENSE.SRC

Code in this directory written at the IDA Supercomputing Research Center carries the following copyright and license.

Copyright 1993 United States Government as represented by the Director, National Security Agency. This software may be used and distributed according to the terms of the GNU General Public License, incorporated herein by reference.

In addition to the disclaimers in the GPL, SRC expressly disclaims any and all warranties, expressed or implied, concerning the enclosed software.

This software was developed at SRC for use in internal research, and the intent in sharing this software is to promote the productive interchange of ideas throughout the research community. All software is furnished on an "as-is" basis. No further updates to this software should be expected. Although updates may occur, no commitment exists.

linux-2.6.29.1/drivers/net/wireless/libertas/LICENSE

Copyright (c) 2010-2011, Marvell International Ltd.

All Rights Reserved

This program is free software; you can redistribute it and/or modify it under the terms of version 2 of the GNU General Public License as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

The files in this directory and elsewhere which refer to this LICENCE file are part of JFFS2, the Journalling Flash File System v2.

Copyright © 2001-2007 Red Hat, Inc. and others

JFFS2 is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

JFFS2 is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with JFFS2; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

As a special exception, if other files instantiate templates or use macros or inline functions from these files, or you compile these files and link them with other works to produce a work based on these files, these files do not by themselves cause the resulting work to be covered by the GNU General Public License. However the source code for these files must still be made available in accordance with section (3) of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

libpcap 0.9.8

Available under license:

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

libtecla 1.4.1

Available under license:

Copyright (c) 2000, 2001 by Martin C. Shepherd.

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Linux-Pam 1.0.1

Available under license:

Unless otherwise *explicitly* stated the following text describes the licensed conditions under which the contents of this libpamc release may be distributed:

Redistribution and use in source and binary forms of libpamc, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU Library General Public License (LGPL), in which case the provisions of the GNU LGPL are required INSTEAD OF the above restrictions.(This clause is necessary due to a potential conflict between the GNU LGPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED '"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

lm_sensors 3.0.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as

separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs.If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

module-init-tools 3.2.2 1.0.0.0900084

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w’ .

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w’ and `show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Ncurses 5.6

Available under license:

Copyright (c) 1998-2004,2011 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

net-snmp 5.4.1

Available under license:

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like)

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc. copyright notice (BSD)

Copyright (c) 2001-2010, Networks Associates Technology, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD)

Portions of this code are copyright (c) 2001-2010, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD)

Copyright 2010 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc. copyright notice (BSD)

Copyright (c) 2010-2011, Sparta, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD)

Copyright (c) 2004, Cisco, Inc. and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc., Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD)

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2010

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NTP 4.2.4p5

Available under license:

This file is automatically generated from html/copyright.html

Copyright Notice

jpg "Clone me," says Dolly sheepishly

Last update: 20:31 UTC Saturday, January 06, 2007

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (c) David L. Mills 1992-2008

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. Mark Andrews <mark_andrews@isc.org controller

2. Bernd Altmeier <altmeier@atlsoft.de line and PCI-bus devices

3. Viraj Bais <vbais@mailman1.intel.com <kirkwood@striderfm.intel.com

4. Michael Barone <michael,barone@lmco.com

5. Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca

6. Karl Berry <karl@owl.HQ.ileaf.com

7. Greg Brackley <greg.brackley@bigfoot.com Clean up recvbuf and iosignal code into separate modules.

8. Marc Brett <Marc.Brett@westgeo.com

9. Piete Brooks <Piete.Brooks@cl.cam.ac.uk Trimble PARSE support

10. Reg Clemens <reg@dwf.com

11. Steve Clift <clift@ml.csiro.au

12. Casey Crellin <casey@csc.co.za help with target configuration

13. Sven Dietrich <sven_dietrich@trimble.com clock driver, NT adj.residuals, integrated Greg's Winnt port.

14. John A.Dundas III <dundas@salt.jpl.nasa.gov

15. Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de port

16. Dennis Ferguson <dennis@mrbill.canet.ca NTP Version 2 as specified in RFC-1119

17. John Hay <jhay@@icomtek.csir.co.za

18. Glenn Hollinger <glenn@herald.usask.ca

19. Mike Iglesias <iglesias@uci.edu

20. Jim Jagielski <jim@jagubox.gsfc.nasa.gov

21. Jeff Johnson <jbj@chatham.usdesign.com overhaul

22. Hans Lambermont <Hans.Lambermont@nl.origin-it.com <H.Lambermont@chello.nl

23. Poul-Henning Kamp <phk@FreeBSD.ORG author)

24. Frank Kardel [27]<kardel (at) ntp (dot) org driver (scripts, syslog cleanup, dynamic interface handling

25. William L.Jones <jones@hermes.chpc.utexas.edu modifications, HPUX modifications

26. Dave Katz <dkatz@cisco.com

27. Craig Leres <leres@ee.lbl.gov GPS clock driver

28. George Lindholm <lindholm@ucs.ubc.ca

29. Louis A.Mamakos <louie@ni.umd.edu

30. Lars H.Mathiesen <thorinn@diku.dk code for Version 3 as specified in RFC-1305

31. Danny Mayer <mayer@ntp.org Maintenance

32. David L.Mills <mills@udel.edu discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG

33. Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de

34. Jeffrey Mogul <mogul@pa.dec.com

35. Tom Moore <tmoore@fievel.daytonoh.ncr.com

36. Kamal A Mostafa <kamal@whence.com

37. Derek Mulcahy <derek@toybox.demon.co.uk Hart-Davis <d@hd.org

38. Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de monitoring/trap scripts, statistics file handling

39. Dirce Richards <dirce@zk3.dec.com

40. Wilfredo Sanchez <wsanchez@apple.com NetInfo

41. Nick Sayer <mrapple@quack.kfu.com

42. Jack Sasportas <jack@innovativeinternet.com space on the stuff in the html/pic/ subdirectory

43. Ray Schnitzler <schnitz@unipress.com

44. Michael Shields <shields@tembel.org

45. Jeff Steinman <jss@pebbles.jpl.nasa.gov driver

46. Harlan Stenn <harlan@pfcs.com makeover, various other bits (see the ChangeLog)

47. Kenneth Stone <ken@sdd.hp.com

48. Ajit Thyagarajan <ajit@ee.udel.edu support

49. Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp driver

50. Paul A Vixie <vixie@vix.com TrueTime clock driver

51. Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de validated HTML documents according to the HTML DTD

References

1. mailto:mark_andrews@isc.org

2. mailto:altmeier@atlsoft.de
3. mailto:vbais@mailman1.intel.co
4. mailto:kirkwood@striderfm.intel.com
5. mailto:michael.barone@lmco.com
6. mailto:Jean-Francois.Boudreault@viagenie.qc.ca
7. mailto:karl@owl.HQ.ileaf.com
8. mailto:greg.brackley@bigfoot.com
9. mailto:Marc.Brett@westgeo.com
10. mailto:Piete.Brooks@cl.cam.ac.uk
11. mailto:reg@dwf.com
12. mailto:clift@ml.csiro.au
13. mailto:casey@csc.co.za
14. mailto:Sven_Dietrich@trimble.COM
15. mailto:dundas@salt.jpl.nasa.gov
16. mailto:duwe@immd4.informatik.uni-erlangen.de
17. mailto:dennis@mrbill.canet.ca
18. mailto:jhay@icomtek.csir.co.za
19. mailto:glenn@herald.usask.ca
20. mailto:iglesias@uci.edu
21. mailto:jagubox.gsfc.nasa.gov
22. mailto:jbj@chatham.usdesign.com
23. mailto:Hans.Lambermont@nl.origin-it.com
24. mailto:H.Lambermont@chello.nl
25. mailto:phk@FreeBSD.ORG
26. http://www4.informatik.uni-erlangen.de/%7ekardel
27. mailto:kardel(at)ntp(dot)org
28. mailto:jones@hermes.chpc.utexas.edu
29. mailto:dkatz@cisco.com
30. mailto:leres@ee.lbl.gov
31. mailto:lindholm@ucs.ubc.ca
32. mailto:louie@ni.umd.edu
33. mailto:thorinn@diku.dk
34. mailto:mayer@ntp.org
35. mailto:mills@udel.edu
36. mailto:moeller@gwdgv1.dnet.gwdg.de
37. mailto:mogul@pa.dec.com
38. mailto:tmoore@fievel.daytonoh.ncr.com
39. mailto:kamal@whence.com

40. mailto:derek@toybox.demon.co.uk
41. mailto:d@hd.org
42. mailto:Rainer.Pruy@informatik.uni-erlangen.de
43. mailto:dirce@zk3.dec.com
44. mailto:wsanchez@apple.com
45. mailto:mrapple@quack.kfu.com
46. mailto:jack@innovativeinternet.com
47. mailto:schnitz@unipress.com
48. mailto:shields@tembel.org
49. mailto:pebbles.jpl.nasa.gov
50. mailto:harlan@pfcs.com
51. mailto:ken@sdd.hp.com
52. mailto:ajit@ee.udel.edu
53. mailto:tsuruoka@nc.fukuoka-u.ac.jp
54. mailto:vixie@vix.com
55. mailto:Ulrich.Windl@rz.uni-regensburg.de

GNU LESSER GENERAL PUBLIC LICENSE

Redistribution and use in source and binary forms, with or without

GNU GENERAL PUBLIC LICENSE

General Public Licence for the software known as MSNTP

openssh 5.1p1

Available under license:

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

1)

OpenSSH contains no GPL code.

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licensed software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility.

You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com

<http://www.core-sdi.com

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be

author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be

author Paulo Barreto <paulo.barreto@terra.com.br

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom

Tim Rice

Andre Lucas

Chris Adams

Corinna Vinschen

Cray Inc.

Denis Parker

Gert Doering

Jakob Schlyter

Jason Downs

Juha Yrj?l?

Michael Stone

Networks Associates Technology, Inc.

Solar Designer

Todd C. Miller

Wayne Schroeder

William Jones

Darren Tucker

Sun Microsystems

The SCO Group

Daniel Walsh

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8)

Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42):

<phk@login.dknet.dk

notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995

his code is based on code written by Patrick Powell

papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.

Todd C. Miller

Reyk Floeter

Chad Mynhier

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

openssl 0.9.8j

Notifications:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Available under license:

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.(http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an Blowfish implementation written by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com).

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an DES implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with MIT's libdes.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of that the SSL library. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

pciutils 3.0.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Copyright (c) 1997--2008 Martin Mares <mj@ucw.cz

All files in this package can be freely distributed and used according to the terms of the GNU General Public License, either version 2 or (at your opinion) any newer version. See http://www.gnu.org/ for details.

List of PCI ID's

Maintained by Martin Mares <mj@ucw.cz

Linux PCI ID's Project at http://pciids.sf.net/.

New data are always welcome, especially if accurate. If you have anything to contribute, please follow the instructions at the web site or send a diff -u against the most recent pci.ids to pci-ids@ucw.cz.

This file can be distributed under either the GNU General Public License (version 2 or higher) or the 3-clause BSD License.

Daily snapshot on Thu 2008-09-11 01:05:01

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

procps 3.2.7

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

sysfsutils 2.1.0

Available under license:

The commands and utilities under the "test" directory are licensed under the GNU General Public License (GPL) Version 2, June 1991. The full text of the GPL is located at:

sysfsutils/cmd/GPL

The sysfs library is licensed under the GNU Lesser Public License (LGPL) Version 2.1, February 1999. The full text of the LGPL is located at:

sysfsutils/lib/LGPL

The GNU General Public License (GPL)

GNU Lesser Public License

sysstat 8.1.3

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it.(Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.(Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.

Copyright (C) 19yy <name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

tcl 8.4.9

Available under license:

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState Corporation and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses.

Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

tcpdump 3.9.8 1.0.1.0801182

Available under license:

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

tipc 1.7.6-bundle

Available under license:

net/tipc/tipc_user_reg.c: TIPC user registry code

Copyright (c) 2000-2011, Ericsson AB

Copyright (c) 2004-2011, Wind River Systems

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

* Alternatively, this software may be distributed under the terms of the GNU General Public License ("GPL") version 2 as published by the Free Software Foundation.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

client_tipc.c

Short description: TIPC benchmark demo (client side)

Copyright (c) 2001-2005, Ericsson Research Canada

Copyright (c) 2004-2011, Wind River Systems

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

util-linux 2.12r

Available under license:

GNU GENERAL PUBLIC LICENSE

Copyright (c) 1989 The Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2000-2001 Gunnar Ritter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. [deleted]

4. Neither the name of Gunnar Ritter nor the names of his contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY GUNNAR RITTER AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL GUNNAR RITTER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

zlib 1.2.3

Available under license:

License attached

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly　　Mark Adler

jloup@gzip.org　　madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

zlib 1.2.3

GLOSSARY

数字

3DES トリプル DES（Data Encryption Standard）。DES をより強力にしたバージョンで、SSH バージョン 1.5 のデフォルトの暗号化方式。センサーと SSH セッションを確立するときに使用されます。センサーでデバイスを管理しているときに使用できます。

802.x LAN プロトコルを定義する一連の IEEE 標準。

A

AAA 認証、許可、アカウンティング。「トリプルエー」と発音します。シスコ デバイスでアクセス コントロールを行う方法として第一に推奨されます。

ACE Access Control Entry（アクセス コントロール エントリ）。ACL 内のエントリで、指定されたアドレスまたはプロトコルに関して実行するアクションを記述します。センサーは、ACE を追加または削除してホストをブロックします。

ACK 確認応答。何かのイベントが発生したことを確認するために（メッセージの受信など）、1 つのネットワーク デバイスから別のネットワーク デバイスに送信される通知です。

ACL Access Control List（アクセス コントロール リスト）。ルータを経由するデータの流れを制御する ACE のリストです。ルータ インターフェイスごとに、受信データ用と送信データ用の 2 つの ACL があります。1 つの方向で同時にアクティブにできる ACL は 1 つだけです。ACL は、番号または名前で識別されます。ACL は、標準、強化、拡張のいずれかになります。センサーで ACL を管理するように設定できます。

ACS サーバ Cisco Access Control Server。ネットワーク ユーザ、ネットワーク管理者、およびネットワーク インフラストラクチャ リソースを管理する集中化されたコントロール ポイントである、RADIUS セキュリティ サーバです。

AIC エンジン アプリケーション検査および制御エンジン。Web トラフィックの詳細な分析を行います。HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。インスタント メッセージングやトンネリング アプリケーション（例：gotomypc）など、特定のポート上でトンネリングを行うアプリケーションに対する管理制御を行います。また、FTP トラフィックを検査し、発行されるコマンドを制御します。

AIM IPS Advanced Integration Module。Cisco ルータに取り付けられる IPS ネットワーク モジュールの一種です。

AIP SSM Advanced Inspection and Prevention Security Services Module。Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの IPS プラグイン モジュールです。AIP SSM は、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタリングおよびリアルタイム分析を行う IPS サービス モジュールです。AIP SSM が不正なアクティビティを検出すると、特定の接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、デバイス マネージャにアラートを送信します。適応型セキュリティ アプライアンスも参照してください。

API アプリケーション プログラミング インターフェイス。アプリケーション プログラムが通信ソフトウェアと対話するために使用する手段です。標準化された API を使用すると、基盤となる通信方法に依存することなくアプリケーション プログラムを開発できます。コンピュータのアプリケーション プログラムは、標準的なソフトウェア割り込み、コール、およびデータ形式のセットを実行して、他のデバイスとの接続を開始します（たとえば、ネットワーク サービス、メインフレームの通信プログラム、他のプログラム間通信など）。一般に、API によって、ソフトウェア開発者はアプリケーションがオペレーティング システムまたはネットワークと通信するために必要なリンクを容易に作成できます。

ARC Attack Response Controller。以前は Network Access Controller（NAC）と呼ばれていました。IPS のコンポーネントの 1 つです。適用可能な場合にブロックおよびブロック解除の機能を提供するソフトウェア モジュールです。

ARP アドレス解決プロトコル。IP アドレスを MAC アドレスにマッピングするために使用されるインターネット プロトコルです。RFC 826 で定義されています。

ASDM Adaptive Security Device Manager。適応型セキュリティ デバイスの設定と管理が可能な Web ベースのアプリケーションです。

ASN.1 抽象構文記法 1。データ表記の標準規格です。

ATOMIC エンジン ATOMIC エンジンは 2 種類あります。Atomic IP は、IP プロトコル パケットおよび関連するレイヤ 4 のトランスポート プロトコルを検査し、Atomic ARP は、レイヤ 2 の ARP プロトコルを検査します。

attack 知的脅威から発生するシステム セキュリティへの攻撃。セキュリティ サービスを回避してシステムのセキュリティ ポリシーを妨害するために、（特に方法や技術に関して）用意周到に計画したうえで試みられた知的行為を意味します。

AuthenticationApp IPS のコンポーネントの 1 つです。IP アドレス、パスワード、およびデジタル証明書に基づいてユーザを許可および認証します。

AV アンチウイルス。

B

BIOS Basic Input/Output System。センサーを起動し、センサー内のデバイスとシステムとの間で通信するプログラムです。

BO BackOrifice。UDP 上でのみ実行される最初の Windows のバック ドア型トロイの木馬。

BO2K BackOrifice 2000。TCP および UDP 上で実行される Windows のバック ドア型トロイの木馬。

BPDU Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワーク内のブリッジ間で情報を交換するために設定可能な間隔で送出される、スパニングツリー プロトコルの hello パケット。

C

CA 認証局（certification authority）。デジタル証明書（特に X.509 証明書）を発行し、証明書内のデータ項目間のバインディングを保証するエンティティです。センサーは、自己署名証明書を使用します。

CA 証明書 別の CA によって発行された、CA の証明書。

CEF シスコ エクスプレス フォワーディング。CEF は、高度なレイヤ 3 IP スイッチング テクノロジーです。CEF によって、大規模で動的なトラフィック パターンを持つネットワーク（インターネットなど）、集中的な Web ベースのアプリケーションを特徴とするネットワーク、または対話型セッションのパフォーマンスおよびスケーラビリティが最適化されます。

certificate 公開キーなどのユーザまたはデバイス属性のデジタル表現であり、信頼できる秘密キーで署名されています。

cidDump 大量の情報を取り込むためのスクリプト。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。

CIDEE Cisco Intrusion Detection Event Exchange。Cisco IPS システムが使用する SDEE への拡張を指定します。CIDEE 標準は、Cisco IPS システムがサポートする可能性のあるすべての拡張を指定しています。

CIDS ヘッダー IPS システム内の各パケットに付加されるヘッダー。これには、パケットの分類、パケットの長さ、チェックサムの結果、タイムスタンプ、および受信インターフェイスが含まれます。

Cisco IOS CiscoFusion アーキテクチャのすべての製品に対して、共通の機能、スケーラビリティ、およびセキュリティを提供するシスコのシステム ソフトウェア。Cisco IOS は、中央集中型の統合された自動インストールとインターネットワークの管理を可能にすると同時に、多様なプロトコル、メディア、サービス、およびプラットフォームをサポートします。

CLI コマンドライン インターフェイス。センサーに付属のシェルで、センサー アプリケーションの設定と制御に使用されます。

CollaborationApp IPS のコンポーネントの 1 つです。グローバル相関データベースを通じて他のデバイスと情報を共有することにより、すべてのデバイスの総合的効果を高めます。

Control Transaction Server IPS のコンポーネントの 1 つです。リモート クライアントからの制御トランザクションを受け付け、ローカル制御トランザクションを開始して、リモート クライアントに応答を返します。

Control Transaction Source IPS のコンポーネントの 1 つです。リモート アプリケーションに向けられた制御トランザクションを待機し、制御トランザクションをリモート ノードに転送し、応答を発信側に返します。

CS-MARS Cisco Security Monitoring, Analysis and Reporting System。シスコの自己防衛型ネットワーク ソリューションのモニタリング コンポーネントです。CS-MARS は CS-Manager と完全に統合されています。

CSA MC Cisco Security Agent Management Center。CSA MC は、管理対象の CSA エージェントからホスト ポスチャ情報を受信します。また、ネットワークからの隔離が必要と判断された IP アドレスのウォッチ リストを保守します。

CSM Cisco Security Manager。シスコの自己防衛型ネットワーク ソリューションのプロビジョニング コンポーネントです。CS-Manager は CS-MARS と完全に統合されています。

CVE Common Vulnerabilities and Exposures。脆弱性の標準名およびセキュリティ上の危険性に関するその他の情報のリスト。保守は http://cve.mitre.org/ で行われます。

D

DCE データ回線終端装置（ITU-T 拡張）。ユーザ / ネットワーク インターフェイスのネットワーク側を形成する、通信ネットワークのデバイスおよび接続。DCE はネットワークと物理的に接続し、トラフィックを転送し、DCE と DTE デバイス間のデータ伝送を同期させるためのクロック信号を提供します。DCE の例として、モデムやインターフェイス カードがあります。

DCOM 分散 COM。ネットワークを経由したソフトウェア コンポーネントの直接通信を可能にするプロトコル。マイクロソフトによって開発され、以前は Network OLE と呼ばれていました。DCOM は、HTTP などのインターネット プロトコルをはじめとする、複数ネットワークにまたがる伝送での利用を目的として設計されています。

DDoS 分散型サービス拒否攻撃。被害を受けた多数のシステムが 1 つのターゲットを攻撃することにより、ターゲット システムのユーザにサービス拒否を引き起こす攻撃。大量の着信メッセージによってターゲット システムが実質的にシャットダウンするために、正規のユーザのシステムへのサービスが拒否されます。

DES データ暗号規格。アルゴリズムではなく 56 ビット キーを基盤とする、強力な暗号化方式。

DIMM デュアル インライン メモリ モジュール。

DMZ 非武装地帯。プライベート（内部）ネットワークとパブリック（外部）ネットワークの間の中立地帯にある別個のネットワーク。

DNS ドメイン ネーム システム（Domain Name System）。インターネット全体にわたるホスト名と IP アドレスのマッピングです。DNS を使用すると、人間が読める形式の名前を、ネットワーク パケットで必要とされる IP アドレスに変換できます。

DoS Denial of Service（サービス拒絶）。特定のシステムまたはネットワークの操作を混乱させることを目的とする攻撃です。

DRAM ダイナミック ランダムアクセス メモリ。キャパシタに情報を保存する RAM のことで、定期的にリフレッシュする必要があります。DRAM がコンテンツをリフレッシュするときは、プロセッサがアクセスできないため、遅延が発生します。ただし、DRAM は SRAM に比べて複雑ではなく、容量も大きくなっています。

DTE データ端末機器。RS-232C 接続のデバイスの役割を指します。DTE は送信回線にデータを書き込み、受信回線からデータを読み取ります。

DTP ダイナミック トランキング プロトコル。VLAN グループにおけるシスコ独自のプロトコルで、2 台のデバイス間のリンク上でトランキングをネゴシエートするだけでなく、使用するトランキング カプセル化のタイプ（ISL または 802.1q）もネゴシエートします。

E

ECLB Ether Channel Load Balancing。Catalyst スイッチで、さまざまな物理パスを流れるトラフィックを分割できるようにします。

ESD 静電放電。静電放電は、1 つの物体から別の物体への急速な電荷の移動により、数千ボルトの電荷が発生することを指します。電気的コンポーネントやサーキット カード アセンブリ全体に重大なダメージを引き起こす場合があります。

evIdsAlert イベント ストアに書き込まれる、アラートを表す XML エンティティ。

F

Fast Flux
Fast Flux は、ボットネットがフィッシングやマルウェアの配信サイトを、被害を受けたホストのネットワークで隠すために使用する DNS 手法です。このネットワークはプロキシとして動作し、絶えず変化し続けます。また、マルウェア ネットワークの発見や対策を困難にするために使用されるピアツーピア ネットワーキング、分散型コマンド / コントロール、Web ベースのロード バランシング、およびプロキシ リダイレクションの組み合わせを指す場合もあります。Storm ワームは、この手法を使用した最近のマルウェア変種の 1 つです。

Flood エンジン
ホストおよびネットワークに向けられた ICMP および UDP フラッドを検出します。

FQDN
完全修飾ドメイン名。DNS のツリー階層構造で正確な場所を指定するドメイン名です。ルート ドメインに対して、トップレベル ドメインを含むすべてのドメインレベルを指定します。完全修飾ドメイン名は、このネーム スペースでの絶対位置によって識別されます。

FTP
File Transfer Protocol（ファイル転送プロトコル）。ネットワーク ノード間でファイルを転送するために使用され、TCP/IP プロトコル スタックの一部であるアプリケーション プロトコル。FTP は、RFC 959 で定義されています。

FTP サーバ
ファイル転送プロトコル（File Transfer Protocol）サーバ。ネットワーク ノード間のファイルの転送に FTP プロトコルを使用するサーバ。

FWSM
Firewall Security Module。Catalyst 6500 シリーズ スイッチに取り付けることができるモジュール。**shun** コマンドを使用してブロックを行います。FWSM は、シングルモードまたはマルチモードのいずれでも設定できます。

G

GBIC
ギガビット インターフェイス コンバータ。多くの場合、ファイバ インター フェイスに光ケーブル接続を適合させる光ファイバ トランシーバを指します。一般に、ファイバ対応のスイッチおよび NIC は、GBIC や SFP スロットを備えています。詳細については、『*Catalyst Switch Cable, Connector, and AC Power Cord Guide*』を参照してください。

Gigabit Ethernet
1996 年に IEEE（Institute of Electrical and Electronics Engineers）802.3z 規格委員会によって承認された、高速イーサネットの規格。

GMT
Greenwich Mean Time（グリニッジ標準時）。経度ゼロの時間帯です。現在は、協定世界時（UTC）と呼ばれます。

GRUB
Grand Unified Bootloader。ブートローダは、コンピュータの起動時に最初に実行されるソフトウェア プログラムです。オペレーティング システムのカーネル ソフトウェアをロードして制御を渡す役割を果たします。その後はカーネルがオペレーティング システムの残りの部分を初期化します。

H

H.225.0
H.225.0 セッションの確立とパケット化を規定する ITU 標準。H.225.0 では、実際には、RAS、Q.931 の使用、RTP の使用など、いくつかの異なるプロトコルが定められています。

H.245
H.245 エンドポイントの制御を規定する ITU 標準。

H.323 異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 は、CODEC の共通セット、コール セットアップとネゴシエーションの手順、および基本的なデータ転送方法を定義しています。

HTTP ハイパーテキスト転送プロトコル。IPS アーキテクチャでリモート データ交換に使用される、ステートレスな要求 / 応答メディア転送プロトコルです。

HTTPS 標準 HTTP プロトコルを拡張したもので、Web サイトからのトラフィックを暗号化することによって機密保持を可能にします。デフォルトでは、このプロトコルは TCP ポート 443 を使用します。

I

ICMP Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。ネットワーク層のインターネット プロトコルであり、エラーを報告し、IP パケット処理に関するその他の情報を提供します。RFC 792 に規定されています。

ICMP フラッド プロトコルの実装で処理可能な数を超える多数の ICMP エコー要求（「ping」）パケットをホストに送信する DoS 攻撃。

IDAPI Intrusion Detection Application Programming Interface。IPS アーキテクチャ アプリケーション間に単純なインターフェイスを提供します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。

IDCONF Intrusion Detection Configuration。侵入検知および防御システムの設定に使用される操作メッセージを定義するデータ形式の標準です。

IDENT RFC 1413 で規定された Ident プロトコル。特定の TCP 接続のユーザを識別するのに役立つインターネット プロトコルです。

IDIOM Intrusion Detection Interchange and Operations Messages。侵入検知システムによって報告されるイベント メッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の標準です。

IDM IPS Device Manager。センサーの設定と管理が可能な Web ベースのアプリケーションです。IDM の Web サーバはセンサーに常駐します。この Web サーバには、Internet Explorer または Firefox などの Web ブラウザでアクセスできます。

IDMEF Intrusion Detection Message Exchange Format。IETF Intrusion Detection Working Group による標準草案です。

IDS MC Management Center for IDS Sensors。Web ベースの IDS マネージャで、最大 300 台のセンサーの設定を管理できます。

IDSM-2 Intrusion Detection System Module。Catalyst 6500 シリーズ スイッチで侵入検知を実行するスイッチング モジュールです。

IME IPS Manager Express。システム ヘルス モニタリング、イベント モニタリング、レポーティング、および最大 10 台のセンサーの設定を提供するネットワーク管理アプリケーションです。

InterfaceApp IPS のコンポーネントの 1 つです。バイパスおよび物理設定を処理し、ペアになっているインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。

IP アドレス
TCP/IP を使用するホストに割り当てられる 32 ビット アドレス。IP アドレスは、5 つのクラス（A、B、C、D、または E）のいずれかに属し、ピリオドで区切られた 4 つのオクテット（ドット付き 10 進形式）で記述されます。各アドレスはネットワーク番号、オプションのサブネットワーク番号、およびホスト番号で構成されます。ルーティングにはネットワーク番号とサブネットワーク番号を組み合わせて使用し、ネットワーク内またはサブネットワーク内の個別のホストのアドレス指定にはホスト番号を使用します。IP アドレスからのネットワーク情報とサブネットワーク情報の抽出には、サブネット マスクを使用します。

IP スプーフィング
IP スプーフィング攻撃は、ネットワーク外の攻撃者が信頼されたユーザになりすますことによって発生します。攻撃者は、ネットワークの IP アドレス範囲内の IP アドレスを使用するか、信頼され、ネットワーク上の指定されたリソースへのアクセスが可能な、許可された外部 IP アドレスを使用して、このなりすましを行います。攻撃者が IPSec セキュリティ パラメータにアクセスした場合は、その攻撃者が企業ネットワークへのアクセスを許可されたリモート ユーザを偽装する可能性があります。

iplog
指定されたアドレスとの間でやり取りされるバイナリ パケットのログ。iplog は、シグニチャにログ イベント アクションが選択されている場合に作成されます。iplog は、WireShark および TCPDUMP で読み取り可能な libpcap 形式で格納されます。

IPS
侵入防御システム。ネットワーク トラフィックの分析技術を使用して、ネットワークへの侵入の存在をユーザに警告するシステムです。

IPS SSP
Intrusion Prevention System Security Services Processor。Cisco ASA 5585-X 適応型セキュリティ アプライアンスの IPS プラグイン モジュールです。IPS SSP は、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタリングおよびリアルタイム分析を行う IPS サービス プロセッサです。IPS SSP が不正なアクティビティを検出すると、特定の接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、デバイス マネージャにアラートを送信します。適応型セキュリティ アプライアンスも参照してください。

IPS データまたはメッセージ
IPS アプリケーション間でコマンド / コントロール インターフェイスを介して転送されるメッセージ。

IPv6
IP バージョン 6。IP の現在のバージョン（バージョン 4）に代わるバージョン。IPv6 ではパケット ヘッダーのフロー ID がサポートされており、フローの識別が可能です。以前は IPng（next generation）と呼ばれていました。

ISL
スイッチ間リンク。スイッチとルータの間のトラフィック フローとして VLAN 情報を維持するシスコ独自のプロトコル。

J

Java Web Start
Java Web Start は、プラットフォームに依存しない安全で堅牢な展開テクノロジーです。これにより開発者は、標準の Web サーバでアプリケーションを利用できるようにすることで、フル機能を持つアプリケーションをユーザに展開できます。どの Web ブラウザを使用しても、アプリケーションを起動することができ、いつでも確実に最新バージョンを使用できます。

JNLP
Java Network Launching Protocol。XML ファイル形式で定義され、Java Web Start アプリケーションの起動方法を指定します。JNLP は、どの程度厳密に起動メカニズムを実装するかを定義する一連の規則で構成されます。

K

KB
ナレッジ ベース。異常検出が学習した一連のしきい値で、ワーム ウイルスの検出に使用されます。

L

LACP Link Aggregation Control Protocol。LACP は、LACP パケットを LAN ポート間で交換することにより、EtherChannel リンクの自動作成を支援します。このプロトコルは IEEE 802.3ad で定義されています。

LAN ローカル エリア ネットワーク。特定ホストのローカルのレイヤ 2 ネットワーク ドメインを指します。同じ LAN 上の 2 つのホスト間で交換されるパケットには、レイヤ 3 ルーティングは必要ありません。

LOKI リモート アクセス、バック ドア型トロイの木馬である、ICMP トンネリング ソフトウェア。コンピュータが感染すると、悪意のあるコードによって、小さなペイロードの ICMP 応答の送信に使用できる ICMP トンネルが作成されます。

M

MainApp IPS のメイン アプリケーション。オペレーティング システムのブート後、センサーで最初に起動するアプリケーションです。設定を読み取ってアプリケーションを起動し、アプリケーションの開始および終了とノードの再起動を扱い、ソフトウェアのアップグレードを処理します。

MD5 Message Digest 5。128 ビット ハッシュを作成する単方向のハッシュ アルゴリズム。MD5 とセキュア ハッシュ アルゴリズム（SHA）は MD4 のバリエーションで、MD4 のハッシュ アルゴリズムのセキュリティを強化したものです。シスコでは、IPSec フレームワーク内での認証にハッシュを使用します。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。

Meta エンジン 変化する時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。

MIB 管理情報ベース。SNMP や CMIP などのネットワーク管理プロトコルによって使用および維持されるネットワーク管理情報のデータベース。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

MIME Multipurpose Internet Mail Extension。インターネット メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を伝送するための標準。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045 で定義されています。

MPF モジュラ ポリシー フレームワーク。Cisco IOS ソフトウェアのモジュラ QoS CLI と同様の方法でセキュリティアプライアンスの機能を設定するための手段です。

MSFC、MSFC2 マルチレイヤ スイッチ フィーチャ カード。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、スイッチの L3 ルーティングを実行します。

MSRPC Microsoft Remote Procedure Call。MSRPC は、マイクロソフトによる DCE RPC メカニズムの実装です。マイクロソフトは、Unicode 文字列、暗黙の処理、インターフェイスの継承（DCOM で広く使用されています）、および可変長文字列での複雑な計算や、DCE/RPC の既存の構造パラダイムに対するサポートを追加しました。

MySDN My Self-Defending Network。IDM および IME のシグニチャ定義セクションの一部。シグニチャに関する詳細な情報を提供します。

N

NAC Network Access Controller。「ARC」を参照してください。

NAS-ID ネットワーク アクセス ID。クライアントが認証を試行しているサービスのタイプを伝達するためにサーバに送信する識別子です。

NAT Native Address Translation。ネットワーク デバイスが外部ネットワークに対してホストの実際の IP アドレスとは異なる IP アドレスを提示できるしくみ。

NBD 翌営業日。シスコ サービス契約に従って交換用ハードウェアが到着します。

never block アドレス ブロックされることのないように指定したホストおよびネットワーク。

never shun アドレス 「never block アドレス」を参照。

NIC ネットワーク インターフェイス カード。コンピュータ システムに出入りするネットワーク通信機能を提供するボードです。

NME IPS Network Module Enhanced。Cisco 2800 および 3800 シリーズ サービス統合型ルータの任意のネットワーク モジュール スロットに取り付けることができる IPS モジュールです。

NMS Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。NMS は、一般的に適度にパワーのある装備の整ったコンピュータで、エンジニアリング ワークステーションなどです。NMS はエージェントと通信して、ネットワーク統計情報やリソースを追跡するのに役立ちます。

NOS ネットワーク OS。分散ファイル システムを指す一般的な用語。たとえば、LAN Manager、NetWare、NFS、VINES などがあります。

NotificationApp IPS のコンポーネントの 1 つです。アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp はパブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的なヘルスに関する情報を提供します。

NTP Network Timing Protocol。インターネット内に置かれている無線時計および原子時計を参照することにより、正確な現地時間を維持するプロトコル。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

NTP サーバ ネットワーク タイム プロトコル（Network Timing Protocol）サーバ。NTP を使用するサーバ。NTP は、TCP 上に構築されたプロトコルで、インターネット上にあるラジオおよびアトミック クロックを参照して正確なローカル タイムを維持します。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

NVRAM Non-Volatile Read/Write Memory。RAM は、ユニットの電源が切られた後も内容を保持します。

O

OIR 活性挿抜。システム電源の中断、コンソール コマンドの入力、他のソフトウェアまたはインターフェイスのシャットダウンを行うことなく、カードの追加、交換、または取り外しができる機能。

OPS Outbreak Prevention Service。

P

PAgP Port Aggregation Control Protocol。PAgP は、PAgP パケットを LAN ポート間で交換することにより、EtherChannel リンクの自動作成を支援します。これはシスコ独自のプロトコルです。

PAM アプリケーションに AAA 機能を提供するソフトウェア モジュール。

PAP パスワード認証プロトコル。最も一般的に使用される RADIUS メッセージング プロトコル。

PASV ポート スプーフィング ファイアウォールを通過し、保護された FTP サーバを経由して FTP 以外のポートへの接続をオープンしようとする試み。これは、不正な接続をオープンすることにより、ファイアウォールが FTP 227 **passive** コマンドを誤って解釈した場合に発生します。

PAT ポート アドレス変換。NAT より制限された変換方式で、1 つの IP アドレスと複数の異なるポートを使用してネットワークのホストを表します。

PAWS Protection Against Wrapped Sequence。高性能な TCP ネットワークでのラップされたシーケンス番号に対する保護。RFC 1323 を参照してください。

PCI Peripheral Component Interface。Intel ベースのコンピュータで、最も一般的に使用されている周辺拡張バス。

PDU プロトコル データ ユニット。OSI の用語で、パケットを表します。「BPDU」、「パケット」も参照してください。

PEP Cisco Product Evolution Program。PEP は、センサーの PID、VID、および SN から構成される UDI 情報です。PEP は、電子的なクエリー、製品ラベル、および出荷項目などを通じて、ハードウェア バージョンおよびシリアル番号を示します。

PER 圧縮符号化規則。PER は、一様の方法ですべてのタイプを符号化する汎用の符号化方式を使用するのではなく、データ タイプに基づいて符号化を特化し、よりコンパクトな表現を生成します。

PFC ポリシー フィーチャ カード（Policy Feature Card）。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、VACL パケットのフィルタ処理をサポートします。

PID Product Identifier。注文可能な製品 ID で、UDI の 3 つの部分の 1 つです。UDI は、PEP ポリシーの一部です。

ping packet internet groper。ネットワーク デバイスの到達可能性をテストするために、IP ネットワークでよく使用されます。ICMP エコー要求パケットをターゲット ホストに送信し、エコー応答の返信をリッスンすることで機能します。

PIX ファイアウォール Private Internet Exchange Firewall。シスコのネットワーク セキュリティ デバイスで、プログラミングによってネットワーク間でアドレスとポートをブロックしたり使用可能にしたりできます。

PKI 公開キー インフラストラクチャ（Public Key Infrastructure）。クライアントの X.509 証明書を使用した HTTP クライアントの認証です。

Point-to-Point（P2P; ポイントツーポイント） ピアツーピア。P2P ネットワークでは、ファイル共有のためにクライアントとサーバの両方として同時に機能できるノードを使用します。

POST 電源投入時自己診断テスト。デバイスに電源が投入されたときに、ハードウェア デバイスで実行されるハードウェア診断のセット。

Post-ACL ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの後ろにエントリを入れる ACL を指定します。

Pre-ACL ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの前にエントリを入れる ACL を指定します。

Q

Q.931 ISDN ネットワーク接続の確立、維持、および終了のシグナリングに関する ITU-T の仕様。

QoS Quality of Service。伝送システムのパフォーマンスを基に、その伝送品質とサービスのアベイラビリティを表します。

R

RADIUS ネットワーク サービスに接続して使用するシステムに、集中化された AAA 機能を提供するネットワーキング プロトコル。

RAM ランダムアクセス メモリ。マイクロプロセッサによる読み取りと書き込みが可能な揮発性メモリです。

RAS Registration, Admission, and Status プロトコル。管理機能を実行するためにエンドポイントとゲートキーパー間で使用されるプロトコルです。RAS シグナリング機能は、VoIP ゲートウェイとゲートキーパー間で、登録、許可、帯域幅変更、ステータス、および解放手順を実行します。

RBCP Router Blade Control Protocol。RBCP は、SCP をベースにしていますが、ルータ アプリケーション用に特別に変更されています。イーサネット インターフェイス上で動作するように設計されており、メッセージには 802.2 SNAP カプセル化を使用します。

regex 「正規表現」を参照。

Remote Authentication Dial In User Service 「RADIUS」を参照してください。

RMA 返品許可。故障したハードウェアを返却して交換用ハードウェアを入手するためのシスコのプログラム。

ROMMON ROM モニタ（Read-Only-Memory Monitor）。ROMMON は、復旧のためにシステム イメージをセンサーに TFTP 転送できます。

RPC リモート プロシージャ コール。クライアント / サーバ コンピューティングの技術的基盤です。RPC は、クライアントで作成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。

RSM Router Switch Module。Catalyst 5000 スイッチに取り付けるルータ モジュール。スタンドアロン ルータとまったく同様に機能します。

RTP Real-Time Transport Protocol（リアルタイム転送プロトコル）。一般に、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャストのネットワーク サービスとして、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供するように設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプ処理、配信のモニタリングなどのサービスをリアルタイム アプリケーションに提供します。

RTT ラウンドトリップ時間。パケットの送信から受信の確認応答までに、ネットワークによってホストに発生する時間遅延の指標。

RU ラック ユニット。ラックは、ラック ユニットで測定します。1 RU は、44 mm つまり 1.75 インチです。

S

SCEP Simple Certificate Enrollment Protocol。PKCS#7 および PKCS#10 の使用によって既存のテクノロジーを活用した、シスコの PKI 通信プロトコルです。SCEP は進化した登録プロトコルです。

SCP Switch Configuration Protocol。イーサネット上で直接動作するシスコの制御プロトコルです。

SDEE Security Device Event Exchange。セキュリティ デバイスのイベントを伝達するための、製品に依存しない標準です。各種のセキュリティ デバイスによって生成されるイベントの伝達に必要な拡張機能が追加されています。

SDEE サーバ リモート クライアントからイベントの要求を受け付けます。

Secure Shell Protocol 伝送制御プロトコル（TCP）アプリケーションを介して、ルータへのセキュア リモート接続を提供するプロトコルです。

Security Monitor Monitoring Center for Security。ネットワーク デバイスに、イベントの収集、表示、および報告の機能を提供します。IDS MC とともに使用されます。

SensorApp IPS のコンポーネントの 1 つです。パケットの取り込みと分析を実行します。SensorApp は、ネットワーク トラフィックを分析して悪意のあるコンテンツを調べます。パケットは、センサー上のネットワーク インターフェイスからパケットを収集するように設計されたプロデューサが提供する、プロセッサのパイプラインを通過します。SensorApp は、分析エンジンで稼動するスタンドアロンの実行可能ファイルです。

session コマンド ルータとスイッチに対して使用されるコマンドで、ルータまたはスイッチ内のモジュールに対して Telnet またはコンソールのいずれかによるアクセスを提供します。

SFP Small Form Factor Pluggable。多くの場合、ファイバ インター フェイスに光ケーブル接続を適合させる光ファイバ トランシーバを指します。詳細については、「GBIC」を参照してください。

shun コマンド 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。PIX Firewall によるブロッキング時に ARC によって使用されます。

SMB サーバ メッセージ ブロック。データをパッケージ化し、他のシステムと情報を交換するために LAN マネージャおよび類似の NOS が使用するファイルシステム プロトコル。

SMTP Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。E メール サービスを提供するインターネット プロトコル。

SN Serial Number（シリアル番号）。UDI の一部です。SN は、ご使用のシスコ製品のシリアル番号です。

SNAP サブネットワーク アクセス プロトコル。サブネットワーク内のネットワーク エンティティとエンド システム内のネットワーク エンティティ間で動作するインターネット プロトコルです。SNAP は、IEEE ネットワーク上で IP データグラムと ARP メッセージをカプセル化する標準方式を指定します。エンド システム内の SNAP エンティティは、サブネットワークのサービスを利用して、3 つの重要な機能（データ転送、接続管理、および QoS 選択）を実行します。

SNMP 簡易ネットワーク管理プロトコル。TCP/IP ネットワークでほぼ独占的に使用されているネットワーク管理プロトコルです。SNMP を使用すると、ネットワーク デバイスのモニタリングと制御、および設定、統計情報収集、パフォーマンス、セキュリティの管理が可能になります。

SNMP2 SNMP バージョン 2。ネットワーク管理プロトコルのバージョン 2 です。SNMP2 では、集中型および分散型のネットワーク管理方式がサポートされ、SMI、プロトコル動作、管理アーキテクチャ、およびセキュリティが改善されています。

SPAN スイッチド ポート アナライザ。Catalyst 5000 スイッチの機能。既存のネットワーク アナライザのモニタリング機能をスイッチ型イーサネット環境に拡張します。SPAN は、1 つのスイッチド セグメントのトラフィックを事前定義済みの SPAN ポートにミラーリングします。SPAN ポートに接続されたネットワーク アナライザで、その他の任意の Catalyst スイッチド ポートからのトラフィックをモニタできます。

SQL 構造化照会言語。リレーショナル データベースの定義およびアクセスに使用する国際的な標準言語です。

SRAM RAM の一種で、電源が供給されている限り、内容を保持します。SRAM では、DRAM のように定期的なリフレッシュは必要ありません。

SSH Secure Shell（セキュア シェル）。強力な認証と安全な通信を使用してネットワーク上の別のコンピュータにログインするユーティリティ。

SSL Secure Socket Layer。e- コマースにおけるクレジットカード番号の転送など、安全なトランザクションを提供するために使用されるインターネット用暗号化テクノロジー。

Stacheldraht ICMP プロトコルに依存する DDoS ツール。

State エンジン HTTP ストリングのステートフル検索。

String エンジン シグニチャ エンジンの 1 つ。正規表現ベースのパターン検査、および、TCP、UDP、ICMP などの複数の転送プロトコルのアラート機能を提供します。

SYN フラッド プロトコルの実装で処理可能な数を超える多数の TCP SYN パケット（接続開始時に使用されるシーケンス番号の同期化要求）をホストに送信する DoS 攻撃。

T

TAC Cisco Technical Assistance Center。TAC は、世界中に 4 箇所にあります。

TACACS+ Terminal Access Controller Access Control System Plus（ターミナル アクセス コントローラ アクセス コントロール システム プラス）。シスコが強化した専用の Terminal Access Controller Access Control System（TACACS）。認証、許可、アカウンティングに追加サポートを提供します。

TCP 伝送制御プロトコル。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

TCP リセット インターフェイス TCP リセットを送信できる、IDSM-2 上のインターフェイス。ほとんどのセンサーでは、パケットがモニタされるセンシング インターフェイスと同じインターフェイスで TCP リセットが送信されますが、IDSM-2 では、センシング インターフェイスを TCP リセットの送信に使用することができません。IDSM-2 の場合、TCP リセット インターフェイスは、Catalyst ソフトウェアでポート 1 として指定され、Cisco IOS ソフトウェアのユーザには表示されません。TCP リセット アクションは、TCP ベースのサービスに関連するシグニチャ上のアクションとして選択したときだけ有効なアクションとなります。

TCPDUMP TCPDUMP ユーティリティは、フリーの Unix および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。さまざまなオプションを使用して、各パケットの要約情報と詳細情報を表示できます。詳細については、http://www.tcpdump.org/ を参照してください。

Telnet TCP/IP プロトコル スタックにおける標準の端末エミュレーション プロトコル。Telnet はリモート端末接続に使用され、ユーザはこれを使用してリモート システムにログインし、そのリソースを、ローカル システムに接続されているかのように使用することができます。Telnet は RFC 854 で定義されています。

TFN Tribe Flood Network。一般的なタイプの DoS 攻撃で、偽造の、またはすぐに変更される送信元 IP アドレスを利用して、攻撃の特定やフィルタリングを攻撃者が阻止できます。

TFN2K Tribe Flood Network 2000。一般的なタイプの DoS 攻撃で、偽造の、またはすぐに変更される送信元 IP アドレスを利用して、攻撃の特定やフィルタリングを攻撃者が阻止できます。

TFTP Trivial File Transfer Protocol。FTP の単純なバージョンで、1 つのコンピュータから別のコンピュータに、通常はクライアント認証（ユーザ名とパスワードなど）を使用せずにネットワークを介してファイルを転送できます。

TLS Transport Layer Security。ピアの ID をネゴシエートし、暗号化通信を確立するために、ストリーム転送で使用されるプロトコル。

TNS Transparent Network Substrate。すべての業界標準ネットワーク プロトコルに対する 1 つの共通インターフェイスをデータベース アプリケーションに提供します。TNS を使用するデータベース アプリケーションは、異なるプロトコルを使用するネットワークを介して他のデータベース アプリケーションに接続できます。

TPKT Transport Packet。RFC 1006 で定義された、パケット内のメッセージのマーキングを解除するための方式。このプロトコルでは TCP の最上位の ISO 転送サービスを使用します。

traceroute パケットが宛先に到達するまでに通過するパスをトレースするプログラムのことで、多数のシステムで使用可能です。主に、ホスト間のルーティングの問題をデバッグする際に使用されます。traceroute プロトコルは、RFC 1393 でも定義されています。

Traffic ICMP エンジン TFN2K、LOKI、DDOS などの非標準プロトコルからのトラフィックを分析します。

Trojan エンジン BO2K および TFN2K などの非標準プロトコルからのトラフィックを分析します。

U

UDI Unique Device Identifier。シスコの各製品を一意に識別できます。UDI は、PID、VID、および SN から構成されています。UDI は Cisco IPS の ID PROM に保存されています。

UDLD 単方向リンク検出。LAN ポートに接続された光ファイバまたは銅製イーサネット ケーブルを使用して接続された装置で、ケーブルの物理構成をモニタし、単方向リンクの存在を検出できるようにするシスコ独自のプロトコルです。単方向リンクが検出されると、UDLD は影響を受ける LAN ポートをシャットダウンし、アラートを送信します。単方向リンクは、スパニング ツリー トポロジのループなど、さまざまな問題を引き起こす可能性があるためです。

UDP ユーザ データグラム プロトコル。TCP/IP プロトコル スタックのコネクションレス型トランスポート層プロトコルです。UDP は、確認応答や配信保証なしでデータグラムを交換する単純なプロトコルです。エラー処理と再送信は、他のプロトコルで処理する必要があります。UDP は RFC 768 で定義されています。

UPS Uninterruptable Power Source。

UTC Coordinated Universal Time（協定世界時）。経度ゼロの時間帯です。以前はグリニッジ標準時（GMT）およびズールー時と呼ばれていました。

UTF-8 8-bit Unicode Transformation Format。Unicode に対応する可変長文字符号化です。UTF-8 は Unicode 文字セットのすべての文字を表示することができ、ASCII と下位互換性があります。

V

VACL VLAN ACL。スイッチを経由して渡されるすべてのパケット（VLAN 内および VLAN 間）をフィルタする ACL。セキュリティ ACL とも言います。

VID バージョン ID。UDI の一部です。

VIP Versatile Interface Processor。Cisco 7000 および Cisco 7500 シリーズ ルータで使用されるインターフェイス カードです。VIP は、マルチレイヤ スイッチングを行い、Cisco IOS を実行します。VIP の最新バージョンは VIP2 です。

VLAN バーチャル LAN（Virtual Local Area Network）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイスのグループで、これらのデバイスは、実際には異なる複数の LAN セグメントに配置されていたとしても、同じケーブルに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づくため、非常に柔軟です。

VMS CiscoWorks VPN/Security Management Solution。さまざまな Web ベース ツールを組み合わせた、ネットワーク セキュリティ アプリケーション スイート。これらのツールは、エンタープライズ VPN、ファイアウォール、ネットワーク侵入検知システム、およびホストベースの侵入防御システムを構成、管理、およびトラブルシューティングするために使用できます。

VoIP Voice over IP。POTS と同様の機能、信頼性、および音声品質を備えた、IP ベースのインターネット上で通常のテレフォニー スタイルの音声を伝送する機能。VoIP を使用すれば、ルータから IP ネットワーク上で音声トラフィック（通話や FAX など）を伝送できます。VoIP では、DSP が音声信号をフレームに分割します。その後、フレームは、2 つずつ連結され、音声パケットに保存されます。これらの音声パケットは、ITU-T 仕様の H.323 に従って、IP を使用して送信されます。

VPN バーチャル プライベート ネットワーク（ネットワーキング）。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

VTP VLAN トランキング プロトコル。ネットワーク全体での VLAN の追加、削除、および名前変更を管理するシスコのレイヤ 2 メッセージング プロトコルです。

VTP VLAN トランキング プロトコル。ネットワーク全体での VLAN の追加、削除、および名前変更を管理するシスコのレイヤ 2 メッセージング プロトコルです。

W

WAN Wide-Area Network（ワイドエリア ネットワーク）。広大な地理的地域のユーザにサービスを提供し、通常は、コモン キャリアが提供する伝送デバイスを使用するデータ通信ネットワークです。フレーム リレー、SMDS、および X.25 が WAN の例です。

Web サーバ IPS のコンポーネントの 1 つです。リモート HTTP クライアント要求を待機し、適切なサーブレット アプリケーションを呼び出します。

WHOIS TCP ベースのクエリー / 応答プロトコルで、公式データベースに照会してドメイン名または IP アドレスの所有者を判別するのに使用します。

Wireshark Wireshark は、フリーの Unix および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。対話的にキャプチャ データをブラウズし、各パケットの要約情報と詳細情報を表示できます。Wireshark には、機能豊富な表示フィルタ言語や TCP セッションの再構築されたストリームの表示機能など、いくつかの強力な機能があります。詳細については、http://www.wireshark.org を参照してください。

X

X.509 証明書に含まれる情報を定義する標準。

XML eXtensible Markup Language。異種ホスト間のデータ交換に使用されるテキスト ファイル形式。

XPI Cross Packet Inspection。TCP で使用されるテクノロジー。複数パケットにわたる検索を可能にすることで、パケットおよびペイロードの再構成を実現します。

あ

アーキテクチャ コンピュータまたは通信システムの全体的な構造。アーキテクチャは、システムの機能と制限に影響を与えます。

アクション イベントに対するセンサーの応答。アクションは、イベントがフィルタ処理されない場合にだけ発生します。たとえば、TCP リセット、ホストのブロック、接続のブロック、IP ロギング、アラート トリガー パケットのキャプチャなどがあります。

アクティブ ACL ARC によって作成、管理される ACL。ルータのブロック インターフェイスに適用されます。

アスペクト バージョン IDIOM デフォルト設定のグループに関連付けられたバージョン情報。たとえば、シスコは、攻撃シグニチャの標準セットを S アスペクトのデフォルト設定の集合として公開しています。S アスペクトのバージョン番号は、シグニチャ アップデート パッケージ ファイル名の S の後に表示されています。その他のアスペクトとして、V アスペクトのウイルス シグニチャ定義や、キーアスペクトの IDIOM 署名キーなどがあります。

アトミック アタック 単一のパケット内に含まれている不正利用を表します。たとえば、「Ping of Death」攻撃は、異常に大きな単一の ICMP パケットです。

アプリケーション Cisco IPS 環境で動作するように設計された任意のプログラム（プロセス）。

アプリケーション イメージ センサーの稼働に使用される永続的なストレージ デバイスに格納された完全な IPS イメージ。

アプリケーション インスタンス IPS 環境の特定のハードウェアで動作する特定のアプリケーション。アプリケーション インスタンスには、その名前と、ホスト コンピュータの IP アドレスによってアドレス可能です。

アプリケーション パーティション IPS ソフトウェア イメージを含むブート可能ディスクまたはコンパクトフラッシュ パーティション。

アラート 厳密には IPS のイベント タイプの 1 つを指し、evidsAlert としてイベント ストアに書き込まれます。一般に、アラートは、ネットワークの不正利用が進行中であるか、潜在的なセキュリティの問題が発生していることを示す IPS メッセージです。アラームとも言います。

アラーム チャネル インスペクタによって生成されたすべてのシグニチャ イベントを処理する IPS ソフトウェア モジュール。主な機能は、受け取った各イベントのアラートを生成することです。

宛先アドレス データを受信するネットワーク デバイスのアドレス。

暗号化 データに特殊なアルゴリズムを適用してそのデータの外見を変更し、その情報を読む許可を与えられていないユーザには理解できないようにすること。

暗号キー 平文と暗号文の間の変換に使用されるシークレット バイナリ データ。暗号化と復号化に同じ暗号キーが使用される場合を対称と言います。暗号キーが暗号化と復号化のいずれかに使用される（両方ではない）場合を非対称と言います。

い

イベント アラート、ブロック要求、ステータス メッセージ、またはエラー メッセージを含む IPS メッセージ。

イベント ストア IPS のコンポーネントの 1 つです。IPS イベントの格納に使用される、固定サイズのインデックス付きストアです。

インライン インターフェイス センサーがペアの一方のインターフェイスで受信したすべてのトラフィックを他方のインターフェイスに転送するように設定された、物理インターフェイスのペア。

インライン モード ネットワークに出入りするすべてのパケットがセンサーを通過する必要があります。

異常検出 AD。正常なネットワーク トラフィックのベースラインを作成し、このベースラインを使用してワームに感染したホストを検出するセンサーのコンポーネント。

う

ウイルス コンピュータ ソフトウェア内で隠れた、自己複製を行うセクション。通常は悪質で、感染により増殖します。感染とは、自身のコピーを挿入して、別のプログラムの一部になることです。ウイルスは、それ自体では実行不可能です。ウイルスをアクティブにするには、ホスト プログラムが実行されている必要があります。

ウイルス アップデート 特にウイルスに対処するシグニチャ アップデート。

ウォッチ リスト レーティング WLR。CSA MC ウォッチ リストに関連付けられた 0 ～ 100 の重みです（CSA MC で使用するのは 0 ～ 35 の範囲のみ）。

え

エスケープ表現 正規表現で使用されます。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。

エンジン センサーのコンポーネントの 1 つ。特定の 1 つのカテゴリで多数のシグニチャをサポートするように設計されています。各エンジンには、シグニチャの作成や既存のシグニチャの調整に使用できるパラメータがあります。

エンタープライズ ネットワーク 企業などの組織内で大部分の主要ポイントを接続する、大規模で多様なネットワーク。私的に所有され、保守される点で WAN とは異なります。

か

カットスルー アーキテクチャ カットスルー アーキテクチャは、パケットスイッチング システムの設計方法の 1 つです。パケットがスイッチに到着すると、スイッチはパケットの最初の数バイトだけを読み取って宛先アドレスを確認し、そのパケットの転送をほぼ即時に開始します。この手法によってパフォーマンスが向上します。

仮想センサー シグニチャ エンジンのセンシング インターフェイスと設定ポリシー、およびシグニチャ エンジンに適用するアラーム フィルタの論理グループ。つまり、それぞれが異なるシグニチャの動作とトラフィック供給で設定された、同一アプライアンス上で動作する複数の仮想センサーです。

仮想化センシング インターフェイス 仮想化インターフェイスは、サブインターフェイスに分割されており、各サブインターフェイスは VLAN のグループで構成されます。仮想センサーを 1 つ以上のサブインターフェイスに関連付けて、さまざまな侵入防御ポリシーをこれらのサブインターフェイスに割り当てることができます。物理インターフェイスとインライン インターフェイスのどちらも仮想化できます。

き

偽陰性 不正なトラフィックが検出されたときにシグニチャが起動されない状態。

偽陽性 正常なトラフィックまたは良好なアクションによってシグニチャが起動される状態。

拒否フィルタ プロセッサ IPS 内のプロセッサの 1 つです。攻撃者拒否機能を処理します。拒否された送信元 IP アドレスのリストを管理します。

共有秘密情報 セキュアな通信の関係者だけに知らされるデータ。共有秘密は、パスワード、パスフレーズ、大きな数値、またはランダムに選択されたバイトの配列です。

脅威レーティング TR。脅威レーティングは、モニタ対象ネットワークでのアラートの脅威を表す応答アクションに基づいて、攻撃に関するリスク レーティングの低下を 0 ～ 100 の数字で表した値です。

く

クッキー Web サーバから Web ブラウザに送信される情報で、ブラウザによって保存されます。ブラウザは、Web サーバに対して追加要求を行うときに、Web サーバにこの情報を送り返します。

グローバル相関 IPS センサーは、グローバル相関データベースを通じて他のデバイスと情報を共有することにより、すべてのデバイスの総合的効果を高めます。

グローバル相関クライアント アップデートを取得してローカルのグローバル相関データベースにインストールする CollaborationApp のソフトウェア コンポーネント

グローバル相関データベース IPS センサーなどのコラボレーション デバイスから取得し、それらと共有する集合的な情報。

こ

コマンド / コントロール インターフェイス IPS マネージャなどのネットワーク デバイスと通信する、センサー上のインターフェイス。このインターフェイスには IP アドレスが割り当てられています。

コミュニティ SNMP における、同じ管理ドメイン内の管理対象デバイスと NMS の論理グループ。

コンソール センサーのモニタと制御に使用される端末またはラップトップ コンピュータ。

コンソール ポート センサーでコンソール デバイスへの接続に使用される、RJ45 シリアル ポートまたは DB9 シリアル ポート。

コンポジット アタック 単一セッションで複数のパケットに及びます。たとえば、FTP、Telnet、およびほとんどの正規表現ベースの攻撃など、ほとんどの会話型攻撃が含まれます。

攻撃の重大度レーティング ASR。脆弱性の不正利用が成功した場合の重大度に関連付けられた重みです。攻撃の重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）からの派生値です。攻撃の重大度レーティングは、シグニチャごとに設定され、検出されたイベントの危険度を示します。

攻撃関連性レーティング ARR。ターゲット OS の関連性に関連付けられた重みです。攻撃関連性レーティングは派生値（relevant、unknown、または not relevant）で、アラート時に決定されます。関連する OS はシグニチャごとに設定されます。

混合モード ネットワーク セグメントのパケットをモニタするパッシブ インターフェイス。センシング インターフェイスには IP アドレスが割り当てられていないため、攻撃者からは見えません。

さ

サービス エンジン DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SQL、NTP、P2P、RPC、SMB、SNMP、SSH、および TNS などの特定のプロトコルを処理します。

サービス パック 障害フィックスのリリース、および新しいシグニチャ エンジンのサポートのために使用されます。サービス パックには、前回のベース バージョン（マイナーまたはメジャー）以降に発生したすべての障害フィックスと、新しい障害フィックスが含まれています。

サブシグニチャ 一般のシグニチャより細分化されたシグニチャ。通常は、より広い範囲のシグニチャをさらに定義します。

再パッケージ リリース パッケージまたはインストーラの障害に対処するリリース。

再構成 送信元または中間ノードでフラグメント化された IP データグラムを、宛先で組み立てて元に戻すこと。

し

しきい値 アラートが送信されるまでに許容される最大 / 最小の条件を定義する、上限または下限の値。

シグニチャ シグニチャは、ネットワーク情報を抽出して、一般的な侵入アクティビティを示した規則セットと比較します。

シグニチャ アップデート ワーム、DDOS、ウイルスなどの悪意のあるネットワーク アクティビティを認識するように設計された一連の規則が含まれる実行可能ファイル。シグニチャ アップデートは単独でリリースされ、必要なシグニチャ エンジン バージョンに依存し、独自のバージョン管理方式を持っています。

シグニチャ イベント アクション オーバーライド リスク レーティング値に基づいて、アクションを追加します。シグニチャ イベント アクション オーバーライドは、設定済みのリスク レーティングしきい値の範囲内にあるすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立しており、各アクション タイプには別個の値が設定されています。

シグニチャ イベント アクション ハンドラ 要求されたアクションを実行します。シグニチャ イベント アクション ハンドラから出力されるのは、実行中のアクションだけでなく、イベント ストアに書き込まれる evIdsAlert である可能性があります。

シグニチャ イベント アクション フィルタ シグニチャ イベントのシグニチャ ID、アドレス、およびリスク レーティングに基づいてアクションを削除します。シグニチャ イベント アクション フィルタへ入力するのは、シグニチャ イベント アクション オーバーライドによって追加される可能性のあるアクションを持つシグニチャ イベントです。

シグニチャ イベント アクション プロセッサ イベント アクションを処理します。イベント アクションは、イベント リスク レーティングしきい値と関連付けできます。アクションが実行されるには、このしきい値を超える必要があります。

シグニチャ エンジン センサーのコンポーネントの 1 つ。特定のカテゴリで多数のシグニチャをサポートします。エンジンは、パーサーとインスペクタで構成されています。各エンジンには規定のパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。

シグニチャ エンジン アップデート 新しいシグニチャ アップデートをサポートするバイナリ コードが含まれた、独自のバージョン管理方式の実行可能ファイル。

シグニチャ忠実度レーティング SFR。ターゲットに関する具体的な情報がない場合に、シグニチャをどの程度忠実に実行するかに関連付けられた重みです。シグニチャ忠実度レーティングは、シグニチャごとに設定され、イベントや記述する条件をシグニチャがどの程度正確に検出するかを示します。

シグニチャ分析プロセッサ IPS 内のプロセッサの 1 つです。ストリームベースでなく、処理中のパケット用に設定されているインスペクタにパケットをディスパッチします。

システム イメージ センサー全体のイメージの再作成に使用される、IPS アプリケーションとリカバリの完全なイメージ。

自動ステート 通常自動ステート モードでは、少なくとも VLAN 上のポートが 1 つでもアップしていればレイヤ 3 インターフェイスはアップしたままになります。VLAN 上のポートにロード バランサやファイア ウォール サーバなどのアプライアンスが接続されている場合、これらのポートを自動ステート機能から除外するように設定して、これらのポートが非アクティブの場合でも転送 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）がダウンしないようにできます。

出力 ネットワークから出ていくトラフィック。

信頼できるキー ユーザが信頼する公開キー。特に、認証パスで最初の公開キーとして使用される公開キー。

信頼できる証明書 検証テストの必要なしに証明書ユーザが有効であることを示す証明書。特に公開キー証明書は、認証パスの最初の公開キーを提供するために使用されます。

侵入検知システム IDS。不正な方法によるシステム リソースへのアクセスの試みを発見し、リアルタイムまたはそれに近い形で警告を与えるために、システム イベントのモニタリングと分析を行うセキュリティ サービス。

す

スイッチ 各フレームの宛先アドレスに基づいて、フレームをフィルタリング、転送、およびフラッディングするネットワーク デバイス。スイッチは OSI モデルのデータリンク層で動作します。

ストリーム再構成プロセッサ IPS 内のプロセッサの 1 つです。さまざまなストリームベース インスペクタでパケットが適切な順序で到着するよう、TCP ストリームを並べ替えます。また、TCP ストリームの正規化も行います。ノーマライザ エンジンを使用すると、アラートおよび拒否アクションをイネーブルまたはディセーブルにできます。

スニファ インターフェイス 「センシング インターフェイス」を参照。

スパニング ツリー ネットワーク トポロジのループフリーのサブセット。

スリーウェイ ハンドシェイク 接続を確立する間に、2 つのプロトコル エンティティが同期するプロセス。

スレーブ ディスパッチ プロセッサ IPS 内のプロセッサの 1 つです。デュアル CPU システムに存在するプロセスです。

据え置き 平らな面に設置する場合にセンサー底部にゴム脚を取り付けます。ゴム脚を使用すると、センサーの周りに適正なエアーフローが確保され、振動を吸収するので、ハードディスク ドライブへの衝撃が軽減されます。

せ

セキュリティ コンテキスト 1 つの適応型セキュリティ アプライアンスは複数の仮想デバイスに分割できます。これをセキュリティ コンテキストと呼びます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチコンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。

センサー 侵入検知エンジンのことです。不正行為の兆候を探してネットワーク トラフィックを分析します。

センシング インターフェイス 目的のネットワーク セグメントをモニタする、センサー上のインターフェイス。センシング インターフェイスは、混合モードです。つまり、IP アドレスを持たず、モニタしたセグメント上では見えません。

制御インターフェイス ARC では、ネットワーク デバイスと Telnet または SSH セッションを開くときに、そのデバイスのルーティング インターフェイスの 1 つがリモート IP アドレスとして使用されます。これが制御インターフェイスです。

制御トランザクション CT。特定のアプリケーション インスタンスに対して出されたコマンドを含む IPS メッセージ。制御トランザクションは、管理アプリケーションと IPS センサー間、または同じ IPS センサー上のアプリケーション間で送信できます。制御トランザクションには、*start*、*stop*、*getConfig* などがあります。

正規表現 データ ストリームまたはファイル内で指定された文字シーケンスを検索する方法を定義できるメカニズム。正規表現は高機能かつ柔軟な表記法で、テキストを表現するためのミニ プログラミング言語のようなものです。パターン マッチングでは、正規表現によりあらゆる任意のパターンを簡潔に表記できます。

脆弱性 コンピュータやネットワークの悪用パターンが開始されやすい状況を許す、当該コンピュータやネットワークの 1 つ以上の属性。

接続ブロック ARC による、特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックのブロック。

全二重 送信ステーションと受信ステーションの間で、同時にデータを伝送する機能。

そ

ソフトウェア バイパス トラフィックを検査することなく IPS システムを通過させます。

ゾーン 異常検出が使用する内部ゾーン、不正ゾーン、または外部ゾーンに分類される一連の宛先 IP アドレス。

送信元アドレス データを送信するネットワーク デバイスのアドレス。

ち

調整 シグニチャ パラメータを調整して既存のシグニチャを変更すること。

た

ターゲットの価値レーティング TVR。認識されるターゲットの価値に関連付けられた重みです。ターゲットの価値レーティングは、ユーザ設定可能な値（zero、low、medium、high、または mission critical）で、ネットワーク資産（IP アドレスを使用）の重要性を示します。

ターミナル サーバ 他のシリアル デバイスに接続された複数の低速な非同期ポートを搭載したルータ。ターミナル サーバは、センサーを含むネットワーク機器をリモートで管理する場合に利用できます。

タイム プロセッサ IPS 内のプロセッサの 1 つです。タイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、失効したデータベース エントリを期限切れにし、時間に依存する統計を計算することです。

ダークネット ユーザが信頼する人にだけ接続するバーチャル プライベート ネットワーク。最も一般的な意味では、ダークネットは、通信を行うあらゆる種類の非公開のプライベート ユーザ グループである可能性がありますが、この名前は、ほとんどの場合、ファイル共有ネットワークに対して使用されます。ダークネットは、すべての隠れた通信ネットワークの総称として使用できます。

単方向リンク検出 「UDLD」を参照してください。

て

データグラム 事前に仮想回線を確立することなく、伝送媒体上のネットワーク層ユニットとして送信される情報の論理的なグループ化。IP データグラムは、インターネットにおける主な情報単位です。セル、フレーム、メッセージ、パケット、およびセグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

データベース プロセッサ IPS 内のプロセッサの 1 つです。シグニチャの状態とフロー データベースを管理します。

適応型セキュリティ アプライアンス ASA。ファイアウォール、VPN コンセントレータ、および侵入防御ソフトウェア機能を 1 つのソフトウェア イメージに結合します。適応型セキュリティ アプライアンスは、シングル モードまたはマルチモードで設定できます。

と

トポロジ 企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

トラップ SNMP エージェントから NMS、コンソール、または端末に送られ、具体的に定義された条件や、しきい値に達したなどの、重要なイベントが発生したことを伝えるメッセージ。

トラフィック分析 データが暗号化されている場合、または直接使用可能でない場合にも、データ フローの観測可能な特徴から情報を推理すること。このような特徴には、発信元と宛先（複数の場合もある）の ID と場所や、事象の存在、回数、頻度、期間などがあります。

トランク ネットワーク トラフィックが通過する 2 つのスイッチ間の物理的および論理的接続。バックボーンは、複数のトランクによって構成されています。

統計情報プロセッサ IPS 内のプロセッサの 1 つです。パケット カウントやパケットの到着レートなど、システム統計情報を継続して追跡します。

な

ナレッジ ベース 「KB」を参照してください。

に

認証 ユーザがシステムを使用する権限を持っていることを確認する処理。通常はパスワード キーまたは証明書によって行われます。

ね

ネイバー探索 IPv6 のプロトコル。同じリンクの IPv6 ノードは、ネイバー探索を使用して、互いの存在の検出、互いのリンク層アドレスの判別、ルータの検索、およびアクティブなネイバーへのパスに関する到着可能性情報の維持を行います。

ネットワーク アクセス ID 「NAS-ID」を参照してください。

ネットワーク デバイス ネットワーク上の IP トラフィックを制御し、攻撃中のホストをブロックできるデバイス。ネットワーク デバイスには、Cisco ルータや PIX Firewall などがあります。

ネットワーク参加 学習した情報をグローバル相関データベースに提供するネットワーク。

ネットワーク参加クライアント データを SensorBase ネットワークに送信する CollaborationApp のソフトウェア コンポーネント。

の

ノード コマンド / コントロール ネットワーク上の物理的な通信要素。たとえば、アプライアンス、IDSM-2、またはルータを指します。

ノーマライザ エンジン IP および TCP ノーマライザが機能する方法を設定し、IP および TCP ノーマライザに関連するシグニチャ イベントの設定を提供します。

は

ハードウェア バイパス 物理インターフェイスのペアを設定する専用のインターフェイス カード。これにより、ソフトウェア エラーの検出時に、物理インターフェイスが直接接続されて、ペア間をトラフィックが流れるようにすることができます。ハードウェア バイパスはトラフィックをネットワーク インターフェイスに渡し、IPS システムには渡しません。

ハンドシェイク 複数のネットワーク デバイス間で、確実に転送を同期化するために交換する一連のメッセージ。

バイパス モード センサーに障害が発生した場合でも、パケットが引き続きセンサーを通過できるようにするモード。バイパス モードは、インラインペアのインターフェイスにのみ適用できます。

バックプレーン シャーシ内でのインターフェイス プロセッサまたはカードとデータ バスおよび電源供給バスとの間の物理的な接続。

パケット 情報を論理的にグループ化したもの。制御情報が格納されたヘッダーと、（通常は）ユーザ データが含まれています。パケットは、ほとんどの場合ネットワーク層のデータの単位を表します。データグラム、フレーム、メッセージ、セグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

パッシブ OS フィンガープリント センサーは、ネットワーク上で交換されるパケットの特性を検査することにより、ホストのオペレーティング システムを判別します。

パッシブ フィンガープリント ネットワークでの対話を受動的に監視することにより、システムで使用可能な OS またはサービスを判別する動作。

パッチ リリース ソフトウェア リリース（サービス パック、マイナー、またはメジャー アップデート）がリリースされた後に、アップデート（マイナー、メジャー、またはサービス パック）バイナリで確認された障害に対処するリリース。

半二重 送信ステーションと受信ステーションの間で、一度に 1 つの方向だけにデータを伝送する機能。BSC は、半二重プロトコルの一例です。

ひ

非仮想化センシング インターフェイス 非仮想化センシング インターフェイスは、サブインターフェイスに分割されていません。インターフェイス全体を関連付けられるのは、最大限でも 1 つの仮想センサーです。

ふ

ブートローダ システムの電源投入時に読み込まれるソフトウェアの小セット。これが（ディスク、ネットワーク、外部コンパクト フラッシュ、外部 USB フラッシュから）オペレーティング システムをロードし、オペレーティング システムが IPS アプリケーションをロードして実行します。AIM-IPS の場合、モジュールをネットワークからブートし、ソフトウェアのインストールおよびアップグレード、ディザスタ リカバリなど、モジュールがソフトウェアにアクセスできない場合の操作を補助します。

ファイアウォール 接続されている任意のパブリック ネットワークとプライベート ネットワーク間のバッファとして指定された、1 つのルータまたはアクセス サーバ、または複数のルータまたはアクセス サーバ。ファイアウォール ルータは、アクセス リストや他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

ファスト イーサネット 各種 100 Mbps イーサネット仕様のいずれか。ファスト イーサネットは、10BaseT イーサネット仕様の 10 倍の速度を実現し、フレーム フォーマット、MAC メカニズム、MTU などの品質を維持します。このような類似点により、ファスト イーサネット ネットワーク上で既存の 10BaseT アプリケーションおよびネットワーク管理ツールの使用が可能になります。IEEE 802.3 仕様の拡張に基づいています。

フェールオープン ハードウェア障害の後、トラフィックがデバイスを通過できるようにすること。

フェールクローズ ハードウェア障害の後、デバイス上のトラフィックをブロックすること。

フォワーディング インターネットワーキング デバイスを経由して最終的な宛先にフレームを送信する処理。

フラグメンテーション 元のパケット サイズをサポートできないネットワーク メディアを介してパケットを送信するときに、パケットをより小さい単位に分割する処理。

フラグメント 大きなパケットの一部で、より小さい単位に分割されます。

フラグメント再構成プロセッサ IPS 内のプロセッサの 1 つです。フラグメント化された IP データグラムを再構成します。センサーがインライン モードの場合、IP フラグメントの正規化も処理します。

フラッディング スイッチやブリッジが使うトラフィックの送出手法。あるインターフェイスで受信したトラフィックが、受信したインターフェイス以外の全インターフェイスに向けて送出されます。

ブラックホール ネットワークの一部分の内部で、劣悪な条件や不適切なシステム設定のために、パケットが入っていくけれども出てこないインターネットワークの領域を指すルーティング用語。

ブロック 指定されたネットワーク ホストまたはネットワークから入ってくるすべてのパケットをネットワーク デバイスが拒否するように指定するセンサーの機能。

ブロック インターフェイス センサーが管理する、ネットワーク デバイス上のインターフェイス。

ブロック解除 それまで適用されていたブロックを削除するようにルータに指示すること。

プラグイン可能な認証モジュール 「PAM」を参照してください。

分析エンジン センサーの設定を処理する IPS ソフトウェア モジュール。インターフェイスをマッピングし、またシグニチャおよびアラーム チャネル ポリシーを設定済みインターフェイスにマッピングします。パケット分析とアラート検出を実行します。分析エンジン機能は、SensorApp プロセスによって提供されます。

へ

ベース バージョン サービス パックまたはシグニチャ アップデートなどのフォローアップ リリースをインストールする前にインストールしておく必要のあるソフトウェア リリース。メジャーおよびマイナー アップデートは、ベース バージョン リリースです。

ほ

ホスト ブロック ARC による、特定 IP アドレスからのすべてのトラフィックのブロック。

ボットネット 自律的かつ自動的に実行されるソフトウェア ロボット、またはボットの集合。この用語は多くの場合、悪意のあるソフトウェアに関連付けられますが、分散コンピューティング ソフトウェアを使用するコンピュータのネットワークを指す場合もあります。ボットネットという用語は、共通の指示管理インフラストラクチャの下で、通常はワーム、トロイの木馬、またはバック ドアを介してインストールされたソフトウェアを実行している、被害を受けたコンピュータ（ゾンビ コンピュータと呼ばれます）の集合を指します。

ま

マイナー アップデート 製品ラインへの小規模な機能強化を含むマイナー バージョン。マイナー アップデートはメジャー バージョンに対する差分であり、サービス パックのベース バージョンです。

マスター ブロッキング センサー 1 つ以上のデバイスを制御するリモート センサーです。ブロッキング転送センサーがブロッキング要求をマスター ブロッキング センサーに送信し、マスター ブロッキング センサーがブロッキング要求を実行します。

マニュファクチャリング イメージ イメージ センサーに対するマニュファクチャリングで使用される IPS システムの完全なイメージ。

マルウェア 不明なホストにインストールされている悪意のあるソフトウェア。

む

無差別デルタ PD。シグニチャごとに設定されている範囲 0 ～ 30 の重み。無差別モードでは、この重みをリスク レーティング全体から減算することができます。

め

メジャー アップデート 製品の主要な新機能または大きなアーキテクチャ上の変更を含むベース バージョン。

メンテナンス パーティション IDSM2 のブート可能なディスク パーティション。ここから IPS イメージをアプリケーション パーティションにインストールできます。IDSM2 がメンテナンス パーティションにブートされている間は、IPS 機能は使用できません。

メンテナンス パーティション イメージ IDSM2 のメンテナンス パーティションにインストールされるブート可能なソフトウェア イメージ。メンテナンス パーティション イメージをインストールできるのは、アプリケーション パーティションにブートされている間だけです。

も

モジュール スイッチ、ルータ、またはセキュリティ アプライアンス シャーシの取り外し可能なカード。AIM IPS、AIP SSM、IDSM2、および NME IPS は、IPS モジュールです。

モニタリング インターフェイス 「センシング インターフェイス」を参照。

ら

ラウンドトリップ時間 「RTT」を参照してください。

ラックマウント センサーを装置ラックに搭載すること。

り

リカバリ パッケージ アプリケーションの完全なイメージとインストーラを含む IPS パッケージ ファイル。センサーでの復旧に使用されます。

リスク レーティング RR。リスク レーティングは、ネットワーク上の特定のイベントに関連付けられたリスクを定量化し、0 ～ 100 の数字で表した値です。攻撃のリスクでは、攻撃の重大度、忠実度、関連性、および資産価値が考慮されますが、対応や軽減のアクションは考慮されません。ネットワークが大きな損害を受けるほど、このリスクは高くなります。

良性トリガー シグニチャは正しく起動されているが、トラフィックの送信元には悪意がない状態。

れ

レイヤ 2 プロセッサ IPS 内のプロセッサの 1 つです。レイヤ 2 関連イベントを処理します。また、不正な形式のパケットを識別し、処理パスから削除します。

レピュテーション レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。これにより、現場にインストールされた IPS センサーは、既存のネットワーク インフラストラクチャを使用して協力することが可能になります。レピュテーションを持つネットワーク デバイスは、悪意のある、または感染した可能性があります。

ろ

ロガー IPS のコンポーネントの 1 つです。アプリケーションのすべてのログ メッセージをログ ファイルに書き出し、アプリケーションのエラー メッセージをイベント ストアに書き出します。

ロギング 発生したアクションをログ ファイルに収集します。セキュリティ情報のログ収集は、イベント（IPS のコマンド、エラー、およびアラート）のログ収集と、個々の IP セッション情報のログ収集という 2 つのレベルで実行されます。

わ

ワーム 単独で実行可能なコンピュータ プログラムで、完全に動作する自身のプログラムを、ネットワークの他のホストに増殖させることができ、きわめて大量のコンピュータ リソースを消費します。

INDEX

A

access-list コマンド 4-5
ACL
  Post-Block 14-22, 14-24
  Pre-Block 14-22, 14-24
  説明 14-3
AIC エンジン
  AIC FTP B-12
  AIC HTTP B-12
  機能 B-12
  シグニチャ カテゴリ 7-19
  説明 B-12
AIC ポリシーの強制
  説明 7-19, B-11
  センサー オーバーサブスクリプション 7-19, B-12
  デフォルト設定 7-19, B-12
alert-frequency コマンド 7-7
alert-severity コマンド 7-9
allocate-ips コマンド 6-3, 18-3
allow-sensor-block コマンド 14-8
anomaly-detection load コマンド 9-41
anomaly-detection save コマンド 9-41
application-policy コマンド 7-20
ARC
  ACL 14-22, A-13
  Catalyst スイッチ
    VACL A-16, A-18
    VACL コマンド A-18
    VLAN A-16
  nac.shun.txt ファイル A-16
  NAT のアドレッシング A-14
  postblock ACL A-15
  preblock ACL A-15
  SSH A-13
  SSH のイネーブル化 C-36
  Telnet A-13
  VACL A-13
  誤って設定されたマスター ブロッキング センサー C-38
  以前の Network Access Controller 14-1, 14-2
  インターフェイス A-14
  機能 14-2, A-13
  最大ブロック数 14-2
  サポートされているデバイス 14-6, A-15
  状態の維持 A-16
  シングル ポイント制御 A-14
  図 A-12
  ステータスの確認 C-31
  ステータスのチェック 14-3, 14-5
  説明 A-3
  前提条件 14-5
  デザイン 14-2
  デバイス アクセスの問題 C-34
  デバイス インターフェイスの確認 C-35
  トラブルシューティング C-30
  認証 A-14
  非アクティブ状態 C-32
  ファイアウォール
    AAA A-18
    NAT A-18
    postblock ACL A-16
    preblock ACL A-16
    shun コマンド A-17
    TACACS+ A-18
    接続のブロッキング A-17

ネットワークのブロッキング A-17
ブロッキング
アプリケーション 14-2
応答 A-13
接続ベース A-17
無条件のブロッキング A-17
ブロック数 A-15
マスター ブロッキング センサー A-13
役割 A-12
レート制限 14-4
ARP
プロトコル B-13
レイヤ 2 シグニチャ B-13
ARP スプーフィング ツール
dsniff B-13
ettercap B-13
ASDM での IPS SSP パスワードのリセット 4-22, 17-2, C-8
Atomic ARP エンジン
説明 B-13
パラメータ（表） B-13
Atomic IP Advanced エンジン
制約事項 B-15
説明 B-14
パラメータ（表） B-15
Atomic IPv6 エンジン
シグニチャ B-26
説明 B-26
ネイバー探索プロトコル B-26
Atomic IP エンジン
説明 B-23
パラメータ（表） B-23
Attack Response Controller
以前の Network Access Controller A-3
説明 A-3
Attack Response Controller。「ARC」を参照。
attemptLimit コマンド 4-20
AuthenticationApp
安全な通信 A-20
説明 A-3
センサーの設定 A-20
メソッド A-20
役割 A-19
ユーザの認証 A-20
ログイン試行の上限 A-20

B

BackOrifice 2000。「BO2K」を参照。
BackOrifice。「BO」を参照。
backup-config コマンド 16-19
banner login コマンド 17-10
block connection コマンド 14-34
block-enable コマンド 14-9
block hosts コマンド 14-32
block network コマンド 14-33
BO
説明 B-68
トロイの木馬 B-68
BO2K
説明 B-68
トロイの木馬 B-68
Bug Toolkit
URL C-2
説明 C-2

C

cidDump の情報の入手 C-76
CIDEE
IPS 拡張 A-33
サポートされている IPS イベント A-33
定義済み A-33
プロトコル A-33
例 A-33
Cisco.com
ソフトウェアのダウンロード 19-2

ソフトウェアへのアクセス 19-2
Cisco.com でのソフトウェアのダウンロード 19-2
Cisco IOS レート制限 14-4
Cisco IPS ソフトウェア ファイル
リスト 19-1, 20-1
cisco-security-agents-mc-settings コマンド 11-5
Cisco Security Intelligence Operations
URL 19-10
説明 19-10
Cisco Security Intelligence Operations の URL 19-10
Cisco Services for IPS
サービス契約 4-43, 19-11
サポートされている製品 4-43, 19-11
clear database コマンド 17-4
clear denied-attackers コマンド 8-37, 17-17
clear events コマンド 4-25, 8-42, 17-16, C-12, C-76
clear line コマンド 17-11
clear os-identification コマンド 8-32
CLI
エラー メッセージ D-1
コマンド モード 1-7
正規表現の構文 1-7
説明 A-3, A-30
デフォルト キーワード 1-10
パスワードの回復 4-23, 17-3, C-9
汎用コマンド 1-9
CLI ガイドの紹介 1-1
CLI セッションの終了 17-12
CLI の動作 1-4
大文字と小文字の区別 1-5
タブ補完 1-5
表示オプション 1-6
プロンプト 1-4
ヘルプ 1-5
呼び出し 1-5
CollaborationApp
説明 A-3, A-28
copy ad-knowledge-base コマンド 9-42
copy anomaly-detection コマンド 9-8
copy backup-config コマンド 16-22, C-3
copy current-config コマンド 16-22, C-3
copy event-action-rules コマンド 8-7
copy iplog コマンド 12-8
copy license-key コマンド 4-44, 19-13
copy packet-file コマンド 13-7
copy signature-definition コマンド 7-2
copy コマンドの構文 9-42
CSA MC
IPS インターフェイスの設定 11-4
隔離された IP アドレス イベント 11-2
サポートされている IPS インターフェイス 11-4
ホスト ポスチャ イベント 11-2, 11-4
CtlTransSource
図 A-11
説明 A-3, A-11
Ctrl+N 1-5
Ctrl+P 1-5
current-config コマンド 16-19

D

DDoS
Stacheldraht B-67
TFN B-67
プロトコル B-67
default service anomaly-detection コマンド 9-8
default service event-action-rules コマンド 8-7
default service signature-definition コマンド 7-2
deny attacker コマンド 8-36
deny-packet-inline の説明 7-16, 8-6, 8-16, B-9
DNS サーバの設定 4-10
DoS ツール
Stacheldraht B-67
DoS ツール stick B-7
DoS ツール
TFN B-67

E

enable-acl-logging コマンド 14-14
enable-detail-traps コマンド 15-4
enable-nvram-write コマンド 14-15
Encryption Software Export Distribution Authorization フォーム
　暗号化アカウント 19-3
　説明 19-3
erase ad-knowledge-base コマンド 9-42
erase packet-file コマンド 13-8
erase コマンド 16-25
evAlert A-8
event-action コマンド 7-16
event-counter コマンド 7-11
evError A-8
evLogTransaction A-8
evShunRqst A-8
evStatus A-8
external-zone コマンド 9-29

F

filters コマンド 8-21
Fixed ICMP エンジンのパラメータ（表） B-27
Fixed TCP エンジンのパラメータ（表） B-28
Fixed UDP エンジンのパラメータ（表） B-29
Fixed エンジンの説明 B-27
Flood Host エンジン パラメータ（表） B-30
Flood Net エンジン パラメータ（表） B-30
Flood エンジンの説明 B-30
fragment-reassembly コマンド 7-32
ftp-timeout コマンド 4-7
FTP サーバ ソフトウェア アップデート 20-2
FTP タイムアウト
　設定 4-7
　説明 4-7

G

global-block-timeout コマンド 8-34, 14-13
global-deny-timeout コマンド 8-34
global-filters-status コマンド 8-34
global-metaevent-status コマンド 8-34
global-overrides-status コマンド 8-34
global-parameters コマンド 6-11
global-summarization コマンド 8-34

H

H.225.0 プロトコル B-40
H.323 プロトコル B-40
health-monitor コマンド 10-7, 17-5
health statistics の設定 17-7
host-ip コマンド 4-3
host-name コマンド 4-2
HTTP/HTTPS サーバのサポート 20-2
HTTP 解読
　ASCII 正規化 7-46, B-42
　説明 7-46, B-42
hw-module module 1 recover configure コマンド 18-10
hw-module module slot_number password-reset コマンド 4-22, 17-2, 18-10, C-8
hw-module module slot_number recover boot コマンド 18-10
hw-module module slot_number recover stop コマンド 18-10
hw-module module slot_number reload コマンド 18-9
hw-module module slot_number reset コマンド 18-9
hw-module module slot_number shutdown コマンド 18-9

I

IDAPI
　機能 A-34
　図 A-34
　説明 A-3

通信 A-3, A-34
役割 A-34
IDCONF
XML A-32
説明 A-32
例 A-32
IDIOM
定義 A-32
メッセージ A-32
IDM
TLS 4-39
証明書 4-39
IDM の証明書 4-39
ignore コマンド 9-10
illegal-zone コマンド 9-20
InterfaceApp の説明 A-3
interface-notifications コマンド 5-4
internal-zone コマンド 9-11
ip-log-bytes コマンド 12-2
ip-log-packets コマンド 12-2
iplog-status コマンド 12-5
ip-log-time コマンド 12-2
ip-log コマンド 7-41
iplog コマンド 12-4
IPS 19-4, 19-5
IPS SSP
hw-module module 1 recover configure 18-10
hw-module module slot_number password-reset 18-10
hw-module module slot_number recover boot 18-10
hw-module module slot_number recover stop 18-10
hw-module module slot_number reload 18-9
hw-module module slot_number reset 18-9
hw-module module slot_number shutdown 18-9
setup コマンド 3-7
show module コマンド 18-2
仮想センサー
インターフェイスの割り当て 6-4, 18-4
順序 6-3, 18-4
セキュリティ コンテキストへの割り当て 18-6
ポリシーの割り当て 6-4, 18-4
仮想センサーの作成 6-4, 18-5
仮想センサーの割り当て 6-7, 18-7
時刻源 4-24, C-10
初期化 3-7
初期化の確認 18-2
設定作業 18-1
センシング インターフェイス 6-3, 18-3
パスワードの回復 4-22, 17-2, C-8
IPS SSP の設定作業 1-2
IPS SSP の設定順序 1-2
IPS SSP へのセッション接続 2-2
IPS アプリケーション
XML 形式 A-3
表 A-35
要約 A-35
IPS イベント
evAlert A-8
evError A-8
evLogTransaction A-8
evShunRqst A-8
evStatus A-8
タイプ A-8
リスト A-8
IPS ソフトウェア
Linux OS A-2
アップデート A-4
アプリケーション リスト A-3
シグニチャのチューニング A-4
使用可能なファイル 19-2
セキュリティ機能 A-4
ディレクトリ構造 A-34
データの取得 A-4
デバイス パラメータの設定 A-4
入手方法 19-2
バージョン管理方式 19-3
プラットフォームに依存するリリースの例 19-7

ユーザ対話 A-4
IPS ソフトウェア ファイル名
サービス パック（図） 19-4
パッチ リリース（図） 19-4
マイナー アップデート（図） 19-4
メジャー アップデート（図） 19-4
IPS データ
XML ドキュメント A-8
タイプ A-8
IPS 内部通信 A-34
IPv4
アドレス形式 8-9
イベント変数 8-9
IPv6
アドレス形式 8-9
イベント変数 8-9
説明 B-26
ipv6-target-value コマンド 8-14
IP パケット ルートのトレース 17-35
IP フラグメンテーションの説明 B-34
IP フラグメント再構成
シグニチャ（表） 7-29
説明 7-29
パラメータ（表） 7-29
IP ロギング
自動 12-2
設定 12-1
説明 7-41, 12-1
ファイルのコピー 12-8
マニュアル 12-4
IP ロギングの停止 12-6
IP ログ
TCPDUMP 12-2
Wireshark 12-2
IP ログの内容
表示 12-5
IP ログ ファイルのコピー 12-8

K

KB
コピー 9-42, 9-43
手動での保存 9-41
手動でのロード 9-41
消去 9-42, 9-43
初期ベースライン 9-3
スキャナしきい値 9-37
説明 9-3
ツリー構造 9-37
名前の変更 9-42, 9-43
比較 9-44
ヒストグラム 9-37
KB しきい値の表示 9-46
KB の名前の変更 9-42, 9-43
KB の比較 9-44
KB の保存 9-41
KB のロード 9-41
KB ファイルの表示 9-40

L

learning-accept-mode コマンド 9-38
[Licensing] ペイン
設定 19-12
説明 4-42, 19-10
list anomaly-detection-configurations コマンド 9-8, 17-19
list event-action-rules-configurations コマンド 8-7, 17-19
list signature-definition-configurations コマンド 7-2, 17-19
log-all-block-events-and-errors コマンド 14-17
login-banner-text コマンド 4-8
login-banner-text の設定 4-8
LOKI
説明 B-67
プロトコル B-67

M

MainApp
- show version コマンド A-6
- コンポーネント A-5
- 説明 A-3, A-5
- ホスト統計情報 A-6
- 役割 A-6

Master エンジン
- アラート頻度 B-7
- アラート頻度のパラメータ（表） B-7
- イベント アクション 8-4, B-8
- 説明 B-4
- 汎用パラメータ（表） B-5
- ユニバーサル パラメータ B-5

max-block-entries コマンド 14-11
max-denied-attackers コマンド 8-34
max-interfaces コマンド 14-18
Meta エンジン
- シグニチャ イベント アクション プロセッサ 7-49, B-31
- 説明 7-49, B-31
- パラメータ（表） B-31

MIB のサポート 15-6, C-13
more current-config コマンド 16-1
more コマンド
- 説明 16-19
- フィルタリング 16-16

Multi String エンジン
- 正規表現 B-32
- 説明 B-32
- パラメータ（表） B-32

N

never-block-hosts コマンド 14-19
never-block-networks コマンド 14-19
no iplog コマンド 12-6
no ipv6-target-value コマンド 8-14
no service anomaly-detection コマンド 9-8
no service event-action-rules コマンド 8-7
no service signature-definition コマンド 7-2
no target-value コマンド 8-14
NotificationApp
- SNMP get A-9
- SNMP トラップ A-9
- アラート情報 A-9
- 機能 A-9
- システム ヘルス情報 A-10
- 説明 A-3
- 統計情報 A-10

no variables コマンド 8-10
NTP
- 誤った設定 C-11
- サーバの設定 4-31
- センサー時刻源 4-31, 4-32
- 認証済み 4-24, 4-32, C-11
- 非認証 4-24, 4-32, C-11

O

OS ID
- クリア 8-32
- 表示 8-32

os-identifications コマンド 8-28
OS 情報のソース 8-27
OS マップ
- 移動 8-30
- 削除 8-31
- 作成 8-29

OS マップの移動 8-30
other コマンド 9-18, 9-26, 9-35
overrides コマンド 8-17

P

P2P ネットワークの説明 B-47
packet capture コマンド 13-4

packet display コマンド 13-2
password コマンド 4-14, 4-17
physical-interfaces コマンド 5-2
ping コマンド 17-34
Post-Block ACL 14-22, 14-24
Pre-Block ACL 14-22, 14-24
privilege
コマンド 4-14, 4-17

Q

Q.931 プロトコル
SETUP メッセージ B-40
説明 B-40

R

raw 正規表現
エキスパート モード 7-55, 7-59, B-59
説明 7-55, 7-59, B-59
raw 表現の構文
エキスパート モード B-59
説明 B-59
recover コマンド 20-10
Regex
Multi String エンジン B-32
説明 1-7
標準化 B-2
rename ad-knowledge-base コマンド 9-42
ROMMON
TFTP 20-3
シリアル コンソール ポート 20-2
RPC ポートマッパー B-48
RSA 認証および許可キー 4-36
RTT
TFTP の制限 20-3
説明 20-3

S

SDEE
HTTP A-33
サーバ要求 A-33
説明 A-33
プロトコル A-33
SensorApp
IP 正規化 A-24
TCP 正規化 A-24
アラーム チャネル A-24
イベント アクション フィルタリング A-25
インライン パケット処理 A-24
シグニチャ イベント アクション プロセッサ A-22
説明 A-3
パケット フロー A-25
プロセッサ A-22
分析エンジン A-24
役割 A-22
リスク レーティング A-25
SensorBase ネットワーク
サーバ 10-2
参加 10-2
説明 10-1, 10-2
ネットワーク参加 10-4
service anomaly-detection コマンド 9-8
Service DNS エンジン
説明 B-36
パラメータ（表） B-36
service event-action-rules コマンド 8-7
Service FTP エンジン
PASV ポート スプーフィング B-38
説明 B-38
パラメータ（表） B-38
Service Generic エンジン
カスタム シグニチャなし B-39
説明 B-38
パラメータ（表） B-39
Service H225 エンジン

ASN.1PER 検証 B-40
TPKT 検証 B-40
機能 B-40
説明 B-40
パラメータ（表） B-41
Service HTTP エンジン
説明 7-46, B-42
パラメータ（表） B-42
Service IDENT エンジン
説明 B-44
パラメータ（表） B-44
Service MSRPC エンジン
DCS/RPC プロトコル B-45
説明 B-45
パラメータ（表） B-45
Service MSSQL エンジン
MSSQL プロトコル B-46
説明 B-46
パラメータ（表） B-46
Service NTP エンジン
説明 B-47
パラメータ（表） B-47
Service P2P エンジンの説明 B-47
Service RPC エンジン
RPC ポートマッパー B-48
説明 B-48
パラメータ（表） B-48
service signature-definition コマンド 7-1
Service SMB Advanced エンジン
説明 B-49
パラメータ（表） B-49
Service SNMP エンジン
説明 B-51
パラメータ（表） B-52
Service SSH エンジン
説明 B-52
パラメータ（表） B-52
Service TNS エンジン
説明 B-53
パラメータ（表） B-53
Service エンジン
説明 B-36
レイヤ 5 トラフィック B-36
setup 4-12
簡素化モード 3-2
コマンド 3-1, 3-4, 3-7
自動 3-2
setup コマンド ユーザ ロール 3-1
show ad-knowledge-base diff コマンド 9-44, 9-45
show ad-knowledge-base files コマンド 9-40, 9-41
show clock コマンド 4-26, 17-16
show configuration コマンド 16-1
show context コマンド 6-6, 18-7
show events コマンド 8-39, 17-13, C-72, C-73
show health コマンド 10-9, 17-10, C-53
show history コマンド 17-34
show interfaces コマンド 5-5, C-71
show ips コマンド 18-7
show module 1 details コマンド C-49
show module コマンド 18-2
show os-identification コマンド 8-32
show settings コマンド 4-23, 16-3, 16-18, 17-3, 17-36, C-9
show statistics anomaly-detection コマンド 9-47
show statistics denied-attackers コマンド 8-37, 17-17
show statistics virtual-sensor コマンド 17-20, C-18, C-61
show statistics コマンド 14-35, 17-20, C-60, C-61
show tech-support コマンド 17-30, C-54
show users コマンド 4-18
show version コマンド 17-31, C-57
sig-fidelity-rating コマンド 7-12, 7-14
SNMP
Get 15-1
GetNext 15-1
Set 15-1
Trap 15-1
一般的なパラメータ 15-2

サポートされている MIB 15-6, C-13
設定
エージェントのパラメータ 15-3
トラップ 15-5
説明 15-1
トラップの説明 15-1
snmp-agent-port コマンド 15-2
snmp-agent-protocol コマンド 15-2
SPAN ポートの問題 C-25
SSH
セキュリティ 4-34
説明 4-34
ホストの追加 4-35
ssh authorized-key コマンド 4-36
ssh generate-key コマンド 4-38
ssh host-key コマンド 4-35
SSH 既知ホスト リストへのホストの追加 4-35
SSH サーバ
公開キー A-21
秘密キー A-21
SSH サーバ ホスト キーの生成 4-38
State エンジン
Cisco Login B-54
LPR Format String B-54
SMTP B-54
説明 B-54
パラメータ（表） B-55
status コマンド 7-13
stream-reassembly コマンド 7-40
String ICMP エンジン
説明 B-56
パラメータ（表） B-57
String TCP XL シグニチャ
例 7-54
String TCP XL シグニチャ（例） 7-54, 7-58
String TCP エンジン
オプション 7-43
説明 B-56
パラメータ（表） B-57
String UDP エンジン
説明 B-56
パラメータ（表） B-58
String XL エンジン
サポートされていないパラメータ B-61
説明 B-59
ハードウェアのサポート B-4
パラメータ（表） B-59
String エンジンの説明 7-43, B-56
summertime-option non-recurring コマンド 4-28
summertime-option recurring コマンド 4-26
Sweep Other TCP エンジン
説明 B-64
パラメータ（表） B-64
Sweep エンジン
説明 B-62
パラメータ（表） B-63
[System Configuration] ダイアログ
説明 3-2
例 3-3

T

TAC
show tech-support コマンド 17-30, C-54
サービス アカウント 4-16, A-31, C-5
トラブルシューティング A-31
target-value コマンド 8-14
IPv4 8-14
IPv6 8-14
TCPDUMP
copy packet-file コマンド 13-7
IP ログ 12-2
packet capture コマンド 13-5
packet display コマンド 13-2
表現の構文 13-2
tcp コマンド 9-13, 9-21, 9-30
TCP ストリーム再構成
シグニチャ（表） 7-34, 7-39

説明 7-33
パラメータ（表） 7-34, 7-39
TCP フラグメンテーションの説明 B-34
Telnet
イネーブル化 4-4
ディセーブル化 4-4
telnet-option
コマンド 4-4
設定 4-4
terminal
コマンド 17-12
TFN2K
説明 B-67
トロイの木馬 B-68
TFTP サーバ
RTT 20-3
最大ファイル サイズ制限 20-3
time-zone-settings コマンド 4-30
TLS
IDM 4-39
Web サーバ 4-39
証明書の生成 4-42
ハンドシェイク 4-39
tls generate-key コマンド 4-41
tls trusted-host コマンド 4-40
trace コマンド 17-35
Traffic Anomaly エンジン
シグニチャ B-65
説明 B-65
プロトコル B-65
Traffic ICMP エンジン
DDoS B-67
LOKI B-67
TFN2K B-67
説明 B-67
パラメータ（表） B-67
trap-community-name 15-4
trap-destinations コマンド 15-4
Tribe Flood Network 2000。「TFN2K」を参照。
Tribe Flood Network。「TFN」を参照。
Trojan エンジン
BO2K B-68
TFN2K B-68
説明 B-68

U

udp コマンド 9-15, 9-24, 9-32
upgrade コマンド 20-9
username コマンド 4-14
user-profile コマンド 14-21

V

VACL
Post-Block 14-26
Pre-Block 14-26
説明 14-3
variables コマンド 7-4, 8-10
IPv4 8-10
IPv6 8-10
virtual-sensor name コマンド 6-4, 18-4

W

Web サーバ
HTTP 1.0 および 1.1 のサポート A-22
SDEE のサポート A-22
TLS 4-39
公開キー A-21
設定の変更 4-12
説明 A-3, A-22
秘密キー A-21
ポート（デフォルト） 4-12
HTTP プロトコル 4-12
設定の実行 4-12
Wireshark

copy packet-file コマンド 13-7
IP ログ 12-2
worm-timeout コマンド 9-10

X

XML 形式のアプリケーション A-3

あ

アカウント ロッキング
セキュリティ 4-20
設定 4-20
アクセス
IPS ソフトウェア 19-2
サービス アカウント 4-16, C-5
アクセス リスト
設定 4-6
設定の誤り C-21
変更 4-6
アップグレード
アプリケーション パーティション 20-10
最新バージョン C-45
リカバリ パーティション 20-9
アドレス解決プロトコル。「ARP」を参照。
アプライアンス
ターミナル サーバ
設定 20-3
説明 20-3
リカバリ パーティションのアップグレード 20-9
アプリケーション検査および制御。「AIC」を参照。
アプリケーション パーティション
イメージの復元 20-11
説明 A-4
アプリケーション ポリシーの強制の説明 7-19, B-11
アプリケーション ポリシーの設定 7-20
アラートおよびログ アクション（リスト） 8-4
アラート重大度の設定 7-10
アラート頻度モード B-7
アラーム チャネル
説明 8-2, A-26
リスク レーティング 10-5
暗号化アカウント
Encryption Software Export Distribution Authorization フォーム 19-3
入手方法 19-3

い

異常検出
イベント アクション 9-6, B-65
学習プロセス 9-3
偽陽性の制限 9-37
検出モード 9-4
シグニチャの説明 9-6
シグニチャ（表） 9-6, B-65
設定順序 9-5
説明 9-2
ゾーン 9-4
注意 9-2
ディセーブル化 9-49, C-14
デフォルト設定（例） 9-4
非アクティブ モード 9-4
非対称トラフィック 9-2
プロトコル 9-3
ワーム
攻撃 9-37
説明 9-3
異常検出および学習受け入れモード 9-3
異常検出ゾーン
内部 9-11
不正 9-20
異常検出の統計情報
クリア 9-48
表示 9-48
異常検出の動作設定
設定 9-10, 9-38
説明 9-10

異常検出ポリシー
コピー 9-8
削除 9-8
作成 9-8
表示 9-8
編集 9-8
リスト 17-19
イネーブル化
Telnet 4-4
シグニチャ 7-13
デバッグ ロギング C-40
イベント
隔離された IP アドレス 11-2
クリア 8-42, 17-16, C-76
表示 8-40, 17-14, C-74
ホスト ポスチャ 11-2
イベント アクション
脅威レーティング 8-13
リスク レーティング 8-13
イベント アクション オーバーライド
説明 8-16
リスク レーティング範囲 8-16
イベント アクション規則
機能 8-2
作業リスト 8-6
説明 8-2
イベント アクション規則ポリシー
コピー 8-7
削除 8-7
作成 8-7
表示 8-7
編集 8-7
イベント アクション規則リストの表示 17-20
イベント アクションの設定 7-17
イベント アクション フィルタ
説明 8-20
変数の使用 8-21
イベント カウンタの設定 7-11
イベント ストア
アラートなし C-27
イベントのクリア 4-25, C-12
クリア 8-42, 17-16, C-76
説明 A-3
タイム スタンプ 4-25, C-12
タイムスタンプ A-6
データ構造 A-7
役割 A-6
例 A-7
イベント タイプ C-72
イベント変数
説明 8-9
例 8-10
インストーラ マイナー バージョン 19-5
インストーラ メジャー バージョン 19-5
インストール
センサー ライセンス 19-12
ライセンス キー 4-45, 19-14
インターフェイス
コマンド / コントロール 5-1
スロット番号 5-1
説明 5-1
センシング 5-2
ポート番号 5-1
ライブ トラフィックの表示 13-3
インターフェイス統計情報の表示 5-6
インライン インターフェイス ペア モード
説明 5-4

う

ウォッチ リスト レーティング
説明 8-13
リスク レーティングの計算 8-13

え

エラー メッセージ

検証 D-5
説明 D-1
エンジン
AIC 7-18, B-11
AIC FTP B-12
AIC HTTP B-12
Atomic ARP B-13
Atomic IP B-23
Atomic IP Advanced B-14
Atomic IPv6 B-26
Fixed B-27
Fixed ICMP B-27
Fixed TCP B-27
Fixed UDP B-27
Flood B-30
Flood Host B-30
Flood Net B-30
Master B-5
Meta 7-49, B-31
Multi String B-32
Service B-36
Service FTP B-38
Service Generic B-38
Service H225 B-40
Service HTTP 7-46, B-42
Service IDENT B-44
Service MSRPC B-45
Service MSSQL B-46
Service NTP B-47
Service P2P B-47
Service RPC B-48
Service SMB Advanced B-49
Service SNMP B-51
Service SSH B-52
Service TNS B-53
State B-54
String 7-43, B-56
String ICMP 7-43, B-56
String TCP 7-43, B-56
String UDP 7-43, B-56
Sweep B-62
Sweep Other TCP B-64
Traffic Anomaly B-65
Traffic ICMP B-67
Trojan B-68
ノーマライザ B-34

お

オプション
グローバル相関 10-10, 10-13
ネットワーク参加 10-11
オペレータ ロール特権 1-3

か

外部製品インターフェイス
説明 11-1
追加 11-6
トラブルシューティング 11-9, C-17
問題 11-3, C-16
外部ゾーン
TCP の設定 9-30
UDP の設定 9-33
設定 9-29
説明 9-29
その他のプロトコルの設定 9-35
学習受け入れモードおよび異常検出 9-3
確認
センサーの初期化 3-12
センサーのセットアップ 3-12
パスワードの回復 4-23, 17-3, C-9
隔離された IP アドレス イベントの説明 11-2
カスタム シグニチャ
Atomic IP Advanced シグニチャ 7-53
Meta シグニチャ 7-51
Service HTTP の例 7-48
String TCP XL 7-54, 7-58

設定順序 7-42
説明 7-4
仮想化
制約事項 6-2, C-12
トラフィック キャプチャ要件 6-2, C-13
利点 6-2, C-12
仮想センサー
KB ファイルの表示 9-40
オプション 6-4, 18-4
作成 6-9
作成（IPS SSP） 6-4, 18-5
説明 6-2
追加 6-9
追加（IPS SSP） 6-4, 18-5
デフォルト仮想センサー 6-2
監査モードの説明 10-9
管理
スイッチ 14-27
ファイアウォール 14-28
ルータ 14-24
管理者ロール特権 1-3

き

キーワード
default 1-10
no 1-10
基本的な設定 3-4
脅威レーティング
説明 8-13
リスク レーティング 8-13
偽陽性の説明 7-3
許可キー
RSA 認証 4-36
定義 4-37
許可キーの定義 4-37
拒否アクション（リスト） 8-4
拒否攻撃者の追加 8-36

く

クライアント マニフェストの説明 A-28
クリア
OS ID 8-32
異常検出の統計情報 9-48
イベント 8-42, 17-16, C-76
拒否攻撃者統計情報 8-37, 17-18
センサー データベース 17-5
統計情報 17-20, C-61
グローバル相関
DNS サーバ 4-10, 10-6
HTTP プロキシ サーバ 10-6
アップデート クライアント（図） 10-8
エラー メッセージ A-29
オプション 10-10, 10-13
機能 10-6
製品アラート 8-4
説明 10-1, 10-2
ディセーブル化 10-13
トラブルシューティング 10-13, C-13
非 IPv6 サポート 8-9, 8-10, 8-14, 8-20, 8-21, 10-7
プロキシ サーバ 4-10
ヘルス ステータス 10-7, 19-8
ヘルス メトリック 10-7
目的 10-6
要件 10-6
ライセンス 3-2, 3-5, 10-6, 10-9
リスク レーティング 10-5
グローバル相関の更新
クライアントの説明 A-28
サーバの説明 A-28
グローバル パラメータ
オプション 6-11
作成 6-11
追加 6-11
開くことのできる最大 IP ログ数 6-11

け

権限レベル
- オペレータ 1-3
- 管理者 1-3
- サービス 1-3
- ビューア 1-3

現在の設定のバックアップ 16-24, C-3
現在の設定の復元 16-23, C-4, C-5
検出モード（異常検出） 9-4
検証エラー メッセージの説明 D-5

こ

攻撃関連性レーティング
- 説明 8-13, 8-26
- リスク レーティングの計算 8-13

攻撃の重大度レーティング
- 説明 8-12
- リスク レーティングの計算 8-12

構文および大文字と小文字の区別 1-5
コピー
- IP ログ ファイル 12-8
- KB 9-42, 9-43
- 異常検出ポリシー 9-8
- イベント アクション規則ポリシー 8-7
- シグニチャ定義ポリシー 7-2
- パケット ファイル 13-7

コマンド 15-4, 18-2
- access-list 4-5
- alert-frequency 7-7
- alert-severity 7-9
- allocate-ips 6-3, 18-3
- allow-sensor-block 14-8
- anomaly-detection load 9-41
- anomaly-detection save 9-41
- application-policy 7-20
- attemptLimit 4-20
- backup-config 16-19
- banner login 17-10
- block connection 14-34
- block-enable 14-9
- block hosts 14-32
- block network 14-33
- cisco-security-agents-mc-settings 11-5
- clear database 17-4
- clear denied-attackers 8-37, 17-17
- clear events 4-25, 8-42, 17-16, C-12, C-76
- clear line 17-11
- clear os-identification 8-32
- copy ad-knowledge-base 9-42
- copy anomaly-detection 9-8
- copy backup-config 16-22, C-3
- copy current-config 16-22, C-3
- copy event-action-rules 8-7
- copy iplog 12-8
- copy license-key 4-44, 19-13
- copy packet-file 13-7
- copy signature-definition 7-2
- current-config 16-19
- default service anomaly-detection 9-8
- default service event-action-rules 8-7
- default service signature-definition 7-2
- deny attacker 8-36
- enable-acl-logging 14-14
- enable-detail-traps 15-4
- enable-nvram-write 14-15
- erase 16-25
- erase ad-knowledge-base 9-42
- erase packet-file 13-8
- event-action 7-16
- event-action-rules-configurations 17-19
- event-counter 7-11
- external-zone 9-29
- filters 8-21
- fragment-reassembly 7-32
- ftp-timeout 4-7
- global-block-timeout 8-34, 14-13

global-deny-timeout 8-34
global-filters-status 8-34
global-metaevent-status 8-34
global-overrides-status 8-34
global-parameters 6-11
global-summarization 8-34
health-monitor 10-7, 17-5
host-ip 4-3
host-name 4-2
hw-module module 1 recover configure 18-10
hw-module module slot_number password-reset 4-22, 17-2, 18-10, C-8
hw-module module slot_number recover boot 18-10
hw-module module slot_number recover stop 18-10
hw-module module slot_number reload 18-9
hw-module module slot_number reset 18-9
hw-module module slot_number shutdown 18-9
ignore 9-10
illegal-zone 9-20
interface-notifications 5-4
internal-zone 9-11
ip-log 7-41
iplog 12-4
ip-log-bytes 12-2
ip-log-packets 12-2
iplog-status 12-5
ip-log-time 12-2
ipv6-target-value 8-14
learning-accept-mode 9-38
list anomaly-detection-configurations 9-8, 17-19
list event-action-rules-configurations 8-7
list signature-definition-configurations 7-2
log-all-block-events-and-errors 14-17
login-banner-text 4-8
max-block-entries 14-11
max-denied-attackers 8-34
max-interfaces 14-18
more 16-19
more current-config 16-1
never-block-hosts 14-19
never-block-networks 14-19
no iplog 12-6
no ipv6-target-value 8-14
no service anomaly-detection 9-8
no service event-action-rules 8-7
no service signature-definition 7-2
no target-value 8-14
no variables 8-10
os-identifications 8-28
other 9-18, 9-26, 9-35
overrides 8-17
packet capture 13-4
packet-display 13-2
password 4-14, 4-17
physical-interfaces 5-2
ping 17-34
privilege 4-14, 4-17
rename ad-knowledge-base 9-42
service anomaly-detection 9-8
service event-action-rules 8-7
service signature-definition 7-1
setup 3-1, 3-4, 3-7
show
show tech-support 17-30, C-54
show ad-knowledge-base diff 9-44, 9-45
show ad-knowledge-base files 9-40, 9-41
show clock 4-26, 17-16
show configuration 16-1
show context 6-6, 18-7
show events 8-39, 17-13, C-73
show health 10-9, 17-10, C-53
show history 17-34
show interfaces 5-5
show ips 18-7
show module 1 details C-49
show os-identification 8-32
show settings 4-23, 16-3, 16-18, 17-3, 17-36, C-9
show statistics 14-35, 17-20, C-61

show statistics anomaly-detection 9-47
show statistics denied-attackers 8-37, 17-17
show statistics virtual-sensor 17-20, C-18, C-61
show users 4-18
show version 17-31, C-57
sig-fidelity-rating 7-12, 7-14
signature-definition-configurations 17-19
snmp-agent-port 15-2
snmp-agent-protocol 15-2
ssh authorized-key 4-36
ssh-generate-key 4-38
ssh host-key 4-35
status 7-13
stream-reassembly 7-40
summertime-option non-recurring 4-28
summertime-option recurring 4-26
target-value 8-14
tcp 9-13, 9-21, 9-30
telnet-option 4-4
terminal 17-12
time-zone-settings 4-30
tls generate-key 4-41
tls trusted-host 4-40
trace 17-35
trap-community-name 15-4
trap-destinations 15-4
udp 9-15, 9-24, 9-32
upgrade 20-9
username 4-14
user-profile 14-21
variables 7-4, 8-10
virtual-sensor name 6-4, 18-4
worm-timeout 9-10
コマンド / コントロール インターフェイスの説明 5-1
コマンド モード 1-7
EXEC 1-7
異常検出コンフィギュレーション 1-7
イベント アクション規則コンフィギュレーション 1-7
グローバル コンフィギュレーション 1-7
サービス モード コンフィギュレーション 1-7
シグニチャ定義コンフィギュレーション 1-7
特権 EXEC 1-7
コマンド ラインの編集（表） 1-6
コンフィギュレーション ファイル
バックアップ 16-24, C-3

さ

サーバのマニフェストの説明 A-28
サービス アカウント
TAC A-31
アクセス 4-16, C-5
作成 4-16, C-6
説明 4-16, A-31, C-5
注意 4-16, C-5
トラブルシューティング A-31
サービス拒否。「DoS」を参照。
サービス パックの説明 19-4
サービス ロール
CLI のバイパス 2-2, A-30
説明 1-4, A-30
特権 1-4
削除
OS マップ 8-31
異常検出ポリシー 9-8
イベント アクション規則ポリシー 8-7
イベント アクション変数 8-10
拒否攻撃者リスト 8-37, 17-18
シグニチャ定義ポリシー 7-2
シグニチャ変数 7-5
ターゲットの価値レーティング 8-15
ユーザ 4-14
作成
Atomic IP Advanced シグニチャ 7-53
Meta シグニチャ 7-51
OS マップ 8-29
Post-Block VACL 14-26

Pre-Block VACL 14-26
Service HTTP シグニチャ 7-48
String TCP XL シグニチャ 7-55, 7-58
String TCP シグニチャ 7-44
異常検出ポリシー 9-8
イベント アクション規則ポリシー 8-7
イベント アクション変数 8-10
カスタム シグニチャ 7-42
仮想センサー 6-9
グローバル パラメータ 6-11
サービス アカウント 4-16, C-6
シグニチャ定義ポリシー 7-2
ユーザ プロファイル 14-21
ログイン バナー 17-10
サブシグニチャの説明 7-3
サブモード コンフィギュレーション
出力の検索 16-18
出力のフィルタリング 16-18
サブモード コンフィギュレーションの検索 16-18
サブモードの設定の表示 17-36
サポート対象
CSA MC 対応 IPS インターフェイス 11-4
FTP サーバ 20-2
HTTP/HTTPS サーバ 20-2
サマライズ
fire-all 8-34
fire-once 8-34
global-summarization 8-34
Meta エンジン 8-33
summary 8-34
説明 8-33

し

時間帯設定の実行 4-30
シグニチャ
false positive 7-3
String TCP 7-44
String TCP XL 7-55, 7-58
一般的なパラメータ 7-6
カスタム 7-4
サブシグニチャ 7-3
説明 7-3
チューニング済み 7-4
デフォルト 7-4
レート制限 14-4
シグニチャ アップデート ファイルの説明 19-5
シグニチャ イベント アクション オーバーライドの説明 8-2, A-26
シグニチャ イベント アクション ハンドラの説明 8-3, A-26
シグニチャ イベント アクション フィルタ
説明 8-2, A-26
パラメータ 8-2, A-26
シグニチャ イベント アクション プロセッサ
アラーム チャネル 8-2, A-26
コンポーネント 8-2, A-26
説明 8-2, A-22, A-26
シグニチャ エンジン
AIC 7-18, B-11
Atomic B-12
Atomic ARP B-13
Atomic IP B-23
Atomic IP Advanced B-14
Atomic IPv6 B-26
Fixed B-27
Flood B-30
Flood Host B-30
Flood Net B-30
Master B-5
Meta 7-49, B-31
Multi String B-32
Regex
構文 B-10
パターン B-10
Service B-36
Service DNS B-36
Service FTP B-38

Service Generic B-38
Service H225 B-40
Service HTTP 7-46, B-42
Service IDENT B-44
Service MSRPC B-45
Service MSSQL B-46
Service NTP B-47
Service P2P B-47
Service RPC B-48
Service SMB Advanced B-49
Service SNMP B-51
Service SSH エンジン B-52
Service TNS B-53
State B-54
String 7-43, B-56
Sweep B-62
Sweep Other TCP B-64
Traffic Anomaly B-65
Traffic ICMP B-67
Trojan B-68
イベント アクション B-8
説明 B-2
ノーマライザ B-34
リスト B-2
シグニチャ エンジン アップデート ファイルの説明 19-5
シグニチャ忠実度レーティング
設定 7-12
説明 8-12
リスク レーティングの計算 8-12
シグニチャ定義ポリシー
コピー 7-2
削除 7-2
作成 7-2
編集 7-2
シグニチャ定義リストの表示 17-20
シグニチャの廃棄 7-13
シグニチャ変数
削除 7-5
説明 7-4
追加 7-5
編集 7-5
時刻
センサー C-10
センサーでの修正 4-25, C-12
時刻源および IPS SSP 4-24, C-10
システム アーキテクチャ
サポートされているプラットフォーム A-1
ディレクトリ構造 A-34
システム クロックの表示 4-26, 17-17
システム コンポーネント IDAPI A-34
システム設計（図） A-2
自動アップデートのトラブルシューティング C-46
自動セットアップ 3-2
重複 IP アドレス C-22
集約
アラート頻度 8-33
動作モード 8-33
出力
現在のラインをクリア 1-6
表示 1-6
手動
KB の保存 9-41
KB のロード 9-41
手動ブロッキング 14-32, 14-34
消去
KB 9-42, 9-43
現在の設定 16-25
パケット ファイル 13-8
初期化
IPS SSP 3-7
確認 3-12
確認（IPS SSP） 18-2
センサー 3-1, 3-4
ユーザ ロール 3-1
信頼できるホストの追加 4-40

せ

正規表現。「Regex」を参照。
正規表現の構文
raw 正規表現 7-55, 7-59, B-59
シグニチャ B-10
説明 1-7
表 1-8
制御トランザクション
特徴 A-8
要求のタイプ A-8
脆弱な OS の設定 7-15
脆弱な OS のフィールド
説明 B-7
生成
SSH サーバ ホスト キー 4-38
TLS 証明書 4-42
セキュリティ
Cisco Security Intelligence Operations に関する情報 19-10
SSH 4-34
アカウント ロッキング 4-20
セキュリティ ポリシーの説明 7-1, 8-1, 9-2
設定
ACL ロギング 14-14
CSA MC IPS インターフェイス 11-4
DNS サーバ 4-10
ftp-timeout 4-7
health statistics 17-7
IP フラグメント再構成 7-32
IP フラグメント再構成パラメータ 7-31, 7-39
IP ロギング 7-41
login-banner-text 4-8
Meta Event Generator 8-34
NTP サーバ 4-31
NTP を使用するセンサー 4-32
NVRAM 書き込み 14-16
OS マップ 8-29
TCP
外部ゾーン 9-30
内部ゾーン 9-13
不正ゾーン 9-22
TCP ストリーム再構成 7-40
telnet-option 4-4
UDP
外部ゾーン 9-33
内部ゾーン 9-16
不正ゾーン 9-24
Web サーバの設定 4-12
アカウント ロッキング 4-20
アクセス リスト 4-6
アプリケーション ポリシー 7-20, 7-28
アラート重大度 7-10
アラート頻度パラメータ 7-8
異常検出の動作設定 9-10, 9-38
イベント アクション 7-17
イベント アクション フィルタ 8-22
イベント カウンタ 7-11
外部ゾーン 9-29
グローバル相関 10-10
最大拒否攻撃者数 8-34
最大ブロッキング インターフェイス数 14-18
最大ブロック エントリ数 14-12
サマライザ 8-34
時間帯設定 4-30
シグニチャ忠実度レーティング 7-12
自動 IP ロギング 12-3
手動 IP ロギング 12-4
ステータス 7-13
すべてのブロッキング イベントとエラーのロギング 14-17
脆弱な OS 7-15
接続のブロッキング 14-35
絶対にブロックしないネットワーク 14-20
絶対にブロックしないホスト 14-20
センサー自体をブロックするためのセンサーの設定 14-8

その他のプロトコル
外部ゾーン 9-35
内部ゾーン 9-18
不正ゾーン 9-27
特権 4-18
トラフィック フロー通知 5-4
内部ゾーン 9-12
夏時間
non-recurring 4-29
recurring 4-27
ネットワーク参加 10-11
ネットワーク ブロック 14-34
パスワード 4-17
パスワード ポリシー 4-19
不正ゾーン 9-21
プロキシ サーバ 4-10
ブロッキング
時間 14-13
スイッチ 14-27
ファイアウォール 14-28
ルータ 14-24
ホスト IP アドレス 4-3
ホスト ブロック 14-33
ホスト名 4-2
マスター ブロッキング センサー 14-31
無差別モード 5-2
ユーザ プロファイル 14-21
論理デバイス 14-21
設定されている OS マッピング（例） 8-28
設定ファイル
マージ 16-24, C-3
設定ファイルのマージ 16-24, C-3
センサー
IP アドレスの競合 C-22
NTP 時刻源 4-32
NTP 時刻源の使用 4-31
NTP を使用するための設定 4-32
setup コマンド 3-1, 3-4
アクセスの問題 C-19
アプリケーション パーティション イメージ 20-11
誤った NTP の設定 C-11
アラートなし C-27
イメージの再作成 19-9
管理
スイッチ 14-27
ファイアウォール 14-28
ルータ 14-24
時刻源 C-10
システム イメージ 19-9
システム イメージの復元 19-9
初期化 3-1, 3-4
設定が誤っているアクセス リスト C-21
設定順序 1-2
センシング プロセスが動作していない C-23
ソフトウェア アップグレードのトラブルシューティング C-47
ディザスタ リカバリ C-6
パーティション A-4
パケットを監視しない C-28
破損した SensorApp 設定 C-29
非対称トラフィックおよび異常検出のディセーブル化 9-49, C-14
物理的な接続性 C-25
予防保守 C-2
ログイン
SSH 2-3
Telnet 2-3
センサー データベースのクリア 17-5
センサーにアクセスできない C-19
センサーのイメージの再作成 19-9, 20-10
センサーの時刻の修正 4-25, C-12
センサー ライセンス
インストール 19-12
入手方法 19-12
センシング インターフェイスの説明 5-2

そ

ゾーン
- 外部 9-4
- 内部 9-4
- 不正 9-4

その他のアクション（リスト） 8-5

ソフトウェア アーキテクチャ
- IDAPI（図） A-34

ソフトウェア アップデート
- サポートされている FTP サーバ 20-2
- サポートされている HTTP/HTTPS サーバ 20-2

ソフトウェア アップデートの適用 C-46

ソフトウェアのダウンロード 19-2

ソフトウェア ファイル名
- シグニチャ / ウイルス アップデート（図） 19-5
- シグニチャ エンジン アップデート（図） 19-5
- システム イメージ（図） 19-6
- リカバリ（図） 19-6

ソフトウェア リリースの例
- プラットフォーム ID 19-8
- プラットフォーム依存 19-7
- プラットフォーム非依存 19-6

た

ターゲットの価値レーティング
- 説明 8-13, 8-14
- リスク レーティングの計算 8-13

ターミナル
- サーバの設定 20-3
- 長さの変更 17-12

ターミナル サーバの設定 20-3

ターミナル プロパティの変更 17-12

タブ補完の使用 1-5

ち

チューニング済みシグニチャの説明 7-4

つ

追加
- SSH の既知のホスト リストへのホストの 4-35
- イベント アクション オーバーライド 8-18
- 外部製品インターフェイス 11-6
- 仮想センサー 6-9
- 仮想センサー（IPS SSP） 6-4, 18-5
- 拒否攻撃者 8-36
- グローバル パラメータ 6-11
- シグニチャ変数 7-5
- 信頼できるホスト 4-40
- ターゲットの価値レーティング 8-15
- ユーザ 4-14, 4-17, 4-18
- ログイン バナー 4-8

て

ディザスタ リカバリ C-6

ディセーブル化
- Telnet 4-4
- 異常検出 9-49, C-14
- グローバル相関 10-14
- シグニチャ 7-13
- パスワードの回復 4-23, 17-3, C-9

データ構造
- 例 A-7

データベースのクリアに関する注意 17-4

デバイス アクセスの問題 C-34

デバッグ ロギングのイネーブル化 C-40

デバッグ ロギングの使用 C-39

デフォルト仮想センサー vs0 6-2

デフォルト キーワード 1-10

デフォルト入力のプロンプト 1-4

デフォルトのブロッキング時間 14-13

と

同時 CLI セッションの制限 18-1

特権
設定 4-18
変更 4-18
トライアル ライセンス キー 4-42, 19-11
トラフィック フロー通知
設定 5-4
説明 5-4
トラブルシューティング C-1
ARC
SSH のイネーブル化 C-36
誤って設定されたマスター ブロッキング センサー C-38
シグニチャに対してブロッキングが発生していない C-37
デバイス アクセスの問題 C-34
デバイス インターフェイスの確認 C-35
非アクティブ状態 C-32
ARC ステータスの確認 C-31
cidDump C-76
IPS SSP コマンド C-49
IPS モジュールの時刻のずれ 4-25, C-11
NTP C-45
show events コマンド C-72
show interfaces コマンド C-70, C-71
show statistics コマンド C-60
show tech-support コマンド C-53, C-54, C-55
show version コマンド C-57
SPAN ポートの問題 C-25
syslog への cidLog メッセージ C-44
アップグレード C-45
アラートなし C-27
外部製品インターフェイス 11-9, C-17
グローバル相関 10-13, C-13
サービス アカウント 4-16, C-5
自動アップデート C-46
重複するセンサー IP アドレス C-22
情報の収集 C-52
設定が誤っているアクセス リスト C-21
センサー イベント C-72
センサーがパケットを監視しない C-28
センサー ソフトウェア アップグレード C-47
センサーにアクセスできない C-19
センシング プロセスが動作していない C-23
ソフトウェア アップデートの適用 C-46
ソフトウェアのアップグレード C-45
通信 C-18
ディザスタ リカバリ C-6
デバッグ ロガー ゾーン名（テーブル） C-43
デバッグ ロギング C-39
デバッグ ロギングをイネーブルにする C-40
パスワードの回復 4-24, 17-4, C-10
破損した SensorApp 設定 C-29
不正なホストに対する手動ブロック C-36
物理的な接続性に関する問題 C-25
ブロッキング
シグニチャに対して発生していない C-37
分析エンジンが実行中であることの確認 C-15
予防保守 C-2
トロイの木馬
BO B-68
BO2K B-68
LOKI B-67
TFN2K B-68

な

内部ゾーン
TCP の設定 9-13
UDP の設定 9-16
設定 9-12
説明 9-11
その他のプロトコルの設定 9-18
プロトコル 9-11
夏時間
設定
non-recurring 4-29
recurring 4-27
ナレッジ ベース。「KB」を参照。

に

入手方法
- IPS ソフトウェア 19-2
- 暗号化アカウント 19-3
- コマンド履歴 17-34
- 使用したコマンドのリスト 17-34
- センサー ライセンス 19-12
- ブロックされているホストおよび接続のリスト 14-35
- ライセンス キー 4-42, 19-10

認証済み NTP 4-24, 4-32, C-11

ね

ネイバー探索
- オプション B-27
- タイプ B-27

ネットワーク参加
- SensorBase ネットワーク 10-4
- オプション 10-11
- 説明 10-4
- データの収集 10-4
- データの使用（表） 10-2
- 統計情報 10-4
- ヘルス メトリック 10-7
- モード 10-4
- 要件 10-4

ネットワーク参加データ
- シグニチャ忠実度の向上 10-5
- センサー導入の概要 10-5

ネットワーク ブロックの設定 14-34
ネットワークの接続性の診断 17-34

の

ノーマライザ エンジン
- IPv6 フラグメント B-34
- IP フラグメント再構成 B-34
- TCP ストリーム再構成 B-34
- 説明 B-34
- パラメータ（表） B-35

は

パーティション
- アプリケーション A-4
- メンテナンス A-4
- リカバリ A-4

廃止フィールドの説明 B-7
パケット ファイル
- 表示
  - TCPDUMP 13-7
  - Wireshark 13-7

パスワード
- 設定 4-17
- 変更 4-17

パスワードの回復
- CLI 4-23, 17-3, C-9
- IPS SSP 4-22, 17-2, C-8
- 確認 4-23, 17-3, C-9
- 設定の表示 4-23, 17-3, C-9
- ディセーブル化 4-23, 17-3, C-9
- トラブルシューティング 4-24, 17-4, C-10

パスワード ポリシー
- 設定 4-19
- 注意 4-19

バックアップ
- 現在の設定 16-23, C-4, C-5
- 設定 16-24, C-3

パッシブ OS フィンガープリント
- イネーブル（デフォルト） 8-27
- コンポーネント 8-26
- 設定 8-27
- 説明 8-26

パッチ リリースの説明 19-4
汎用コマンド 1-9

ひ

非アクティブ モード（異常検出） 9-4
ピアツーピア。「P2P」を参照。
非対称トラフィック
  異常検出 9-2
  異常検出のディセーブル化 9-49, C-14
  注意 9-2
非認証の NTP 4-24, 4-32, C-11
ビューア特権のモニタ 1-4
ビューア ロール特権 1-4
表示
  IP ログの内容 12-5
  KB しきい値 9-46
  KB ファイル 9-40
  OS ID 8-32
  tech サポート情報 17-30, C-54
  異常検出の統計情報 9-48
  異常検出ポリシー 9-8
  異常検出ポリシー リスト 17-19
  イベント 8-40, 17-14, C-74
  イベント アクション規則ポリシー 8-7
  イベント アクション規則リスト 17-20
  インターフェイス統計情報 5-6
  現在のサブモード コンフィギュレーション 16-3
  現在の設定 16-1
  サブモードの設定 17-36
  シグニチャ定義リスト 17-20
  システム クロック 4-26, 17-17
  統計 17-20, C-61
  バージョン 17-31, C-57
  パスワードの回復の設定 4-23, 17-3, C-9
  ヘルス ステータス 17-10, C-53
  ポリシー リスト 17-19
  ユーザ情報 4-19
  ライセンス キーのステータス 4-43, 19-11
  ライブ トラフィック 13-3
  論理ファイルの内容 16-20
標準
  CIDEE A-33
  IDCONF A-32
  IDIOM A-32
  SDEE A-33
開くことのできる最大 IP ログ数 6-11

ふ

ファイル
  Cisco IPS（リスト） 19-1, 20-1
  [Download Software] サイト 19-2
  サービス パック 19-2
  シグニチャ エンジン アップデート 19-2
  マイナー アップデート 19-2
  メジャー アップデート 19-2
  リカバリ 19-2
フィルタリング
  more コマンド 16-16
  サブモード コンフィギュレーション 16-18
復元
  アプリケーション パーティション イメージ 20-11
不正ゾーン
  TCP の設定 9-22
  UDP の設定 9-24
  設定 9-21
  説明 9-20
  その他のプロトコルの設定 9-27
  プロトコル 9-20
不正なホストに対する手動ブロック C-36
物理的な接続性に関する問題 C-25
プラットフォームでの同時 CLI セッション 18-1
プロキシ サーバの設定 4-10
ブロッキング
  show statistics 14-35
  シグニチャに対して発生していない C-37
  スイッチの管理 14-27
  接続 14-34, 14-35
  説明 14-2

タイプ 14-2
必要な情報 14-3
ファイアウォールの管理 14-28
ホスト 14-32
ユーザ プロファイル 14-21
ルータの管理 14-24
ブロッキングの前提条件 14-5
ブロック
最大エントリ 14-11
サポートされているデバイス 14-6
センサー自体のブロック 14-8
前提条件 14-5
ブロックされたホストのリスト 14-35
ブロックされないアドレス 14-19
ブロック時間 14-13
プロパティ 14-7
マスター ブロッキング センサー 14-29
無効化 14-10
ブロックされたホストのリスト 14-35
プロトコル
ARP B-13
CIDEE A-33
DCE B-45
DDoS B-67
H225.0 B-40
H.323 B-40
HTTP 4-12
ICMPv6 B-14
IDAPI A-34
IDCONF A-32
IDIOM A-32
IPv6 B-26
LOKI B-67
MSSQL B-46
Q.931 B-40
RPC B-45
SDEE A-33
ネイバー探索 B-26
分散型サービス拒否攻撃。「DDoS」を参照。
分析エンジン
エラー C-46
エラー メッセージ C-18
仮想センサー 6-1
実行中であることの確認 C-15
説明 6-1
分析エンジンに関するエラー C-46

へ

平時の学習（異常検出） 9-3
ヘルス ステータス グローバル相関 10-7, 19-8
ヘルプ
疑問符 1-5
使用 1-5
変更
FTP タイムアウト 4-7
Web サーバの設定 4-12
アクセス リスト 4-6
特権 4-18
パスワード 4-17
ホスト IP アドレス 4-3
ホスト名 4-2
編集
異常検出ポリシー 9-8
イベント アクション規則ポリシー 8-7
イベント アクション変数 8-10
シグニチャ定義ポリシー 7-2
シグニチャ変数 7-5
ターゲットの価値レーティング 8-15

ほ

ホスト IP アドレス
設定 4-3
変更 4-3
ホスト ブロックの設定 14-33
ホスト ポスチャ イベント
CSA MC 11-4

説明 11-2
ホスト名
設定 4-2
変更 4-2
ポリシー リストの表示 17-19

ま

マイナー アップデートの説明 19-3
マスター エンジン パラメータ
脆弱な OS B-7
廃止 B-7
無差別デルタ B-6
マスター ブロッキング センサー
設定の確認 C-38
説明 14-29
適切に設定されていない C-38
マニフェスト
クライアント A-28
サーバ A-28

む

無効化
ブロッキング 14-10
無差別デルタ
説明 7-7, 8-13
リスク レーティングの計算 8-13
無差別デルタの説明 B-6
無差別モード
アトミック アタック 5-3
設定 5-2
説明 5-3
パケット フロー 5-3

め

メジャー アップデートの説明 19-3
メンテナンス パーティションの説明 A-4

も

モード
異常検出学習受け入れ 9-3
異常検出による検出 9-4
インライン インターフェイス ペア 5-4
非アクティブ（異常検出） 9-4
無差別 5-3

ゆ

有効性
説明 10-5
測定 10-5
ユーザ
削除 4-14
追加 4-14
ユーザ情報の表示 4-19
ユーザ プロファイル 14-21
ユーザ ロール
オペレータ 1-3
管理者 1-3
サービス 1-3
ビューア 1-3

よ

呼び出し
使用 1-5
ヘルプおよびタブ補完 1-5

ら

ライセンシング
IPS デバイスのシリアル番号 4-42, 19-10
説明 4-42, 19-10

ライセンス キー
インストール 4-45, 19-14
ステータスの表示 4-43, 19-11
トライアル 4-42, 19-11
入手方法 4-42, 19-10
ライブ トラフィックのキャプチャ 13-5
ラウンドトリップ時間。「RTT」を参照。

り

リカバリ パーティション
アップグレード 20-9
説明 A-4
リスク レーティング
アラーム チャネル 10-5
グローバル相関 10-5
計算 8-12
説明 8-26
レピュテーション スコア 10-5
リスク レーティングの計算
ウォッチ リスト レーティング 8-13
攻撃関連性レーティング 8-13
攻撃の重大度レーティング 8-12
シグニチャ忠実度レーティング 8-12
ターゲットの価値レーティング 8-13
無差別デルタ 8-13
リセット
IPS SSP パスワード 4-22, 17-2, C-8

れ

レート制限
ACL 14-5
サービス ポリシー 14-5
サポートされているシグニチャ 14-4
説明 14-4
ルータ 14-4
レピュテーション
サーバ 10-3
図 10-3
説明 10-3

ろ

ロガー
syslog メッセージ A-19
機能 A-19
説明 A-3, A-19
ログイン
サービス ロール 2-2
センサー
SSH 2-3
Telnet 2-3
ターミナル サーバ 20-3
ユーザ ロール 2-1
ログイン バナーの追加 4-8

わ

ワーム
Blaster 9-3
Code Red 9-2, 9-3
Nimbda 9-2
Sasser 9-3
Slammer 9-3
SQL Slammer 9-2
スキャナ 9-3
ヒストグラム 9-37
プロトコル 9-3
ワーム タイムアウトの指定 9-10, 9-38
割り当て
仮想センサーへのインターフェイスの割り当て（IPS SSP） 6-4, 18-4
仮想センサーへのポリシーの割り当て（IPS SSP） 6-4, 18-4