Cisco Intrusion Prevention System Device Manager インストレーション ユーザ ガイド 5.1

Text Part Number: OL-8674-01-J

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。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。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、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、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、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性が シスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、および StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、StrataView Plus、TeleRouter、The Fastest Way to Increase Your Internet Quotient、および TransPath は、米国および一部の国における Cisco Systems, Inc. とその関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のものです。「パートナー」という語の使用は、シスコと他社の提携関係を意味するものではありません。（0502R）

Cisco Intrusion Prevention System Device Manager インストレーション ユーザ ガイド 5.1
Copyright © 2005 Cisco Systems, Inc.
All rights reserved.

このマニュアルについて xxi
対象読者 xxii
表記法 xxii
関連資料 xxiii
技術情報の入手方法 xxiii
Cisco.com xxiii
Product Documentation DVD（英語版） xxiii
マニュアルの発注方法（英語版） xxiv
シスコシステムズマニュアルセンター xxiv
シスコ製品のセキュリティの概要 xxv
シスコ製品のセキュリティ問題の報告 xxv
テクニカル サポート xxvi
Cisco Technical Support & Documentation Web サイト xxvi
Japan TAC Web サイト xxvi
サービス リクエストの発行 xxvii
サービス リクエストのシビラティの定義 xxvii
その他の資料および情報の入手 xxviii

CHAPTER 1
使用する前に 1-1
勧告 1-2
IDM の概要 1-2
システム要件 1-3
Java プラグインのメモリ サイズの増加 1-4
Windows での Java プラグイン 1-4
Linux と Solaris での Java プラグイン 1-5
センサーの初期化 1-6
概要 1-6
センサーの初期化 1-6
初期化の確認 1-12
IDM へのログイン 1-16
概要 1-16

前提条件 1-16
サポートされるユーザのロール 1-16
IDM へのログイン 1-16
IDM と Cookie 1-17
IDM と証明書 1-18
証明書について 1-18
Internet Explorer での CA の検証 1-19
Netscape での CA の検証 1-21
Mozilla の CA の検証 1-22
センサーのライセンスの入手 1-23
概要 1-23
IPS 製品のサービス プログラム 1-24
サポートされるユーザのロール 1-25
フィールド定義 1-25
ライセンス キーの取得とインストール 1-26

CHAPTER 2 センサーのセットアップ 2-1
ネットワーク設定の構成 2-2
概要 2-2
サポートされるユーザのロール 2-2
フィールド定義 2-2
ネットワーク設定の構成 2-3
許可されたホストの設定 2-5
概要 2-5
サポートされているユーザ ロール 2-5
フィールド定義 2-5
Allowed Hosts パネル 2-6
Add and Edit Allowed Host ダイアログボックス 2-6
許可されたホストの設定 2-6
SSH の設定 2-8
許可鍵の定義 2-8
概要 2-8
サポートされるユーザのロール 2-9
フィールド定義 2-9
許可鍵の定義 2-10
既知のホスト鍵の定義 2-12
概要 2-12
サポートされるユーザのロール 2-12
フィールド定義 2-12

既知のホスト鍵の定義 2-13
センサー SSH ホスト鍵の表示と生成 2-15
概要 2-15
サポートされるユーザのロール 2-15
フィールド定義 2-15
センサー SSH ホスト鍵の表示と生成 2-15
証明書の設定 2-17
信頼できるホストの追加 2-17
概要 2-17
サポートされるユーザのロール 2-17
フィールド定義 2-17
信頼できるホストの追加 2-18
サーバ証明書の表示と生成 2-19
概要 2-19
サポートされるユーザのロール 2-20
フィールド定義 2-20
サーバ証明書の表示と生成 2-20
時刻の設定 2-21
概要 2-21
時刻源およびセンサー 2-21
サポートされるユーザのロール 2-23
フィールド定義 2-23
Time パネル 2-23
Configure Summertime ダイアログボックス 2-24
センサー上の時刻の設定 2-25
センサー上の時刻の修正 2-27
ユーザの設定 2-28
概要 2-28
サポートされるユーザのロール 2-29
フィールド定義 2-29
Users パネル 2-29
Add and Edit User ダイアログボックス 2-30
ユーザの設定 2-30

CHAPTER 3
インターフェイスの設定 3-1
インターフェイスの説明 3-2
混合モードの説明 3-3
インライン インターフェイス モードの説明 3-3
インライン VLAN ペア モードの説明 3-4

インターフェイス サポート 3-5
インターフェイスの設定上の制限 3-7
サマリー 3-9
概要 3-9
サポートされるユーザのロール 3-9
フィールド定義 3-9
インターフェイスの設定 3-10
概要 3-10
TCP リセットの説明 3-10
サポートされるユーザのロール 3-11
フィールド定義 3-11
Interfaces パネル 3-11
Edit Interface ダイアログボックス 3-12
インターフェイスの設定 3-13
インライン インターフェイス ペアの設定 3-14
概要 3-14
サポートされるユーザのロール 3-14
フィールド定義 3-14
Interface Pairs パネル 3-14
Add and Edit Interface Pair ダイアログボックス 3-15
インライン インターフェイス ペアの設定 3-15
インライン VLAN ペアの設定 3-17
概要 3-17
サポートされるユーザのロール 3-17
フィールド定義 3-17
VLAN Pairs パネル 3-18
Add and Edit VLAN Pair ダイアログボックス 3-18
インライン VLAN ペアの設定 3-19
バイパス モードの設定 3-21
概要 3-21
サポートされるユーザのロール 3-21
フィールド定義 3-22
トラフィック フロー通知の設定 3-23
概要 3-23
サポートされるユーザのロール 3-23
フィールド定義 3-23
トラフィック フロー通知の設定 3-23

CHAPTER 4 分析エンジン 4-1
分析エンジンについて 4-1
仮想センサーの設定 4-2
概要 4-2
サポートされるユーザのロール 4-2
フィールド定義 4-2
Virtual Sensor パネル 4-3
Edit Virtual Sensor ダイアログボックス 4-3
インターフェイスの仮想センサーへの割り当て 4-3
グローバル変数の設定 4-5
概要 4-5
サポートされるユーザのロール 4-5
フィールド定義 4-5

CHAPTER 5 シグニチャの定義 5-1
シグニチャの説明 5-2
シグニチャ変数の設定 5-3
概要 5-3
サポートされるユーザのロール 5-3
フィールド定義 5-3
Signature Variables パネル 5-3
Add and Edit Signature Variable ダイアログボックス 5-4
シグニチャ変数の設定 5-4
シグニチャの設定 5-6
概要 5-6
サポートされるユーザのロール 5-6
フィールド定義 5-7
Signature Configuration パネル 5-7
Add Signatures ダイアログボックス 5-8
Clone and Edit Signature ダイアログボックス 5-12
Assign Actions ダイアログボックス 5-16
シグニチャの追加 5-17
シグニチャの複製 5-19
シグニチャのチューニング 5-21
シグニチャのイネーブル化とディセーブル化 5-22
シグニチャのアクティブ化とリタイア化 5-23
シグニチャへのアクションの割り当て 5-24
Miscellaneous パネルの設定 5-27

概要 5-27
サポートされるユーザのロール 5-27
フィールド定義 5-28
アプリケーション ポリシーの設定 5-28
概要 5-29
AIC 要求メソッド シグニチャ 5-30
AIC MIME 定義コンテンツ タイプ シグニチャ 5-31
AIC 転送符号化シグニチャ 5-34
AIC FTP コマンド シグニチャ 5-34
アプリケーション ポリシーの設定 5-35
認識済みの定義コンテンツ タイプ（MIME）シグニチャの例 5-36
IP フラグメント再構成の設定 5-37
概要 5-37
IP フラグメント再構成と設定可能なパラメータ 5-37
IP フラグメント再構成シグニチャの設定 5-38
IP フラグメント再構成方法の設定 5-39
TCP ストリーム再構成の設定 5-40
概要 5-40
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 5-40
TCP ストリーム再構成シグニチャの設定 5-42
TCP ストリーム再構成モードの設定 5-43
IP ロギングの設定 5-44
MEG シグニチャの例 5-45

CHAPTER 6
カスタム シグニチャの作成 6-1
Custom Signature Wizard について 6-2
シグニチャ エンジンを使用する方法 6-3
シグニチャ エンジンを使用しない方法 6-4
サポートされるユーザのロール 6-5
フィールド定義 6-5
Welcome フィールド定義 6-5
Protocol Type フィールド定義 6-6
Signature Identification フィールド定義 6-7
Atomic IP Engine Parameters フィールド定義 6-7
Service HTTP Engine Parameters フィールド定義 6-8
Service MSRPC Engine Parameters フィールド定義 6-9
Service RPC Engine Parameters フィールド定義 6-10
State Engine Parameters フィールド定義 6-11
String ICMP Engine Parameters フィールド定義 6-11

String TCP Engine Parameters フィールド定義 6-12
String UDP Engine Parameters フィールド定義 6-13
Sweep Engine Parameters フィールド定義 6-14
ICMP Traffic Type フィールド定義 6-15
UDP Traffic Type フィールド定義 6-15
TCP Traffic Type フィールド定義 6-15
UDP Sweep Type フィールド定義 6-16
TCP Sweep Type フィールド定義 6-16
Service Type フィールド定義 6-16
Inspect Data フィールド定義 6-17
Alert Response フィールド定義 6-17
Alert Behavior フィールド定義 6-18
Advanced Alert Behavior ウィザード 6-18
Event Count and Interval フィールド定義 6-18
Alert Summarization フィールド定義 6-19
Alert Dynamic Response Summary フィールド定義 6-19
Alert Dynamic Response Fire All フィールド定義 6-20
Alert Dynamic Response Fire Once フィールド定義 6-20
Global Summarization フィールド定義 6-21
カスタム シグニチャの作成 6-22
Custom Signature Wizard でサポートされていないシグニチャ エンジン 6-22
マスター カスタム シグニチャの手順 6-23
String TCP シグニチャの例 6-29
Service HTTP シグニチャの例 6-34

CHAPTER 7 イベント アクション ルールの設定 7-1
イベント アクション ルールについて 7-2
リスク評価の計算 7-2
イベント オーバーライド 7-3
イベント アクション フィルタ 7-3
イベント アクションの要約と集約 7-3
イベント アクションの要約 7-3
イベント アクションの集約 7-4
Signature Event Action Processor 7-4
イベント アクション 7-7
イベント アクション ルールの例 7-9
イベント変数の設定 7-11
概要 7-11

サポートされるユーザのロール 7-11
フィールド定義 7-12
Event Variables パネル 7-12
Add and Edit Event Variable ダイアログボックス 7-12
イベント変数の設定 7-12
Target Value Rating の設定 7-14
概要 7-14
サポートされるユーザのロール 7-14
フィールド定義 7-14
Target Value Rating パネル 7-14
Add and Edit Target Value Rating ダイアログボックス 7-15
Target Value Rating の設定 7-15
イベント アクション オーバーライドの設定 7-17
概要 7-17
サポートされるユーザのロール 7-17
フィールド定義 7-17
Event Action Overrides パネル 7-17
Add and Edit Event Action Overrides ダイアログボックス 7-18
イベント アクション オーバーライドの設定 7-20
イベント アクション フィルタの設定 7-22
概要 7-22
サポートされるユーザのロール 7-22
フィールド定義 7-22
Event Action Filters パネル 7-22
Add and Edit Event Action Filters ダイアログボックス 7-24
イベント アクション フィルタの設定 7-26
一般的な設定値の設定 7-30
概要 7-30
サポートされるユーザのロール 7-30
フィールド定義 7-30
イベント アクション ルールの一般的な設定値の設定 7-31
イベントの監視 7-33
概要 7-33
サポートされるユーザのロール 7-33
フィールド定義 7-33
Events パネル 7-33
Event Viewer ページ 7-34
イベント表示の設定 7-35

CHAPTER 8 ブロッキングとレート制限のための ARC の設定 8-1
ブロッキングについて 8-2
レート制限について 8-4
ARC を設定する前に 8-5
サポートされているデバイス 8-6
ブロッキング プロパティの設定 8-8
概要 8-8
サポートされているユーザ ロール 8-9
フィールド定義 8-9
Blocking Properties パネル 8-9
Add and Edit Never Block Address ダイアログボックス 8-11
ブロッキング プロパティの設定 8-11
アクティブなレート制限の管理 8-14
概要 8-14
サポートされるユーザのロール 8-14
フィールド定義 8-14
Rate Limits パネル 8-15
Add Rate Limit ダイアログボックス 8-15
レート制限の設定および管理 8-16
デバイス ログイン プロファイルの設定 8-18
概要 8-18
サポートされるユーザのロール 8-18
フィールド定義 8-18
Device Login Profiles パネル 8-18
Add and Edit Device Login Profile ダイアログボックス 8-19
デバイス ログイン プロファイルの設定 8-20
ブロッキング デバイスおよびレート制限デバイスの設定 8-22
概要 8-22
サポートされるユーザのロール 8-22
フィールド定義 8-22
Blocking Devices パネル 8-23
Add/Edit Blocking Devices ダイアログボックス 8-23
ブロッキング デバイスおよびレート制限デバイスの設定 8-24
ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定 8-27
Sensor がデバイスを管理する方法 8-27
レート制限のサービス ポリシーについて 8-28
概要 8-28
サポートされるユーザのロール 8-29

フィールド定義 8-29
Router Blocking Device Interfaces パネル 8-30
Add and Edit Router Blocking Device Interface ダイアログボックス 8-30
ルータのブロッキングおよびレート制限のデバイス インターフェイスの設定 8-31
Catalyst 6000 のブロッキング デバイス インターフェイスの設定 8-33
概要 8-33
サポートされるユーザのロール 8-34
フィールド定義 8-34
Cat 6K Blocking Device Interfaces パネル 8-34
Add and Edit Cat 6K Blocking Device Interface ダイアログボックス 8-35
Catalyst 6000 のブロッキング デバイス インターフェイスの設定 8-35
マスター ブロッキング センサーの設定 8-37
概要 8-37
サポートされるユーザのロール 8-38
フィールド定義 8-38
Master Blocking Sensor パネル 8-38
Add and Edit Master Blocking Sensor ダイアログボックス 8-39
マスター ブロッキング センサーの設定 8-39
アクティブなホスト ブロックの管理 8-42
概要 8-42
サポートされるユーザのロール 8-42
フィールド定義 8-42
Active Host Blocks パネル 8-42
Add Active Host Block ダイアログボックス 8-43
アクティブなホスト ブロックの設定および管理 8-44
ネットワーク ブロックの管理 8-46
概要 8-46
サポートされるユーザのロール 8-46
フィールド定義 8-46
Network Blocks パネル 8-46
Add Network Block ダイアログボックス 8-47
ネットワーク ブロックの設定および管理 8-47

CHAPTER 9
SNMP の設定 9-1
SNMP の説明 9-2
SNMP の設定 9-3

概要 9-3
サポートされるユーザのロール 9-3
フィールド定義 9-3
SNMP の設定 9-4
SNMP トラップの設定 9-5
概要 9-5
サポートされているユーザ ロール 9-5
フィールド定義 9-5
SNMP Traps Configuration パネル 9-5
Add and Edit SNMP Trap Destination ダイアログボックス 9-6
SNMP トラップの設定 9-6

CHAPTER 10
センサーの保守 10-1
センサーの自動更新 10-2
概要 10-2
サポートされるユーザのロール 10-2
フィールド定義 10-2
自動更新の設定 10-3
デフォルト設定の復元 10-5
概要 10-5
サポートされるユーザのロール 10-5
フィールド定義 10-5
デフォルト設定の復元 10-5
センサーのリブート 10-6
概要 10-6
サポートされるユーザのロール 10-6
フィールド定義 10-6
センサーのリブート 10-7
センサーのシャットダウン 10-8
概要 10-8
サポートされるユーザのロール 10-8
フィールド定義 10-8
センサーのシャットダウン 10-8
センサーの更新 10-9
概要 10-9
サポートされるユーザのロール 10-9
フィールド定義 10-9
センサーの更新 10-10
診断レポートの生成 10-12

概要 10-12
サポートされるユーザのロール 10-12
フィールド定義 10-12
診断レポートの生成 10-13
統計情報の表示 10-14
概要 10-14
サポートされるユーザのロール 10-14
フィールド定義 10-14
統計情報の表示 10-15
システム情報の表示 10-16
概要 10-16
サポートされるユーザのロール 10-16
フィールド定義 10-16
システム情報の表示 10-16

CHAPTER 11
センサーの監視 11-1
拒否された攻撃者 11-2
概要 11-2
サポートされるユーザのロール 11-2
フィールド定義 11-2
拒否された攻撃者リストの監視 11-3
アクティブなホスト ブロックの設定および管理 11-4
概要 11-4
サポートされるユーザのロール 11-4
フィールド定義 11-4
Active Host Blocks パネル 11-4
Add Active Host Block ダイアログボックス 11-5
アクティブなホスト ブロックの設定および管理 11-6
ネットワーク ブロックの設定および管理 11-8
概要 11-8
サポートされるユーザのロール 11-8
フィールド定義 11-8
Network Blocks パネル 11-8
Add Network Block ダイアログボックス 11-9
ネットワーク ブロックの設定および管理 11-9
レート制限の設定および管理 11-11
概要 11-11
サポートされるユーザのロール 11-11
フィールド定義 11-12

Rate Limits パネル 11-12
Add Rate Limit ダイアログボックス 11-12
レート制限の設定および管理 11-13
IP ロギングの設定 11-15
概要 11-15
サポートされるユーザのロール 11-16
フィールド定義 11-16
IP Logging パネル 11-16
Add and Edit IP Logging ダイアログボックス 11-17
IP ロギングの設定 11-17

CHAPTER 12
ソフトウェアの入手方法 12-1
Cisco IPS ソフトウェアの入手方法 12-2
IPS ソフトウェアのバージョン管理 12-4
IPS ソフトウェア イメージの命名規則 12-4
5.x ソフトウェア リリースの例 12-6
Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード 12-7
暗号化アクセスが可能な Cisco.com アカウントの申し込み 12-8
Cisco.com からのライセンス キーの取得 12-9
概要 12-9
ライセンスのインストール 12-9
IDM の使用方法 12-10
CLI の使用方法 12-11
Cisco Intrusion Prevention Alert Center 12-14
Cisco IPS のアクティブなアップデート通知 12-15
Network Security Database 12-16
IPS ドキュメントへのアクセス 12-16

APPENDIX A
システム アーキテクチャ A-1
システムの概要 A-2
システムの設計 A-2
IPS 5.1 の新機能 A-4
ユーザによる対話操作 A-4
セキュリティ機能 A-5
MainApp A-6
MainApp の機能 A-6
イベント ストア A-7
イベント ストアについて A-7
イベントのデータ構造 A-8

IPS イベント A-9
NotificationApp A-9
CtlTransSource A-11
ARC 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-16
再起動前後の状態の維持 A-16
接続ベースおよび無条件のブロッキング A-17
Cisco ファイアウォールでのブロッキング A-18
Catalyst スイッチでのブロッキング A-19
LogApp A-20
AuthenticationApp A-20
AuthenticationApp の機能 A-20
ユーザの認証 A-21
センサーでの認証の設定 A-21
TLS と SSH の信頼関係の管理 A-22
Web サーバ A-23
SensorApp A-24
機能とコンポーネント A-24
パケット フロー A-25
SEAP A-26
新機能 A-27
CLI A-29
ユーザ ロール A-29
サービス アカウント A-30
CLI の動作 A-31
通信 A-33
IDAPI A-33
RDEP2 A-34
IDIOM A-36
IDCONF A-36
SDEE A-37
CIDEE A-37
IPS 5.1 ファイル構造 A-38
IPS 5.1 アプリケーションの要約 A-39

APPENDIX B シグニチャ エンジン B-1
シグニチャ エンジンについて B-2
Master エンジン B-4
汎用パラメータ B-4
アラートの頻度 B-5
イベント アクション B-6
AIC エンジン B-9
概要 B-9
AIC エンジンのパラメータ B-9
Atomic エンジン B-11
Atomic ARP エンジン B-11
Atomic IP エンジン B-11
Flood エンジン B-13
Meta エンジン B-14
Multi String エンジン B-15
Normalizer エンジン B-16
概要 B-16
Normalizer エンジンのパラメータ B-17
Service エンジン B-18
Service DNS エンジン B-18
Service FTP エンジン B-20
Service Generic エンジン B-20
Service H225 エンジン B-21
概要 B-21
Service H255 エンジンのパラメータ B-23
Service HTTP エンジン B-24
概要 B-24
Service HTTP エンジンのパラメータ B-24
Service IDENT エンジン B-26
Service MSRPC エンジン B-26
概要 B-26
Service MSRPC エンジンのパラメータ B-27
Service MSSQL エンジン B-27
Service NTP エンジン B-28
Service RPC エンジン B-28
Service SMB エンジン B-29
Service SNMP エンジン B-31
Service SSH エンジン B-32

State エンジン B-33
String エンジン B-35
概要 B-35
String ICMP エンジンのパラメータ B-35
String TPC エンジンのパラメータ B-36
String UDP エンジンのパラメータ B-37
Sweep エンジン B-38
Traffic ICMP エンジン B-40
Trojan エンジン B-41

APPENDIX C
トラブルシューティング C-1
予防保守 C-2
障害リカバリ C-3
パスワード リカバリ C-4
4200 シリーズ アプライアンスのトラブルシューティング C-5
通信の問題 C-5
Telnet または SSH を使用してセンサー CLI にアクセスできない C-5
設定が誤っているアクセス リスト C-8
重複する IP アドレスによりインターフェイスがシャットダウンする C-9
SensorApp およびアラート C-11
SensorApp が動作していない C-11
物理接続、SPAN、または VACL ポートの問題 C-12
アラートが表示されない C-14
センサーがパケットを検出しない C-16
破損した SensorApp コンフィギュレーションの削除 C-18
IDS-4250-XL の不良なメモリ C-18
ブロッキング C-19
ブロッキングのトラブルシューティング C-19
ARC が動作していることを確認する C-20
ARC 接続がアクティブであることを確認する C-20
デバイス アクセスの問題 C-22
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 C-24
ネットワーク デバイスへの SSH 接続をイネーブルにする C-25
シグニチャに対してブロッキングが実行されない C-25
マスター ブロッキング センサーのコンフィギュレーションを確認する C-26
ロギング C-28
デバッグ ロギングをイネーブルにする C-28

ゾーン名 C-33
SysLog への cidLog メッセージの転送 C-33
センサーが NTP サーバと同期していることを確認する C-34
シグニチャに対して TCP リセットが実行されない C-35
ソフトウェア アップグレード C-37
ソフトウェア アップグレードの間、IDS-4235 および IDS-4250 が機能停止する C-37
適用するアップグレードとそれらの前提条件 C-37
自動アップデートの問題 C-38
センサーに保存されているアップデートでセンサーをアップデートする C-39
IDM のトラブルシューティング C-41
Java プラグインのメモリ サイズを増やす C-41
Windows での Java プラグイン C-41
Linux および Solaris での Lava プラグイン C-42
IDM を起動できない - Java アプレットのロードに失敗 C-43
IDM を起動できない - 分析エンジンがビジー状態 C-44
IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない C-44
シグニチャがアラートを生成しない C-45
IDSM-2 のトラブルシューティング C-46
IDSM-2 問題の診断 C-46
トラブルシューティング用の switch コマンド C-47
ステータス LED がオフになっている C-47
ステータス LED がオンだが IDSM-2 がオンラインにならない C-50
IDSM-2 コマンド / コントロール ポートと通信できない C-51
TCP リセット インターフェイスの使用方法 C-52
シリアル ケーブルを IDSM-2 に接続する C-53
AIP SSM のトラブルシューティング C-54
情報の収集 C-56
テクニカル サポート情報 C-56
概要 C-56
テクニカル サポート情報の表示 C-57
Tech Support コマンドの出力 C-58
バージョン情報 C-59
概要 C-59
バージョン情報の表示 C-59
統計情報 C-61
概要 C-61

統計情報の表示 C-62
インターフェイスの情報 C-71
概要 C-71
インターフェイス コマンドの出力 C-72
イベント情報 C-72
センサー イベント C-73
概要 C-73
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 サイトのファイルのアップロードとアクセス C-77

GLOSSARY 用語集

INDEX 索引

このマニュアルについて

このマニュアルは、Intrusion Prevention System Device Manager (IDM) 5.1 のインストール方法、設定方法、および使用方法を説明しています。略語および関連する IPS の用語を数多く含む用語集があります。これは Cisco Intrusion Prevention System 5.1 のマニュアル セットの一部です。P.xxiii の「関連資料」で記載されているマニュアルとこのマニュアルを併用してください。

この章の構成は次のとおりです。

- 対象読者（P.xxii）
- 表記法（P.xxii）
- 関連資料（P.xxiii）
- 技術情報の入手方法（P.xxiii）
- シスコ製品のセキュリティの概要（P.xxv）
- テクニカル サポート（P.xxvi）
- その他の資料および情報の入手（P.xxviii）

対象読者

このマニュアルは、次の作業を行う必要のある管理者を対象としています。

- IDM のインストールおよび設定を行う。
- IPS センサーによりネットワークをセキュリティ保護する。
- ネットワーク上の不正侵入を防御し、発生したアラームを監視する。

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
手順の実行中に選択する必要があるコマンド、キーワード、専門用語、およびオプション	太字
ユーザが値を指定する変数、および新しい用語や重要な用語	イタリック体
セッション情報、システム情報、パス、およびファイル名の表示出力	`screen` フォント
ユーザが入力する情報	太字の screen フォント
ユーザが入力する変数	イタリック体の screen フォント
メニュー項目およびボタン名	太字
メニュー項目の選択順序	**Option > Network Preferences**

(注) 「注釈」です。作業を続行する前に確認すべき重要な情報や役立つ情報、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷、データの損失、またはネットワーク セキュリティの侵犯を予防するための注意事項が記述されています。

ヒント ご使用の製品を有効活用するために役立つヒントを示しています。

警告 怪我、ソフトウェアの破壊、または機器の損傷を防止するために留意すべき情報を示しています。この記号がある場合、記載されている情報に従って慎重に作業しないと、明らかなセキュリティ侵犯につながります。

関連資料

次のマニュアルは、Cisco Intrusion Prevention System 5.1 をサポートし、Cisco.com の次の URL で参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids12/index.htm

- *Installing Cisco Intrusion Prevention System Appliances and Modules 5.0*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Command Reference for Cisco Intrusion Prevention System 5.1*

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

最新のシスコのマニュアルには、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコ Web サイトには、次の URL からアクセスできます。

http://www.cisco.com

シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、次の URL にアクセスし、Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support & Documentation Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

使用する前に

この章では、IDM について説明し、IDM を使用するための情報を提供します。この章は、次の項で構成されています。

- 勧告（P.1-2）
- IDM の概要（P.1-2）
- システム要件（P.1-3）
- Java プラグインのメモリ サイズの増加（P.1-4）
- センサーの初期化（P.1-6）
- IDM へのログイン（P.1-16）
- センサーのライセンスの入手（P.1-23）

（注）『*Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1*』は、ASDM の IPS セクションにも適用されます。ASDM のパスは IDM よりも長く、Configuration > Features > IPS > Licensing などのようになっています。

勧告

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコ暗号化製品の出荷は、暗号の輸入、輸出、配布、使用を行うサードパーティの権限を包含するものではありません。輸入者、輸出者、配布者、ユーザは、米国およびその他の国の法律を遵守する責任があります。この製品を使用すると、適用される法律および規則を遵守することに合意したことになります。米国およびその他の国の法律を遵守できない場合は、同封された品目をすぐに返品してください。

シスコ暗号化製品を規制する米国法の概要は、次の Web サイトで参照できます。

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

詳細な情報が必要な場合は、export@cisco.com に電子メールでお問い合せください。

IDM の概要

IDM は、センサーの設定と管理が可能な Web ベースの Java 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、Netscape、または Mozilla Web ブラウザでアクセスできます。

IDM のユーザ インターフェイスは、File メニューと Help メニュー、Configuration ボタンと Monitoring ボタン（これらのボタンのメニューは左側の TOC ペインで開きます）、ページの右側にある Configuration パネルで構成されています。Configuration ボタンと Monitoring ボタンの横に、次の 4 つのボタンが表示されます。

- Back：前に表示していたパネルに戻ります。
- Forward：一度表示したことのある次のパネルに進みます。
- Refresh：現在のコンフィギュレーションをセンサーからロードします。
- Help：新しいウィンドウでオンライン ヘルプを開きます。

センサーを設定するには、**Configuration** をクリックし、左側のペインのメニューで該当するものを探します。**Monitoring** をクリックし、左側のペインのメニューでモニタリングを設定します。

新しい設定は、設定中のパネルの **Apply** をクリックすると有効になります。**Reset** をクリックすると、現在の変更が廃棄され、設定は以前のパネルの状態に戻ります。

システム要件

IDM のシステム要件を次に示します。

- Windows 2000、Windows XP
  - Java プラグイン 1.4.2 または 1.5 がインストールされている Internet Explorer 6.0。または Java プラグイン 1.4.2 または 1.5 がインストールされている Netscape 7.1。
  - Pentium III または 450 Mhz 以上で動作する同等品
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）
- Sun SPARC Solaris
  - Sun Solaris 2.8 または 2.9
  - Mozilla 1.7
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）
- Linux
  - Red Hat Linux 9.0 または Red Hat Enterprise Linux WS、GNOME または KDE を実行するバージョン 3
  - Mozilla 1.7
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）

（注） IDM で使用できるその他の Web ブラウザもありますが、サポートされているのはここに示したブラウザだけです。

Java プラグインのメモリ サイズの増加

IDM を正しく実行するには、Java プラグイン 1.4.2 または 1.5 がブラウザにインストールされている必要があります。デフォルトでは、Java プラグインは 64 MB のメモリを IDM に割り当てます。IDM は使用中にメモリを使い果たしてしまうことがあります。この場合、IDM は停止するか、空白の画面を表示します。**Refresh** をクリックした場合にも、メモリ不足になることがあります。メモリ不足になると、Java コンソールに `OutofMemoryError` メッセージが表示されます。

(注) Sun Microsystems Java を使用することを推奨します。その他のバージョンの Java を使用すると、IDM に問題を引き起こすことがあります。

IDM を使用する前に Java プラグインのメモリ設定を変更する必要があります。必要最小メモリサイズは、256 MB です。

この項で取り上げる事項は次のとおりです。

- Windows での Java プラグイン（P.1-4）
- Linux と Solaris での Java プラグイン（P.1-5）

Windows での Java プラグイン

Windows で Java プラグイン 1.4.2 と 1.5 の設定を変更するには、次の手順を実行します。

ステップ 1　Internet Explorer または Netscape のすべてのインスタンスを閉じます。

ステップ 2　**Start** > **Settings** > **Control Panel** をクリックします。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. Java プラグラインをクリックします。

Java Plug-in Control Panel が表示されます。

b. **Advanced** タブをクリックします。

c. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。

d. **Apply** をクリックして Java Control Panel を終了します。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. Java をクリックします。

Java Control Panel パネルが表示されます。

b. **Java** タブをクリックします。

c. Java Applet Runtime Settings の下で **View** をクリックします。

Java Runtime Settings Panel が表示されます。

d. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力して、**OK** をクリックします。

e. **OK** をクリックして Java Control Panel を終了します。

Linux と Solaris での Java プラグイン

Linux と Solaris での Java プラグイン 1.4.2 または 1.5 の設定を変更するには、次の手順を実行します。

ステップ 1　Netscape または Mozilla のすべてのインスタンスを閉じます。

ステップ 2　ControlPanel 実行可能ファイルを起動すると、Java Plug-in Control Panel が表示されます。

（注） Java 2 SDK では、このファイルは <SDK インストール ディレクトリ >/jre/bin/ControlPanel にあります。たとえば、Java 2 SDK を /usr/j2se にインストールした場合、フルパスは /usr/j2se/jre/bin/ControlPanel です。

（注） Java 2 Runtime Environment をインストールした場合は、ファイルは <JRE インストール ディレクトリ >/bin/ControlPanel にあります。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. **Advanced** タブをクリックします。
b. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。
c. **Apply** をクリックして Java Control Panel を閉じます。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. **Java** タブをクリックします。
b. Java Applet Runtime Settings の下で **View** をクリックします。
c. Java Runtime Parameters フィールドに `-Xmx256m` と入力し、**OK** をクリックします。
d. **OK** をクリックして Java Control Panel を終了します。

センサーの初期化

この項では、センサーの初期化方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.1-6）
- センサーの初期化（P.1-6）
- 初期化の確認（P.1-12）

概要

センサーをネットワークに設置した後、**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。**setup** コマンドを使用して、ホスト名、IP インターフェイス、Telnet サーバ、Web サーバポート、アクセス コントロール リスト、時間設定、およびインターフェイスの割り当てとイネーブル化など、センサーの基本的な設定を行います。センサーを初期化すると、ネットワーク経由でセンサーと通信できるようになります。その後、侵入防御を設定できます。

センサーの初期化

センサーを初期化するには、次の手順を実行します。

ステップ 1　管理者特権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。

- シリアル接続、またはモニタとキーボードを使用して、アプライアンスにログインします。

（注） IDS-4215、IPS-4240、または IPS-4255 では、モニタとキーボードは使用できません。

- IDSM-2 とのセッション：
  - Catalyst ソフトウェアの場合

```
cat6k> enable
cat6k> (enable) session module_number
```

  - Cisco IOS ソフトウェアの場合

```
router# session slot slot_number processor 1
```

- NM-CIDS とのセッション：

```
router# service-module IDS-Sensor slot_number/port_number session
```

- AIP SSM とのセッション：

```
asa# session 1
```

（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　センサーへの初回ログインでは、デフォルト パスワードの変更を求められます。

パスワードは 8 文字以上の長さとし、容易に推測できないもの、つまり辞書に出ていない単語にする必要があります。

注意　パスワードを忘れた場合、センサー イメージの再作成が必要になることもあります（『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照）。ただし、管理者特権を持つ別のユーザがいる場合を除きます。別の管理者がログインして、パスワードを忘れたユーザに新しいパスワードを割り当てることができます。または、サポートのためにサービス アカウントを作成している場合には、TAC でパスワードを作成してもらうことができます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

パスワードを変更すると、`sensor#` プロンプトが表示されます。

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。

（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ています。

```
    --- 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 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
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 443
exit


Current time: Wed May 5 10:25:35 2004
```

ステップ 4　Space キーを押して次の質問を表示します。

```
Continue with configuration dialog?[yes]:
```

一度に 1 ページずつ表示するには Space キーを押します。一度に 1 行ずつ表示するには **Enter** キーを押します。

ステップ 5　`yes` を入力して続行します。

ステップ 6　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、“_”、“-” は有効ですが、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 7　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、IP アドレス / ネットマスク、ゲートウェイ（X.X.X.X/nn,Y.Y.Y.Y）の形式で指定します。ここで、X.X.X.X（X は 0 ～ 255）は、32 ビット アドレスのセンサーの IP アドレスで、ピリオドで区切った 4 つのオクテットで記述されています。nn はネットマスクの番号です。Y.Y.Y.Y（Y は 0 ～ 255）は、32 ビット アドレスのデフォルト ゲートウェイで、ピリオドで区切った 4 つのオクテットで記述されています。

ステップ 8　Telnet サーバのステータスを指定します。

Telnet サービスは disable または enable に設定できます。デフォルトは disable です。

ステップ 9　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 ポートを変更した場合は、IDM への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。指定する形式は `https://`*sensor_ip_address*`:port`（たとえば、`https://10.1.9.201:1040`）です。

（注）　デフォルトでは、Web サーバは TLS および SSL の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、暗号化は無効になりません。

ステップ 10　`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** キーを押すか、または **Enter** キーを押して Permit 行に進みます。

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指定します。

IP ネットワーク インターフェイスは、IP アドレス / ネットマスクの形式、つまり X.X.X.X/nn 形式で表されます。X.X.X.X には、ネットワーク IP アドレスをピリオドで区切った 4 オクテットで記述された 32 ビットのアドレスで指定します。X = 0 ～ 255 です。nn には、そのネットワークのネットマスクのビット数を指定します。

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、10.1.1.0/24 は 10.1.1.0 サブネット上の IP アドレスだけ（10.1.1.0 ～ 10.1.1.255）を許可します。

ネットワーク全体ではなく単一の IP アドレスへのアクセスを許可する場合は、32 ビット 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 のアドレスだけを許可します。

c. アクセス リストに追加するネットワークの入力がすべて終わるまで、ステップ b を繰り返します。

d. 空白の Permit 行で **Enter** キーを押して、次の手順に進みます。

ステップ 11 システム クロックの設定値を修正するには、`yes` を入力します。

a. NTP を使用する場合は `yes` を入力します。

NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。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。手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring the Sensor to Use an NTP Server as its Time Source」を参照してください。

b. サマータイム設定を修正するには、`yes` を入力します。

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

c. サマータイムの設定方法を指定するには、recurring、date、または disable を入力します。

デフォルトは recurring です。

d. recurring を選択した場合は、サマータイム設定の開始月を入力します。

有効な値は、january、february、march、april、may、june、july、august、september、october、november、および december です。

デフォルトは april です。

e. 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、および last です。

デフォルトは first です。

f. 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、および saturday です。

デフォルトは sunday です。

g. 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。デフォルト値は、開始時刻が 4 月の第 1 日曜日午前 2 時、終了時刻が 10 月の第 4 日曜日午前 2 時と指定します。デフォルトのサマータイム オフセットは 60 分です。

h. 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、および december です。

デフォルトは october です。

i. 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、および last です。

デフォルトは last です。

j. 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、および saturday です。

デフォルトは sunday です。

k. サマータイム設定の終了時刻を指定します。

l. DST ゾーンを指定します。

ゾーン名は、最長で 24 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ を使用できます。

m. サマータイム オフセットを指定します。

世界標準時（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 0 です。

n. システムの時間帯を修正するには、**yes** を入力します。

o. 標準時の時間帯名を指定します。

ゾーン名は 24 文字までの文字列です。

p. 標準時のオフセットを指定します。

デフォルトは 0 です。

世界標準時（UTC）からの標準時間帯の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）。

ステップ 12 **yes** を入力して、仮想センサーの設定を修正します（vs0）。

現在のインターフェイス設定が表示されます。

```
Current interface configuration
  Command control: GigabitEthernet0/1
  Unused:
    GigabitEthernet2/1
    GigabitEthernet2/0
  Promiscuous:
    GigabitEthernet0/0
  Inline:
    None
  Inline VLAN Pair:
    None
```

ステップ 13 混合インターフェイスまたはモニタリング インターフェイスを追加するには、**yes** と入力します。

ステップ 14 たとえば **GigabitEthernet0/1** のように、追加するインターフェイスを入力します。

ステップ 15 **yes** と入力して、インライン インターフェイス ペアを追加します（プラットフォームがインライン インターフェイス ペアをサポートしている場合だけ表示されます）。

a. インライン インターフェイス ペアの名前を入力します。

b. インライン インターフェイス ペアの説明を入力します。

デフォルトは、`Created via setup by user <yourusername>` です。

c. インライン ペアの最初のインターフェイスの名前 **interface1** を入力します。

d. インライン ペアの 2 番目のインターフェイスの名前 **interface2** を入力します。

e. ステップ a から d を繰り返して別のインライン インターフェイス ペアを追加するか、または **Enter** キーを押して次のオプションに進みます。

ステップ 16 **yes** と入力して、インライン VLAN ペアを追加します（プラットフォームがインライン VLAN ペアをサポートしている場合だけ表示されます）。

インライン VLAN ペアで使用可能なインターフェイスのリストが表示されます。

```
Available Interfaces:
 [1] GigabitEthernet0/0
 [2] GigabitEthernet2/0
 [3] GigabitEthernet2/1
```

ステップ 17 インライン VLAN ペアに分割するインターフェイスの番号を入力します。

そのインターフェイスの現在のインライン VLAN ペア設定が表示されます。

```
Inline Vlan Pairs for GigabitEthernet0/0
  None
```

a. 追加するサブインターフェイル番号を入力します。

b. インライン VLAN ペアの説明を入力します。

c. 1 番目の VLAN 番号（vlan1）を入力します。

d. 2 番目の VLAN 番号（vlan2）を入力します。

e. ステップ a から d を繰り返して別のインライン VLAN ペアをこのインターフェイスに追加するか、または **Enter** キーを押して次のオプションに進みます。

ステップ 18 **yes** を入力して、別のインターフェイスを分割します。インライン VLAN ペアの追加を完了するには、**no** と入力するか、または **Enter** キーを押します。

設定した内容が次のオプションと共に表示されます。

```
[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 19 **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 20 システムの日付と時刻を修正するには、**yes** を入力します。

（注） このオプションは、モジュールでは使用できません。また NTP が設定されている場合も使用できません。このモジュールは、設置されているルータまたはスイッチ、あるいは設定済みの NTP サーバから時刻を取得します。

a. 現地日付を入力します（yyyy-mm-dd）。

b. 現地時間を入力します（hh:mm:ss）。

ステップ 21 センサーをリブートします。

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

ステップ 22 **yes** を入力してリブートを続行します。

ステップ 23 自己署名 X.509 証明書を表示します（TLS で必要です）。

```
sensor# 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 24 証明書のフィンガープリントを書き留めます。

この情報は、Web ブラウザでこのセンサーへ接続した際に証明書の信頼性を確認するために必要になります。

ステップ 25 最新のサービス パックおよびシグニチャ アップデートを適用します。

最新版のソフトウェアを入手する方法については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。最新のソフトウェア アップデートを適用する方法は Readme で説明されています。

これでセンサーの侵入防御設定を行う準備ができました。

初期化の確認

センサーが初期化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 センサーにログインします。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Logging In to the Sensor」を参照してください。

ステップ 2　設定を表示します。

```
sensor# show configuration
generating current config:
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
```

```
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTAlVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESM
BAGA1UECxMJU1NNLUlQUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEPudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVwHji12vBLo+biULJG95hbTFlqO+ba3R6nPD3tepgx5zTdOr2onnlFHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ1lAQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfM3HlOEwN
exit
! ------------------------------
service web-server
exit
sensor#
```

(注)　また、**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 証明書を表示します（TLS で必要です）。

```
sensor# 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。

この情報は、Web ブラウザでこのセンサーへ接続した際に証明書の信頼性を確認するために必要になります。

IDM へのログイン

この項では、IDM へのログイン方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.1-16）
- 前提条件（P.1-16）
- サポートされるユーザのロール（P.1-16）
- IDM へのログイン（P.1-16）
- IDM と Cookie（P.1-17）
- IDM と証明書（P.1-18）

概要

同時 CLI セッションの数は、プラットフォームに応じて制限されています。IDS-4210、IDS-4215、および NM-CIDS の同時 CLI セッションの数は、3 つに制限されています。その他のプラットフォームは 10 の同時セッションを許容します。

前提条件

IDM は、バージョン 5.0 センサーの一部です。**setup** コマンドを使用してセンサーを初期化し、IDM と通信できるようにする必要があります。手順については、P.1-6 の「センサーの初期化」を参照してください。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

IDM へのログイン

IDM へログインするには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力します。

https://*sensor_ip_address*

（注）　IDM はセンサーにインストール済みです。

（注）　デフォルト アドレスは `https://10.1.9.201` です。センサーを初期化するときに、ネットワーク環境を反映するように変更します。Web サーバ ポートを変更した場合は、IDM への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。指定する形式は `https://sensor_ip_address:port`（たとえば、`https://10.1.9.201:1040`）です。

Security Alert ダイアログボックスが表示されます。セキュリティと IDM の詳細については、P.1-18 の「IDM と証明書」を参照してください。

ステップ 2　Enter Network Password ダイアログボックスにユーザ名とパスワードを入力し、**OK** をクリックします。

(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。センサーの初期化のときに、パスワードを変更するプロンプトが表示されます。手順については、P.1-6 の「センサーの初期化」を参照してください。

Cisco IDM 5.0 Information ウィンドウが開き、IDM をロードしていることが示されます。別のブラウザ ウィンドウに IDM が表示されます。

Memory Warning ダイアログボックスに次のメッセージが表示されます。

```
Your current Java memory heap size is less than 256 MB. You must increase the Java
memory heap size before launching IDM. Click Help for information on changing the Java
memory heap size.
```

ステップ 3　**Help** をクリックし、Java メモリのヒープ サイズを変更する手順を確認します。

ステップ 4　Java メモリのヒープ サイズを変更する手順を実行します。

ステップ 5　開いているブラウザ ウィンドウをすべて閉じます。

ステップ 6　ブラウザ ウィンドウを開いてセンサーの IP アドレスを入力し、IDM を再起動します。

ステップ 7　Password Needed - Networking ダイアログボックスにユーザ名とパスワードを入力し、**Yes** をクリックします。

Warning ダイアログボックスに次のメッセージが表示されます。

```
There is no license key installed on the sensor. To install a new license, go to
Configuration > Licensing.
```

センサーのライセンスを入手する手順については、P.1-23 の「センサーのライセンスの入手」を参照してください。

Status ダイアログボックスに次のメッセージが表示されます。

```
Please wait while the IDM is loading the current configuration from the Sensor.
```

IDM のメイン ウィンドウが表示されます。

IDM と Cookie

IDM は Cookie を使用してセッションを追跡し、一貫性のあるビューを提供します。IDM はセッション Cookie（一時的）のみを使用し、保管された Cookie は使用しません。Cookie がローカルに保管されることはないため、ブラウザの Cookie ポリシーに反することはありません。Cookie はブラウザではなく、IDM Java アプレットによって処理されます。

IDM と証明書

この項では、IDM において証明書がどのように機能するかについて説明します。取り上げる事項は次のとおりです。

- 証明書について（P.1-18）
- Internet Explorer での CA の検証（P.1-19）
- Netscape での CA の検証（P.1-21）
- Mozilla の CA の検証（P.1-22）

証明書について

IPS 5.1 には、IDM を実行し、VMS などの管理ステーションの接続先である Web サーバが含まれています。ブロッキング転送センサーは、マスター ブロッキング センサーの Web サーバにも接続します。セキュリティを提供するため、この Web サーバは TLS として知られる暗号化プロトコルを使用します。TLS は SSL プロトコルに密接に関連しています。Web ブラウザに `https://`*ip_address* から始まる URL を入力すると、Web ブラウザは TLS または SSL プロトコルを使用して応答し、暗号化セッションをホストとネゴシエートします。

注意　Web ブラウザは、IDM が提示する証明書を最初に拒否します。これは、認証局（CA）を信頼しないためです。

（注）　IDM は、デフォルトで TLS および SSL を使用できるようになっています。TLS および SSL を使用することを強く推奨します。

TLS での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間で多数の協調的な交換が発生するため、「ハンドシェイク」と呼ばれます。サーバはクライアントに証明書を送信します。クライアントは、この証明書に対して、次の 3 つの部分で構成されるテストを実行します。

1. 証明書で識別される発行元は信頼できるか。

   Web ブラウザは、信頼されたサードパーティ CA のリストと共に出荷されます。証明書で識別された発行元が、ブラウザが信頼する CA のリストに含まれている場合、最初のテストに合格します。

2. 日付は、証明書が有効だと見なされる日付範囲内か。

   証明書には、日付のペアで構成される Validity フィールドがあります。日付がこの日付範囲内の場合、2 番目のテストに合格します。

3. 証明書で識別され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。一致した場合、3 番目のテストに合格します。

IDM に接続するように Web ブラウザに指示すると、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）、ブラウザが信頼する CA のリストにセンサーが含まれていないため、返される証明書は失敗します。

ブラウザのエラー メッセージが表示されたときに、3 つのオプションがあります。

- サイトから即座に接続解除する。
- 残りの Web ブラウザ セッション用に証明書を受け入れる。
- 証明書で識別される発行元を 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。

最も便利なオプションは、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、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査します。これによって、センサーを詐称した攻撃者から被害を受けることを防ぎます。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ことを確認します。

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、次にセンサーを再度ブートしたときに、新しい証明書が生成されます。次に Web ブラウザが IDM に接続するときに、手動上書きダイアログボックスが表示されます。Internet Explorer、Netscape および Mozilla 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。

Internet Explorer での CA の検証

Internet Explorer を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

```
https://sensor_ ip_address
```

Security Alert パネルが表示されます。

ステップ 2　**View Certificate** をクリックします。

Certificate Information パネルが表示されます。

ステップ 3　**Details** タブをクリックします。

ステップ 4　リストを下にスクロールして **Thumbprint** を検索し、選択します。

テキスト フィールドにサムプリントが表示されます。

(注)　Certificate パネルは開いたままにします。

ステップ 5　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 6　TLS フィンガープリントを表示します。

```
sensor# 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 7　SHA1 フィンガープリントと、開いている証明書のサムプリント テキスト フィールドに表示されている値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 8　**General** タブをクリックします。

ステップ 9　**Install Certificate** をクリックします。

Certificate Import Wizard が表示されます。

ステップ 10　**Next** をクリックします。

Certificate Store ダイアログボックスが表示されます。

ステップ 11　**Place all certificates in the following store** を選択して、**Browse** をクリックします。

Select Certificate Store ダイアログボックスが表示されます。

ステップ 12　**Trusted Root Certification Authorities** をクリックして、**OK** をクリックします。

ステップ 13　**Next** をクリックして、**Finish** をクリックします。

Security Warning ダイアログボックスが表示されます。

ステップ 14　**Yes** をクリックして、**OK** をクリックします。

ステップ 15　**OK** をクリックして、Certificate ダイアログボックスを閉じます。

ステップ 16　**Yes** をクリックして IDM を開きます。

Netscape での CA の検証

Netscape を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

```
https://sensor_ip_address
```

New Site Certificate パネルが表示されます。

ステップ 2　**Next** をクリックし、**More Info** をクリックします。

View A Certificate パネルが表示されます。

ステップ 3　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 4　TLS フィンガープリントを表示します。

```
sensor# 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 5　MD5 フィンガープリントと View A Certificate パネルに表示された値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 6　**OK** をクリックして、View A Certificate パネルを閉じます。

ステップ 7　**Next** をクリックし、**Accept this certificate forever (until it expires)** オプション ボタンをクリックします。

ステップ 8　**Next** を 2 回クリックして、**Finish** をクリックします。

Mozilla の CA の検証

Mozilla を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

```
https://sensor_ip_address
```

Website Certified by an Unknown Authority パネルが表示されます。

ステップ 2　**Examine Certificate** をクリックします。

Certificate Viewer パネルが表示されます。

ステップ 3　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 4　TLS フィンガープリントを表示します。

```
sensor# 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 5　MD5 フィンガープリントと Certificate Viewer General タブに表示された値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 6　**Close** をクリックして、Certificate Viewer パネルを閉じます。

ステップ 7　**Accept this certificate permanently** を選択し、**OK** をクリックしてパネルを閉じます。

ログイン ダイアログボックスが表示されます。

ステップ 8　**Prompt** ダイアログボックスにユーザ名とパスワードを入力します。

ステップ 9　**Yes** をクリックして証明書を受け入れます。

センサーのライセンスの入手

この項では、センサーのライセンスの入手方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.1-23）
- IPS 製品のサービス プログラム（P.1-24）
- サポートされるユーザのロール（P.1-25）
- フィールド定義（P.1-25）
- ライセンス キーの取得とインストール（P.1-26）

概要

センサーはライセンス キーがなくても動作しますが、シグニチャ アップデートを取得するには、ライセンス キーが必要です。ライセンス キーを入手するには、IPS に関するシスコのサービス契約が必要です。契約を購入するには、代理店、シスコのサービス担当者または営業担当者にお問い合せください。詳細については、P.1-24 の「IPS 製品のサービス プログラム」を参照してください。

トライアル ライセンス キーも使用可能です。契約内容が不明なためにセンサーのライセンスを入手できない場合は、ライセンスが必要なシグニチャ アップデートをサポートしている 60 日のトライアル ライセンスを入手してください。

Cisco.com のライセンシング サーバから取得したライセンス キーは、センサーに送信されます。または、ローカル ファイルに含まれているセンサー ライセンス キーからセンサーのライセンス キーをアップデートすることもできます。ライセンス キーを申し込むには、http://www.cisco.com/go/license にアクセスして、**IPS Signature Subscription Service** をクリックします。手順については、P.1-26 の「ライセンス キーの取得とインストール」を参照してください。

ライセンス キーの取得には、IPS デバイスのシリアル番号が必要です。IDM で IPS デバイスのシリアル番号を見つけるには、**Configuration** > **Licensing** をクリックするか、CLI で **show version** コマンドを実行します。

ライセンス キーのステータスは、IDM の Licensing パネルで確認できます。IDM を起動するたびに、ライセンスのステータスが表示されます。ライセンス キーのステータスは、trial、invalid、または expired のいずれかです。ライセンス キーがない場合や、無効な場合、または期限が切れている場合でも、IDM を継続して使用できますが、シグニチャ アップデートはダウンロードできません。

CLI に入ると、ライセンス ステータスが通知されます。たとえば、ライセンスがインストールされていない場合は、次のメッセージが表示されます。

```
***LICENSE NOTICE***
There is no license key installed on the system.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```

このメッセージは、ライセンス キーをインストールするまで毎回表示されます。

IPS 製品のサービス 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 アップデートを入手したりするには、IPS 製品の Cisco Services for IPS サービス契約を購入している必要があります。シスコシステムズと直接のお付き合いがある場合は、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てください。シスコシステムズと直接のお付き合いがない場合は、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。

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

ASA 製品の場合、IPS を含まない次の ASA 製品のいずれかを購入したときは、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ハードウェア交換（NBD）を提供します。

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

AIP SSM がインストールされた状態で出荷される次の ASA 製品のいずれかを購入した場合、または AIP SSM を購入してご使用の ASA 製品に追加した場合は、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 シグニチャのアップデート、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ハードウェア交換（NBD）を提供します。

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

たとえば、ASA-5510 を購入した後で IPS および購入済み ASA-SSM-AIP-10-K9 を追加する場合は、Cisco Services for IPS サービス契約を購入する必要があります。

Cisco Services for IPS サービス契約を購入したら、製品シリアル番号を入力してライセンス キーを申し込む必要があります。手順については、P.1-26 の「ライセンス キーの取得とインストール」を参照してください。

注意　お使いの製品に対して RMA を実行した場合、シリアル番号は変更されます。次に、新規シリアル番号用の新規ライセンス キーを取得する必要があります。

サポートされるユーザのロール

Licensing パネルにライセンス情報を表示したり、センサーのライセンス キーをインストールしたりするには、管理者である必要があります。

フィールド定義

Licensing パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Current License**：現在のライセンスのステータスが表示されます。
  - **License Status**：センサーの現在のライセンスのステータスです。
  - **Expiration Date**：ライセンス キーの有効期限が切れる（または切れた）日付。
    ライセンス キーが無効な場合、日付は表示されません。
  - **Serial Number**：センサーのシリアル番号です。
- **Update License**：新しいライセンス キーの取得先を指定します。
  - **Cisco Connection Online**：ライセンス キーを取得するために、Cisco.com のライセンス サーバに接続します。
  - **License File**：ライセンス ファイルを使用するように指定します。
  - **Local File Path**：ライセンス キーが含まれているローカル ファイルを示します。

ボタンの機能：

- **Download**：IDM を実行しているコンピュータにライセンスのコピーをダウンロードし、ローカル ファイルに保存します。その後、紛失または破損したライセンスと置き換えたり、センサーのイメージの再作成後に再インストールしたりできます。
  センサー上に有効なライセンスがない場合、**Download** ボタンはディセーブルになっています。
- **Browse Local**：ライセンス キーを探すためのファイル ブラウザを起動します。
- **Update License**：選択したオプションに基づいて、新しいライセンス キーをセンサーに送信します。

ライセンス キーの取得とインストール

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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Licensing** をクリックします。

Licensing パネルに現在のライセンスのステータスが表示されます。ライセンスがインストール済みの場合、必要に応じて **Download** をクリックして保存します。

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 からライセンスを取得するには、**Cisco Connection Online** を選択します。

  IDM は、Cisco.com のライセンス サーバに接続し、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法です。ステップ 4 に進みます。
- ライセンス ファイルを使用するには、**License File** を選択します。

  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 キーを申し込む必要があります。

  ライセンス キーは、電子メールで送られてきます。送られてきたライセンス キーは、IDM がアクセスできるドライブに保存してください。コンピュータが Cisco.com にアクセスできない場合に、このオプションが役立ちます。ステップ 7 に進みます。

ステップ 4　**Update License** をクリックします。

Licensing ダイアログボックスが表示されます。

ステップ 5　**Yes** をクリックして続行します。

Status ダイアログボックスに、センサーが Cisco.com に接続中であることが示されます。Information ダイアログボックスで、ライセンス キーが更新されたことを確認できます。

ステップ 6　**OK** をクリックします。

ステップ 7　www.cisco.com/go/license にアクセスします。

ステップ 8　必須フィールドに入力します。

注意　IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

ライセンス キーは指定した電子メール アドレスに送られます。

ステップ 9　ライセンス キーは、IDM を動作中のクライアントがアクセス可能なハードディスク ドライブまたはネットワーク ドライブに保存します。

ステップ 10　IDM にログインします。

ステップ 11 **Configuration** > **Licensing** をクリックします。

ステップ 12 Update License で、**Update From: License File** を選択します。

ステップ 13 **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、または **Browse Local** をクリックしてライセンス ファイルを参照します。

Select License File Path ダイアログボックスが表示されます。

ステップ 14 ライセンス ファイルを参照して、**Open** をクリックします。

ステップ 15 **Update License** をクリックします。

センサーのセットアップ

この章では、センサーのセットアップについて説明します。

センサーをネットワークに設置した後、**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。**setup** コマンドを使用すると、ホスト名、IP インターフェイス、Telnet サーバ、Web サーバ ポート、アクセス コントロール リスト、時間設定、およびインターフェイスの割り当てと有効化など、センサーの基本的な設定を行います。センサーを初期化すると、ネットワーク経由でセンサーと通信できるようになります。その後、侵入防御を設定できます。

注意

Configuration >Sensor Setup in IDM を使用してセンサーをセットアップする前に、センサーを初期化する必要があります。手順については、P.1-6 の「センサーの初期化」を参照してください。

センサーを初期化したら、**Sensor Setup** でその他のネットワーク パラメータの変更と設定ができます。

この章は、次の項で構成されています。

- ネットワーク設定の構成（P.2-2）
- 許可されたホストの設定（P.2-5）
- SSH の設定（P.2-8）
- 証明書の設定（P.2-17）
- 時刻の設定（P.2-21）
- ユーザの設定（P.2-28）

ネットワーク設定の構成

この項では、ネットワークの設定を変更する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.2-2）
- サポートされるユーザのロール（P.2-2）
- フィールド定義（P.2-2）
- ネットワーク設定の構成（P.2-3）

概要

Network パネルを使用して、センサーのネットワーク パラメータと通信パラメータを指定します。

（注）

setup コマンドを使用してセンサーを初期化すると、ネットワーク パラメータと通信パラメータの値が Network パネルに表示されます。これらのパラメータを変更する必要がある場合は、Network パネルで変更できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ネットワーク設定を構成するには、管理者である必要があります。

フィールド定義

Network パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Hostname**：センサーの名前。

  ホスト名は 1 ～ 64 文字の文字列で、^[A-Za-z0-9_/-]+$ に一致するパターンです。デフォルトは sensor です。ホスト名にスペースが含まれているか、または英数字が 64 文字を超えていると、エラー メッセージが表示されます。
- **IP Address**：センサーの IP アドレス。

  デフォルトは 10.1.9.201 です。
- **Network Mask**：IP アドレスに対応するマスク。

  デフォルトは 255.255.255.0 です。
- **Default Route**：デフォルトのゲートウェイ アドレス。

  デフォルトは 10.1.9.1 です。
- **FTP Timeout**：センサーと FTP サーバの通信中にタイムアウトになるまで FTP クライアントが待機する時間（秒単位）を設定します。

  有効な範囲は 1 ～ 86400 秒です。デフォルトは 300 秒です。
- **Web Server Settings**：Web サーバのセキュリティ レベルとポートを設定します。

  ー　**Enable TLS/SSL**：Web サーバの TLS と SSL をイネーブルにします。

デフォルトはイネーブルです。TLS と SSL をイネーブルにすることを強くお勧めします。

— **Web server port**：Web サーバが使用する TCP ポート。

デフォルトは 443（HTTPS の場合）です。1 ～ 65535 以外の値を入力すると、エラー メッセージが表示されます。

- **Remote Access**：センサーのリモート アクセスをイネーブルにします。
  - — **Enable Telnet**：Telnet によるセンサーへのリモート アクセスをイネーブルまたはディセーブルにします。

（注） Telnet は安全なアクセス サービスではないので、デフォルトでは使用不可です。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

ネットワーク設定の構成

ネットワーク設定を構成するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > Network** の順にクリックします。

Network パネルが表示されます。

ステップ 3　センサーのホスト名を編集するには、**Hostname** フィールドに新しい名前を入力します。

ステップ 4　センサーの IP アドレスを変更するには、**IP Address** フィールドに新しいアドレスを入力します。

ステップ 5　ネットワーク マスクを変更するには、**Network Mask** フィールドに新しいマスクを入力します。

ステップ 6　デフォルトのゲートウェイを変更するには、**Default Route** フィールドに新しいアドレスを入力します。

ステップ 7　FTP タイムアウトの時間を変更するには、**FTP Timeout** フィールドに新しい時間を入力します。

ステップ 8　TLS/SSL をイネーブルまたはディセーブルにするには、**Enable TLS/SSL** を選択または選択解除します。

（注） TLS/SSL を使用可能にすることを強くお勧めします。

（注） TLS と SSL は、Web ブラウザと Web サーバ間の暗号化通信を可能にするプロトコルです。TLS/SSL をイネーブルにした場合、`https://`*sensor_ip_address* を使用して IDM に接続します。TLS/SSL をディセーブルにした場合、`http://`*sensor_ip_address*`:`*port_number* を使用して IDM に接続します。

ステップ 9 Web サーバのポートを変更するには、**Web Server Port** フィールドに新しいポート番号を入力します。

（注） Web サーバのポートを変更する場合、IDM に接続するときに、ブラウザの URL アドレスでポートを指定する必要があります。その場合、`https://`*sensor_ip_address:port_number*（`https://10.1.9.201:1040` など）の形式を使用します。

ステップ 10 リモート アクセスをイネーブルまたはディセーブルにするには、**Enable Telnet** を選択します。

（注） Telnet は安全なアクセス サービスではないので、デフォルトでは使用不可です。ただし、安全なサービスである SSH が常にセンサーで実行されています。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 11 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

（注） ネットワーク設定を変更すると、センサーへの接続が中断し、新しいアドレスでの再接続が必要になることがあります。

許可されたホストの設定

この項では、許可されたホストをシステムに追加する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.2-5）
- サポートされているユーザ ロール（P.2-5）
- フィールド定義（P.2-5）
- 許可されたホストの設定（P.2-6）

概要

Allowed Hosts パネルを使用して、センサーへのアクセスを許可されたホストまたはネットワークを指定します。

（注） **setup** コマンドを使用してセンサーを初期化すると、許可されたホストのパラメータ値が Allowed Hosts パネルに表示されます。これらのパラメータを変更する必要がある場合は、Allowed Hosts パネルで変更できます。

デフォルトでは、リストには何もエントリがないため、ホストを追加するまで許可されたホストはありません。

（注） 許可されたホストのリストに、ASDM、IDM、IDS MC などの管理ホスト、および IDS Security Monitor などのモニタリング ホストを追加する必要があります。追加しないと、センサーと通信できません。

注意 許可ホストを追加、編集、削除するときは、センサーのリモート管理に使用する IP アドレスを削除しないように注意してください。

サポートされているユーザ ロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

許可されたホストとネットワークを設定するには、管理者である必要があります。

フィールド定義

この項では、許可されたホストのフィールド定義を示します。取り上げる事項は次のとおりです。

- Allowed Hosts パネル（P.2-6）
- Add and Edit Allowed Host ダイアログボックス（P.2-6）

Allowed Hosts パネル

Allowed Hosts パネルには、次のフィールドがあります。

フィールドの説明：

- **IP Address**：ホストがセンサーへのアクセスを許可する IP アドレス。
- **Network Mask**：ホストの IP アドレスに対応するマスク。

ボタンの機能：

- **Add**：Add Allowed Host ダイアログボックスを開きます。

  このダイアログボックスでは、許可されたホストのリストにホストまたはネットワークを追加できます。
- **Edit**：Edit Allowed Host ダイアログボックスを開きます。

  このダイアログボックスでは、このホストまたはネットワークに関連付けられた値を変更できます。
- **Delete**：許可されたホストのリストからホストまたはネットワークを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Allowed Host ダイアログボックス

Add and Edit Allowed Host ダイアログボックスには、次のフィールドがあります。

フィールドの説明：

- **IP Address**：ホストがセンサーへのアクセスを許可する IP アドレス。
- **Network Mask**：ホストの IP アドレスに対応するマスク。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

許可されたホストの設定

センサーへのアクセスが許可されたホストとネットワークを指定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > Allowed Hosts** の順にクリックします。

Allowed Hosts パネルが表示されます。

ステップ 3　**Add** をクリックして、ホストまたはネットワークをリストに追加します。

Add Allowed Hosts ダイアログボックスが表示されます。

許可されたホストは最大 512 台追加できます。

ステップ 4　**IP Address** フィールドにホストまたはネットワークの IP アドレスを入力します。

入力した IP アドレスが既存のリストのエントリに含まれている場合、エラー メッセージが表示されます。

ステップ 5　ホストまたはネットワークのネットワーク マスクを **Network Mask** フィールドに入力するか、またはドロップダウン リストからネットワーク マスクを選択します。

IDM では、IP アドレスがホストであるかネットワークであるかに関係なく、必ずネットマスクを指定する必要があります。ネットマスクを指定しないと、`Network Mask is not valid` というエラーが表示されます。

また、ネットワーク マスクが IP アドレスと一致しない場合も、エラー メッセージが表示されます。

ステップ 6　**OK** をクリックします。

新しいホストまたはネットワークが、Allowed Hosts パネルにある許可されたホストのリストに表示されます。

ステップ 7　許可されたホストのリストにある既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Allowed Host ダイアログボックスが表示されます。

ステップ 8　**IP Address** フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 9　**Network Mask** フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ステップ 10　**OK** をクリックします。

編集されたホストまたはネットワークが、Allowed Hosts パネルの許可されたホストのリストに表示されます。

ステップ 11　リストからホストまたはネットワークを削除するには、ホストまたはネットワークを選択して **Delete** をクリックします。

削除されたホストは、Allowed Hosts パネルの許可されたホストのリストに表示されなくなります。

注意　ホストを削除すると、それ以降のホストからのネットワーク接続は、すべて拒否されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 12　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

SSH の設定

SSH は強力な認証を提供し、安全ではないチャネル上の通信を安全なものにします。

SSH は、センサーへの接続を暗号化し、正しいセンサーに接続中であることを検証できるように鍵を提供します。また、SSH は、ブロッキング目的で、センサーが接続しているその他のデバイスに対しても認証済みで暗号化されたアクセスを提供します。

SSH は、次のいずれか 1 つまたは複数を使用して、ホストまたはネットワークを認証します。

- Password
- ユーザ RSA 公開鍵

SSH は次のものからネットワークを保護します。

- IP スプーフィング：リモート ホストは、別の信頼できるホストから送信されたかのように偽装してパケットを送信します。

  SSH は、外部へのルータであるかのように偽装する可能性のあるローカル ネットワーク上のスプーファーを阻止します。
- IP ソース ルーティング：ホストは別の信頼できるホストから送信されたかのように 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。
- 中間ホストによるクリア テキスト パスワードとその他のデータの傍受
- 中間ホストを支配する攻撃者によるデータの操作
- X 認証データの傍受と X11 サーバへの偽装接続に基づく攻撃

（注）　SSH はパスワードをクリア テキストで送信することは決してありません。

この項で取り上げる事項は次のとおりです。

- 許可鍵の定義（P.2-8）
- 既知のホスト鍵の定義（P.2-12）
- サーバ証明書の表示と生成（P.2-19）

許可鍵の定義

この項では、公開鍵の定義方法について説明します。取り上げる事項は次のとおりですます。

- 概要（P.2-8）
- サポートされるユーザのロール（P.2-9）
- フィールド定義（P.2-9）
- 許可鍵の定義（P.2-8）

概要

Authorized Keys パネルを使用して、RSA 認証によってローカル SSH サーバへのログインが許可されるクライアントの公開鍵を定義できます。Authorized Keys パネルには、センサーへのアクセスが許可されたすべての SSH クライアントの公開鍵が表示されます。

センサーにログインできる各ユーザは、そのユーザがログインする各クライアントから収集した許可鍵のリストを持ちます。SSH を使用してセンサーにログインするときは、パスワードを使用する代わりに RSA 認証を使用できます。

秘密鍵を保存するクライアントで RSA 鍵生成ツールを使用します。次に、生成された公開鍵を 3 つの数字のセット（Key Modulus Length、Public Exponent、Public Modulus）として表示し、これらの数字を Authorized Keys パネルの該当するフィールドに入力します。

表示できるのは自分の鍵だけで、他のユーザの鍵は表示できません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

許可鍵を追加したり編集したりするには、管理者である必要があります。オペレータ特権またはビューア特権で許可鍵の追加または編集を試みると、`Delivery Failed` メッセージが表示されます。

フィールド定義

この項では、許可鍵のフィールド定義を示します。取り上げる事項は次のとおりです。

- Authorized Keys パネル（P.2-9）
- Add and Edit Authorized Key ダイアログボックス（P.2-10）

Authorized Keys パネル

Authorized Keys パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **ID**：鍵を識別する一意の文字列（1 ～ 256 文字）。

  ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。

  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。

  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。

  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Add**：Add Authorized Key ダイアログボックスを開きます。

  このダイアログボックスでは、新しい許可鍵を追加できます。
- **Edit**：Edit Authorized Key ダイアログボックスを開きます。

  このダイアログボックスでは、この許可鍵に関連付けられた値を変更できます。
- **Delete**：リストから許可鍵を削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Authorized Key ダイアログボックス

Add and Edit Authorized Key ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **ID**：鍵を識別する一意の文字列（1 ～ 256 文字）。

  ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。

  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。

  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。

  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

許可鍵の定義

公開鍵を定義するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > SSH > Authorized Keys** の順にクリックします。

Authorized Keys パネルが表示されます。

ステップ 3　**Add** をクリックして、公開鍵をリストに追加します。

Add Authorized Key ダイアログボックスが表示されます。

最大 50 個の SSH 許可鍵を追加できます。

ステップ 4　**ID** フィールドに、許可鍵を識別するための一意の ID を入力します。

ステップ 5　**Modulus Length** フィールドに整数を入力します。

係数の長さは、係数の有意ビットの数です。RSA 鍵の強度は、係数のサイズに依存します。係数のビット数が多いほど、鍵は強力になります。

（注）　係数の長さ、公開指数、および公開係数が不明の場合は、秘密鍵を常駐させるクライアント上で RSA 鍵生成ツールを使用します。生成された公開鍵を 3 つの数字セット（係数の長さ、公開指数、および公開係数）として表示し、ステップ 5 ～ 7 でこれらの数字を入力します。

ステップ 6　**Public Exponent** フィールドに整数を入力します。

RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。公開指数の有効値は、3 ～ 2147483647 です。

ステップ 7　**Public Modulus** フィールドに値を入力します。

公開係数は文字列値です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。

RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 8　**OK** をクリックします。

Authorized Keys パネルの許可鍵リストに、新しい鍵が表示されます。

ステップ 9　許可鍵リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Authorized Key ダイアログボックスが表示されます。

ステップ 10　**Modulus Length**、**Public Exponent**、および **Public Modulus** フィールドを編集します。

注意　エントリを作成した後は、**ID** フィールドは変更できません。

ステップ 11　**OK** をクリックします。

Authorized Keys パネルの許可鍵リストに、編集された鍵が表示されます。

ステップ 12　公開鍵をリストから削除するには、それを選択して **Delete** をクリックします。

削除された鍵は、Authorized Keys パネルの許可鍵リストに表示されなくなります。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 13　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

既知のホスト鍵の定義

この項では、既知のホスト鍵を定義する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.2-12）
- サポートされるユーザのロール（P.2-12）
- フィールド定義（P.2-12）
- 既知のホスト鍵の定義（P.2-13）

概要

Known Host Keys パネルを使用して、センサーが管理するブロッキング デバイスの公開鍵と、アップダートのダウンロードまたはファイルのコピーに使用される SSH（SCP）サーバの公開鍵を定義します。Known Host Keys パネルの設定に必要な情報を取得するために、各デバイスとサーバから公開鍵の報告を受ける必要があります。公開鍵を正しい形式で取得できない場合は、Add Known Host Keys ダイアログボックスの **Retrieve Host Key** をクリックします。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

既知のホスト鍵を追加したり編集したりするには、管理者である必要があります。

フィールド定義

この項では、既知のホスト鍵のフィールド定義を示します。取り上げる事項は次のとおりです。

- Known Host Keys パネル（P.2-12）
- Add and Edit Known Host Key ダイアログボックス（P.2-13）

Known Host Keys パネル

Known Host Keys パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：鍵を追加するホストの IP アドレス。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。
  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。
  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。
  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Add**：Add Known Host Key ダイアログボックスを開きます。
  このダイアログボックスで、新しい既知のホスト鍵を追加できます。
- **Edit**：Edit Known Host Key ダイアログボックスを開きます。
  このダイアログボックスで、この既知のホスト鍵に関連付けられた値を変更できます。
- **Delete**：リストから既知のホスト鍵を削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Known Host Key ダイアログボックス

Add and Edit Known Host Key ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：鍵を追加するホストの IP アドレス。
- **Modulus Length**：係数の有意ビットの数（511 ～ 2048）。
  長さが範囲外の場合は、エラー メッセージが表示されます。
- **Public Exponent**：RSA アルゴリズムがデータを暗号化するために使用します。
  有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- **Public Modulus**：RSA アルゴリズムがデータを暗号化するために使用します。
  公開係数は 1 ～ 2048 文字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外の場合は、エラー メッセージが表示されます。

ボタンの機能：

- **Retrieve Host Key**：IDM は、IP アドレスで指定されたホストから既知のホスト鍵を取得しようとします。取得に成功した場合、IDM は取得したホスト鍵を Add Known Host Key パネルに入力します。
  Add ダイアログボックスでのみ使用できます。IP アドレスが無効な場合、エラー メッセージが表示されます。
- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

既知のホスト鍵の定義

既知のホスト鍵を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > SSH > Known Host Keys** の順にクリックします。

Known Host Keys パネルが表示されます。

ステップ 3　**Add** をクリックして、既知のホスト鍵をリストに追加します。

Add Known Host Key ダイアログボックスが表示されます。

ステップ 4　**IP Address** フィールドに、鍵を追加するホストの IP アドレスを入力します。

ステップ 5　**Retrieve Host Key** をクリックします。

Device Manager は、ステップ 3 で入力した IP アドレスのホストから鍵を取得しようとします。取得が成功した場合、ステップ 8 に進みます。取得が失敗した場合、ステップ 5 ～ 7 を実行してください。

注意　取得した鍵が指定されたアドレスに適していることを確認し、サーバの IP アドレスがスプーフィングされてないことを確認します。

ステップ 6　**Modulus Length** フィールドに整数を入力します。

係数の長さは、係数の有意ビットの数です。RSA 鍵の強度は、係数のサイズに依存します。係数のビット数が多いほど、鍵は強力になります。

ステップ 7　**Public Exponent** フィールドに整数を入力します。

RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。

ステップ 8　**Public Modulus** フィールドに値を入力します。

公開係数は文字列値です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。

RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 9　**OK** をクリックします。

Known Host Keys パネルの既知のホスト鍵リストに、新しい鍵が表示されます。

ステップ 10　許可鍵リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Authorized Key ダイアログボックスが表示されます。

ステップ 11　**Modulus Length**、**Public Exponent**、および **Public Modulus** フィールドを編集します。

注意　エントリを作成した後は、**ID** フィールドは変更できません。

ステップ 12　**OK** をクリックします。

Known Host Keys パネルの既知のホスト鍵リストに、編集された鍵が表示されます。

ステップ 13　公開鍵をリストから削除するには、それを選択して **Delete** をクリックします。

削除された鍵は、Known Host Keys パネルの既知のホスト鍵リストに表示されなくなります。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 14　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

センサー SSH ホスト鍵の表示と生成

この項では、センサー SSH ホスト鍵を表示および生成する方法を説明します。取り上げる事項は次のとおりです。

- 概要（P.2-15）
- サポートされるユーザのロール（P.2-15）
- フィールド定義（P.2-15）
- センサー SSH ホスト鍵の表示と生成（P.2-15）

概要

サーバは SSH ホスト鍵を使用して、ID を証明します。クライアントは、既知の鍵を見つけると、正しいサーバに接続したことを認識します。

センサーでは、最初に起動したときに SSH ホスト鍵が生成されます。この SSH ホスト鍵は Sensor Key パネルに表示されます。**Generate Key** をクリックして、この鍵を新しい鍵に置換します。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー SSH ホスト鍵を生成するには、管理者である必要があります。

フィールド定義

Sensor Key パネルにセンサー SSH ホスト鍵が表示されます。**Generate Key** ボタンによって新しいセンサー SSH ホスト鍵が生成されます。

センサー SSH ホスト鍵の表示と生成

センサー SSH ホスト鍵の表示と生成を行うには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Sensor Setup** > **SSH** > **Sensor Key** の順にクリックします。

Sensor Key パネルが表示されます。

センサー SSH ホスト鍵が表示されます。

ステップ 3　新しいセンサー SSH ホスト鍵を生成するには、**Generate Key** をクリックします。

ダイアログボックスに次の警告が表示されます。

```
Generating a new SSH host key requires you to update the known hosts tables on remote
systems with the new key so that future connections succeed. Do you want to continue?
```

注意　新しい鍵で既存の鍵を置換するため、以後の接続が成功するようにリモート システムの既知のホスト テーブルを新しいホスト鍵で更新する必要があります。

ステップ 4　**OK** をクリックして続行します。

新しいホスト鍵が生成され、古いホスト鍵が削除されます。

ステータス メッセージに鍵の更新が成功したことが表示されます。

証明書の設定

センサーと証明書の詳細については、P.1-18 の「IDM と証明書」を参照してください。この項で取り上げる事項は次のとおりです。

- 信頼できるホストの追加（P.2-17）
- サーバ証明書の表示と生成（P.2-19）

信頼できるホストの追加

この項では、信頼できるホストを追加する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.2-17）
- サポートされるユーザのロール（P.2-17）
- フィールド定義（P.2-17）
- 信頼できるホストの追加（P.2-18）

概要

Trusted Hosts パネルを使用して、マスター ブロッキング センサーの証明書と、このセンサーがアップデートのダウンロードに使用する TLS サーバと SSL サーバの証明書を追加します。

Trusted Hosts パネルには、追加したすべての信頼できるホスト証明書のリストが表示されます。IP アドレスを入力することにより、証明書を追加できます。IDM は証明書を取得して、そのフィンガープリントを表示します。フィンガープリントを受け入れると、証明書が信頼されます。リストにエントリを追加したり、リストからエントリを削除したりできますが、エントリを編集することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

信頼できるホストを追加するには、管理者である必要があります。

フィールド定義

この項では、信頼できるホストのフィールド定義を示します。取り上げる事項は次のとおりです。

- Trusted Hosts パネル（P.2-17）
- Add Trusted Host ダイアログボックス（P.2-18）

Trusted Hosts パネル

Trusted Hosts パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：信頼できるホストの IP アドレス。
- **MD5**：Message Digest 5 暗号化。
  MD5 は、メッセージの 128 ビット ハッシュの計算に使用するアルゴリズムです。

- **SHA1**：Secure Hash Algorithm。
  SHA1 は、暗号メッセージ ダイジェスト アルゴリズムです。

ボタンの機能：

- **Add**：Add Trusted Host ダイアログボックスを開きます。
  このダイアログボックスでは、新しい信頼できるホストを追加できます。
- **View**：View Trusted Host ダイアログボックスを開きます。
  このダイアログボックスでは、信頼できるホストに関連付けられた証明書データを表示できます。
- **Delete**：リストから信頼できるホストを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add Trusted Host ダイアログボックス

Add Trusted Host ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：信頼できるホストの IP アドレス。
- **Port**：（オプション）ホスト証明書を取得するポート番号を指定します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

信頼できるホストの追加

信頼できるホストを追加するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Sensor Setup** > **Certificate** > **Trusted Hosts** の順にクリックします。

Trusted Hosts パネルが表示されます。

ステップ 3　**Add** をクリックして、信頼できるホストをリストに追加します。

Add Trusted Host ダイアログボックスが表示されます。

ステップ 4　**IP Address** フィールドに、追加する信頼できるホストの IP アドレスを入力します。

ステップ 5　センサーが 443 以外のポートを使用している場合は、**Port** フィールドにポート番号を入力します。

ステップ 6　**OK** をクリックします。

IDM は、ステップ 3 で入力した IP アドレスのホストから証明書を取得します。この新しい信頼できるホストは、Trusted Hosts パネルの信頼できるホストのリストに表示されます。

IDM がセンサーと通信中であることが、ダイアログボックスに示されます。

```
Communicating with the sensor, please wait ...
```

信頼できるホストの追加が成功したかどうかのステータスが、ダイアログボックスに示されます。

```
The new host was added successfully.
```

ステップ 7　表示される値と、直接端末接続またはコンソールなどで安全に取得した値を比較して、フィンガープリントが正しいことを検証します。ステップ 7 を参照してください。両方の値が一致しない場合、その信頼できるホストをすぐに削除してください。ステップ 8 を参照してください。

ステップ 8　信頼できるホストのリストにある既存のエントリを表示するには、それを選択して **View** をクリックします。

View Trusted Host ダイアログボックスが表示されます。証明書データが表示されます。このダイアログボックスで表示されるデータは、読み取り専用です。

ステップ 9　**OK** をクリックします。

ステップ 10　信頼できるホストをリストから削除するには、それを選択して **Delete** をクリックします。

削除された信頼できるホストは、Trusted Hosts パネルの信頼できるホストのリストに表示されなくなります。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 11　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

サーバ証明書の表示と生成

この項では、サーバ証明書を表示および生成する方法を説明します。取り上げる事項は次のとおりです。

- 概要（P.2-19）
- サポートされるユーザのロール（P.2-20）
- フィールド定義（P.2-20）
- サーバ証明書の表示と生成（P.2-20）

概要

Server Certificate パネルに、センサー サーバ X.509 の証明書が表示されます。このパネルで、新しいサーバの自己署名付き X.509 証明書を生成できます。証明書は、センサーを最初に起動したときに生成されます。**Generate Certificate** をクリックして、新しいホスト証明書を生成します。

注意　センサーの IP アドレスが証明書に含まれます。センサーの IP アドレスを変更した場合は、新しい証明書を生成する必要があります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

サーバ証明書を生成するには、管理者である必要があります。

フィールド定義

Server Certificate パネルに、センサー サーバ X.509 の証明書が表示されます。**Generate Certificate** をクリックすると、新しいセンサー X.509 証明書が生成されます。

サーバ証明書の表示と生成

センサー サーバ X.509 証明書の表示と生成を行うには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > Certificate > Server Certificate** の順にクリックします。

Server Certificate パネルが表示されます。

センサー サーバ X.509 証明書が表示されます。

ステップ 3　新しいセンサー サーバ X.509 証明書を生成するには、**Generate Certificate** をクリックします。

ダイアログボックスに次の警告が表示されます。

```
Generating a new server certificate requires you to verify the new fingerprint the
next time you connect or when you add the sensor as a trusted host. Do you want to
continue?
```

注意　新しいフィンガープリントを書き込みます。後で接続したとき、またはセンサーを信頼できるホストとして追加するときに、Web ブラウザに表示されるフィンガープリントを確認する必要があります。センサーがマスター ブロッキング センサーの場合は、マスター ブロッキング センサーにブロックを送信するリモート センサーの、信頼できるホスト テーブルを更新する必要があります。

ステップ 4　**OK** をクリックして続行します。

新しいサーバ証明書が生成され、古いサーバ証明書が削除されます。

時刻の設定

この項では、時刻源とセンサーについて説明します。取り上げる事項は次のとおりです。

- 概要（P.2-21）
- 時刻源およびセンサー（P.2-21）
- サポートされるユーザのロール（P.2-23）
- フィールド定義（P.2-23）
- センサー上の時刻の設定（P.2-25）
- センサー上の時刻の修正（P.2-27）

概要

Time パネルを使用して、日付、時刻、時間帯、サマータイム（DST）を設定し、センサーが時刻源に NTP サーバを使用するかどうかを設定します。

（注） センサーの時刻源として NTP サーバを使用する方法を推奨します。

時刻源およびセンサー

センサーには、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 Coordinated Universal Time（UTC; 世界標準時）と現地時間のタイムスタンプが必要です。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に、時間帯とサマータイム設定をセットアップします。詳細については、P.1-6 の「センサーの初期化」を参照してください。

センサーに時刻を設定する方法を要約して示します。

- アプライアンスの場合
  - **clock set** コマンドを使用して、時刻を設定する。これがデフォルトの方法です。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Manually Setting the System Clock」を参照してください。
  - NTP を使用する。

    アプライアンスは、NTP 同期時刻源から時刻を取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NTP をアプライアンスにセットアップすることも、CLI、IDM、または ASDM を通して NTP を設定することもできます。

    （注） NTP 同期時刻源を使用する方法を推奨します。

- IDSM-2 の場合
  - IDSM-2 は、自動的にその時計をスイッチ時刻と同期させることができる。これがデフォルトの方法です。

    （注） UTC 時刻は、スイッチと IDSM-2 の間で同期が取られます。時間帯とサマータイム設定は、スイッチと IDSM-2 間で同期が取られません。

注意 スイッチと IDSM-2 の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイム設定が IDSM-2 とスイッチとで一致していない場合、IDSM2 の現地時間は不正確になる可能性があります。

- NTP を使用する。

  IDSM-2 は、その時刻を NTP 同期時刻源から取得するように設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NTP を使用するように IDSM-2 を設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

  (注) NTP 同期時刻源を使用する方法を推奨します。

- NM-CIDS の場合
  - NM-CIDS は、自動的にその時計を取り付け先（親ルータ）のルータ シャーシの時計と同期させることができる。これがデフォルトの方法です。

    (注) UTC 時刻は、親ルータと NM-CIDS の間で同期が取られます。時間帯とサマータイム設定は、親ルータと NM-CIDS の間で同期が取られません。

注意 親ルータと NM-CIDS の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が NM-CIDS とルータとで一致していない場合、NM-CIDS の現地時間は不正確になる可能性があります。

- NTP を使用する。

  NM-CIDS は、その時刻を 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設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に NM-CIDS を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

  (注) NTP 同期時刻源を使用する方法を推奨します。

- AIP SSM の場合
  - AIP SSM は、自動的にその時計を取り付け先の ASA の時計と同期させることができる。これがデフォルトの方法です。

    (注) UTC 時刻は、ASA と AIP SSM の間で同期が取られます。時間帯とサマータイム設定は、ASA と AIP SSM の間で同期が取られません。

注意　ASA と AIP SSM の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを保証します。時間帯やサマータイムの設定が AIP SSM と ASA とで一致していない場合、AIP SSM の現地時間は不正確になる可能性があります。

— NTP を使用する。

AIP SSM は、その時刻を 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設定できます。『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring a Cisco Router to be an NTP Server」を参照してください。NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。初期化中に AIP SSM を NTP を使用するように設定することも、CLI、IDM、または ASDM を通して NTP をセットアップすることもできます。

（注）　NTP 同期時刻源を使用する方法を推奨します。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

時刻設定を設定するには、管理者である必要があります。

フィールド定義

この項では、時刻のフィールド定義を示します。取り上げる事項は次のとおりです。

- Time パネル（P.2-23）
- Configure Summertime ダイアログボックス（P.2-24）

Time パネル

Time パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Sensor Local Date**：センサー上の現在の日付。

  デフォルトは 1970 年 1 月 1 日です。日付の値が月の範囲外の場合、エラー メッセージが表示されます。

- **Sensor Local Time**：センサー上の現在の時刻（hh:mm:ss）。

  デフォルトは 00:00:00 です。時間、分、または秒が範囲外の場合はエラー メッセージが表示されます。

（注）　センサーが日付フィールドや時刻フィールドをサポートしていない場合、またはセンサー上で NTP 設定を設定していない場合、これらのフィールドはディセーブルになっています。

- **Standard Time Zone**：時間帯の名前と UTC オフセットを設定します。
  - **Zone Name**：サマータイムが実施されていない場合のローカル時間帯。

    デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24　文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
  - **UTC Offset**：ローカル時間帯のオフセット（分単位）。

    デフォルトは 0 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。
- **NTP Server**：センサーが時刻源として NTP サーバを使用するように設定します。
  - **IP Address**：NTP サーバを使用してセンサー上の時刻を設定する場合、NTP サーバの IP アドレス。
  - **Key**：NTP MD5 鍵タイプ。
  - **Key ID**：NTP サーバ上で認証に使用される鍵の ID（1 ～ 65535）。

    鍵 ID が範囲外の場合は、エラー メッセージが表示されます。
- **Summertime**：サマータイム設定をイネーブルにし、その設定をします。
  - **Enable Summertime**：ここをクリックすると、サマータイム モードがイネーブルになります。

    デフォルトはディセーブルです。

ボタンの機能：

- **Configure Summertime**：ここをクリックすると、Configure Summertime ダイアログボックスが開きます。

  Configure Summertime ダイアログボックスを開くことができるのは、**Enable Summertime** を選択した場合のみです。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。

  Time パネル上のその他の設定（NTP、サマータイム、標準時間帯の設定など）が変更された場合、**Apply** がイネーブルになります。**Apply** は、日付と時刻を除く、Time パネル上のすべてのフィールドに対応しています。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。
- **Apply Time to Sensor**：センサー上の日付と時刻を設定します。

  Apply Time to Sensor は日付と時刻を変更した場合にのみ、イネーブルになります。変更した日付と時刻をセンサーに保存する場合は、**Apply Time to Sensor** をクリックする必要があります。

Configure Summertime ダイアログボックス

Configure Summertime ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summer Zone Name**：サマータイム時間帯の名前。

  デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
- **Offset**：サマータイム中に付加する時間数。

  デフォルトは 60 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。
- **Start Time**：サマータイム開始時刻の設定。

  値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- **End Time**：サマータイム終了時刻の設定。

  値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。

- **Summertime Duration**：サマータイム期間が毎年実施されるか、1 回だけの日付かを設定します。
  - **Recurring**：サマータイム期間は recurring（毎年実施される）モードです。
  - **Date**：サマータイム期間は、nonrecurring（毎年実施されない）モードです。
  - **Start**：開始の週、日、月の設定。
  - **End**：終了の週、日、月の設定。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

センサー上の時刻の設定

センサー上の時刻を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > Time** の順にクリックします。

Time パネルが表示されます。

ステップ 3　**Date** で、ドロップダウン ボックスから現在の時刻を選択します。

日付は、ローカル ホストの日付を示しています。

ステップ 4　**Time** で、現在の時刻（hh:mm:ss）を入力します。

時間は、ローカル ホストの時間を示しています。現在の時刻を表示するには、**Refresh** をクリックします。

注意　間違えて誤った時刻を指定すると、ストアされたイベントに間違ったタイムスタンプが設定されます。この場合は、イベントをクリアする必要があります。詳細については、P.2-27 の「センサー上の時刻の修正」を参照してください。

（注）　NTP を設定済みの場合、モジュール上の日付や時刻は変更できません。

ステップ 5　Standard Time Zone で次を実行します。

a.　**Zone Name** フィールドのドロップダウン ボックスから時間帯を選択するか、または作成済みの時間帯を入力します。

これは、サマータイム時間が実施されていない場合に表示される時間帯です。

b.　**UTC Offset** フィールドに、UTC のオフセットを分単位で入力します。

事前に定義された時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 6　NTP 時刻同期を使用している場合は、**NTP Server** で次を入力します。

a. **IP Address** フィールドに NTP サーバの IP アドレスを入力する。

b. **Key** フィールドに NTP サーバの鍵を入力する。

c. **Key ID** フィールドに NTP サーバの鍵 ID を入力する。

（注） NTP サーバを定義すると、センサーの時刻は NTP サーバによって設定されます。CLI の **clock set** コマンドを実行するとエラーが発生しますが、時間帯とサマータイムのパラメータは有効です。

ステップ 7　サマータイムをイネーブルにするには、Summertime で **Enable Summertime** を選択します。

ステップ 8　**Configure Summertime** をクリックします。

Configure Summertime ダイアログボックスが表示されます。

ステップ 9　ドロップダウン ボックスから Summer Zone Name を選択するか、または作成済みのサマータイム名を入力します。

これは、サマータイム時間が実施されている間に表示される時間帯名です。

ステップ 10　サマータイム中に付加する時間数を入力します。

事前に定義されたサマータイム時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 11　**Start Time** フィールドに、サマータイム設定に適用する時刻を入力します。

ステップ 12　**End Time** フィールドに、サマータイム設定から削除する時刻を入力します。

ステップ 13　**Summertime Duration** で、サマータイム設定が毎年指定された日付に発生する（recurring）か、または指定された日付で開始および終了する（date）かを選択します。

a. Recurring：ドロップダウン ボックスから開始時刻と終了時刻を選択します。

デフォルトは 4 月の第 1 日曜日と 10 月の最終日曜日です。

b. Date：ドロップダウン ボックスから開始時刻と終了時刻を選択します。

開始および終了時刻のデフォルトは、1 月 1 日です。

ステップ 14　**OK** をクリックします。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 15　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

ステップ 16　時刻と日付の設定を変更した場合（ステップ 1 と 2）、**Apply Time to Sensor** の順にクリックして、変更した設定をセンサーに保存します。

センサー上の時刻の修正

イベントには発生時の時刻が刻印されるため、時刻を誤って設定した場合、保存されたイベントの時刻は不正確になります。

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。イベント発生元になるセンサーのセットアップ中に、8:00 a.m. と間違えて 8:00 p.m. に時間を設定した場合、エラーを修正すると、修正された時間は過去に設定されます。新しいイベントが、古いイベントよりも古くなることがあります。

たとえば、初期セットアップ中にセンサーを中部時間でサマータイムが使用可能と設定し、現地時間が 8:04 p.m. だった場合、時間は 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、時計が 21:00:23 CDT と表示され、エラーに気づいたとします。時間を 9:00 a.m. に変更すると、時計は 09:01:33 CDT と表示されます。UTC からのオフセットは変更されていないので、UTC 時間は 14:01:33 UTC になりますが、これがタイムスタンプの問題の原因になります。

イベント レコード上のタイムスタンプの整合性を保証するには、**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。**clear events** コマンドの詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Clearing Events from the Event Store」を参照してください。

注意　イベントを個別に削除することはできません。

ユーザの設定

この項では、ユーザをシステムに追加する方法およびシステムから削除する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.2-28）
- サポートされるユーザのロール（P.2-29）
- フィールド定義（P.2-29）
- ユーザの設定（P.2-30）

概要

IDM では、一度に複数のユーザがログインできます。ローカル センサーからユーザを作成および削除することができます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。

ユーザには、次の 4 つのロールがあります。

- ビューア：イベントの表示と設定ができますが、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：すべてを表示でき、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、使用不可、使用可能）
  - 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：すべてを表示でき、オペレータが修正できるすべてのオプションを修正でき、さらに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できるホストのリスト
  - 物理検知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をイネーブルまたはディセーブルにする
  - ユーザとパスワードの追加と削除
  - 新しい SSH ホスト鍵とサーバ証明書の生成
- サービス：サービス特権が付与されたユーザは、1 つのセンサーに 1 人だけ作成できます。サービス ユーザは、IDM 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。

（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。許可されるサービス アカウントは 1 つだけです。トラブルシューティング用には、サービス ロールのアカウントのみを作成してください。サービス アカウントを編集できるのは、管理者特権を持つユーザだけです。

注意 サービス アカウントを作成するかどうかは慎重に検討してください。サービス アカウントは、システムへのシェル アクセスを提供します。これにより、システムは脆弱になります。しかし、サービス アカウントを使用すると、管理者パスワードを喪失した場合に新規パスワードを作成することができます。状況を分析して、サービス アカウントをシステム上に存在させるかどうかを決定します。

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.
*********************************************************
```

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ユーザの追加と編集を行うには、管理者である必要があります。

フィールド定義

この項では、ユーザのフィールド定義を示します。取り上げる事項は次のとおりです。

- Users パネル（P.2-29）
- Add and Edit User ダイアログボックス（P.2-30）

Users パネル

Users パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Username**：ユーザ名。
  値は、1 ～ 64 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ に一致するパターンです。
- **Role**：ユーザ ロール。
  値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。
- **Status**：現在のユーザ アカウントのステータス（active、expired、または locked）を表示します。

ボタンの機能：

- **Add**：Add User ダイアログボックスを開きます。
  このダイアログボックスでは、新しいユーザをユーザ リストに追加できます。
- **Edit**：Edit User ダイアログボックスを開きます。
  このダイアログボックスでは、ユーザ リストにあるユーザを編集できます。
- **Delete**：ユーザ リストからユーザを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit User ダイアログボックス

Add and Edit User ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Username**：ユーザ名。
  有効な値は、1 ～ 64 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ に一致するパターンです。
- **User Role**：ユーザ ロール。
  有効な値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。
- **Password**：ユーザのパスワード。
  パスワードは 6 文字以上である必要があります。
- **Confirm Password**：パスワードを確認します。
  確認パスワードとユーザ パスワードが一致しない場合、エラー メッセージが表示されます。
- **Change the password to access the sensor**：ユーザのパスワードを変更します。
  Edit ダイアログボックスでのみ使用できます。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ユーザの設定

センサー上のユーザを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Sensor Setup > Users** の順にクリックします。

Users パネルが表示されます。

ステップ 3　**Add** をクリックして、ユーザを追加します。

Add User ダイアログボックスが表示されます。

ステップ 4　**Username** フィールドにユーザ名を入力します。

ステップ 5　**User Role** フィールドのドロップダウン リストから、次のいずれかのユーザ ロールを選択します。

- 管理者
- オペレータ
- ビューア
- サービス

ステップ 6　**Password** フィールドに、そのユーザの新しいパスワードを入力します。

ステップ 7　**Confirm Password** フィールドで、そのユーザの新しいパスワードを確認します。

ステップ 8　**OK** をクリックします。

新しいユーザが、Users パネルのユーザ リストに表示されます。

ステップ 9　ユーザを編集するには、ユーザ リストにあるユーザを選択し、**Edit** をクリックします。

Edit User ダイアログボックスが表示されます。

ステップ 10　**Change the password to access the sensor** チェックボックスをオンにします。

ステップ 11　**User Role** フィールドと **Password** フィールドに必要な変更を行います。

ステップ 12　**OK** をクリックします。

編集したユーザが、Users パネルのユーザ リストに表示されます。

ステップ 13　ユーザをユーザ リストから削除するには、それを選択して **Delete** をクリックします。

削除されたユーザは、User パネルのユーザ リストに表示されなくなります。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 14　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

インターフェイスの設定

この章では、さまざまなインターフェイス モードとセンサー上のインターフェイスの設定方法について説明します。この章は、次の項で構成されています。

- インターフェイスの説明（P.3-2）
- 混合モードの説明（P.3-3）
- インライン インターフェイス モードの説明（P.3-3）
- インライン VLAN ペア モードの説明（P.3-4）
- インターフェイス サポート（P.3-5）
- インターフェイスの設定上の制限（P.3-7）
- サマリー（P.3-9）
- インターフェイスの設定（P.3-10）
- インライン インターフェイス ペアの設定（P.3-14）
- インライン VLAN ペアの設定（P.3-17）
- バイパス モードの設定（P.3-21）
- トラフィック フロー通知の設定（P.3-23）

インターフェイスの説明

コマンド / コントロール インターフェイスは、特定のインターフェイスに恒常的にマッピングされます。この物理インターフェイスは、使用しているセンサーのタイプによって異なります。センシング インターフェイスは、混合モード、インライン インターフェイス モード、またはインライン VLAN ペア モードで動作するように設定できます。インライン インターフェイス モードをサポートするセンサーでは、センシング インターフェイスを「インライン ペア」と呼ばれる論理インターフェイスのペアにできます。VLAN をサポートするセンサーでは、VLAN をインライン VLAN ペアにできます。センサーがトラフィックを監視する前に、インターフェイス、インターフェイス ペア、または VLAN ペアをイネーブルにする必要があります。

(注) アプライアンスでは、センシング インターフェイスはデフォルトでディセーブルになっています。モジュールでは、センシング インターフェイスは常にイネーブルで、ディセーブルにはできません。

インライン VLAN ペア（on-a-stick）機能の追加により、各センシング インターフェイスは混合モード、インライン インターフェイス モード、インライン VLAN ペア モードの 3 つのモードのいずれかで動作するようになりました。複数のセンシング インターフェイスを備えたセンサー上では、同一センサー上でモードを任意に組み合せて使用できます。

- センシング インターフェイスがインライン インターフェイス ペアの別のセンシング インターフェイスとペアになり、そのサブインターフェイス タイプが none に設定されている（デフォルト）場合、そのセンシング インターフェイスはインライン モードになります。
- センシング インターフェイスのサブインターフェイス タイプがインライン VLAN ペアに設定されている場合、そのセンシング インターフェイスはインライン VLAN ペア モードになります。
- デフォルト、つまり他の 2 つのどちらのモードでもない場合、センシング インターフェイスは混合モードです。

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。このため、センサーは、見張っていることを攻撃者に気づかれずにデータ ストリームを監視できます。混合モードは、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るインライン インターフェイス モードと対照的です。詳細については、P.3-3 の「混合モードの説明」、P.3-3 の「インライン インターフェイス モードの説明」、および P.3-4 の「インライン VLAN ペア モードの説明」を参照してください。

センサーは、デフォルトの仮想センサーに割り当てられているインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア上のトラフィックのみを監視します。詳細については、P.4-3 の「インターフェイスの仮想センサーへの割り当て」を参照してください。

SensorApp が動作していない場合にもトラフィックがインライン ペアを経由して流れるようにセンサーを設定するには、バイパス モードをイネーブルにします。バイパス モードでは、再設定、サービス パックのインストール、またはソフトウェア障害時のデータフローの中断が最小限に抑えられます。

センサーは、シャーシの電源が切れている間に、インストールされているモジュールのインターフェイスを検出します。それらのインターフェイスは、次回センサーを起動するときに設定できます。モジュールが取り外されている場合、センサーは次回の起動時に、インターフェイスがないことを検出します。インターフェイス設定は保持されますが、インターフェイスが存在しない場合はセンサーによって無視されます。

次のインターフェイス設定イベントは、ステータス イベントとして報告されます。

- リンク アップまたはリンク ダウン

- トラフィックの開始または停止
- バイパス モードの自動アクティブ化または非アクティブ化
- パケット失敗率のしきい値の超過

混合モードの説明

混合モードでは、パケットは IPS を経由して流れません。センサーは、実際に転送されたパケットではなく、監視したトラフィックのコピーを分析します。混合モードで運用する利点は、転送されたトラフィックでパケットのフローに IPS が影響を与えないことです。ただし、混合モードで運用する場合の短所は、悪意のあるトラフィックがアトミック アタック（シングル パケット攻撃）などの特定の種類の攻撃のために意図したターゲットに到達するのを、IPS が阻止できないことです。混合 IPS 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、攻撃に応答するには、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です。このような応答アクションは一部の種類の攻撃を防ぐことができますが、アトミック アタックの場合、混合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 モードの説明

インライン インターフェイス モードで動作すると、IPS は直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。パケット転送速度は遅延を加えられることによって遅くなります。インライン IPS はファースト パスにあります。ファースト パスでは、センサーが、意図したターゲットに到達する前に悪意のあるトラフィックを廃棄することによって攻撃を阻止し、保護サービスを提供できます。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）。このより詳細な分析では、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、停止またはブロックすることができます。

インライン インターフェイス モードでは、パケットはセンサーのペアの 1 つ目のインターフェイスを経由して入り、ペアの 2 つ目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限り、ペアの 2 つ目のインターフェイスに送信されます。

（注） ASA SSM は、センシング インターフェイスが 1 つしかない場合にもインラインで動作するように設定できます。

インライン VLAN ペア モードの説明

物理インターフェイス上で VLAN をペアで関連付けることができます。これは「inline on a stick」として知られています。ペアの VLAN のいずれかで受信されたパケットは、分析された後、別の VLAN にペアで転送されます。インライン VLAN ペアは、NM-CIDS、AIP SSM 10、および AIP SSM 20 を除く、IPS 5.1 と互換性があるすべてのセンサーでサポートされています。

インライン VLAN ペア モードは、アクティブ センシング モードです。このモードでは、センシング インターフェイスが 802.1q トランク ポートとして動作し、センサーがトランク上の VLAN ペア間の VLAN ブリッジングを実行します。センサーは、ペアごとに各 VLAN 上で受信するトラフィックを調べ、そのパケットをペアの他方の VLAN へ転送するか、または侵入の試行が検出された場合はパケットを破棄することができます。IPS センサーでは、各センシング インターフェイスで最大 255 個の VLAN ペアを同時にブリッジするように設定できます。センサーは、受信した各パケットの 802.1q ヘッダー内の VLAN ID フィールドをセンサーがパケットを転送する出力 VLAN の ID に置き換えます。センサーは、インライン VLAN ペアに割り当てられていない VLAN 上で受信されたパケットをすべてドロップします。

インターフェイス サポート

表 3-1 は、IPS 5.1 を実行するアプライアンスおよびモジュールのインターフェイス サポートを示します。

表 3-1　インターフェイス サポート

ベース シャーシ	追加された PCI カード	インラインをサポートするインターフェイス	可能なポートの組み合せ	インラインをサポートしていないインターフェイス
IDS-4210	—	なし	なし	すべて
IDS-4215	—	なし	なし	すべて
IDS-4215	4FE	FastEthernet0/1 4FE FastEthernetS/0[1] FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3 0/1<->1/0 0/1<->1/1 0/1<->1/2 0/1<->1/3	FastEthernet0/0
IDS-4235	—	なし	なし	すべて
IDS-4235	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4235	TX (GE)	TX オンボード + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 または GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	—	なし	なし	すべて
IDS-4250	4FE	4FE FastEthernetS/0 FastEthernetS/1 FastEthernetS/2 FastEthernetS/3	1/0<->1/1 1/0<->1/2 1/0<->1/3 1/1<->1/2 1/1<->1/3 1/2<->1/3	GigabitEthernet0/0 GigabitEthernet0/1
IDS-4250	TX (GE)	TX オンボード + TX PCI GigabitEthernet0/0 + GigabitEthernet1/0 または GigabitEthernet2/0	0/0<->1/0 0/0<->2/0	GigabitEthernet0/1
IDS-4250	SX	なし	なし	すべて
IDS-4250	SX + SX	2 SX GigabitEthernet1/0 GigabitEthernet2/0	1/0<->2/0	GigabitEthernet0/0 GigabitEthernet0/1

表 3-1　インターフェイス サポート（続き）

ベース シャーシ	追加された PCI カード	インラインをサポートするインターフェイス	可能なポートの組み合せ	インラインをサポートしていないインターフェイス
IDS-4250	XL	XL GigabitEthernet2/0 の 2 SX GigabitEthernet2/1	2/0<->2/1	GigabitEthernet0/0 GigabitEthernet0/1
IDSM-2	—	ポート 7 および 8 GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2
IPS-4240	—	4 オンボード GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS-4255	—	4 オンボード GE GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
NM-CIDS	—	なし	なし	すべて
AIP SSM 10	—	GigabitEthernet0/1	セキュリティコンテキストによる	GigabitEthernet0/0
AIP SSM 20	—	GigabitEthernet0/1	セキュリティコンテキストによる	GigabitEthernet0/0

1. 4FE カードはスロット 1 または 2 のどちらかにインストールできます。S はスロット番号を示しており、1 または 2 のどちらかになります。

インターフェイスの設定上の制限

センサー上のインターフェイスの設定については、次の制限があります。

- インライン モードをサポートするセンサー プラットフォームでは、バイパス モードを設定してインライン インターフェイス ペアを作成することしかできません。
- インライン インターフェイス ペアには、物理インターフェイスのタイプ（銅または光ファイバ）、速度、またはインターフェイスの二重通信設定に関係なく、任意のセンシング インターフェイスの組み合せを含めることができます。ただし、メディア タイプ、速度、および二重通信設定の異なるインターフェイスの組み合せについては、テストが不完全だったり、正式にサポートされていなかったりする場合があります。
- モジュール（IDSM-2、NM-CIDS、AIP SSM 10、および AIP SSM 20）、IPS-4240、および IPS-4255 では、すべてのバックプレーン インターフェイスの速度、二重通信、状態の設定は固定です。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。
- NM-CIDS 上で、センシング インターフェイスとして機能する同一バックプレーン インターフェイスは、RBCP 制御トラフィックも伝送します。このインターフェイスがダウンすると、モジュールも失敗します。バックプレーン インターフェイスは保護されているため、このインターフェイスがダウン状態になるよう設定することはできません。ただし、Linux ifconfig ユーティリティを使用してこのインターフェイスのダウン状態を設定している場合、RBCP 通信は失敗します。
- 代替 TCP リセット インターフェイス
  - 代替 TCP リセット インターフェイスはセンシング インターフェイスにしか割り当てできません。管理インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。代替 TCP リセット インターフェイス オプションは、デフォルトとして **none** に設定されており、センシング インターフェイスを除くすべてのインターフェイス用に保護されています。
  - 同じ物理インターフェイスを複数のセンシング インターフェイスの代替 TCP リセット インターフェイスとして割り当てることができます。
  - 物理インターフェイスは、センシング インターフェイスと代替 TCP リセット インターフェイスの両方として機能できます。
- インライン VLAN ペア内で VLAN を指定する順序は重要ではありません。
- インライン VLAN ペア モードのセンシング インターフェイスは、1 ～ 255 個のインライン VLAN ペアを保持できます。

次のインターフェイスの組み合せは無効です。

- 管理インターフェイスはセンシング インターフェイスとして機能することはできません。
- 管理インターフェイスは、センシング インターフェイスの代替 TCP リセット インターフェイスとして機能することはできません。
- 管理インターフェイスは、インライン インターフェイス ペアのメンバにすることはできません。
- 物理インターフェイスとインライン インターフェイス ペア内のそれ自体とをペアにすることはできません。
- 物理インターフェイスは、最大 1 つのインライン インターフェイス ペアのメンバにすることができます。
- センシング インターフェイスは、それ自身の代替 TCP リセット インターフェイスとしては機能できません。
- TCP リセットに対応しているインターフェイスのみを代替 TCP リセット インターフェイスとして設定できます。

（注）この制限事項の例外が IDSM-2 です。両方のセンシング インターフェイスに対する代替 TCP リセット インターフェイスの割り当ては System0/1 です（保護されています）。

- VLAN はそれ自体とペアにすることはできません。
- 特定のセンシング インターフェイスの場合、VLAN は最大 1 つのインライン VLAN ペアのメンバにすることができます。ただし、特定の VLAN を複数のセンシング インターフェイスのインライン VLAN ペアのメンバーにすることができます。
- 物理インターフェイスは、インライン インターフェイス ペアのメンバにすることはできません。ただし、物理インターフェイスのサブインターフェイス モードが **none** の場合は除きます。
- 非バックプレーン FastEthernet インターフェイスの場合、有効な速度設定は 10 Mbps、100 Mbps、および自動です。有効な二重通信設定は、全、半、自動です。
- ギガビット ファイバ インターフェイス（IDS-4250 上の 1000-SX および XL）の場合、有効な速度設定値は 1000 Mbps および自動のみです。
- ギガビット 銅線 インターフェイス（IDS-4235 および IDS-4250 上の 1000-TX）の場合、有効な速度設定値は 10 Mbps、100 Mbps、1000 Mbps、および自動です。
- ギガビット（銅線またはファイバ）インターフェイスの場合は、速度が 1000 Mbps に設定されている場合、有効な二重通信設定値は自動のみです。

サマリー

この項では、Summary パネルについて説明します。取り上げる事項は次のとおりです。

- 概要（P.3-9）
- サポートされるユーザのロール（P.3-9）
- フィールド定義（P.3-9）

概要

Summary パネルには、センシング インターフェイスをどのように設定したか、つまり、混合モードに設定したインターフェイス、インライン ペアに設定したインターフェイス、およびインライン VLAN ペアに設定したインターフェイスが表示されます。インターフェイス設定を変更すると、このパネルの内容も変更されます。

注意　1 つの物理インターフェイスを混合モード、インライン ペア モード、またはインライン VLAN ペア モードのいずれかで動作するように設定できますが、これらのモードを組み合せたインターフェイスを設定することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

フィールド定義

Summary パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：インターフェイスの名前。

  混合インターフェイスでは、この値は **FastEthernet** または **GigabitEthernet** になります。インライン インターフェイスでは、ペアに割り当てた名前になります。
- **Details**：インターフェイスが混合またはインラインであるかどうかを示し、VLAN ペアの有無を示します。
- **Description**：インターフェイスの説明。
- **Assigned Virtual Sensor**：インターフェイスまたはインターフェイス ペアが仮想センサー vs0 に割り当て済みであるかどうかを示します。

インターフェイスの設定

この項では、センサー上のインターフェイスの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.3-10）
- TCP リセットの説明（P.3-10）
- サポートされるユーザのロール（P.3-11）
- フィールド定義（P.3-11）
- インターフェイスの設定（P.3-13）

概要

Interfaces パネルには、センサー上の既存の物理インターフェイスとそれらに関連する設定が表示されます。センサーはインターフェイスを検出し、インターフェイス リストを Interfaces パネルに代入します。

センサーがトラフィックを監視するように設定するには、インターフェイスをイネーブルにする必要があります。**setup** コマンドを使用してセンサーを初期化したときに、インターフェイスまたはインライン ペアをデフォルトの仮想センサー vs0 に割り当て、そのインターフェイスまたはインライン ペアをイネーブルにしています。インターフェイス設定を変更する必要がある場合は、Interfaces パネルから変更できます。インターフェイスまたはインライン ペアの仮想センサー vs0 への割り当ては、Edit Virtual Sensor ダイアログボックスの **Configuration > Analysis Engine > Virtual Sensor > Edit** で実行できます。

TCP リセットの説明

次の場合には、代替 TCP リセット インターフェイスを指定する必要があります。

- スイッチが SPAN または VACL キャプチャを使用して監視され、スイッチが SPAN または VACL キャプチャ ポートで着信パケットを受け入れない場合。
- スイッチが複数の VLAN の SPAN キャプチャまたは VACL キャプチャのどちらかを使用して監視され、スイッチが 802.1q ヘッダーのある着信パケットを受け入れない場合。

（注） TCP リセットには、リセットを送信する VLAN を指定する 802.1q ヘッダーが必要です。

- 接続の監視にネットワーク タップが使用される場合。

（注） タップは、センサーからの着信トラフィックを許可しません。

センシング インターフェイスは代替 TCP リセット インターフェイスとしてのみ割り当てることができます。管理インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー上のインターフェイスを編集するには、管理者である必要があります。

フィールド定義

この項では、インターフェイスのフィールド定義を示します。取り上げる事項は次のとおりです。

- Interfaces パネル（P.3-11）
- Edit Interface ダイアログボックス（P.3-12）

Interfaces パネル

Interfaces パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インターフェイスの名前。
  すべてのインターフェイスで、この値は **FastEthernet** または **GigabitEthernet** になります。
- **Enabled**：インターフェイスをイネーブルにするかどうかを指定します。
- **Media Type**：メディア タイプを示します。
  メディア タイプのオプションは次のとおりです。
  - **TX**：銅メディア
  - **SX**：光ファイバ メディア
  - **XL**：ネットワーク アクセラレータ カード
  - **Backplane interface**：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- **Duplex**：インターフェイスの二重通信設定を示します。
  二重通信タイプのオプションは次のとおりです。
  - **Auto**：インターフェイスを自動ネゴシエーション二重に設定します。
  - **Full**：インターフェイスを全二重に設定します。
  - **Half**：インターフェイスを半二重に設定します。
- **Speed**：インターフェイスの速度設定を示します。
  速度タイプのオプションは次のとおりです。
  - **Auto**：インターフェイスを自動ネゴシエーション速度に設定します。
  - **10 MB**：インターフェイスを 10 MB に設定します（TX インターフェイスの場合のみ）。
  - **100 MB**：インターフェイスを 100 MB に設定します（TX インターフェイスの場合のみ）。
  - **1000**：インターフェイスを 1 GB に設定します（ギガビット インターフェイスの場合のみ）。
- **Alternate TCP Reset Interface**：これを選択すると、代替インターフェイスが混合モニタリングに使用され、シグニチャ反応によってリセット アクションがトリガーされた場合、代替インターフェイス上の TCP リセットが送信されます。
- **Description**：インターフェイスの説明を入力します。

ボタンの機能：

- **Select All**：リストにあるすべてのエントリを選択できます。
- **Edit**：Edit Interface ダイアログボックスを開きます。

  このダイアログボックスで、このインターフェイスに関連付けられた値の一部を変更できます。
- **Enable**：インターフェイスをイネーブルにします。
- **Disable**：インターフェイスをディセーブルにします。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Edit Interface ダイアログボックス

Edit Interface ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インターフェイスの名前。

  すべてのインターフェイスで、この値は FastEthernet または GigabitEthernet になります。
- **Description**：インターフェイスの説明を入力します。
- **Media Type**：メディア タイプを示します。

  メディア タイプは次のとおりです。
  - **TX**：銅メディア
  - **SX**：光ファイバ メディア
  - **XL**：ネットワーク アクセラレータ カード
  - **Backplane interface**：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- **Enabled**：インターフェイスをイネーブルにするかどうかを指定します。
- **Duplex**：インターフェイスの二重通信設定を示します。

  二重通信タイプは次のとおりです。
  - **Auto**：インターフェイスを自動ネゴシエーション二重に設定します。
  - **Full**：インターフェイスを全二重に設定します。
  - **Half**：インターフェイスを半二重に設定します。
- **Speed**：インターフェイスの速度設定を示します。

  速度タイプは次のとおりです。
  - **Auto**：インターフェイスを自動ネゴシエーション速度に設定します。
  - **10**MB：インターフェイスを 10 MB に設定します（TX インターフェイスの場合のみ）。
  - **100 MB**：インターフェイスを 100 MB に設定します（TX インターフェイスの場合のみ）。
  - **1000**：インターフェイスを 1 GB に設定します（ギガビット インターフェイスの場合のみ）。
- **Use Alternate TCP Reset Interface**：これを選択すると、代替インターフェイスが混合モニタリングに使用され、シグニチャ反応によってリセット アクションがトリガーされた場合、代替インターフェイス上の TCP リセットが送信されます。
  - **Select Interface**：TCP リセットを送信するインターフェイスを設定します。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

インターフェイスの設定

インターフェイスをイネーブルまたはディセーブルにする、またはインターフェイス設定を編集するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Interface Configuration** > **Interfaces** の順にクリックします。

Interfaces パネルが表示されます。

ステップ 3　行を選択またはダブルクリックして、**Enable** をクリックします。

インターフェイスがイネーブルになります。インターフェイスがトラフィックを監視するためには、そのインターフェイスを仮想センサーに割り当てる必要があります。手順については、P.4-3 の「インターフェイスの仮想センサーへの割り当て」を参照してください。

ステップ 4　インターフェイスに関連付けられている値の一部を編集するには、インターフェイスを選択して、**Edit** をクリックします。

Edit Interface ダイアログボックスが表示されます。

ステップ 5　**Description** フィールドの説明を変更できます。また、**No** または **Yes** チェックボックスをオンにすることで、状態を enabled から disabled に変更できます。**Use Alternative TCP Reset Interface** を選択することで、インターフェイスが代替 TCP リセットを使用するように設定できます。

ステップ 6　**OK** をクリックします。

変更内容が Interfaces パネルのリストに表示されます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 7　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

インライン インターフェイス ペアの設定

この項では、インライン インターフェイス ペアの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.3-14）
- サポートされるユーザのロール（P.3-14）
- フィールド定義（P.3-14）
- インライン インターフェイス ペアの設定（P.3-15）

概要

センサーがインライン モニタリングに対応している場合、センサー上でインターフェイスのペアを作成できます。

（注）AIP SSM には、モニタリング用のインライン ペアは必要ありません。物理インターフェイスを仮想センサーに追加するだけです。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

インターフェイス ペアを設定するには、管理者である必要があります。

フィールド定義

この項では、インターフェイス ペアのフィールド定義を示します。取り上げる事項は次のとおりです。

- Interface Pairs パネル（P.3-14）
- Add and Edit Interface Pair ダイアログボックス（P.3-15）

Interface Pairs パネル

Interface Pairs パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Pair Name**：インターフェイス ペアに指定する名前。
- **Paired Interfaces**：ペアを作成した 2 つのインターフェイス（GigabitEthernet0/0<->GigabitEthernet0/1 など）。
- **Description**：このインターフェイス ペアの説明を追加します。

ボタンの機能：

- **Select All**：すべてのインターフェイス ペアを選択します。
- **Add**：Add Interface Pair ダイアログボックスを開きます。
  このダイアログボックスでは、新しいインターフェイス ペアを追加できます。

- **Edit**：Edit Interface Pair ダイアログボックスを開きます。
  このダイアログボックスでは、インターフェイス ペアの値を編集できます。
- **Delete**：選択したインターフェイス ペアを削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit Interface Pair ダイアログボックス

Add and Edit Interface Pair ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Pair Name**：インターフェイス ペアに指定する名前。
- **Select two interfaces**：リストからペアを作成する 2 つのインターフェイスを選択します（GigabitEthernet0/0<->GigabitEthernet0/1 など)。
- **Description**：このインターフェイス ペアの説明を追加します。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

インライン インターフェイス ペアの設定

インライン インターフェイス ペアを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Interface Configuration** > **Interface Pairs** の順にクリックします。

Interface Pairs パネルが表示されます。

ステップ 3　インライン インターフェイス ペアを追加するには、**Add** をクリックします。

Add Interface Pair ダイアログボックスが表示されます。

ステップ 4　**Interface Pair Name** フィールドに名前を入力します。

インライン インターフェイス名は、作成した名前になります。

ステップ 5　**Select two interfaces** フィールドで、ペアを作成する 2 つのインターフェイスを選択します。

たとえば、GigabitEthernet0/0 と GigabitEthernet0/1 のように選択します。

ステップ 6　必要であれば、**Description** フィールドにインライン インターフェイス ペアの説明を追加できます。

ステップ 7　**OK** をクリックします。

Interface Pairs パネルのリストに、新しいインライン インターフェイス ペアが表示されます。

ステップ 8　インライン インターフェイス ペアを編集するには、これを選択し、**Edit** をクリックします。

Edit Interface Pair ダイアログボックスが表示されます。

ステップ 9　このダイアログボックスで、名前の変更、新しいインライン インターフェイス ペアの選択、説明の編集ができます。

ステップ 10　**OK** をクリックします。

Interface Pairs パネルのリストに、編集されたインライン インターフェイス ペアが表示されます。

ステップ 11　インライン インターフェイス ペアを削除するには、これを選択し、**Delete** をクリックします。

削除されたインライン インターフェイス ペアは、Interface Pairs パネルのリストに表示されなくなります。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 12　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

インライン VLAN ペアの設定

この項では、インライン VLAN ペアの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.3-17）
- サポートされるユーザのロール（P.3-17）
- フィールド定義（P.3-17）
- インライン VLAN ペアの設定（P.3-19）

概要

VLAN Pairs パネルには、各物理インターフェイスの既存のインライン VLAN ペアが表示されます。インライン VLAN ペアを作成するには、**Add** をクリックします。

（注） 別のインターフェイスとペアになっているインターフェイスや、混合モードで動作し仮想センサーに割り当てられているインターフェイスでは、インライン VLAN ペアは作成できません。

混合モードで動作するインターフェイスに対してインライン VLAN ペを作成するには、仮想センサーからそのインターフェイスを除外してから、インライン VLAN ペアを作成します。インライン VLAN ペアを作成するときに、インターフェイスが別のインターフェイスとペアになっていたり、混合モードになっていたりすると、エラー メッセージが表示されます。

（注） センサーが「on-a-stick」機能をサポートしていない場合、VLAN Pairs パネルは表示されません。AIP SSM と NM-CIDS は、インライン VLAN ペアをサポートしていません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

インライン VLAN ペアを設定するには、管理者である必要があります。

フィールド定義

この項では、インライン VLAN ペアのフィールド定義を示します。取り上げる事項は次のとおりです。

- VLAN Pairs パネル（P.3-18）
- Add and Edit VLAN Pair ダイアログボックス（P.3-18）

VLAN Pairs パネル

Interface Pairs パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Interface Name**：インライン VLAN ペアの名前。
- **Subinterface (VLAN Pair)**：インライン VLAN ペアのサブインターフェイス番号。
  値は 1 ～ 255 です。
- **VLAN1**：VLAN1 の VLAN 番号を表示します。
  値は 1 ～ 4095 です。
- **VLAN2**：VLAN2 の VLAN 番号を表示します。
  値は 1 ～ 4095 です。
- **Description**：インライン VLAN ペアの説明。

ボタンの機能：

- **Select All**：すべての VLAN ペアを選択します。
- **Add**：Add VLAN Pair ダイアログボックスを開きます。
  このダイアログボックスでは、新しい VLAN ペアを追加できます。
- **Edit**：Edit VLAN Pair ダイアログボックスを開きます。
  このダイアログボックスで、VLAN ペアの値を編集できます。
- **Delete**：選択した VLAN ペアを削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit VLAN Pair ダイアログボックス

Add and Edit Inline VLAN Pair ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

（注） VLAN はそれ自体とペアにすることはできません。

- **Interface Name**：インライン VLAN ペアを作成するために使用可能なインターフェイスを選択します。
- **Subinterface Number**：サブインターフェイス番号を割り当てます。
  1 から 255 までの数字を割り当てることができます。
- **VLAN 1**：インライン VLAN ペアの最初の VLAN を指定します。
  1 から 4095 までの任意の VLAN を割り当てることができます。
- **VLAN 2**：インライン VLAN ペアの 2 番目の VLAN を指定します。
  1 から 4095 までの任意の VLAN を割り当てることができます。
- **Description**：インライン VLAN ペアの説明を追加します。

（注） サブインターフェイス番号と VLAN 番号は、各物理インターフェイスで一意である必要があります。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

インライン VLAN ペアの設定

インライン VLAN ペアを設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Interface Configuration** > **VLAN Pairs** の順にクリックします。

VLAN Pairs パネルが表示されます。

ステップ 3　インライン VLAN ペアを追加するには、**Add** をクリックします。

Add Inline VLAN Pair ダイアログボックスが表示されます。

ステップ 4　**Interface Name** リストからインターフェイスを選択します。

ステップ 5　**Subinterface Number** フィールドに、インライン VLAN ペアのサブインターフェイス番号（1 ～ 255）を入力します。

ステップ 6　**VLAN 1** フィールドに、インライン VLAN ペアの最初の VLAN（1 ～ 4095）を指定します。

ステップ 7　**VLAN 2** フィールドに、インライン VLAN ペアの 2 番目の VLAN（1 ～ 4095）を指定します。

ステップ 8　必要であれば、**Description** フィールドにインライン VLAN ペアの説明を追加できます。

ステップ 9　**OK** をクリックします。

VLAN Pairs パネルのリストに、新しいインライン VLAN ペアが表示されます。

ステップ 10　インライン VLAN ペアを編集するには、これを選択し、**Edit** をクリックします。

Edit Inline VLAN Pair ダイアログボックスが表示されます。

ステップ 11　このダイアログボックスでサブインターフェイス番号の変更、VLAN 番号の変更、説明の編集ができます。

ステップ 12　**OK** をクリックします。

VLAN Pairs パネルのリストに、編集されたインライン VLAN ペアが表示されます。

ステップ 13　VLAN ペアを削除するには、これを選択し、**Delete** をクリックします。

削除された VLAN ペアは、VLAN Pairs パネルのリストに表示されなくなります。

ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 14 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

バイパス モードの設定

この項では、バイパス モードの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.3-21）
- サポートされるユーザのロール（P.3-21）
- フィールド定義（P.3-22）

概要

バイパス モードは、診断ツールおよびフェールオーバー保護メカニズムとして使用できます。すべての IPS 処理サブシステムをバイパスし、トラフィックが直接インライン ペアに流れることが可能なモードにセンサーを設定できます。このバイパス モードにより、アップグレードのためにセンサーのプロセスが一時的に停止した場合や、センサーのモニタリング プロセスが失敗した場合でも、センサーへのパケット フローは続行します。オン、オフ、自動の 3 つのモードがあります。デフォルトでは、バイパス モードは自動に設定されています。

（注） バイパス　モードは、初めはインラインでペアを組んでいるインターフェイスに対してのみ適用されていました。不具合のため、混合モードには適用されません。今後のバージョンでこの不具合に対応できる可能性があります。混合モードでは、バイパス モードを自動またはオフに設定し、オンで使用しないことをお勧めします。

注意 センサーをバイパス モードにすると、セキュリティに影響を及ぼします。バイパス モードをオンにすると、トラフィックはセンサーをバイパスし検査されないため、センサーは悪意のある攻撃を防止できません。

（注） バイパス モードが機能するのは、オペレーティング システムの実行中だけです。センサーの電源を切ったり、センサーがシャットダウンされたりすると、バイパス モードは機能しません。つまり、トラフィックはセンサーに渡されなくなります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサー上のバイパス モードを設定するには、管理者である必要があります。

フィールド定義

Bypass パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Auto**：センサーのモニタリング　プロセスがダウンしている場合を除き、トラフィックがセンサーに流れて検査されます。

  センサーのモニタリング プロセスがダウンしていると、センサーが再び動作するようになるまで、トラフィックはセンサーをバイパスします。センサーが動作を再開すると、トラフィックを検査します。自動モードは、センサーがアップグレード中でもトラフィックのフローが続行するので、センサー アップグレードのときに役立ちます。また、モニタリング プロセスが失敗した場合でも、トラフィックのフローを続行するのに役立ちます。
- **Off**：バイパス モードをディセーブルにします。

  トラフィックはセンサーに流れて検査されます。センサーのモニタリング プロセスがダウンしていると、トラフィックのフローが停止します。つまり、インライン トラフィックの検査は必ず行われます。
- **On**：トラフィックは SensorApp をバイパスし、検査は行われません。つまり、インライン トラフィックの検査は行われません。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

トラフィック フロー通知の設定

この項では、トラフィック フロー通知の設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.3-23）
- サポートされるユーザのロール（P.3-23）
- フィールド定義（P.3-23）
- トラフィック フロー通知の設定（P.3-23）

概要

センサーがインターフェイスのパケット フローを監視し、指定された時間間隔内でパケット フローに変化があった（開始や停止）場合、通知を送信するように設定できます。特定の通知間隔内の非受信パケットしきい値を設定できます。また、ステータス イベントが報告されるまでのインターフェイス アイドル遅延も設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

トラフィック フロー通知を設定するには、管理者である必要があります。

フィールド定義

Traffic Flow Notifications パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Missed Packets Threshold**：通知が送信される前に、指定された時間内で受信できなかったパケットの率。
- **Notification Interval**：センサーが未受信パケット率をチェックする時間間隔。
- **Interface Idle Threshold**：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パケットを受信していない時間（秒数）。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

トラフィック フロー通知の設定

トラフィック フロー通知を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Interface Configuration** > **Traffic Flow Notifications** の順にクリックします。

Traffic Flow Notifications パネルが表示されます。

ステップ 3　通知を受信する前に発生した未受信パケット率を選択し、**Missed Packets Threshold** フィールドにその値を入力します。

ステップ 4　未受信パケット率をチェックする秒数を選択し、**Notification Interval** フィールドにその値を入力します。

ステップ 5　通知を受信する前に、インターフェイスがアイドル状態でパケットを受信していない状況を許可する時間（秒数）を選択し、**Interface Idle Threshold** フィールドにその値を入力します。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 6　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

分析エンジン

この章では、分析エンジンの機能と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説明します。この章は、次の項で構成されています。

- 分析エンジンについて（P.4-1）
- 仮想センサーの設定（P.4-2）
- グローバル変数の設定（P.4-5）

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知を行います。指定されたインターフェイスとインターフェイス ペアを通過するトラフィックを監視します。

仮想センサーの設定

この項では、仮想センサーの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.4-2）
- サポートされるユーザのロール（P.4-2）
- フィールド定義（P.4-2）
- インターフェイスの仮想センサーへの割り当て（P.4-3）

概要

センサーは、1 つまたは複数の監視対象データ ストリームからデータ入力を受信できます。これらの監視対象データ 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 ポートのいずれかです。たとえば、1 台のセンサーはファイアウォールの前方、後方、または同時に前後からのトラフィックを監視できます。また、1 つまたは複数のデータ ストリームを監視できます。この場合、1 つのセンサー ポリシーまたは設定が、すべての監視対象データ ストリームに適用されます。

仮想センサーは複数のセグメントを監視でき、1 台の物理センサー内の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。分析する監視対象セグメントごとに異なるポリシーを設定できます。

（注） IPS 5.1 では、1 つの仮想センサー vs0 だけがサポートされます。

インターフェイス、インターフェイス ペア、および VLAN ペアを仮想センサーに割り当てることができます。仮想センサーの説明は変更できますが、仮想センサーの追加や仮想センサー名の変更はできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

仮想センサーを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、仮想センサーのフィールド定義を示します。取り上げる事項は次のとおりです。

- Virtual Sensor パネル（P.4-3）
- Edit Virtual Sensor ダイアログボックス（P.4-3）

Virtual Sensor パネル

Virtual Sensor パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：仮想センサーの名前。

  IPS 5.1 にある仮想センサーは 1 つだけで、名前は「vs0」です。
- **Assigned Interfaces (or Pairs)**：仮想センサーに属しているインターフェイスまたはインターフェイス ペア。
- **Description**：仮想センサーの説明。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Edit Virtual Sensor ダイアログボックス

Edit Virtual Sensor ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Virtual Sensor Name**：仮想センサーの名前。

  IPS 5.1 にある仮想センサーは 1 つだけで、名前は「vs0」です。
- **Description**：仮想センサーの説明。
- **Assign Interfaces**：インターフェイスを仮想センサーに割り当てます。
  - **Name**：仮想センサーに割り当て可能なインターフェイスまたはインターフェイス ペアのリスト。
  - **Details**：インターフェイスのモード（インラインまたは混合）をリストし、インライン ペアのインターフェイスをリストします。
  - **Assigned**：インターフェイスまたはインターフェイス ペアが仮想センサーに割り当て済みであるかどうかを示します。

ボタンの機能：

- **Select All**：リストにあるすべてのインターフェイスを選択します。
- **Assign**：選択したインターフェイスまたはインターフェイス ペアを Assigned Interfaces (or Pairs) リストに追加します。
- **Remove**：選択したインターフェイスまたはインターフェイス ペアを Assigned Interfaces (or Pairs) リストから削除します。

インターフェイスの仮想センサーへの割り当て

インターフェイス、インライン インターフェイス ペア、またはインライン VLAN ペアを仮想センサーに追加する、または仮想センサーから削除するには、次の手順を実行します。

(注) トラフィックを監視する前に、すべてのインターフェイスを仮想センサーに割り当ててイネーブルにする必要があります。センサー インターフェイスをイネーブルにする手順については、第 3 章「インターフェイスの設定」を参照してください。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Analysis Engine** > **Virtual Sensor** の順にクリックします。

Virtual Sensor パネルが表示されます。

ステップ 3　**Edit** をクリックします。

Edit Virtual Sensor ダイアログボックスが表示されます。

ステップ 4　インターフェイス、インターフェイス ペア、またはインライン VLAN ペアを仮想センサーに割り当てるには、Available Interfaces (or Pairs) リストから選択し、**Add** をクリックします。

ステップ 5　インターフェイス、インターフェイス ペア、またはインライン VLAN ペアを仮想センサーから削除するには、Assigned Interfaces (or Pairs) リストから選択し、**Remove** をクリックします。

ステップ 6　「default virtual sensor（デフォルトの仮想センサー）」という説明を変更するには、Description フィールドに新しい説明を入力します。

ヒント　変更を元に戻してダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 7　**OK** をクリックします。

該当するインターフェイスが Virtual Sensor パネルのリストに表示されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 8　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

グローバル変数の設定

この項では、グローバル変数の設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.4-5）
- サポートされるユーザのロール（P.4-5）
- フィールド定義（P.4-5）

概要

分析エンジン コンポーネント内部のグローバル変数を設定できます。グローバル変数は、Maximum Open IP Log Files の 1 つだけです。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

グローバル変数を設定するには、管理者またはオペレータである必要があります。

フィールド定義

Global Variables パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Maximum Open IP Log Files**：同時に開ける IP ログ ファイルの最大数。
  有効範囲は 20 ～ 100 です。デフォルトは 20 です。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

シグニチャの定義

この章では、シグニチャを設定する方法について説明します。この章は、次の項で構成されています。

- シグニチャの説明（P.5-2）
- シグニチャ変数の設定（P.5-3）
- シグニチャの設定（P.5-6）
- Miscellaneous パネルの設定（P.5-27）
- MEG シグニチャの例（P.5-45）

シグニチャの説明

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は、ネットワークへの侵入を検出できます。*シグニチャ*は、DoS 攻撃（サービス拒絶攻撃）などの典型的な不正侵入行為を検出するためにセンサーが使用する規則の集まりです。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ト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、false positive 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、ネットワーク アプリケーションやオペレーティング システムによっては多数の ICMP メッセージを送信する場合がありますが、シグニチャ ベースの検出システムでは、これを攻撃者がネットワーク セグメントを調査しようとしていると解釈してしまう可能性があります。センサーをチューニングすると、false positives 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 トラフィックを監視するようにセンサーを設定するには、そのシグニチャを使用可能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ニチャ アップデートのインストール時に使用可能になります。使用可能になっているシグニチャと一致する攻撃を検出すると、センサーはアラートを生成します。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 の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。

IPS 5.1 には、1000 個を超えるデフォルトの組み込みシグニチャがあります。組み込みシグニチャのリストでシグニチャの名前を変更したり、シグニチャを削除したりすることはできません。ただし、シグニチャをリタイアさせ、センシング エンジンから除去することができます。リタイアにしたシグニチャは後でアクティブ化できます。ただし、このプロセスを実行すると、センシング エンジンは設定を再構築する必要があり時間がかかるため、トラフィック処理が遅れ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できます。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。

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。これらは、UDP 接続におけるストリング照合、ネットワーク フラッドの追跡、および各種スキャンなどの多数の用途について設定できます。シグニチャは、監視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

この項では、シグニチャ変数の作成方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.5-3）
- サポートされるユーザのロール（P.5-3）
- フィールド定義（P.5-3）
- シグニチャ変数の設定（P.5-4）

概要

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、すべてのシグニチャの変数が更新されます。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） 変数の前にドル記号（$）を付けて、文字列ではなく変数を使用していることを示す必要があります。

シグニチャ システムに必要なため、削除できない変数もあります。変数が保護されている場合は、それを選択して編集することはできません。保護された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。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

シグニチャ変数を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、シグニチャ変数のフィールド定義を示します。取り上げる事項は次のとおりです。

- Signature Variables パネル（P.5-3）
- Add and Edit Signature Variable ダイアログボックス（P.5-4）

Signature Variables パネル

Signature Variables パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に割り当てる名前を指定します。
- **Type**：変数を Web ポートまたは IP アドレス範囲として指定します。
- **Value**：この変数によって表される値を指定します。

  1 つの変数に対して複数のポート番号を指定するには、エントリをカンマで区切ります。たとえば、80, 3128, 8000, 8010, 8080, 8888, 24326 のように指定します。

ボタンの機能：

- **Add**：Add Signature Variable ダイアログボックスを開きます。
  このダイアログボックスで、新しい変数を追加し、この変数に関連付けられた値を指定できます。
- **Edit**：Edit Signature Variable ダイアログボックスを開きます。
  このダイアログボックスで、この変数に関連付けられた値を変更できます。
- **Delete**：選択した変数を使用可能な変数リストから削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit Signature Variable ダイアログボックス

Add and Edit Signature Variable ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に割り当てる名前を指定します。
- **Type**：変数を Web ポートまたは IP アドレス範囲として指定します。
- **Value**：この変数によって表される値を指定します。
  1 つの変数に対して複数のポート番号を指定するには、エントリをカンマで区切ります。たとえば、80, 3128, 8000, 8010, 8080, 8888, 24326 のように指定します。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

シグニチャ変数の設定

シグニチャ変数を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Variables** をクリックします。

Signature Variables パネルが表示されます。

ステップ 3　**Add** をクリックして、変数を追加します。

Add Signature Variable ダイアログボックスが表示されます。

ステップ 4　**Name** フィールドに、シグニチャ変数の名前を入力します。

（注）　名前には、数字または文字だけを使用できます。ハイフン（-）または下線（_）は使用できます。

ステップ 5　**Value** フィールドに、新しいシグニチャ変数の値を入力します。

（注）　デリミタにはカンマが使用できます。カンマの後にはスペースを入れないでください。スペースを入力すると、`Validation failed` エラーが生じます。

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。

ステップ 6　**OK** をクリックします。

Signature Variables パネルのシグニチャ変数リストに、新しい変数が表示されます。

ステップ 7　シグニチャ変数リストにある既存の変数を編集するには、それを選択して **Edit** をクリックします。

選択した変数の Edit Signature Variable ダイアログボックスが表示されます。

ステップ 8　**Value** フィールドで必要な変更を行います。

ステップ 9　**OK** をクリックします。

Signature Variables パネルのシグニチャ変数リストに、編集された変数が表示されます。

ステップ 10　シグニチャ変数リストにある既存の変数を削除するには、それを選択して **Delete** をクリックします。

削除された変数は、Signature Variables パネルのシグニチャ変数リストに表示されなくなります。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 11　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャの設定

この項では、シグニチャの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.5-6）
- サポートされるユーザのロール（P.5-6）
- フィールド定義（P.5-7）
- シグニチャの追加（P.5-17）
- シグニチャの複製（P.5-19）
- シグニチャのチューニング（P.5-21）
- シグニチャのイネーブル化とディセーブル化（P.5-22）
- シグニチャのアクティブ化とリタイア化（P.5-23）
- シグニチャへのアクションの割り当て（P.5-24）

概要

Signature Configuration パネルでは、次の作業を実行できます。

- センサーに保存されているすべてのシグニチャのソートと表示。

  攻撃タイプ、プロトコル、サービス、オペレーティング システム、実行するアクション、エンジン、シグニチャ ID、シグニチャ名によるソートが可能です。
- 選択したシグニチャに関する NSDB 情報の表示。

  NSDB ページには、選択したシグニチャのキー アトリビュート、説明、良性トリガー、および推奨されるフィルタが表示されます。
- 既存のシグニチャのパラメータに関連付けられた値（複数可）を変更する、編集（チューニング）。
- 既存のシグニチャを複製し、そのシグニチャのパラメータを新しいシグニチャの始点として使用する方法、または最初から新しいシグニチャを作成する方法のいずれかによる、シグニチャの作成。

  Custom Signature Wizard を使用してシグニチャを作成することもできます。このウィザードは、適切なシグニチャ エンジンの選択のほか、カスタム シグニチャを設定するために必要なパラメータの選択を手引きします。
- 既存のシグニチャのイネーブル化またはディセーブル化。
- シグニチャのデフォルトの復元。
- カスタム シグニチャの削除。

  組み込みシグニチャは削除できません。
- 既存のシグニチャのアクティブ化またはリタイア化。
- シグニチャへのアクションの割り当て。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

シグニチャを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、シグニチャ変数のフィールド定義を示します。取り上げる事項は次のとおりです。

- Signature Configuration パネル（P.5-7）
- Add Signatures ダイアログボックス（P.5-8）
- Clone and Edit Signature ダイアログボックス（P.5-12）
- Assign Actions ダイアログボックス（P.5-16）

Signature Configuration パネル

Signature Configuration パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Select By**：プロトコル、サービス、またはアクションなどソートするアトリビュートを選択して、シグニチャ リストをソートします。
- **Select Criteria**：カテゴリ内のクラスを選択して、カテゴリ内の詳細なソートを実行します。

  たとえば、プロトコルによるソートを選択した場合、L2/L3/L4 プロトコルを選択でき、L2/L3/L4 プロトコルに関連するシグニチャのみを表示できます。
- **Sig ID**：このシグニチャに割り当てられた固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。
- **SubSig ID**：このサブシグニチャに割り当てられた固有の数値を示します。

  SubSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。
- **Name**：このシグニチャに割り当てる名前を示します。
- **Enabled**：このシグニチャがイネーブルであるかどうかを示します。

  シグニチャによって指定されたトラフィックをセンサーが保護するようにするには、シグニチャをイネーブルにする必要があります。
- **Action**：このシグニチャが反応したときにセンサーが行うアクションを示します。
- **Severity**：シグニチャが報告する重大度（High、Informational、Low、Medium）を示します。
- **Fidelity Rating**：対象とする特定の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値を示します。
- **Base RR**：各シグニチャの基本リスク評価値を表示します。IDM は、忠実度評価と重大度要素を掛けたものを 100 で割って（Fidelity Rating x Severity Factor /100）、基本 RR を自動的に計算します。

  Severity Factor には次の値があります。

  - Severity Factor = 100（シグニチャの重大度が high の場合）
  - Severity Factor = 75（シグニチャの重大度が medium の場合）
  - Severity Factor = 50（シグニチャの重大度が low の場合）
  - Severity Factor = 25（シグニチャの重大度が informational の場合）
- **Type**：このシグニチャがデフォルト（組み込み）、チューニング済み、またはカスタム シグニチャであるかどうかを示します。
- **Engine**：このシグニチャによって指定されたトラフィックを解析および検査するエンジンを示します。
- **Retired**：このシグニチャがリタイアであるかどうかを示します。

  リタイアにしたシグニチャは、シグニチャ エンジンから削除されます。リタイアにしたシグニチャをアクティブにして、シグニチャ エンジンに戻すことができます。

ボタンの機能：

- **Select All**：すべてのシグニチャを選択します。

- **NSDB Link**：選択したシグニチャの NSDB ページを開きます。

  NSDB ページには、選択したシグニチャのキー アトリビュート、説明、良性トリガー、および推奨されるフィルタが表示されます。
- **Add**：Add Signature ダイアログボックスを開きます。

  このダイアログボックスで、適切なパラメータを選択してシグニチャを作成できます。
- **Clone**：Clone Signature ダイアログボックスを開きます。

  このダイアログボックスで、複製元である既存シグニチャの設定済みの値を変更して、シグニチャを作成できます。
- **Edit**：Edit Signature ダイアログボックスを開きます。

  このダイアログボックスで、選択したシグニチャに関連付けらたパラメータを変更し、効率的にシグニチャをチューニングできます。

  一度に編集できるシグニチャは 1 つだけです。
- **Enable**：選択したシグニチャをイネーブルにします。
- **Disable**：選択したシグニチャをディセーブルにします。
- **Actions**：Assign Actions ダイアログボックスを表示します。
- **Restore Defaults**：すべてのパラメータを、選択したシグニチャのデフォルト設定に戻します。
- **Delete**：選択したカスタム シグニチャを削除します。

  組み込みシグニチャは削除できません。
- **Activate**：選択したシグニチャがリタイアになっている場合、アクティブにします。

  このプロセスは、センサーがシグニチャを該当するシグニチャ エンジンに戻し、シグニチャ エンジンを再構築する必要があるため、少々時間がかかる場合があります。
- **Retire**：選択したシグニチャをリタイアにし、シグニチャ エンジンから削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に保存した値で置き換えてパネルをリフレッシュします。

Add Signatures ダイアログボックス

Add Signature ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。この値を使用すると、センサーが特定のシグニチャを識別できます。

  値は 1000 ～ 65000 です。
- **SubSignature　ID**：このサブシグニチャに割り当てられた固有の数値を示します。サブシグニチャ ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。

  値は 0 ～ 255 です。
- **Alert Severity**：シグニチャの重大度レベルを選択します（High、Informational、Low、Medium）。
- **Sig Fidelity Rating**：対象とする特定の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値を選択します。

  値は 0 ～ 100 です。デフォルトは 75 です。
- **Promiscuous Delta**：アラートの重大度を決定します。
- **Sig　Description**：このシグニチャをその他のシグニチャと区別するために次のアトリビュートを指定します。
  - **Signature Name**：シグニチャの名前。デフォルトは MySig です。
  - **Alert Notes**：このフィールドにはアラートの注釈を加えます。
  - **User Comments**：このフィールドにはシグニチャについてのコメントを加えます。

- **Alarm Traits**：このフィールドにはアラーム特性を指定します。値は 0 ～ 65535 です。デフォルトは 0 です。
- **Release**：シグニチャが最初に現れたソフトウェア リリースを指定します。

- **Engine**：シグニチャによって指定されたトラフィックを解析および検査するエンジンを選択します。
  - **AIC FTP**：FTP トラフィックを検査します。発行されているコマンドを制御できます。
  - **AIC HTTP**：HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。
  - **Atomic ARP**：レイヤ 2 ARP プロトコルを検査します。ほとんどのエンジンはレイヤ 3 IP に基づいているため、Atomic ARP エンジンはその他の大半のエンジンとは異なっています。
  - **Atomic IP**：IP プロトコル パケットと関連付けられたレイヤ 4 転送プロトコルを検査します。
  - **Flood Host**：ホストを宛先とする ICMP および UDP フラッドを検出します。
  - **Flood Net**：ネットワークを宛先とする ICMP および UDP フラッドを検出します。
  - **Meta**：スライドする時間間隔内で、関連する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して複数の文字列を照合することでレイヤ 4 転送プロトコル（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。シグニチャを生成するために一致している必要のある一連の正規表現パターンを指定できます。
  - **Normalizer**：IP および TCP 正規化エンジンがどのように機能するかを設定し、IP および TCP 正規化エンジンに関連するシグニチャ イベントの設定を行います。RFC に準拠させることができます。
  - **Service DNS**：DNS（TCP および UDP）トラフィックを検査します。
  - **Service FTP**：FTP トラフィックを検査します。
  - **Service Generic**：カスタム サービスとペイロードをデコードします。
  - **Service H225**：VoIP トラフィックを検査します。
  - **Service HTTP**：HTTP トラフィックを検査します。WEBPORTS 変数が HTTP トラフィックの検査ポートを定義します。
  - **Service 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。
  - **Service MSRPC**：MSRPC トラフィックを検査します。
  - **Service MSSQL**：Microsoft SQL トラフィックを検査します。
  - **Service NTP**：NTP トラフィックを検査します。
  - **Service RPC**：RPC トラフィックを検査します。
  - **Service SMB**：SMB トラフィックを検査します。
  - **Service SNMP**：SNMP トラフィックを検査します。
  - **Service SSH**：SSH 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をステートフル検索します。
  - **String ICMP**：ICMP プロトコルに基づいて正規表現文字列を検索します。
  - **String TCP**：TCP プロトコルに基づいて正規表現文字列を検索します。
  - **String UDP**：UDP プロトコルに基づいて正規表現文字列を検索します。
  - **Sweep**：1 つのホスト（ICMP および TCP）、宛先ポート（TCP および 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、ポート、ホスト、およびサービスのスイープを分析します。
  - **Sweep Other TCP**：1 つのホストに関する情報を取得しようとしている監視スキャンから TCP フラグの組み合せを分析します。シグニチャは、フラグ A、B、および C を監視します。3 つのフラグがすべて検出されると、アラートを生成します。

- **Traffic ICMP**：TFN2K、LOKI、および DDOS など、非標準のプロトコルを解析します。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**：非標準プロトコルの BO2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan Tfn2k**：非標準プロトコルの TFN2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan UDP**：UDP プロトコルからのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。

• **Event Action**：センサーがイベントに応答するときに実行するアクションを割り当てます。

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

  センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

  （注） これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

- **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

  （注） 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。

- **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

(注)　ブロック　アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

(注)　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Event Counter**：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、同じシグニチャが同じアドレス セットに対して 5 回カウントを実行した場合にだけ、センサーがアラートを送信するように指定できます。
  - **Event Count**：アラートを生成するまでのイベントの発生回数。値は 1 ～ 65535 です。デフォルトは 1 です。
  - **Event Count Key：シグニチャのイベントをカウントするために使用するストレージ タイプ。**攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Alert Interval**：イベント カウントをリセットするまでの秒数を指定します。**Yes または No を選択してから、時間を指定します。**
- **Alert Frequency**：シグニチャの動作中にセンサーがアラートを生成する頻度を設定します。次のパラメータをシグニチャに指定します。
  - **Summary Mode**：アラート要約のモード。Fire All、Fire Once、Global Summarize、または Summarize を選択します。
  - **Summary Interval**：各サマリー アラートを生成する間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。

- **Summary Key**：アラートの要約に使用するストレージ タイプ。攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
- **Specify Global Summary Threshold：グローバル サマリーにアラートを組み込むためのイベント数のしきい値を指定します。Yes** または **No** を選択してから、時間を指定します。

- **Status**：シグニチャをイネーブルまたはディセーブルにするか、シグニチャをリタイアまたは非リタイアにします。
  - **Enabled**：シグニチャをイネーブルまたはディセーブルのどちらにするかを選択します。デフォルトは yes です。
  - **Retired**：シグニチャをリタイアにするかどうかを選択します。デフォルトは no です。

Clone and Edit Signature ダイアログボックス

Clone and Edit Signature ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。この値を使用すると、センサーが特定のシグニチャを識別できます。

  値は 1000 ～ 65000 です。
- **SubSignature　ID**：このサブシグニチャに割り当てられた固有の数値を示します。サブシグニチャ ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。

  値は 0 ～ 255 です。
- **Alert Severity**：シグニチャの重大度レベルを選択します（High、Informational、Low、Medium）。
- **Sig Fidelity Rating**：対象とする特定の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値を選択します。

  値は 0 ～ 100 です。デフォルトは 75 です。
- **Promiscuous Delta**：アラートの重大度を決定します。
- **Sig　Description**：このシグニチャをその他のシグニチャと区別するために次のアトリビュートを指定します。
  - **Signature Name**：シグニチャの名前。デフォルトは MySig です。
  - **Alert Notes**：このフィールドにはアラートの注釈を加えます。
  - **User Comments**：このフィールドにはシグニチャについてのコメントを加えます。
  - **Alarm Traits**：このフィールドにはアラーム特性を指定します。値は 0 ～ 65535 です。デフォルトは 0 です。
  - **Release**：シグニチャが最初に現れたソフトウェア リリースを指定します。
- **Engine**：シグニチャによって指定されたトラフィックを解析および検査するエンジンを選択します。
  - **AIC FTP**：FTP トラフィックを検査します。発行されているコマンドを制御できます。
  - **AIC HTTP**：HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。
  - **Atomic ARP**：レイヤ 2 ARP プロトコルを検査します。ほとんどのエンジンはレイヤ 3 IP に基づいているため、Atomic ARP エンジンはその他の大半のエンジンとは異なっています。
  - **Atomic IP**：IP プロトコル パケットと関連付けられたレイヤ 4 転送プロトコルを検査します。
  - **Flood Host**：ホストを宛先とする ICMP および UDP フラッドを検出します。
  - **Flood Net**：ネットワークを宛先とする ICMP および UDP フラッドを検出します。

- **Meta**：スライドする時間間隔内で、関連する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して複数の文字列を照合することでレイヤ 4 転送プロトコル（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。シグニチャを生成するために一致している必要のある一連の正規表現パターンを指定できます。
- **Normalizer**：IP および TCP 正規化エンジンがどのように機能するかを設定し、IP および TCP 正規化エンジンに関連するシグニチャ イベントの設定を行います。RFC に準拠させることができます。
- **Service DNS**：DNS（TCP および UDP）トラフィックを検査します。
- **Service FTP**：FTP トラフィックを検査します。
- **Service Generic**：カスタム サービスとペイロードをデコードします。
- **Service H225**：VoIP トラフィックを検査します。
- **Service HTTP**：HTTP トラフィックを検査します。WEBPORTS 変数が HTTP トラフィックの検査ポートを定義します。
- **Service 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。
- **Service MSRPC**：MSRPC トラフィックを検査します。
- **Service MSSQL**：Microsoft SQL トラフィックを検査します。
- **Service NTP**：NTP トラフィックを検査します。
- **Service RPC**：RPC トラフィックを検査します。
- **Service SMB**：SMB トラフィックを検査します。
- **Service SNMP**：SNMP トラフィックを検査します。
- **Service SSH**：SSH 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をステートフル検索します。
- **String ICMP**：ICMP プロトコルに基づいて正規表現文字列を検索します。
- **String TCP**：TCP プロトコルに基づいて正規表現文字列を検索します。
- **String UDP**：UDP プロトコルに基づいて正規表現文字列を検索します。
- **Sweep**：1 つのホスト（ICMP および TCP）、宛先ポート（TCP および 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、ポート、ホスト、およびサービスのスイープを分析します。
- **Sweep Other TCP**：1 つのホストに関する情報を取得しようとしている監視スキャンから TCP フラグの組み合せを分析します。シグニチャは、フラグ A、B、および C を監視します。3 つのフラグがすべて検出されると、アラートを生成します。
- **Traffic ICMP**：TFN2K、LOKI、および DDOS など、非標準のプロトコルを解析します。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**：非標準プロトコルの BO2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan Tfn2k**：非標準プロトコルの TFN2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan UDP**：UDP プロトコルからのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。

• **Event Action**：センサーがイベントに応答するときに実行するアクションを割り当てます。

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

  センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行

されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

(注) これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

- **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

(注) 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。
- **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

(注) ブロック アクションの場合、ブロックの期間を設定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Event Counter**：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、同じシグニチャが同じアドレス セットに対して 5 回カウントを実行した場合にだけ、センサーがアラートを送信するように指定できます。
  - **Event Count**：アラートを生成するまでのイベントの発生回数。値は 1 ～ 65535 です。デフォルトは 1 です。
  - **Event Count Key：シグニチャのイベントをカウントするために使用するストレージ タイプ。**攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Alert Interval**：イベント カウントをリセットするまでの秒数を指定します。**Yes または No を選択してから、時間を指定します。**
- **Alert Frequency**：シグニチャの動作中にセンサーがアラートを生成する頻度を設定します。次のパラメータをシグニチャに指定します。
  - **Summary Mode**：アラート要約のモード。Fire All、Fire Once、Global Summarize、または Summarize を選択します。
  - **Summary Interval**：各サマリー アラートを生成する間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。
  - **Summary Key**：アラートの要約に使用するストレージ タイプ。攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Global Summary Threshold：グローバル サマリーにアラートを組み込むためのイベント数のしきい値を指定します。Yes** または **No** を選択してから、時間を指定します。
- **Status**：シグニチャをイネーブルまたはディセーブルにするか、シグニチャをリタイアまたは非リタイアにします。
  - **Enabled**：シグニチャをイネーブルまたはディセーブルのどちらにするかを選択します。デフォルトは yes です。
  - **Retired**：シグニチャをリタイアにするかどうかを選択します。デフォルトは no です。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

Assign Actions ダイアログボックス

Assign Actions ダイアログボックスには、次のフィールドとボタンがあります。

イベント アクションとは、イベントに対するセンサーの応答です。イベント アクションは、シグニチャごとに設定可能です。

フィールドの説明：

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

  センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

  （注） これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

  - **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

  （注） 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

  - **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
  - **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
  - **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
  - **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
  - **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
  - **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。
  - **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。

— **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

— **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注） ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

— **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注） Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

— **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。

— **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

ボタンの機能：

- **Select All**：リストにあるすべてのイベント アクションを選択します。
- **Select None**：すべてのイベント アクションの選択をクリアします。

シグニチャの追加

シグニチャを追加するには、次の手順を実行します。

ヒント + アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータが現在デフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　既存のシグニチャを使用しないでカスタム シグニチャを追加するには、次の手順を実行します。

a. **Add** をクリックして、Add Signature ダイアログボックスを開きます。
b. **Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。
c. **Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。
d. **Alert Severity** フィールドの隣にある緑のアイコンをクリックし、シグニチャに関連付ける重大度を選択します。
e. **Signature Fidelity Rating** フィールドの隣にある緑のアイコンをクリックし、シグニチャのシグニチャ忠実度評価を表す値（1 ～ 100）を指定します。
f. シグニチャ説明フィールドにシグニチャに関するコメントを入力します。
g. センサーがこのシグニチャを有効にするために使用するエンジンを選択します。

（注）　選択するエンジンが不明な場合、Custom Signature Wizard を使用してカスタム シグニチャを作成してください。詳細については、P.6-22 の「カスタム シグニチャの作成」を参照してください。

h. **Event Actions** フィールドの横にある緑色のアイコンをクリックし、センサーがイベントに応答するときに起こすアクションを選択します。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押した状態で選択します。

i. イベントをカウントする場合は、Event Counter の下にある **Event Counter** フィールドを設定します。
j. Alert Frequency の下にある **Alert Frequency** フィールドで、アラートを受信する方法を指定します。
k. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

l. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント　変更を元に戻し、Add Signature ダイアログを閉じるには、**Cancel** をクリックします。

m. **OK** をクリックします。

Type が Custom に設定された新しいシグニチャがリストに現れます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 4　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャの複製

Signature Configuration パネルでは、既存のシグニチャを複製する方法でシグニチャを作成できます。既存のシグニチャと類似したシグニチャを作成する場合、この方法が便利です。

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータが現在デフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

シグニチャを複製するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　既存のシグニチャをベースとして使用する方法でシグニチャを作成するには、既存のシグニチャを選択し、次の手順を実行します。

a. **Clone** をクリックして、Clone Signature ダイアログボックスを開きます。

b. **Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。

c. **Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。

d. パラメータの値を確認し、新しいシグニチャ用に変更する場合はパラメータの値を変更します。

ヒント　複数のイベント アクションを選択するには、**Ctrl** キーを押した状態で選択します。

e. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

f. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント　変更を元に戻し、Clone Signature ダイアログボックスを閉じるには、**Cancel** をクリックします。

g. **OK** をクリックします。

Type が Custom に設定されている、複製されたシグニチャがリストに表示されます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのチューニング

シグニチャをチューニングするには、次の手順を実行します。

ヒント + アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータが現在デフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 1 管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3 シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4 既存のシグニチャをチューニングするには、シグニチャを選択し、次の手順を実行します。

a. **Edit** をクリックして、Edit Signature ダイアログボックスを開きます。

b. パラメータの値を確認し、チューニングするパラメータの値を変更します。

ヒント 複数のイベント アクションを選択するには、**Ctrl** キーを押した状態で選択します。

c. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

(注) シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

d. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

(注) シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント 変更を元に戻し、Edit Signature ダイアログボックスを閉じるには、**Cancel** をクリックします。

e. **OK** をクリックします。

Type が Custom に設定されている、編集されたシグニチャがリストに表示されます。

ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのイネーブル化とディセーブル化

シグニチャ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 管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3 シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4 既存のシグニチャをイネーブルまたはディセーブルにするには、シグニチャを選択し、次の手順を実行します。

a. Enabled カラムを表示し、シグニチャのステータスを判断します。イネーブルになっているシグニチャは、このカラムが Yes になっています。

b. ディセーブルになっているシグニチャをイネーブルにするには、シグニチャを選択し、**Enable** をクリックします。

c. イネーブルになっているシグニチャをディセーブルにするには、シグニチャを選択し、**Disable** をクリックします。

ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのアクティブ化とリタイア化

注意　シグニチャのアクティブ化およびリタイア化は、非常に時間を要する作業で、30 分以上かかる場合もあります。

シグニチャをアクティブまたはリタイアにするには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　リタイアになっているシグニチャをアクティブにするには、シグニチャを選択し、**Activate** をクリックします。

ステップ 5　アクティブになっているシグニチャをリタイアにするには、シグニチャを選択し、**Retire** をクリックします。

（注）　シグニチャをリタイアにすると、そのシグニチャはエンジンから削除されますが、シグニチャ コンフィギュレーション リストには保持されます。リタイアにしたシグニチャを後でアクティブにできますが、そのためにはセンサーがエンジンのシグニチャ リストを再構築する必要があり、シグニチャ処理が遅れる可能性があります。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 6　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャへのアクションの割り当て

シグニチャにアクションを割り当てるには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Signature Definition** > **Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　シグニチャまたはシグニチャ セットにアクションを割り当てるには、シグニチャを選択し、**Actions** をクリックします。

Assign Actions ダイアログボックスが表示されます。

a.　シグニチャに割り当てるアクションを選択します。

チェック マークが付いている場合は、そのアクションが選択したシグニチャに割り当てられていることを示します。チェック マークが付いていない場合は、そのアクションが選択したシグニチャのどれにも割り当てられていないことを示します。灰色のチェック マークが付いている場合は、そのアクションが選択したシグニチャのどれかに割り当てられていることを示します。

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

  センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

  （注）　これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

  — **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

（注）拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。
- **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。

－ **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

ヒント 複数のアクションを選択するには、**Ctrl** キーを押した状態で選択します。

b. 選択したシグニチャにすべてのアクションを割り当てる場合は、**All** をクリックします。または、選択したシグニチャからすべてのアクションを削除する場合は、**None** を選択します。

ヒント 変更を元に戻し、Assign Actions ダイアログボックスを閉じるには、**Cancel** をクリックします。

c. 変更内容を保存してダイアログボックスを閉じるには、**OK** をクリックします。

新しいアクションが Action カラムに表示されます。

Miscellaneous パネルの設定

この項では、Miscellaneous パネルの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.5-27）
- サポートされるユーザのロール（P.5-27）
- フィールド定義（P.5-28）
- アプリケーション ポリシーの設定（P.5-28）
- IP フラグメント再構成の設定（P.5-37）
- TCP ストリーム再構成の設定（P.5-40）
- IP ロギングの設定（P.5-44）

概要

Miscellaneous パネルでは、次の作業を実行できます。

- アプリケーション ポリシー パラメータの設定。

  センサーは、Web サービス関連の悪意のある攻撃を防ぐために、レイヤ 4 ～ レイヤ 7 のパケット検査を行うように設定できます。

- IP フラグメント再構成オプションの設定。

  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、データグラムの数と、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が指定できます。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。

- TCP ストリーム再構成の設定。

  センサーは、完全な 3 ウェイ ハンドシェイクによって確立された TCP セッションだけを監視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監視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 セッションの再組み立て機能は、センサーに対するこのような攻撃の緩和に役立ちます。

- IP ロギング オプションの設定。

  センサーは、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反応すると、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ログに記録されます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

Miscellaneous パネルでパラメータを設定するには、管理者またはオペレータである必要があります。

フィールド定義

Miscellaneous パネルには、次のフィールドとボタンがあります。

- **Application Policy**：アプリケーション ポリシーの実施を設定します。
  - **Enable HTTP** ：Web サービスの保護をイネーブルにします。HTTP トラフィックが RFC に準拠しているかどうかをセンサーが検査するようにするには、**Yes** を選択します。
  - **Max HTTP Requests**：未処理の HTTP 要求の最大数（1 接続あたり）を指定します。
  - **AIC Web Ports**：AIC トラフィックを監視するポートの変数を指定します。
  - **Enable FTP** ：Web サービスの保護をイネーブルにします。センサーが FTP トラフィックを検査するようにするには、**Yes** を選択します。
- **Fragment Reassembly**：IP フラグメント再構成を設定します。
  - **IP Reassembly Mode**：センサーが使用する、オペレーティング システムに基づくフラグメントの再構成方法を指定します。
- **Stream Reassembly**：TCP ストリーム再構成を設定できます。
  - **TCP Handshake Required**：センサーが、3 ウェイ ハンドシェイクが完了したセッションのみを追跡するように指定します。
  - **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、次のオプション付きで指定します。

    Asymmetric：双方向のトラフィック フローの一方向のみを対象にします。

    （注） Asymmetric モードでは、センサーはトラフィック フローの状態と同期をとり、双方向のうち一方向だけでよいエンジンの検査を継続します。完全に保護するには、トラフィックの双方向を対象にする必要があるため、Asymmetric モードではセキュリティが低下します。

    Strict：何らかの理由でパケットを受信しなかった場合、以後のパケットはすべて処理しません。

    Loose：パケットが廃棄される可能性がある場合に使用します。
- **IP Log**：次のいずれかの条件が満たされた場合、センサーが IP ロギングを停止するように設定します。
  - **Max IP Log Packets**：ログを作成するパケットの数を指定します。
  - **IP Log Time**：ログを作成する時間を指定します。有効な値は、1 ～ 60 秒です。デフォルトは 30 秒です。
  - **Max IP Log Bytes**：ログを作成する最大バイト数を指定します。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

アプリケーション ポリシーの設定

この項では、Application Policy（AIC）シグニチャとその設定方法について説明します。シグニチャ エンジンの詳細については、P.B-9 の「AIC エンジン」を参照してください。この項で取り上げる事項は次のとおりです。

- 概要（P.5-29）
- AIC 要求メソッド シグニチャ（P.5-30）
- AIC MIME 定義コンテンツ タイプ シグニチャ（P.5-31）

- AIC 転送符号化シグニチャ（P.5-34）
- AIC FTP コマンド シグニチャ（P.5-34）
- アプリケーション ポリシーの設定（P.5-35）
- 認識済みの定義コンテンツ タイプ（MIME）シグニチャの例（P.5-36）

概要

AIC は Web トラフィックの詳細分析を行います。HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。たとえば、インスタント メッセージや、gotomypc などのトンネリング アプリケーションなど、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。これらのアプリケーションが HTTP を介して稼働している場合は、P2P およびインスタント メッセージの検査とポリシー チェックを実行できます。

AIC は、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方法を提供します。

事前定義されたシグニチャをイネーブルまたはディセーブルにすることもできますし、カスタム シグニチャでポリシーを作成することもできます。

（注） AIC エンジンは、HTTP トラフィックが AIC Web ポートで受信されたときに実行されます。トラフィックが Web トラフィックであっても、AIC Web ポートで受信されない場合は、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ている任意のポートで実行できます。検査されるトラフィックは HTTP トラフィックです。

AIC には、次のシグニチャのカテゴリがあります。

- HTTP 要求メソッド
  - 定義要求メソッド
  - 認識済み要求メソッド

  シグニチャ ID のリストとその説明については、AIC 要求メソッド シグニチャ（P.5-30）を参照してください。
- 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

  シグニチャ ID のリストとその説明については、P.5-31 の「AIC MIME 定義コンテンツ タイプ シグニチャ」を参照してください。カスタム MIME シグニチャを作成する手順については、P.5-36 の「認識済みの定義コンテンツ タイプ（MIME）シグニチャの例」を参照してください。
- 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場合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です。
- 転送符号化
  - アクションと各メソッドを関連付けます。
  - センサーが認識済みのメソッドのリストを表示します。
  - チャンク符号化エラーが検出された場合に実行する必要のあるアクションを指定します。

  シグニチャ ID のリストとその説明については、P.5-34 の「AIC 転送符号化シグニチャ」を参照してください。

- FTP コマンド

  アクションを FTP コマンドに関連付けます。シグニチャ ID のリストとその説明については、P.5-34 の「AIC FTP コマンド シグニチャ」を参照してください。

AIC 要求メソッド シグニチャ

HTTP 要求メソッドには 2 つのシグニチャのカテゴリがあります。

- 定義要求メソッド：アクションと要求メソッドの関連付けを可能にします。シグニチャを拡張し変更できます（Define Request Method）。
- 認識済み要求メソッド：センサーが認識済みのメソッドのリストを表示します（Recognized Request Methods）。

表 5-1 は、事前定義済みの定義要求メソッド シグニチャを示しています。必要とする事前定義済みのメソッドを持つシグニチャをイネーブルにしてください。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-1　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ていない
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
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

AIC MIME 定義コンテンツ タイプ シグニチャ

MIME タイプには 2 つのポリシーが関連付けられています。

- 定義コンテンツ タイプ：次の場合に特定のアクションを関連付けます（Define Content Type）。
  - image/jpeg などの特定の MIME タイプを拒否する
  - メッセージ サイズ違反
  - ヘッダーと本体に記述された MIME タイプが一致しない
- 認識されるコンテンツ タイプ（Recognized Content Type）

表 5-2 は、事前定義済みの定義コンテンツ タイプ シグニチャを示しています。必要とする事前定義済みのメソッドを持つシグニチャをイネーブルにしてください。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。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。手順については、P.5-36 の「認識済みの定義コンテンツ タイプ（MIME）シグニチャの例」を参照してください。

表 5-2　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。
12624 0 12624 1 12624 2	コンテンツ タイプ image/x-3ds のヘッダー チェック。 コンテンツ タイプ image/x-3ds のメッセージ長が無効です。 コンテンツ タイプ image/x-3ds の検証に失敗しました。
12626 0 12626 1 12626 2	コンテンツ タイプ image/x-portable-bitmap のヘッダー チェック。 コンテンツ タイプ image/x-portable-bitmap のメッセージ長が無効です。 コンテンツ タイプ image/x-portable-bitmap の検証に失敗しました。
12627 0 12627 1 12627 2	コンテンツ タイプ image/x-portable-graymap のヘッダー チェック。 コンテンツ タイプ image/x-portable-graymap のメッセージ長が無効です。 コンテンツ タイプ image/x-portable-graymap の検証に失敗しました。
12628 0 12628 1 12628 2	コンテンツ タイプ image/jpeg のヘッダー チェック。 コンテンツ タイプ image/jpeg のメッセージ長が無効です。 コンテンツ タイプ image/jpeg の検証に失敗しました。
12629 0 12629 1	コンテンツ タイプ image/cgf のヘッダー チェック。 コンテンツ タイプ image/cgf のメッセージ長が無効です。
12631 0 12631 1	コンテンツ タイプ image/x-xpm のヘッダー チェック。 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 12633 1 12633 2	コンテンツ タイプ audio/midi のヘッダー チェック。 コンテンツ タイプ audio/midi のメッセージ長が無効です。 コンテンツ タイプ audio/midi の検証に失敗しました。
12634 0 12634 1 12634 2	コンテンツ タイプ audio/basic のヘッダー チェック。 コンテンツ タイプ audio/basic のメッセージ長が無効です。 コンテンツ タイプ audio/basic の検証に失敗しました。
12635 0 12635 1 12635 2	コンテンツ タイプ audio/mpeg のヘッダー チェック。 コンテンツ タイプ audio/mpeg のメッセージ長が無効です。 コンテンツ タイプ audio/mpeg の検証に失敗しました。

表 5-2　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
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。
12644 0	コンテンツ タイプ text/plain のヘッダー チェック。
12644 1	コンテンツ タイプ text/richtext のメッセージ長が無効です。
12645 0	コンテンツ タイプ text/sgml のヘッダー チェック。
12645 1	コンテンツ タイプ text/sgml のメッセージ長が無効です。
12645 2	コンテンツ タイプ text/sgml の検証に失敗しました。
12646 0	コンテンツ タイプ text/xml のヘッダー チェック。
12646 1	コンテンツ タイプ text/xml のメッセージ長が無効です。
12646 2	コンテンツ タイプ text/xml の検証に失敗しました。
12648 0	コンテンツ タイプ video/flc のヘッダー チェック。
12648 1	コンテンツ タイプ video/flc のメッセージ長が無効です。
12648 2	コンテンツ タイプ video/flc の検証に失敗しました。
12649 0	コンテンツ タイプ video/mpeg のヘッダー チェック。
12649 1	コンテンツ タイプ video/mpeg のメッセージ長が無効です。
12649 2	コンテンツ タイプ video/mpeg の検証に失敗しました。
12650 0	コンテンツ タイプ text/xmcd のヘッダー チェック。
12650 1	コンテンツ タイプ text/xmcd のメッセージ長が無効です。
12651 0	コンテンツ タイプ video/quicktime のヘッダー チェック。
12651 1	コンテンツ タイプ video/quicktime のメッセージ長が無効です。
12651 2	コンテンツ タイプ video/quicktime の検証に失敗しました。
12652 0	コンテンツ タイプ video/sgi のヘッダー チェック。
12652 1	コンテンツ タイプ video/sgi の検証に失敗しました。
12653 0	コンテンツ タイプ video/x-avi のヘッダー チェック。
12653 1	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	コンテンツ タイプ video/x-fli のヘッダー チェック。
12654 1	コンテンツ タイプ video/x-fli のメッセージ長が無効です。
12654 2	コンテンツ タイプ video/x-fli の検証に失敗しました。

表 5-2　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
12655 0	コンテンツ タイプ video/x-mng のヘッダー チェック。
12655 1	コンテンツ タイプ video/x-mng のメッセージ長が無効です。
12655 2	コンテンツ タイプ video/x-mng の検証に失敗しました。
12656 0	コンテンツ タイプ application/x-msvideo のヘッダー チェック。
12656 1	コンテンツ タイプ application/x-msvideo のメッセージ長が無効です。
12656 2	コンテンツ タイプ application/x-msvideo の検証に失敗しました。
12658 0	コンテンツ タイプ application/ms-word のヘッダー チェック。
12658 1	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	コンテンツ タイプ application/octet-stream のヘッダー チェック。
12659 1	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	コンテンツ タイプ application/postscript のヘッダー チェック。
12660 1	コンテンツ タイプ application/postscript のメッセージ長が無効です。
12660 2	コンテンツ タイプ application/postscript の検証に失敗しました。
12661 0	コンテンツ タイプ application/vnd.ms-excel のヘッダー チェック。
12661 1	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	コンテンツ タイプ application/vnd.ms-powerpoint のヘッダー チェック。
12662 1	コンテンツ タイプ application/vnd.ms-powerpoint のメッセージ長が無効です。
12663 0	コンテンツ タイプ application/zip のヘッダー チェック。
12663 1	コンテンツ タイプ application/zip のメッセージ長が無効です。
12663 2	コンテンツ タイプ application/zip の検証に失敗しました。
12664 0	コンテンツ タイプ application/x-gzip のヘッダー チェック。
12664 1	コンテンツ タイプ application/x-gzip のメッセージ長が無効です。
12664 2	コンテンツ タイプ application/x-gzip の検証に失敗しました。
12665 0	コンテンツ タイプ application/x-java-archive のヘッダー チェック。
12665 1	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	コンテンツ タイプ application/x-java-vm のヘッダー チェック。
12666 1	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	コンテンツ タイプ application/pdf のヘッダー チェック。
12667 1	コンテンツ タイプ application/pdf のメッセージ長が無効です。
12667 2	コンテンツ タイプ application/pdf の検証に失敗しました。
12668 0	コンテンツ タイプ unknown のヘッダー チェック。
12668 1	コンテンツ タイプ unknown のメッセージ長が無効です。
12669 0	コンテンツ タイプ image/x-bitmap のヘッダー チェック。
12669 1	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

AIC 転送符号化シグニチャ

転送符号化に関連するポリシーは 3 つあります。

- アクションを各メソッドと関連付ける（Define Transfer Encoding）
- センサーによって認識されたメソッドをリストする（Recognized Transfer Encodings）
- チャンク符号化エラーが検出された場合に、どのアクションを実行するかを指定する（Chunked Transfer Encoding Error）

表 5-3 は、事前定義済みの転送符号化シグニチャを示しています。必要な事前定義済み転送符号化メソッドがあるシグニチャをイネーブルにします。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-3　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	Recognized Transfer Encoding
12687	Define Transfer Encoding Deflate
12688	Define Transfer Encoding Identity
12689	Define Transfer Encoding Compress
12690	Define Transfer Encoding GZIP
12693	Define Transfer Encoding Chunked
12694	Chunked Transfer Encoding Error

AIC FTP コマンド シグニチャ

表 5-4 は、事前定義済みの FTP コマンド シグニチャを示しています。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。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-4　FTP コマンド シグニチャ

シグニチャ ID	FTP コマンド
12900	認識されていない FTP コマンド
12901	FTP コマンド abor の定義
12902	FTP コマンド acct の定義
12903	FTP コマンド allo の定義
12904	FTP コマンド appe の定義
12905	FTP コマンド cdup の定義
12906	FTP コマンド cwd の定義
12907	FTP コマンド dele の定義
12908	FTP コマンド help の定義
12909	FTP コマンド list の定義
12910	FTP コマンド mkd の定義
12911	FTP コマンド mode の定義
12912	FTP コマンド nlst の定義
12913	FTP コマンド noop の定義
12914	FTP コマンド pass の定義
12915	FTP コマンド pasv の定義

表 5-4　FTP コマンド シグニチャ（続き）

シグニチャ ID	FTP コマンド
12916	FTP コマンド port の定義
12917	FTP コマンド pwd の定義
12918	FTP コマンド quit の定義
12919	FTP コマンド rein の定義
12920	FTP コマンド rest の定義
12921	FTP コマンド retr の定義
12922	FTP コマンド rmd の定義
12923	FTP コマンド rnfr の定義
12924	FTP コマンド rnto の定義
12925	FTP コマンド site の定義
12926	FTP コマンド smnt の定義
12927	FTP コマンド stat の定義
12928	FTP コマンド stor の定義
12929	FTP コマンド stou の定義
12930	FTP コマンド stru の定義
12931	FTP コマンド syst の定義
12932	FTP コマンド type の定義
12933	FTP コマンド user の定義

アプリケーション ポリシーの設定

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

アプリケーション ポリシーの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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Signature Definition** > **Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　Application Policy で、**Enable HTTP** の横にある緑色のアイコンをクリックし、**Yes** を選択して HTTP トラフィックの検査をイネーブルにします。

ステップ 4　**Max HTTP Requests** の横にある緑色のアイコンをクリックし、サーバからの応答を受信していない未処理状態の未処理 HTTP 要求の数（1 接続あたり）を指定します。

ステップ 5　**AIC Web Ports** の横にある緑色のアイコンをクリックし、アクティブにするポートを指定します。

ステップ 6　**Enable FTP** の横にある緑色のアイコンをクリックし、**Yes** を選択して FTP トラフィックの検査をイネーブルにします。

（注）　HTTP または FTP のアプリケーション ポリシーをイネーブルにすると、トラフィックが RFC に準拠しているかどうかセンサーがチェックします。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 7　変更を適用し、変更したコンフィギュレーションを保存するには、**Apply** をクリックします。

認識済みの定義コンテンツ タイプ（MIME）シグニチャの例

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

次の例は、Recognized Content Type（MIME）シグニチャをチューニングする方法を示しています。

シグニチャ 12623 1（コンテンツ タイプ イメージ /tiff のメッセージ長が無効）などの MIME タイプのポリシー シグニチャをチューニングするには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　Select By ボックスで、**Engine** を選択します。

ステップ 4　Select Engine ボックスで、**AIC HTTP** を選択します。

ステップ 5　リストをスクロール ダウンして Sig ID 12623 1 を選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6　Status で、Enabled の横にある緑色のアイコンをクリックし、**Yes** を選択します。

ステップ 7　Content Type Details の横にある緑色のアイコンをクリックし、次のいずれかのオプション、たとえば **Length** を選択します。

ステップ 8　**Length** フィールドで、デフォルトを 30,000 に変更し、長さの値を小さくします。

ステップ 9　**OK** をクリックします。

ステップ 10　**Apply** をクリックして変更内容を保存するか、**Reset** をクリックして変更内容を廃棄します。

IP フラグメント再構成の設定

この項では、IP フラグメント再構成について説明し、設定可能なパラメータを持つ IP フラグメント再構成シグニチャを示し、それらの設定方法について説明します。シグニチャ エンジンの詳細については、P.B-16 の「Normalizer エンジン」を参照してください。

この項で取り上げる事項は次のとおりです。

- 概要（P.5-37）
- IP フラグメント再構成と設定可能なパラメータ（P.5-37）
- IP フラグメント再構成シグニチャの設定（P.5-38）
- IP フラグメント再構成方法の設定（P.5-39）

概要

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、センサーが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り、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ために完全に再組み立てができなくなっているデータグラムに、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。

IP フラグメント再構成はシグニチャごとに設定します。

IP フラグメント再構成と設定可能なパラメータ

表 5-5 は、IP フラグメント再構成用に設定可能なパラメータを持つ IP フラグメント再構成シグニチャを示しています。IP フラグメント再構成シグニチャは、Normalizer エンジンの一部です。

表 5-5　IP フラグメント再構成シグニチャ

IP フラグメント再構成シグニチャ	デフォルト値のあるパラメータ
1200 IP Fragmentation Buffer Full	最大フラグメント 10000 を指定
1201 IP Fragment Overlap	なし
1202 IP Fragment Overrun - Datagram Too Long	最大データグラム サイズ 65536 を指定
1203 IP Fragment Overwrite - Data is Overwritten	なし
1204 IP Fragment Missing Initial Fragment	なし
1205 IP Fragment Too Many Datagrams	最大部分データグラム 1000 を指定
1206 IP Fragment Too Small	小さいフラグメントの最大値 2 を指定 最小フラグメント サイズ 400 を指定
1207 IP Fragment Too Many Datagrams	データグラムごとの最大フラグメント 170 を指定
1208 IP Fragment Incomplete Datagram	フラグメント再構成タイムアウト 60 を指定
1220 Jolt2 Fragment Reassembly DoS attack	最後のフラグメントの最大値 4 を指定
1225 Fragment Flags Invalid	なし

IP フラグメント再構成シグニチャの設定

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

特定のシグニチャに対して 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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

ステップ 3　Select By ボックスで、**Engine** を選択します。

ステップ 4　Select Engine ボックスで、**Normalizer** を選択します。

ステップ 5　リストから設定する IP フラグメント再構成シグニチャ、たとえば Sig ID 1200 SubSig 0 などを選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6　シグニチャ 1200 の設定可能な IP フラグメント再構成パラメータのデフォルト設定を変更します。たとえば、**Max Fragments** の横にある緑色のアイコンをクリックし、設定をデフォルトの 10000 から 20000 に変更します。

シグニチャ 1200 では、次のオプションのパラメータを変更できます。

- **Specify TCP Idle Timeout**
- **Specify Service Ports**
- **Specify SYN Flood Max Embryonic**

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 7　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

IP フラグメント再構成方法の設定

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

センサーが IP フラグメント再構成に使用する方法を設定するには、次の手順を実行します。

(注)　このオプションは、センサーが混合モードで動作しているときに設定できます。センサーがラインモードで動作している場合、このメソッドは NT 専用です。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　Fragment Reassembly で、**IP Reassembly Mode** の横にある緑色のアイコンをクリックし、フラグメントの再構成に使用するオペレーティング システムを選択します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 4　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

TCP ストリーム再構成の設定

この項では、TCP ストリーム再構成について説明し、設定可能なパラメータを持つ TCP ストリーム再構成シグニチャを示し、TCP ストリーム シグニチャの設定方法と TCP ストリーム再構成のモードの設定方法について説明します。シグニチャ　エンジンの詳細については、P.B-16 の「Normalizer エンジン」を参照してください。

この項で取り上げる事項は次のとおりです。

- 概要（P.5-40）
- 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.5-40）
- TCP ストリーム再構成シグニチャの設定（P.5-42）
- TCP ストリーム再構成モードの設定（P.5-43）

概要

センサーは、完全な 3 ウェイ ハンドシェイクによって確立された TCP セッションだけを監視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監視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 セッションの再組み立て機能は、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、シグニチャごとに設定します。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 5-6 は、TCP ストリーム再構成用に設定可能なパラメータを持つ TCP ストリーム再構成シグニチャを示しています。TCP ストリーム再構成シグニチャは、Normalizer エンジンの一部です。

表 5-6　TCP ストリーム再構成シグニチャ

TCP ストリーム再構成シグニチャ	デフォルト値のあるパラメータ
1300 TCP Segment Overwrite	なし
1301 TCP Session Inactivity Timeout	tcp-idle-timeout 3600
1302 TCP Session Embryonic Timeout	tcp-embryonic-timeout 15
1303 TCP Session Closing Timeout	tcp-closed-timeout 5
1304 TCP Session Packet Queue Overflow	tcp-max-queue 32
1305 TCP Urgent Flag Set	なし
1306 0 TCP Option Others 1306 1 TCP SACK Allowed Option 1306 2 TCP SACK Data Option 1306 3 TCP Timestamp Option 1306 4 TCP Window Scale Option 1306 5 TCP MSS Option	tcp-option-number 6-7,9-255

表 5-6　TCP ストリーム再構成シグニチャ（続き）

TCP ストリーム再構成シグニチャ	デフォルト値のあるパラメータ
1307 TCP Window Size Variation	なし
1308 TTL Evasion	なし
1309 TCP Reserved Flags Set	なし
1310 TCP Retransmit Data Different	なし
1311 TCP Packet Exceeds MSS	なし
1312 TCP MSS Below Minimum	tcp-min-mss 400
1313 TCP MSS Exceed Maximum	tcp-max-mss 1460
1314 TCP SYN Packet with Data	なし
1330[1] 0 TCP Drop - Bad Checksum 1330 1 TCP Drop - Bad TCP Flags 1330 2 TCP Drop - Urgent Pointer Without Flag 1330 3 TCP Drop - Bad Option List 1330 4 TCP Drop - Bad Option Length 1330 5 TCP Drop - MSS Option in Non-SYN 1330 6 TCP Drop - WinScale Option in Non-SYN 1330 7 TCP Drop - Bad WinScale Option Value 1330 8 TCP Drop - Bad SACK Allow 1330 9 TCP Drop - Data in SYN|ACK 1330 10 TCP Drop - Data Past FIN 1330 11 TCP Drop - Timestamp not Allowed 1330 12 TCP Drop - Segment Out of Order 1330 13 TCP Drop - Invalid TCP Packet 1330 14 TCP Drop - RST or SYN in window 1330 15 TCP Drop - Segment Already ACKed by Peer 1330 16 TCP Drop - PAWS Check Failed 1330 17 TCP Drop - Segment out of State Order 1330 18 TCP Drop - Segment out of Window	なし
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. これらのサブシグニチャは、正規化エンジンが TCP パケットをドロップする理由を示しています。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、正規化エンジンで検査に合格しなかったパケットに IPS を通過させることができます。ドロップの理由は、TCP 統計情報内にエントリがあります。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。

TCP ストリーム再構成シグニチャの設定

ヒント + アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

特定のシグニチャに対して 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 管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Signature Definition > Signature Configuration** をクリックします。

ステップ 3 Select By ボックスで、**Engine** を選択します。

ステップ 4 Select Engine ボックスで、**Normalizer** を選択します。

ステップ 5 リストから設定する TCP フラグメント再構成シグニチャ、たとえば Sig ID 1313 SubSig 0 などを選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6 シグニチャ 1313 の設定可能な IP フラグメント再構成パラメータのデフォルト設定を変更します。たとえば、**TCP Max MSS** の横にある緑色のアイコンをクリックし、設定をデフォルトの 1460 から 1380 に変更します。

(注) このパラメータをデフォルトの 1460 から 1380 へ変更すると、VPN トンネルを通過するトラフィックのフラグメント化を防ぐことができます。

シグニチャ 1313 0 では、次のオプションのパラメータを変更できます。

- Specify Hijack Max Old Ack
- Specify TCP Idle Timeout
- Specify Service Ports
- Specify SYN Flood Max Embryonic

ヒント **Reset** をクリックして、変更を削除します。

ステップ 7 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

TCP ストリーム再構成モードの設定

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

TCP ストリーム再構成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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　Stream Reassembly で、**TCP Handshake Required** の横にある緑色のアイコンをクリックし、**yes** を選択します。

TCP Handshake Required を選択すると、3 ウェイ ハンドシェイクが完了したセッションのみをセンサーが追跡するように指定します。

ステップ 4　**TCP Reassembly Mode** の横にある緑色のアイコンをクリックし、センサーが TCP セッションの再構成に使用するモードを選択します。

- **Asymmetric**：センサーが、トラフィック　フローの状態と同期をとり、双方向のうち一方向だけでよいエンジンの検査を継続するようにします。
- **Strict**：何らかの理由でパケットを受信しなかった場合でも、以後のパケットをすべて処理します。
- **Loose**：パケットが廃棄される可能性がある場合に使用します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

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反応すると、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ログに記録されます。

ヒント + アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータが現在デフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

IP ロギングのパラメータを設定するには、次の手順を実行します。

（注） センサーは、IP ロギング条件のいずれかを検出すると、IP ロギングを停止します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　IP Log で、**Max IP Log Packets** の横にある緑色のアイコンをクリックし、ログを作成するパケットの数を指定します。

ステップ 4　**IP Log Time** の横にある緑色のアイコンをクリックし、ログを作成する時間を指定します。

有効な値は、1 ～ 60 分です。デフォルトは 30 分です。

ステップ 5　**Max IP Log Bytes** の横にある緑色のアイコンをクリックし、ログを作成する最大バイト数を指定します。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 6　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

MEG シグニチャの例

Meta エンジンは、スライドする時間間隔内で、関連する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。シグニチャ イベントが生成されると、Meta エンジンがそれらを検査して、1 つまたはいくつかの Meta 定義と一致するかどうかを判別します。Meta エンジンは、このイベントに対するすべての要件が満たされた後に、シグニチャ イベントを生成します。

シグニチャ イベントはすべて SEAP によって Meta エンジンに渡されます。SEAP は、minimum hits オプションを処理した後で、イベントを渡します。要約とイベント アクションは、Meta 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。SEAP の詳細については、P.7-4 の「Signature Event Action Processor」を参照してください。

注意　多数の Meta シグニチャが、意図せずセンサー パフォーマンス全体に影響を及ぼす可能性があります。

次の例は、Meta エンジンに基づいて MEG シグニチャを作成する方法を示しています。

たとえば、シグニチャ 64000 のサブシグニチャ 0 は、同一送信元アドレスでシグニチャ 2000 のサブシグニチャ 0 とシグニチャ 3000 のサブシグニチャ 0 からのアラートを確認すると、反応します。送信元アドレス選択は、メタ キーのデフォルト値 Axxx の結果です。メタ キー設定を xxBx（宛先アドレス）に変更することによって、動作を変更できます。たとえば、次のようになります。

ヒント　メタ エンジンは、ほとんどのエンジンが入力としてパケットを取るのに対し、入力としてアラートを取る点で、その他のエンジンとは異なります。Meta エンジンの詳細については、P.B-14 の「Meta エンジン」を参照してください。

メタ エンジンに基づいて MEG シグニチャを作成するには、次の手順を実行します。

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータが現在デフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　**Add** をクリックして、Add Signature ダイアログボックスを開きます。

ステップ 4　**Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。

ステップ 5　**Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。

ステップ 6　**Alert Severity** フィールドの隣にある緑のアイコンをクリックし、シグニチャに関連付ける重大度を選択します。

ステップ 7　**Signature Fidelity Rating** フィールドの隣にある緑のアイコンをクリックし、シグニチャのシグニチャ忠実度評価を表す値（1 ～ 100）を指定します。

ステップ 8　**Promiscuous Delta** フィールドの値は、デフォルトのままにしておいてください。

ステップ 9　シグニチャ説明フィールドにシグニチャに関するコメントを入力します。

ステップ 10　**Engine** フィールドで Meta を選択します。

ステップ 11　Meta エンジン固有のパラメータを設定します。

a. **Meta Reset Interval** フィールドの横にある緑色のアイコンをクリックし、Meta シグニチャをリセットする時間を秒単位で指定します。

   有効な範囲は 0 ～ 3600 秒です。デフォルトは 60 秒です。

b. **Meta Key** リストから、Meta シグニチャのストレージ タイプを選択します。

   - 攻撃者のアドレス
   - 攻撃者アドレスと被害先アドレス
   - 攻撃者と被害先のアドレスおよびポート
   - 被害先のアドレス

c. **Component List** の横にある鉛筆のアイコンをクリックし、新しい MEG シグニチャを挿入します。

   Component List ダイアログボックスが表示されます。

d. **Add** をクリックして、最初の MEG シグニチャを挿入します。

   Add List Entry ダイアログボックスが表示されます。

e. **Entry Key** フィールドで、Entry1 のようにエントリの名前を指定します。

   デフォルトは MyEntry です。

f. Component Group の下の **Component Count** フィールドで、このコンポーネントが何回反応したら満たされるかを指定します。

g. Component Group の下の **Component Sig ID** フィールドで、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（この例では 2000）。

h. Component Group の下の **Component SubSig ID** フィールドで、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（この例では 0）。

i. **OK** をクリックします。

   Add List Entry ダイアログボックスが再び表示されます。

j. エントリを強調表示し、**Select** をクリックしてそれを Selected Entries リストに移動します。

k. **OK** をクリックします。

l. **Add** をクリックして、次の MEG シグニチャを挿入します。

Add List Entry ダイアログボックスが表示されます。

m. **Entry Key** フィールドで、Entry2 のようにエントリの名前を指定します。

n. Component Group の下の **Component Count** フィールドで、このコンポーネントが何回反応したら満たされるかを指定します。

o. Component Group の下の **Component Sig ID** フィールドで、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（この例では 3000）。

p. Component Group の下の **Component SubSig ID** フィールドで、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（この例では 0）。

q. **OK** をクリックします。

Add List Entry ダイアログボックスが再び表示されます。

r. エントリを強調表示し、**Select** をクリックしてそれを Selected Entries リストに移動します。

s. 新しいエントリを強調表示し、**Move Up** または **Move Down** をクリックして新しいエントリの順序を決めます。

ヒント **Reset Ordering** をクリックすると、エントリは Entry Key リストに戻ります。

t. **OK** をクリックします。

u. **Component List in Order** フィールドの横にある緑色のアイコンをクリックし、**Yes** を選択してコンポーネント リストを順序どおりに並べます。

ステップ 12 **Event Action** フィールドの横にある緑色のアイコンをクリックし、センサーがイベントに応答するときに起こすアクションを選択します。

ヒント 複数のアクションを選択するには、**Ctrl** キーを押してすべてのアクションが選択された状態にします。

ステップ 13 イベントをカウントする場合は、Event Counter の下にある **Event Counter** フィールドを設定します。

ステップ 14 Alert Frequency の下にある **Alert Frequency** フィールドで、アラートを受信する方法を指定します。

ステップ 15 Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注） シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

ステップ 16 Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注） シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント 変更を元に戻し、Add Signature ダイアログを閉じるには、**Cancel** をクリックします。

ステップ 17 **OK** をクリックします。

Type が Custom に設定された新しいシグニチャがリストに現れます。

ヒント 変更を元に戻す場合は、**Reset** をクリックします。

ステップ 18 **Apply** をクリックし、変更を適用して、変更された設定を保存します。

カスタム シグニチャの作成

この章では、Custom Signature Wizard ウィザードを使用してカスタム シグニチャを作成する方法について説明します。個々のシグニチャ エンジンの詳細については、付録 B「シグニチャ エンジン」を参照してください。

この章は、次の項で構成されています。

- Custom Signature Wizard について（P.6-2）
- サポートされるユーザのロール（P.6-5）
- フィールド定義（P.6-5）
- カスタム シグニチャの作成（P.6-22）

Custom Signature Wizard について

Custom Signature Wizard は、カスタム シグニチャを作成する手順を順を追って示します。シグニチャ エンジンを使用してカスタム シグニチャを作成する方法と、シグニチャ エンジンを使用せずにカスタム シグニチャを作成する方法の 2 つの手順があります。

IPS 5.1 の Custom Signature Wizard では、次のシグニチャ エンジンを使用してカスタム シグニチャを作成する方法はサポートされていません。

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

これらの既存のシグニチャ　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、Configuration > Signature Configuration > Clone をクリックしてエンジンから既存のシグニチャを複製します。詳細については、P.5-19 の「シグニチャの複製」を参照してください。

これらのシグニチャ エンジンを使用し、カスタム シグニチャを CLI によって作成する方法の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』を参照してください。

この項で取り上げる事項は次のとおりです。

- シグニチャ エンジンを使用する方法（P.6-3）
- シグニチャ エンジンを使用しない方法（P.6-4）

シグニチャ エンジンを使用する方法

次の手順は、シグニチャ エンジンを使用してカスタム シグニチャを作成する場合に適用されます。

ステップ 1　シグニチャ エンジンを選択します。

- Atomic IP
- Service HTTP
- Service MSRPC
- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

ステップ 2　シグニチャの識別子を割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラートの注釈（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。

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マスター パラメータのグループが 1 つあります。

ステップ 4　アラート応答を割り当てます。

- シグニチャ忠実度評価
- 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。

デフォルトのアラート動作を受け入れることもできますし、**Advanced** をクリックして Advanced Alert Behavior Wizard を開き、変更することもできます。このウィザードでは、このシグニチャのアラートを処理する方法を設定できます。

ステップ 6　**Finish** をクリックします。

シグニチャ エンジンを使用しない方法

次の手順は、シグニチャ エンジンを使用せずにカスタム シグニチャを作成する場合に適用されます。

ステップ 1　Welcome ウィンドウで **No** を選択します。

ステップ 2　使用するプロトコルを選択します。

- IP：ステップ 4 に進みます。
- ICMP：ステップ 3 に進みます。
- UDP：ステップ 3 に進みます。
- TCP：ステップ 3 に進みます。

ステップ 3　ICMP プロトコルと UDP プロトコルの場合は、トラフィック タイプと検査データ タイプを選択します。TCP プロトコルの場合は、トラフィック タイプを選択します。

ステップ 4　シグニチャの識別子を割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラートの注釈（オプション）
- ユーザ コメント（オプション）

ステップ 5　エンジン固有のパラメータを割り当てます。

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マスター パラメータのグループが 1 つあります。

ステップ 6　アラート応答を割り当てます。

- シグニチャ忠実度評価
- アラートの重大度

ステップ 7　アラート動作を割り当てます。

デフォルトのアラート動作を受け入れることもできますし、**Advanced** をクリックして Advanced Alert Behavior Wizard を開き、変更することもできます。このウィザードでは、このシグニチャのアラートを処理する方法を設定できます。

ステップ 8　**Finish** をクリックします。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

カスタム シグニチャを作成するには、管理者またはオペレータである必要があります。

フィールド定義

次の項では、Custom Signature Wizard のフィールド定義をウィンドウごとに説明します。取り上げる事項は次のとおりです。

- Welcome フィールド定義（P.6-5）
- Protocol Type フィールド定義（P.6-6）
- Signature Identification フィールド定義（P.6-7）
- Atomic IP Engine Parameters フィールド定義（P.6-7）
- Service HTTP Engine Parameters フィールド定義（P.6-8）
- Service MSRPC Engine Parameters フィールド定義（P.6-9）
- Service RPC Engine Parameters フィールド定義（P.6-10）
- State Engine Parameters フィールド定義（P.6-11）
- String ICMP Engine Parameters フィールド定義（P.6-11）
- String TCP Engine Parameters フィールド定義（P.6-12）
- String UDP Engine Parameters フィールド定義（P.6-13）
- Sweep Engine Parameters フィールド定義（P.6-14）
- ICMP Traffic Type フィールド定義（P.6-15）
- UDP Traffic Type フィールド定義（P.6-15）
- TCP Traffic Type フィールド定義（P.6-15）
- UDP Sweep Type フィールド定義（P.6-16）
- TCP Sweep Type フィールド定義（P.6-16）
- Service Type フィールド定義（P.6-16）
- Inspect Data フィールド定義（P.6-17）
- Alert Response フィールド定義（P.6-17）
- Alert Behavior フィールド定義（P.6-18）
- Advanced Alert Behavior ウィザード（P.6-18）

Welcome フィールド定義

Custom Signature Wizard の Welcome ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Yes**：**Select Engine** フィールドをアクティブにし、リストからシグニチャ エンジンを選択します。

- **Select Engine**：使用可能なシグニチャ エンジンのリストを表示します。シグニチャの作成にどのシグニチャ エンジンを使用するかが不明な場合は、**Yes** をクリックし、リストからエンジンタイプを選択します。
  - **Atomic IP**：Atomic IP シグニチャを作成します。
  - **Service HTTP**：HTTP トラフィック用のシグニチャを作成します。
  - **Service MSRPC**：MSRPC トラフィック用のシグニチャを作成します。
  - **Service RPC**：RPC トラフィック用のシグニチャを作成します。
  - **State SMTP**：SMTP トラフィック用のシグニチャを作成します。
  - **String ICMP**：ICMP 文字列用のシグニチャを作成します。
  - **String TCP**：TCP 文字列用のシグニチャを作成します。
  - **String UDP**：UDP 文字列用のシグニチャを作成します。
  - **Sweep**：スイープ用のシグニチャを作成します。
- **No**：Custom Signature Wizard のエンジン選択画面を継続します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Protocol Type フィールド定義

特定のプロトコルを使用した悪意のある動作を検出するシグニチャを定義できます。シグニチャによるデコードと検査が可能なプロトコルは、次のとおりです。

- IP
- ICMP
- UDP
- TCP

Custom Signature Wizard の Protocol Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP**：IP トラフィックのデコードと検査を行うシグニチャを作成します。
- **ICMP**：ICMP トラフィックのデコードと検査を行うシグニチャを作成します。
- **UDP**：UDP トラフィックのデコードと検査を行うシグニチャを作成します。
- **TCP**：TCP トラフィックのデコードと検査を行うシグニチャを作成します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Signature Identification フィールド定義

Custom Signature Wizard の Signature Identification ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。

  シグニチャ ID を使用すると、センサーが特定のシグニチャを識別できます。アラートが生成されると、シグニチャ ID は Event Viewer に報告されます。有効な範囲は 60000 ～ 65000 です。
- **SubSignature ID**：このサブシグニチャに割り当てられた固有の数値を示します。

  サブシグニチャ ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。有効な値は 0 ～ 255 です。アラートが生成されると、サブシグニチャは Event Viewer に報告されます。
- **Signature Name**：このシグニチャに割り当てられた名前を示します。

  アラートが生成されると、Event Viewer に報告されます。
- **Alert Notes**：（オプション）このシグニチャが反応した場合、アラートに関連付けられているテキストを指定します。

  アラートが生成されると、Event Viewer に報告されます。
- **User Comments**：（オプション）このシグニチャに関して、シグニチャ パラメータといっしょに保存する注釈などのコメントを指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Atomic IP Engine Parameters フィールド定義

Custom Signature Wizard の Atomic IP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Fragment Status**：フラグメント化されている、またはフラグメント化されていないトラフィックを検査する場合に指定します。
- **Specify Layer 4 Protocol**：（オプション）特定のプロトコルをこのシグニチャに適用するかどうかを選択します。

  Yes を選択した場合、次のプロトコルから選択できます。

  － **ICMP Protocol**：ICMP のシーケンス、タイプ、コード、識別子、および合計の長さを指定します。

- **Other Protocols**：識別子を選択します。
- **TCP Protocol**：TCP フラグ、ウィンドウ サイズ、マスク、ペイロード長、緊急ポインタ、ヘッダー長、予約済みのアトリビュート、および送信元と宛先のポート範囲を設定します。
- **UDP Protocol**：有効な UDP 長、長さのミスマッチ、および送信元と宛先のポート範囲を指定します。

- **Specify Payload Inspection**：（オプション）次のペイロード検査オプションを指定します。
- **Specify IP Payload Length**：（オプション）ペイロード長を指定します。
- **Specify IP Header Length**：（オプション）IP ヘッダー長を指定します。
- **Specify IP Type of Service**：（オプション）サービスのタイプを指定します。
- **Specify IP Time-to-Live**：（オプション）パケットの存続可能時間を指定します。
- **Specify IP Version**：（オプション）IP バージョンを指定します。
- **Specify IP Identifier**：（オプション）IP 識別子を指定します。
- **Specify Total IP Length**：（オプション）IP の合計の長さを指定します。
- **Specify IP Option Inspection Options**：（オプション）IP 検査オプションを指定します。
  次からを選択します。
  - **IP Option**：照合する IP オプション コード。
  - **IP Option Abnormal Options**：オプションの不正形式リスト。
- **Specify IP Addr Options**：（オプション）次の IP アドレス オプションを指定します。
  - **Address with Localhost**：ローカル ホストのアドレスが送信元アドレスまたは宛先アドレスとして使用されているトラフィックを示します。
  - **IP Addresses**：送信元アドレスまたは宛先アドレスを指定します。
  - **RFC 1918 Address**：アドレスのタイプが RFC 1918 であることを示します。
  - **Src IP Equal Dst IP**：送信元アドレスと宛先アドレスが同一のトラフィックを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service HTTP Engine Parameters フィールド定義

Custom Signature Wizard の Service HTTP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

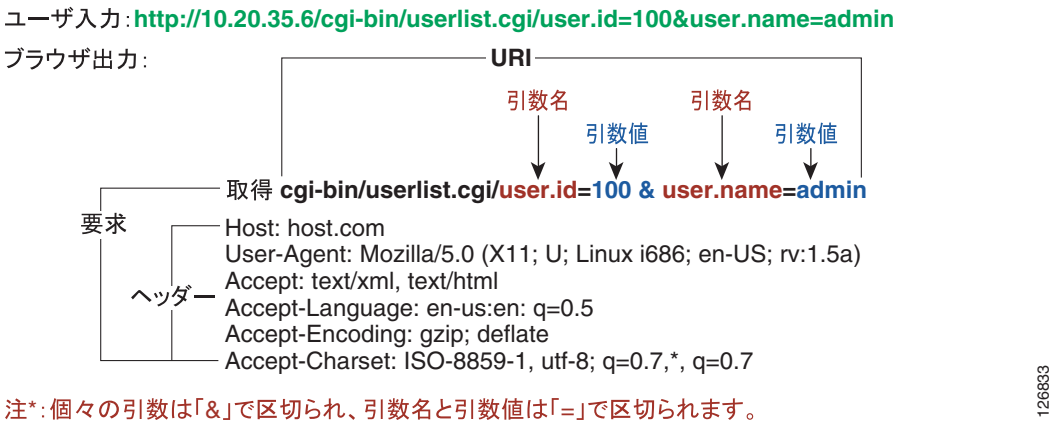
- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。
  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **De Obfuscate**：反回避 HTTP 解読を適用するかどうかを指定します。
  デフォルトは **Yes** です。

- **Max Field Sizes**：（オプション）URI、Arg、Header、および Request フィールドの最大の長さを指定します。

  次の図は、最大フィールド サイズを示しています。



- **Regex**：URI、Arg、Header、および Request Regex の正規表現を指定します。
- **Service Ports**：トラフィックが使用する特定のサービス ポートを指定します。

  値は、ポートのカンマ区切りのリストです。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service MSRPC Engine Parameters フィールド定義

Custom Signature Wizard の MSRPC Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、非常に汎用的または非常に特殊なタイプのトラフィックを検出するシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Specify Regex String**：（オプション）完全一致オフセットを指定します。これには最小および最大一致オフセット、Regex 文字列、最小一致の長さが含まれます。

- **Protocol**：TCP または UDP をプロトコルとして指定できます。
- **Specify Operation**：（オプション）操作を指定します。
- **Specify UUID**：（オプション）UUID を指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service RPC Engine Parameters フィールド定義

Custom Signature Wizard の Service RPC Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。
  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Direction**：センサーがサービス ポートを宛先または送信元とするトラフィックを監視するかどうかを示します。
  デフォルトは **To Service** です。
- **Protocol**：TCP または UDP をプロトコルとして指定できます。
- **Service Ports**：ターゲット サービスが常駐できるポートまたはポート範囲を示します。
  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Specify Port Map Program**：シグニチャの対象ポート マッパーに送信されるプログラム番号を示します。
  有効な範囲は 0 ～ 9999999999 です。
- **Specify RPC Program**：シグニチャの対象 RPC プログラム番号を示します。
  有効な範囲は 0 ～ 1000000 です。
- **Specify Spool Src**：送信元アドレスが 127.0.0.1 に設定された場合、アラームを生成します。
- **Specify RPC Max Length**：RPC メッセージ全体の最大許容長。
  長さがこの値を超えている場合は、アラームが生成されます。有効な範囲は 0 ～ 65535 です。
- **Specify RPC Procedure**：シグニチャの対象 RPC プロシージャ番号を示します。
  有効な範囲は 0 ～ 1000000 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

State Engine Parameters フィールド定義

Custom Signature Wizard の State Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **State Machine**：正規表現文字列の照合を制限する状態の名前を示します。

  オプションは、**Cisco Login**、**LPR Format String**、および **SMTP** です。
- **Specify Min Match Length**：照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Regex String**：状態遷移のトリガーとなる正規表現文字列を示します。
- **Direction**：遷移のために検査するデータ ストリームの方向を示します。

  デフォルトは **To Service** です。
- **Service Ports**：ターゲット サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。
- **Specify Exact Match Offset**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  有効な範囲は 0 ～ 65535 です。

  No を選択すると、最小および最大一致オフセットを設定できます。

  有効な範囲は 1 ～ 65535 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String ICMP Engine Parameters フィールド定義

Custom Signature Wizard の String ICMP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Specify Min Match Length**：照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Regex String**：単一のパケットで検索する正規表現文字列を示します。
- **Direction**：遷移のために検査するデータ ストリームの方向を示します。

  デフォルトは **To Service** です。
- **ICMP Type**：ICMP ヘッダーの TYPE 値。

  有効範囲は 0 ～ 18 です。デフォルトは 0 ～ 18 です。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。
- **Specify Exact Match Offset**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  No を選択すると、最小および最大一致オフセットを設定できます。

  最大一致オフセットの有効範囲は 1 ～ 65535 です。最小一致オフセットの有効範囲は 0 ～ 65535 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String TCP Engine Parameters フィールド定義

Custom Signature Wizard の String TCP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、非常に汎用的または非常に特殊なタイプのトラフィックを検出するシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Strip Telnet Options**：パターンを検索する前に、データ ストリームから Telnet オプション制御文字を削除します。

  これは、主に反回避ツールとして使用します。デフォルトは **No** です。

- **Specify Min Match Length**：照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Regex String**：単一のパケットで検索する正規表現文字列を示します。
- **Service Ports**：ターゲット サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Direction**：遷移のために検査するデータ ストリームの方向を示します。

  デフォルトは **To Service** です。
- **Specify Exact Match Offset**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  No を選択すると、最小および最大一致オフセットを設定できます。

  最大一致オフセットの有効範囲は 1 ～ 65535 です。最小一致オフセットの有効範囲は 0 ～ 65535 です。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String UDP Engine Parameters フィールド定義

Custom Signature Wizard の String UDP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Specify Min Match Length**：照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Specify Exact Match Offset**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  有効な範囲は 0 ～ 65535 です。

  No を選択すると、最小および最大一致オフセットを設定できます。

  有効な範囲は 1 ～ 65535 です。
- **Regex String**：単一のパケットで検索する正規表現文字列を示します。

- **Service Ports**：ターゲット サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Direction**：遷移のために検査するデータ ストリームの方向を示します。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Sweep Engine Parameters フィールド定義

Custom Signature Wizard の Sweep Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定のタイプのトラフィックを検出するためのシグニチャを作成できます。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合にセンサーで実行するアクションを指定します。

  デフォルトは **Produce Alert** です。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **Unique**：一意なホスト接続数のしきい値を示します。

  インターバル中に一意のホスト接続数を超えた場合には、アラームが生成されます。
- **Protocol**：プロトコルを示します。
  - **ICMP**：ICMP ストレージ タイプを指定し、攻撃者アドレス、攻撃者アドレスと被害先ポート、攻撃者と被害者のアドレスのいずれか 1 つのストレージ キーを選択します。
  - **TCP**：サプレス リバース、インバーテッド スイープ、マスク、TCP フラグ、フラグメント ステータス、ストレージ キーを選択するか、またはポート範囲を指定します。
  - **UDP**：ストレージ キーを選択するか、またはポート範囲を指定します。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

ICMP Traffic Type フィールド定義

Custom Signature Wizard の ICMP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Sweeps**：スイープ攻撃を検出するシグニチャを作成していることを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

UDP Traffic Type フィールド定義

Custom Signature Wizard の UDP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Sweeps**：スイープ攻撃を検出するシグニチャを作成していることを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

TCP Traffic Type フィールド定義

Custom Signature Wizard の TCP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Single TCP Connection**：単一の TCP 接続を検査して攻撃を検出するためのシグニチャを作成するように指定します。
- **Multiple Connections**：複数の接続を検査して攻撃を検出するためのシグニチャを作成するように指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

UDP Sweep Type フィールド定義

Custom Signature Wizard の UDP Sweep Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Host Sweep**：ネットワークでホストを検索するスイープを示します。
- **Port Sweep**：ホストでオープン ポートを検索するスイープを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

TCP Sweep Type フィールド定義

Custom Signature Wizard の TCP Sweep Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Host Sweep**：ネットワークでホストを検索するスイープを示します。
- **Port Sweep**：ホストでオープン ポートを検索するスイープを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service Type フィールド定義

Custom Signature Wizard の Service Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **HTTP**：HTTP　サービスを使用する攻撃を説明するためのシグニチャを作成するように指定します。
- **SMTP**：SMTP　サービスを使用する攻撃を説明するためのシグニチャを作成するように指定します。
- **RPC**：RPC　サービスを使用する攻撃を説明するためのシグニチャを作成するように指定します。
- **MSRPC**：MSRPC サービスを使用する攻撃を説明するためのシグニチャを作成するように指定します。
- **Other**：HTTP、SMTP、RPC、MSRPC 以外のサービスを使用する攻撃を説明するためのシグニチャを作成するように指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。

- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Inspect Data フィールド定義

Custom Signature Wizard の Inspect Data ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Header Data Only**：センサーが検査するパケットの一部としてヘッダーを指定します。
- **Payload Data Only**：センサーが検査するパケットの一部としてペイロードを指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Response フィールド定義

Custom Signature Wizard の Alert Response ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature Fidelity Rating**：対象とする特定の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。

  SFR は、シグニチャ作成者によってシグニチャごとに計算されます。きわめて具体的なルール（特定の Regex など）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高い SFR を持ちます。
- **Severity of the Alert**：アラートが報告される重大度。

  次のオプションから選択できます。
  - **High**：最も重大なセキュリティ アラート。
  - **Medium**：中程度のセキュリティ アラート。
  - **Low**：最も低いセキュリティ アラート。
  - **Information**：ネットワーク アクティビティを示します。セキュリティ アラートではありません。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Behavior フィールド定義

Custom Signature Wizard の Alert Behavior ウィンドウには、次のボタンがあります。

- **Advanced**：Advanced Alert Behavior ウィンドウを開きます。このウィンドウでは、デフォルトの動作を変更し、センサーがアラートを送信する頻度を設定できます。
- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Advanced Alert Behavior ウィザード

次の項では、Advanced Alert Behavior ウィザードのフィールド定義について説明します。取り上げる事項は次のとおりです。

- Event Count and Interval フィールド定義（P.6-18）
- Alert Summarization フィールド定義（P.6-19）
- Alert Dynamic Response Summary フィールド定義（P.6-19）
- Alert Dynamic Response Fire All フィールド定義（P.6-20）
- Alert Dynamic Response Fire Once フィールド定義（P.6-20）
- Global Summarization フィールド定義（P.6-21）

Event Count and Interval フィールド定義

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Event Count**：このシグニチャのアラートを送信する前に、センサーが受信すべき最小ヒット数を示します。
- **Event Count Key**：イベントのカウントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Event Count Key** として **Attacker Address** を選択します。
- **Use Event Interval**：センサーがレートに基づいてイベントをカウントするように指定します。

  たとえば、**Event Count** に 500 イベントを設定し、**Event Interval** に 30 秒を設定すると、センサーは、30 秒以内に 500 イベントを受信した場合にアラートを送信します。
- **Event Interval (seconds)**：センサーがレートに基づいてイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Summarization フィールド定義

Advanced Alert Behavior ウィザードの Alert Summarization ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Alert Every Time the Signature Fires**：シグニチャが悪意のあるトラフィックを検出するたびに、センサーがアラートを送信するように指定します。

  その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。
- **Alert the First Time the Signature Fires**：シグニチャが初めて悪意のあるトラフィックを検出したときに、センサーがアラートを送信するように指定します。

  その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。
- **Send Summary Alerts**：シグニチャが反応するたびにアラートを送信するのではなく、センサーがこのシグニチャのサマリー アラートだけを送信するように指定します。

  その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。
- **Send Global Summary Alerts**：シグニチャがアドレス セットで初めて反応したときにアラートをセンサーが送信し、その後は所定の時間間隔におけるすべてのアドレス セットのすべてのアラートのサマリーを示すグローバル サマリー アラートだけを送信するように指定します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Summary フィールド定義

Advanced Alert Behavior ウィザードの Alert Dynamic Response Summary ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summary Interval (seconds)**：センサーが要約のためにイベントをカウントする時間間隔を示します。
- **Summary Key**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Summary Key** として **Attacker Address** を選択します。
- **Use Dynamic Global Summarization**：センサーが動的にグローバル サマリー モードに入るようにします。
- **Global Summary Threshold**：グローバル サマリー アラートを送信する前にセンサーが受信すべき最小のヒット数を示します。

  アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーは単一のサマリー アラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。

- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Fire All フィールド定義

Alert Every Time the Signature Fires を選択した場合、Advanced Alert Behavior ウィザードの Alert Dynamic Response ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Use Dynamic Summarization**：設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。
- **Summary Threshold**：このシグニチャのサマリー アラートを送信する前に、センサーが受信すべき最小ヒット数を示します。
- **Summary Interval (seconds)**：レートに基づいてイベントをカウントするように指定し、時間間隔に使用する秒数を示します。
- **Summary Key**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Summary Key** として **Attacker Address** を選択します。
- **Specify Global Summary Threshold**：センサーが動的にグローバル サマリー モードに入るようにします。

  アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャごとにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。グローバル サマリーでは、すべての攻撃者の IP アドレスとポート、およびすべての被害先 IP アドレスとポートに対してシグニチャが反応した件数がカウントされます。
- **Global Summary Threshold**：グローバル サマリー アラートを送信する前にセンサーが受信すべき最小のヒット数を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Fire Once フィールド定義

Alert the First Time the Signature Fires を選択した場合、Alert Behavior ウィザードの Alert Dynamic Response ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summary Key**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Summary Key** として **Attacker Address** を選択します。
- **Use Dynamic Global Summarization**：センサーが動的にグローバル サマリー モードに入るようにします。

- **Global Summary Threshold**：グローバル サマリー アラートを送信する前にセンサーが受信すべき最小のヒット数を示します。

  アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャが初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。
- **Global Summary Interval (seconds)**：センサーが要約のためにイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Global Summarization フィールド定義

Advanced Alert Behavior ウィザードの Global Summarization ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Global Summary Interval (seconds)**：センサーが要約のためにイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

カスタム シグニチャの作成

この項では、カスタム シグニチャの例を示します。取り上げる事項は次のとおりです。

- Custom Signature Wizard でサポートされていないシグニチャ エンジン（P.6-22）
- マスター カスタム シグニチャの手順（P.6-23）
- String TCP シグニチャの例（P.6-29）
- Service HTTP シグニチャの例（P.6-34）

Custom Signature Wizard でサポートされていないシグニチャ エンジン

IPS 5.1 の Custom Signature Wizard では、次のシグニチャ エンジンを使用してカスタム シグニチャを作成する方法はサポートされていません。

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

これらの既存のシグニチャ　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、Configuration > Signature Configuration > Clone をクリックしてエンジンから既存のシグニチャを複製します。詳細については、P.5-19 の「シグニチャの複製」を参照してください。

これらのシグニチャ エンジンを使用し、カスタム シグニチャを CLI によって作成する方法の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』を参照してください。

マスター カスタム シグニチャの手順

Custom Signature Wizard は、カスタム シグニチャを設定する手順を順を追って示します。個々のシグニチャ エンジンの詳細については、付録 B「シグニチャ エンジン」を参照してください。

Custom Signature Wizard を使用してカスタム 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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意　カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　新しいシグニチャの作成に使用する特定のシグニチャ エンジンがわかっている場合は、**Yes** オプション ボタンをクリックし、**Select Engine** リストからシグニチャ エンジンを選択し、**Next** をクリックします。ステップ 13 に進みます。

使用するエンジンが不明の場合は、**No** オプション ボタンをクリックし、**Next** をクリックします。

Protocol Type ウィンドウが表示されます。

ステップ 5　このシグニチャによる検査の対象となるトラフィック タイプに最適なプロトコルを次から選択し、**Next** をクリックします。

- **IP**（IP を選択した場合は ステップ 13 に進みます）。
- **ICMP**（ICMP を選択した場合は ステップ 6 に進みます）。
- **UDP**（UDP を選択した場合は ステップ 7 に進みます）。
- **TCP**（TCP を選択した場合は ステップ 9 に進みます）。

ステップ 6　ICMP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Single Packet**

  Atomic IP エンジン（ヘッダー データ用）または String ICMP エンジンを使用して、単一パケットの攻撃を検査するシグニチャを作成します。

  ステップ 12 に進みます。
- **Sweeps**

  新しいシグニチャにスイープ エンジンを使用して、スイープ攻撃を検出するシグニチャを作成します。

  ステップ 13 に進みます。

ステップ 7　UDP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Single Packet**

  Atomic IP エンジン（ヘッダー データ用）または String UDP エンジンを使用して、単一パケットの攻撃を検査するシグニチャを作成します。

  ステップ 12 に進みます。

- **Sweeps**

  シグニチャにスイープ エンジンを使用して、スイープ攻撃を検出するシグニチャを作成します。

  ステップ 8 に進みます。

ステップ 8　UDP Sweep Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Host Sweep**

  ホストでオープン ポートを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは Axxx に設定されます。

  ステップ 13 に進みます。

- **Port Sweep**

  ネットワークでホストを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは AxBx に設定されます。

  ステップ 13 に進みます。

ステップ 9　TCP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Single Packet**

  単一のパケットを検査して攻撃を検出するためのシグニチャを作成します。Atomic IP エンジンを使用してシグニチャを作成します。

  ステップ 13 に進みます。

- **Single TCP Connection**

  TCP サービスを使用する攻撃を検出するためのシグニチャを作成します。

  ステップ 10 に進みます。

- **Multiple Connections**

  複数の接続を検査して攻撃を検出するためのシグニチャを作成します。

  ステップ 11 に進みます。

ステップ 10　Service Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **HTTP**

  HTTP サービスを使用する攻撃を検出するためのシグニチャを作成します。Service HTTP エンジンを使用してシグニチャを作成します。

- **SMTP**

  SMTP サービスを使用する攻撃を検出するためのシグニチャを作成します。SMTP エンジンを使用してシグニチャを作成します。

- **RPC**

  RPC サービスを使用する攻撃を検出するためのシグニチャを作成します。Service RPC エンジンを使用してシグニチャを作成します。

- **MSRPC**

  MSRPC サービスを使用する攻撃を検出するためのシグニチャを作成します。Service MSRPC エンジンを使用してシグニチャを作成します。

- **Other**

  HTTP、SMTP、RPC 以外のサービスを使用する攻撃を検出するためのシグニチャを作成します。String TCP エンジンを使用してシグニチャを作成します。

ステップ 13 に進みます。

ステップ 11 TCP Sweep Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Host Sweep**

  ホストでオープン ポートを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用してシグニチャを作成し、ストレージ キーは Axxx に設定されます。

- **Port Sweep**

  ネットワークでホストを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは AxBx に設定されます。

ステップ 13 に進みます。

ステップ 12 単一パケットの場合、次のいずれかの検査オプションを選択します。

- **Header Data Only**

  センサーが検査するパケットの一部としてヘッダーを指定します。

- **Payload Data Only**

  センサーが検査するパケットの一部としてペイロードを指定します。

ステップ 13 に進みます。

ステップ 13 このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。

カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. **SubSignature ID** フィールドに数値を入力します。

デフォルトは 0 です。

似ているシグニチャをグループにまとめるには、サブシグニチャ ID を設定します。

c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドにデフォルトの名前が表示されます。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注） アラートが生成されると、シグニチャ名はシグニチャ ID とサブシグニチャ ID とともにイベント ビューアに報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるようにテキストを追加できます。アラートが生成されると、このテキストはイベント ビューアに報告されます。

e. （オプション）**User Comments** フィールドにテキストを入力します。

ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。

ステップ 14 エンジン固有のパラメータに値を割り当て、**Next** をクリックします。

ヒント + アイコンは、このシグニチャに使用可能なパラメータがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑色のアイコンをクリックしてこのパラメータのフィールドをアクティブにし、値を編集します。

ステップ 15 次のアラート応答オプションを指定します。

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。

b. センサーがアラートを送信したときにイベント ビューアが報告する重大度を選択します。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 16 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。

（注） シグニチャの反応頻度は制御できます。たとえば、センサーから送られるアラートの量を減らす場合があります。または、シグニチャの反応を 1 つのアラートにまとめたい場合があります。また、IPS に偽のトラフィックを送り、IDS が短時間に大量のアラートを発生させるようにする「Stick」などの IPS 対抗ツールに対応させる場合があります。

ステップ 17 イベント カウント、キー、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. **Event Count Key** として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Event Count Key** として **Attacker address** を選択します。

c. レートに基づいてイベントをカウントする場合は、**Use Event Interval** を選択してから、間隔に使用する秒数を指定します。

d. **Next** をクリックして続行します。

Alert Summarization ウィンドウが表示されます。

ステップ 18 アラートの量を制御し、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択します。

- **Alert Every Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを検出するたびにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応するたびにアラートを送信するのではなく、このシグニチャのサマリー アラートだけを送信することを指定します。その後、追加のしきい値を指定して、センサーがアラートのボリュームを動的に調整できるようにします。

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔におけるすべてのアドレス セットのすべてのアラートのサマリーを示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

- **Summary Interval (seconds)**

  レートに基づいてイベントをカウントすることを指定し、時間間隔に使用する秒数を示します。

- **Specify Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャが初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

- **Global Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーは単一のサマリー アラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

d. Global Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

e. **Next** をクリックして続行します。

ステップ 19 **Finish** をクリックし、変更を保存します。

Create Custom Signature ダイアログボックスが表示されます。

ステップ 20 **Yes** をクリックして、カスタム シグニチャを作成します。

ヒント 変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。

String TCP シグニチャの例

String エンジンは、ICMP、TCP、および UDP の各プロトコル用の汎用のパターン マッチング検査エンジンです。String エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現エンジンを使用します。

String ICMP、String TCP、および String UDP の 3 つの String エンジンがあります。

Custom Signature Wizard を使用して、カスタム String TCP シグニチャを作成します。String エンジンの詳細については、付録 B「シグニチャ エンジン」を参照してください。

(注) 次の手順は、カスタム String ICMP シグニチャと UDP シグニチャを作成する場合にも適用されます。

カスタム String TCP 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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意 カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　**Yes** オプション ボタンをクリックし、**String TCP** を **Select Engine** リストから選択し、**Next** をクリックします。

Signature Identification ウィンドウが表示されます。

ステップ 5　このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。

   カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. **SubSignature ID** フィールドに数値を入力します。

   デフォルトは 0 です。

   似ているシグニチャをグループにまとめるには、サブシグニチャ ID を設定します。

c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドに、デフォルトの名前である My Sig が表示されます。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注） アラートが生成されると、シグニチャ名はシグニチャ ID とサブシグニチャ ID とともに Event Viewer に報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるようにテキストを追加できます。アラートが生成されると、このテキストはイベント ビューアに報告されます。デフォルトは My Sig Info です。

e. （オプション）**User Comments** フィールドにテキストを入力します。

ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは Sig Comment です。

Next をクリックします。

Engine Specific Parameters ウィンドウが表示されます。

ヒント + アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 6　イベント アクションを割り当てます。

デフォルトは Produce Alert です。セキュリティ ポリシーに基づいて、拒否やブロックなど、より多くのアクションを割り当てることができます。

ヒント 複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

ステップ 7　**Direction** の横にある緑色のアイコンをクリックし、トラフィックの方向を選択します。

- **From Service**：サービス ポートからクライアント ポートに向かうトラフィック。
- **To Service**：クライアント ポートからサービス ポートに向かうトラフィック。

ステップ 8　**Regex String** フィールドで、シグニチャが TCP パケットに対して検査する文字列を指定します。

ステップ 9　**Service Ports** フィールドに、ポート（23 など）を指定します。

Service Ports は、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です。

ステップ 10（オプション）このシグニチャに次のオプション パラメータを設定できます。

- **Specify Exact Match Offset**：完全一致オフセットをイネーブルにします。これは、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のある実際のストリーム オフセットです（0 ～ 65535）。
- **Specify Min Match Length**：最小一致の長さをイネーブルにします。これは、正規表現文字列が一致する必要のある最小バイト数です（0 ～ 65535）。
- **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。
- **Swap Attacker Victim**：アドレス（およびポート）の送信元と宛先をアラート メッセージでスワップします。

ステップ 11 **Next** をクリックします。

Alert Response ウィンドウが表示されます。

ステップ 12 必要に応じて、次のデフォルトのアラート応答オプションを変更します。

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。デフォルトは 75 です。

b. センサーがアラートを送信したときにイベント　ビューアが報告する重大度を選択します。デフォルトは Medium です。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 13 **Next** をクリックします。

Alert Behavior ウィンドウが表示されます。

ステップ 14 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。デフォルト アラート動作を変更する場合は、ステップ 15 ～ 21 を実行します。変更しない場合は、**Finish** をクリックすると、カスタム シグニチャが作成されます。

（注） シグニチャの反応頻度は制御できます。たとえば、センサーから送られるアラートの量を減らす場合があります。または、シグニチャの反応を 1 つのアラートにまとめたい場合があります。また、IPS に偽のトラフィックを送り、IDS が短時間に大量のアラートを発生させるようにする「Stick」などの IPS 対抗ツールに対応させる場合があります。

ステップ 15 イベント カウント、キー、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. Event Count Key として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、Event Count Key として **Attacker Address** を選択します。

c. レートに基づいてイベントをカウントする場合は、**Use Event Interval** を選択してから、間隔に使用する秒数を指定します。

d. **Next** をクリックして続行します。

Alert Summarization ウィンドウが表示されます。

ステップ 16 アラートの量を制御し、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択して、**Next** をクリックします。

- **Alert Every Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを検出するたびにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応するたびにアラートを送信するのではなく、このシグニチャのサマリー アラートだけを送信することを指定します。その後、追加のしきい値を指定して、センサーがアラートのボリュームを動的に調整できるようにします。

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔におけるすべてのアドレス セットのすべてのアラートのサマリーを示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

Alert Dynamic Response ウィンドウが表示されます。

ステップ 17 アラートの動的な応答を設定します。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

- **Summary Interval (seconds)**

  レートに基づいてイベントをカウントすることを指定し、時間間隔に使用する秒数を示します。

- **Specify Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャが初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

- **Global Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーは単一のサマリー アラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

d. Global Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

ステップ 18 **Finish** をクリックし、変更を保存します。

Alert Behavior ウィンドウが表示されます。

ステップ 19 **Finish** をクリックします。

Create Custom Signature ダイアログボックスが表示され、このカスタム シグニチャがセンサーに適用されます。

ステップ 20 **Yes** をクリックして、カスタム シグニチャを作成します。

ヒント 変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。

Service HTTP シグニチャの例

Service HTTP エンジンは、サービス固有で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よく使用されているプロトコルです。また、これには最も長い事前処理時間が必要であり、検査を必要とする最大数のシグニチャを持つため、システムのパフォーマンス全体にとって重大となります。

Service HTTP エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現ライブラリを使用します。このエンジンは、Web サービスだけに送られるトラフィック、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。このエンジンの各シグニチャで、該当する個別の Web ポートを指定できます。

HTTP 解読は、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。これは、ASCII 正規化とも呼ばれます。

HTTP パケットを検査するには、まずデータを、ターゲット システムでデータの処理時に表示されるものと同じ表記に解読または正規化する必要があります。どのオペレーティング システムおよび Web サーバ バージョンがターゲットで動作しているかを認識している、カスタマイズされたデコード技術をホスト ターゲット タイプごとに用意することを推奨します。Service HTTP エンジンには、Microsoft IIS Web サーバに対するデフォルトの解読動作があります。

Custom Signature Wizard を使用して、カスタム Service HTTP シグニチャを作成します。Service HTTP エンジンの詳細については、P.B-24 の「Service HTTP エンジン」を参照してください。

カスタム Service HTTP 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 管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2 **Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意 カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　**Yes** オプション ボタンをクリックし、**Service HTTP** を Select Engine リストから選択し、**Next** をクリックします。

Signature Identification ウィンドウが表示されます。

ステップ 5　このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。

カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. **SubSignature ID** フィールドに数値を入力します。

デフォルトは 0 です。

似ているシグニチャをグループにまとめるには、サブシグニチャ ID を設定します。

c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドに、デフォルトの名前である My Sig が表示されます。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注）　アラートが生成されると、シグニチャ名はシグニチャ ID とサブシグニチャ ID とともにイベント ビューアに報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるようにテキストを追加できます。アラートが生成されると、このテキストはイベント ビューアに報告されます。デフォルトは My Sig Info です。

e. （オプション）**User Comments** フィールドにテキストを入力します。

ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは Sig Comment です。

Next をクリックします。

Engine Specific Parameters ウィンドウが表示されます。

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 6　イベント アクションを割り当てます。

デフォルトは Produce Alert です。セキュリティ ポリシーに基づいて、拒否やブロックなど、より多くのアクションを割り当てることができます。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

ステップ 7　**De Obfuscate** の横にある緑色のアイコンをクリックし、**Yes** を選択し、検索の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。

ステップ 8　（オプション）Max Field Sizes で、最大フィールド サイズに対して次のオプション パラメータを設定できます。

- Specify Max URI Field Length：最大 URI フィールド長をイネーブルにします。
- Specify Max Arg Field Length：最大引数フィールド長をイネーブルにします。
- Specify Max Header Field Length：最大ヘッダー フィールド長をイネーブルにします。
- Specify Max Request Field Length：最大要求フィールド長をイネーブルにします。

ステップ 9　Regex で、regex パラメータを設定します。

a. Specify URI Regex には **Yes** を選択します。

b. **URI Regex** フィールドで URI Regex を指定します（[Mm][Yy][Ff][Oo][Oo] など）。

c. 次のオプション パラメータの値を指定できます。

- Specify Arg Name Regex：特定の正規表現の Arguments フィールドの検索をイネーブルにします。
- Specify Header Regex：特定の正規表現の Header フィールドの検索をイネーブルにします。
- Specify Request Regex：特定の正規表現の Request フィールドの検索をイネーブルにします。

ステップ 10　**Service Ports** フィールドで、ポートを指定します。たとえば、Web ポート変数の $WEBPORTS を使用します。

Service Ports は、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です。

ステップ 11　（オプション）**Swap Attacker Victim** の横にある緑色のアイコンをクリックし、**Yes** を選択し、送信元と宛先のアドレス（およびポート）をアラート メッセージでスワップするようにします。

ステップ 12　**Next** をクリックします。

Alert Response ウィンドウが表示されます。

ステップ 13　（オプション）次のデフォルトのアラート応答オプションを変更します。

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。デフォルトは 75 です。

b. センサーがアラートを送信したときにイベント　ビューアが報告する重大度を選択します。デフォルトは Medium です。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 14 **Next** をクリックします。

Alert Behavior ウィンドウが表示されます。

ステップ 15 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。デフォルト アラート動作を変更する場合は、ステップ 15 ～ 21 を実行します。変更しない場合は、**Finish** をクリックすると、カスタム シグニチャが作成されます。

(注) シグニチャの反応頻度は制御できます。たとえば、センサーから送られるアラートの量を減らす場合があります。または、シグニチャの反応を 1 つのアラートにまとめたい場合があります。また、IPS に偽のトラフィックを送り、IDS が短時間に大量のアラートを発生させるようにする「Stick」などの IPS 対抗ツールに対応させる場合があります。

ステップ 16 イベント カウント、キー、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. Event Count Key として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、Event Count Key として **Attacker Address** を選択します。

c. レートに基づいてイベントをカウントする場合は、**Use Event Interval** を選択してから、間隔に使用する秒数を指定します。

d. **Next** をクリックして続行します。

Alert Summarization ウィンドウが表示されます。

ステップ 17 アラートの量を制御し、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択して、**Next** をクリックします。

- **Alert Every Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを検出するたびにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、センサーがアラートのボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応するたびにアラートを送信するのではなく、このシグニチャのサマリー アラートだけを送信することを指定します。**その後、追加のしきい値を指定して、センサーがアラートのボリュームを動的に調整できるようにします。**

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔におけるすべてのアドレス セットのすべてのアラートのサマリーを示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

Alert Dynamic Response ウィンドウが表示されます。

ステップ 18 アラートの動的な応答を設定します。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

- **Summary Interval (seconds)**

  レートに基づいてイベントをカウントすることを指定し、時間間隔に使用する秒数を示します。

- **Specify Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャが初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

- **Global Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **Global Summary Threshold**

  グローバル サマリー アラートを送信する前にセンサーが受信すべき最小ヒット数を示します。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーは単一のサマリー アラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

d. Global Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

ステップ 19 **Finish** をクリックし、変更を保存します。

Alert Behavior ウィンドウが表示されます。

ステップ 20 **Finish** をクリックします。

Create Custom Signature ダイアログボックスが表示され、このカスタム シグニチャがセンサーに適用されます。

ステップ 21 **Yes** をクリックして、カスタム シグニチャを作成します。

ヒント 変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。

イベント アクション ルールの設定

この章では、イベント アクション ルールを設定する方法を説明します。この章は、次の項で構成されています。

- イベント アクション ルールについて（P.7-2）
- イベント変数の設定（P.7-11）
- Target Value Rating の設定（P.7-14）
- イベント アクション オーバーライドの設定（P.7-17）
- イベント アクション フィルタの設定（P.7-22）
- 一般的な設定値の設定（P.7-30）
- イベントの監視（P.7-33）

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用の設定のグループです。これらのルールは、イベントが発生したときにセンサーが実行するアクションを指定します。

イベント アクション処理コンポーネントは、次の機能を担当します。

- リスク評価の計算
- 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
- 結果のイベント アクションの実行
- イベントの要約と集約
- 拒否された攻撃者リストの管理

この項で取り上げる事項は次のとおりです。

- リスク評価の計算（P.7-2）
- イベント オーバーライド（P.7-3）
- イベント アクション フィルタ（P.7-3）
- イベント アクションの要約と集約（P.7-3）
- Signature Event Action Processor（P.7-4）
- イベント アクション（P.7-7）
- イベント アクション ルールの例（P.7-9）

リスク評価の計算

RR 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、0 から 100 の間の数値で表した評価です。計算では、攻撃されているネットワーク資産（特定のサーバなど）の価値も考慮されるため、RR はシグニチャ単位（ASR および SFR）およびサーバ単位（TVR）で設定されます。

RR を使用すると、注意の必要なアラートの優先順位を高くすることができます。このような RR の要素としては、成功した場合の攻撃の重大度、シグニチャの忠実度、およびターゲット ホストの全体の価値が考慮に入れられています。RR は evIdsAlert で報告されます。

特定のイベントの RR の計算には、次の値が使用されます。

- **Attack Severity Rating（ASR）**：脆弱性の不正利用に成功した場合の重大度に関連付ける重み値。

  ASR は、シグニチャのアラート重大度パラメータから取得されます。
- **Sig Fidelity Rating（SFR）**：対象とする特定の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値。

  SFR は、シグニチャ作成者によってシグニチャごとに計算されます。シグニチャ作成者は、資格を与える情報がターゲットにない場合のシグニチャの精度について、基本的な信頼度を定義します。この信頼度は、分析中のパケットの送達が許可された場合に、検出された動作がどの程度確実にターゲット プラットフォームに目的とする効果を与えるかを表します。たとえば、きわめて具体的なルール（特定の正規表現など）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高い SFR を持ちます。
- **Target Value Rating（TVR）**：明確化されたターゲットの価値に関連付ける重み値。

  TVR は、ネットワーク資産（IP アドレスを経由する）の重要性を示す、ユーザが設定可能な値です。価値の高い企業リソースにはより厳しいセキュリティ ポリシーを作成し、そうでないリソースにはある程度緩やかなポリシーを作成できます。たとえば、企業の Web サーバには、デ

スクトップ ノードに割り当てる TVR より高い TVR を割り当てることができます。この場合、企業の Web サーバに対する攻撃は、デスクトップ ノードに対する攻撃よりも高い RR を持ちます。

（注）RR は、ASR、SFR、TVR、およびオプションの Promiscuous Delta（PD; 混合デルタ）から計算されます。

イベント オーバーライド

イベントの RR に基づいて、イベントに関連付けられたアクションを変更するために、イベント アクション オーバーライドを追加できます。イベント アクション オーバーライドを使用すると、各シグニチャを個別に設定しなくても、グローバルにイベント アクションを追加することができます。各イベント アクションには、一定範囲の RR が関連付けられています。シグニチャ イベントが発生し、そのイベントの RR が特定のイベント アクションの範囲内にある場合は、そのアクションがイベントに追加されます。たとえば、RR が 85 以上のイベントでは SNMP トラップを生成する場合には、**Request SNMP Trap** の RR 範囲を **85 ～ 100** に設定できます。アクションの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。

イベント アクション フィルタ

イベント アクション フィルタは、順番に並べられたリストとして処理されます。フィルタのリスト内の順番は上下に移動できます。

センサーは、フィルタの使用により、イベントに応答してすべてのアクションを実行せずに特定のアクションを実行したり、イベント全体を削除することができます。フィルタは、イベントからアクションを削除することによって機能します。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、効果的にイベントを消滅させます。

（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お勧めします。複数の宛先アドレスが存在する場合は、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 アクションの要約と集約

この項では、イベント アクションの要約方法と集約方法について説明します。取り上げる事項は次のとおりです。

- イベント アクションの要約（P.7-3）
- イベント アクションの集約（P.7-4）

イベント アクションの要約

要約すると、センサーから送出されるアラームの量を減らし、多数のイベントを 1 つのアラームにまとめる基本的な集約を実行します。各シグニチャに対して特別なパラメータが指定され、それぞれアラートの処理に影響を与えます。各シグニチャは、最適な通常の動作を反映したデフォルトの設定で作成されます。ただし、各シグニチャを調整して、各エンジン タイプの制限内でこのデフォルトの動作を変更できます。

要約されていない各シグニチャ イベントでは、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）はフィルタを通過します。このような要約されたアラートでは、アラートを生成するアクションは実行されません。代わりに、そのようなアクションは 1 つのサマリー アラートに適用され、その後フィルタにかけられます。

その他のアラート生成アクションのいずれかを選択し、それにフィルタを適用しない場合は、**Produce Alert** を選択していない場合でもアラートが作成されます。アラートが生成されないようするには、アラートを生成するすべてのアクションがフィルタリングによって排除されるようにする必要があります。

要約とイベント アクションは、META 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。この処理により、センサーは一連のイベントにまたがって発生する不審なアクティビティを監視することができます。

イベント アクションの集約

基本集約機能には、2 種類の動作モードがあります。簡易モードでは、いくつのヒットがあるとアラートが送信されるかを示すしきい値をシグニチャに設定します。より高度なモードでは、間隔カウントを行います。このモードでは、センサーは 1 秒あたりのヒット数を追跡し、そのしきい値に達したときのみアラートを送信します。この例では、「ヒット」とはイベントを表すために使用する用語で、基本的にはアラートのことです。ただし、ヒット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出されません。

次の要約オプションを選択できます。

- **Fire All**：Fire All モードではシグニチャがトリガーされるたびにアラートが送出されます。要約にしきい値が設定されている場合は、要約が発生するまでは実行のたびにアラートが発生します。要約が開始されると、各アドレス セットで要約の間隔ごとに 1 つのアラートのみが発生します。異なるアドレス セットのアラートは、すべて表示されるか、個別に要約されます。該当のシグニチャで一定期間アラートが発生しないと、シグニチャは Fire All モードに戻ります。
- **Summary**：Summary モードでは、最初にシグニチャがトリガーされたときにアラートを送出します。そのシグニチャのそれ以降のアラートは、要約間隔ごとに要約されます。各アドレス セットで要約の間隔ごとに 1 つのアラートのみが発生します。グローバル サマリーのしきい値に達すると、シグニチャは Global Summarization モードに入ります。
- **Global Summarization**：Global Summarization モードでは、要約間隔ごとに 1 つのアラートを送出します。シグニチャにグローバル サマリーを事前設定しておくこともできます。
- **Fire Once**：Fire Once モードではアドレス セットごとにアラートを送出します。このモードを Global Summarization モードにアップグレードすることができます。

Signature Event Action Processor

SEAP は、アラーム チャネル内のシグニチャ イベントから、SEAO、SEAF の処理を経由して SEAH で処理されるまでのデータ フローを調整します。これ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

  Sensor App 検査パスからシグニチャ イベント処理へ向かうシグニチャ イベントと通信するエリアを表す単位。
- シグニチャ イベント アクション オーバーライド（SEAO）

  RR 値に基づいて、アクションを追加します。SEAO は、設定済みの RR しきい値の範囲に該当するすべてのシグニチャに適用されます。各 SEAO 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。詳細については、P.7-2 の「リスク評価の計算」を参照してください。

- シグニチャ イベント アクション フィルタ（SEAF）

  シグニチャ イベントのシグニチャ ID、アドレス、および RR に基づいてアクションを削除します。SEAF へ入力するのは、SEAO 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） SEAF が実行できるのはアクションの削除だけであり、新規アクションの追加はできません。

  SEAF には、次のパラメータが適用されます。

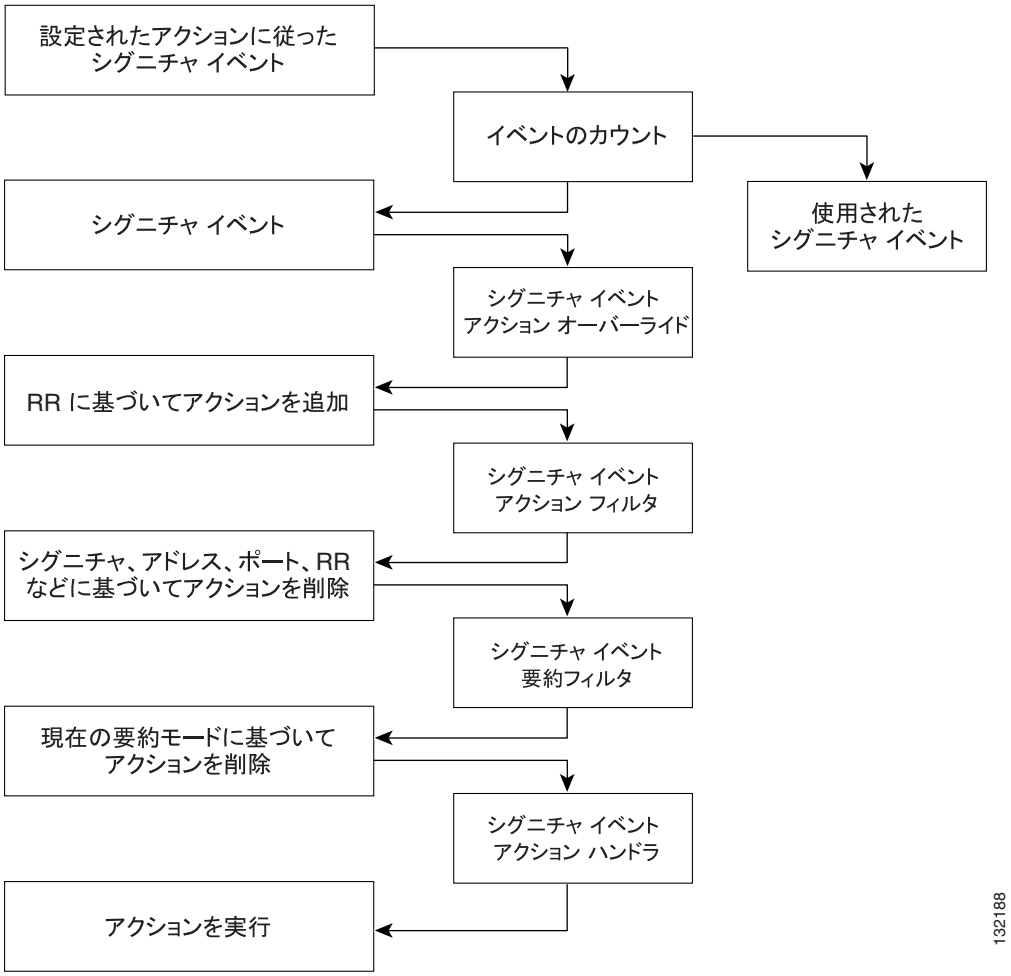
  — シグニチャ ID
  — サブシグニチャ ID
  — 攻撃者のアドレス
  — 攻撃者のポート
  — 被害先のアドレス
  — 被害先のポート
  — RR しきい値の範囲
  — 削除するアクション
  — シーケンス識別子（オプション）
  — ストップ ビットまたは継続ビット
  — アクション フィルタ行をイネーブルにするビット

- シグニチャ イベント アクション ハンドラ（SEAH）

  要求されたアクションを実行します。SEAH 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 7-1 は、SEAP を通過するシグニチャ イベントの論理フローと、このイベントのアクションで実行される操作を示しています。これは、アラーム チャネルで受信された設定済みアクションを持つシグニチャ イベントで開始され、シグニチャ イベントが SEAP 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 7-1　SEAP を通過するシグニチャ イベント



イベント アクション

表 7-1 は、イベント アクションについて説明しています。

表 7-1　イベント アクション

イベント アクション名	説明
Deny Attacker Inline	（インライン モードのみ）指定された期間、攻撃者アドレスから発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。[1] **（注）** これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。
Deny Attacker Service Pair Inline	（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。 **（注）** 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。
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 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。
Log Attacker Packets	攻撃者アドレスを含む IP ロギング パケットを開始します。 **（注）** このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Log Pair Packets	攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。 **（注）** このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Log Victim Packets	被害先アドレスを含む IP ロギング パケットを開始します。

表 7-1　イベント アクション（続き）

イベント アクション名	説明
Modify Packet Inline	パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。 (注) Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。
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	違反パケットの符号化ダンプをアラートに組み込みます。 (注) このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Request Block Connection	この接続をブロックする要求を ARC に送信します。 (注) ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
Request Block Host	この攻撃者ホストをブロックする要求を ARC に送信します。 (注) ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 (注) ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。
Request Rate Limit	レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 (注) Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

表 7-1　イベント アクション（続き）

イベント アクション名	説明
Request SNMP Trap	SNMP 通知を実行する要求を NotificationApp に送信します。 **（注）** このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
Reset TCP Connection	TCP リセットを送信し、TCP フローを乗っ取って終了します。 **（注）** Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

1. センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

注意　シグニチャに対してアラートをイネーブルにした場合、Produce Alert アクションは自動にはなりません。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。2 番目のアクションを追加する場合、イベント ストアにアラートを送信するには、Produce Alert を組み込む必要があります。また、イベント アクションを設定するたびに、新規リストが作成され、古いリストが置換されます。各シグニチャに必要なイベント アクションを必ずすべて組み込んでください。

イベント アクション ルールの例

次の例は、イベント アクション ルールの個々のコンポーネントがどのように連携して動作するかを示しています。

例 1 のリスク評価範囲

- **Produce Alert**：1 ～ 100
- **Produce Verbose Alert**：90 ～ 100
- **Request SNMP Trap**：50 ～ 100
- **Log Pair Packets**：90 ～ 100
- **Log Victim Packets**：90 ～ 100
- **Log Attacker Packets**：90 ～ 100
- **Reset TCP Connection**：90 ～ 100
- **Request Block Connection**：70 ～ 89
- **Request Block Host**：90 ～ 100
- **Deny Attacker Inline**：0 ～ 0
- **Deny Connection Inline**：90 ～ 100
- **Deny Packet Inline**：90 ～ 100

例 1 のイベント アクション フィルタ

1. SigID=2004, Attacker Address=*, Victim Address=20.1.1.1, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
2. SigID=2004, Attacker Address=30.1.1.1, Victim Address=*, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
3. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=None, Risk Rating Range=95-100, StopOnMatch=True
4. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, requestBlockConnection, Risk Rating Range=56-94, StopOnMatch=True
5. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, produceAlert, resetTcpConnection, logAttackerPackets, Risk Rating Range=1-55, StopOnMatch=True

例 1 の結果

SIG 2004 が検出された場合：

- 攻撃者アドレスが 30.1.1.1 であるか、または被害先のアドレスが 20.1.1.1 である場合、イベントは消滅します（ALL アクションは削除されます）。

攻撃者アドレスが 30.1.1.1 以外で、被害先アドレスが 20.1.1.1 以外である場合：

- RR が 50 の場合、**Produce Alert** および **Request SNMP Trap** はイベント アクション オーバーライド コンポーネントによって追加されますが、**Produce Alert** はイベント アクション フィルタによって削除されます。ただし、**Request SNMP Trap** は <evIdsAlert> に依存しているため、イベント アクション ポリシーがアラート アクションを強制的に適用します。
- RR が 89 の場合、**Request SNMP Trap** および **Request Block Connection** はイベント アクション オーバーライド コンポーネントによって追加されます。ただし、**Request Block Connection** はイベント アクション フィルタによって削除されます。
- RR が 96 の場合、**Deny Attacker Inline** および **Request Block Connection** を除くすべてのアクションがイベント アクション オーバーライド コンポーネントによって追加され、イベント アクション フィルタは何も削除しません。フィルタ アクションが NONE に指定された 3 番目のフィルタ行はオプションですが、このタイプのフィルタを定義するより明確な方法として示されています。

イベント変数の設定

この項では、イベント変数の設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-11）
- サポートされるユーザのロール（P.7-11）
- フィールド定義（P.7-12）
- イベント変数の設定（P.7-12）

概要

イベント変数を作成し、イベント アクション フィルタの中でそれらの変数を使用できます。複数のフィルタ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フィルタは新しい値で更新されます。

（注） 変数の前にドル記号（$）を付けて、文字列ではなく変数を使用していることを示す必要があります。

シグニチャ システムに必要なため、削除できない変数もあります。変数が保護されている場合は、それを選択して編集することはできません。保護された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。

IP アドレスを設定する場合は、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。次の例を参考にしてください。

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

ワンポイント・アドバイス たとえば、社内の技術グループに対応する IP アドレス空間があるとします。グループ内には Windows システムがなく、Windows ベースの攻撃を心配する必要はありません。このような場合、変数を技術グループの IP アドレス空間として設定します。その後、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。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント変数を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント変数のフィールドの定義を示します。取り上げる事項は次のとおりです。

- Event Variables パネル（P.7-12）
- Add and Edit Event Variable ダイアログボックス（P.7-12）

Event Variables パネル

Event Variables パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に名前を割り当てます。
- **Type**：変数をアドレスとして指定します。
- **Value**：この変数によって表される値を追加します。

ボタンの機能：

- **Add**：Add Variable ダイアログボックスを表示します。
  このダイアログボックスで、変数を追加し、その変数に関連付ける値を指定できます。
- **Edit**：Edit Variable ダイアログボックスを表示します。
  このダイアログボックスで、この変数に関連付けられた値を変更できます。
- **Delete**：使用可能な変数のリストから選択した変数を削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Variable ダイアログボックス

Add and Edit Event Variable ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に名前を割り当てます。
- **Type**：変数をアドレスとして指定します。
- **Value**：この変数によって表される値を追加します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

イベント変数の設定

イベント変数を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Event Action Rules > Event Variables** をクリックします。

Event Variables パネルが表示されます。

ステップ 3　**Add** をクリックして、変数を作成します。

Add Variable ダイアログボックスが表示されます。

ステップ 4　**Name** フィールドに変数の名前を入力します。

（注）　名前には、数字または文字だけを使用できます。ハイフン（-）または下線（_）は使用できます。

ステップ 5　**Value** フィールドに変数の値を入力します。

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。次の例を参考にしてください。

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

（注）　デリミタにはカンマが使用できます。カンマの後にはスペースを入れないでください。スペースを入力すると、`Validation failed` エラーが生じます。

ヒント　変更を元に戻し、Add Variable ダイアログを閉じるには、**Cancel** をクリックします。

ステップ 6　**OK** をクリックします。

Event Variables パネルのリストに新しい変数が表示されます。

ステップ 7　既存の変数を編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Variable ダイアログボックスが表示されます。

ステップ 8　**Value** フィールドの値を変更します。

ヒント　変更を元に戻し、Edit Variable ダイアログを閉じるには、**Cancel** をクリックします。

ステップ 9　**OK** をクリックします。

Event Variables パネルのリストに編集したイベント変数が表示されます。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 10　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

Target Value Rating の設定

この項では、ターゲットの価値評価を設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-14）
- サポートされるユーザのロール（P.7-14）
- フィールド定義（P.7-14）
- Target Value Rating の設定（P.7-15）

概要

TVR をネットワーク資産に割り当てることができます。TVR は各アラートの RR 値の計算に使用される要素の 1 つです。ターゲットごとに異なる TVR を割り当てることができます。RR の高いイベントほど、より厳しいシグニチャ イベント アクションをトリガーします。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ターゲットの価値評価を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、TVR のフィールドの定義を示します。取り上げる事項は次のとおりです。

- Target Value Rating パネル（P.7-14）
- Add and Edit Target Value Rating ダイアログボックス（P.7-15）

Target Value Rating パネル

Target Value Rating パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Target Value Rating (TVR)**：このネットワーク資産に割り当てる値を示します。値は、High、Low、Medium、Mission Critical、No Value のいずれかになります。
- **Target IP Address**：TVR によって優先順位付けするネットワーク資産の IP アドレスを示します。

ボタンの機能：

- **Select All**：設定済みのターゲットをすべて選択します。
- **Add**：Add Target Value Rating ダイアログボックスを表示します。

  このダイアログボックスで、ネットワーク資産の IP アドレスを追加し、その資産に TVR を割り当てることができます。
- **Edit**：Edit Target Value Rating ダイアログボックスを表示します。

  このダイアログボックスで、ネットワーク資産の IP アドレスを変更できます。
- **Delete**：使用可能な評価のリストから選択した TVR を削除します。

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Target Value Rating ダイアログボックス

Add and Edit Target Value Rating ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Target Value Rating (TVR)**：このネットワーク資産に割り当てる値を示します。値は、High、Low、Medium、Mission Critical、No Value のいずれかになります。
- **Target IP Address(es)**：TVR によって優先順位付けするネットワーク資産の IP アドレスを示します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

Target Value Rating の設定

TVR を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Event Action Rules > Target Value Rating** をクリックします。

Target Value Rating パネルが表示されます。

ステップ 3　**Add** をクリックして、TVR を作成します。

Add Target Value Rating ダイアログボックスが表示されます。

ステップ 4　新しい資産グループに TVR を割り当てるには、次の手順を実行します。

a. **Add** をクリックして、新しいネットワーク資産のグループを追加します。

b. Target Value Rating リスト ボックスから評価を選択します。

値は、**High**、**Low**、**Medium**、**Mission Critical**、**No Value** のいずれかになります。

c. **Target IP Address(es)** フィールドにネットワーク資産の IP アドレスを入力します。

IP アドレスの範囲を入力するには、範囲の最小のアドレスに続けて、ハイフンと範囲の最大のアドレスを入力します。例：10.10.2.1-10.10.2.30。

ヒント　変更を元に戻して Add Target Value Rating ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 5　**OK** をクリックします。

Target Value Rating パネルのリストに新しい資産の新しい TVR が表示されます。

ステップ 6　既存の TVR を編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Target Value Rating ダイアログボックスが表示されます。

ステップ 7　**Target IP Address(es)** フィールドの値を変更します。

ヒント　変更を元に戻して Edit Target Value Rating ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 8　**OK** をクリックします。

Target Value Rating パネルのリストに編集したネットワーク資産が表示されます。

ステップ 9　ネットワーク資産を削除するには、リスト内でそれを選択して **Delete** をクリックします。

このネットワーク資産は Target Value Rating パネルのリストから消去されます。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 10　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

イベント アクション オーバーライドの設定

この項では、イベント アクション オーバーライドの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-17）
- サポートされるユーザのロール（P.7-17）
- フィールド定義（P.7-17）
- イベント アクション オーバーライドの設定（P.7-20）

概要

イベントの詳細に基づいてイベントに関連付けられたアクションを変更するために、イベント アクション オーバーライドを追加できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション オーバーライドを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント アクション オーバーライドのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Event Action Overrides パネル（P.7-17）
- Add and Edit Event Action Overrides ダイアログボックス（P.7-18）

Event Action Overrides パネル

Event Action Overrides パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Use Event Action Overrides**：選択すると、イネーブルなイベント アクション オーバーライドをすべて使用できます。
- **Event Action**：このイベント アクション オーバーライドの条件が満たされた場合に、イベントに追加するイベント アクションを指定します。
- **Enabled**：このオーバーライドがイネーブルであるかどうかを示します。
- **Risk Rating**：このイベント アクション オーバーライドをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合に、イベント アクションをこのイベントに追加します。

ボタンの機能：

- **Select All**：テーブルに表示されたすべてのイベント アクション オーバーライドを選択します。

- **Add**：Add Event Action Override ダイアログボックスを表示します。

  このダイアログボックスで、イベント アクション オーバーライドを追加し、そのオーバーライドに関連付ける値を指定できます。
- **Edit**：Edit Event Action Override ダイアログボックスを表示します。

  このダイアログボックスで、このイベント アクション オーバーライドに関連付けられた値を変更できます。
- **Enable**：選択したイベント アクション オーバーライドをイネーブルにします。

  Event Action Overrides パネルの **Use Event Action Overrides** チェックボックスをオンにする必要があります。オンにしないと、設定した値に関係なくイベント アクション オーバーライドはイネーブルになりません。
- **Disable**：選択したイベント アクション オーバーライドをディセーブルにします。
- **Delete**：使用可能なオーバーライドのリストから選択したイベント アクションを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Action Overrides ダイアログボックス

Add and Edit Event Action Overrides ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Event Action**：このイベント アクション オーバーライドの条件が満たされた場合に、イベントに追加するイベント アクションを指定します。
  - **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

    センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

    （注） これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

  - **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

    （注） 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。

（注） Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。

- **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注） ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Enabled**：**Yes** チェックボックスをオンにするとオーバーライドはイネーブルになり、**No** チェックボックスをオンにするとオーバーライドはディセーブルになります。
- **Risk Rating**：このイベント アクション オーバーライドをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合に、イベント アクションをこのイベントに追加します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

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 オーバーライドを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Event Action Rules** > **Event Action Overrides** をクリックします。

Event Action Overrides パネルが表示されます。

ステップ 3　**Add** をクリックして、イベント アクション オーバーライドを作成します。

Add Event Action Override ダイアログボックスが表示されます。

ステップ 4　**Event Action** リストから、このイベント アクション オーバーライドに対応するイベント アクションを選択します。

ステップ 5　Enabled の下の **Yes** チェックボックスをオンにします。

ステップ 6　Risk Rating の下の **Minimum** フィールドおよび **Maximum** フィールドで、RR 範囲をこのネットワークに割り当てます。

値はすべて 0 ～ 100 までで、**Minimum** フィールドの値は **Maximum** フィールドの値以下にする必要があります。

ヒント　変更を元に戻して Add Event Action Override ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 7　**OK** をクリックします。

Event Action Overrides パネルのリストに新しいイベント アクション オーバーライドが表示されます。

ステップ 8　**Use Event Action Overrides** チェックボックスをオンにします。

（注）　Event Action Overrides パネルの **Use Event Action Overrides** チェックボックスをオンにする必要があります。オンにしないと、設定した値に関係なくイベント アクション オーバーライドはイネーブルになりません。

ステップ 9 既存のイベント アクション オーバーライドを編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Action Override ダイアログボックスが表示されます。

ステップ 10 Enabled の下の **Yes** チェックボックスをオンにします。

ステップ 11 Risk Rating の下の **Minimum** フィールドおよび **Maximum** フィールドで、RR 範囲をこのネットワークに割り当てます。

値はすべて 0 ～ 100 までで、**Minimum** フィールドの値は **Maximum** フィールドの値以下にする必要があります。

ヒント 変更を元に戻して Edit Event Action Override ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 12 **OK** をクリックします。

Event Action Overrides パネルのリストに編集したイベント アクション オーバーライドが表示されます。

ステップ 13 **Use Event Action Overrides** チェックボックスをオンにします。

(注) Event Action Overrides パネルの **Use Event Action Overrides** チェックボックスをオンにする必要があります。オンにしないと、設定した値に関係なくイベント アクション オーバーライドはイネーブルになりません。

ステップ 14 既存のイベント アクション オーバーライドを削除するには、リスト内でそれを選択して **Delete** をクリックします。

Event Action Overrides パネルのリストからそのイベント アクション オーバーライドが消去されます。

ステップ 15 イベント アクション オーバーライドをイネーブルまたはディセーブルにするには、**Enable** または **Disable** をクリックします。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 16 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

イベント アクション フィルタの設定

この項では、イベント アクション フィルタの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-22）
- サポートされるユーザのロール（P.7-22）
- フィールド定義（P.7-22）
- イベント アクション フィルタの設定（P.7-22）

概要

イベント アクション フィルタを設定して、イベントから特定のアクションを削除したり、センサーがそれ以上処理しないようにイベント全体を廃棄したりすることができます。Event Variables パネルで定義した変数を使用すれば、アドレスをグループ化してフィルタを適用できます。

（注） 変数の前にドル（$）記号を付けて、文字列ではなく変数を使用していることを示す必要があります。「$」を付けないと、`Bad source and destination` エラーが生じます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション フィルタを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント アクション フィルタのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Event Action Filters パネル（P.7-22）
- Add and Edit Event Action Filters ダイアログボックス（P.7-24）

Event Action Filters パネル

Event Action Filters パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Use Event Action Filters**：イベント アクション フィルタのコンポーネントをイネーブルにします。

  イネーブルなフィルタを使用するには、このチェックボックスをオンにする必要があります。
- **Name**：追加するフィルタに名前を指定します。

  必要に応じてフィルタをリスト内で移動したり、非アクティブ リストへ移動したりできるように、フィルタに名前を付けておく必要があります。

- **Active**：フィルタがフィルタ リストに配置されており、イベントのフィルタリングにおいて有効であるかどうかを示します。
- **Enabled**：このフィルタがイネーブルであるかどうかを示します。
- **Sig ID**：このシグニチャに割り当てられた固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。シグニチャの範囲を入力することもできます。
- **SubSig ID**：このサブシグニチャに割り当てられた固有の数値を示します。

  subSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。subSig ID の範囲を入力することもできます。
- **Attacker (address/port)**：違反パケットを送信したホストの IP アドレスまたはポート、もしくはその両方を示します。

  アドレスの範囲を入力することもできます。
- **Attacker (address/port)**：攻撃者のホストによって使用された IP アドレスまたはポート、もしくはその両方を示します。

  これは、違反パケットの発信元ポートです。ポートの範囲を入力することもできます。
- **Risk Rating**：このイベント アクション フィルタをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合、そのイベントはこのイベント フィルタのルールに従って処理されます。
- **Actions to Subtract**：イベントの条件がイベント アクション フィルタの基準を満たす場合に、イベントから除去する必要のあるアクションを示します。
- **Deny Pct**：拒否攻撃者機能によって拒否するパケットの率を示します。
- **Stop on Match**：このイベントをイベント アクション フィルタ リストの残りのフィルタについても処理するかどうかを決定します。

  No に設定すると、ストップ フラグが見つかるまで、残りのフィルタに対しても照合されます。

  Yes に設定すると、それ以上は処理されません。このフィルタによって指定されたアクションは除去され、残りのアクションが実行されます。
- **Comments**：このフィルタに関連付けられたユーザ コメントを示します。

ボタンの機能：

- **Select All**：リストに示されたイベント アクション フィルタをすべて選択します。
- **Add**：Add Event Action Filter ダイアログボックスを開きます。このダイアログボックスで、イベント アクション フィルタを追加し、そのフィルタに関連付ける値を指定できます。
- **Insert Before**：選択したイベント アクション フィルタの上にイベント アクション フィルタを追加します。

  Add Event Action Filter ダイアログボックスを開きます。
- **Insert After**：選択したイベント アクション フィルタの後ろにイベント アクション フィルタを追加します。

  Add Event Action Filter ダイアログボックスを開きます。
- **Move Up**：選択したフィルタをリスト内で 1 行上に移動し、フィルタの処理順序を変更します。
- **Move Down**：選択したフィルタをリスト内で 1 行下に移動し、フィルタの処理順序を変更します。
- **Edit**：Edit Event Action Filter ダイアログボックスを表示します。このダイアログボックスで、このフィルタに関連付けられた値を変更できます。
- **Active**：イベントのフィルタリングにおいて有効となるように、フィルタをフィルタ リストに追加します。
- **Inactive**：イベントのフィルタリングにおいて無効となるようにフィルタをリストから外します。

- **Enable**：選択したイベント アクション フィルタをイネーブルにします。

  Event Action Filters パネルの **Use Event Action Filters** チェックボックスをオンにする必要があります。オンにしないと、設定した値に関係なくイベント アクション フィルタはイネーブルになりません。
- **Disable**：選択したイベント アクション フィルタをディセーブルにします。
- **Delete**：使用可能なフィルタのリストからこのイベント アクション フィルタを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Action Filters ダイアログボックス

Add and Edit Event Action Filters ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：追加するフィルタに名前を指定します。

  必要に応じてフィルタをリスト内で移動したり、非アクティブ リストへ移動したりできるように、フィルタに名前を付けておく必要があります。
- **Active**：イベントのフィルタリングにおいて有効となるように、フィルタをフィルタ リストに追加します。
- **Enabled**：このフィルタがイネーブルであるかどうかを示します。
- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。シグニチャの範囲を入力することもできます。
- **SubSignature ID**：このサブシグニチャに割り当てられた固有の数値を示します。

  subSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。subSig ID の範囲を入力することもできます。
- **Attacker Address**：違反パケットを送信したホストの IP アドレスを示します。

  アドレスの範囲を入力することもできます。
- **Attacker Port**：攻撃者のホストによって使用されたポートを示します。

  これは、違反パケットの発信元ポートです。ポートの範囲を入力することもできます。
- **Victim Address**：攻撃を受けたホスト（違反パケットの受信者）の IP アドレスを示します。

  アドレスの範囲を入力することもできます。
- **Victim Port**：違反パケットを受信した場合にそのパケットが経由したポートを示します。

  ポートの範囲を入力することもできます。
- **Risk Rating**：このイベント アクション フィルタをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合、そのイベントはこのイベント フィルタのルールに従って処理されます。
- **Actions to Subtract**：イベントの条件がイベント アクション フィルタの基準を満たす場合に、イベントから除去する必要のあるアクションを示します。
  - **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

    センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

（注）これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

- **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

（注）拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。

（注）Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。

- **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**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

(注) ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request SNMP Trap**：SNMP 通知を実行する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ます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Deny Percentage**：拒否攻撃者機能によって拒否するパケットの率を決定します。有効範囲は 1 ～ 100 です。デフォルトは 100% です。
- **Stop on Match**：このイベントをイベント アクション フィルタ リストの残りのフィルタについても処理するかどうかを決定します。

  No に設定すると、ストップ フラグが見つかるまで、残りのフィルタに対しても照合されます。

  Yes に設定すると、それ以上は処理されません。このフィルタによって指定されたアクションは除去され、残りのアクションが実行されます。
- **Comments**：このフィルタに関連付けられたユーザ コメントを示します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Event Action Rules > Event Action Filters** をクリックします。

Event Action Filters パネルが表示されます。

ステップ 3　イベント アクション フィルタを作成するには、次のいずれかを実行します。

- 新しいイベント アクション フィルタを追加するには、**Add** をクリックします。
- もしくは、フィルタを現在のフィルタの上または下に追加するには、フィルタを右クリックして、**Insert Before** または **Insert After** を選択します。

Add Event Action Filter ダイアログボックスが表示されます。

ステップ 4　**Signature ID** フィールドに、フィルタを適用するすべてのシグニチャのシグニチャ ID を入力します。

シグニチャはリスト（2001, 2004）または範囲（2001–2004）で指定するか、Event Variables パネルで定義してあれば SIG 変数を使用して指定することもできます。変数の前には $ を付けます。

ステップ 5　**SubSignature ID** フィールドに、フィルタを適用するサブシグニチャのサブシグニチャ ID を入力します。

ステップ 6　**Attacker Address** フィールドに送信元ホストの IP アドレスを入力します。

Event Variables パネルで定義した場合は、変数のいずれかを使用できます。変数の前には $ を付けます。アドレスの範囲を入力することもできます（0.0.0.0 ～ 255.255.255.255）。

ステップ 7　**Attacker Port** フィールドに違反パケットを送信した攻撃者によって使用されたポート番号を入力します。

ステップ 8　**Victim Address** フィールドに受信側ホストの IP アドレスを入力します。

Event Variables パネルで定義した場合は、変数のいずれかを使用できます。変数の前には $ を付けます。アドレスの範囲を入力することもできます（0.0.0.0 ～ 255.255.255.255）。

ステップ 9　**Victim Port** フィールドに違反パケットを受信した被害先ホストによって使用されたポート番号を入力します。

ステップ 10　**Risk Rating** フィールドで、RR 範囲をこのフィルタに割り当てます。

イベントの RR が指定した範囲内の場合、イベントはこのフィルタの条件に従って処理されます。

ステップ 11　**Actions to Subtract** リストで、このフィルタによってイベントから削除するアクションを選択します。

ヒント　リスト内で複数のイベント アクションを選択するには、**Ctrl** キーを押した状態で選択します。

ステップ 12　**Deny Percentage** フィールドに、拒否攻撃者機能によって拒否するパケットの率を入力します。デフォルトは 100% です。

ステップ 13　Stop on Match の隣にある次のチェックボックスのいずれかをオンにします。

a.　**Yes**：この特定のフィルタのアクションが削除された後、イベント アクション フィルタ コンポーネントの処理を停止する場合。

残りのフィルタは処理されません。したがって、イベントからそれ以上のアクションは削除できません。

b.　**No**：追加のフィルタも継続して処理する場合。

ステップ 14　Enabled の隣にある **Yes** をオンにして、このフィルタをイネーブルにします。

（注） Event Action Filters パネルの **Use Event Action Filters** チェックボックスもオンにする必要があります。オンにしないと、Add Event Action Filter ダイアログボックスで **Yes** をオンにしたかどうかに関係なくイベント アクション フィルタはイネーブルになりません。

ステップ 15 Active の隣にある **Yes** をオンにして、イベントのフィルタリングにおいて有効になるようにこのフィルタをリストに追加します。

ステップ 16 **Comments** フィールドについてこのフィルタとともに保存するコメントを入力します。コメントには、このフィルタの目的や、このフィルタを特定の方法で設定した理由などを記述します。

ヒント 変更を元に戻して Add Event Action Filter ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 17 **OK** をクリックします。

Event Action Filters パネルのリストに新しいイベント アクション フィルタが表示されます。

ステップ 18 **Use Event Action Overrides** チェックボックスをオンにします。

（注） Event Action Overrides パネルの **Use Event Action Overrides** チェックボックスをオンにする必要があります。オンにしないと、Add Event Action Filter ダイアログボックスで設定した値に関係なくイベント アクション オーバーライドはイネーブルになりません。

ステップ 19 既存のイベント アクション フィルタを編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Action Filter ダイアログボックスが表示されます。

ステップ 20 必要に応じてフィールドの値を変更します。

フィールドの入力を完了する手順については、手順 3 ～ 14 を参照してください。

ヒント 変更を元に戻して Edit Event Action Filter ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 21 **OK** をクリックします。

Event Action Filters パネルのリストに編集したイベント アクション フィルタが表示されます。

ステップ 22 **Use Event Action Overrides** チェックボックスをオンにします。

（注） Event Action Overrides パネルの **Use Event Action Overrides** チェックボックスをオンにする必要があります。オンにしないと、Edit Event Action Filter ダイアログボックスで設定した値に関係なくイベント アクション オーバーライドはイネーブルになりません。

ステップ 23 イベント アクション フィルタを削除するには、リスト内でそれを選択して **Delete** をクリックします。

Event Action Filters パネルのリストからそのイベント アクション フィルタが消去されます。

ステップ 24 イベント アクション フィルタをイネーブルまたはディセーブルにするには、**Enable** または **Disable** をクリックします。

ステップ 25 イベント アクション フィルタをリスト内で上または下に移動するには、**Move Up** または **Move Down** をクリックします。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 26 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

一般的な設定値の設定

この項では、一般的な設定値の設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-30）
- サポートされるユーザのロール（P.7-30）
- フィールド定義（P.7-30）
- イベント アクション ルールの一般的な設定値の設定（P.7-31）

概要

Summarizer および Meta Event Generator を使用するかどうかなど、イベント アクション ルールに適用する一般的な設定値を設定できます。Summarizer はイベントを 1 つのアラートにグループ化するため、センサーが送出するアラート数を削減できます。Meta Event Generator はコンポーネント イベントを処理します。コンポーネント イベントによって、センサーは一連のイベントにまたがって発生する不審なアクティビティを監視することができます。

注意　トラブルシューティングを目的とする場合以外、Summarizer や Meta Event Generator はオフにしないでください。Summarizer をオフにすると、すべてのシグニチャが要約なしの Fire All に設定されます。Meta Event Generator をオフにすると、すべての Meta エンジン シグニチャがディセーブルになります。

攻撃者を拒否する期間、拒否された攻撃者の最大数、ブロックを続ける期間を設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション ルールの一般的な設定値を設定するには、管理者またはオペレータである必要があります。

フィールド定義

General Settings パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Use Summarizer**：Summarizer コンポーネントをイネーブルにします。

  デフォルトでは、Summarizer はイネーブルです。ディセーブルにすると、すべてのシグニチャが要約なしの **Fire All** に設定されます。個々のシグニチャを要約するように設定しても、Summarizer がイネーブルでない場合は、この設定は無視されます。

- **Use Meta Event Generator**：Meta Event Generator をイネーブルにします。

  デフォルトでは、Meta Event Generator はイネーブルです。Meta Event Generator をディセーブルにすると、すべての Meta エンジン シグニチャがディセーブルになります。

- **Deny Attacker Duration**：インラインで攻撃者を拒否する秒数。
  有効範囲は 1 ～ 518400 です。デフォルトは 3600 です。
- **Block Attack Duration**：ホストまたは接続をブロックする分数。
  有効範囲は 1 ～ 10000000 です。デフォルトは 30 です。
- **Maximum Denied Attackers**：あらゆる時点において、システム内で拒否された攻撃者の数を制限します。
  有効範囲は 1 ～ 10000000 です。デフォルトは 10000 です。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

イベント アクション ルールの一般的な設定値の設定

注意　Summarizer および Meta Event Generator はグローバル レベルで動作するため、それらをイネーブルにするとこれらの機能のすべてのセンサー処理に影響します。

イベント アクション ルールの一般的な設定値を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Event Action Rules > General Settings** をクリックします。

General Settings パネルが表示されます。

ステップ 3　**Use Summarizer** を選択して Summarizer 機能をイネーブルにします。

注意　Summarizer をディセーブルにするのは、トラブルシューティングを目的とする場合だけです。それ以外の場合は、要約対象として設定するすべてのシグニチャが実際に要約されるように、必ず Summarizer をイネーブルにします。

ステップ 4　**Use Meta Event Generator** を選択して、Meta Event Generator をイネーブルにします。

注意　Meta Event Generator をディセーブルにするのは、トラブルシューティングを目的とする場合だけです。それ以外の場合は、すべての Meta エンジン シグニチャが機能するように、必ず Meta Event Generator をイネーブルにします。

ステップ 5　**Deny Attacker Duration** フィールドにインラインで攻撃者を拒否する秒数を入力します。

ステップ 6　**Block Action Duration** フィールドに、ホストまたは接続をブロックする分数を入力します。

ステップ 7　**Maximum Denied Attackers** フィールドに、すべての時点におけるシステム内で拒否された攻撃者の最大数を入力します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 8　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

イベントの監視

この項では、イベントを監視する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.7-33）
- サポートされるユーザのロール（P.7-33）
- フィールド定義（P.7-33）
- イベント表示の設定（P.7-35）

概要

Events パネルで、イベント データをフィルタしたり表示したりできます。イベントの種類、時間、またはその両方に基づいて、イベントをフィルタリングできます。デフォルトでは、過去 1 時間のすべてのアラートとエラー イベントが表示されます。**View** をクリックすると、これらのイベントを表示できます。

View をクリックすると、IDM がイベントの時間範囲を定義します（未設定の場合）。範囲の終了時間を指定しなかった場合には、**View** をクリックした時点で終了するものとして定義されます。

センサーから多数のイベントを取得するときにシステム エラーが発生するのを防ぐために、IDM は 1 回に表示可能なイベント数を制限しています（ページあたりの最大行数は 500）。**Back** および **Next** をクリックすれば、さらに多くのイベントを表示できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベントの表示を設定するには、管理者である必要があります。

フィールド定義

この項では、イベントを設定および表示するためのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Events パネル（P.7-33）
- Event Viewer ページ（P.7-34）

Events パネル

Events パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Show alert events**：表示するアラートのレベルを設定します。
  - **Informational**
  - **Low**
  - **Medium**
  - **High**

    デフォルトではすべてのレベルがイネーブルです。

- **Show error events**：表示するエラーの種類を設定します。
  - **Warning**
  - **Error**
  - **Fatal**

  デフォルトではすべてのレベルがイネーブルです。
- **Show Network Access Controller events**：ARC（以前は Network Access Controller と呼ばれていました）イベントを表示します。

  デフォルトはディセーブルです。
- **Show status events**：ステータス イベントを表示します。

  デフォルトはディセーブルです。
- **Select the number of the rows per page**：ページごとに表示する行数を決定します。

  有効範囲は 1 ～ 500 です。デフォルトは 100 です。
- **Show all events currently stored on the sensor**：センサーに保存されたすべてのイベントを取得します。
- **Show past events**：指定した時間数または分数を遡って、過去のイベントを表示します。
- **Show events from the following time range**：指定した時間範囲のイベントを取得します。

ボタンの機能：

- **View**：Event Viewer を表示します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Event Viewer ページ

Event Viewer ページには次のフィールドとボタンがあります。

- **#**：結果クエリーでのイベントのオーダー番号を示します。
- **Type**：イベントの種類を Error、NAC、Status、または Alert として示します。
- **Sensor UTC Time**：イベントがいつ発生したかを示します。
- **Event ID**：センサーがイベントに割り当てた数値の識別子。
- **Events**：イベントを簡潔に説明します。
- **Sig ID**：生成されアラート イベントを引き起こしたシグニチャを示します。

ボタンの機能：

- **Details**：選択したイベントの詳細を個別のダイアログボックスで表示します。

  アプリケーション、攻撃者、ターゲット、およびシグニチャの詳細を表示します。
- **Refresh**：Event Viewer を新しいイベントでリフレッシュします。
- **Back**：Event Viewer で前のページを表示します。
- **Next**：Event Viewer で次のページを表示します。
- **Close**：開いているダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

イベント表示の設定

イベントの表示方法を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring** > **Events** をクリックします。

Events パネルが表示されます。

ステップ 3　Events の下で、表示するアラートのレベルを選択します。

ステップ 4　Events の下で、表示するエラーの種類を選択します。

ステップ 5　ARC（以前は Network Access Controller と呼ばれていました）イベントを表示する場合は、**Show Network Access Controller events** を選択します。

ステップ 6　ステータス イベントを表示する場合は、**Show status events** を選択します。

ステップ 7　表示するページあたりの行数を選択します。

デフォルトは 100 です。有効な値は、100、200、300、400、または 500 です。

ステップ 8　イベントを表示する時間を設定する場合は、次のいずれかを選択します。

- **Show all events currently stored on the sensor**
- **Show past events**
  過去のイベントを表示するために遡る時間数と分数を入力します。
- **Show events from the following time range**
  開始時間と終了時間を選択します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 9　**View** をクリックして、設定したイベントを表示します。

Event Viewer が表示されます。

ステップ 10　1 つの列で昇順または降順にソートするには、右側にある上向き矢印または下向き矢印をクリックします。

ステップ 11　**Next** または **Back** をクリックして、100 行ずつ表示されたページを移動します。

ステップ 12　イベントの詳細を表示するには、それを選択して **Details** をクリックします。

イベントの詳細は、別のダイアログボックスに表示されます。ダイアログボックスにはタイトルとしてイベント ID が示されます。

ブロッキングとレート制限のための ARC の設定

この章では、Attack Response Controller（ARC）がセンサー上でブロッキングとレート制限を実行するように設定する方法について説明します。

（注）ARC は、以前は Network Access Controller と呼ばれていました。IPS 5.1 から名前が変更されましたが、IDM には引き続き Network Access Controller という用語が含まれています。

この章は、次の項で構成されています。

- ブロッキングについて（P.8-2）
- レート制限について（P.8-4）
- ARC を設定する前に（P.8-5）
- サポートされているデバイス（P.8-6）
- ブロッキング プロパティの設定（P.8-8）
- アクティブなレート制限の管理（P.8-14）
- デバイス ログイン プロファイルの設定（P.8-18）
- ブロッキング デバイスおよびレート制限デバイスの設定（P.8-22）
- ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定（P.8-27）
- Catalyst 6000 のブロッキング デバイス インターフェイスの設定（P.8-33）
- マスター ブロッキング センサーの設定（P.8-37）
- アクティブなホスト ブロックの管理（P.8-42）
- ネットワーク ブロックの管理（P.8-46）

ブロッキングについて

センサー上のブロッキング アプリケーションである ARC は、ルータ、スイッチ、PIX.Firewall、FWSM、および ASA 上でブロックを開始したり停止したりします。ARC は、管理しているデバイス上で IP アドレスをブロックします。ARC は、他のマスター ブロッキング センサーも含めて、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監視し、その時間が満了するとブロックを削除します。

注意　FWSM がマルチモードで設定されている場合、管理コンテキストではブロッキングはサポートされません。ブロッキングは、シングルモードおよびマルチモードのカスタマー コンテキストでのみサポートされます。

（注）　ARC は、4 ～ 7 秒未満で新しいブロックの応答アクションを完了するように設計されています。ほとんどの場合、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上の目標を実現するため、センサーでは、過度なレートでのブロックの実行やデバイスとインターフェイスに対する過剰なブロックの管理を設定しないでください。ブロックの最大数は 250 未満、ブロックする項目の最大数は 10 未満にすることをお勧めします。ブロックする項目の最大数を計算する場合は、ファイアウォール、ASA、または FWSM を、ブロックするコンテキストごとに 1 つのブロックする項目として数えます。ルータは、ブロックするインターフェイス / 方向ごとに 1 つのブロックする項目として数えます。Catalyst ソフトウェアを実行するスイッチは、ブロックする VLAN ごとに 1 つのブロックする項目として数えます。推奨される制限を越えると、ARC がブロックをちょうどよいタイミングで適用しなかったり、ブロックをまったく適用しなかったりする可能性があります。

マルチモードで設定された ASA、PIX Firewall 7.0、FWSM 2.1 以降などのファイアウォールの場合、IPS 5.1 はブロック要求に VLAN 情報を挿入しません。このため、ブロックされている IP アドレスが正しいかどうかをファイアウォールごとに確認する必要があります。たとえば、センサーが VLAN A 用に設定されたファイアウォールのカスタマー コンテキストでパケットを監視し、VLAN B 用に設定された別のファイアウォールのカスタマー コンテキストでブロッキングを実行しているとします。この場合、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 つのタイプがあります。

- ホスト ブロック：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。
- 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のブロック。

  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を指定すると、そのブロックは接続ブロックからホスト ブロックに自動的に切り替えられます。

  （注）　ファイアウォールでは、接続ブロックはサポートされません。ファイアウォールでは、接続情報を追加したホスト ブロックのみがサポートされます。

- ネットワーク ブロック：特定ネットワークからのすべてのトラフィックのブロック。

  ホスト ブロックと接続ブロックは、シグニチャがトリガーされたときに手動または自動で開始できます。ネットワーク ブロックは、手動でのみ開始することができます。

注意　ブロッキングと、センサーがパケットをドロップする機能を混同しないでください。センサーは、そのセンサーに対して、Deny Packet Inline、Deny Connection Inline、および Deny Attacker Inline アクションがインライン モードで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、特定のシグニチャのイベント アクションとして **Request Block Host** または **Request Block Connection** を選択し、それらを設定したイベント アクション オーバーライドに追加する必要があります。それによって、SensorApp はシグニチャがトリガーされたときにブロック要求を ARC に送信できます。ARC は、SensorApp からブロック要求を受信すると、ホストまたは接続をブロックするようにデバイスのコンフィギュレーションを更新します。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、P.5-24 の「シグニチャへのアクションの割り当て」を参照してください。また、Request Block Host または Request Block Connection イベント アクションを特定のリスク評価のアラームに追加するオーバーライドを設定する手順については、P.7-17 の「イベント アクション オーバーライドの設定」を参照してください。

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 を適用することでブロックを作成します。ACL と VACL は、インターフェイスの方向または VLAN 上のデータパケットの追加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または拒否の条件が記述されています。PIX Firewall、FWSM、および ASA では、ACL または VACL は使用されません。組み込みの **shun** コマンドおよび **no shun** コマンドを使用します。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新規 ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。詳細については、P.8-27 の「Sensor がデバイスを管理する方法」を参照してください。

デバイスを管理するには、ARC に関する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（ユーザがイネーブル特権を持っている場合は不要）
- 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 で、最初に適用する任意の既存 ACL または VACL 情報（Pre-Block ACL または VACL）、または最後に適用する ACL または VACL 情報（Post-Block ACL または VACL）

  これは、PIX Firewall、FWSM、または ASA には当てはまりません。それらはブロックするために ACL を使用しないためです。
- デバイスとの通信で Telnet または SSH を使用するかどうか
- ブロックしない IP アドレス（ホストまたはホストの範囲）
- ブロックを続ける期間

ヒント　ARC のステータスを確認するには、`sensor#` で **show statistics network-access** と入力します。この操作を行うと、管理しているデバイス、アクティブなブロック（存在する場合）、およびすべてのデバイスのステータスが表示されます。または、IDM で、**Monitoring > Statistics** をクリックして ARC のステータスを確認します。

（注）ARC は、以前は Network Access Controller（NAC）と呼ばれていました。名前は変更されましたが、IDM と CLI では引き続き Network Access Controller、**nac**、および **network-access** として示されています。

レート制限について

レート制限を使用すると、センサーがネットワーク 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します。レート制限の応答は、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 は、Cisco IOS バージョン 12.3 以降を実行するネットワーク デバイスでレート制限を設定することができます。ルータでのレート制限の設定については、P.8-22 の「ブロッキング デバイスおよびレート制限デバイスの設定」を参照してください。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。詳細については、マスター ブロッキング センサーの設定 を参照してください。

アクティブなレート制限のリストは、ARC の統計情報で確認できます。詳細については、P.10-14 の「統計情報の表示」を参照してください。

レート制限を追加するには、プロトコル、宛先 IP アドレス、およびレート制限イベントの生成が可能なシグニチャのいずれかに一致するデータ値の組み合せを指定します。手順については、P.8-14 の「アクティブなレート制限の管理」を参照してください。また、アクションを Request Rate Limit に設定し、さらにこれらのシグニチャの率を設定する必要があります。表 8-1 に、サポートされているシグニチャとパラメータを示します。

表 8-1　レート制限のシグニチャ

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	○	echo-request
2153	ICMP Smurf Attack	ICMP	○	echo-reply
4002	UDP Flood Host	UDP	○	なし
6901	Net Flood ICMP Reply	ICMP	×	echo-reply
6902	Net Flood ICMP Request	ICMP	×	echo-request
6903	Net Flood ICMP Any	ICMP	×	なし
6910	Net Flood UDP	UDP	×	なし
6920	Net Flood TCP	TCP	×	なし
3050	TCP HalfOpenSyn	TCP	×	halfOpenSyn

ARC を設定する前に

ブロッキングまたはレート制限を実行するために ARC を設定する前に、次のことを実行してください。

- ネットワーク トポロジを分析して、どのデバイスをどのセンサーでブロックするかや、ブロックしないアドレスを確認します。

注意　2 つのセンサーが同一のデバイスでブロッキングやレート制限を制御することはできません。このようにする必要がある場合は、1 つのセンサーをデバイス管理のためのマスター ブロッキング センサーとして設定します。このように設定すると、他のセンサーはマスター ブロッキング センサーに要求を転送することができます。手順については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

（注）　マスター ブロッキング センサーを追加する場合は、センサーごとにブロックするデバイスの数を減らしてください。たとえば、10 のファイアウォールと 10 のルータでブロッキングを行い、ブロックするインターフェイス / 方向がそれぞれ 1 つずつある場合は、そのうちの 10 をセンサーに割り当て、残りの 10 をマスター ブロッキング センサーに割り当てます。

- 各デバイスにログインするために必要なユーザ名、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）の情報を入手します。
- デバイスのインターフェイス名を確認します。
- 必要に応じて、Pre-Block ACL または VACL、および Post-Block ACL または VACL の名前を確認します。
- ブロックするインターフェイスとブロックしないインターフェイス、およびその方向（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遮断しないでください。

サポートされているデバイス

デフォルトでは、ARC は任意の組み合せで最大 250 のデバイスをサポートします。ARC によるブロッキングがサポートされるデバイスは、次のとおりです。

（注） ARC は、4 ～ 7 秒未満で新しいブロックの応答アクションを完了するように設計されています。ほとんどの場合、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上の目標を実現するため、センサーでは、過度なレートでのブロックの実行やデバイスとインターフェイスに対する過剰なブロックの管理を設定しないでください。ブロックの最大数は 250 未満、ブロックする項目の最大数は 10 未満にすることをお勧めします。ブロックする項目の最大数を計算する場合は、ファイアウォール、ASA、または FWSM を、ブロックするコンテキストごとに 1 つのブロックする項目として数えます。ルータは、ブロックするインターフェイス / 方向ごとに 1 つのブロックする項目として数えます。Catalyst ソフトウェアを実行するスイッチは、ブロックする VLAN ごとに 1 つのブロックする項目として数えます。

注意 推奨される制限を越えると、ARC がブロックをちょうどよいタイミングで適用しなかったり、ブロックをまったく適用しなかったりする可能性があります。

- Cisco IOS 11.2 以降を使用する Cisco シリーズ ルータ（ACL）
  - 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
- IOS 11.2(9)P 以降を使用する RSM 搭載 Catalyst 5000 スイッチ（ACL）
- IOS 12.1(13)E 以降を使用する Catalyst 6500 スイッチおよび 7600 ルータ（ACL）
- Catalyst ソフトウェア バージョン 7.5(1) 以降を使用する Catalyst 6500 スイッチおよび 7600 ルータ（VACL）
  - PFC 組み込みのスーパーバイザ エンジン 1A
  - MSFC1 組み込みのスーパーバイザ エンジン 1A
  - MFSC2 組み込みのスーパーバイザ エンジン 1A
  - MSFC2 組み込みのスーパーバイザ エンジン 2
  - MSFC3 組み込みのスーパーバイザ エンジン 720

（注） スーパーバイザ エンジンでの 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）

ACL、VACLS、または **shun** コマンドのいずれかを使用してブロッキングを設定します。すべてのファイアウォールと ASA モデルが **shun** コマンドをサポートしています。

ARC によるレート制限がサポートされるデバイスは、次のとおりです。

- 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

ブロッキング プロパティの設定

この項では、ブロッキング プロパティを設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-8）
- サポートされているユーザ ロール（P.8-9）
- フィールド定義（P.8-9）
- ブロッキング プロパティの設定（P.8-11）

概要

Blocking Properties パネルを使用して、ブロッキングとレート制限をイネーブルにするために必要な基本的な設定を行えます。

ARC が、管理対象デバイスでのブロッキングとレート制限を制御します。

手動で実行を試みてもブロックされるべきではないホストおよびネットワークを識別できるように、センサーをチューニングする必要があります。信頼されたネットワーク デバイスの通常の動作が、攻撃として扱われる可能性があるためです。このようなデバイスや信頼された内部ネットワークもブロックする必要はありません。シグニチャを適切にチューニングすることにより、false positive の数を減らし、ネットワークが正しく動作することを保証できます。シグニチャのチューニングとフィルタリングを行うと、アラームの生成が防止できます。アラームが生成されない場合、それに関連付けられたブロックも実行されません。

（注） **Never Block Address** オプションはレート制限には適用されません。

ネットマスクを指定すると、それが決してブロックされるべきではないネットワークのネットマスクになります。ネットマスクを指定しない場合、指定した IP アドレスだけがブロック対象外になります。

注意 センサーが自らをブロックすることは許可しないことをお勧めします。これを許可すると、センサーがブロッキング デバイスと通信しなくなる可能性があります。このオプションは、センサーが自分の IP アドレスをブロックする規則を作成した場合に、そのためにセンサーがブロックしているデバイスにアクセスできなくなることはないと保証されている場合にだけ設定します。

デフォルトでは、ブロッキングはセンサー上でイネーブルです。ARC が管理しているデバイスに手動で設定をしなければならない場合は、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。管理者と ARC が同じデバイスに同時に変更を加えないようにしてください。同時に変更を加えると、デバイスまたは ARC の失敗を引き起こします。

（注） デフォルトでは、Cisco IOS デバイス上ではブロッキングのみがサポートされています。レート制限、またはブロッキングとレート制限を選択することで、ブロッキングのデフォルト値を上書きできます。

サポートされているユーザ ロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ブロッキング プロパティを追加または編集するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、ブロッキング プロパティのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Blocking Properties パネル（P.8-9）
- Add and Edit Never Block Address ダイアログボックス（P.8-11）

Blocking Properties パネル

Blocking Properties パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Enable blocking**：ホストのブロッキングをイネーブルにするかどうかを指定します。

  デフォルトはイネーブルです。Enable blocking がディセーブルで、その他のフィールドにデフォルト以外の値が指定されていると、エラー メッセージが表示されます。

  （注） ブロッキングをイネーブルにした場合は、レート制限もイネーブルにします。ブロッキングをディセーブルにした場合は、レート制限もディセーブルにします。つまり、ARC は新たにブロックまたはレート制限を追加したり、既存のブロックまたはレート制限を削除したりすることはできません。

  （注） ブロッキングをイネーブルにしない場合でも、その他のブロッキング設定値はすべて設定できます。

- **Allow the sensor IP address to be blocked**：センサー IP アドレスをブロック可能にするかどうかを指定します。

  デフォルトはディセーブルです。

- **Log all block events and errors**：センサーが、開始から終了までのブロックに伴うイベントと発生したすべてのエラー メッセージをログに記録するように設定します。

  デバイスに対してブロックが追加または削除されたときには、イベントがログに記録されます。このようなすべてのイベントやエラーをログに記録する必要のない場合もあります。このオプション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。

  （注） Log all block events and errors はレート制限にも適用されます。

- **Enable NVRAM write**：ARC が最初に接続したときに NVRAM に書き込むように、センサーがルータに指示します。

  イネーブルの場合は、ACL が更新されるたびに NVRAM に書き込まれます。デフォルトはディセーブルです。

  NVRAM への書き込みをイネーブルにすると、ブロッキングとレート制限の変更がすべて NVRAM に書き込まれます。ルータをリブートしても、正しいブロックとレート制限はアクティブなままです。NVRAM への書き込みがディセーブルの場合、ルータはリブート後にブロッキングまたはレート制限を実行しないため短時間でアップします。NVRAM への書き込みをイネーブルにしないと、NVRAM の寿命が延び、新しいブロックおよびレート制限を設定する時間は短縮されます。

- **Enable ACL Logging**：ARC が ACL または VACL のブロック エントリにログ パラメータを付加します。

  パケットがフィルタリングされると、デバイスは syslog イベントを生成します。このオプションは、ルータおよびスイッチだけに適用されます。デフォルトはディセーブルです。

- **Maximum Block Entries**：ブロックするエントリの最大数。

  値は 1 ～ 65535 です。デフォルトは 250 です。

- **Maximum Interfaces**：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 と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 とカウントされます。インターフェイスの最大数はデバイスあたり 250 です。デフォルトは 250 です。

（注） Maximum Interfaces は、ARC が管理可能なデバイスおよびインターフェイスの数の上限に設定します。ブロッキング デバイスの合計数（マスター ブロッキング センサーを除く）はこの値以下でなければなりません。ブロックする項目の合計数もこの値を超えることはできません。ファイアウォール コンテキスト、ルータがブロックするインターフェイス / 方向、またはスイッチがブロックする VLAN は、それぞれ 1 つのブロックする項目と見なされます。

（注） さらに、最大限度は固定されており、それらを変更することはできません。最大限度は、デバイスあたり 100 インターフェイス、250 のファイアウォール、250 のルータ、250 の Catalyst Software スイッチ、および 100 のマスター ブロッキング センサーです。

- **Maximum Rate Limit Entries**：レート制限エントリの最大数。

  最大レート制限の数は、最大ブロック数以下である必要があります。レート制限数をブロック数より多く設定すると、エラーが発生します。値は 1 ～ 32767 です。デフォルトは 250 です。

- **Never Block Addresses**：センサーによるブロッキングを回避する IP アドレスを設定します。
  - **IP Address**：ブロックしない IP アドレス。
  - **Mask**：ブロックしない IP アドレスに対応するマスク。

ボタンの機能：

- **Add**：Add Never Block Address ダイアログボックスを表示します。

  このダイアログボックスで、ブロックしないホストおよびネットワークのリストにホストまたはネットワークを追加できます。

- **Edit**：Edit Never Block ダイアログボックスを表示します。

  このダイアログボックスで、ブロックしないホストまたはネットワークを変更できます。

- **Delete**：ブロックしないホストおよびネットワークのリストからホストまたはネットワークを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Never Block Address ダイアログボックス

Add and Edit Never Block Address ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロックしない IP アドレス。
- **Mask**：ブロックしない IP アドレスに対応するマスク。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ブロッキング プロパティの設定

ブロッキング プロパティを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Blocking > Blocking Properties** をクリックします。

Blocking Properties パネルが表示されます。

ステップ 3　**Enable blocking** チェックボックスをオンにして、ブロッキングとレート制限をイネーブルにします。

（注）　ブロッキングまたはレート制限を動作させるには、ブロッキングまたはレート制限を実行するようにデバイスをセットアップする必要があります。手順については、P.8-27 の「ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定」、および P.8-33 の「Catalyst 6000 のブロッキング デバイス インターフェイスの設定」を参照してください。

ステップ 4　必要な場合以外は、**Allow the sensor IP address to be blocked** チェックボックスはオンにしないでください。

注意　センサーが自らをブロックすることは許可しないことをお勧めします。これを許可すると、センサーがブロッキング デバイスと通信しなくなる可能性があります。このオプションは、センサーが自分の IP アドレスをブロックする規則を作成した場合に、そのためにセンサーがブロックしている装置にアクセスできなくなることはないと保証されている場合にだけ選択します。

ステップ 5　ブロッキングのイベントとエラーをログに記録する場合は、**Log all block events and errors** チェックボックスをオンにします。

ステップ 6　ARC が最初に接続したときに NVRAM に書き込みように、センサーによってルータに指示する場合は、**Enable NVRAM write** チェックボックスをオンにします。

ステップ 7　ARC によって ACL または VACL のブロック エントリにログ パラメータを付加させる場合は、**Enable ACL logging** チェックボックスをオンにします。

ステップ 8　**Maximum Block Entries** フィールドに、同時に実行できるブロックの数を入力します（0 ～ 65535）。

（注）　最大ブロック数は 250 を超えて設定しないことをお勧めします。

（注）　ブロックの数は、最大ブロック数を超えることはできません。最大数になると、既存のブロックがタイムアウトしてなくなるまで、新しいブロックはできません。

ステップ 9　**Maximum Interfaces** フィールドにブロックを実行するインターフェイス数を入力します。

ステップ 10　**Maximum Rate Limit Entries** フィールドにレート制限のエントリ数（1 ～ 32767）を入力します。

注意　最大レート制限の数は、最大ブロック数以下である必要があります。レート制限数をブロック数より多く設定すると、エラーが発生します。

ステップ 11　**Add** をクリックして、ブロックしないアドレスのリストにホストまたはネットワークを追加します。

Add Never Block Address ダイアログボックスが表示されます。

ステップ 12　**IP Address** フィールドにホストまたはネットワークの IP アドレスを入力します。

ステップ 13　**Network Mask** フィールドで、ホストまたはネットワークのネットワーク マスクを入力するか、またはリストからネットワーク マスクを選択します。

ヒント　変更を元に戻して Add Never Block Address ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 14　**OK** をクリックします。

エントリが重複する場合は、エラー メッセージが表示されます。

新しいホストまたはネットワークが、Blocking Properties パネルの Never Block Addresses リストに現れます。

ステップ 15 ブロックしないアドレスのリストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Never Block Address ダイアログボックスが表示されます。

ステップ 16 **IP Address** フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 17 **Network Mask** フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ヒント 変更を元に戻して Edit Never Block Address ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 18 **OK** をクリックします。

編集したホストまたはネットワークが、Allowed Hosts パネルの Never Block Addresses リストに現れます。

ステップ 19 リストからホストまたはネットワークを削除するには、ホストまたはネットワークを選択して **Delete** をクリックします。

そのホストは Blocking Properties パネルの Never Block Addresses リストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 20 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

アクティブなレート制限の管理

この項では、アクティブなレート制限を管理する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-14）
- サポートされるユーザのロール（P.8-14）
- フィールド定義（P.8-14）
- レート制限の設定および管理（P.8-16）

概要

Rate Limits パネルで、レート制限を設定および管理することができます。

レート制限は、ネットワーク デバイスのインターフェイス上で、指定されたタイプのトラフィックの量を帯域幅の最大容量の一定の率までに制限します。この率を超えるトラフィックは、ネットワーク デバイスによってドロップされます。レート制限では、指定されたターゲット ホストへのトラフィック、または設定されたインターフェイスや方向を通過するすべてのトラフィックを制限することができます。レート制限は、恒常的に、または指定した期間だけ使用することができます。レート制限は、プロトコル、オプションの宛先アドレス、およびオプションのデータ値によって指定されます。

注意　パネルには送信元アドレス、送信元ポート、および宛先ポートが表示されますが、このバージョンではそれらのフィールドをサポートしていません。

レート制限は率（パーセント）で指定されるため、異なる帯域幅容量を持つインターフェイスでは別の実際の制限値に変換される場合があります。レート制限のパーセント値は、1 ～ 100 までの整数で指定します。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

レート制限を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、レート制限のフィールドの定義を示します。取り上げる事項は次のとおりです。

- Rate Limits パネル（P.8-15）
- Add Rate Limit ダイアログボックス（P.8-15）

Rate Limits パネル

Rate Limits パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レートを制限するトラフィックのプロトコル。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
  この率を超えて一致したトラフィックはドロップされます。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Data**：（オプション）特定のプロトコルのトラフィックをさらに正確に限定するために必要な追加の識別情報。
  たとえば、echo-request の場合、ICMP プロトコルのトラフィックはレート制限の ping に絞られます。
- **Minutes Remaining**：該当のレート制限が有効である残り時間（分単位）。
- **Timeout (minutes)**：該当のレート制限の合計時間（分単位）。

ボタンの機能：

- **Add**：Add Rate Limit ダイアログボックスを表示します。
  このダイアログボックスから、レート制限のオプションを設定できます。
- **Delete**：テーブルから該当エントリを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Rate Limit ダイアログボックス

Add Rate Limit ダイアログボックスには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レート制限されたトラフィックのプロトコル（ICMP、TCP、または UDP）。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：（オプション）レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Use Additional Data**：（オプション）echo-reply、echo-request、halfOpenSyn などの追加データを指定するかどうかを選択できます。
- **Timeout**：タイムアウトをイネーブルにするかどうかを選択できます。
  - **No Timeout**：タイムアウトをイネーブルにしません。
  - **Enable Timeout**：タイムアウト（分単位）を指定できます（1 ～ 70560）。

ボタンの機能：

- **Apply**：変更を適用してダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

レート制限の設定および管理

レート制限の詳細については、P.8-4 の「レート制限について」を参照してください。

レート制限を設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring** > **Rate Limits** をクリックします。

Rate Limits パネルが表示されます。

ステップ 3　**Add** をクリックして、レート制限を追加します。

Add Rate Limit ダイアログボックスが表示されます。

ステップ 4　レートを制限するトラフィックのプロトコル（ICMP、TCP、または UDP）を **Protocol** リストから選択します。

ステップ 5　**Rate** フィールドにレート制限（1 ～ 100）を入力します。

ステップ 6　（オプション）**Destination IP** フィールドに宛先 IP アドレスを入力します。

ステップ 7　レート制限で追加データを使用するように設定する場合は、**Use Additional Data** チェックボックスを選択します。

ステップ 8　**Select Data** リストから、追加データ（echo-reply、echo-request、または halfOpenSyn）を選択します。

ステップ 9　タイムアウト（分単位）を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 10　**Timeout** フィールドに、時間を分単位で入力します（1 ～ 70560）。

ヒント　変更を元に戻して Add Rate Limit ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 11　レート制限に一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

ステップ 12　**Apply** をクリックします。

Rate Limits パネルのリストに新しいレート制限が表示されます。

ステップ 13　**Refresh** をクリックして、Rate Limits リストの内容をリフレッシュします。

ステップ 14　レート制限を削除するには、リストからレート制限を選択して、**Delete** をクリックします。

Delete Rate Limit ダイアログボックスで、該当のレート制限を本当に削除するかどうかをたずねられます。

ヒント **No** をクリックすると、Delete Rate Limit ダイアログボックスが閉じます。

ステップ 15 **Yes** をクリックしてレート制限を削除します。

該当のレート制限はレート制限のリストに表示されなくなります。

デバイス ログイン プロファイルの設定

この項では、デバイス ログイン プロファイルを設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-18）
- サポートされるユーザのロール（P.8-18）
- フィールド定義（P.8-18）
- デバイス ログイン プロファイルの設定（P.8-20）

概要

Device Login Profiles パネルで、センサーがブロッキング デバイスへのログイン時に使用するプロファイルを設定できます。

センサーが管理するその他のハードウェアについてもデバイス ログイン プロファイルをセットアップする必要があります。デバイス ログイン プロファイルには、作成した名前の下に、ユーザ名、ログイン パスワード、およびイネーブル パスワードに関する情報が含まれます。たとえば、同じパスワードとユーザ名を使用するルータはすべて 1 つのデバイス ログイン プロファイル名の下にまとめることができます。

（注） ブロッキング デバイスを設定する前に、デバイス ログイン プロファイルを作成しておく必要があります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

デバイス ログイン プロファイルを追加または編集するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、デバイス ログイン プロファイルのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Device Login Profiles パネル（P.8-18）
- Add and Edit Device Login Profile ダイアログボックス（P.8-19）

Device Login Profiles パネル

Device Login Profile パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Profile Name**：プロファイルの名前。
- **Username**：ブロッキング デバイスへのログインに使用されるユーザ名（オプション）。

- **Login Password**：ブロッキング デバイスへのログインに使用されるパスワード（オプション）。Add Device Login Profile ダイアログボックスのみの項目です。

（注）パスワードが存在する場合、パスワードは固定数のアスタリスクで表示されます。

- **Enable Password**：ブロッキング デバイスで使用されるイネーブル パスワード（オプション）。Add Device Login Profile ダイアログボックスのみの項目です。

（注）パスワードが存在する場合、パスワードは固定数のアスタリスクで表示されます。

ボタンの機能：

- **Add**：Add Device Login Profile ダイアログボックスを表示します。
  このダイアログボックスで、デバイス ログイン プロファイルを追加できます。
- **Edit**：Edit Device Login Profile ダイアログボックスを表示します。
  このダイアログボックスで、このデバイス ログイン プロファイルに関連付けられた値を変更できます。
- **Delete**：デバイス ログイン プロファイルのリストから該当のデバイス ログイン プロファイルを削除します。
  使用中のプロファイル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。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Device Login Profile ダイアログボックス

Add and Edit Device Login Profile ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Profile Name**：プロファイルの名前。
- **Username**：ブロッキング デバイスへのログインに使用されるユーザ名（オプション）。
- **Login Password**：ブロッキング デバイスへのログインに使用されるパスワード（オプション）。Add Device Login Profile ダイアログボックスのみの項目です。

（注）パスワードが存在する場合、パスワードは固定数のアスタリスクで表示されます。

- **Enable Password**：ブロッキング デバイスで使用されるイネーブル パスワード（オプション）。Add Device Login Profile ダイアログボックスのみの項目です。

（注）パスワードが存在する場合、パスワードは固定数のアスタリスクで表示されます。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

デバイス ログイン プロファイルの設定

デバイス ログイン プロファイルを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Blocking > Device Login Profiles** をクリックします。

Device Login Profiles パネルが表示されます。

ステップ 3　**Add** をクリックして、プロファイルを追加します。

Add Device Login Profile ダイアログボックスが表示されます。

ステップ 4　**Profile Name** フィールドにプロファイル名を入力します。

ステップ 5　**Username** フィールドにブロッキング デバイスにログインするために使用するユーザ名を入力します。

ステップ 6　**New Password** フィールドにログイン パスワードを入力し、**Confirm New Password** フィールドにも再度入力します。

ステップ 7　**New Password** フィールドにイネーブル パスワードを入力し、**Confirm New Password** フィールドにも再度入力します。

ヒント　変更を元に戻して Add Device Login Profile ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 8　**OK** をクリックします。

プロファイル名がすでに存在する場合は、エラー メッセージが表示されます。

Device Login Profile パネルのリストに新しいデバイス ログイン プロファイルが表示されます。

ステップ 9　デバイス ログイン プロファイル リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Device Login Profile ダイアログボックスが表示されます。

ステップ 10　**Username** フィールドでブロッキング デバイスにログインするために使用するユーザ名を編集します。

ステップ 11　ログイン パスワードを変更するには、**Change the login password** を選択します。

ステップ 12 **New Password** フィールドに新しいログイン パスワードを入力し、**Confirm New Password** フィールドにも再度入力します。

ステップ 13 イネーブル パスワードを変更するには、**Change the enable password** を選択します。

ステップ 14 **New Password** フィールドに新しいイネーブル パスワードを入力し、**Confirm New Password** フィールドにも再度入力します。

ヒント 変更を元に戻して Edit Device Login Profile ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 15 **OK** をクリックします。

Device Login Profile パネルのリストに編集したデバイス ログイン プロファイルが表示されます。

ステップ 16 リストからデバイス ログイン プロファイルを削除するには、それを選択して **Delete** をクリックします。

そのデバイス ログイン プロファイルは、Device Login Profile パネルのリストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 17 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

ブロッキング デバイスおよびレート制限デバイスの設定

この項では、ブロッキング デバイスおよびレート制限デバイスを設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-22）
- サポートされるユーザのロール（P.8-22）
- フィールド定義（P.8-22）
- ブロッキング デバイスおよびレート制限デバイスの設定（P.8-24）

概要

Blocking Devices パネルで、ブロッキングおよびレート制限を実装するために、センサーが使用するデバイスを設定できます。

Cisco IOS ルータまたは Catalyst 6500 ファミリのスイッチに配置する ACL 規則を生成したり、PIX Firewall または ASA で排除規則を生成することにより、攻撃をブロックするようにセンサーを設定できます。このルータ、スイッチ、ファイアウォールは、ブロッキング デバイスと呼ばれます。

レート制限では ACL が使用されますが、使用方法はブロックの場合とは異なります。レート制限は、ACL と class-map エントリを使用して、トラフィック、およびトラフィックをポリシングするための policy-map エントリと service-policy エントリを識別します。

注意　1 つのセンサーで複数のデバイスを管理することはできますが、複数のセンサーで 1 つのデバイスだけを管理することはできません。その場合には、マスター ブロッキング センサーを使用する必要があります。マスター ブロッキング センサーのセットアップ手順については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

あらかじめセンサーが管理するデバイスごとにデバイス ログイン プロファイルを指定しておかないと、Blocking Devices パネルでデバイスを設定することはできません。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ブロッキング デバイスを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、ブロッキング デバイスのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Blocking Devices パネル
- Add and Edit Blocking Devices ダイアログボックス

Blocking Devices パネル

Blocking Devices パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロッキング デバイスの IP アドレス。
- **Sensor's NAT Address**：（オプション）センサーの NAT アドレス。
- **Device Login Profile**：ブロッキング デバイスへのログインに使用されるデバイスのログイン プロファイル。
- **Device Type**：デバイスのタイプ（Cisco Router、Cat 6K、PIX/ASA）。

  デフォルトは Cisco Router です。
- **Response Capabilities**：デバイスで、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- **Communication**：ブロッキング デバイスへのログインに使用される通信メカニズムを示します（SSH 3DES、SSH DES、Telnet）。

  デフォルトは、SSH 3DES です。

ボタンの機能：

- **Add**：Add Blocking Device ダイアログボックスを表示します。

  このダイアログボックスで、ブロッキング デバイスを追加できます。

  IP アドレスがすでに存在する場合は、エラー メッセージが表示されます。
- **Edit**：Edit Blocking Device ダイアログボックスを表示します。

  このダイアログボックスで、このブロッキング デバイスに関連付けられた値を変更できます。
- **Delete**：ブロッキング デバイスのリストから該当のブロッキング デバイスを削除します。

  使用中のブロッキング デバイス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。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add/Edit Blocking Devices ダイアログボックス

Add and Edit Blocking Device ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロッキング デバイスの IP アドレス。
- **Sensor's NAT Address**：（オプション）センサーの NAT アドレス。
- **Device Login Profile**：ブロッキング デバイスへのログインに使用されるデバイスのログイン プロファイル。
- **Device Type**：デバイスのタイプ（Cisco Router、Cat 6K、PIX/ASA）。

  デフォルトは Cisco Router です。
- **Response Capabilities**：デバイスで、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- **Communication**：ブロッキング デバイスへのログインに使用される通信メカニズムを示します（SSH 3DES、SSH DES、Telnet）。

  デフォルトは、SSH 3DES です。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ブロッキング デバイスおよびレート制限デバイスの設定

ブロッキング デバイスおよびレート制限デバイスを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration** > **Blocking** > **Blocking Devices** をクリックします。

Blocking Devices パネルが表示されます。

ステップ 3　**Add** をクリックし、ブロッキング デバイスを追加します。

デバイス ログイン プロファイルが設定されていない場合は、エラー メッセージが表示されます。手順については、P.8-18 の「デバイス ログイン プロファイルの設定」を参照してください。

Add Blocking Device ダイアログボックスが表示されます。

ステップ 4　**IP Address** フィールドにブロッキング デバイスの IP アドレスを入力します。

ステップ 5　（オプション）**Sensor's NAT Address** フィールドにセンサーの NAT アドレスを入力します。

ステップ 6　**Device Login Profile** ドロップダウン リストからデバイス ログイン プロファイルを選択します。

ステップ 7　**Device Type** ドロップダウン リストからデバイスのタイプを選択します。

ステップ 8　Response Capabilities の隣にある **Block** または **Rate Limit**、もしくは両方をオンにして、デバイスがブロッキング、レート制限、または両方のそれを実行するかを選択します。

（注）　シグニチャがトリガーされたときに SensorApp が ARC にブロック要求またはレート制限要求を送信できるように、特定のシグニチャのブロッキングおよびレート制限のアクションを選択する必要があります。詳細については、P.5-24 の「シグニチャへのアクションの割り当て」を参照してください。

ステップ 9　**Communication** ドロップダウン リストから通信タイプを選択します。

SSH 3DES または SSH DES を選択した場合は、手順 11 に進みます。

ヒント　変更を元に戻して Add Blocking Device ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 10　**OK** をクリックします。

IP アドレスがすでに追加されている場合は、エラー メッセージが発生します。

Blocking Devices パネルのリストに新しいデバイスが表示されます。

ステップ 11　SSH 3DES または SSH DES を選択した場合、デバイスを既知のホストのリストに追加する必要があります。

(注) SSH 3DES または SSH DES を選択する場合、ブロッキング デバイスに目的の 3DES/DES の暗号化をサポートする機能セットまたはライセンスがある必要があります。

(注) また、**Configuration** > **SSH** > **Known Host Keys** > **Add Known Host Key** をクリックして、Add Known Host Key ダイアログボックスで既知のホストのリストにデバイスを追加することもできます。手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

a. センサーに Telnet 接続し、CLI にログインします。

b. グローバル コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

c. 公開鍵を入手します。

```
sensor(config)# ssh host-key blocking_device_ip_address
```

d. 公開鍵を既知のホストのリストに追加することを確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

e. **yes** と入力します。

f. グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

ステップ 12 ブロッキング デバイスのリストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Blocking Device ダイアログボックスが表示されます。

ステップ 13 必要に応じてセンサーの NAT アドレスを編集します。

ステップ 14 必要に応じてデバイス ログイン プロファイルを変更します。

ステップ 15 必要に応じてデバイスのタイプを変更します。

ステップ 16 必要に応じて、デバイスがブロッキングまたはレート制限のどちらを実行するかを変更します。

ステップ 17 必要に応じて通信タイプを変更します。

ヒント 変更を元に戻して Edit Blocking Device ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 18 **OK** をクリックします。

Blocking Devices パネルのリストに編集したブロッキング デバイスが表示されます。

ステップ 19 ブロッキング デバイスをリストから削除するには、それを選択して **Delete** をクリックします。

そのブロッキング デバイスは、Blocking Device パネルのリストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 20 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定

この項では、ルータのブロッキングまたはレート制限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。取り上げる事項は次のとおりです。

- Sensor がデバイスを管理する方法（P.8-27）
- 概要（P.8-28）
- サポートされるユーザのロール（P.8-29）
- フィールド定義（P.8-29）
- ルータのブロッキングおよびレート制限のデバイス インターフェイスの設定（P.8-31）

Sensor がデバイスを管理する方法

ARC は Cisco ルータおよびスイッチ上の ACL を使用して、それらのデバイスを管理します。これらの ACL は、次のもので構成されています。

（注）ACL はレート制限のあるデバイスには適用されません。

1. センサーの IP アドレス、または指定されている場合はセンサーの NAT アドレスが示された **permit** 行

   （注）センサーのブロックを許可する場合は、この行は ACL に表示されません。

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 はこの ACL の行を読み取り、その行を ACL の先頭にコピーします。

3. すべてのアクティブなブロック
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 はこの ACL の行を読み取り、その行を ACL の最後にコピーします。

     （注）一致しないパケットをすべて許可する場合は、ACL の最後の行を必ず **permit ip any any** にします。

   - **permit ip any any**（Post-Block ACL が指定されている場合は使用しません。）

ARC は、2 つの ACL を使用してデバイスを管理します。一時点でアクティブになるのは、どちらか 1 つだけです。ARC は、オフラインになっている ACL の名前を使用して新しい ACL を作成し、それをインターフェイスに適用します。その後、次のサイクルでは、ARC はこの逆のプロセスを実行します。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新規 ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

Pre-Block または Post-Block ACL を変更する必要がある場合は、次の手順を実行します。

1. センサーでのブロッキングをディセーブルにします。
2. デバイスのコンフィギュレーションを変更します。
3. センサーでのブロッキングを再度イネーブルにします。

ブロッキングが再度有効になると、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。手順については、P.8-8 の「ブロッキング プロパティの設定」を参照してください。

注意　1 つのセンサーで複数のデバイスを管理することはできますが、複数のセンサーで 1 つのデバイスを制御することはできません。このような場合は、マスター ブロッキング センサーを使用します。手順については、P.8-37 の「マスター ブロッキング センサーの設定」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

IPS 5.1 は、ユーザが定義しレート制限と一緒に適用されるサービス ポリシーをサポートしていません。サービス ポリシーには、センサー レート制限との互換性がありません。サービス ポリシーは、レート制限用に設定されたインターフェイス / 方向には適用しないでください。適用すると、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、存在する場合にはそれを削除してください。

レート制限では ACL が使用されますが、使用方法はブロックの場合とは異なります。レート制限は、ACL と class-map エントリを使用して、トラフィック、およびトラフィックをポリシングするための policy-map エントリと service-policy エントリを識別します。

概要

Router Blocking Device Interfaces パネルで、ルータ上のブロッキング インターフェイスまたはレート制限インターフェイスを設定し、ブロックまたはレート制限するトラフィックの方向を指定する必要があります。

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。

(注)　Pre-Block および Post-Block ACL は、レート制限には適用されません。

Pre-Block ACL と Post-Block ACL の各フィールドに、ルータにすでに設定されている 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 の最後に **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 アドレスの **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
- Pre-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。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ルータのブロッキング デバイスのインターフェイスを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、ルータ インターフェイスのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Router Blocking Device Interfaces パネル（P.8-30）
- Add and Edit Router Blocking Device Interface ダイアログボックス（P.8-30）

Router Blocking Device Interfaces パネル

Router Blocking Device Interfaces パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Router Blocking Device**：ブロッキングまたはレート制限を実行するルータ デバイスの IP アドレス。
- **Blocking Interface**：ブロッキングまたはレート制限を実行するルータ デバイスで使用されるインターフェイス。

  a ～ z、A ～ Z、0 ～ 9、「.」および「/」で構成された 1 ～ 64 文字の値が有効です。
- **Direction**：ブロッキング ACL を適用する方向。

  有効な値は In または Out です。
- **Pre-Block ACL**：ブロッキング用の ACL の前に適用する ACL。

  0 ～ 64 文字の値が有効です。このフィールドはレート制限には適用されません。
- **Post-Block ACL**：ブロッキング用の ACL の後で適用する ACL。

  0 ～ 64 文字の値が有効です。このフィールドはレート制限には適用されません。

（注） Post-Block ACL と Pre-Block ACL を同じにすることはできません。

ボタンの機能：

- **Add**：Add Router Blocking Device Interface ダイアログボックスを開きます。

  このダイアログボックスで、ルータのブロッキング デバイスまたはレート制限デバイスのインターフェイスを追加できます。

  ルータのブロッキング デバイスがない場合は、エラー メッセージが表示されます。
- **Edit**：Edit Router Blocking Device Interface ダイアログボックスを表示します。

  このダイアログボックスで、このルータのブロッキング デバイスまたはレート制限デバイスのインターフェイスに関連付けられた値を変更できます。
- **Delete**：ルータのブロッキング デバイス インターフェイスのリストから該当のルータ ブロッキング デバイス インターフェイスを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Router Blocking Device Interface ダイアログボックス

Add and Edit Router Blocking Device Interface ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Router Blocking Device**：ブロッキングまたはレート制限を実行するルータ デバイスの IP アドレス。
- **Blocking Interface**：ブロッキングまたはレート制限を実行するルータ デバイスで使用されるインターフェイス。

  a ～ z、A ～ Z、0 ～ 9、「.」および「/」で構成された 1 ～ 64 文字の値が有効です。
- **Direction**：ブロッキング ACL を適用する方向。

  有効な値は In または Out です。

- **Pre-Block ACL**：ブロッキング用の ACL の前に適用する ACL。
  0 ～ 64 文字の値が有効です。このフィールドはレート制限には適用されません。
- **Post-Block ACL**：ブロッキング用の ACL の後で適用する ACL。
  0 ～ 64 文字の値が有効です。このフィールドはレート制限には適用されません。

（注） Post-Block ACL と Pre-Block ACL を同じにすることはできません。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ルータのブロッキングおよびレート制限のデバイス インターフェイスの設定

ルータのブロッキングおよびレート制限のデバイス インターフェイスを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Blocking > Router Blocking Device Interfaces** をクリックします。

Router Blocking Device Interfaces パネルが表示されます。

ステップ 3　**Add** をクリックし、ルータのブロッキングまたはレート制限のデバイス インターフェイスを追加します。

Add Router Blocking Device Interface ダイアログボックスが表示されます。

ステップ 4　ルータのブロッキング デバイスまたはレート制限デバイスの IP アドレスをドロップダウン リストから選択します。

ステップ 5　**Blocking Interface** フィールドにブロッキングまたはレート制限のインターフェイスの名前を入力します。

ステップ 6　Direction ドロップダウン リストから方向（インまたはアウト）を選択します。

ステップ 7　（オプション）**Pre-Block ACL** フィールドに Pre-Block ACL の名前を入力します。

（注） この手順はレート制限デバイスには適用されません。

ステップ 8　（オプション）**Post-Block ACL** フィールドに Post-Block ACL の名前を入力します。

（注） この手順はレート制限デバイスには適用されません。

ヒント 変更を元に戻して Add Router Blocking Device Interface ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 9 **OK** をクリックします。

IP アドレス / インターフェイス / 方向の組み合せがすでに存在する場合は、エラー メッセージが表示されます。

Router Blocking Device Interfaces パネルのリストに新しいインターフェイスが表示されます。

ステップ 10 ルータのブロッキング デバイス インターフェイスのリストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Router Blocking Device ダイアログボックスが表示されます。

ステップ 11 ブロッキングまたはレート制限のインターフェイスの名前を編集します。

ステップ 12 方向を変更します。

ステップ 13（オプション）Pre-Block ACL の名前を編集します。

ステップ 14（オプション）Post-Block ACL の名前を編集します。

ヒント 変更を元に戻して Edit Router Blocking Device Interface ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 15 **OK** をクリックします。

Router Blocking Device Interfaces パネルのリストに編集したルータのブロッキングまたはレート制限のデバイス インターフェイスが表示されます。

ステップ 16 ブロッキングまたはレート制限のデバイス インターフェイスをリストから削除するには、それを選択して **Delete** をクリックします。

そのルータのブロッキングまたはレート制限のデバイス インターフェイスは、Router Blocking Device Interfaces パネルのリストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 17 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

Catalyst 6000 のブロッキング デバイス インターフェイスの設定

この項では、Catalyst 6500 シリーズ スイッチ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。取り上げる事項は次のとおりです。

- 概要（P.8-33）
- サポートされるユーザのロール（P.8-34）
- フィールド定義（P.8-34）
- Catalyst 6000 のブロッキング デバイス インターフェイスの設定（P.8-35）

概要

Cat 6K Blocking Device Interfaces パネルで、ブロックする Catalyst 6500 シリーズ スイッチの VLAN ID と VACL を指定します。

ARC のブロッキングを設定するときには、Cisco Catalyst ソフトウェアを実行している場合にはスイッチ自体にある VACL を、また、Cisco IOS ソフトウェアを実行している場合には MSFC 上またはスイッチ自体にあるルータの ACL を使用できます。この項では、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で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 スイッチ上でブロッキング 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。

スイッチの設定に Pre-Block VACL と Post-Block VACL を作成して保存します。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。VACL を使用してパケットがチェックされる場合は、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 VACL の許可の行である場合、VACL 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 VACL 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 VACL は、同じ VLAN で追加的な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 に既存の VACL がある場合、その VACL を Post-Block VACL として使用できます。Post-Block VACL がない場合、センサーは新しい VACL の最後に **permit ip any any** を挿入します。

（注） IDSM-2 は、新しい VACL の最後に **permit ip any any capture** を挿入します。

センサーが起動すると、2 つの VACL 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 VACL が作成されます。

- センサーの IP アドレスの **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

センサーは新しい VACL を、指定した VLAN に適用します。

（注）スイッチの VLAN に新しい VACL が適用されると、該当の VLAN に対して他のすべての VACL は適用されなくなります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

Catalyst 6500 シリーズ スイッチのブロッキング デバイスのインターフェイスを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、Catalyst 6500 シリーズ スイッチ インターフェイスのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Cat 6K Blocking Device Interfaces パネル（P.8-34）
- Add and Edit Cat 6K Blocking Device Interface ダイアログボックス（P.8-35）

Cat 6K Blocking Device Interfaces パネル

Cat 6K Blocking Device Interfaces パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Cat 6K Blocking Device**：ブロッキング デバイス（Catalyst 6500 シリーズ スイッチ）の IP アドレス。
- **VLAN ID**：ブロッキング デバイス（Catalyst 6500 シリーズ スイッチ）で使用される VLAN ID。

  値は 1 ～ 4094 です。
- **Pre-Block VACL**：ブロッキング用の VACL の前に適用する VACL。

  0 ～ 64 文字の値です。
- **Post-Block VACL**：ブロッキング用の VACL の後で適用する VACL。

  0 ～ 64 文字の値です。

（注）Post-Block VACL と Pre-Block VACL を同じにすることはできません。

ボタンの機能：

- **Add**：Add Cat 6K Blocking Device Interface ダイアログボックスを表示します。

  このダイアログボックスで、Catalyst 6500 シリーズスイッチのブロッキング デバイス インターフェイスを追加することができます。

  Catalyst 6500 シリーズ スイッチがない場合は、エラーが表示されます。

- **Edit**：Edit Cat 6K Blocking Device Interface ダイアログボックスを表示します。

  このダイアログボックスで、この Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスに関連付けられた値を変更できます。
- **Delete**：スイッチのブロッキング デバイス インターフェイスのリストから該当のスイッチ インターフェイスを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Cat 6K Blocking Device Interface ダイアログボックス

Add and Edit Cat 6K Blocking Device Interface ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Cat 6K Blocking Device**：ブロッキング デバイス（Catalyst 6500 シリーズ スイッチ）の IP アドレス。
- **VLAN ID**：ブロッキング デバイス（Catalyst 6500 シリーズ スイッチ）で使用される VLAN ID。

  値は 1 ～ 4094 です。
- **Pre-Block VACL**：ブロッキング用の VACL の前に適用する VACL。

  0 ～ 64 文字の値です。
- **Post-Block VACL**：ブロッキング用の VACL の後で適用する VACL。

  0 ～ 64 文字の値です。

（注） Post-Block VACL と Pre-Block VACL を同じにすることはできません。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

Catalyst 6000 のブロッキング デバイス インターフェイスの設定

Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Blocking > Cat 6K Blocking Device Interfaces** をクリックします。

CAT 6K Blocking Device Interfaces パネルが表示されます。

ステップ 3　**Add** をクリックし、Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスを追加します。

Add Cat 6K Blocking Device Interface ダイアログボックスが表示されます。

ステップ 4　Catalyst 6500 シリーズ スイッチの IP アドレスをドロップダウン リストから選択します。

ステップ 5　**VLAN ID** フィールドに VLAN ID を入力します。

ステップ 6　（オプション）**Pre-Block VACL** フィールドに Pre-Block VACL の名前を入力します。

ステップ 7　（オプション）**Post-Block VACL** フィールドに Post-Block VACL の名前を入力します。

ヒント　変更を元に戻して Add Cat 6K Blocking Device Interface ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 8　**OK** をクリックします。

IP アドレス /VLAN の組み合せがすでに存在する場合は、エラー メッセージが表示されます。

Cat 6K Blocking Device Interfaces パネルのリストに新しいインターフェイスが表示されます。

ステップ 9　Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスのリストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Cat 6K Blocking Device Interface ダイアログボックスが表示されます。

ステップ 10　VLAN ID を編集します。

ステップ 11　Pre-Block VACL の名前を編集します。

ステップ 12　Post-Block VACL の名前を編集します。

ヒント　変更を元に戻して Edit Cat 6K Blocking Device Interface ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 13　**OK** をクリックします。

Cat 6K Blocking Device Interfaces パネルのリストに編集した Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスが表示されます。

ステップ 14　Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスをリストから削除するには、それを選択して **Delete** をクリックします。

その Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスは、Cat 6K Blocking Device Interfaces パネルのリストから消去されます。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 15　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

マスター ブロッキング センサーの設定

この項では、マスター ブロッキング センサーの設定方法について説明します。取り上げる事項は次のとおりです。

(注) マスター ブロッキング センサーは、マスター レート制限センサーとしても動作できます。

- 概要
- サポートされるユーザのロール（P.8-38）
- フィールド定義（P.8-38）
- マスター ブロッキング センサーの設定（P.8-39）

概要

Master Blocking Sensor パネルで、ブロッキング デバイスを制御するために使用するマスター ブロッキング センサーを指定します。

ブロッキング要求は、複数のセンサー（ブロッキング転送センサー）から、1 つ以上のデバイスを制御する、マスター ブロッキング センサーに転送できます。マスター ブロッキング センサーは、1 つ以上のセンサーに代わって 1 つ以上のデバイスのブロッキングを管理するセンサーで実行される ARC です。マスター ブロッキング センサーの ARC は、他のセンサーで実行されている ARC の要求により、デバイスのブロッキングを制御します。

注意 2 つのセンサーが同一のデバイスでブロッキングやレート制限を制御することはできません。このようにする必要がある場合は、1 つのセンサーをデバイス管理のためのマスター ブロッキング センサーとして設定します。このように設定すると、他のセンサーはマスター ブロッキング センサーに要求を転送することができます。

(注) マスター ブロッキング センサーを追加する場合は、センサーごとにブロックするデバイスの数を減らしてください。たとえば、10 のファイアウォールと 10 のルータでブロッキングを行い、ブロックするインターフェイス / 方向がそれぞれ 1 つずつある場合は、そのうちの 10 をセンサーに割り当て、残りの 10 をマスター ブロッキング センサーに割り当てます。

また、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。

これには、ブロッキング転送センサーで、どのリモート ホストがマスター ブロッキング センサーであるかを特定し、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 センサーで Web 接続に TLS が必要である場合は、ブロッキング転送センサーの ARC がマスター ブロッキング センサーであるリモート ホストの X.509 証明書を受け入れるように設定する必要があります。センサーでは、デフォルトで TLS がイネーブルになっていますが、このオプションは変更可能です。

（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ために設定されます。ブロッキング転送センサーは、通常は他のネットワーク デバイスの管理目的では設定されませんが、設定することはできます。

ブロッキングやレート制限用に設定されたデバイスが存在しない場合であっても、ブロッキングやレート制限を実行するように設定されたセンサーは、ブロッキング要求やレート制限要求をマスター ブロッキング センサーに転送できます。イベント アクションとしてブロッキング要求やレート制限要求が設定されたシグニチャが発生すると、センサーはそのブロッキング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、そこでブロッキングやレート制限が実行されます。

注意　デバイス上のすべてのブロッキング インターフェイスは、1 つのセンサーのみで制御する必要があります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

マスター ブロッキング センサーを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、マスター ブロッキング センサーのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Master Blocking Sensor パネル（P.8-38）
- Add and Edit Master Blocking Sensor ダイアログボックス（P.8-39）

Master Blocking Sensor パネル

Master Blocking Sensor パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：マスター ブロッキング センサーの IP アドレス。
- **Port**：マスター ブロッキング センサーに接続するためのポート。
  デフォルトは 443 です。
- **Username**：マスター ブロッキング センサーへのログインに使用されるユーザ名。
  1 ～ 64 文字の値が有効です。
- **TLS Used**：TLS を使用するかどうかを指定します。

ボタンの機能：

- **Add**：Add Master Blocking Sensor ダイアログボックスを表示します。
  このダイアログボックスで、マスター ブロッキング センサーを追加できます。
- **Edit**：Edit Master Blocking Sensor ダイアログボックスを表示します。
  このダイアログボックスで、このマスター ブロッキング センサーに関連付けられた値を変更できます。
- **Delete**：マスター ブロッキング センサーのリストから該当のマスター ブロッキング センサーを削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Master Blocking Sensor ダイアログボックス

Add and Edit Master Blocking Sensor ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：マスター ブロッキング センサーの IP アドレス。
  IP アドレスがすでに存在する場合は、警告が表示されます。
- **Port**：（オプション）マスター ブロッキング センサーの接続先ポート。
  デフォルトは 443 です。
- **Username**：マスター ブロッキング センサーへのログインに使用されるユーザ名。
  1 ～ 16 文字の値が有効です。
- **Change the password**：パスワードを変更するかどうかを指定します。
- **New Password**：マスター ブロッキング センサーへのログインに使用されるログイン パスワード。
- **Confirm Password**：ログイン パスワードの確認。
- **Use TLS**：TLS を使用するかどうかを指定します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

マスター ブロッキング センサーの設定

マスター ブロッキング 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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Blocking > Master Blocking Sensor** をクリックします。

Master Blocking Sensor パネルが表示されます。

ステップ 3　**Add** をクリックし、マスター ブロッキング センサーを追加します。

Add Master Blocking Sensor ダイアログボックスが表示されます。

ステップ 4　**IP Address** フィールドにマスター ブロッキング センサーの IP アドレスを入力します。

ステップ 5　（オプション）**Port** フィールドにポート番号を入力します。

デフォルトは 443 です。

ステップ 6　**Username** フィールドにユーザ名を入力します。

ステップ 7　**Password** フィールドにユーザのパスワードを入力します。

ステップ 8　**Confirm New Password** フィールドにパスワードを再度入力します。

ステップ 9　**TLS** チェックボックスをオンにします。

ヒント　変更を元に戻して Add Master Blocking Sensor ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 10　**OK** をクリックします。

IP アドレスがすでに追加されている場合は、エラー メッセージが発生します。

Master Blocking Sensor パネルのリストに新しいマスター ブロッキング センサーが表示されます。

ステップ 11　TLS を選択した場合は、マスター ブロッキング センサー リモート ホストの TLS/SSL X.509 証明書を受け取るためにブロッキング転送センサーの ARC を設定します。

（注）　また、**Configuration > Certificates > Trusted Hosts > Add Trusted Host** をクリックして、X.509 証明書を受け取るためのブロッキング転送センサーを設定することもできます。手順については、P.2-17 の「信頼できるホストの追加」を参照してください。

a.　管理者特権を持つアカウントを使用してブロッキング転送センサーの CLI にログインします。

b.　グローバル コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

c.　信頼できるホストを追加します。

```
sensor(config)# tls trusted-host ip-address master_blocking_sensor_ip_address
```

信頼できるホストの追加を確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

d.　**yes** を入力して、ホストを追加します。

e.　グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

（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に求めるプロンプトが表示されます。センサーは自己署名証明書のみを提示します（公認の認証局の証明書ではありません）。マスター ブロッキング センサーのホスト センサーの証明書は、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の証明書のフィンガープリントが一致していることを調べることで、確認できます。

ステップ 12 マスター ブロッキング センサー リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit Master Blocking Sensor ダイアログボックスが表示されます。

ステップ 13（オプション）ポートを編集します。

ステップ 14 ユーザ名を編集します。

ステップ 15 このユーザのパスワードを変更する場合は、**Change the password** を選択します。

a. **New Password** フィールドに新しいパスワードを入力します。

b. 確認のため、**Confirm New Password** フィールドに新しいパスワードを再度入力します。

ステップ 16 **TLS** チェックボックスをオンまたはオフにします。

ヒント 変更を元に戻して Edit Master Blocking Sensor ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 17 **OK** をクリックします。

Master Blocking Sensor パネルのリストに編集したマスター ブロッキング センサーが表示されます。

ステップ 18 リストからマスター ブロッキング センサーを削除するには、それを選択して **Delete** をクリックします。

そのマスター ブロッキング センサーは、Master Blocking Sensor パネルのリストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 19 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

アクティブなホスト ブロックの管理

この項では、アクティブなホスト ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-42）
- サポートされるユーザのロール（P.8-42）
- フィールド定義（P.8-42）
- アクティブなホスト ブロックの設定および管理（P.8-44）

概要

Active Host Blocks パネルで、ホストのブロッキングを設定および管理できます。

アクティブなホスト ブロックは、特定のホストからのトラフィックを（そのブロックを削除するまで）永続的にブロックするか、指定された期間ブロックします。宛先 IP アドレスと、宛先のプロトコルおよびポートを指定することにより、接続をベースにしたブロックを実行することもできます。

アクティブなホスト ブロックは、送信元 IP アドレスによって定義されます。既存のブロックと同じ送信元 IP アドレスを持つブロックを追加すると、新しいブロックによって古いブロックが上書きされます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ホスト ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

アクティブなホスト ブロックを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、アクティブなホスト ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Active Host Blocks パネル（P.8-42）
- Add Active Host Block ダイアログボックス（P.8-43）

Active Host Blocks パネル

Active Host Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Destination IP**：ブロックの宛先 IP アドレス。
- **Destination Port**：ブロックの宛先ポート。

- **Protocol**：プロトコルのタイプ（TCP、UDP、または ANY）。
  デフォルトは ANY です。
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **VLAN**：シグニチャを発生させたデータを伝送した VLAN を示します。

注意　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

- **Connection Block Enabled**：ホストへの接続をブロックするかどうか。

ボタンの機能：

- **Add**：Add Active Host Block ダイアログボックスを開きます。
  このダイアログボックスから、ホストの手動ブロックを追加できます。
- **Delete**：アクティブなホスト ブロックのリストから該当の手動ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Active Host Block ダイアログボックス

Add Active Host Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Enable connection blocking**：ホストへの接続をブロックするかどうか。
- **Connection Blocking**：接続ブロッキングのパラメータを設定できます。
  - **Destination IP**：ブロックの宛先 IP アドレス。
  - **Destination Port**：（オプション）ブロックの宛先ポート。
  - **Protocol**：（オプション）プロトコルのタイプ（TCP、UDP、または ANY）。
    デフォルトは ANY です。
- **VLAN**：（オプション）シグニチャを発生させたデータを伝送した VLAN を示します。

注意　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

- **Enable Timeout**：ブロックのタイムアウト値（分単位）を設定できます。
- **Timeout**：ブロックを続ける時間（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。

- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

アクティブなホスト ブロックの設定および管理

アクティブなホスト ブロックを設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring > Active Host Blocks** をクリックします。

Active Host Blocks パネルが表示されます。

ステップ 3　**Add** をクリックして、アクティブなホスト ブロックを追加します。

Add Active Host Block ダイアログボックスが表示されます。

ステップ 4　ブロックするホストの送信元 IP アドレスを入力します。

ステップ 5　ブロックを接続ベースにする場合は、**Enable Connection Blocking** チェックボックスを選択します。

（注）　接続ブロックでは、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がブロックされます。

a. **Destination IP** フィールドに宛先 IP アドレスを入力します。
b. （オプション）**Destination Port** フィールドに宛先ポートを入力します。
c. Protocol ドロップダウン リストからプロトコルを選択します。

ステップ 6　（オプション）**VLAN** フィールドに、接続ブロックの VLAN を入力します。

ステップ 7　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 8　**Timeout** フィールドに、時間（分単位）を入力します。

ヒント　変更を元に戻して Add Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 9　ブロックに一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

ステップ 10　**Apply** をクリックします。

その IP アドレスにブロックが設定されている場合は、エラー メッセージが発生します。

Active Host Blocks パネルのリストに新しいアクティブなホスト ブロックが表示されます。

ステップ 11　**Refresh** をクリックして、アクティブなホスト ブロックのリストの内容をリフレッシュします。

ステップ 12 ブロックを削除するには、リストでアクティブなホスト ブロックを選択して、**Delete** をクリックします。

Delete Active Host Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

ヒント 変更を元に戻して Delete Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 13 **Yes** をクリックしてブロックを削除します。

ネットワーク ブロックの管理

この項では、ネットワーク ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.8-46）
- サポートされるユーザのロール（P.8-46）
- フィールド定義（P.8-46）
- ネットワーク ブロックの設定および管理（P.8-47）

概要

Network Blocks パネルで、ネットワークのブロッキングを設定および管理できます。

ネットワーク ブロックは、特定のネットワークからのトラフィックを（そのブロックを削除するまで）恒常的にブロックするか、指定された期間ブロックします。

ネットワーク ブロックは、送信元 IP アドレスとネットマスクによって定義されます。ネットマスクは、ブロックされるサブネットを定義します。ホストのサブネット マスクも受け入れられます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ネットワーク ブロックを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、ネットワーク ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Network Blocks パネル（P.8-46）
- Add Network Block ダイアログボックス（P.8-47）

Network Blocks パネル

Network Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロックの IP アドレス。
- **Mask**：ブロックのネットワーク マスク
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。

ボタンの機能：

- **Add**：Add Network Block ダイアログボックスを表示します。
  このダイアログボックスから、ネットワークのブロックを追加できます。
- **Delete**：ブロックのリストから該当のネットワーク ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Network Block ダイアログボックス

Add Network Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの IP アドレス。
- **Netmask**：ブロックのネットワーク マスク。
- **Enable Timeout**：ブロックのタイムアウト値（分単位）を示します。
- **Timeout**：ブロックの期間（分単位）を示します。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：該当のブロックをすぐにセンサーに送信します。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ネットワーク ブロックの設定および管理

ネットワーク ブロックを設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring > Features > IPS > Network Blocks** をクリックします。

Network Blocks パネルが表示されます。

ステップ 3　**Add** をクリックして、ネットワーク ブロックを追加します。

Add Network Block ダイアログボックスが表示されます。

ステップ 4　ブロックするネットワークの送信元 IP アドレスを入力します。

ステップ 5　Netmask ドロップダウン リストからネットマスクを選択します。

ステップ 6　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 7　**Timeout** フィールドに、時間（分単位）を入力します。

ヒント　変更を元に戻して Add Network Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 8　**Apply** をクリックします。

ブロックがすでに追加されている場合は、エラー メッセージが発生します。

Network Blocks パネルのリストに新しいネットワーク ブロックが表示されます。

ステップ 9　**Refresh** をクリックして、ネットワーク ブロックのリストの内容をリフレッシュします。

ステップ 10　ブロックを削除するには、リストでネットワーク ブロックを選択して **Delete** をクリックします。

Delete Network Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

ステップ 11　**Yes** をクリックしてブロックを削除します。

SNMP の設定

この章では、SNMP および SNMP トラップを使用するようにセンサーを設定する方法について説明します。

(注) センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **Request SNMP Trap** をイベント アクションとして選択します。詳細については、P.5-24 の「シグニチャへのアクションの割り当て」を参照してください。

この章は、次の項で構成されています。

- SNMP の説明（P.9-2）
- SNMP の設定（P.9-3）
- SNMP トラップの設定（P.9-5）

SNMP の説明

SNMP は、ネットワーク デバイス間の管理情報の交換を促進するアプリケーション レイヤ 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 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、ネットワーク成長の計画を立てることができます。

SNMP は単純な要求 / 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、Get、GetNext、Set、および Trap の 4 つのプロトコル操作のいずれかを使用することによって実装されます。

SNMP によるモニタリングのためにセンサーを設定することができます。SNMP は、ネットワーク管理ステーションが、スイッチ、ルータ、センサーなどさまざまな種類のデバイスの健全性とステータスを監視する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することができます。SNMP トラップを使用すると、エージェントが割り込み SNMP メッセージによって管理ステーションに重大なイベントを通知することができます。

トラップで指示された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に責任を負っていて、各デバイスに多数のオブジェクトがある場合、すべてのデバイス上のすべてのオブジェクトからの情報をポーリングまたは要求するのは実際的ではありません。解決法は、管理対象デバイス上の各エージェントが送信要求なしでマネージャに通知することです。これは、イベントのトラップとして知られているメッセージを送信することによって実行されます。

イベントの受信後、マネージャはそれを表示し、イベントに基づいてアクションを実行することができます。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こともできますし、イベントをよりよく理解するためにその他の関連するデバイス エージェントをポーリングすることもできます。

(注) トラップで指示された通知は、重要でない SNMP 要求を排除することによって、ネットワークおよびエージェントのリソースを実質的に節約できます。ただし、SNMP ポーリングを完全に排除することはできません。SNMP 要求は、ディスカバリとトポロジの変更に必要です。さらに、深刻な停止の場合、管理対象デバイス エージェントはトラップを送信できません。

SNMP の設定

この項では、SNMP の設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.9-3）
- サポートされるユーザのロール（P.9-3）
- フィールド定義（P.9-3）
- SNMP の設定（P.9-4）

概要

SNMP General Configuration パネルで、SNMP を使用するようにセンサーを設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

SNMP を使用するようにセンサーを設定するには、管理者である必要があります。

フィールド定義

SNMP General Configuration パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Enable SNMP Gets/Sets**：選択すると、SNMP get および SNMP set が許可されます。
- **SNMP Agent Parameters**：SNMP エージェントのパラメータを設定します。
  - **Read-Only Community String**：読み取り専用アクセスのコミュニティ ストリングを示します。
  - **Read-Write Community String**：読み取りと書き込みアクセスのコミュニティ ストリングを示します。
  - **Sensor Contact**：センサーの問い合せ先担当者、問い合せ先、またはその両方を示します。
  - **Sensor Location**：センサーの場所を示します。
  - **Sensor Agent Port**：センサーの IP ポートを示します。
    デフォルトは 161 です。
  - **Sensor Agent Protocol**：センサーの IP プロトコルを示します。
    デフォルトは 443 です。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

SNMP の設定

（注） センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **Request SNMP Trap** をイベント アクションとして選択します。詳細については、P.5-24 の「シグニチャへのアクションの割り当て」を参照してください。

一般的な SNMP 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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > SNMP > SNMP General Configuration** をクリックします。

SNMP General Configuration パネルが表示されます。

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、**Enable SNMP Gets/Sets** を選択して SNMP をイネーブルにします。

ステップ 4　SNMP エージェント パラメータを設定します。

SNMP 管理ワークステーションがセンサー SNMP エージャントに対して要求できる値があります。

a. **Read-Only Community String** フィールドに読み取り専用コミュニティ ストリングを割り当てます。

   読み取り専用コミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

b. **Read-Write Community String** フィールドに、リード / ライト（read/write）コミュニティ ストリングを割り当てます。

   リード/ライト コミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

（注） 管理ワークステーションは SNMP 要求を、センサーに常駐するセンサー SNMP エージェントに送信します。管理ワークステーションが要求を発行し、コミュニティ ストリングがセンサー上のコミュニティ ストリングと一致しない場合、センサーはその要求を拒否します。

c. **Sensor Contact** フィールドにセンサーの問い合せ先のユーザ ID を入力します。

d. **Sensor Location** フィールドにセンサーの場所を入力します。

e. **Sensor Agent Port** フィールドにセンサー SNMP エージェントのポートを入力します。

   デフォルト SNMP ポート番号は 161 です。

f. **Sensor Agent Protocol** リストからセンサー SNMP エージェントが使用するプロトコルを選択します。

g. デフォルト プロトコルは UDP です。

ヒント　変更を元に戻すには、**Reset** をクリックします。

ステップ 5　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

SNMP トラップの設定

この項では、SNMP トラップの設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.9-5）
- サポートされているユーザ ロール（P.9-5）
- フィールド定義（P.9-5）
- SNMP トラップの設定（P.9-6）

概要

SNMP Traps Configuration パネルで、SNMP トラップとセンサーのトラップ宛先をセットアップできます。

SNMP トラップは通知です。イベントが fatal、error、または warning のいずれかであるかに基づいて、センサーがトラップを送信するように設定します。

サポートされているユーザ ロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

センサーに SNMP トラップを設定するには、管理者である必要があります。

フィールド定義

この項では、SNMP トラップのフィールドの定義を示します。取り上げる事項は次のとおりです。

- SNMP Traps Configuration パネル（P.9-5）
- Add and Edit SNMP Trap Destination ダイアログボックス（P.9-6）

SNMP Traps Configuration パネル

SNMP Traps Configuration パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Enable SNMP Traps**：選択すると、プル アップデートを使用するようにリモート サーバに指示します。
- **SNMP を使用して通知するエラー イベントを選択します。**
  - **Fatal**：すべての *fatal* エラー イベントについてトラップを生成します。
  - **Error**：すべての *error* エラー イベントについてトラップを生成します。
  - **Warning**：すべての *warning* エラー イベントについてトラップを生成します。
- **Enable detailed traps for alerts**：選択すると、トラップにアラートの全テキストが含まれます。選択しない場合は、希薄モードが使用されます。希薄モードでは、484 バイト未満のアラートのテキストが含まれます。
- **Default Trap Community String**：トラップに特定のストリングが設定されていない場合に使用するコミュニティ ストリング。

- **Specify SNMP trap destinations**：トラップの宛先を示します。
  宛先について次の情報を指定する必要があります。
  - **IP Address**：トラップ宛先の IP アドレス。
  - **UDP Port**：トラップ宛先の UDP ポート。
  - **Trap Community String**：トラップ コミュニティ ストリング。

ボタンの機能：

- **Add**：Add SNMP Trap Destination ダイアログボックスを表示します。
  このダイアログボックスで、SNMP トラップの新しい宛先を追加できます。
- **Edit**：Edit SNMP Trap Destination ダイアログボックスを表示します。
  このダイアログボックスで、選択した宛先を定義するパラメータを変更できます。
- **Delete**：選択した宛先を削除します。
- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit SNMP Trap Destination ダイアログボックス

Add and Edit SNMP Trap Destination ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：トラップ宛先の IP アドレス。
- **UDP Port**：トラップ宛先の UDP ポート。
  デフォルトはポート 162 です。
- **Trap Community String**：トラップ コミュニティ ストリング。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

SNMP トラップの設定

（注） センサーに SNMP トラップを送信させるには、シグニチャを設定する際に **Request SNMP Trap** をイベント アクションとして選択します。詳細については、P.5-24 の「シグニチャへのアクションの割り当て」を参照してください。

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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > SNMP > SNMP Traps Configuration** をクリックします。

SNMP Traps Configuration パネルが表示されます。

ステップ 3　**Enable SNMP Traps** を選択して SNMP トラップをイネーブルにします。

ステップ 4　SNMP トラップのパラメータを設定します。

a. SNMP トラップを使用して通知するエラー イベントを選択します。

センサーが、fatal、error、warning のエラー イベントのいずれかに基づいて SNMP トラップを送信するか、またはすべてに基づいて SNMP トラップを送信するかを選択できます。

b. 詳細な SNMP トラップが必要な場合は、**Enable detailed traps for alerts** チェックボックスをオンにします。

c. **Default Trap Community String** フィールドに、詳細な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。

ステップ 5　どの管理ワークステーションに送信するかをセンサーに知らせるため、SNMP トラップ宛先のパラメータを設定します。

a. **Add** をクリックします。

Add SNMP Trap Destination ダイアログボックスが表示されます。

b. **IP Address** フィールドに SNMP 管理ステーションの IP アドレスを入力します。

c. **UDP Port** フィールドに SNMP 管理ステーションの UDP ポートを入力します。

d. **Trap Community String** フィールドにトラップ コミュニティ ストリングを入力します。

(注) コミュニティ ストリングがトラップに表示されます。これは、複数のエージェントから複数のタイプのトラッ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がトラップを送信する場合に、具体的にルータまたはセンサーを識別する何かをコミュニティ ストリングに入力すると、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リングすることができます。

ヒント 変更を元に戻して Add SNMP Trap Destination ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 6　**OK** をクリックします。

SNMP Traps Configuration パネルのリストに新しい SNMP トラップ宛先が表示されます。

ステップ 7　SNMP トラップ宛先を編集するには、それを選択して **Edit** をクリックします。

Edit SNMP Trap Destination ダイアログボックスが表示されます。

ステップ 8　**UDP Port** フィールドおよび **Trap Community String** フィールドを編集します。

ヒント 変更を元に戻して Edit SNMP Trap Destination ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 9　**OK** をクリックします。

SNMP Traps Configuration パネルのリストに編集した SNMP トラップ宛先が表示されます。

ステップ 10 SNMP トラップ宛先を削除するには、それを選択して **Delete** をクリックします。

その SNMP トラップ宛先は、SNMP Traps Configuration パネルのリストから消去されます。

ヒント 変更を元に戻すには、**Reset** をクリックします。

ステップ 11 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

センサーの保守

この章では、最新のソフトウェアによるセンサーの自動更新、即座の更新、工場出荷時のデフォルト設定の復元、センサーのシャットダウンなどの手段で、センサーを保守する方法について説明します。また、トラブルシューティングを目的として情報を生成しておき、TAC に問い合せるときに必要な場合にそれを使用することもできます。

この章は、次の項で構成されています。

- センサーの自動更新（P.10-2）
- デフォルト設定の復元（P.10-5）
- センサーのリブート（P.10-6）
- センサーのシャットダウン（P.10-8）
- センサーの更新（P.10-9）
- 診断レポートの生成（P.10-12）
- 統計情報の表示（P.10-15）
- システム情報の表示（P.10-16）

センサーの自動更新

この項では、センサーの自動更新を設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-2）
- サポートされるユーザのロール（P.10-2）
- フィールド定義（P.10-2）
- 自動更新の設定（P.10-3）

概要

サービス パックとシグニチャの自動更新を設定し、これらのアップデートが中央の FTP または SCP サーバにロードされたときにダウンロードが行われ、センサーに適用されるようにすることができます。

自動更新は、DOS 形式のパスで設定された Windows FTP サーバでは動作しません。サーバの設定が DOS 形式のパスではなく、UNIX 形式のパス オプションに対応していることを確認してください。

（注） センサーは、サービス パックとシグニチャ アップデートを Cisco.com から自動的にダウンロードできません。サービス パックとシグニチャ アップデートは Cisco.com から FTP または SCP サーバにダウンロードし、この FTP または SCP サーバからセンサーがダウンロードするように設定する必要があります。

注意 Cisco.com から更新をダウンロードしたら、FTP または SCP サーバ上のダウンロード ファイルが完全な状態であることを保証できるように対策を講じる必要があります。

サポートされるユーザのロール

Auto Update パネルを表示したり、自動更新を設定したりするには、管理者である必要があります。

フィールド定義

Auto Update パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Enable Auto Update**：センサーはリモート サーバに保存されたアップデートをインストールします。

  Enable Auto Update が選択されていない場合は、すべてのフィールドがディセーブルになり値は消去されます。その他のすべての設定値を失わずに、このオン / オフを切り替えることはできません。
- **Remote Server Settings**：次のオプションを指定します。
  - **IP Address**：リモート サーバの IP アドレスを示します。
  - **File Copy Protocol**：FTP または SCP のどちらを使用するかを指定します。
  - **Directory**：リモート サーバ上のアップデートへのパスを示します。

- **Username**：リモート サーバ上のユーザ アカウントに対応するユーザ名を示します。
- **Password**：リモート サーバ上のユーザ アカウントのパスワードを示します。
- **Confirm Password**：リモート サーバのパスワードの再入力を要求してパスワードを確認します。

- **Schedule**：次のオプションを指定します。
  - **Start Time**：更新プロセスの開始時間を示します。

    これは、センサーがリモート サーバに接続し、使用可能なアップデートを検索する時点での時間です。
  - **Frequency**：更新を時間単位で実行するか、または週単位で実行するかを指定します。

    Hourly：*n* 時間ごとに更新を確認するように指定します。

    Daily：更新を実行する曜日を指定します。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

自動更新の設定

自動更新を設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Auto Update** をクリックします。

Auto Update パネルが表示されます。

ステップ 3　**Enable Auto Update** チェックボックスをオンにして、自動更新を使用可能にします。

ステップ 4　**IP Address** フィールドに、アップロードをダウンロードし保存するリモート サーバの IP アドレスを入力します。

ステップ 5　リモート サーバに接続するために使用するプロトコルを識別するため、File Copy Protocol リストから **FTP** または **SCP** のどちらかを選択します。

ステップ 6　**Directory** フィールドに、アップデートが配置されたリモート サーバのディレクトリへのパスを入力します。

パスの有効な値は 1 ～ 128 文字です。

ステップ 7　**Username** フィールドに、リモート サーバにログインするために使用するユーザ名を入力します。

ユーザ名の有効な値は 1 ～ 2047 文字です。

ステップ 8　**Password** フィールドに、リモート サーバのユーザ名パスワードを入力します。

パスワードの有効な値は 1 ～ 2047 文字です。

ステップ 9　**Confirm Password** フィールドにパスワードを再度入力します。

ステップ 10 更新を時間単位で指定するには、**Hourly** を選択し、次の手順を実行します。

a. **Start Time** フィールドに、アップデートを開始する時刻を入力します。

有効な値は hh:mm:ss です。

b. **Every_hours** フィールドに、各更新を実行する時間間隔を入力します。

有効な値は 1 ～ 8760 です。

たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新できるものがあれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーは、インストール可能な最新のアップデートを判別し、そのファイルをインストールします。

ステップ 11 更新を週単位で指定するには、**Daily** を選択し、次の手順を実行します。

a. **Start Time** フィールドに、アップデートを開始する時刻を入力します。

有効な値は hh:mm:ss です。

b. **Days** フィールドで、センサーが使用可能なアップデートを確認しダウンロードする曜日を選択します。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 12 **Apply** をクリックし、変更を保存します。

デフォルト設定の復元

この項では、センサーに工場出荷時のデフォルト設定を復元する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-5）
- サポートされるユーザのロール（P.10-5）
- フィールド定義（P.10-5）
- デフォルト設定の復元（P.10-5）

概要

センサーはデフォルト設定に復元できます。

警告　デフォルト設定を復元すると、現在のアプリケーションの設定が削除され、デフォルトの設定が復元されます。ネットワークの設定もデフォルトに戻り、センサーへの接続も即座に失われます。

サポートされるユーザのロール

Restore Defaults パネルを表示したり、センサーのデフォルト設定を復元したりするには、管理者である必要があります。

フィールド定義

Restore Defaults パネルには次のフィールドとボタンがあります。

ボタンの機能：

- **Restore Defaults**：Restore Defaults ダイアログボックスを表示します。

  このダイアログボックスで、デフォルト設定の復元プロセスを開始できます。このプロセスは、センサーの設定をデフォルト設定に戻し、即座にセンサーへの接続を終了します。
- **OK**：デフォルト設定の復元プロセスを開始します。
- **Cancel**：Restore Defaults ダイアログボックスを閉じ、デフォルト設定の復元プロセスを実行せずに Restore Defaults パネルに戻ります。

デフォルト設定の復元

デフォルト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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Restore Defaults** をクリックします。

Restore Defaults パネルが表示されます。

ステップ 3　**Restore Configuration Defaults** をクリックし、デフォルトの設定を復元します。

Restore Defaults ダイアログボックスが表示されます。

ステップ 4　**Yes** をクリックし、デフォルト設定の復元プロセスを開始します。

（注） デフォルト設定を復元すると、IP アドレス、ネットマスク、デフォルト ゲートウェイ、およびアクセス リストはリセットされます。パスワードと時間はリセットされません。手動および自動ブロックも有効なままになります。

センサーのリブート

この項では、IDM からセンサーをリブートする方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-6）
- サポートされるユーザのロール（P.10-6）
- フィールド定義（P.10-6）
- センサーのリブート（P.10-7）

概要

Reboot Sensor パネルからセンサーをシャットダウンし再起動することができます。

サポートされるユーザのロール

Restore Sensor パネルを表示したり、センサーをリブートしたりするには、管理者である必要があります。

フィールド定義

Reboot Sensor パネルには次のボタンがあります。

ボタンの機能：

- **Reboot Sensor**：Reboot Sensor ダイアログボックスを表示します。

  このダイアログボックスで、センサーをシャットダウンし再起動するプロセスを開始できます。
- **OK**：センサーをシャットダウンし再起動します。これによって、即座にセンサーへの接続は失われます。センサーの再起動後にログインし直すことができます。
- **Cancel**：Reboot Sensor ダイアログボックスを閉じ、センサーをシャットダウンせずに Reboot Sensor パネルに戻ります。

センサーのリブート

センサーをリブートするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Reboot Sensor** をクリックします。

Reboot Sensor パネルが表示されます。

ステップ 3　**Reboot Sensor** をクリックします。

Reboot Sensor ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックして、センサーをシャットダウンし再起動します。

センサーのアプリケーションがシャットダウンし、その後、センサーがリブートします。リブート後に、ログインする必要があります。

（注）　CLI にログインしているユーザに対して、センサーがシャットダウンするという通知が表示されてから、30 秒後にシャットダウンされます。

センサーのシャットダウン

この項では、IDM からセンサーをシャットダウンする方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-8）
- サポートされるユーザのロール（P.10-8）
- フィールド定義（P.10-8）
- センサーのシャットダウン（P.10-8）

概要

IPS アプリケーションをシャットダウンしてから、センサーを安全に電源を切断できる状態にします。

サポートされるユーザのロール

Shut Down Sensor パネルを表示したり、センサーをシャットダウンしたりするには、管理者である必要があります。

フィールド定義

Shut Down Sensor パネルには次のフィールドとボタンがあります。

ボタンの機能：

- **Shut Down Sensor**：Shut Down Sensor ダイアログボックスを表示します。
  このダイアログボックスで、センサーをシャットダウンするプロセスを開始できます。
- **OK**：センサーをシャットダウンし、開いているセンサーへの接続を即座に閉じます。
- **Cancel**：シャットダウン プロセスを開始せずに、Shut Down Sensor ダイアログボックスを閉じます。

センサーのシャットダウン

センサーをシャットダウンするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Shut Down Sensor** をクリックします。

Shut Down Sensor パネルが表示されます。

ステップ 3　**Shut Down Sensor** をクリックします。

Shut Down Sensor ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックして、センサーをシャットダウンします。

センサーのアプリケーションがシャットダウンし、開いているセンサーへの接続は閉じられます。

（注）　CLI にログインしているユーザに対して、センサーがシャットダウンするという通知が表示されてから、30 秒後にシャットダウンされます。

センサーの更新

この項では、最新のソフトウェアでセンサーを更新する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-9）
- サポートされるユーザのロール（P.10-9）
- フィールド定義（P.10-9）
- センサーの更新（P.10-10）

概要

Update Sensor パネルから、即座にサービス パックとシグニチャ アップデートを適用できます。

（注）　センサーは、サービス パックとシグニチャ アップデートを Cisco.com からダウンロードできません。サービス パックとシグニチャ アップデートは Cisco.com から FTP サーバにダウンロードし、この FTP サーバからセンサーがダウンロードするように設定する必要があります。

サポートされるユーザのロール

Update Sensor パネルを表示したり、サービス パックやシグニチャ アップデートでセンサーを更新したりするには、管理者である必要があります。

フィールド定義

Update Sensor パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Update is located on a remote server and is accessible by the sensor**：次のオプションを指定します。
  - **URL**：アップデートが配置されているサーバのタイプを示します。FTP、HTTP/S、または SCP のどれを使用するかを指定します。
  - **://**：リモート サーバ上のアップデートへのパスを示します。
  - **Username**：リモート サーバ上のユーザ アカウントに対応するユーザ名を示します。
  - **Password**：リモート サーバ上のユーザ アカウントのパスワードを示します。
- **Update is located on this client**：次のオプションを指定します。
  - **Local File Path**：このローカル クライアント上のアップデート ファイルへのパスを示します。
  - **Browse Local**：このローカル クライアント上のファイル システムの Browse ダイアログボックスを表示します。このダイアログボックスで、アップデート ファイルにナビゲートできます。

ボタンの機能：

- **Update Sensor**：Update Sensor ダイアログボックスを表示します。このダイアログボックスで、インスタント アップデートを開始できます。
- **OK**：Update Sensor パネルに設定されたパラメータに従って、即座にセンサーを更新します。
- **Cancel**：更新を実行せずに Update Sensor ダイアログボックスを閉じます。

センサーの更新

サービス パックとシグニチャ アップデートをすぐに適用するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Update Sensor** をクリックします。

Update Sensor パネルが表示されます。

ステップ 3　アップデートをリモート サーバからプルダウンしてセンサーにインストールするには、次の手順を実行します。

a. **Update is located on a remote server and is accessible by the sensor** を選択します。

b. **URL** フィールドにアップデートを検索できる URL を入力します。

サポートされる URL タイプは、次のとおりです。

- FTP：FTP ネットワーク サーバの発信元 URL。

  このプレフィクスの構文は、次のとおりです。

  `ftp://location/relative_directory/filename`

  または

  `ftp://location//absolute_directory/filename`

- HTTPS：Web サーバの発信元 URL

  このプレフィクスの構文は、次のとおりです。

  `https://location/directory/filename`

  （注） HTTPS プロトコルを使用する前に、**tls trusted-host** コマンドを使用して TLS 信頼ホストを設定します。

- SCP：SCP ネットワーク サーバの発信元 URL。

  このプレフィクスの構文は、次のとおりです。

  `scp://location/relative_directory/filename`

  または

  `scp://location/absolute_directory/filename`

- HTTP：Web サーバの発信元 URL

  このプレフィクスの構文は、次のとおりです。

  `http://location/directory/filename`

次の例は、FTP プロトコルを示しています。

```
ftp://user@ip_address/UPDATES/file_name.rpm.pkg
```

(注) アップデートをあらかじめ Cisco.com からダウンロードし、FTP サーバに保存しておく必要があります。

c. **Username** フィールドに、リモート サーバ上のアカウントのユーザ名を入力します。

d. **Password** フィールドに、リモート サーバ上のこのアカウントに関連付けられたパスワードを入力します。

ステップ 4 ローカル　クライアントからセンサーにプッシュしてインストールするには、次の手順を実行します。

a. **Update is located on this client** を選択します。

b. ローカル クライアント上のアップデート ファイルへのパスを指定するか、または **Browse Local** をクリックしてローカル クライアント上のファイルをナビゲートします。

ステップ 5 **Update Sensor** をクリックします。

Update Sensor ダイアログボックスに、更新するとセンサーへの接続が失われ再度ログインする必要が生じることを示すメッセージが表示されます。

ステップ 6 **OK** をクリックして、センサーを更新します。

ヒント 変更を元に戻してダイアログボックスを閉じるには、**Cancel** をクリックします。

(注) サービス パック、マイナー アップデート、メジャー アップデート、エンジニアリング パッチによる更新時には、IDM および CLI の接続は失われます。これらのアップデートのいずれかを適用すると、インストーラが自動的に IPS アプリケーションを再起動します。センサーをリブートできます。シグニチャ アップデートを適用する場合は、接続が失われないため、システムをリブートする必要はありません。

診断レポートの生成

この項では、診断レポートを生成する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-12）
- サポートされるユーザのロール（P.10-12）
- フィールド定義（P.10-12）
- 診断レポートの生成（P.10-13）

概要

トラブルシューティング用に、センサーの診断情報を取得できます。診断レポートには、TAC がセンサーのトラブルシューティングに使用することを目的として、ログ、ステータス、設定などの内部システムの情報が含まれています。

（注） 診断レポートの生成には数分かかることがあります。

Diagnostics Report パネルでレポートを表示できます。また、**Save** をクリックして、それをハードディスク ドライブに保存することもできます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

診断を実行するには、管理者である必要があります。

フィールド定義

Diagnostics Report パネルには次のボタンがあります。

ボタンの機能：

- **Save**：**Save As** ダイアログボックスが表示されます。ここで、診断レポートのコピーをハードディスク ドライブに保存できます。
- **Generate Report**：診断プロセスを開始します。

  このプロセスが完了するまでに数分かかることがあります。プロセスが完了すると、レポートが生成され、更新されたレポートで表示がリフレッシュされます。

診断レポートの生成

診断を実行するには、次の手順を実行します。

注意　診断プロセスが開始したら、IDM 内のその他のオプションをクリックしたり、Diagnostics パネルを終了したりしないでください。このプロセスが完了するまで、センサーのその他のタスクは一切実行できません。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring > Support Information > Diagnostics Report** をクリックします。

Diagnostics パネルが表示されます。

ステップ 3　**Generate New Report** をクリックします。

（注）　診断プロセスが完了するまでに数分かかることがあります。プロセスの実行が完了すると、更新された結果で表示がリフレッシュされます。

（注）　このレポートをファイルとして保存するには、**Save** をクリックします。**Save As** ダイアログボックスが表示され、レポートをハードディスク ドライブに保存できます。

統計情報の表示

この項では、センサーの統計情報を表示する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-14）
- サポートされるユーザのロール（P.10-14）
- フィールド定義（P.10-14）
- 統計情報の表示（P.10-15）

概要

Statistics パネルには、次のカテゴリの統計情報が表示されます。

- 分析エンジン
- イベント サーバ
- イベント ストア
- ホスト
- インターフェイスのコンフィギュレーション
- ロガー
- Attack Response Controller（以前は Network Access Controller と呼ばれていました）
- 通知
- トランザクション サーバ
- トランザクション ソース
- 仮想センサー
- Web サーバ

サポートされるユーザのロール

管理者、オペレータ、およびビューアがシステムの統計情報を表示できます。

フィールド定義

Statistics パネルには次のボタンがあります。

ボタンの機能：

- **Refresh**：Web サーバ、トランザクション ソース、トランザクション サーバ、Network Access Controller（IPS 5.1 では Attack Response Controller と呼ばれていますが、統計情報では引き続き Network Access Controller として示されています。）、Logger、ホスト、イベント ストア、イベント サーバ、分析エンジン、インターフェイスのコンフィギュレーション、および認証を含め、センサー アプリケーションに関する最新の情報を表示します。

統計情報の表示

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　**Monitoring** > **Support Information** > **Statistics** の順に選択します。

Statistics ページが表示されます。

ステップ 2　統計情報が変化した場合にそれらを更新するには、**Refresh** をクリックします。

システム情報の表示

この項では、システム情報を表示する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.10-16）
- サポートされるユーザのロール（P.10-16）
- フィールド定義（P.10-16）
- システム情報の表示（P.10-16）

概要

System Information ページには、次の情報が表示されます。

- TAC 接続情報
- センサーの稼働時間
- センサーのタイプ
- ソフトウェア バージョン
- アプリケーションの状態
- インストールされているアップグレード
- PEP 情報
- メモリの使用状況
- ディスクの使用状況

サポートされるユーザのロール

システム情報を表示するには、管理者またはオペレータである必要があります。ビューアは、センサーの稼働時間とディスクの使用状況を除くすべてのシステム情報を表示できます。

フィールド定義

System Information パネルには次のボタンがあります。

ボタンの機能：

- **Refresh**：ソフトウェア バージョンや PEP 情報を含む、センサーに関する最新の情報を表示します。

システム情報の表示

システム情報を表示するには、次の手順を実行します。

ステップ 1　**Monitoring** > **Support Information** > **System Information** をクリックします。

System Information パネルに、システムに関する情報が表示されます。

ステップ 2　**Refresh** をクリックします。

パネルがリフレッシュされ、新しい情報が表示されます。

センサーの監視

この章では、拒否された攻撃者リストを監視およびクリアする方法、アクティブなホスト ブロックとネットワーク ブロックを監視および設定する方法、レート制限を設定および管理する方法、IP ログを設定およびダウンロードする方法について説明します。

この章は、次の項で構成されています。

- 拒否された攻撃者（P.11-2）
- アクティブなホスト ブロックの設定および管理（P.11-4）
- ネットワーク ブロックの設定および管理（P.11-8）
- レート制限の設定および管理（P.11-11）
- IP ロギングの設定（P.11-15）

拒否された攻撃者

この項では、拒否された攻撃者を設定する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.11-2）
- サポートされるユーザのロール（P.11-2）
- フィールド定義（P.11-2）
- 拒否された攻撃者リストの監視（P.11-3）

概要

Denied Attackers パネルに、拒否された攻撃者のすべての IP アドレスとヒット カウントが表示されます。すべての IP アドレスのヒット カウントをリセットしたり、拒否された攻撃者のリストをクリアしたりすることができます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

拒否された攻撃者のリストを監視およびクリアするには、管理者である必要があります。

フィールド定義

Denied Attackers パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Attacker IP**：センサーが拒否している攻撃者の IP アドレス。
- **Victim IP**：センサーが拒否している被害先の IP アドレス。
- **Port**：センサーが拒否しているホストのポート。
- **Protocol**：攻撃者が使用しているプロトコル。
- **Percentage**：インライン モードでセンサーによって拒否されるトラフィックの率。
- **Hit Count**：拒否された攻撃者のヒット カウントを表示します。
- **Virtual Sensor**：仮想センサーの名前。現在、IPS 5.1 では 1 つの仮想センサー「vs0」だけをサポートしています。

ボタンの機能：

- **Reset All Hit Counts**：拒否された攻撃者のヒット カウントをクリアします。
- **Clear List**：拒否された攻撃者のリストをクリアします。
- **Refresh**：パネルの内容をリフレッシュします。

拒否された攻撃者リストの監視

拒否された攻撃者のリストとそれらのヒット カウントを表示するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring** > **Denied Attackers** をクリックします。

Denied Attackers パネルが表示されます。

ステップ 3　**Refresh** をクリックして、リストをリフレッシュします。

ステップ 4　**Reset All Hit Counts** をクリックして、ヒット カウントを最初からやり直します。

ステップ 5　**Clear List** をクリックして、拒否された攻撃者のリスト全体をクリアします。

アクティブなホスト ブロックの設定および管理

この項では、アクティブなホスト ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.11-4）
- サポートされるユーザのロール（P.11-4）
- フィールド定義（P.11-4）
- アクティブなホスト ブロックの設定および管理（P.11-6）

概要

Active Host Blocks パネルで、ホストのブロッキングを設定および管理できます。

アクティブなホスト ブロックは、特定のホストからのトラフィックを（そのブロックを削除するまで）永続的にブロックするか、指定された期間ブロックします。宛先 IP アドレスと、宛先のプロトコルおよびポートを指定することにより、接続をベースにしたブロックを実行することもできます。

アクティブなホスト ブロックは、送信元 IP アドレスによって定義されます。既存のブロックと同じ送信元 IP アドレスを持つブロックを追加すると、新しいブロックによって古いブロックが上書きされます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ホスト ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

アクティブなホスト ブロックを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、アクティブなホスト ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Active Host Blocks パネル（P.11-4）
- Add Active Host Block ダイアログボックス（P.11-5）

Active Host Blocks パネル

Active Host Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Destination IP**：ブロックの宛先 IP アドレス。
- **Destination Port**：ブロックの宛先ポート。

- **Protocol**：プロトコルのタイプ（TCP、UDP、または ANY）。
  デフォルトは ANY です。
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **VLAN**：シグニチャを発生させたデータを伝送した VLAN を示します。

注意　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

- **Connection Block Enabled**：ホストへの接続をブロックするかどうか。

ボタンの機能：

- **Add**：Add Active Host Block ダイアログボックスを開きます。
  このダイアログボックスから、ホストの手動ブロックを追加できます。
- **Delete**：アクティブなホスト ブロックのリストから該当の手動ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Active Host Block ダイアログボックス

Add Active Host Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの送信元 IP アドレス。
- **Enable connection blocking**：ホストへの接続をブロックするかどうか。
- **Connection Blocking**：接続ブロッキングのパラメータを設定できます。
  - **Destination IP**：ブロックの宛先 IP アドレス。
  - **Destination Port**：（オプション）ブロックの宛先ポート。
  - **Protocol**：（オプション）プロトコルのタイプ（TCP、UDP、または ANY）。
    デフォルトは ANY です。
- **VLAN**：（オプション）シグニチャを発生させたデータを伝送した VLAN を示します。

注意　ブロック要求に VLAN ID が含まれていても、その ID はファイアウォールに渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降ではブロックを実行できません。

このフィールドはオプションです。

- **Enable Timeout**：ブロックのタイムアウト値（分単位）を設定できます。
- **Timeout**：ブロックを続ける時間（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

アクティブなホスト ブロックの設定および管理

アクティブなホスト ブロックを設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring** > **Active Host Blocks** をクリックします。

Active Host Blocks パネルが表示されます。

ステップ 3　**Add** をクリックして、アクティブなホスト ブロックを追加します。

Add Active Host Block ダイアログボックスが表示されます。

ステップ 4　ブロックするホストの送信元 IP アドレスを入力します。

ステップ 5　ブロックを接続ベースにする場合は、**Enable Connection Blocking** チェックボックスを選択します。

（注）　接続ブロックでは、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がブロックされます。

a. **Destination IP** フィールドに宛先 IP アドレスを入力します。
b. （オプション）**Destination Port** フィールドに宛先ポートを入力します。
c. **Protocol** リストからプロトコルを選択します。

ステップ 6　（オプション）**VLAN** フィールドに、接続ブロックの VLAN を入力します。

ステップ 7　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 8　**Timeout** フィールドに、時間（分単位）を入力します。

ヒント　変更を元に戻して Add Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 9　ブロックに一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

ステップ 10　**Apply** をクリックします。

その IP アドレスにブロックが設定されている場合は、エラー メッセージが発生します。

Active Host Blocks パネルのリストに新しいアクティブなホスト ブロックが表示されます。

ステップ 11 **Refresh** をクリックして、アクティブなホスト ブロックのリストの内容をリフレッシュします。

ステップ 12 ブロックを削除するには、リストでアクティブなホスト ブロックを選択して、**Delete** をクリックします。

Delete Active Host Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

ヒント 変更を元に戻して Delete Active Host Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 13 **Yes** をクリックしてブロックを削除します。

ネットワーク ブロックの設定および管理

この項では、ネットワーク ブロックを管理する方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.11-8）
- サポートされるユーザのロール（P.11-8）
- フィールド定義（P.11-8）
- ネットワーク ブロックの設定および管理（P.11-9）

概要

Network Blocks パネルで、ネットワークのブロッキングを設定および管理できます。

ネットワーク ブロックは、特定のネットワークからのトラフィックを（そのブロックを削除するまで）恒常的にブロックするか、指定された期間ブロックします。

ネットワーク ブロックは、送信元 IP アドレスとネットマスクによって定義されます。ネットマスクは、ブロックされるサブネットを定義します。ホストのサブネット マスクも受け入れられます。

ブロックの期間を指定する場合は、値を 1 ～ 70560 分（49 日）の範囲にする必要があります。時間を指定しない場合、ブロックはセンサーがリブートされるかブロックが削除されるまで有効になります。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ネットワーク ブロックを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、ネットワーク ブロックのフィールドの定義を示します。取り上げる事項は次のとおりです。

- Network Blocks パネル（P.11-8）
- Add Network Block ダイアログボックス（P.11-9）

Network Blocks パネル

Network Blocks パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ブロックの IP アドレス。
- **Mask**：ブロックのネットワーク マスク
- **Minutes Remaining**：ブロックの残り時間（分単位）。
- **Timeout (minutes)**：ブロックのオリジナルのタイムアウト値（分単位）。
  有効な値は 1 ～ 70560 分（49 日）です。

ボタンの機能：

- **Add**：Add Network Block ダイアログボックスを表示します。
  このダイアログボックスから、ネットワークのブロックを追加できます。
- **Delete**：ブロックのリストから該当のネットワーク ブロックを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Network Block ダイアログボックス

Add Network Block ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Source IP**：ブロックの IP アドレス。
- **Netmask**：ブロックのネットワーク マスク。
- **Enable Timeout**：ブロックのタイムアウト値（分単位）を示します。
- **Timeout**：ブロックの期間（分単位）を示します。
  有効な値は 1 ～ 70560 分（49 日）です。
- **No Timeout**：ブロックにタイムアウトを指定しません。

ボタンの機能：

- **Apply**：該当のブロックをすぐにセンサーに送信します。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

ネットワーク ブロックの設定および管理

ネットワーク ブロックを設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring > Network Blocks** をクリックします。

Network Blocks パネルが表示されます。

ステップ 3　**Add** をクリックして、ネットワーク ブロックを追加します。

Add Network Block ダイアログボックスが表示されます。

ステップ 4　ブロックするネットワークの送信元 IP アドレスを入力します。

ステップ 5　**Netmask** リストからネットマスクを選択します。

ステップ 6　ブロックに一定の時間を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 7　**Timeout** フィールドに、時間（分単位）を入力します。

ヒント　変更を元に戻して Add Network Block ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 8　**Apply** をクリックします。

ブロックがすでに追加されている場合は、エラー メッセージが発生します。

Network Blocks パネルのリストに新しいネットワーク ブロックが表示されます。

ステップ 9　**Refresh** をクリックして、ネットワーク ブロックのリストの内容をリフレッシュします。

ステップ 10　ブロックを削除するには、リストでネットワーク ブロックを選択して **Delete** をクリックします。

Delete Network Block ダイアログボックスで、該当のブロックを本当に削除するかどうかをたずねられます。

ステップ 11　**Yes** をクリックしてブロックを削除します。

レート制限の設定および管理

この項では、レート制限とその設定方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.11-11）
- サポートされるユーザのロール（P.11-11）
- フィールド定義（P.11-12）
- レート制限の設定および管理（P.11-13）

概要

レート制限を使用すると、センサーがネットワーク 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します。レート制限の応答は、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 は、Cisco IOS バージョン 12.3 以降を実行するネットワーク デバイスでレート制限を設定することができます。ルータでのレート制限の設定については、P.8-27 の「ルータのブロッキングまたはレート制限のデバイス インターフェイスの設定」を参照してください。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。詳細については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

アクティブなレート制限のリストは、ARC の統計情報で確認できます。詳細については、P.10-14 の「統計情報の表示」を参照してください。

レート制限を追加するには、プロトコル、宛先 IP アドレス、およびレート制限イベントの生成が可能なシグニチャのいずれかに一致するデータ値の組み合せを指定します。手順については、P.11-13 の「レート制限の設定および管理」を参照してください。また、アクションを Request Rate Limit に設定し、さらにこれらのシグニチャの率を設定する必要があります。表 11-1 に、サポートされているシグニチャとパラメータを示します。

表 11-1　レート制限のシグニチャ

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	○	echo-request
2153	ICMP Smurf Attack	ICMP	○	echo-reply
4002	UDP Flood Host	UDP	○	なし
6901	Net Flood ICMP Reply	ICMP	×	echo-reply
6902	Net Flood ICMP Request	ICMP	×	echo-request
6903	Net Flood ICMP Any	ICMP	×	なし
6910	Net Flood UDP	UDP	×	なし
6920	Net Flood TCP	TCP	×	なし
3050	TCP HalfOpenSyn	TCP	×	halfOpenSyn

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

レート制限を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、レート制限のフィールドの定義を示します。取り上げる事項は次のとおりです。

- Rate Limits パネル（P.11-12）
- Add Rate Limit ダイアログボックス（P.11-12）

Rate Limits パネル

Rate Limits パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レートを制限するトラフィックのプロトコル。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
  この率を超えて一致したトラフィックはドロップされます。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Data**：（オプション）特定のプロトコルのトラフィックをさらに正確に限定するために必要な追加の識別情報。
  たとえば、echo-request の場合、ICMP プロトコルのトラフィックはレート制限の ping に絞られます。
- **Minutes Remaining**：該当のレート制限が有効である残り時間（分単位）。
- **Timeout (minutes)**：該当のレート制限の合計時間（分単位）。

ボタンの機能：

- **Add**：Add Rate Limit ダイアログボックスを表示します。
  このダイアログボックスから、レート制限のオプションを設定できます。
- **Delete**：テーブルから該当エントリを削除します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add Rate Limit ダイアログボックス

Add Rate Limit ダイアログボックスには次のフィールドとボタンがあります。

フィールドの説明：

- **Protocol**：レート制限されたトラフィックのプロトコル（ICMP、TCP、または UDP）。
- **Rate**：レート制限されたトラフィックに許可された、帯域幅の最大容量に対する率。
- **Source IP**：（オプション）レート制限されたトラフィックの送信元ホストの IP アドレス。
- **Source Port**：（オプション）レート制限されたトラフィックの送信元ホストのポート。
- **Destination IP**：（オプション）レート制限されたトラフィックの宛先ホストの IP アドレス。
- **Destination Port**：（オプション）レート制限されたトラフィックの宛先ホストのポート。
- **Use Additional Data**：（オプション）echo-reply、echo-request、halfOpenSyn などの追加データを指定するかどうかを選択できます。
- **Timeout**：タイムアウトをイネーブルにするかどうかを選択できます。
  - **No Timeout**：タイムアウトをイネーブルにしません。
  - **Enable Timeout**：タイムアウト（分単位）を指定できます（1 ～ 70560）。

ボタンの機能：

- **Apply**：変更を適用してダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

レート制限の設定および管理

レート制限を設定および管理するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring** > **Rate Limits** をクリックします。

Rate Limits パネルが表示されます。

ステップ 3　**Add** をクリックして、レート制限を追加します。

Add Rate Limit ダイアログボックスが表示されます。

ステップ 4　レートを制限するトラフィックのプロトコル（ICMP、TCP、または UDP）を **Protocol** リストから選択します。

ステップ 5　**Rate** フィールドにレート制限（1 ～ 100）を入力します。

ステップ 6　（オプション）**Destination IP** フィールドに宛先 IP アドレスを入力します。

ステップ 7　レート制限で追加データを使用するように設定する場合は、**Use Additional Data** チェックボックスを選択します。

ステップ 8　**Select Data** リストから、追加データ（echo-reply、echo-request、または halfOpenSyn）を選択します。

ステップ 9　タイムアウト（分単位）を設定する場合は、**Enable Timeout** チェックボックスを選択します。

ステップ 10　**Timeout** フィールドに、時間を分単位で入力します（1 ～ 70560）。

ヒント　変更を元に戻して Add Rate Limit ダイアログボックスを閉じるには、**Cancel** をクリックします。

ステップ 11　レート制限に一定の時間を設定しない場合は、**No Timeout** チェックボックスを選択します。

ステップ 12　**Apply** をクリックします。

Rate Limits パネルのリストに新しいレート制限が表示されます。

ステップ 13　**Refresh** をクリックして、Rate Limits リストの内容をリフレッシュします。

ステップ 14 レート制限を削除するには、リストからレート制限を選択して、**Delete** をクリックします。

Delete Rate Limit ダイアログボックスで、該当のレート制限を本当に削除するかどうかをたずねられます。

ヒント **No** をクリックすると、Delete Rate Limit ダイアログボックスが閉じます。

ステップ 15 **Yes** をクリックしてレート制限を削除します。

該当のレート制限はレート制限のリストに表示されなくなります。

IP ロギングの設定

最も単純な IP ロギングは 1 つの IP アドレスから構成されます。IP アドレスで指定したホストに関連するすべての IP トラフィックを取り込むように、センサーを設定できます。センサーは、この IP アドレスを持つ最初の IP パケットを認識するとすぐに収集を開始し、設定されているパラメータに基づいて収集を継続します。その IP アドレスで IP トラフィックをログに記録する期間を分単位で指定することもできれば、ログに記録するパケット数、またはログに記録するバイト数を指定することもできます。センサーは、指定した最初のパラメータで IP トラフィックのロギングを停止します。

ログ ファイルは次の 3 つの状態のいずれかになります。

- Added：IP ロギングが追加された場合
- Started：センサーが最初のパケットを認識した時点で、ログ ファイルが開き Started 状態になります。
- Completed：IP ロギング制限に達した場合

3 つの状態すべてのファイル数は 20 までに制限されています。IP ログは循環バッファに保存されます。循環バッファでは、新しい IP ログが古い IP ログを上書きするため、いっぱいになることはありません。

(注) ログは、センサーがそれらを再要求するまでセンサー上に残ります。センサー上の IP ログ ファイルを管理することはできません。

IP ログ ファイルを Ethereal や TCP Dump などのスニフィング ツールで表示できるように、それらを FTP サーバまたは SCP サーバにコピーできます。ファイルは、PCAP バイナリ形式で保存され、pcap ファイル拡張子が付きます。

注意 IP ロギングを有効にすると、システム パフォーマンスは低下します。

この項で取り上げる事項は次のとおりです。

- 概要（P.11-15）
- サポートされるユーザのロール（P.11-16）
- フィールド定義（P.11-16）
- IP ロギングの設定（P.11-17）

概要

IP Logging パネルには、このシステムでダウンロードできるすべての IP ログが表示されます。

IP ログは、2 通りの方法で生成されます。

- Add IP Logging ダイアログボックスで IP ログを追加する場合
- シグニチャのイベント アクションとして次のいずれかを選択する場合
  - **Log Attacker Packets**
  - **Log Pair Packets**
  - **Log Victim Packets**

  このシグニチャに基づく攻撃をセンサーが検出したときに、IP ログが作成されます。IP ログをトリガーしたイベント アラートは、IP ロギング テーブルに表示されます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

IP ロギングを設定するには、管理者である必要があります。

フィールド定義

この項では、IP ロギングのフィールドの定義を示します。取り上げる事項は次のとおりです。

- IP Logging パネル（P.11-16）
- Add and Edit IP Logging ダイアログボックス（P.11-17）

IP Logging パネル

IP Logging パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Log ID**：IP ログの ID。
- **IP Address**：ログを取り込むホストの IP アドレス。
- **Status**：IP ログのステータス。
  有効な値は、added、started、または completed です。
- **Event Alert**：ある場合は IP ログをトリガーしたイベント アラート。
- **Start Time**：最初に取り込んだパケットのタイムスタンプ。
- **Current End Time**：最後に取り込んだパケットのタイムスタンプ。
  取り込みが完了していない場合は、タイムスタンプは表示されません。
- **Packets Captured**：現在の取り込んだパケット数。
- **Bytes Captured**：現在の取り込んだバイト数。

ボタンの機能：

- **Add**：Add IP Logging ダイアログボックスを表示します。
  このダイアログボックスで、IP ログを追加できます。
- **Edit**：Edit IP Logging ダイアログボックスを表示します。
  このダイアログボックスで、この IP ログに関連付けられた値を変更できます。
- **Download**：変更を適用し、改訂したコンフィギュレーションを保存します。
- **Stop**：開始した IP ログの取り込みを停止します。
- **Refresh**：テーブルの内容をリフレッシュします。

Add and Edit IP Logging ダイアログボックス

Add and Edit IP Logging ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP Address**：ログを取り込むホストの IP アドレス。
- **Maximum Values**：IP ロギングの値を設定します。
  - **Duration**：パケットを取り込む最長期間。

    (注) Edit IP Logging ダイアログボックスの場合、**Duration** フィールドは、IP ロギングに編集を適用した後に延長された時間です。

    値は 1 ～ 60 分です。デフォルトは 10 分です。
  - **Packets**：（オプション）取り込むパケットの最大数。
    範囲は、1 ～ 4294967295 個のパケットです。
  - **Bytes**：（オプション）取り込む最大バイト数。
    範囲は、0 ～ 4294967295 バイトです。

ボタンの機能：

- **Apply**：変更を適用してダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

IP ロギングの設定

特定のホストの IP トラフィックをログに記録するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Monitoring > IP Logging** をクリックします。

IP Logging パネルが表示されます。

ステップ 3　**Add** をクリックして、IP ロギングを追加します。

Add IP Logging ダイアログボックスが表示されます。

ステップ 4　IP ログの取り込み元となるホストの IP アドレスを入力します。

Added または Started 状態で取り込みが追加されると、エラー メッセージが表示されます。

ステップ 5　**Duration** フィールドに IP ログを取り込む分数を入力します。

ステップ 6　（オプション）**Packets** フィールドに取り込むパケット数を入力します。

ステップ 7　（オプション）**Bytes** フィールドに取り込むバイト数を入力します。

ステップ 8　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

IP Logging パネルのリストに IP ログとログ ID が表示されます。

ステップ 9　リストに既存のエントリを編集するには、それを選択して **Edit** をクリックします。

Edit IP Logging ダイアログボックスが表示されます。

ステップ 10　パケットを取り込む期間を編集します。

ステップ 11　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

IP Logging パネルのリストに編集した IP ログが表示されます。

ステップ 12　IP ロギングを停止するには、停止するログのログ ID を選択し、**Stop** をクリックします。

Stop IP Logging ダイアログボックスが表示されます。

ステップ 13　**OK** をクリックして、そのログの IP ロギングを停止します。

ステップ 14　IP ログをダウンロードするには、ログ ID を選択し、**Download** をクリックします。

Save As ダイアログボックスが表示されます。

ステップ 15　ログをローカル マシンに保存します。保存したログは、Ethereal で表示できます。

ソフトウェアの入手方法

この章では、センサー用の Cisco IPS ソフトウェアの入手方法について説明します。この章は、次の項で構成されています。

- Cisco IPS ソフトウェアの入手方法（P.12-2）
- IPS ソフトウェアのバージョン管理（P.12-4）
- Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード（P.12-7）
- 暗号化アクセスが可能な Cisco.com アカウントの申し込み（P.12-8）
- Cisco.com からのライセンス キーの取得（P.12-9）
- Cisco Intrusion Prevention Alert Center（P.12-14）
- Cisco IPS のアクティブなアップデート通知（P.12-15）
- Network Security Database（P.12-16）
- IPS ドキュメントへのアクセス（P.12-16）

Cisco IPS ソフトウェアの入手方法

メジャー バージョン アップデート、マイナー バージョン アップデート、シグニチャ アップデート、サービス パック 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 Downloads にあります。

（注） Downloads 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。

シグニチャ アップデートは、約 1 週間ごとに Cisco.com に掲示されますが、必要な場合は、さらに頻繁に更新されます。サービス パックも、必要に応じて Cisco.com に用意されます。メジャー バージョン アップデートおよびマイナー バージョン アップデートも定期的に掲示されます。

アップデート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。暗号化アクセス用の Cisco.com アカウントを入手する方法については、P.12-8 の「暗号化アクセスが可能な Cisco.com アカウントの申し込み」を参照してください。

最新の IPS ソフトウェア アップデートがないかどうか、定期的に Cisco.com を確認してください。

（注） 5.x からは、シグニチャ アップデートを適用するためのライセンスが必要になりました。詳細については、P.12-9 の「Cisco.com からのライセンス キーの取得」を参照してください。

Cisco.com の Downloads にアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com に移動します。

ステップ 2　Cisco.com にログインします。

ステップ 3　**Technical Support** > **Downloads** をクリックします。

ステップ 4　Software Products & Downloads の下にある **Cisco Secure Software** をクリックします。

ステップ 5　Cisco Secure Software の下にある **Cisco Intrusion Detection System (IDS)** をクリックします。

ステップ 6　Downloads ページで対象のセンサーを特定し、Version 5.x の下で該当するソフトウェアのリンク（**Latest Service Pack**、**Minor**、**Major Updates** など）をクリックします。

BIOS のアップグレードの場合は、**Firmware** をクリックします。

ステップ 7　Download ページで必要なファイルをクリックします。

Filename、Release、Date、または Size で並べ替えるには、メニューでオプションを選択して **Go** をクリックします。

（注） IPS ファイルのバージョン管理方式の説明については、P.12-4 の「IPS ソフトウェア イメージの命名規則」を参照してください。

ステップ 8　Cisco.com 用のユーザ名とパスワードを再入力する必要があります。

（注） Cisco.com からファイルを初めて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して **Submit** をクリックしない限り、ソフトウェアをダウンロードできません。

ステップ 9　ダウンロードするファイルをクリックします。

ステップ 10　Readme の説明に従って、更新をインストールします。

ソフトウェアのアップグレードが何らかの理由で失敗し、センサーが使用できない状態になった場合は、必要に応じてシステムを復旧します。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

（注） メジャー バージョン アップグレード、マイナー バージョン アップグレード、サービス パック、リカバリ ファイル、およびシグニチャ アップデートは、すべてのセンサーで同一です。システム イメージ ファイルは、プラットフォームごとに用意されます。

IPS ソフトウェアのバージョン管理

この項では、IPS ソフトウェアのバージョン管理について説明します。取り上げる事項は次のとおりです。

- IPS ソフトウェア イメージの命名規則（P.12-4）
- 5.x ソフトウェア リリースの例（P.12-6）

IPS ソフトウェア イメージの命名規則

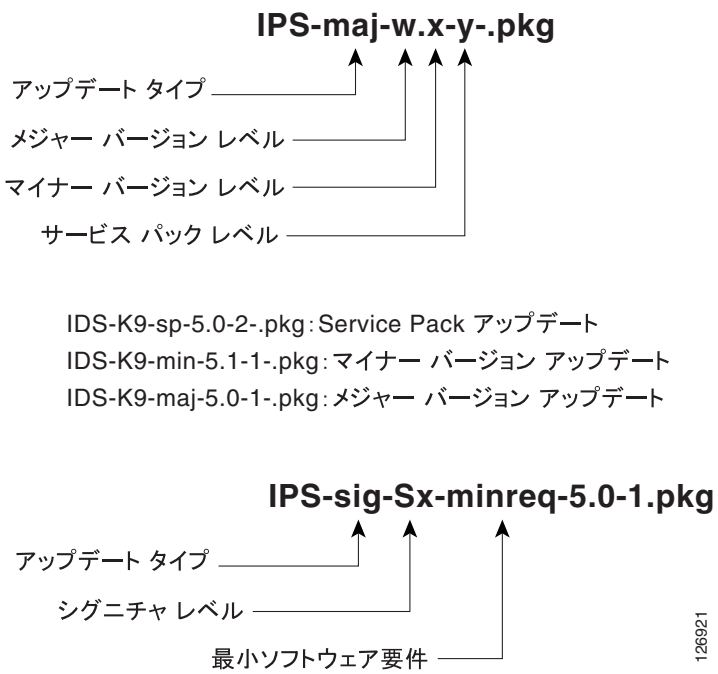
Cisco.com から IPS ソフトウェア イメージをダウンロードするときは、そのバージョン管理方式を理解して、ファイルがそれぞれ、ベース ファイル、累積ファイル、あるいは差分ファイルのどれであるかを知っておく必要があります。

（注）

show version コマンドを使用すると、センサーにインストールされているソフトウェアのバージョンを特定できます。

図 12-1 は、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 12-1　IPS ソフトウェアのファイル名



メジャー バージョン アップグレードには、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、IPS 5.0 ベース バージョン リリースでは、前回のメジャー リリース以降の内容すべて（マイナー バージョンの機能、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）に加えて、新しい変更が組み込まれます。メジャー アップグレード 5.0(1) には、4.1 が必要です。

（注）5.0(1) メジャー アップグレードは、4.1 センサーを 5.0(1) にアップグレードする場合にだけ使用します。5.0(1) がすでにインストールされているセンサーに 5.0(1) を再インストールする場合は、メジャー アップグレードではなくシステム イメージまたはリカバリ手順を使用します。

マイナー バージョン アップグレードは、メジャー バージョンに対する差分です。マイナー バージョン アップグレードは、サービス パックのベース バージョンでもあります。5.0 の最初のマイナー バージョン アップグレードは、5.1(1) です。マイナー バージョン アップグレードは、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 バージョン アップグレードには、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、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。マイナー アップグレードには、メジャー バージョンが必要です。

サービス パックは、ベース バージョンのリリース（マイナーまたはメジャー）の後で、複数のプログラムが累積した形で提供されるものです。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 パックを適用するには、マイナー バージョンが必要です。

シグニチャ アップデートは、新しいリリースにつき 1 つずつ（S145、S146、S147 など）発生する累積および差分です。シグニチャ アップデートには、最初のシグニチャ リリース（S1）以降に発生したすべてのシグニチャに加えて、新しいシグニチャのリリースが組み込まれます。シグニチャ アップデートには、ファイル名にリストされた最小バージョンが必要です。

最新のシグニチャ アップデートをインストールするには、最新のマイナー バージョンが必要です。サービス パックは最新のマイナー バージョンに依存しており、マイナー バージョンは最新のメジャー バージョンに依存しています。

（注）ファイルのタイプ（ファイル名の例）と対応するソフトウェア リリースのリストについては、P.12-6 の「5.x ソフトウェア リリースの例」を参照してください。

この他に、IDS-4215、IPS-4240、IPS-4255、NM-CIDS、IDSM-2、AIP SSM 10、および AIP ASA 20 のシステム イメージ ファイル、すべてのセンサーのリカバリ パーティション ファイル、および IDSM-2 のメンテナンス パーティション ファイルなども存在します。

- システム イメージ ファイル（IDS-4215、IPS-4240、IPS-4255、NM-CIDS、IDSM-2、AIP ASA 10、および AIP ASA 20）：センサー全体のイメージの再作成に使用される IPS の完全なアプリケーションとリカバリのイメージです。
- リカバリ パーティション イメージ ファイル：リカバリ パーティション イメージ ファイルは、リカバリに使用される IPS の完全なアプリケーション イメージが組み込まれたセンサーのパーティションです。
- メンテナンス パーティション イメージ ファイル（IDSM-2 のみ）：IDSM-2 のメンテナンス 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ます。メンテナンス パーティション イメージ ファイルは、新しいバージョン（メジャーまたはマイナー）のメンテナンス パーティションと一緒にリリースされます。メンテナンス パーティション イメージ ファイルは、メンテナンス パーティションのサービス パックの際にはリリースされません。既存のメンテナンス パーティション イメージで特定された障害のフィックスのためにサービス パックがリリースされることはありますが、それ以降にリリースされるサービス パックのために新しいメンテナンス パーティション イメージが作成されることはありません。

（注）　メンテナンス パーティション イメージ ファイルにシグニチャ識別子は含まれていません。

5.x ソフトウェア リリースの例

表 12-1 に、プラットフォームに依存しない IDS 5.x ソフトウェア リリースの例を示します。ファイルの詳細なインストール手順については、ソフトウェア ファイルに添付されている Readme を参照してください。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、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

表 12-1　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	識別子	サポートされているプラットフォーム	ファイル名の例
シグニチャ アップデート[1]	毎週	sig	すべて	IPS-sig-S70-minreq-5.0-1.pkg
サービス パック[2]	半年ごとまたは必要に応じて	sp	すべて	IPS-K9-sp-5.0-2.pkg
マイナー バージョン[3]	毎年	min	すべて	IPS-K9-min-5.1-1.pkg
メジャー バージョン[4]	毎年	maj	すべて	IPS-K9-maj-5.0-1.pkg
パッチ リリース[5]	必要に応じて	patch	すべて	IPS-K9-patch-5.0-1pl.pkg
リカバリ パッケージ[6]	毎年または必要に応じて	r	すべて	IPS-K9-r-1.1-a-5.0-1.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. サービス パックには、障害のフィックスが含まれます。
3. マイナー バージョンには、新しい特性や機能（シグニチャ エンジンなど）が含まれます。
4. メジャー バージョンには、新しい機能やアーキテクチャが含まれます。
5. パッチ リリースは暫定的なフィックスです。
6. 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 5.0(1) 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 12-2 に、プラットフォームに依存するリリースの例を示します。

表 12-2　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	識別子	サポートされてい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	すべて	IPS-4240-K9-sys-1.1-a-5.0-1.img
メンテナンス パーティション イメージ[2]	毎年	mp	IDSM-2 のみ	c6svc-mp.2-1-2.bin.gz
リカバリ / アップグレード CD	毎年または必要に応じて	cd	CD-ROM ドライブがあるすべてのアプライアンス	—

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、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。これはプラットフォーム固有のファイルです。IDSM-2 をメンテナンス パーティションから復旧する必要がある場合、復旧処理が完了した後で、適用可能な 5.0 バージョンがアプリケーション パーティションに反映されます。

Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード

（注） IDSM（WS-X6381）を Cisco IDS 5.x にアップグレードすることはできません。IDSM（WS-X6381）は、Version 5.x をサポートしている IDSM-2（WS-SVC-IDSM2-K9）に置き換える必要があります。

5.1 にアップグレードするために最低限必要なバージョンは 5.0 です。5.0 にアップグレードするために最低限必要なバージョンは 4.1(1) です。Cisco 5.0 から 5.1 へのアップグレードおよび Cisco 4.1 から 5.0 へのアップグレードは、Cisco.com からのダウンロードで入手できます。Cisco.com の Downloads にアクセスする手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

5.1 アップグレード ファイルをダウンロードしたら、**upgrade** コマンドを使用して 5.1 アップグレード ファイルをインストールする手順について、添付の Readme を参照してください。または、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading the Sensor」を参照してください。

センサーに Auto Update を設定している場合は、センサーがアップデートの有無をポーリングするサーバ上のディレクトリに 5.1 アップグレード ファイルをコピーします。P.10-2 の「センサーの自動更新」を参照してください。

センサーにアップグレード ファイルをインストールし、リブート後にセンサーが使用できない場合は、センサーのイメージを再作成する必要があります。また、Cisco IDS Version 4.1 より前のバージョンからセンサーをアップグレードするには、**recover** コマンドを使用するか、リカバリ / アップグレード CD を使用する必要があります。

センサーのイメージは、次の方法で再作成できます。

- CD-ROM ドライブがある IDS アプライアンスの場合、リカバリ / アップグレード CD を使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Using the Recovery/Upgrade CD」を参照してください。
- すべてのセンサー の場合、**recover** コマンドを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Recovering the Application Partition」を参照してください。
- IDS-4215、IPS-4240、および IPS 4255 の場合、システム イメージの復元には ROMMON を使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the IDS-4215 System Image」および「Installing the IPS-4240 and IPS-4255 System Image」を参照してください。
- NM-CIDS の場合、ブート ローダーを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the NM-CIDS System Image」を参照してください。
- IDSM-2 の場合、アプリケーション パーティションのイメージは、メンテナンス パーティションからイメージを再作成します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the IDSM-2 System Image」を参照してください。
- AIP SSM の場合、ASA からのイメージの再作成には、**hw-module module 1 recover configure/boot** コマンドを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the ASA-SSM System Image」を参照してください。

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。

暗号化アクセスが可能な Cisco.com アカウントの申し込み

ソフトウェア アップデートをダウンロードするには、暗号化アクセス用の Cisco.com アカウントが必要です。

暗号化アクセスを申し込むには、次の手順を実行します。

ステップ 1　Cisco.com アカウントを持っている場合はステップ 2 に進みます。Cisco.com アカウントを持っていない場合は、次の URL に移動してアカウントを登録します。
http://tools.cisco.com/RPF/register/register.do

ステップ 2　次の URL に移動します。http://www.cisco.com/pcgi-bin/Software/Crypto/crypto_main.pl

Enter Network Password ダイアログボックスが表示されます。

ステップ 3　Cisco.com アカウントでログインします。

Encryption Software Export Distribution Authorization Form ページが表示されます。

ステップ 4　リスト ボックスでソフトウェアを選択して **Submit** をクリックします。

Encryption Software Export Distribution Authorization Form が表示されます。

ステップ 5　Encryption Software Export Distribution Authorization Form を検討し、各項目に入力し、**Submit** をクリックします。

「`Cisco Encryption Software: Crypto Access Granted`」というメッセージが表示されます。

(注)　申し込みの処理には、約 4 時間かかります。受け付け処理が完了するまで、ソフトウェアのダウンロードはできません。完了通知は送信されません。

Cisco.com からのライセンス キーの取得

この項では、Cisco.com からのライセンス キーの取得方法と、CLI または IDM を使用したインストール方法を説明します。取り上げる事項は次のとおりです。

- 概要（P.12-9）
- ライセンスのインストール（P.12-9）

概要

センサーはライセンスなしでも動作しますが、シグニチャ アップデートを取得するには、ライセンスが必要です。ライセンスを入手するには、IPS に関するシスコのサービス契約が必要です。契約を購入するには、代理店、シスコのサービス担当者または営業担当者にお問い合せください。

（注） ライセンスがない場合でも、5.x の最初のいくつかのシグニチャ アップデートをインストールできます。この作業により、センサーのライセンスを入手する時間ができます。契約内容が不明なためにセンサーのライセンスを入手できない場合は、ライセンスが必要なシグニチャ アップデートをサポートしている 60 日のトライアル ライセンスを入手してください。

IPS の登録ライセンス キーのステータスは、IDM の Licensing パネルで確認できます。Cisco.com のライセンシング サーバから取得したライセンス キーは、センサーに送信されます。または、ローカル ファイルに含まれているライセンス キーからセンサーのライセンス キーをアップデートすることもできます。

ライセンス キーの取得には、IPS デバイスのシリアル番号が必要です。IPS デバイスのシリアル番号は、**Configuration > Licensing** をクリックして IDM で確認することができます。また、CLI で **show version** コマンドを実行して確認することもできます。

IDM を起動するたびに、ダイアログボックスによってライセンスのステータスが表示されます。ライセンス キーのステータスは、trial、invalid、または expired のいずれかです。ライセンス キーがない場合や、無効な場合、または期限が切れている場合でも、IDM を継続して使用できますが、シグニチャ アップデートはダウンロードできません。

ライセンスがインストールされていない場合は、CLI に入ると次のメッセージが表示されます。

```
***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.
```

このメッセージは、ライセンスをインストールするまで毎回表示されます。ライセンスを申し込むには、http://www.cisco.com/go/license にアクセスして、IPS Signature Subscription Service をクリックします。

ライセンスのインストール

この項では、IDM または CLI を使用してライセンスをインストールする方法を説明します。取り上げる事項は次のとおりです。

- IDM の使用方法（P.12-10）
- CLI の使用方法（P.12-11）

IDM の使用方法

センサーのライセンス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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Licensing** をクリックします。

Licensing パネルが表示されます。現在のライセンスのステータスに関する情報が表示されます。すでにライセンスがインストールされている場合は、必要に応じて **Download** をクリックしてライセンスを更新します。

ステップ 3　ライセンスを入手する方法を選択します。

a.　Cisco.com からライセンスを取得するには、**Cisco Connection Online** を選択します。

IDM は、Cisco.com のライセンス サーバに接続し、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法です。ステップ 4 に進みます。

b.　ライセンス ファイルを使用するには、**License File** を選択します。

このオプションを使用するには、www.cisco.com/go/license で、ライセンスを申し込む必要があります。

ライセンスは、電子メールで送られてきます。送られてきたライセンスは、IDM がアクセスできるドライブに保存してください。このオプションは、Cisco.com にアクセスできないコンピュータを使用している場合に役立ちます。

ステップ 7 に進みます。

ステップ 4　**Update License** をクリックします。

Licensing ダイアログボックスが表示されます。

ステップ 5　**Yes** をクリックして続行します。

Status ダイアログボックスには、センサーが Cisco.com に接続しようとしていることが示されます。

Information ダイアログボックスによって、ライセンスがアップデートされたことが示されます。

ステップ 6　**OK** をクリックします。

ステップ 7　www.cisco.com/go/license にアクセスします。

ステップ 8　必須フィールドに入力します。

注意　IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

シスコの IPS Signature Subscription Service のライセンス 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。

ステップ 9　ライセンス ファイルは、IDM が動作中のクライアントでアクセス可能なハードディスク ドライブまたはネットワーク ドライブに保存します。

ステップ 10 IDM にログインします。

ステップ 11 **Configuration > Licensing** をクリックします。

ステップ 12 Update License で、**Update From: License File** を選択します。

ステップ 13 **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、または **Browse Local** をクリックしてファイルを参照します。

Select License File Path ダイアログボックスが表示されます。

ステップ 14 ライセンス ファイルを参照して、**Open** をクリックします。

ステップ 15 **Update License** をクリックします。

CLI の使用方法

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

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。URL またはキーワードです。
- *destination-url*：コピー先のファイルの場所。URL またはキーワードです。
- **license-key**：登録ライセンス ファイル。
- *license_file_name*：受け取るライセンス ファイルの名前。

（注） 新しいライセンス キーを上書きするように古いライセンス キーをインストールすることはできません。

コピー元およびコピー先の 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 サーバのコピー元またはコピー先 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 サーバのコピー元またはコピー先 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
- http:：Web サーバのコピー元 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） FTP または SCP を使用する場合は、パスワードの入力を求められます。

（注） SCP を使用する場合は、リモート ホストが SSH の既知ホスト リストに含まれている必要があります。手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

（注） HTTPS を使用する場合、リモート ホストは TLS の信頼できるホストである必要があります。手順については、P.2-17 の「信頼できるホストの追加」を参照してください。

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 で、ライセンス キーを申し込みます。

ステップ 2　必須フィールドに入力します。

（注） IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

シスコの IPS Signature Subscription Service のライセンス 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。

ステップ 3　ライセンス キーを Web サーバ、FTP サーバ、または SCP サーバのあるシステムに保存します。

ステップ 4　管理者特権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　センサーのライセンスがあることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23%
usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_15_03.00   (QATest)    2005-02-15T12:59:35-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


Upgrade History:

    IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

ステップ 7　センサーからサーバにライセンス キーをコピーして、ライセンスのバックアップ コピーを保存します。

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

Cisco Intrusion Prevention Alert Center

Cisco Intrusion Prevention Alert Center を使用すると、発生している脅威に関する情報を表示し、ネットワークを保護するために Cisco ネットワーク IPS シグニチャを使用できます。アクティブな脅威および詳細な情報のリンクのリストが用意されています。また、アクティブなアップデート通知を受信するように登録できます。アクティブなアップデート通知の詳細については、P.12-15 の「Cisco IPS のアクティブなアップデート通知」を参照してください。このサイトから、NSDB を検索することもできます。NSDB の詳細については、P.12-16 の「Network Security Database」を参照してください。

また、役に立つ関連ツールのリンクのリストには、Software Center、Cisco IPS ホームページ、IPS Technical Documentation、Cisco NetPro Forum、および TAC Case Open などが含まれています。

Cisco Intrusion Prevention Alert Center にアクセスするには、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　**Technical Support** > **Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

Cisco IPS のアクティブなアップデート通知

Cisco.com にある Active Update Notifications に加入すると、シグニチャ アップデートおよびサービス パック アップデートがあった場合に電子メールを受け取ることができます。

アップデートに関する通知を受信するには、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　**Technical Support & Documentation** > **Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

ステップ 4　Active Updates で、**Active Update Notifications** をクリックします。

ステップ 5　次のように必要な情報を入力します。

- **a.** IPS Active Update Notifications を受信するかどうかを指定します。メニューから **Yes** または **No** を選択します。
- **b.** **First Name** フィールドに名前を入力します。
- **c.** **Middle Name/Initial** フィールドにミドル ネームまたはそのイニシャルを入力します。
- **d.** **Last Name/Surname** フィールドに姓を入力します。
- **e.** **Organization** フィールドに所属組織名を入力します。
- **f.** メニューから国を選択します。
- **g.** **E-mail** フィールドに電子メール アドレスを入力します。

ステップ 6　シスコの製品やオファリングについての詳細情報を電子メールで受け取ることを希望する場合は、チェックボックスをオンにします。

ステップ 7　メニューから希望する電子メール形式を選択します。

ステップ 8　必要に応じてその他の情報を入力します。

- **a.** メニューから職種を選択します。
- **b.** メニューから役職を選択します。
- **c.** メニューから業種を選択します。
- **d.** メニューから、所属組織の世界全体における従業員数を選択します。
- **e.** メニューから、会社または組織のタイプを選択します。

ステップ 9　**Submit Form** をクリックします。

これで、アップデートが行われたとき、電子メールの通知とアップデート入手方法の説明が送られてくるようになります。

Network Security Database

NSDB は、ネットワークの脆弱性情報の辞書を HTML ベースで示したものです。

通常、NSDB のエントリには次の重要なセキュリティ情報が含まれています。

- Signature Name：シグニチャの名前。
- Signature ID：シグニチャの一意の ID。
- Default Alarm Severity：そのシグニチャのデフォルトのアラーム レベル。
- Release Version：この番号は、そのシグニチャが最初に掲載されたリリースを示します。
- Release Date：シグニチャがリリースされた日付。
- Description：シグニチャと検出する不正利用についての簡潔な説明。
- Benign Trigger(s)：不正利用のように表示されるが、実際は通常のネットワーク アクティビティである任意の「false positives」についての簡潔な説明。
- Recommended Filters：そのシグニチャに推奨するフィルタのリスト。
- Related Threats：各シグニチャには、0 個以上の関連する脅威があります。それぞれの脅威情報のページでは、脅威の背景と利用可能な対抗策のリンクが提供されます。

NSDB にアクセスするには、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　**Technical Support** > **Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

ステップ 4　シグニチャ ID によって並べ替えたシグニチャのリストを表示するには、左側の TOC の **List Signatures by Signature ID** をクリックします。

シグニチャ ID 順のリストが表示されます。

ステップ 5　特定のリリースのシグニチャのリストを表示するには、左側の TOC の **List Signatures by Release** をクリックします。

シグニチャ リリースによってグループ化されたシグニチャのリストが表示されます。

ステップ 6　シグニチャのキーワード、シグニチャ ID、脅威のキーワード、CVE ID、および脅威の重大度で検索を行うには、検索対象のカテゴリを選択し、キーワード、ID、または重大度を入力して、**Go** をクリックします。

条件に一致するシグニチャのリストが表示されます。

IPS ドキュメントへのアクセス

次の URL には、IPS 5.1 のマニュアルが用意されています。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids12/index.htm

システム アーキテクチャ

この付録では、IPS 5.1 のシステム アーキテクチャについて説明します。この章は、次の項で構成されています。

- システムの概要（P.A-2）
- MainApp（P.A-6）
- SensorApp（P.A-24）
- 通信（P.A-33）
- IPS 5.1 ファイル構造（P.A-38）
- IPS 5.1 アプリケーションの要約（P.A-39）

システムの概要

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（最新のアプライアンスとモジュールのリストについては、『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』の「Supported Sensors」を参照してください）。

この項で取り上げる事項は次のとおりです。

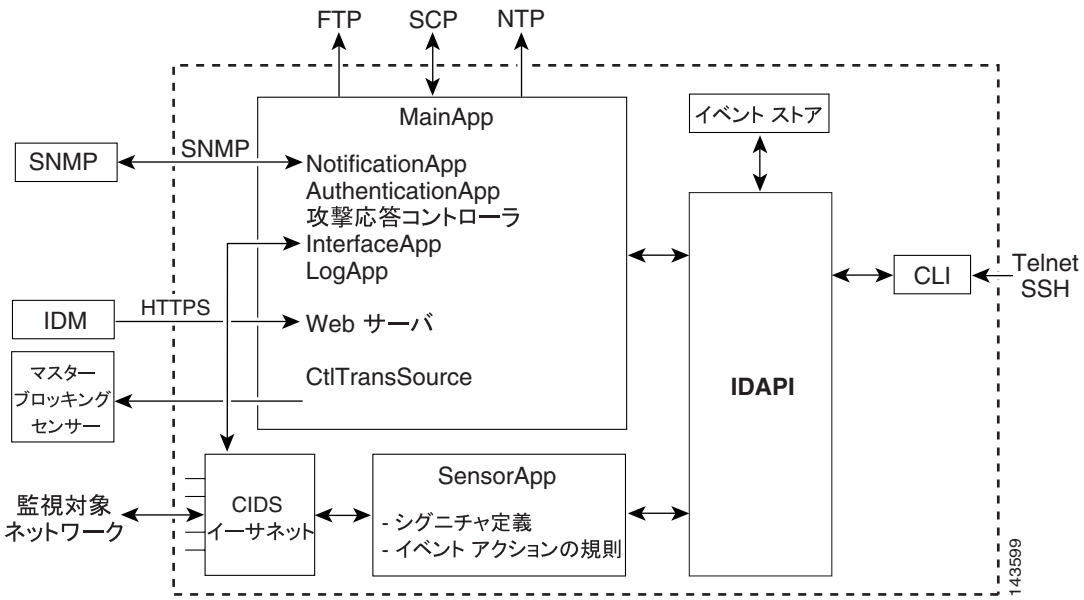
- システムの設計（P.A-2）
- IPS 5.1 の新機能（P.A-4）
- ユーザによる対話操作（P.A-4）
- セキュリティ機能（P.A-5）

システムの設計

IPS ソフトウェアは、Linux オペレーティング システムで動作します。これまで、不必要なパッケージを OS から削除し、使用しないサービスをディセーブルにし、ネットワーク アクセスを制限し、シェルへのアクセスを削除することによって、Linux OS を強化してきました。

図 A-1 は、システムの設計を示しています。

図 A-1　システムの設計



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。

（注）　アプリケーションには XML 形式でそれぞれ独自のコンフィギュレーション ファイルがあります。

- MainApp：システムを初期化し、その他のアプリケーションを開始および停止し、OS を設定して、アップグレードを実行します。これには、次のコンポーネントが含まれています。
  - 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許可します。これは、Attack Response Controller（以前は Network Access Controller と呼ばれていました）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されます。

- Event Store：CLI、IDM、ASDM、または RDEP でアクセスできる 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（エラー、ステータス、およびアラート システム メッセージ）。
- InterfaceApp：バイパス設定と物理設定を処理し、対になったインターフェイスを定義します。物理的な設定は、速度、二重、および管理状態です。
- LogApp：すべてのアプリケーションのログ メッセージをログ ファイルに書き込み、アプリケーションのエラー メッセージをイベント ストアに書き込みます。
- Attack Response Controller（以前は Network Access Controller と呼ばれていました）：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）を管理して、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、制御されたネットワーク デバイスで ACL を作成し適用するか、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る 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、センサーの一般的な健全性に関する情報を提供します。
- Web サーバ（HTTP RDEP2 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、Web インターフェイスおよび通信に RDEP2 を介したその他の IPS デバイスを提供します。
- AuthenticationApp：CLI、IDM、ASDM、または RDEP アクションを実行する許可がユーザにあることを確認します。

- SensorApp (Analysis Engine)：パケットの取り込みと分析を実行します。
- CLI：Telnet または SSH でセンサーに正常にログインしたときに動作してい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がシェルとして CLI を使用します（ただし、サービス アカウントを除きます。許可されるサービス アカウントは 1 つだけです）。許可される CLI コマンドは、ユーザの特権によって異なります。

すべての IPS アプリケーションが、IDAPI と呼ばれる共通 API で互いに通信します。リモート アプリケーション（その他のセンサー、管理アプリケーション、サードパーティ ソフトウェア）は、RDEP2 プロトコルと SDEE プロトコルで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：IDSM-2 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、特別な目的の 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、すべてのコンフィギュレーション設定が失われます。
- 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、特別な目的のイメージ。ブートしてリカバリ パーティションに入ると、アプリケーション パーティションのイメージ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、その他のコンフィギュレーションはすべて失われます。

IPS 5.1 の新機能

Cisco IPS 5.1 には、次の新機能があります。

- Incident Control System（ICS）のサポート

  ICS サービスは、侵入する脅威に対してより迅速に的を絞って対応できるようにすることによって、シスコの現在の IPS シグニチャ サービスを強化します。

- インライン VLAN（on a stick）

  センサーでは、1 つのセンサー インターフェイス上で 1 つまたは複数の VLAN ペア間のインライン センシングを実行できます。スイッチのバックプレーンに直接接続された Cisco Catalyst ラインカード、およびスイッチの外部ポートに接続されたアプライアンスで、この機能を使用することができます。

- レート制限

  レート制限は、ネットワーク デバイスのインターフェイス上で、指定されたタイプのトラフィックの量を帯域幅の最大容量の一定の率までに制限します。この率を超えるトラフィックは、ネットワーク デバイスによってドロップされます。レート制限では、指定されたターゲット ホストへのトラフィック、または設定されたインターフェイスや方向を通過するすべてのトラフィックを制限することができます。レートは、恒常的に、または指定した期間だけ制限することができます。レート制限は、プロトコル、オプションの宛先アドレス、およびオプションのデータ値によって指定されます。

- 新しいイベント アクション

  リリース 5.1 では、2 つの新しい拒否攻撃者イベント アクション、Deny Attacker Service Pair Inline と Deny Attacker Victim Pair Inline が追加されています。レート制限をサポートするために、新しい Request Rate Limit イベント アクションも追加されています。このイベント アクションには、拒否された攻撃者からのトラフィックの率を指定できるパラメータが用意されています。

- GRE/IPV4-in-IPV4 トンネリング

  IPS 5.1 センサーで、GRE および IPV4-in-IPV4 カプセル化トラフィックの監視が可能になりました。

ユーザによる対話操作

ユーザは、次の場合に IPS 5.1 を対話的に操作します。

- デバイスのパラメータ設定

  ユーザは、システムとその機能の初期設定を行います。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。IPS 5.1 は、CLI、IDM、IDS MC、ASDM を使用して設定できるほか、別のアプリケーションで RDEP2 および IDCONF を使用して設定することができます。

- 調整

  ユーザは、主として分析エンジンに対して、わずかなコンフィギュレーションの変更を行います。分析エンジンは、アプリケーションでネットワークのトラフィックを監視する部分です。ネットワークに最初にシステムをインストールした後で、システムが効率的に動作し、有用な情報のみが生成されるようになるまで、何度もシステムを調整することができます。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 パックの適用、およびシグニチャのアップデートが可能です。IPS 5.1 は、CLI、IDM、IDS MC、ASDM を使用して調整できるほか、別のアプリケーションで RDEP2 および IDCONF を使用して調整することができます。

- 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のデータ ファイルにすぐにアップデートを適用することができます。IPS 5.1 は、CLI、IDM、IDS MC、ASDM を使用してアップデートできるほか、別のアプリケーションで RDEP2 および IDCONF を使用してアップデートすることができます。

- 情報の取得

  CLI、IDM、IDS MC、ASDMY を使用して、または、別のアプリケーションで RDEP または RDEP2 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、アラーム）を取得できます。

セキュリティ機能

IPS 5.1 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することができます。
- デフォルトでは、SSH アクセスはイネーブルです。
- FTP サーバはセンサー上では実行されません。SCP を使用すると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することができます。
- 不要なサービスはディセーブルになります。
- 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です。

MainApp

SensorApp と CLI を除くすべての IPS コンポーネントは、MainApp に含まれるようになりました。

この項では、MainApp について説明します。取り上げる事項は次のとおりです。

- MainApp の機能（P.A-6）
- イベント ストア（P.A-7）
- NotificationApp（P.A-9）
- CtlTransSource（P.A-11）
- ARC（P.A-12）
- LogApp（P.A-20）
- AuthenticationApp（P.A-20）
- Web サーバ（P.A-23）

MainApp の機能

MainApp には、次の機能があります。

- シスコでサポートされるハードウェア 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 コンポーネントのバージョンの起動、停止、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とアンインストール
- オペレーティング システムのシャットダウンとリブート

MainApp は、**show version** コマンドに対して、次の情報を表示して応答します。

- センサーのビルドのバージョン
- 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とタイムスタンプ
- 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（IDS-4240 や WS-SVC-IDSM2 など）
- 別のパーティション上に構築されたセンサーのバージョン

また、MainApp はホストの統計情報も収集します。

MainApp の一部となった、イベント ストア、NotificationApp、CtlTransSource、ARC（以前は Network Access Controller と呼ばれていました）、LogApp の各アプリケーションは、イベントの保存、管理、アクション、および通信を担当します。

これらのアプリケーションには、次の新機能が含まれます。

- NotificationApp を使用した SNMP サポート

  SNMP のサポートは、このシステムの管理インターフェイスにとって最も重要な変更です。SNMP の使用により、システムの健全性と稼働状況に関する標準的な情報を入手することができます。シグニチャには、シグニチャが発生すると SNMP トラップが送信されるという新しい SNMP 通知のアクションが加わりました。

  サポートされる SNMP のバージョンは、SNMP バージョン 2 のみです。

- イベントの保存と取得

  新しいエントリ用の空き領域がなくなると、イベント ストアで最も古いエントリの有効期限が切れます。RDEP では、監査データまたは IPS アラート データのみを取得する、各種のクエリーを実行できます。すべての RDEP および RDEP2 SDEE クエリーがサポートされます。すべてのイベントは SDEE CIDEE 形式で保存されます。

- 新しい「健全性」制御トランザクション

  IDCONF の仕様では、健全性と稼働環境に関する新しいタイプの制御トランザクションが定義されています。この制御トランザクションは、システムの状態と稼働状況を報告します。

イベント ストア

この項では、イベント ストアについて説明します。取り上げる事項は次のとおりです。

- イベント ストアについて（P.A-7）
- イベントのデータ構造（P.A-8）
- IPS イベント（P.A-9）

イベント ストアについて

各 IPS イベントは、タイムスタンプおよび一意の単調な昇順 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主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。SensorApp は、イベント ストアにアラート イベントを書き込む唯一のアプリケーションです。すべてのアプリケーションが、ログ、ステータス、およびエラー イベントをイベント 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、優先順位、および限られた数のユーザ定義アトリビュートに基づいて、単純なイベント クエリーを実行できます。各イベントに、low、medium、または high の優先順位が割り当てられている場合は、1 つのイベント クエリーで、目的のイベント タイプ、侵入イベントの優先順位、および時間範囲を指定できます。

表 A-1 に、いくつか例を示します。

表 A-1　IPS イベントの例

IPS イベント タイプ	侵入イベントの優先順位	開始タイムスタンプの値	終了タイムスタンプの値	意味
status	—	0	最大値	保存されているすべてのステータス イベントを取得します。
error status	—	0	65743	時刻 65743 より前に保存されたすべてのエラー イベントおよびステータス イベントを取得します。
status	—	65743	最大値	時刻 65743 以降に保存されたステータス イベントを取得します。
intrusion attack response	low	0	最大値	保存されている、優先順位が low のすべての侵入イベントおよび攻撃対応イベントを取得します。
attack response error status intrusion	medium high	4123000000	4123987256	4123000000 と 4123987256 の間の時刻に保存された、優先順位が medium または high の攻撃対応、エラー、ステータス、侵入の各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場合にも十分なバッファリングが可能な大きさです。十分なバッファリングは、要件および使用されるノードの性能によって異なります。循環バッファ内の最も古いイベントが最新のイベントで置き換えられます。

イベントのデータ構造

各種の機能ユニットは、次の 7 種類のデータを交換します。

- 侵入イベント：SensorApp によって生成されます。センサーは侵入イベントを検出します。
- エラー イベント：ハードウェアまたはソフトウェアの誤作動によって発生します。
- ステータス イベント：コンフィギュレーションが更新された場合など、アプリケーションのステータスの変化を報告します。
- 制御トランザクション ログ イベント：センサーは制御トランザクションの結果をログに記録します。
- 攻撃対応イベント：ARC 用のアクション。ブロック要求などがあります。
- デバッグ イベント：デバッグに使用される、アプリケーションのステータス変化の詳細な報告です。
- 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付けられたデータです。アプリケーションの診断データ、セッション ログ、アプリケーションとの間でやりとりされるコンフィギュレーション データなどがあります。

この全 7 種類のデータは、集合的に *IPS データ*と呼ばれます。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、デバッグの 6 つのイベント タイプは、類似した特性を持ち、集合的に *IPS イベント*と呼ばれます。IPS イベントは、IPS を構成する複数の異なるアプリケーションによって生成され、他の IPS アプリケーションはこれらのイベントに登録しています。IPS イベントには、次の特性があります。

- イベントを発生させるように設定されたアプリケーション　インスタンスから自然発生的に生成されます。別のアプリケーション インスタンスから特定のイベントを生成するように要求があるわけではありません。
- 特定の宛先を持ちません。イベントは保存され、その後 1 つまたは複数のアプリケーション インスタンスによって取得されます。

制御トランザクションには、次のタイプの要求が関係します。

- アプリケーション インスタンスのコンフィギュレーション データの更新要求
- 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のリセット要求
- アプリケーション インスタンスの再起動要求
- ブロック要求など、ARC に対する要求

制御トランザクションには、次の特性があります。

- 常に要求とそれに続く応答で構成されます。

  要求と応答には、任意の量のデータを関連付けることができます。応答には、必ず少なくとも肯定または否定の確認応答が含まれます。
- 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）から別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 文書として、XML 形式で表現されます。ユーザ設定可能なパラメータは、複数の XML ファイルに保存されます。

IPS イベント

IPS アプリケーションは、IPS イベントを生成していくつかの stimulus メッセージの発生を報告します。イベントは、SensorApp によって生成されるアラートや、任意のアプリケーションによって生成されるエラーなどのデータです。イベントは、イベント ストアと呼ばれるローカル データベースに保存されます。

イベントには、次の 5 つのタイプがあります。

- <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ると報告されるアラート 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エラー 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処理された制御トランザクションを報告するログ トランザクション メッセージ。
- <evShunRqst>：ARC がブロック要求を発行すると報告されるブロック要求メッセージ。

ステータス メッセージとエラー メッセージは、CLI、IDM、および ASDM を使用して表示することができます。

SensorApp と ARC は、応答アクション（TCP リセット、IP ロギングの開始と終了、ブロッキングの開始と終了、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 により、センサーは、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することができます。NotificationApp はイベント ストアのイベントに登録し、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 では、センサーの健全性に関する基本情報を取得できます。

希薄モードでは、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
- 要約
- 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> 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、warning）に基づいてフィルタリングすることができます。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一般的な健全性情報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
- パケット拒否数
- 生成されたアラーム数
- FRP 内のフラグメント数
- FRP 内のデータグラム数
- 初期状態の TCP ストリーム数
- 確立状態の TCP ストリーム数
- 終了状態の TCP ストリーム数
- システム内の TCP ストリーム数
- 再構成用にキューイングされた TCP パケット数
- アクティブなノードの合計数
- 両方の IP アドレスと両方のポートでキー付けされた TCP ノード数
- 両方の IP アドレスと両方のポートでキー付けされた UDP ノード数
- 両方の IP アドレスでキー付けされた IP ノード数
- センサー メモリのクリティカルな段階
- インターフェイスのステータス
- コマンド / コントロール パケットの統計情報
- フェールオーバーの状態
- システムの動作時間
- CPU 使用状況
- システムのメモリ使用状況
- PEP

（注）すべての IDS および IPS プラットフォームで PEP がサポートされ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 要求数
- SNMP SET 要求数

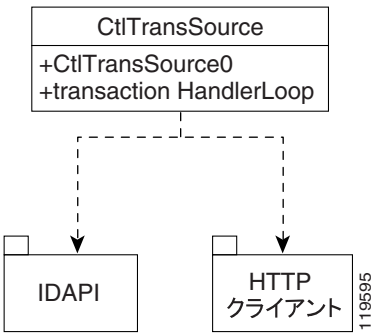
CtlTransSource

CtlTransSource は、ローカルに開始されたリモート制御トランザクションを RDEP および 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、このような接続を介してリモート制御トランザクションが HTTP サーバと通信するようにします。

CtlTransSource は、リモート制御トランザクションを実行するために、リモート HTTP サーバに対して十分なクレデンシャルを確立する必要があります。CtlTransSource は、リモート ノード上の HTTP サーバに対してユーザ名とパスワードの形式（基本認証）で ID を提示することにより、クレデンシャルを確立します。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 Cookie が割り当てられます。

CtlTransSource の transactionHandlerLoop メソッドは、リモート制御トランザクションのプロキシの役割を果たします。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開始すると、IDAPI は最初にそのトランザクションを CtlTransSource に送ります。transactionHandlerLoop メソッドは、CtlTransSource に送られたリモート制御トランザクションを待つループです。図 A-2 は、CtlTransSource の transactionHandlerLoop メソッドを示しています。

図 A-2　CtlTransSource



transactionHandlerLoop は、リモートに対するトランザクションを受け取ると、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しようとします。transactionHandlerLoop は、トランザクションを RDEP 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 RDEP 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、HTTP 応答で適切な RDEP 応答メッセージを返します。リモート HTTP サーバが IPS Web サーバの場合、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、RDEP 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 サーバが未認可のステータス応答（HTTP クライアントの HTTP サーバに対するクレデンシャルが不十分であることを示す）を返すと、transactionHandlerLoop は要求者の ID を認証するために、CtlTransSource の指定されたユーザ名とパスワードを使用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け取るか、終了イベントのシグナルが発生するまでループを続けます。

ARC

この項では、ARC について説明します。ARC は、ルータ、スイッチ、およびファイアウォールでブロッキングを開始および終了する IPS アプリケーションです。*ブロック*は、デバイスのコンフィギュレーションまたは ACL 内で、特定のホスト IP アドレスまたはネットワーク アドレスの着信および発信トラフィックをブロックするエントリです。また、ARC は Cisco IOS 12.3 を実行するルータでレート制限の制御も実行します。

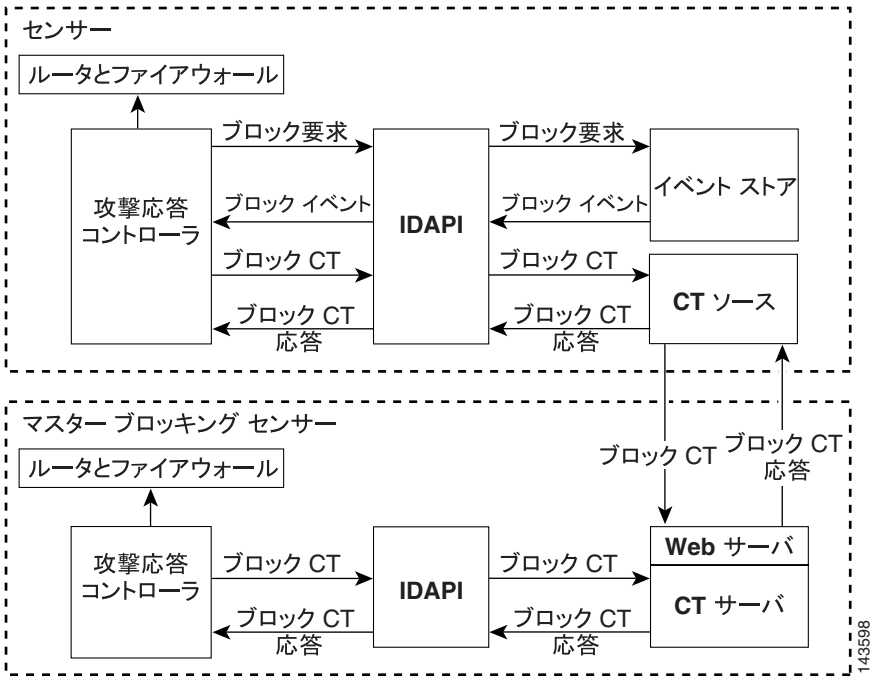
この項で取り上げる事項は次のとおりです。

- 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-16）
- 再起動前後の状態の維持（P.A-16）
- 接続ベースおよび無条件のブロッキング（P.A-17）
- Cisco ファイアウォールでのブロッキング（P.A-18）
- Catalyst スイッチでのブロッキング（P.A-19）

ARC について

ARC の主な機能はイベントをブロックすることです。ブロックに応答する場合、ARC は、管理しているデバイスと直接対話してブロックをイネーブルにするか、制御トランザクション サーバを使用してマスター 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り、制御トランザクション サーバに渡します。その後、トランザクションは ARC に渡されます。マスター ブロッキング センサーの ARC は、その後管理している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 を示しています。

図 A-3　ARC



(注)

1 つの ARC インスタンスは、0 台以上のネットワーク デバイスを制御することができます。ARC は、他の ARC アプリケーション、IPS 管理ソフトウェア、その他のネットワーク管理ソフトウェア、またはシステム管理者とネットワーク デバイスの制御を分担することはありません。特定のセンサー上では、1 つの ARC インスタンスのみの実行が許可されます。

ARC は次のいずれかに応答してブロックを開始します。

- ブロック アクションとともに設定されているシグニチャから生成されたアラート イベント
- CLI、IDM、または ASDM を使用して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 はデバイスと Telnet 接続または SSH 接続を開始します。ARC は、各デバイスとの接続を維持します。ブロックが開始されると、ARC は新しいコンフィギュレーションまたは ACL のセット（インターフェイスの方向ごとに 1 つずつ）を制御対象の各デバイスに配信します。ブロックが完了すると、すべてのコンフィギュレーションまたは ACL が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（デフォルト）または DES 暗号化に対応した Telnet および SSH 1.5 を使用した通信

  該当デバイスの ARC コンフィギュレーション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に失敗すると、ARC は接続を再び確立しようとします。

- 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コンフィギュレーションにマージするように指定することができます。マージは、preblock ACL を指定してすべてのブロックの前で実行するか、postblock ACL を指定してすべてのブロックの後で実行することができます。Catalyst 6000 VACL デバイス タイプでは、ARC が制御するインターフェイスごとに preblock VACL および postblock VACL を指定することができます。ファイアウォール デバイス タイプでは、別の API を使用してブロックが実行されるため、ARC はファイアウォール上の既存の ACL にはまったく影響しません。

  (注) Catalyst 5000 RSM および Catalyst 6000 MSFC2 の各ネットワーク デバイスは、Cisco ルータと同様にサポートされます。

  詳細については、P.A-16 の「ACL と VACL」を参照してください。

- リストに記載されたリモート センサーへのブロックの転送

  ARC は、リストに記載された複数のリモート センサーにブロックを転送して、事実上それらが共同で 1 つのネットワーク デバイスを制御できるように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 センサーと呼びます。マスター ブロッキング センサーの詳細については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

- ネットワーク デバイス上でのブロッキング インターフェイスの指定

  ルータの ARC コンフィギュレーションでは、ブロッキングを実行するインターフェイスと方向を指定できます。VACL のコンフィギュレーションでは、ブロッキングを実行するインターフェイスを指定できます。

  (注) Cisco ファイアウォールでは、インターフェイスや方向に基づいたブロッキングは行われないため、このコンフィギュレーションが指定されることはありません。

  ARC は、最高 250 のインターフェイスを同時に制御できます。

- ホストまたはネットワークの指定された期間のブロッキング

  ARC は、ホストまたはネットワークを指定された期間（分単位）または無限にブロックすることができます。ARC は、ブロックの有効期限が切れるとそれを確認し、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のアクションが正常に完了するか、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リカバリ、コンフィギュレーション エラー、ネットワーク デバイスから報告されたエラーなどの重要なイベントもログに記録します。

- ARC の再起動前後のブロッキング状態の維持

  ARC は、シャットダウンまたは再起動が発生した時点で有効期限が切れていないブロックを再適用します。ARC は、シャットダウン中に有効期限が切れたブロックを削除します。

  (注) ARC は、アプリケーションのシャットダウン中にシステム時間が変更されていない場合にのみ、ブロッキング状態を維持します。

  詳細については、P.A-16 の「再起動前後の状態の維持」を参照してください。

- ネットワーク デバイスの再起動前後のブロッキング状態の維持

  ARC は、ネットワーク デバイスがシャットダウンおよび再起動されると、必要に応じてブロックを再適用し、有効期限が切れたブロックは削除します。ARC は ARC の同時または重複したシャットダウンと再起動の影響を受けません。

- 認証と認可

  ARC は、リモート TACACS+ サーバを使用の使用も含めて、AAA 認証および認可を使用するネットワーク デバイスとの間に通信セッションを確立することができます。

- 2 タイプのブロッキング

  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。

  詳細については、P.A-17 の「接続ベースおよび無条件のブロッキング」を参照してください。

- NAT アドレッシング

  ARC は、センサーに NAT アドレスを使用するネットワーク デバイスを制御することができます。ネットワーク デバイスの設定時に NAT アドレスを指定すると、そのデバイスのブロックからセンサーのアドレスがフィルタリングされるときに、ローカル IP アドレスではなく、その NAT アドレスが使用されます。

- シングル ポイント制御

  ARC は、管理者やその他のソフトウェアとネットワーク デバイスの制御を分担することはありません。コンフィギュレーションを更新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ください。ARC は、CLI または任意の IPS マネージャを使用してイネーブルまたはディセーブルにできます。ARC は、再度イネーブルになると、制御対象の各ネットワーク デバイスの最新コンフィギュレーションの再読み取りも含めて、ARC 自体を完全に再度初期化します。

  (注) ファイアウォールなどのネットワーク デバイスを設定するときには、ARC のブロッキングをディセーブルにすることをお勧めします。

- 任意の時点で最高 250 のアクティブなブロックを維持

  ARC は、同時に最高 250 のアクティブなブロックを維持できます。ARC は最高 65535 のブロックをサポートできますが、同時に許可する数は 250 までにすることをお勧めします。

  (注) ブロックの数は、インターフェイスおよび方向の数と同じではありません。

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 エンジンでスーパーバイザ エンジン ソフトウェア 5.3(1) 以降を実行し、RSM で IOS 11.2(9)P 以降を実行する Catalyst 5000 シリーズ スイッチ

  (注) ブロッキングは RSM で実行されるため、RSM が必要です。

- Catalyst ソフトウェア 5.3 以降を実行する、PFC がインストールされた Catalyst 6000 シリーズ スイッチ
- Catalyst ソフトウェア 5.4(3) 以降がインストールされ、MSFC2 に Cisco IOS 12.1(2)E 以降がインストールされた Catalyst 6000 MSFC2
- Cisco ASA 500 シリーズの、ASA 5510、ASA 5520、ASA 5540 の各モデル
- 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 で制御されるインターフェイスまたは方向でパケットをフィルタリングする場合は、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で ACL を適用する（postblock ACL）ように ARC を設定することができます。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 ACL 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、このリストを取得してキャッシュし、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ときに、ブロッキングを行う ACE とその内容をマージします。ほとんどの場合は、既存の ACL を postblock ACL として指定して、その ACL がブロックの有効な動作を妨げないようにします。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って動作します。この最初の ACE でパケットが許可されると、それより後ろの deny 文は検索されません。

インターフェイスと方向ごとに異なる preblock ACL や postblock ACL を指定したり、同じ ACL を複数のインターフェイスや方向に再利用することができます。preblock リストを維持しない場合は、ブロック対象外オプションを使用し、既存の設定文を使用して常にホストやネットワークをブロックすることができます。永久ブロックは、タイムアウト値が -1 の通常のブロックです。

ARC は、その ARC が所有している ACL のみを変更します。ARC はユーザ定義の ACL は変更しません。ARC によって管理される ACL では特殊な形式が使用されますが、これはユーザ定義の ACL では使用できません。命名規則は、**IPS_**<interface_name>**_[in | out]_[0 | 1]** です。<interface_name> は、ARC のコンフィギュレーションで指定されている、ブロックするインターフェイスの名前です。

Catalyst スイッチの場合は、ブロックするインターフェイスの VLAN 番号になります。これらの名前を preblock ACL や postblock ACL に使用しないでください。

Catalyst 6000 の VACL では、preblock および postblock VACL を指定でき、インターフェイスのみの指定が可能です（VLAN では方向は使用されません）。

ファイアウォールの場合は、ブロッキングに異なる API が使用されるため、preblock ACL と postblock ACL は使用できません。代わりに、ファイアウォールに直接 ACL を作成する必要があります。詳細については、P.A-18 の「Cisco ファイアウォールでのブロッキング」を参照してください。

再起動前後の状態の維持

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 によって管理されるローカル ファイル（nac.shun.txt）に書き込みます。ARC が起動すると、管理対象のネットワーク デバイスでブロックのアップデートが必要かどうかがこのファイルを使用して判断されます。ファイル内に有効期限が切れていないブロックがあれば、起動時にすべてネットワーク デバイスに適用されます。ARC がシャットダウンされるときには、未完了の有効なブロックがあっても ACL に対して特別なアクションは実行されません。nac.shun.txt ファイルが正確であるのは、ARC が実行されていない間にシステム時間が変更されなかった場合のみです。

注意　nac.shun.txt ファイルを手動で変更しないでください。

次のシナリオは、ARC が再起動の前後でどのように状態を維持するかを示しています。

シナリオ 1

ARC の停止時点で 2 つのブロックが有効であり、ARC の再起動前に 1 つの有効期限が切れます。ARC は、再起動すると、最初に nac.shun.txt ファイルを読み取ります。その後、ARC は preblock および postblock の ACL または VACL を読み取ります。アクティブな ACL または VACL が次の順序で作成されます。

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に限られます）
2. preblock ACL
3. コンフィギュレーションからの **always block** コマンド入力
4. nac.shun.txt からの期限が切れていないブロック
5. postblock ACL

ARC のコンフィギュレーションで、特定のホストがブロック対象外として指定されている場合、そのホストは ACL 内の permit 文に入れられません。代わりに、そのホストは ARC によってキャッシュされ、着信する addShunEvent イベントおよび addShunEntry 制御トランザクションのフィルタリングに使用されます。

シナリオ 2

preblock または postblock ACL は指定されていませんが、既存のアクティブな ACL が存在します。新しい ACL は、次の順序で作成されます。

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に限られます）
2. コンフィギュレーションからの **always block** コマンド入力
3. nac.shun.txt からの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、ホストとネットワークで、それぞれ 2 種類と 1 種類のブロッキングをサポートします。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 アトリビュートを確認します。connectionShun が true に設定されている場合、ARC は接続ブロッキングを実行します。ホスト ブロックでは、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコルなどのオプション パラメータを指定できます。接続ブロックを実行するには、少なくとも送信元と宛先の IP アドレスが必要です。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。

次の条件に当てはまる場合、ARC はブロックを強制的に無条件にし、必要に応じてブロックを接続タイプから変換します。

- 指定された送信元 IP アドレスに関して任意のタイプのブロックがアクティブである
- その送信元 IP アドレスに関する任意のタイプの新しいブロックを受け取った

- 新しいブロックは、古いブロックとオプション パラメータ（送信元ポート以外）が異なっている

ブロックが更新される（たとえば、該当の送信元 IP アドレスまたはネットワークに関する既存のブロックがすでに有効であるときに新しいブロックを受け取る）と、既存のブロックの残り時間（分単位）が確認されます。新しいブロックの時間が残り時間（分単位）以下である場合は、アクションは発生しません。そうでない場合は、新しいブロックのタイムアウトで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　Cisco 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のブロックのように扱います。また、Cisco 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 は、Cisco ファイアウォールにネットワーク ブロックを適用しません。

Cisco ファイアウォールでのブロッキング

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キングを実行します。**shun** コマンドの形式は、次のようになっています。

- IP アドレスをブロックする場合

  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場合

  no shun ip

- すべてのブロックをクリアする場合

  clear shun

- アクティブなブロックを表示したり、実際にブロックされたグローバル アドレスを表示する場合

  show shun ［*ip_address*］

ARC は、**show shun** コマンドへの応答を使用して、ブロックが実行されたかどうかを確認します。

shun コマンドは、既存の ACL、コンジット、または outbound コマンドを置き換えないため、既存のファイアウォール コンフィギュレーションをキャッシュしたり、ブロックをファイアウォール コンフィギュレーションにマージする必要はありません。

注意　ARC の実行中は、手動のブロックや、既存のファイアウォール コンフィギュレーションの変更を実行しないでください。

block コマンドで送信元 IP アドレスのみが指定されている場合、既存のアクティブな TCP 接続は切断されませんが、ブロックされたホストからのすべての着信パケットはドロップされます。

ARC が最初に起動すると、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。内部リストに対応するエントリのないブロックはすべて削除されます。

ARC は、ファイアウォール上でローカル ユーザ名または TACACS+ サーバを使用した認証をサポートします。TACACS+ サーバを使用せずに AAA で認証を実行するようにファイアウォールを設定すると、ARC は予約されたユーザ名 *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 TACACS+ サーバを認証に使用する場合は、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 コンフィギュレーションでは、最初のファイアウォール パスワード、AAA パスワード、およびイネーブル パスワードの入力を求める 3 つのプロンプトが表示されます。ARC では、最初のファイアウォール パスワードと AAA パスワードが同じである必要があります。

ファイアウォールが NAT または PAT を使用するように設定され、センサーがファイアウォール外部のネットワークのパケットをチェックしている場合、ファイアウォール内部のネットワークから発信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によって提供される変換された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、ブロックが無効になったり、正常なホストがブロックされる場合があります。PAT アドレッシングを使用している場合は、ファイアウォールで内部ネットワーク全体がブロックされる場合があります。このような状況を避けるためには、センサーを内部インターフェイス上に配置するか、センサーがブロックを実行しないように設定します。

Catalyst スイッチでのブロッキング

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リングします。VACL は、VLAN 間、および VLAN 内でパケットをフィルタリングします。

MSFC ルータの ACL は、WAN カードがインストールされている場合にサポートされ、その場合はセンサーが MSFC2 を介してインターフェイスを制御します。

（注） VACL を使用したブロッキングの場合、MSFC2 カードは Catalyst スイッチのコンフィギュレーションに必須の構成要素ではありません。

注意 Catalyst スイッチ用に 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、次のコマンドが適用されます。

- 既存の VACL を表示する場合
  show security acl info *acl_name*
- アドレスをブロックする場合（*address_spec* は、ルータの ACL で使用されるものと同じ）
  set security acl ip *acl_name* **deny** *address_spec*
- リストの作成後に VACL をアクティブにする場合
  commit security acl all
- 1 つの VACL をクリアする場合
  clear security acl map *acl_name*
- すべての VACL をクリアする場合
  clear security acl map all
- VACL を VLAN にマッピングする場合
  set sec acl *acl_name vlans*

LogApp

センサーは、すべてのイベント（アラート、エラー、ステータス、およびデバッグ メッセージ）のログを、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。メッセージと IP ログには、CLI、IDM、ASDM、および RDEP クライアントを使用してアクセスできます。

IPS アプリケーションは、LogApp を使用してメッセージのログを記録します。LogApp は、debug、timing、warning、error、fatal の 5 つの重大度レベルのログ メッセージをすべて送信します。LogApp は、循環テキスト ファイルである /usr/cids/idsRoot/log/main.log にログ メッセージを書き込みます。ファイルが最大サイズに達すると、新しいメッセージが古いメッセージを上書きするため、最後に書き込まれたメッセージが main.log の最後に表示されるとは限りません。main.log に最後に書き込まれた行を探すには、文字列「= END OF FILE =」を検索します。

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 およびそれ以上（error または fatal）のレベルでログに記録されると、LogApp はそのメッセージを evError イベント（対応するエラー重大度の）に変換し、イベント ストアに挿入します。

（注） テクニカル サポート情報を表示する手順については、P.10-12 の「診断レポートの生成」を参照してください。イベントを表示する手順については、P.7-35 の「イベント表示の設定」を参照してください。

LogApp は、cron メッセージを除いて、informational およびそれ以上のレベルのすべての syslog メッセージを受け取り（*.info;cron.none）、それらをエラー重大度が Warning に設定された <evErrors> としてイベント ストアに挿入します。LogApp およびアプリケーションのロギングは、service logger コマンドで制御されます。

LogApp では、異なるロギング ゾーンの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でどのようなログ メッセージを生成するかを制御することができます。ユーザは、TAC のエンジニアまたは開発者の要請と指示の下でのみ、logger service の個別ゾーン コントロールにアクセスします。TAC は、トラブルシューティングの目的で、ユーザにデバッグ ロギングを有効にするように要請する場合があります。詳細については、P.C-28 の「デバッグ ロギングをイネーブルにする」を参照してください。

AuthenticationApp

この項では、AuthenticationApp について説明します。取り上げる事項は次のとおりです。

- AuthenticationApp の機能（P.A-20）
- ユーザの認証（P.A-21）
- センサーでの認証の設定（P.A-21）
- TLS と SSH の信頼関係の管理（P.A-22）

AuthenticationApp の機能

AuthenticationApp には、次の機能があります。

- ユーザの ID の認証
- ユーザのアカウント、特権、鍵、および証明書の管理
- AuthenticationApp　およびセンサー上のその他のアクセス　サービスで使用される認証方式の設定

ユーザの認証

ユーザのアクセスに関して適切なセキュリティを確立するために、センサーに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、有効期限切れのパスワードを持つ初期の cisco 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つユーザは、CLI、または IDM や ASDM などの IPS マネージャを使用して、このデフォルトの管理アカウント（cisco）を使用してログインすることによってセンサーにアクセスします。CLI では、管理者はパスワードを変更するように求められます。IPS マネージャでは、アカウントのパスワードを変更するために、setEnableAuthenticationTokenStatus 制御トランザクションが開始されます。

管理者は、CLI または IPS マネージャを使用して、使用する認証方式を設定します。たとえば、ユーザ名とパスワードや、SSH 許可鍵の使用です。管理者にサービスを提供するアプリケーションが setAuthenticationConfig 制御トランザクションを開始し、認証のコンフィギュレーションが実行されます。

認証のコンフィギュレーションには、アカウントのロックの処理方法を指定するために使用されるログイン試行回数の制限値なども含まれます。アカウントのロックは、特定のアカウントで連続してログインの試行に失敗した回数がログイン試行の制限値を超えると発生します。アカウントがロックされると、そのアカウントに対するそれ以降のログインの試行は拒否されます。アカウントは、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することによってロック解除されます。ログイン試行の制限値がゼロに設定されている場合、アカウントのロック機能はディセーブルになります。

管理者は、CLI または IPS マネージャを使用して、ユーザ アカウントを追加することができます。詳細については、P.A-29 の「ユーザ ロール」を参照してください。

センサーでの認証の設定

ユーザが Web サーバや CLI などのサービスを使用してセンサーにアクセスしようとする場合は、ユーザの ID が認証され、ユーザの特権が確定される必要があります。ユーザのアクセスを可能にするサービスにより、ユーザの ID を認証するように AuthenticationApp に求める execAuthenticateUser 制御トランザクション要求が開始されます。この制御トランザクション要求には、通常、ユーザ名とパスワードが含まれます。また、ユーザの ID は SSH 許可鍵によっても認証できます。

AuthenticationApp は、ユーザの ID の認証を試行して、execAuthenticateUser 制御トランザクション要求に応答します。AuthenticationApp は、ユーザの認証ステータスと特権を含んだ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、制御トランザクション応答で未認証のステータスと匿名ユーザ特権を返します。また、この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の有効期限が切れてい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してユーザを認証するユーザ インターフェイス アプリケーションによって、パスワードの変更を求めるプロンプトが表示されます。

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制御トランザクションを AuthenticationApp に送信し、AuthenticationApp がオペレーティング システムを使用して応答を作成します。

リモート シェル サービスの Telnet と SSH は、IPS アプリケーションではありません。これらは直接オペレーティング システムを呼び出します。ユーザが認証されると、IPS の CLI が起動されます。この場合、CLI は特別な形式の execAuthenticateUser 制御トランザクションを送信して、ログインしたユーザの特権レベルを確認します。その後、CLI は、この特権レベル基づいて、使用可能にするコマンドを調整します。

TLS と SSH の信頼関係の管理

IP ネットワーク上の暗号化された通信は、受動的攻撃者が交換されているパケットのみからパケット内のデータの復号化に必要な秘密鍵を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。

一方、同じように危険な攻撃として、接続のサーバ エンドを装う偽者に対しても注意を向ける必要があります。すべての暗号化プロトコルは、クライアントがこのような攻撃を防御するための手段を提供しています。IPS は、SSH と TLS の 2 つの暗号化プロトコルをサポートし、センサーが暗号化通信においてクライアントまたはサーバのいずれかとなる場合には、AuthenticationApp が信頼の管理を支援します。

IPS Web サーバと 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、自身の ID を秘密鍵で保護し、接続してくるクライアントに公開鍵を提供します。TLS では、この公開鍵は他の情報とともに X.509 証明書の中に含まれています。センサーに接続する各リモート システムは、接続の確立時に受け取る公開鍵が目的のものであるかどうかを確認する必要があります。

クライアントは、信頼された公開鍵のリストを維持し、man-in-the-middle 攻撃から自身を保護する必要があります。この信頼が確立される過程は、プロトコルとクライアント ソフトウェアによって異なります。一般に、クライアントは 16 または 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オペレータは、信頼を確立しようとする前に、アウトオブバンド方式を使用して、サーバの鍵のフィンガープリントを知る必要があります。このフィンガープリントが一致する場合は、信頼関係が確立され、それ以降クライアントは自動的にそのサーバに接続し、リモート サーバが偽者でないことを確信することができます。

センサーの鍵のフィンガープリントを表示するには、**show ssh server-key** および **show tls fingerprint** を使用することができます。センサーのコンソールに直接接続しているときにこれらのコマンドの出力を記録しておくことにより、後から信頼関係を確立する際、この情報を使用して、ネットワーク上で確実にセンサーの ID を確認することができます。

たとえば、Microsoft Internet Explorer Web ブラウザを使用して初めてセンサーに接続すると、証明書が信頼できないことを示すセキュリティ警告ダイアログボックスが表示されます。Internet Explorer のユーザ インターフェイスを使用すると、証明書のサムプリントを検査できます。サムプリントは、**show tls fingerprint** コマンドによって表示される SHA1 のフィンガープリントと完全に一致する値です。これを確認した後で、この証明書をブラウザの信頼された CA のリストに追加して、永続的な信頼を確立します。

この信頼を確立するための手順は、各 TLS クライアントで異なります。センサー自体にも、他のセンサーに制御トランザクションを送信し、他の TLS Web サーバからアップグレード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ために使用される TLS クライアントが含まれています。センサーが通信する TLS サーバの信頼を確立するには、**tls trusted-host** コマンドを使用します。

同様に、センサーには、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、およびコンフィギュレーション ファイルやサポート ファイルのリモート ホストへのコピーに使用される SSH クライアントも含まれます。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 の trusted certificate と SSH の既知のホストのリストは、**service trusted-certificates** コマンドと **service ssh-known-hosts** コマンドで管理することができます。

X.509 証明書には、信頼関係のセキュリティを強化するその他の情報も含まれていますが、このような情報が混乱につながる場合もあります。たとえば、X.509 証明書には、証明書を信頼できる有効期間が含まれます。一般に、この期間は、証明書が作成された瞬間を起点とした年数です。X.509 証明書が使用されている瞬間に、それが有効であることを確認するためには、クライアント システムが正確なクロックを維持している必要があります。

また、X.509 証明書は、特定のネットワーク アドレスに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 / コントロール インターフェイスの IP アドレスを設定します。したがって、センサーのコマンド / コントロールの 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。ネットワーク上でこの古い証明書を信頼していたすべてのクライアントが新しい IP アドレスでセンサーを探し、新しい証明書を信頼するように、再設定を行う必要があります。

AuthenticationApp で SSH の既知のホストと TLS の trusted certificate の各サービスを使用することにより、センサーをより高いセキュリティ レベルで運用することができます。

Web サーバ

Web サーバは、RDEP2 サポートを提供します。RDEP2 を使用すると、センサーでセキュリティ イベントの報告、IDIOM トランザクションの受信、およびサーバの IP ログの記録が可能になります。

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、多くの場合、パスワードなど、攻撃者に盗聴された場合にシステムのセキュリティを大きく危険にさらすことになる機密情報が伴います。このような理由から、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。

SensorApp

この項では、SensorApp について説明します。取り上げる事項は次のとおりです。

- 機能とコンポーネント（P.A-24）
- パケット フロー（P.A-25）
- SEAP（P.A-26）
- 新機能（P.A-27）

機能とコンポーネント

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、プロセッサのパイプラインを通過します。このパイプラインは、設計者が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します。

SensorApp は次のプロセッサをサポートします。

- Time Processor（TP）

  このプロセッサは、タイムスライス カレンダ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 エントリを廃棄し、時間に依存する統計を計算することです。

- Deny Filters Processor（DFP）

  このプロセッサは、拒否攻撃者機能を処理します。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、仮想センサーのコンフィギュレーション内で設定できます。

- Signature Event Action Processor（SEAP）

  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 パケットの取り込み

  イベント アクションは、イベントの RR 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。

- Statistics Processor（SP）

  このプロセッサは、パケットのカウントやパケットの到達率など、システム統計情報を継続して追跡します。

- Layer 2 Processor（L2P）

  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、異常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、取り込みパケット、拒否パケットなど、形式の正しくないパケットを検出するための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更新します。

- Database Processor（DBP）

  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。

- Fragment Reassembly Processor（FRP）

  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。

- Stream Reassembly Processor（SRP）

  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。正規化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有効または無効にできます。

  TCP SRP の正規化エンジンはホールドダウン 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。ユーザがタイマーを設定することはできません。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、3 ウェイ ハンドシェイクを使用してオープンさ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静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。

- Signature Analysis Processor（SAP）

  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送信します。

- Slave Dispatch Processor（SDP）

  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、シグニチャの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。

また、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、センサーのコンフィギュレーションを処理します。インターフェイスをマップし、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プします。

- 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。

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 SEAP 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。

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が取り出され、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

  TP --> L2P --> DFP --> FRP --> SP --> DBP --> SAP --> SRP --> EAP

- デュアル プロセッサの実行

  実行スレッド 1 TP --> L2P --> DFP --> FRP --> SP --> DBP --> SAP --> SDP --> | 実行スレッド 2 DBP --> SRP --> EAP

SEAP

SEAP は、アラーム チャネル内のシグニチャ イベントから、SEAO、SEAF の処理を経由して SEAH で処理されるまでのデータ フローを調整します。これ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

  Sensor App 検査パスからシグニチャ イベント処理へ向かうシグニチャ イベントと通信するエリアを表す単位。

- シグニチャ イベント アクション オーバーライド（SEAO）

  RR 値に基づいて、アクションを追加します。SEAO は、設定済みの RR しきい値の範囲に該当するすべてのシグニチャに適用されます。各 SEAO 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。詳細については、P.7-2 の「リスク評価の計算」を参照してください。

- シグニチャ イベント アクション フィルタ（SEAF）

  シグニチャ イベントのシグニチャ ID、アドレス、および RR に基づいてアクションを削除します。SEAF へ入力するのは、SEAO 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） SEAF が実行できるのはアクションの削除だけであり、新規アクションの追加はできません。

  SEAF には、次のパラメータが適用されます。

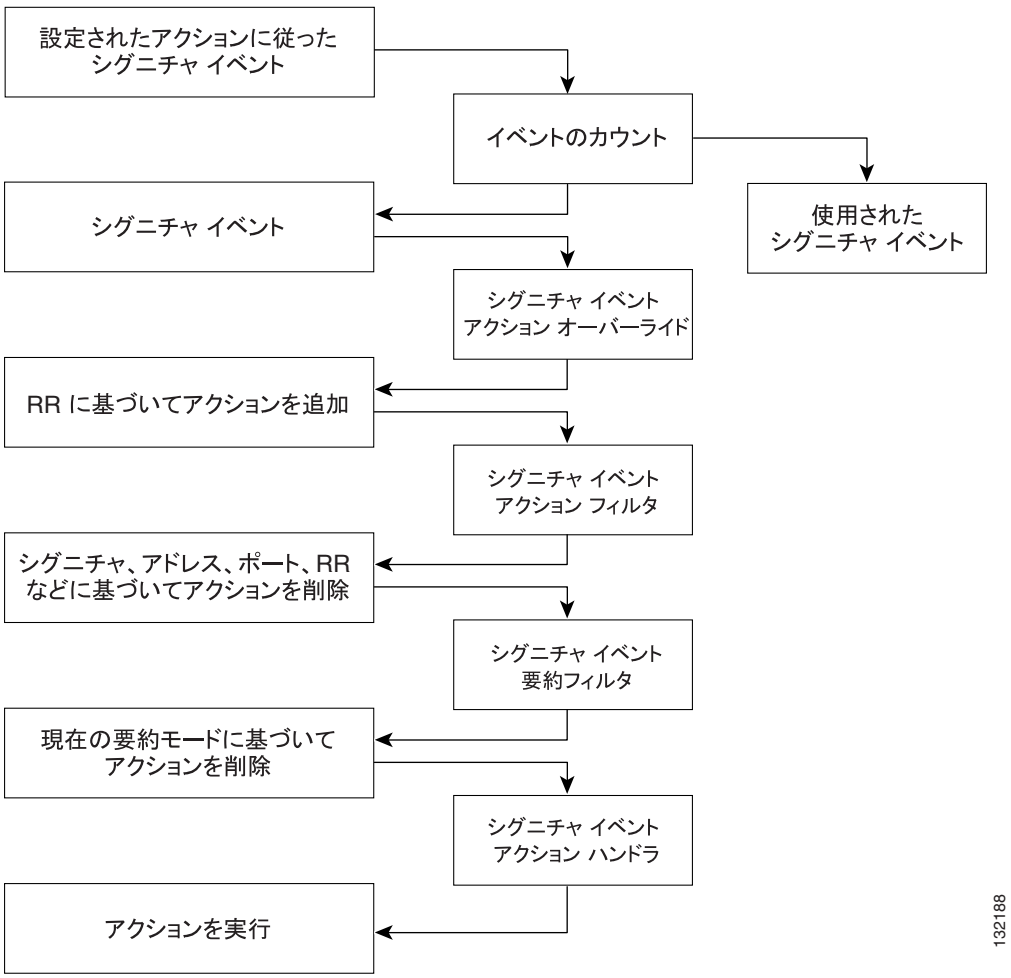
  — シグニチャ ID
  — サブシグニチャ ID
  — 攻撃者のアドレス
  — 攻撃者のポート
  — 被害先のアドレス
  — 被害先のポート
  — RR しきい値の範囲
  — 削除するアクション
  — シーケンス識別子（オプション）
  — ストップ ビットまたは継続ビット
  — アクション フィルタ行をイネーブルにするビット

- シグニチャ イベント アクション ハンドラ（SEAH）

  要求されたアクションを実行します。SEAH 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 は、SEAP を通過するシグニチャ イベントの論理フローと、このイベントのアクションで実行される操作を示しています。これは、アラーム チャネルで受信された設定済みアクションを持つシグニチャ イベントで開始され、シグニチャ イベントが SEAP 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　SEAP を通過するシグニチャ イベント



新機能

SensorApp には、次の新機能が含まれます。

- 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 コンフィギュレーションで明示的に拒否されていないかぎり、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っています。

  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（または混合モード）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。混合モードにおける 802.1q パケットの現在のサポートが、インライン モードまで拡張されます。
- 拡張コンフィギュレーション
- インライン処理でのデータフローのバックアップ

- ホールドダウン タイマー

  SensorApp は、最初に起動したときに、その時点で存在するすべてのフローの状態情報を構築する必要があります。ホールドダウン タイマーは、SensorApp がこの状態情報を構築している間にパケットを拒否しないようにします。ホールドダウン タイマーの期間中も、SensorApp は十分な情報があればポリシーを実施します。

- IP の正規化

  IP データグラムのフラグメンテーションは、意図的であってもなくても不正利用の隠蔽につながり、その検知を困難または不可能にします。フラグメント化は、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することもできます。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メソッドを使用して、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送出したりします。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チェックする必要がある場合、センサーは DoS 攻撃（サービス拒絶攻撃）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 フラグメント化の正規化の装置は、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非表示になることもあります。ポリシーが false positive や false negative 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ません。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 スタックの実装が破損しています。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、正規化エンジン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。

- イベントの RR

  イベントの RR に、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 ホストの全体の価値

  イベントの RR はシステムからの false positive の減少に役立ち、アラーム発生原因のより適切な制御を可能にします。

- イベント アクション フィルタとイベント アクションの処理

  4.*x* のイベント フィルタは、すべてのアクションをフィルタリングしていました。5.*x* のイベント フィルタでは、イベントを個別に処理することができます。アラームの送信もアクションと見なされるようになり、その他のアクションと同様にフィルタリングおよび設定することができます。

- SensorApp と TCPdump による同時取得に対応したドライバ サポート

  データ インターフェイス用ドライバは、SensorApp と TCPdump またはその他の libpcap ベースリーダーによるインターフェイスの同時使用をサポートします。

CLI

CLI は、Telnet、SSH、シリアル インターフェイスなど、ノードへの直接アクセスすべてを提供するセンサーのユーザ インターフェイスです。センサーのアプリケーションは、CLI を使用して設定します。基盤となる OS には、サービス ロールを使用すると直接アクセスできます。

この項で取り上げる事項は次のとおりです。

- ユーザ ロール（P.A-29）
- サービス アカウント（P.A-30）
- CLI の動作（P.A-31）

ユーザ ロール

IPS 5.1 の CLI では、複数ユーザの同時ログインが許可されます。ローカル センサーからユーザを作成および削除することができます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。

CLI は、管理者、オペレータ、ビューア、およびサービスの 4 つのユーザ ロールをサポートします。特権レベルはロールごとに異なるので、メニューや使用できるコマンドもロールによって異なります。

- **管理者**：このユーザ ロールは、最高レベルの特権を持ちます。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。
  - ユーザの追加とパスワードの割り当て
  - 物理インターフェイスおよび仮想センサーの制御のイネーブル化とディセーブル化
  - 仮想センサーへの物理センシング インターフェイスの割り当て
  - 設定または表示エージェントとしてセンサーへ接続することを許可されたホストのリストの変更
  - センサー アドレス コンフィギュレーションの変更
  - シグニチャの調整
  - 仮想センサーへのコンフィギュレーションの割り当て
  - ルータの管理
- **オペレータ**：このユーザ ロールは、2 番目に高いレベルの特権を持ちます。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
  - 仮想センサーへのコンフィギュレーションの割り当て
- **ビューア**：このユーザ　ロールは、最低レベルの特権を持ちます。ビューアは、コンフィギュレーションおよびイベント データの表示と、パスワードの変更を実行できます。

ヒント　アプリケーションのモニタリングでは、センサーに対するビューア アクセス権のみが必要とされます。CLI を使用してビューア特権を持つユーザ アカウントをセットアップし、このアカウントを使用してセンサーに接続するようイベント ビューアを設定することができます。

- **サービス**：このユーザ ロールは、CLI への直接アクセス権を持ちません。サービス アカウントユーザは、バッシュ シェルに直接ログインします。このアカウントは、サポートとトラブルシューティングにのみ使用します。不正な変更はサポートされません。不正に変更が行われた場合、適切な操作を保証するためデバイスのイメージを再作成する必要があります。サービス ロールを持つユーザは 1 人しか作成できません。

  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。サービス アカウントを編集できるのは、管理者特権を持つユーザだけです。

サービス アカウント

サービス アカウントは、TAC が 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直接ログインできるようにする、サポートおよびトラブルシューティング用ツールです。デフォルトでは、このアカウントはセンサー上に存在しません。TAC がセンサーのトラブルシューティングに使用できるように、このアカウントを作成する必要があります。サービス アカウントを作成する手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

サービス アカウントはセンサーごとに 1 つのみ許可されます。また、サービス ロールを許可されるアカウントは 1 つのみです。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。このように設定すると、サービス アカウントのユーザは同じパスワードを使用して root に su することができます。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、コンフィギュレーションに使用することを目的としたものではありません。サービス アカウントでは、TAC の指示の下でセンサーを変更する場合にのみ使用することができます。サービス アカウントを使用したオペテーティング システムへのその他のサービスの追加またはそのようなサービスの実行は、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与えるため、シスコシステムズはこれをサポートしません。TAC は、その他のサービスが追加さ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 アカウントのログインがあるとレコードが更新されます。

（注） IPS 5.1 には、CLI または IDM 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場面でサービス アカウントは不要です。きわめてまれな問題では、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場合があります。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、通常はディセーブルになっている root 特権でセンサーにアクセスすることができます。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お勧めします。サービス アカウントは、不要になったら削除してください。

CLI の動作

IPS CLI を使用する際は、これらのヒントに従ってください。

プロンプト

- CLI コマンドに対して表示されるプロンプトは変更できません。
- システムから質問が表示され、ユーザの入力待ちになる場合は、対話型のプロンプトになります。デフォルト入力はカッコ [ ] 内に表示されます。デフォルト入力を受け入れるには、**Enter** キーを押します。

ヘルプ

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

  次の例では、? の機能を示します。

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

(注)　プロンプトがヘルプの表示から戻ると、前に入力されたコマンドが ? なしで表示されます。

- 不完全なトークンの後に **?** を入力して、コマンドを完成させる有効なトークンを表示することもできます。トークンと ? の間にスペースがある場合は、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ると、コマンドを完成させるために使用できるトークンの選択肢が表示されます（ヘルプの説明なしで）。

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

- 現在のモードで使用できるコマンドだけがヘルプによって表示されます。

タブ補完

- 現在のモードで使用できるコマンドだけがタブ補完およびヘルプによって表示されます。
- コマンドの完全な構文がわからない場合は、コマンドの一部を入力して **Tab** キーを押し、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。

再呼び出し

- あるモードで入力されたコマンドを再呼び出しするには、↑キーまたは↓キーを使用するか、あるいは **Ctrl+P** キーまたは **Ctrl+N** キーを押します。

(注)　ヘルプおよびタブ補完の要求は、再呼び出しリストでは報告されません。

- ブランクのプロンプトは、再呼び出しリストの最後を示します。

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、テキストは入力された大文字と小文字の状態を保ってエコー バックされます。たとえば、次のように入力します。

  ```
  sensor# CONF
  ```

  Tab キーを押すと、次のように表示されます。

  ```
  sensor# CONFigure
  ```

表示オプション

- `–More–` は、ターミナル出力が割り当てられた表示スペースを超えていることを示しています。残りの出力を表示する場合は、**Space** キーを押して出力の次のページを表示するか、**Enter** キーを押して出力を 1 行ずつ表示します。
- 現在の行の内容をクリアしてブランクのコマンドラインに戻るには、**Ctrl+C** キーを押します。

通信

この項では、IPS 5.1 で使用される通信プロトコルについて説明します。取り上げる事項は次のとおりです。

- IDAPI（P.A-33）
- RDEP2（P.A-34）
- IDIOM（P.A-36）
- IDCONF（P.A-36）
- SDEE（P.A-37）
- CIDEE（P.A-37）

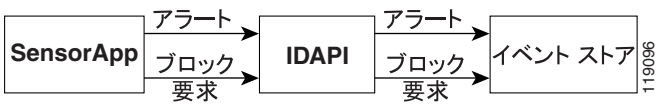
IDAPI

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の通信に使用されるインターフェイスです。

SensorApp は、それ自体のインターフェイス上でネットワーク トラフィックを取得し、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、アラートはイベント ストアに保存されます。ブロッキング応答アクションを実行するようにシグニチャが設定されている場合、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 ストアに保存されます。

図 A-5 は、IDAPI インターフェイスを示しています。

図 A-5　IDAPI



各アプリケーションは、IDAPI に登録してイベントと制御トランザクションを送受信します。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の開始
  - 着信制御トランザクションの待機
  - 制御トランザクションへの応答
- IPS イベント
  - リモート IPS イベント（受信時にイベント ストアに保存される）への登録
  - イベント ストアからの IPS イベントの読み取り
  - イベント ストアへの IPS イベントの書き込み

IDAPI は、アトミックなデータ アクセスを保証するために必要な同期化メカニズムを提供します。

RDEP2

外部通信では、RDEP2 が使用されます。RDEP2 は、IPS クライアントと IPS サーバ間で、IPS イベント、IP ログ、コンフィギュレーション、および制御メッセージの交換に使用される、アプリケーションレベルの通信プロトコルです。RDEP2 の通信は、要求メッセージと応答メッセージで構成されます。RDEP2 クライアントは、RDEP2 サーバに対して要求メッセージを開始します。RDEP2 サーバは、要求メッセージに対して応答メッセージで応答します。

RDEP2 では、イベント、IP ログ、トランザクションの 3 つのクラスの要求 / 応答メッセージが定義されています。イベント メッセージには、IPS アラート、ステータス、エラーの各メッセージがあります。クライアントは、IP ログ要求を使用して、サーバから IP ログ データを取得します。トランザクション メッセージは、IPS サーバの設定と制御に使用されます。

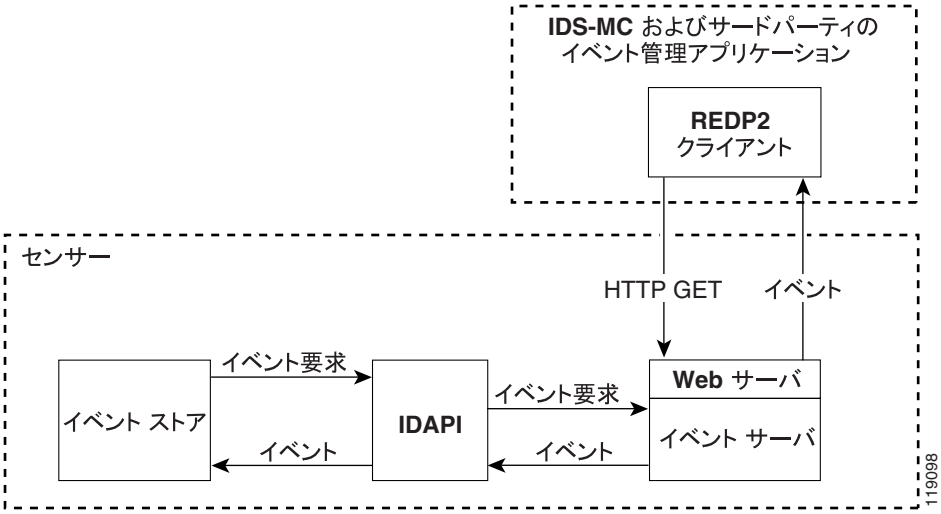
RDEP2 は、業界標準の HTTP、TLS および SSL、および XML を使用して、RDEP2 エージェント間に標準化されたインターフェイスを提供します。RDEP2 プロトコルは HTTP 1.1 プロトコルのサブセットです。すべての RDEP2 メッセージは、有効な HTTP 1.1 メッセージです。RDEP2 は、HTTP のメッセージ形式とメッセージ交換プロトコルを使用して、RDEP2 エージェント間でメッセージを交換します。

ネットワーク経由でセンサーへのアクセスが許可されるホストを指定するには、IPS マネージャを使用します。センサーは、1 ～ 10 の RDEP2 クライアントからの接続を同時に受け入れます。クライアントは、時間範囲、イベントのタイプ（アラート、エラー、またはステータス メッセージ）、およびイベントのレベル（アラートの場合、high、medium、low、informational、エラーの場合、high、medium、low）別に、データを選択して取得します。イベントは、クエリー（1 回のバルク取得）または登録（リアルタイムの永続的な接続）、またはその両方によって取得されます。通信の安全は、TLS または SSL で保護されます。

（注） イベントの取得に関しては、RDEP2 が取得用の新しい標準ですが、センサーは下位互換で、RDEP にも対応します。IPS 5.1 のイベントの取得とコンフィギュレーション変更の送信には、RDEP2 を使用することをお勧めします。

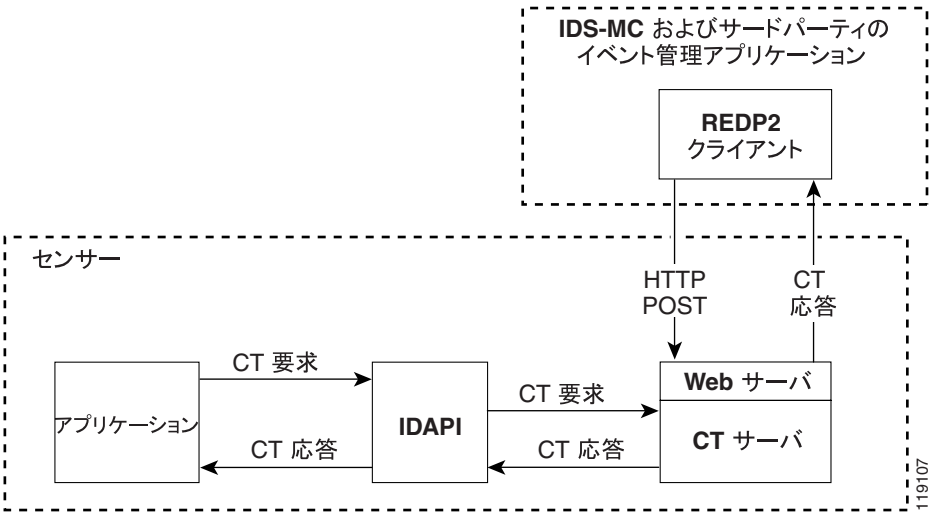
リモート アプリケーションは、RDEP2 を使用してセンサーからイベントを取得します。リモート クライアントが RDEP2 のイベント要求をセンサーの Web サーバに送信すると、Web サーバがそれをイベント サーバに渡します。イベント サーバは、IDAPI を使用してイベント ストアをクエリーし、その結果を返します。図 A-6 は、RDEP2 を通じてセンサーからイベントを取得するリモート アプリケーションを示しています。

図 A-6　RDEP2 を使用したイベントの取得



リモート アプリケーションは、RDEP2 を使用してセンサーにコマンドを送信します。リモート クライアントが RDEP2 の制御トランザクションをセンサーの Web サーバに送信すると、Web サーバがそれを制御トランザクション サーバに渡します。制御トランザクション サーバは、IDAPI を使用して制御トランザクションを適切なアプリケーションに渡し、アプリケーションの応答を待機し、その後、その結果を返します。図 A-7 は、RDEP2 を使用してセンサーにコマンドを送信するアプリケーションを示しています。

図 A-7　RDEP2 を使用したコマンドの送信



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規格です。これらのメッセージは、IDIOM XML スキーマに準拠した XML 文書で構成されます。

IDIOM は、イベントと制御トランザクションの 2 つのタイプのインタラクションをサポートします。イベント インタラクションは、アラートなどの IPS イベントの交換に使用されます。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 メッセージの 2 つのタイプのメッセージを使用します。制御トランザクションは、1 つのホストが別のホストでアクションを開始したり、別のホストの状態の変更や読み取りを実行する手段となります。制御トランザクションでは、要求、応答、コンフィギュレーション、エラーの 4 つのタイプの IDIOM メッセージが使用されます。同じホスト内のアプリケーション間で通信されるイベントと制御トランザクションは、ローカル イベントおよびローカル制御トランザクションと呼ばれ、集合的にローカル IDIOM メッセージと呼ばれます。異なるホスト間で RDEP2 プロトコルを使用して通信されるイベントと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、集合的にリモート IDIOM メッセージと呼ばれます。

(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

IPS 5.1 は、XML 文書を使用して自身のコンフィギュレーションを管理します。IDCONF は、IPS 5.1 の制御トランザクションも含めた XML スキーマを指定します。IDCONF スキーマは、コンフィギュレーション文書の内容を指定するのではなく、コンフィギュレーション文書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。このスキーマは、特定の機能でサポートされるアトリビュート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、RDEP2 によって交換されます。

IDCONF の例を次に示します。

```
<?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、専用の RDEP2 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。また、シスコは、IPS 業界の主要プロトコルである SDEE も開発しました。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規格です。SDEE は、現行バージョンの RDEP2 を強化して、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を追加したものです。

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、イベントを、HTTP プロトコル、または SSL および TLS を介した HTTP プロトコルを使用して転送するように指定できます。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、クライアントの特権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 規格は、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 では、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 の拡張が指定されています。

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すると生成されます。<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 つのメッセージが生成されます。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、監査の目的で役立つ場合があります。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。

CDIEE の拡張イベントの例を次に示します。

```
<sd:events xmlns:cid="http://www.cisco.com/cids/2004/04/cidee"
xmlns:sd="“http://example.org/2003/08/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>
  …
```

IPS 5.1 ファイル構造

IPS 5.1 のディレクトリ構造は次のようになっています。

- /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保存されます。
- /usr/cids/idsRoot/var：センサーの実行中にダイナミックに作成されたファイルが保存されます。
- /usr/cids/idsRoot/var/updates：アップデート インストールのファイルとログが保存されます。
- /usr/cids/idsRoot/var/virtualSensor：SensorApp で正規表現の分析に使用されるファイルが保存されます。
- /usr/cids/idsRoot/var/eventStore：イベント ストア アプリケーションが格納されます。
- /usr/cids/idsRoot/var/core：システムがクラッシュしたときに作成されるコア ファイルが保存されます。
- /usr/cids/idsRoot/var/iplogs：iplog ファイルのデータが保存されます。
- /usr/cids/idsRoot/bin：バイナリ実行可能ファイルが格納されます。
- /usr/cids/idsRoot/bin/authentication：認証アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/cidDump：テクニカル サポート用のデータを収集するスクリプトが格納されます。
- /usr/cids/idsRoot/bin/cidwebserver：Web サーバ アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/cidcli：CLI アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/nac：ARC アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/logApp：ロガー アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/mainApp：メイン アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/sensorApp：センサー アプリケーションが格納されます。
- /usr/cids/idsRoot/bin/falcondump：IDS-4250-XL および IDSM-2 のセンシング ポートでパケット ダンプを取得するためのアプリケーションが格納されます。
- /usr/cids/idsRoot/etc：センサーのコンフィギュレーション ファイルが保存されます。
- /usr/cids/idsRoot/htdocs：Web サーバ用の IDM ファイルが格納されます。
- /usr/cids/idsRoot/lib：センサー アプリケーションのライブラリ ファイルが格納されます。
- /usr/cids/idsRoot/log：デバッグ用ログ ファイルが格納されます。
- /usr/cids/idsRoot/tmp：センサーの実行時に作成される一時ファイルが保存されます。

IPS 5.1 アプリケーションの要約

表 A-2 に、IPS を構成するアプリケーションの要約を示します。

表 A-2　アプリケーションの要約

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、ユーザを認可および認証します。
CLI	コマンドライン入力を受け入れ、IDAPI を使用してローカル コンフィギュレーションを変更します。
イベント サーバ[1]	リモート クライアントからイベントに対する RDEP2 要求を受け入れます。
MainApp	コンフィギュレーションを読み取ってアプリケーションを起動します。また、アプリケーションの起動と停止、ノードのリブート、およびソフトウェア アップグレードを処理します。
InterfaceApp	バイパスと物理的な設定を処理し、ペアのインターフェイスを定義します。物理的な設定は、速度、二重、および管理状態です。
LogApp	アプリケーションのすべてのログ メッセージをログ ファイルに書き込み、エラー メッセージをイベント ストアに書き込みます。
Attack Response Controller	ARC は各センサーで実行されます。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 イベントに登録します。ARC のコンフィギュレーションには、各センサー、およびそのセンサーのローカル ARC で制御されるネットワーク アクセス デバイスのリストが含まれます。マスター ブロッキング センサーにネットワーク アクセス イベントを送信するように設定されている場合、ARC は該当デバイスを制御するリモート ARC に対してネットワーク アクセス制御トランザクションを開始します。また、このようなネットワーク アクセス アクションの制御トランザクションは、IPS マネージャでも随時発生するネットワーク アクセス アクションの発行に使用されます。
NotificationApp	アラート、ステータス、およびエラー イベントによって起動された場合に、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 では、センサーの一般的な健全性情報を取得できます。
SensorApp	監視対象ネットワークのトラフィックを取り込んで分析し、侵入イベントやネットワーク アクセス イベントを生成します。IP ロギング制御トランザクションに応答します。IP ロギング制御トランザクションは、ロギングのオン / オフの切り替えや、IP ログ ファイルの送信と削除を実行します。
制御トランザクション サーバ[2]	リモート RDEP2 クライアントからの制御トランザクションを受入れてローカルの制御トランザクションを開始し、リモート クライアントに応答を返します。
制御トランザクション ソース[3]	リモート アプリケーションに送られる制御トランザクションを待ち、RDEP2 を使用してその制御トランザクションをリモート ノードに転送し、発信側に応答を返します。
IDM	HTML の IPS 管理インターフェイスを提供する Java アプレットです。
Web サーバ	リモート HTTP クライアント要求を待ち、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 Web サーバ サーブレットです。
3. これは、リモート制御トランザクションのプロキシです。

シグニチャ エンジン

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。この章は、次の項で構成されています。

- シグニチャ エンジンについて（P.B-2）
- Master エンジン（P.B-4）
- AIC エンジン（P.B-9）
- Atomic エンジン（P.B-11）
- Flood エンジン（P.B-13）
- Meta エンジン（P.B-14）
- Multi String エンジン（P.B-15）
- Normalizer エンジン（P.B-16）
- Service エンジン（P.B-18）
- State エンジン（P.B-33）
- String エンジン（P.B-35）
- Sweep エンジン（P.B-38）
- Traffic ICMP エンジン（P.B-40）
- Trojan エンジン（P.B-41）

シグニチャ エンジンについて

シグニチャ エンジンは、特定のカテゴリの多数のシグニチャをサポートするように設計された 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から構成されます。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) 5.1 エンジンは、標準化された正規表現をサポートします。

IPS 5.1 には次のシグニチャ エンジンが搭載されています。

- AIC：Web トラフィックの徹底的な分析を行います。

  HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。これは、インスタント メッセージや、gotomypc など、特定のポート上でトンネリングを試行するアプリケーションに対する管理制御を可能にします。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 FTP と AIC HTTP の 2 つの AIC エンジンがあります。

  AIC エンジン シグニチャの設定の詳細については、P.5-28 の「アプリケーション ポリシーの設定」を参照してください。

- Atomic：Atomic エンジンは、現在、2 つのエンジンが組み合され、マルチレベルで選択できます。たとえば、IP + TCP のように、レイヤ 3 およびレイヤ 4 のアトリビュートを組み合せて 1 つのシグニチャを作成できます。Atomic エンジンは標準化された正規表現をサポートします。

  - Atomic IP：IP プロトコル パケットと関連付けられたレイヤ 4 転送プロトコルを検査します。

    このエンジンでは、IP ヘッダーとレイヤ 4 ヘッダー内のフィールドと照合する値を入力し、正規表現を使用してレイヤ 4 ペイロードを検査できます。

    (注) すべての IP パケットが Atomic IP エンジンに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 エンジンに取って代わります。

  - Atomic ARP：レイヤ 2 ARP プロトコルを検査します。ほとんどのエンジンはレイヤ 3 IP に基づいているため、Atomic ARP エンジンはその他の大半のエンジンとは異なっています。

- Flood：ホストおよびネットワークを宛先とする ICMP および UDP フラッドを検出します。

  Flood HOST と Flood NET の 2 つの Flood エンジンがあります。

- Meta：スライドする時間間隔内で、関連する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：複数の文字列を 1 つのシグニチャに対して照合し、レイヤ 4 転送プロトコルと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。

  (注) Multi String エンジンは、IPS 5.1 からの新機能です。

- Normalizer：IP および TCP の正規化エンジンがどのように機能するかを設定し、IP および TCP の正規化エンジンに関連するシグニチャ イベントの設定を行います。RFC に準拠させることができます。

- 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 タイプがあります。
  - 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。
  - GENERIC：カスタム サービスとペイロードをデコードします。
  - H225：VoIP トラフィックを検査します。

    ネットワーク管理者は、VoIP ネットワークに入力された SETUP メッセージが有効であり、ポリシーの規定範囲内であることを確認できます。また、url-ids、email-ids、および表示情報などのアドレス フィールドや Q.931 文字列フィールドが固有の長さであり、考えられる攻撃パターンは含まれていないことを確認できます。
  - HTTP：HTTP トラフィックを検査します。

    WEBPORTS 変数が HTTP トラフィックの検査ポートを定義します。
  - IDENT：IDENT（クライアントとサーバ）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。
  - RPC：RPC トラフィックを検査します。
  - SMB：SMB トラフィックを検査します。
  - 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。
- State：SMTP などのプロトコル内の文字列をステートフル検索を行います。

  State エンジンには現在、非表示の設定ファイルがあります。これは、シグニチャ アップデートで新しい状態定義を配信できるように状態遷移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て正規表現文字列を検索します。

  String ICMP、String TCP、および String UDP の 3 つの String エンジンがあります。
- Sweep：1 つのホスト（ICMP および TCP）、宛先ポート（TCP および 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。
- Traffic ICMP：TFN2K、LOKI、および DDOS など、非標準の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 などの非標準のプロトコルからのトラフィックを分析します。

  Bo2k、Tfn2k、および UDP の 3 つの Trojan エンジンがあります。これらのエンジンには、ユーザ設定可能なパラメータはありません。

Master エンジン

Master エンジンは、その他のエンジンに構造とメソッドを提供し、設定からの入力とアラート出力を処理します。この項では、Master エンジンについて説明します。取り上げる事項は次のとおりです。

- 汎用パラメータ（P.B-4）
- アラートの頻度（P.B-5）
- イベント アクション（P.B-6）

汎用パラメータ

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。

表 B-1 に、Master エンジンの汎用パラメータを示します。

表 B-1　Master エンジンの汎用パラメータ

パラメータ	説明	値
alert-severity	アラートの重大度： • 危険なアラート • 中レベルのアラート • 低レベルのアラート • 情報アラート	high medium low informational
engine	シグニチャが所属するエンジンを指定します。	—
event-counter	イベント カウント設定をグループ化します。	—
event-count	アラートを生成するまでのイベントの発生回数。	1 ～ 65535
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： • 攻撃者のアドレス • 攻撃者アドレスと被害先アドレス • 攻撃者アドレスと被害先ポート • 被害先のアドレス • 攻撃者と被害先のアドレスおよびポート	Axxx AxBx Axxb xxBx AaBb
specify-alert-interval	アラートの間隔をイネーブルにします。	yes | no
alert-interval	イベント カウントをリセットするまでの秒数。	2 ～ 1000
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。	0 ～ 30
sig-fidelity-rating	このシグニチャの忠実度の評価。	0 ～ 100
sig-description	シグニチャの説明をグループ化します。	—
sig-name	シグニチャの名前。	*sig-name*
sig-string-info	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補足情報。	*sig-string-info*
sig-comment	このシグニチャに関するコメント。	sig-comment
alert-traits	このシグニチャについて文書化する特性。	0 ～ 65335
release	シグニチャが最近更新されたリリース。	*release*
status	シグニチャが使用可能か使用不可か、アクティブかリタイア（これ以上使用しない）かどうかを示します。	enabled retired

注意　シグニチャの promisc-delta 設定を変更することはお勧めしません。

混合モードでは、混合デルタは特定のアラートの RR より小さくなります。センサーはターゲット システムのアトリビュートを認識しませんが、混合モードではパケットを拒否できないため、混合アラートの優先順位を（優先順位の低いリスク評価より）低く設定しておくと役立ちます。このように設定すると、管理者は優先順位の高いリスク評価アラートの調査に集中できます。

インライン モードでは、センサーが違反パケットを拒否することができます。その場合、違反パケットがターゲット ホストに到達することはないので、ターゲットが脆弱であっても問題になりません。攻撃はネットワーク上で許されなかったため、リスク評価値は下げません。

サービス、OS、およびアプリケーションに固有のもの以外のシグニチャの混合デルタは 0 です。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ものである場合は、5、10、または 15 の混合デルタがカテゴリごとに 5 つのポイントから計算されます。

アラートの頻度

アラート頻度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 の 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要約が開始されます。

表 B-2 にアラート頻度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	要約に使用するモード。	—
fire-all	すべてのイベントについてアラートを生成します。	—
fire-once	1 回だけアラートを生成します。	—
global-summarize	攻撃者や被害先の数に関係なく 1 回だけアラートが生成されるようにアラートを要約します。	—
summarize	アラートを要約します。	—
specify-summary-threshold	（オプション）サマリーのしきい値をイネーブルにします。	yes | no
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
specify-global-summary-threshold	グローバル サマリーのしきい値をイネーブルにします。	yes | no
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 サマリーに要約されます。	1 ～ 65535
summary-interval	各サマリー アラートを生成する間隔（秒数）。	1 ～ 1000

表 B-2　Master エンジンのアラート頻度パラメータ（続き）

パラメータ	説明	値
summary-key	シグニチャを要約するストレージ タイプ： • 攻撃者のアドレス • 攻撃者アドレスと被害先アドレス • 攻撃者アドレスと被害先ポート • 被害先のアドレス • 攻撃者と被害先のアドレスおよびポート	Axxx AxBx Axxb xxBx AaBb

イベント アクション

次のほとんどのイベント アクションは、特定のエンジンに特化していない限り、各シグニチャに属しています。

表 B-3 は、イベント アクションについて説明しています。

表 B-3　イベント アクション

イベント アクション名	説明
Deny Attacker Inline	（インライン モードのみ）指定された期間、攻撃者アドレスから発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。[1] **（注）** これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。
Deny Attacker Service Pair Inline	（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、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、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。 **（注）** 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。
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 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。

表 B-3　イベント アクション（続き）

イベント アクション名	説明
Log Attacker Packets	攻撃者アドレスを含む IP ロギング パケットを開始します。 (注) このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Log Pair Packets	攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。 (注) このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Log Victim Packets	被害先アドレスを含む IP ロギング パケットを開始します。
Modify Packet Inline	パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。 (注) Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。
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	違反パケットの符号化ダンプをアラートに組み込みます。 (注) このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
Request Block Connection	この接続をブロックする要求を ARC に送信します。 (注) ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
Request Block Host	この攻撃者ホストをブロックする要求を ARC に送信します。 (注) ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 (注) ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

表 B-3　イベント アクション（続き）

イベント アクション名	説明
Request Rate Limit	レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 （注）Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。
Request SNMP Trap	SNMP 通知を実行する要求を NotificationApp に送信します。 （注）このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
Reset TCP Connection	TCP リセットを送信し、TCP フローを乗っ取って終了します。 （注）Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

1. センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

注意　シグニチャに対してアラートをイネーブルにした場合、Produce Alert アクションは自動にはなりません。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。2 番目のアクションを追加する場合、イベント ストアにアラートを送信するには、Produce Alert を組み込む必要があります。また、イベント アクションを設定するたびに、新規リストが作成され、古いリストが置換されます。各シグニチャに必要なイベント アクションを必ずすべて組み込んでください。

AIC エンジン

AIC エンジンは、HTTP Web トラフィックを検査し、FTP コマンドを実行します。この項では、AIC エンジンとそのパラメータについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-9）
- AIC エンジンのパラメータ（P.B-9）

概要

AIC エンジンは、Web トラフィックを詳細に検査するためのシグニチャを定義します。また、FTP コマンドの実行権限を持ちそれを実行するシグニチャも定義します。

AIC HTTP と AIC FTP の 2 つの AIC エンジンがあります。

AIC エンジンには、次の機能があります。

- Web トラフィック：
  - RFC 準拠の実施
  - HTTP 要求メソッドの許可と実施
  - 応答メッセージの検証
  - MIME タイプの指定
  - 転送符号化タイプの検証
  - 転送されるメッセージのコンテンツとデータのタイプに基づくコンテンツ制御
  - URI 長の指定
  - 設定されたポリシーとヘッダーに応じたメッセージ サイズの指定
  - トンネリング、P2P およびインスタント メッセージの実施

    この実施は、正規表現を使用して実行されます。事前定義済みのシグニチャが存在しますが、リストは拡張できます。
- FTP トラフィック：
  - FTP コマンドの許可と実施

AIC エンジンのパラメータ

AIC は Web トラフィックの徹底的な分析を行います。HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。これは、インスタント メッセージや、gotomypc など、特定のポート上でトンネリングを試行するアプリケーションに対する管理制御を可能にします。これらのアプリケーションが HTTP を介して稼働している場合は、P2P およびインスタント メッセージの検査とポリシー チェックを実行できます。

AIC は、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方法を提供します。

事前定義されたシグニチャをイネーブルまたはディセーブルにすることもできますし、カスタム シグニチャでポリシーを作成することもできます。

（注） AIC エンジンは、HTTP トラフィックが AIC Web ポートで受信されたときに実行されます。トラフィックが Web トラフィックであっても、AIC Web ポートで受信されない場合は、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ている任意のポートで実行できます。検査されるトラフィックは HTTP トラフィックです。

AIC エンジン シグニチャの設定の詳細については、P.5-28 の「アプリケーション ポリシーの設定」を参照してください。カスタム AIC シグニチャの例は、P.5-36 の「認識済みの定義コンテンツ タイプ（MIME）シグニチャの例」を参照してください。

表 B-4 は、AIC HTTP エンジンに固有のパラメータを示しています。

表 B-4　AIC HTTP エンジンのパラメータ

パラメータ	説明
signature-type	AIC シグニチャのタイプを指定します。
content-types	MIME タイプを処理する AIC シグニチャ： • define-content-type は、特定の MIME タイプ（image/gif）の拒否、メッセージサイズ違反の定義、ヘッダーと本体に記述された MIME タイプの不一致の判別といったアクションを関連付けます。 • define-recognized-content-types は、センサーが認識したコンテンツ タイプのリストを表示します。
define-web-traffic-policy	非準拠の HTTP トラフィックを検出した場合に実行するアクションを指定します。**alarm-on-non-http-traffic [true | false]** コマンドはシグニチャをイネーブルにします。このシグニチャはデフォルトではディセーブルです。
max-outstanding-requests-overrun	接続あたりの HTTP 要求の許容最大数（1 ～ 16）。
msg-body-pattern	正規表現を使用して、メッセージ本体内の特定のパターンを検索するシグニチャを定義します。
request-methods	アクションを HTTP 要求メソッドに関連付けることのできる AIC シグニチャ： • 取得、挿入などの define-request-method • recognized-request-methods　はセンサーが認識したメソッドのリストを表示します。
transfer-encodings	転送符号化を処理する AIC シグニチャ： • define-transfer-encoding は、圧縮、チャンクなどのアクションを各メソッドに関連付けます。 • recognized-transfer-encodings は、センサーが認識したメソッドのリストを表示します。 • chunked-transfer-encoding-error は、チャンク符号化エラーを検出した場合に実行するアクションを指定します。

表 B-5 は、AIC FTP エンジンに固有のパラメータを示しています。

表 B-5　AIC FTP エンジンのパラメータ

パラメータ	説明
signature-type	AIC シグニチャのタイプを指定します。
ftp-commands	アクションを FTP コマンドに関連付けます。 • ftp-command：検査する FTP コマンドを選択します。
unrecognized-ftp-command	認識されない FTP コマンドを検査します。

Atomic エンジン

Atomic エンジンには、アラートの生成を引き起こす単純な単一のパケットの条件に対応するシグニチャが含まれます。この項では、Atomic エンジンについて説明します。取り上げる事項は次のとおりです。

- Atomic ARP エンジン（P.B-11）
- Atomic IP エンジン（P.B-11）

Atomic ARP エンジン

Atomic ARP エンジンは、基本レイヤ 2 ARP シグニチャを定義し、ARP スプーフィング ツールの dsniff および ettercap の高度な検出も実行します。

表 B-6 は、Atomic ARP エンジンに固有のパラメータを示しています。

表 B-6　Atomic ARP エンジンのパラメータ

パラメータ	説明
specify-mac-flip	この IP アドレスに対して MAC アドレスが指定した回数以上変化した場合にアラームを生成します。
specify-type-of-arp-sig	生成する ARP シグニチャのタイプを指定します。 • Source Broadcast（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ムを生成します。 • Destination Broadcast：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ムを生成します。 • Same Source and Destination：同一の送信元および宛先 MAC アドレスを持つ 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ムを生成します。 • Source Multicast：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ムを生成します。
specify-request-inbalance	IP アドレスに対する応答と比べて、要求が指定した数より多い場合にアラームを生成します。
specify-arp-operation	このシグニチャの ARP 演算コード。

Atomic IP エンジン

Atomic IP エンジンは、IP プロトコル ヘッダー、および関連付けられたレイヤ 4 転送プロトコル（TCP、UDP、および ICMP）とペイロードを検査するシグニチャを定義します。

（注） Atomic エンジンは複数のパケットにまたがって固定データを保存しません。その代わりに、1 つのパケットの解析からアラートを発生できます。

表 B-7 は、Atomic IP エンジンに固有のパラメータを示しています。

表 B-7　Atomic IP エンジンのパラメータ

パラメータ	説明
fragment-status	フラグメント化するかどうかを指定します。
specify-ip-payload-length	IP データグラムのペイロード長を指定します。
specify-ip-header-length	IP データグラムのヘッダー長を指定します。
specify-ip-addr-options	IP アドレスを指定します。
specify-ip-id	IP 識別子を指定します。
specify-ip-total-length	IP データグラムの合計の長さを指定します。
specify-ip-option-inspection	IP オプションの検査を指定します。
specify-l4-protocol	レイヤ 4 プロトコルを指定します。
specify-ip-tos	サーバのタイプを指定します。
specify-ip-ttl	存続可能時間を指定します。
specify-ip-version	IP プロトコルのバージョンを指定します。

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監視するシグニチャを定義します。たとえば、1 秒あたりに（特定タイプの）150 以上のパケットが被害先のホストに送信されていることを検出した場合に生成されるシグニチャを作成できます。

Flood Host と Flood Net の 2 つの Flood エンジンがあります。

表 B-8 は、Flood Host エンジンに固有のパラメータを示しています。

表 B-8　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	秒あたりのパケットのしきい値数。	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 プロトコルを選択した場合の送信元ポートを指定します。	0 ～ 65535[3] a-b[,c-d]

1. 秒あたりのパケットよりもレートが大きくなると、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-9 は、Flood Net エンジン固有のパラメータを示しています。

表 B-9　Flood Net エンジンのパラメータ

パラメータ	説明	値
gap	フラッド シグニチャの許容ギャップ時間（秒単位）。	0 ～ 65535
peaks	フラッド トラフィックの許容ピーク回数。	0 ～ 65535
protocol	検査するトラフィックの種類。	ICMP TCP UDP
rate	秒あたりのパケットのしきい値数。	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. 秒あたりのパケットよりもレートが大きくなると、アラートが起動します。

Meta エンジン

Meta エンジンは、スライドする時間間隔内で、関連する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。シグニチャ イベントが生成されると、Meta エンジンがそれらを検査して、1 つまたはいくつかの Meta 定義と一致するかどうかを判別します。Meta エンジンは、このイベントに対するすべての要件が満たされた後に、シグニチャ イベントを生成します。

シグニチャ イベントはすべて SEAP によって Meta エンジンに渡されます。SEAP は、minimum hits オプションを処理した後で、イベントを渡します。要約とイベント アクションは、Meta 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。SEAP の詳細については、P.7-4 の「Signature Event Action Processor」を参照してください。

注意　多数の Meta シグニチャが、意図せずセンサー パフォーマンス全体に影響を及ぼす可能性があります。

表 B-10 は、Meta エンジンに固有のパラメータを示しています。

表 B-10　Meta エンジンのパラメータ

パラメータ	説明	値
meta-reset-interval	META シグニチャをリセットする時間間隔（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：リストに新しいエントリを挿入します。 　— 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 リストの終わりに配置します。 　— inactive：エントリを非アクティブ リストに入れます。 　— before：エントリを指定したエントリの前に配置します。 　— after：エントリを指定したエントリの後ろに配置します。 • move：リスト内のエントリを移動します。	*name1*
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 • 攻撃者アドレスと被害先アドレス • 攻撃者と被害先のアドレスおよびポート • 被害先のアドレス	AaBb AxBx Axxx xxBx
unique-victim-ports	Meta シグニチャごとに一意の必須被害先ポートの番号。	1 ～ 256
component-list-in-order	コンポーネント リストを順序立てて生成するかどうかを指定します。	true | false

カスタム Meta エンジン シグニチャの例は、P.5-45 の「MEG シグニチャの例」を参照してください。

Multi String エンジン

Multi String エンジンでは、1 つのシグニチャに対して複数の文字列を照合することでレイヤ 4 転送プロトコル（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。シグニチャを生成するために一致している必要の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の方向で実行されます。

1 つ以上の正規表現パターンを指定する必要がある場合に Multi String エンジンを使用します。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、該当するプロトコル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-11 は、Multi String エンジンに固有のパラメータを示しています。

表 B-11　Multi String エンジンのパラメータ

パラメータ	説明	値
inspect-length	生成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のあるストリームまたはパケットの長さ。	0 ～ 4294967295
protocol	レイヤ 4 プロトコル選択。	icmp tcp udp
regex-component	正規表現コンポーネントのリスト： • regex-string：検索文字列。 • spacing-type：前回の一致箇所から、またはそれが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スペーシングのタイプ。	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最小バイト数。	0 ～ 4294967296
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラートメッセージでスワップされる場合は、true。スワップされない場合は 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、source-ports 値が 80 の場合、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。

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。

Normalizer エンジン

Normalizer 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。この項では、Normalizer エンジンについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-16）
- Normalizer エンジンのパラメータ（P.B-17）

概要

Normalizer エンジンは、IP フラグメント再構成および TCP ストリーム再構成を処理します。Normalizer エンジンでは、たとえば、センサーが同時に追跡するフラグメントの最大数など、システム リソースの使用状況に関する制限を設定できます。

（注）　Normalizer エンジンに、カスタム シグニチャを追加することはできません。既存のシグニチャはチューニングできます。

- IP フラグメンテーションの正規化

  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は、不正利用を隠し、それらの検出を困難または不可能にしてしまうことがあります。フラグメント化は、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することもできます。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メソッドを使用して、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送出したりします。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方法をすべてチェックする必要がある場合は、センサーが DoS 攻撃（サービス拒絶攻撃）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 フラグメント化の正規化の装置は、この機能を実行します。

- TCP 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非表示になることもあります。ポリシーが false positive や false negative 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ません。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 スタックの実装が破損しています。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、正規化エンジン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。

混合モードのセンサーは、違反を検出すると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、modify-packet-inline などの event-action パラメータに指定したアクションを実行します。

Normalizer エンジンでシグニチャを設定する手順については、P.5-37 の「IP フラグメント再構成の設定」および P.5-40 の「TCP ストリーム再構成の設定」を参照してください。

Normalizer エンジンのパラメータ

表 B-12 は、Normalizer エンジンに固有のパラメータを示しています。

表 B-12　Normalizer 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	（オプション）フラグメント再構成タイムアウトをイネーブルにします。
specify-hijack-max-old-ack	（オプション）hijack-max-old-ack をイネーブルにします。
specify-max-dgram-size	（オプション）最大データグラム サイズをイネーブルにします。
specify-max-fragments	（オプション）最大フラグメントをイネーブルにします。
specify-max-fragments-per-dgram	（オプション）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	（オプション）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	（オプション）最大部分データグラムをイネーブルにします。
specify-max-small-frags	（オプション）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	（オプション）最小フラグメント サイズをイネーブルにします。
specify-service-ports	（オプション）サービス ポートをイネーブルにします。
specify-syn-flood-max-embryonic	（オプション）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	（オプション）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	（オプション）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	（オプション）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	（オプション）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	（オプション）TCP 最大キューをイネーブルにします。
specify-tcp-min-mss	（オプション）TCP 最小 mss をイネーブルにします。
specify-tcp-option-number	（オプション）TCP オプション番号をイネーブルにします。

Service エンジン

Service エンジンは、2 つのホスト間で L5+ トラフィックを解析します。これらは、固定データを追跡する 1 対 1 シグニチャです。このエンジンは、ライブ サービスに似た方法で L5+ ペイロードを解析します。

Service エンジンには共通の特性があります。ただし、各エンジンには、検査対象のサービスに関する固有の情報があります。Service エンジンは、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、アルゴリズム向けの汎用文字列エンジンの機能を補足します。

この項で取り上げる事項は次のとおりです。

- Service DNS エンジン（P.B-18）
- Service FTP エンジン（P.B-20）
- Service Generic エンジン（P.B-20）
- Service H225 エンジン（P.B-21）
- Service HTTP エンジン（P.B-24）
- Service IDENT エンジン（P.B-26）
- Service MSRPC エンジン（P.B-26）
- Service MSSQL エンジン（P.B-27）
- Service NTP エンジン（P.B-28）
- Service RPC エンジン（P.B-28）
- Service SMB エンジン（P.B-29）
- Service SNMP エンジン（P.B-31）
- Service SSH エンジン（P.B-32）

Service DNS エンジン

Service DNS エンジンは高度な DNS デコード専用です。これには次の複数のジャンプのような反回避技術が含まれています。長さ、命令コード、文字列などの多数のパラメータがあります。Service DNS エンジンは、TCP ポート 53 と UDP ポート 53 の両方で稼働し、2 つのプロトコルに対応するインスペクタです。TCP ではストリーム、UDP ではクワッドが使用されます。

表 B-13 は、Service DNS エンジンに固有のパラメータを示しています。

表 B-13　Service DNS エンジンのパラメータ

パラメータ	説明	値
protocol	インスペクタの対象プロトコル。	TCP UDP
specify-query-chaos-string	（オプション）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*
specify-query-class	（オプション）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	（オプション）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 クエリ長	true | false

表 B-13　Service DNS エンジンのパラメータ（続き）

パラメータ	説明	値
specify-query-jump-count-exceeded	（オプション）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	（オプション）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	（オプション）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	（オプション）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 データ長	0 ～ 65535
specify-query-src-port-53	（オプション）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　パケットの送信元ポート 53	true | false
specify-query-stream-len	（オプション）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	（オプション）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	（オプション）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

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** コマンドと 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、**port** コマンドのデコードで、さまざまなエラー トラップ条件に割り当てられるブール値です。Service FTP エンジンは TCP ポート 20 および 21 で稼働します。ポート 20 はデータ用で、Service FTP エンジンはこのポートを検査しません。ポート 21 の制御トランザクションを検査します。

表 B-14 は、Service FTP エンジンに固有のパラメータを示しています。

表 B-14　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　ポートに向かうトラフィック。 • クライアント　ポートからサービス　ポートに向かうトラフィック。	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 pasv
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	アドレス（およびポート）の送信元と宛先がアラート メッセージでスワップされる場合は、true。スワップされない場合は 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。

Service Generic エンジン

Service Generic エンジンでは、設定ファイルのみのシグニチャ アップデートで、プログラム シグニチャを発行できます。設定ファイルで定義された簡易マシンおよびアセンブリ言語を持っています。仮想マシンを通じて（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 コードで指定された比較および演算を実行します。

これは、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。

（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 Service Generic エンジンのチューニングは、熟練したユーザのみが行ってください。

表 B-15 は、Service Generic エンジンに固有のパラメータを示しています。

表 B-15　Service Generic エンジンのパラメータ

パラメータ	説明	値
specify-dst-port	（オプション）宛先ポートをイネーブルにします。 • dst-port：シグニチャの対象宛先ポート。	0 ～ 65535
specify-ip-protocol	（オプション）IP プロトコルをイネーブルにします。 • ip-protocol：インスペクタが検査する IP プロトコル。	0 ～ 255
specify-payload-source	（オプション）ペイロード送信元の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-data
specify-src-port	（オプション）送信元ポートをイネーブルにします。 • src-port：シグニチャの対象送信元ポート。	0 ～ 65535

Service H225 エンジン

この項では、Service H225 エンジンについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-21）
- Service H255 エンジンのパラメータ（P.B-23）

概要

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から構成されており、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 シグナリングとステータス 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の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 スタックの実装を稼働しています。Service H225 エンジンは、H.255.0 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への攻撃を検出します。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パケットを詳細に検査します。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。このアドレスは、制御プロトコル（H.245）チャネルの確立に使用されます。

SETUP コール シグナリング メッセージは特に重要です。これが、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となるからです。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チェックし、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法です。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 長さシグニチャをチューニングし、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 検証と長さチェック
- Q.931 情報要素の検証
- Q.931 情報要素のテキスト 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 ASN.1 シグニチャの数は固定です。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のみ変更する必要があります。ASN.1 の場合、パラメータは一切変更しないでください。Q.931 シグニチャでは、テキスト フィールドの新しい正規表現シグニチャを追加できます。SETUP シグニチャの場合は、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チェックするためのシグニチャを追加できます。

Service H255 エンジンのパラメータ

表 B-16 は、Service H225 エンジンに固有のパラメータを示しています。

表 B-16　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 • フィールドの検証を検査する • 値を検査する TPKT シグニチャの場合は regex と presence は有効な値ではありません。	length presence regex validate value
specify-field-name	（オプション）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 タイプの場合のみ有効です。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	（オプション）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索引をイネーブルにします。 • invalid-packet-index：無効なパケット索引を検査します。	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。 • 単一の TCP パケット内で検索する正規表現。 • （オプション）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。TPKT シグニチャには設定しないでください。	regex-string specify-min-match-length
specify-value-range	length または value ポリシー タイプの場合に有効です（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

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。

Service HTTP エンジン

この項では、Service HTTP エンジンについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-24）
- Service HTTP エンジンのパラメータ（P.B-24）

概要

Service HTTP エンジンは、サービス固有で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よく使用されているプロトコルです。また、これには最も長い事前処理時間が必要であり、検査を必要とする最大数のシグニチャを持つため、システムのパフォーマンス全体にとって重大となります。

Service HTTP エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現ライブラリを使用します。このエンジンは、Web サービスだけに送られるトラフィック、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。このエンジンの各シグニチャで、該当する個別の Web ポートを指定できます。

HTTP 解読は、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。これは、ASCII 正規化とも呼ばれます。

HTTP パケットを検査するには、まずデータを、ターゲット システムでデータの処理時に表示されるものと同じ表記に解読または正規化する必要があります。どのオペレーティング システムおよび Web サーバ バージョンがターゲットで動作しているかを認識している、カスタマイズされたデコード技術をホスト ターゲット タイプごとに用意することを推奨します。Service HTTP エンジンには、Microsoft IIS Web サーバに対するデフォルトの解読動作があります。

Service HTTP エンジンのパラメータ

Service HTTP のカスタム シグニチャの例は、P.6-34 の「Service HTTP シグニチャの例」を参照してください。

表 B-17 は、Service HTTP エンジンに固有のパラメータを示しています。

表 B-17　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。	true | false
max-field-sizes	最大フィールド サイズ グループ	—
specify-max-arg-field-length	（オプション）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	（オプション）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

表 B-17　Service HTTP エンジンのパラメータ（続き）

パラメータ	説明	値
specify-max-request-length	（オプション）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	（オプション）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	（オプション）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（Content-Length で定義されているとおり、? の後ろのエンティティ本体の中）で検索する正規表現	—
specify-header-regex	（オプション）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-regex：HTTP 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	（オプション）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-regex：HTTP URI および HTTP 引数の両方のフィールド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	（オプション）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
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	アドレス（およびポート）の送信元と宛先がアラート メッセージでスワップされる場合は、true。スワップされない場合は 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。

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を提供します。

表 B-18 は、Service IDENT エンジンに固有のパラメータを示しています。

表 B-18　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-bad-port	不良ポートのペイロードを検査します。	true | false
has-newline	ペイロードの非終端改行文字を検査します。	true | false
size	指定値より長いペイロード長を検査します。	0 ～ 65535
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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	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。

Service MSRPC エンジン

この項では、Service MSRPC エンジンについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-26）
- Service MSRPC エンジンのパラメータ（P.B-27）

概要

Service MSRPC エンジンは、MSRPC パケットを処理します。MSRPC によって、ネットワーク環境内の複数のコンポーネント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、チャネルを確立するために一連の通信が行われ、処理要求と応答が渡されます。

MSRPC は、ISO レイヤ 5 ～ 6 プロトコルで、UDP、TCP、SMB などのその他の転送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に対応したファシリティ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 のセキュリティ上の弱点の原因です。

Service MSRPC エンジンは、最も一般的なトランザクション タイプに対応し DCE および RPC プロトコルだけをデコードします。

Service MSRPC エンジンのパラメータ

表 B-19 は、Service MSRPC エンジンに固有のパラメータを示しています。

表 B-19　Service MSRPC エンジンのパラメータ

パラメータ	説明	値
protocol	インスペクタの対象プロトコル。	tcp udp
specify-operation	（オプション）MSRPC 動作の使用をイネーブルにします。 • operation：要求された MSRPC 動作。SMB_COM_TRANSACTION コマンドに必要です。完全一致。	0 ～ 65535
specify-regex-string	（オプション）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のある実際のストリーム 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のあるバイトの最小数。	0 ～ 65535
specify-uuid	（オプション）UUID をイネーブルにします。 • uuid：MSRPC UUID フィールド	000001a000000000 c000000000000046

Service MSSQL エンジン

Service MSSQL エンジンは、Microsoft の SQL server （MSSQL）によって使用されるプロトコルを検査します。

1 つの MSSQL シグニチャがあります。デフォルトの sa アカウントを使用した MSSQL へのログイン試行を検出すると、アラートを生成します。

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の 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-20 は、Service MSSQL エンジンに固有のパラメータを示しています。

表 B-20　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	（オプション）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中のユーザのユーザ名（完全一致）	sa

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。1 つの NTP シグニチャ（NTPd readvar オーバーフロー シグニチャ）があります。これは、readvar コマンドに NTP サービスが取り込むには大き過ぎる NTP データが指定されていることを検出した場合にアラートを生成します。

モードや制御パケットのサイズなどの NTP プロトコルの値に基づいて、シグニチャのチューニングやカスタム シグニチャの作成を行えます。

表 B-21 は、Service NTP エンジンに固有のパラメータを示しています。

表 B-21　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	Inspects NTP パケット： • control-opcode：RFC1305、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

Service RPC エンジン

Service RPC エンジンは、RPC プロトコル専用で、反回避方式としてフル デコードが含まれています。この方式によって、断片化メッセージ（複数のパケット内の 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のメッセージ）を処理できます。

RPC ポートマッパーは、ポート 111 で動作します。正規の RPC メッセージは番号が 551 以上の任意のポートでやり取りできます。RPC スイープは、有効な RPC メッセージが送信されたときに一意のポートだけをカウントする点を除けば、TCP ポート スイープと同様です。RPC は UDP 上でも稼働します。

表 B-22 は、Service RPC エンジンに固有のパラメータを示しています。

表 B-22　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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	from-service to-service
protocol	対象のプロトコル。	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]

表 B-22　Service RPC エンジンのパラメータ（続き）

パラメータ	説明	値
specify-is-spoof-src	（オプション）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生成します。	true | false
specify-port-map-program	（オプション）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：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	（オプション）RPC 最小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生成します。	0 ～ 65535
specify-rpc-procedure	（オプション）IP プロシージャをイネーブルにします。 • rpc-procedure：シグニチャの対象 RPC プロシージャ番号	0 ～ 1000000
specify-rpc-program	（オプション）IP プログラムをイネーブルにします。 • rpc-program：シグニチャの RPC プログラム番号	0 ～ 1000000

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。

Service SMB エンジン

Service SMB エンジンは、SMB パケットを検査します。SMB 制御トランザクション交換および SMB NT_Create_AndX 交換に基づいて、SMB シグニチャのチューニングやカスタム SMB シグニチャの作成を行えます。

表 B-23 は、Service SMB エンジンに固有のパラメータを示しています。

表 B-23　Service SMB 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-allocation-hint	（オプション）MSRPC 割り当てのヒントをイネーブルにします。 • allocation-hint：MSRPC 割り当てヒント。SMB_COM_TRANSACTION コマンドの解析で使用されます。[2]	0 ～ 42949677295
specify-byte-count	（オプション）バイト カウントをイネーブルにします。 • byte-count：SMB_COM_TRANSACTION 構造からのバイト カウント[3]	0 ～ 65535

表 B-23　Service SMB エンジンのパラメータ（続き）

パラメータ	説明	値
specify-command	（オプション）SMB コマンドをイネーブルにします。 • command：SMB コマンド値[4]	0 ～ 255
specify-direction	（オプション）トラフィックの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します。 — サービス ポートからクライアント ポートに向かうトラフィック。 — クライアント ポートからサービス ポートに向かうトラフィック。	from-service to service
specify-file-id	（オプション）トランザクション ファイル ID の使用をイネーブルにします。 • file-id：トランザクション ファイル ID[5] （注）このパラメータはシグニチャを特定の不正利用インスタンスだけに制限することがあるため、使用する場合は慎重に検討する必要があります。	0 ～ 65535
specify-function	（オプション）名前付きパイプ機能をイネーブルにします。 • function：名前付きパイプ機能[6]	0 ～ 65535
specify-hit-count	（オプション）ヒット カウントをイネーブルにします。 • hit-count：スキャン間隔の間の発生数のしきい値。この値を超えるとアラートを生成します。[7]	0 ～ 65535
specify-operation	（オプション）MSRPC 動作をイネーブルにします。 • operation：要求された MSRPC 動作。SMB_COM_TRANSACTION コマンドに必要です。完全一致は必須です。	0 ～ 65535
specify-resource	（オプション）リソースをイネーブルにします。 • resource：アラートを制限するために使用するパイプまたは SMB ファイル名を指定します。ASCII 形式です。完全一致は必須です。	*resource*
specify-scan-interval	（オプション）トラフィックの方向をイネーブルにします。 • scan-interval：アラート率を計算するために使用する間隔（秒単位）[8]	0 ～ 131071
specify-set-count	（オプション）セットアップ ワードのカウントをイネーブルにします。 • set-count：セットアップ ワードの数[9]	0 ～ 255

表 B-23　Service SMB エンジンのパラメータ（続き）

パラメータ	説明	値
specify-type	（オプション）MSRPC パケットのタイプ フィールドの検索をイネーブルにします。 • type：MSRPC パケットのタイプ フィールド。0 = Request、2 = Response、11 = Bind、12 = Bind Ack	0 ～ 255
specify-word-count	（オプション）コマンド パラメータのワード カウントをイネーブルにします。 • word-count：SMB_COM_TRANSACTION コマンド パラメータのワード カウント[10]	0 ～ 255
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラートメッセージでスワップされる場合は、true。スワップされない場合は 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. 完全一致はオプションです。
3. 完全一致はオプションです。
4. 完全一致は必須です。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。
5. 完全一致はオプションです。
6. 完全一致は必須です。SMB_COM_TRANSACTION コマンドに必要です。
7. シグニチャ 3302 および 6255 に対してのみ有効です。
8. シグニチャ 3302 および 6255 に対してのみ有効です。
9. 完全一致は必須です。通常、SMB_COM_TRANSACTION コマンドの場合は 2 個必要です。
10. 完全一致は必須です。16 個のワードのトランザクションだけがデコードされます。

Service SNMP エンジン

Service SNMP エンジンは、ポート 161 宛てのすべての 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 シグニチャのチューニングやカスタム SNMP シグニチャの作成を行えます。

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-24 は、Service SNMP エンジンに固有のパラメータを示しています。

表 B-24　Service SNMP 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。	—
brute-force-inspection	総当たり攻撃を検査します。 • 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 宛ての非 SNMP トラフィックを検査します。	—

表 B-24　Service SNMP エンジンのパラメータ（続き）

パラメータ	説明	値
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、つまり 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*

Service SSH エンジン

Service SSH エンジンはポート 22 の SSH トラフィック専用です。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、エンジンはセットアップのフィールドのみを監視します。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はチューニングできますが、カスタム シグニチャは作成できません。

表 B-25 は、Service SSH エンジンに固有のパラメータを示しています。

表 B-25　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 鍵の長さ： — length：鍵がこれより大きくなると、RSAREF オーバーフローが起動します。 • user-length：ユーザ長 SSH 検査： — length：鍵がこれより大きくなると、RSAREF オーバーフローが起動します。	0 ～ 65535
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	（オプション）パケット数をイネーブルにします。 • packet-depth：セッション鍵が失われたと判断するまでに監視するパケット数	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。

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ることができます。ステート マシンは、出力またはアラーム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-26 は、State エンジンに固有のパラメータを示しています。

表 B-26　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。	—
cisco-login	Cisco login のステート マシンを指定します。 • state-name：シグニチャがアラートを起動する前に必要な状態の名前。 — 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 Format String の弱点を検査するステート マシンを指定します。 • state-name：シグニチャがアラートを起動する前に必要な状態の名前。 — LPR Format String 検査を終了させる中断状態 — 形式文字の状態 — 開始状態	abort format-char start
smtp	SMTP プロトコルのステート マシンを指定します。 • state-name：シグニチャがアラートを起動する前に必要な状態の名前。 — LPR Format String 検査を終了させる中断状態 — 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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	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 a-b[,c-d] [1]

表 B-26　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	（オプション）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のある実際のストリーム オフセット。	0 ～ 65535
specify-min-match-length	（オプション）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のあるバイトの最小数。	0 ～ 65535
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラートメッセージでスワップされる場合は、true。スワップされない場合は 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。

String エンジン

この項では、String エンジンについて説明します。取り上げる事項は次のとおりです。

- 概要（P.B-35）
- String ICMP エンジンのパラメータ（P.B-35）
- String TPC エンジンのパラメータ（P.B-36）
- String UDP エンジンのパラメータ（P.B-37）

概要

String エンジンは、ICMP、TCP、および UDP の各プロトコル用の汎用のパターン マッチング検査エンジンです。String エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現エンジンを使用します。

String ICMP、String TCP、および String UDP の 3 つの String エンジンがあります。

String ICMP エンジンのパラメータ

カスタム String エンジン シグニチャの例は、P.6-29 の「String TCP シグニチャの例」を参照してください。

表 B-27 は、String ICMP エンジンに固有のパラメータを示しています。

表 B-27　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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	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	（オプション）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のある実際のストリーム オフセット。	0 ～ 65535
specify-min-match-length	（オプション）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のあるバイトの最小数。	0 ～ 65535
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラート メッセージでスワップされる場合は、true。スワップされない場合は 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。

String TPC エンジンのパラメータ

カスタム String エンジン シグニチャの例は、P.6-29 の「String TCP シグニチャの例」を参照してください。

表 B-28 は、String TCP エンジンに固有のパラメータを示しています。

表 B-28　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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	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	（オプション）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のある実際のストリーム オフセット。	0 ～ 65535
specify-min-match-length	（オプション）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のあるバイトの最小数。	0 ～ 65535
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	アドレス（およびポート）の送信元と宛先がアラート メッセージでスワップされる場合は、true。スワップされない場合は 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。

String UDP エンジンのパラメータ

カスタム String エンジン シグニチャの例は、P.6-29 の「String TCP シグニチャの例」を参照してください。

表 B-29 は、String UDP エンジンに固有のパラメータを示しています。

表 B-29　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 ポートに向かうトラフィック。 • クライアント ポートからサービス ポートに向かうトラフィック。	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	（オプション）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のある実際のストリーム オフセット。	0 ～ 65535
specify-min-match-length	（オプション）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のあるバイトの最小数。	0 ～ 65535
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラート メッセージでスワップされる場合は、true。スワップされない場合は 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。

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解析します。既存のシグニチャをチューニングするか、またはカスタム シグニチャを作成できます。Sweep エンジンには、ICMP、UDP、および TCP 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、一定の間隔内にアドレス 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 トラッキング処理はカウンティングと呼ばれます。

一意のパラメータは、Sweep エンジンのすべてのシグニチャに対して指定する必要があります。スイープに適用される制限は 2 ～ 40（包含）です。2 はスイープの絶対最小数です。2 未満の場合は、スイープではありません（1 つのホストまたはポート）。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値範囲は、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 スイープでは、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。

表 B-30 は、Sweep エンジンに固有のパラメータを示しています。

表 B-30　Sweep エンジンのパラメータ

パラメータ	説明	値
protocol	インスペクタの対象プロトコル。	icmp udp tcp
specify-icmp-type	（オプション）ICMP ヘッダー タイプをイネーブルにします。 • icmp-type：ICMP ヘッダーの TYPE 値。	0 ～ 255
specify-port-range	（オプション）検査対象としてのポート範囲の使用をイネーブルにします。 • port-range：検査に UDP ポート範囲を使用します。	0 ～ 65535 a-b[,c-d]
fragment-status	フラグメント化するかどうかを指定します。 • 任意のフラグメント状態 • 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

表 B-30　Sweep エンジンのパラメータ（続き）

パラメータ	説明	値
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 • 攻撃者アドレスと被害先アドレス • 攻撃者アドレスと被害先ポート	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、アラートを生成しない。	true | false
swap-attacker-victim	アドレス（およびポート）の送信元と宛先がアラートメッセージでスワップされる場合は、true。スワップされない場合は false（デフォルト）。	true | false
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

Traffic ICMP エンジン

Traffic ICMP エンジンは、TFN2K、LOKI、および DDOS などの非標準プロトコルを解析します。ユーザ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）のみがあります

Tribe Flood Net 2000（TFN2K）は比較的新しいバージョンの TFN です。これは感染したコンピュータ（ゾンビ）による調整された攻撃を制御して、無数の未確認の攻撃ホストから偽のトラフィックフラッドで 1 つのコンピュータ（またはドメイン）をターゲットとするために使用される Distributed DOS（DDoS）エージェントです。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キャラクタ 64「A」が検出されたかどうかを示しています。TFN2K は、任意のポートで実行可能で、ICMP、TCP、UDP、またはこれらのプロトコルの組み合せで通信できます。

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、悪意のあるコードが ICMP 応答で小さなペイロードを送信するために使用できる「ICMP トンネル」を作成します（ICMP をブロックするように設定していない場合、この応答はファイアウォールを通過できます）。LOKI シグニチャは、応答に対する ICMP エコー要求のアンバランス、簡易 ICMP コードおよびペイロード識別子を監視します。

（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（Tribe Flood Net）と Stacheldraht です。これらは TFN2K と同様に動作しますが、ICMP のみに依存し、固定コマンド（整数および文字列）があります。

表 B-31 は、Traffic ICMP エンジンに固有のパラメータを示しています。

表 B-31　TRAFFIC.ICMP エンジンのパラメータ

パラメータ	説明	値
parameter-tunable-sig	シグニチャに設定可能なパラメータがあるかどうかを示します。	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	要求に対する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、アラートを生成します。	0 ～ 65535
want-request	アラートの生成前に、ECHO REQUEST の検出が必要となります。	true | false

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解析します。Trojan BO2K、Trojan TFN2K、および Trojan UDP の 3 つの Trojan エンジンがあります。

BackOrifice（BO）は、UDP 上でのみ実行された最初の Windows のバック ドア型トロイの木馬でした。すぐに BackOrifice 2000（BO2K）がそれに取って代わりました。BO2K は、基本的な XOR 暗号化された UDP および TCP の両方に対応しています。それらには、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、ほとんど認知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。

Trojan UDP エンジンの swap-attacker-victimngine を除き、Trojan エンジンに固有のパラメータはありません。

トラブルシューティング

この付録では、センサーとソフトウェアのトラブルシューティングのヒントと手順を示します。この章は、次の項で構成されています。

- 予防保守（P.C-2）
- 障害リカバリ（P.C-3）
- パスワード リカバリ（P.C-4）
- 4200 シリーズ アプライアンスのトラブルシューティング（P.C-5）
- IDM のトラブルシューティング（P.C-41）
- IDSM-2 のトラブルシューティング（P.C-46）
- AIP SSM のトラブルシューティング（P.C-54）
- 情報の収集（P.C-56）

予防保守

次のアクションは、センサーの保守に役立ちます。

- 適切なコンフィギュレーションをバックアップします。現在のコンフィギュレーションが使用できなくなった場合に、バックアップ バージョンに置換できます。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating and Using a Backup Configuration File」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をリモート システムに保存します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Copying and Restoring the Configuration File Using a Remote Server」を参照してください。
- 手動でアップグレードする前に、必ずコンフィギュレーションをバックアップしてください。自動アップグレードを設定してある場合は、定期的なバックアップを実行してください。
- 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、パスワードのリカバリや、TAC によって指示されたその他の特別なデバッグ状況に必要です。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

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 アクセスを提供します。これにより、システムは脆弱になります。しかし、サービス アカウントを使用すると、管理者パスワードを喪失した場合に新規パスワードを作成することができます。状況を分析して、サービス アカウントをシステム上に存在させるかどうかを決定します。

（注）　AIP SSM へのシェル アクセスを取得できないので、AIP SSM でパスワード リカバリ用のサービス アカウントを使用することはできません。AIP SSM へのシェル アクセスを取得するには、ROMMON を使用する必要があります。

障害リカバリ

この項では、障害の後にセンサーを復旧する必要がある場合の推奨事項と実行すべきステップを示します。

障害が発生した場合に備えて、これらの推奨事項に従ってください。

- コンフィギュレーションに CLI または IDM を使用している場合は、変更を加えるたびに現在のコンフィギュレーションをセンサーから FTP または SCP サーバへコピーします。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating and Using a Backup Configuration File」を参照してください。

  (注) そのコンフィギュレーションの特定のソフトウェア バージョンをメモしておく必要があります。コピーしたコンフィギュレーションは、同じバージョンのセンサーにしか適用できません。

  (注) また、そのセンサーで使用したユーザ ID のリストも必要です。ユーザ ID とパスワードのリストは、コンフィギュレーションに保存されません。現在のセンサー上のユーザのリストを取得する手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Viewing User Status」を参照してください。

- IDS MC を使用している場合、現在のコンフィギュレーションは IDS MC データベースに保存されるので、別のコピーは必要ありません。

  (注) ユーザ ID のリストは、IDS MC データベースには保存されません。ユーザ ID をメモしておく必要があります。

  (注) そのコンフィギュレーションの特定のソフトウェア バージョンをメモしておく必要があります。コピーしたコンフィギュレーションは、同じバージョンのセンサーにしか適用できません。

障害が発生し、センサーを回復する必要がある場合は、次の手順を実行します。

1. センサーのイメージを再作成します。

   アプライアンスとモジュールの場合の手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

2. デフォルト 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) cisco パスワードを変更するよう求めるプロンプトが表示されます。

3. **setup** コマンドを実行します。

   手順については、P.1-6 の「センサーの初期化」を参照してください。

4. コンフィギュレーションが最後に保存されコピーされたときの IPS ソフトウェア バージョンにセンサーをアップグレードします。

   IPS ソフトウェアのバージョンを確認し、それらをインストールする方法の詳細については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

警告　センサーを障害前と同じ IPS ソフトウェア バージョンに戻さずに、保存したコンフィギュレーションをコピーしようとすると、コンフィギュレーション エラーが発生する可能性があります。

5. 最後に保存したコンフィギュレーションをセンサーにコピーします。

   手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1* 』の「Creating and Using a Backup Configuration File」を参照してください。

6. センサーの新しい鍵と証明書を使用するようにクライアントをアップデートします。

   イメージを再作成すると、センサーの SSH 鍵と HTTPS 証明書が変更されます。手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

7. 前のユーザを作成します。

   手順については、P.2-28 の「ユーザの設定」を参照してください。

パスワード リカバリ

次のパスワード リカバリ オプションが存在します。

- 別の管理者アカウントが存在する場合、もう一方の管理者はパスワードを変更できます。
- サービス アカウントが存在する場合は、サービス アカウントにログインし、コマンド **su - root** を使用してユーザ root に切り替えることができます。CLI 管理者アカウントのパスワードを変更するには、**password** コマンドを使用します。たとえば、管理者のユーザ名が「adminu」である場合、コマンドは **password adminu** になります。新規パスワードを 2 度入力するよう求めるプロンプトが表示されます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

リカバリ パーティションまたはシステム 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ことができます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

4200 シリーズ アプライアンスのトラブルシューティング

この項では、4200 シリーズ アプライアンスのトラブルシューティングについて説明します。

ヒント アプライアンスをトラブルシューティングする前に、センサーにインストールしたソフトウェア バージョンの Readme で警告の項を調べて、既知の問題を確認してください。

この項で取り上げる事項は次のとおりです。

- 通信の問題（P.C-5）
- SensorApp およびアラート（P.C-11）
- ブロッキング（P.C-19）
- ロギング（P.C-28）
- センサーが NTP サーバと同期していることを確認する（P.C-34）
- シグニチャに対して TCP リセットが実行されない（P.C-35）
- ソフトウェア アップグレード（P.C-37）

通信の問題

この項では、4200 シリーズのセンサーでの通信の問題のトラブルシューティングについて説明します。取り上げる事項は次のとおりです。

- Telnet または SSH を使用してセンサー CLI にアクセスできない（P.C-5）
- 設定が誤っているアクセス リスト（P.C-8）
- 重複する IP アドレスによりインターフェイスがシャットダウンする（P.C-9）

Telnet または SSH を使用してセンサー 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 でセンサー CLI にアクセスできない場合は、次の手順を実行します。

（注） センサーで Telnet をイネーブルまたはディセーブルにする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Enabling and Disabling Telnet」を参照してください。

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 CLI にログインします。

センサー上で CLI セッションを直接開くさまざまな方法については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Logging In to the Sensor」を参照してください。

ステップ 2　センサーの管理インターフェイスがイネーブルになっていることを確認します。

```
sensor# 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
sensor#
```

管理インターフェイスは、ステータス行 `Media Type = TX` が記述されたリスト内のインターフェイスです。Link Status が `Down` である場合はステップ 3 に進んでください。Link Status が `Up` である場合はステップ 5 に進んでください。

ステップ 3　センサーの IP アドレスが固有であることを確認します。

```
sensor# 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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

ネットワーク上の別のデバイスが同じ IP アドレスを持っていることを管理インターフェイスが検出した場合、管理インターフェイスは起動しません。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the IP Address, Netmask, and Gateway」を参照してください。

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されていない場合、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のアクセス リストで許可されていることを確認してください。

```
sensor# 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 10.89.130.108/23,10.89.130.1
host-name sensor
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のネットワーク アドレスがセンサーのアクセス 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のネットワーク アドレス用に許可エントリを追加し、コンフィギュレーションを保存し、接続を再試行します。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the Access List」を参照してください。

ステップ 7　ネットワーク　コンフィギュレーションでワークステーションがセンサーに接続できるようになっていることを確認します。

ファイアウォールの後ろでセンサーが保護されていて、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は、ワークステーションがセンサーにアクセスでき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。あるいは、ワークステーションの IP アドレスでネットワーク アドレス変換を実行しているファイアウォールの後ろにワークステーションがあり、センサーがファイアウォールの前にある場合は、センサーのアクセス リストにワークステーションの変換済みアドレス用の許可エントリが含まれていることを確認します。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the Access List」を参照してください。

設定が誤っているアクセス リスト

設定が誤っているアクセス リストを訂正するには、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　コンフィギュレーションを表示してアクセス リストを確認します。

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

ステップ 3　許可されたネットワークのリストにクライアントの IP アドレスがあることを確認します。ない場合は、追加します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

ステップ 4　設定を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: qsensor-238 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>
   ------------------------------------------------
sensor(config-hos-net)#
```

重複する IP アドレスによりインターフェイスがシャットダウンする

同じ IP アドレスで新しくイメージが作成されたセンサーが 2 つあり、それらが同じネットワーク上で同時に起動すると、インターフェイスはシャットダウンします。Linux は、別のホストとのアドレスの競合を検出すると、コマンド / コントロール インターフェイスがアクティブ化するのを妨げます。

該当するセンサーにネットワーク上の別のホストとの IP アドレスの競合が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起動しているかどうかを判別します。

```
sensor# 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
sensor#
```

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であることが出力で示されている場合は、ハードウェアの問題または IP アドレスの競合があります。

ステップ 3　センサーの配線が正しいことを確認します。

『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のセンサーの章を参照してください。

ステップ 4　**setup** コマンドを実行して、IP アドレスが正しいことを確認します。

手順については、P.1-6 の「センサーの初期化」を参照してください。

SensorApp およびアラート

この項では、SensorApp およびアラートでのトラブルシューティングの問題について説明します。取り上げる事項は次のとおりです。

- SensorApp が動作していない（P.C-11）
- 物理接続、SPAN、または VACL ポートの問題（P.C-12）
- アラートが表示されない（P.C-14）
- センサーがパケットを検出しない（P.C-16）
- 破損した SensorApp コンフィギュレーションの削除（P.C-18）
- IDS-4250-XL の不良なメモリ（P.C-18）

SensorApp が動作していない

センシング プロセスの SensorApp は、常に動作している必要があります。動作していない場合は、アラートを受信しません。SensorApp は分析エンジンの一部なので、分析エンジンが動作していることを確認する必要があります。

分析エンジンが動作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　分析エンジン サービスのステータスを判別します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor up-time is 19 days.
Using 505495552 out of 1984704512 bytes of available memory (25% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 37.7M out of 166.6M bytes of available disk space (24%
usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Running
AnalysisEngine   2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not
Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

sensor#
```

ステップ 3　分析エンジンが動作していない場合は、それにつながるエラーを検索します。

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 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）　最後の再起動の日付と時刻がリストされます。この例では、最後の再起動は 2004 年 2 月 19 日の 7 時 34 分でした。

ステップ 4　最新のソフトウェア アップデートを持っていることを確認してください。

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

最新のソフトウェア アップデートを持っていない場合は、Cisco.com からそれらをダウンロードします。手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

ステップ 5　ソフトウェア アップグレードに付属している Readme を参照して、SensorApp または分析エンジンの既知の DDTS を確認してください。

物理接続、SPAN、または VACL ポートの問題

センサーが適切に接続されていない場合は、アラートを受信しません。

センサーが適切に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起動していることと、パケット カウントが増加していることを確認します。

```
sensor# 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 = 1830137
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 3　Link Status がダウンである場合は、センシング ポートが適切に接続されていることを確認します。

a.　センシング ポートがアプライアンスで適切に接続されていることを確認します。

『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のアプライアンスの章を参照してください。

b.　センシング ポートが IDSM-2 で正しい SPAN または VACL キャプチャ ポートに接続されていることを確認します。

『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の IDSM-2 の章を参照してください。

ステップ 4　インターフェイス コンフィギュレーションを確認します。

a.　インターフェイスが正しく設定されていることを確認します。

手順については、P.3-10 の「インターフェイスの設定」を参照してください。

b. Cisco スイッチで SPAN および VACL キャプチャ ポート コンフィギュレーションを確認します。

手順についてはスイッチのマニュアルを参照してください。

ステップ 5 インターフェイスが起動していることと、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。

```
sensor# show interfaces
```

アラートが表示されない

アラートが表示されない場合は、次のことを試してください。

- シグニチャがイネーブルになっていることを確認します。
- シグニチャが非アクティブになっていないことを確認します。
- Produce Alert がアクションとして設定されていることを確認します。

（注） Produce Alert を選択した後、戻って別のイベント アクションを追加し、Produce Alert を新規コンフィギュレーションに追加しないと、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、新規コンフィギュレーションが古いコンフィギュレーションを上書きするので、各シグニチャに必要なイベント アクションをすべて設定してあることを確認してください。

- センサーがパケットを検出していることを確認します。
- アラートが生成中で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 シグニチャがイネーブルになっていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   ----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   ----------------------------------------------
sensor(config-sig-sig-sta)#
```

ステップ 3　Produce Alert が設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   ----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      ----------------------------------------------
sensor#
```

ステップ 4　センサーがパケットを検出していることを確認します。

```
sensor# 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
sensor#
```

ステップ 5　アラートをチェックします。

```
sensor# 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検出しない

センサーがネットワーク上のパケットを検出していない場合は、インターフェイスのセットアップが正しくない可能性があります。

センサーがパケットを検出していない場合は、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起動し、パケットを受信していることを確認します。

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   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
sensor#
```

ステップ 3　インターフェイスが起動していない場合は、次の手順を実行します。

a.　配線を確認します。

センサーが適切にインストールされているかどうか確認する手順については、『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のセンサーの章を参照してください。

b. インターフェイスをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   ----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      ----------------------------------------------
         none
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
sensor(config-int-phy)#
```

ステップ 4　インターフェイスが起動し、パケットを受信しているかどうかを確認します。

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   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 = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
   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 ...
```

破損した SensorApp コンフィギュレーションの削除

SensorApp コンフィギュレーションが破損し SensorApp を実行できない場合は、コンフィギュレーションを完全に削除して SensorApp を再起動する必要があります。

SensorApp 設定を削除するには、次の手順を実行します。

ステップ 1　サービス アカウントにログインします。

ステップ 2　su で root になります。

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 ファイルを置換します。

```
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 サービスを開始します。

```
sensor# cids start
```

ステップ 9　管理者特権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。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? [yes]:yes
Request Succeeded.
sensor#
```

IDS-4250-XL の不良なメモリ

IDS-4250-XL の中には、問題のある DIMM を XL カードに搭載して出荷されたものがあります。問題のある DIMM によって、センサーが停止したり、SensorApp が機能を停止してコア ファイルを生成したりすることがあります。

IDS-4250-XL のメモリに問題があるかどうかを確認する手順については、Partner Field 52563 を参照してください。

ブロッキング

この項では、ブロッキングと ARC サービスのためのトラブルシューティングのヘルプを提供します。取り上げる事項は次のとおりです。

- ブロッキングのトラブルシューティング（P.C-19）
- ARC が動作していることを確認する（P.C-20）
- ARC 接続がアクティブであることを確認する（P.C-20）
- デバイス アクセスの問題（P.C-22）
- 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（P.C-24）
- ネットワーク デバイスへの SSH 接続をイネーブルにする（P.C-25）
- シグニチャに対してブロッキングが実行されない（P.C-25）
- マスター ブロッキング センサーのコンフィギュレーションを確認する（P.C-26）

ブロッキングのトラブルシューティング

ARC を設定した後、**show version** コマンドを使用して、ARC が適切に動作するかどうかを確認できます。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。IPS 5.1 から名前は変更されましたが、IDM と CLI では引き続き Network Access Controller、**nac**、および **network-access** として示されています。

ARC をトラブルシューティングするには、次の手順を実行します。

1. ARC が動作していることを確認します。

   手順については、P.C-20 の「ARC が動作していることを確認する」を参照してください。

2. ARC がネットワーク デバイスに接続していることを確認します。

   手順については、P.C-20 の「ARC 接続がアクティブであることを確認する」を参照してください。

3. Event Action が特定のシグニチャの Block Host に設定されていることを確認します。

   手順については、P.C-25 の「シグニチャに対してブロッキングが実行されない」を参照してください。

4. 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します。

   手順については、P.C-26 の「マスター ブロッキング センサーのコンフィギュレーションを確認する」を参照してください。

（注） ARC アーキテクチャの説明については、P.A-12 の「ARC」を参照してください。

ARC が動作していることを確認する

ARC が動作していることを確認するには、**show version** コマンドを使用します。MainApp が動作していないと、ARC は実行できません。ARC は MainApp の一部です。

ステップ 1　CLI にログインします。

ステップ 2　MainApp が動作していることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1.1)S152.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 3 days.
Using 734863360 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 35.6M out of 166.8M bytes of available disk space (23%
usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not
Running
AnalysisEngine   2005_Mar_18_12.53   (Release)   2005-03-18T13:03:21-0600   Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-sp-5.0-1.1-   12:53:00 UTC Fri Mar 18 2005

Recovery Partition Version 1.1 - 5.0(1.1)

sensor#
```

ステップ 3　MainApp が `Not Running` と表示した場合、ARC は動作していません。TAC に連絡します。

ARC 接続がアクティブであることを確認する

ARC 統計情報で State が `Active` でない場合は、問題が生じています。

統計情報内で 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 が接続してい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中であることを確認します。

```
sensor# 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
sensor#
```

ステップ 3　ARC が接続していない場合は、繰り返し発生するエラーを検索してください。

```
sensor# show events error hh:mm:ss month day year | include : nac
```

例

```
sensor# show events error 00:00:00 Apr 01 2005 | include : nac
```

ステップ 4　最新のソフトウェア アップデートを持っていることを確認してください。

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

最新のソフトウェア アップデートを持っていない場合は、Cisco.com からそれらをダウンロードします。手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

ステップ 5　ソフトウェア アップグレードに付属している Readme を参照して、ARC の既知の DDTS を確認してください。

ステップ 6　各デバイスのコンフィギュレーション設定が正しいことを確認します（ユーザ名、パスワード、IP アドレス）。

手順については、P.C-22 の「デバイス アクセスの問題」を参照してください。

ステップ 7　各ネットワーク デバイスのインターフェイスと方向が正しいことを確認します。

手順については、P.C-24 の「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」を参照してください。

ステップ 8　ネットワーク デバイスが SSH-DES または SSH-3DES を使用している場合は、デバイスへの SSH 接続がイネーブルになっていることを確認します。

手順については、P.C-25 の「ネットワーク デバイスへの SSH 接続をイネーブルにする」を参照してください。

ステップ 9　制御されている各デバイスのインターフェイスと方向がそれぞれ正しいことを確認します。

手順については、P.C-24 の「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」を参照してください。

デバイス アクセスの問題

ARC が管理対象のデバイスにアクセスできない場合があります。管理対象デバイスの 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ます。

(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 アクセスの問題をトラブルシューティングするには、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　管理対象デバイスの IP アドレスを確認します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor(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)
   ----------------------------------------------
   ----------------------------------------------
sensor(config-net)#
```

ステップ 3　デバイスに手動で接続して、ユーザ名、パスワード、およびイネーブル　パスワードが正しいことと、デバイスがセンサーから到達可能であることを確認します。

a. サービス アカウントにログインします。

b. ネットワーク デバイスに Telnet または SSH で接続して、コンフィギュレーションを確認します。

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 デバイスのインターフェイスと方向がそれぞれ正しいことを確認します。

手順については、P.C-24 の「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」を参照してください。

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

管理対象のデバイスごとに各インターフェイスと方向が正しいことを確認するために、偽のホストに手動ブロックを送信し、ルータの ACL 内にブロックされたアドレスに対応する deny エントリがあるかどうかを確認できます。

(注)　また、**Monitoring** > **Active Host Blocks** をクリックして、IDM から手動ブロックを実行することもできます。

偽の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 汎用サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

ステップ 2　偽のホスト IP アドレスに対する手動ブロックを開始します。

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 3　汎用サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 4　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 5　ルータに Telnet 接続し、ブロックされる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ために、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** を入れます。

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

ネットワーク デバイスへの SSH 接続をイネーブルにする

SSH-DES または SSH-3DES をネットワーク デバイスの通信プロトコルとして使用している場合は、それがデバイスでイネーブルになっていることを確認する必要があります。

ネットワーク デバイスへの SSH 接続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　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 モードに入ります。

```
sensor# configure terminal
```

ステップ 3　SSH をイネーブルにします。

```
sensor(config)# ssh host blocking_device_ip_ address
```

ステップ 4　デバイスを受け入れるかどうかを確認するプロンプトで、**yes** と入力します。

シグニチャに対してブロッキングが実行されない

特定のシグニチャに対してブロッキングが実行されない場合は、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ことを確認します。

特定のシグニチャに対してブロッキングが実行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　シグニチャ定義サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

ステップ 3　ホストをブロックするようにイベント アクションが設定されていることを確認します。

(注) アラートを受け取る場合は、イベント アクションの設定時に必ず **produce-alert** を追加する必要があります。

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(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。

```
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 5　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

マスター ブロッキング センサーのコンフィギュレーションを確認する

マスター ブロッキング センサーが適切にセットアップされていることを確認したり、適切にセットアップされていないマスター ブロッキング センサーをトラブルシューティングしたりするために、**show statistics network-access** コマンドを使用できます。リモート マスター ブロッキング センサーが Web アクセスに TLS を使用している場合は、転送センサーが信頼できる TLS ホストとしてセットアップされていることを確認します。

センサーのマスター ブロッキング センサー コンフィギュレーションを確認するには、次の手順を実行します。

ステップ 1　ARC の統計情報を表示して、マスター ブロッキング センサー エントリが統計情報内にあることを確認します。

```
sensor# 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 2　マスター ブロッキング センサーが統計情報内にない場合は、追加する必要があります。

手順については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

ステップ 3　マスター ブロッキング センサーが確実にブロックを開始するように、偽のホスト IP アドレスに対する手動ブロックを開始します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 4　ネットワーク アクセス汎用サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 5　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 6　ブロックが ARC の統計情報に表示されることを確認します。

```
sensor# 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 7　マスター ブロッキング センサーのホストの 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が表示されることを確認します。

```
sensor# 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 8　リモート マスター ブロッキング センサーが Web アクセスに TLS を使用している場合は、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。

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

ロギング

TAC は、トラブルシューティングの目的でユーザにデバッグ ロギングを有効にするように要請する場合があります。LogApp 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って、各アプリケーションによってどのログ メッセージが生成されるかを制御します。デフォルトでは、デバッグ ロギングはオンになりません。

個々のゾーン制御をイネーブルにすると、各ゾーンはそれが設定されているロギングのレベルを使用します。それ以外の場合は、すべてのゾーンに対して同じロギング レベルが使用されます。

この項で取り上げる事項は次のとおりです。

- デバッグ ロギングをイネーブルにする（P.C-28）
- ゾーン名（P.C-33）
- SysLog への cidLog メッセージの転送（P.C-33）

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とパフォーマンスに大きく影響するため、TAC によって指示された場合にだけイネーブルにしてください。

デバッグ ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　サービス アカウントにログインします。

ステップ 2　log.conf ファイルを編集して、追加のログ ステートメントを格納できるよう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　ファイルのゾーンおよび CID セクションを見つけて、デバッグの重大度を設定します。

```
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　管理者として CLI にログインします。

ステップ 7　マスター コントロール サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

ステップ 8　すべてのゾーンに対してデバッグ ロギングをイネーブルにするには、次の手順を実行します。

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   ----------------------------------------------
sensor(config-log-mas)#
```

ステップ 9　個々のゾーン制御をオンにするには、次の手順を実行します。

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
sensor(config-log-mas)#
```

ステップ 10　マスター ゾーン制御を終了します。

```
sensor(config-log-mas)# exit
```

ステップ 11 ゾーン名を表示します。

```
sensor(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>
   ----------------------------------------------
sensor(config-log)#
```

各ゾーン名の参照先リストについては、P.C-33 の「ゾーン名」を参照してください。

ステップ 12 特定のゾーンの重大度レベル（デバッグ、タイミング、警告、またはエラー）を変更します。

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(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>
   -----------------------------------------------
sensor(config-log)#
```

ステップ 13 特定のゾーンのデバッグをオンにします。

```
sensor(config-log)# zone-control nac severity debug
sensor(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>
   ----------------------------------------------
sensor(config-log)#
```

ステップ 14 ログ サブモードを終了します。

```
sensor(config-log)# exit
Apply Changes:?[yes]:
```

ステップ 15 変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ゾーン名

表 C-1 にデバッグ ログ ゾーン名を示します。

表 C-1　デバッグ ログ ゾーン名

ゾーン名	説明
AuthenticationApp	認証ゾーン
Cid	汎用ロギング 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
cmgr	Card Manager サービス ゾーン[1]
cplane	Control Plane ゾーン[2]
csi	CIDS サーブレット インターフェイス[3]
ctlTransSource	送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
SensorApp	AnalysisEngine 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および状態の情報を交換するために、AIP SSM で使用されます。
2. Control Plane は、Card Manager によって AIP SSM で使用されるトランスポート通信レイヤです。
3. CIDS サーブレット インターフェイスは、CIDS Web サーバとサーブレットの間のインターフェイス レイヤです。

SysLog への cidLog メッセージの転送

syslog に cidLog メッセージを転送すると役に立つ場合があります。

cid ログ メッセージを syslog へ送信するには、次の手順を実行します。

ステップ 1　idsRoot/etc/log.conf ファイルへ移動します。

ステップ 2　次の変更を加えます。

a. [logApp] `enabled=false` と設定します。

`enabled=false` がデフォルトであるため、`enabled=true` のコメント化を解除します。

b. [drain/main] `type=syslog` を設定します。

次の例は、ロギング コンフィギュレーション ファイルを示しています。

```
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 出力が、syslog メッセージの優先度への次の通信とともに syslog ファシリティ local6 に送信されます。

```
LOG_DEBUG,        //   debug
LOG_INFO,            //    timing
LOG_WARNING,   //    warning
LOG_ERR,            //    error
LOG_CRIT            //     fatal
```

(注) /etc/syslog.conf　でそのファシリティが適切なプロパティでイネーブルになっていることを確認します。

注意 syslog は、logApp よりずっと低速です（毎秒約 1000 メッセージに対して、約 50 メッセージ）デバッグ重大度は一度に 1 つのゾーンでイネーブルにすることをお勧めします。

センサーが NTP サーバと同期していることを確認する

IPS 5.1 では、無効な NTP 鍵値や ID など、正しくない NTP コンフィギュレーションをセンサーに適用することはできません。正しくないコンフィギュレーションを適用しようとすると、エラーメッセージが表示されます。NTP コンフィギュレーションを確認するには、**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 統計情報があります。

NTP コンフィギュレーションを確認するには、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　ホスト統計情報を生成します。

```
sensor# 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　数分後にホスト統計情報を再び生成します。

```
sensor# 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` である場合は、NTP サーバ管理者と一緒に、NTP サーバが正しく設定されていることを確認します。

シグニチャに対して TCP リセットが実行されない

リセットするように設定されたイベント アクションがない場合は、特定のシグニチャに対して TCP リセットが実行されません。

特定のシグニチャに対してリセットが実行されないことをトラブルシューティングするには、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　イベント アクションが TCP リセットに設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
   ----------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-payload-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-header-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-tos
      ----------------------------------------------
--MORE--
```

ステップ 3　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 4　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 5　正しいアラームが生成されていることを確認します。

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

ステップ 6　スイッチでセンサーからの着信 TCP リセット パケットが許可されていることを確認します。

手順についてはスイッチのマニュアルを参照してください。

ステップ 7　リセットが送信されていることを確認します。

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

ソフトウェア アップグレード

この項では、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ついて説明します。取り上げる事項は次のとおりです。

- ソフトウェア アップグレードの間、IDS-4235 および IDS-4250 が機能停止する（P.C-37）
- 適用するアップグレードとそれらの前提条件（P.C-37）
- 自動アップデートの問題（P.C-38）
- センサーに保存されているアップデートでセンサーをアップデートする（P.C-39）

ソフトウェア アップグレードの間、IDS-4235 および IDS-4250 が機能停止する

IDS-4235 および IDS-4250 の BIOS が A03 の場合は、最新の IPS ソフトウェアを適用する前に、BIOS を A04 にアップグレードする必要があります。アップグレードしないと、ソフトウェア アップグレードのプロセス中にアプライアンスが機能停止します。BIOS をアップグレードする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1* 』の「Upgrading the BIOS」を参照してください。最新の IPS ソフトウェアを適用する手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

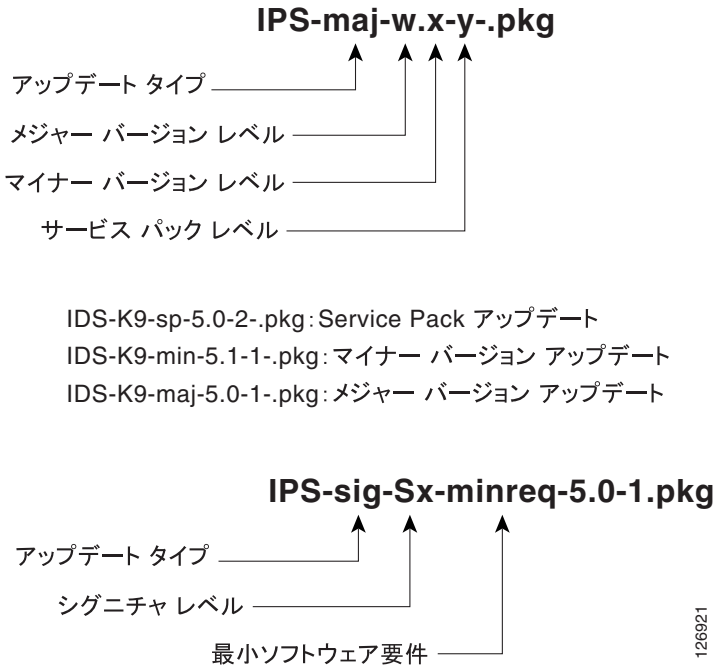
適用するアップグレードとそれらの前提条件

ソフトウェアの正しいサービス パック、マイナー バージョン、およびメジャー バージョンを用意する必要があります。新規ソフトウェアの適用でトラブルが発生した場合は、適切な前提条件で正しいアップデートを適用していることを確認してください。

- シグニチャ アップデートには、ファイル名にリストされた最小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 バージョンには前のメジャー バージョンが必要です。

図 C-1 は、IPS ソフトウェアのファイル名の解釈方法を示しています。

図 C-1　IPS ソフトウェアのファイル名



自動アップデートの問題

自動アップデートの推奨されるトラブルシューティング方法は次のとおりです。

- tcpDump の実行
  - サービス アカウントを作成します。センサーと FTP サーバの間でパケットを取得するには、su で root になり、コマンド / コントロール インターフェイスで tcpDump を実行します。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。
  - **upgrade** コマンドを使用して、手動でセンサーをアップグレードします。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。
  - tcpDump 出力で、FTP サーバから戻されるエラーを検索します。
- 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。

  ディレクトリが正しく指定されている必要があります。これを行わないと、Windows FTP サーバで問題が発生します。ディレクトリ名の前にもう 1 つまたは 2 つの「/」が必要な場合があります。

  これを確認するため、ご使用の FTP 接続による tcpDump 出力で表示される同じ FTP コマンドを使用します。
- カスタム プロンプトを使用するために FTP サーバを変更していないことを確認してください。

  たとえば、FTP プロンプトを変更してセキュリティ警告を提供するようにすると、センサーがハードコード化された応答のリストを期待するため、問題が発生します。

（注） プロンプトを変更しないことは、4.1(4) より前のバージョンにのみ当てはまります。

- Windows FTP サーバ セットアップ オプションを使用して、UNIX ファイル構造と非 MS-DOS ファイル構造をエミュレートする必要があります。
- SCP を使用している場合は、既知のホスト リストに SSH ホスト鍵を追加したことを確認してください。

  手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

自動アップデートを実行する前に、手動で **upgrade** コマンドを実行してみます。**upgrade** コマンドでは動作したが、自動アップデートでは動作しない場合には、次のことを試しています。

- センサーの IPS ソフトウェア バージョンを調べます（手順については、P.C-59 の「バージョン情報」を参照してください）。

  バージョン 4.0(1) には、自動アップデートに既知の問題があります。自動アップデートの設定と使用を試行する前に、4.1(1) へ手動でアップグレードします。
- 自動アップデート用にパスワードが設定されていることを確認します。手動アップデートに使用したパスワードと一致することを確認します。
- FTP サーバ内のファイル名が、大文字小文字の区別も含め、Cisco.com の Downloads に表示されるものと完全に一致することを確認します。

  Windows FTP サーバの中には、大文字小文字の区別が正しくないファイルへのアクセスを許可するものもありますが、最終的にはセンサーが名前の変更を理由にそのファイルを拒否します。

必要に応じて、自動アップデートで tcpDump を実行します。成功した手動アップデートと失敗した自動アップデートを比較して、そこからトラブルシューティングすることができます。

センサーに保存されているアップデートでセンサーをアップデートする

アップデート パッケージをセンサーの /var ディレクトリに保存し、必要に応じてそのアップデートを使用してセンサーをアップデートできます。

センサーに保存されているアップデートでセンサーをアップデートするには、次の手順を実行します。

ステップ 1　サービス 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。

手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

ステップ 3　アップデート ファイルをセンサーの /usr/cids/idsRoot/var ディレクトリへ FTP または SCP で送信します。

ステップ 4　ファイル許可を設定します。

```
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　管理者特権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 7　センサーのホスト鍵を保存します。

```
sensor# configure terminal
sensor(config)# service ssh
sensor(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。

```
sensor(config)# upgrade scp://service@sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

IDM のトラブルシューティング

この項では、IDM のトラブルシューティング手順を示します。

（注）これらの手順は、ASDM の IPS セクションにも適用されます。

この項で取り上げる事項は次のとおりです。

- Java プラグインのメモリ サイズを増やす（P.C-41）
- IDM を起動できない - Java アプレットのロードに失敗（P.C-43）
- IDM を起動できない - 分析エンジンがビジー状態（P.C-44）
- IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない（P.C-44）
- シグニチャがアラートを生成しない（P.C-45）

Java プラグインのメモリ サイズを増やす

IDM を正しく動作させるには、ブラウザに Java プラグイン 1.4.2 または 1.5 をインストールする必要があります。デフォルトでは、Java プラグインは 64 MB のメモリを IDM に割り当てます。IDM は使用中にメモリを使い果たしてしまうことがあります。この場合、IDM は停止するか、空白の画面を表示します。**Refresh** をクリックしたときに、メモリが使い果たされてしまうこともあります。メモリが使い果たされるたびに、Java コンソールに `OutofMemoryError` メッセージが表示されます。

（注）Sun Microsystems Java を使用することを推奨します。その他のバージョンの Java を使用すると、IDM に問題を引き起こすことがあります。

IDM を使用する前に Java プラグインのメモリ設定を変更する必要があります。必要最小メモリサイズは、256 MB です。

この項で取り上げる事項は次のとおりです。

- Windows での Java プラグイン（P.C-41）
- Linux および Solaris での Lava プラグイン（P.C-42）

Windows での Java プラグイン

Java プラグイン 1.4.2 および 1.5 に対応した Windows で Java プラグインの設定を変更するには、次の手順を実行します。

ステップ 1　Internet Explorer または Netscape のすべてのインスタンスを閉じます。

ステップ 2　**Start** > **Settings** > **Control Panel** をクリックします。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. Java プラグラインをクリックします。

Java Plug-in Control Panel が表示されます。

b. **Advanced** タブをクリックします。

c. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。

d. **Apply** をクリックして Java Control Panel を終了します。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. Java をクリックします。

Java Control Panel パネルが表示されます。

b. **Java** タブをクリックします。

c. Java Applet Runtime Settings の下で **View** をクリックします。

Java Runtime Settings Panel が表示されます。

d. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力し、**OK** をクリックします。

e. **OK** をクリックして Java Control Panel を終了します。

Linux および Solaris での Lava プラグイン

Linux および Solaris 上で Java プラグイン 1.4.2 および 1.5 の設定を変更するには、次の手順を実行します。

ステップ 1　Netscape または Mozilla のすべてのインスタンスを閉じます。

ステップ 2　ControlPanel 実行可能ファイルを起動すると、Java Plug-in Control Panel が表示されます。

（注） Java 2 SDK では、このファイルは <SDK インストール ディレクトリ >/jre/bin/ControlPanel にあります。たとえば、Java 2 SDK を /usr/j2se にインストールした場合、フルパスは /usr/j2se/jre/bin/ControlPanel です。

（注） Java 2 Runtime Environment をインストールした場合は、ファイルは <JRE インストール ディレクトリ >/bin/ControlPanel にあります。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. **Advanced** タブをクリックします。

b. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。

c. **Apply** をクリックして Java Control Panel を終了します。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. **Java** タブをクリックします。

b. Java Applet Runtime Settings の下で **View** をクリックします。

c. Java Runtime Parameters フィールドに `-Xmx256m` と入力し、**OK** をクリックします。

d. **OK** をクリックして Java Control Panel を終了します。

IDM を起動できない - Java アプレットのロードに失敗

症状　ブラウザに、`Loading Cisco IDM.Please wait ...` と表示されます。ウィンドウの左下隅に、`Loading Java Applet Failed` と表示されます。

考えられる原因　この状態は、IDM を起動するマシンに複数の Java プラグイン（1.4.*x* および / または 1.3.*x*）がインストールされている場合に発生します。

推奨処置　Java キャッシュをクリアして temp ファイルを削除し、使用しているブラウザの履歴をクリアします。結果として、これらのプラグインのどれもデフォルトでは使用されません。各アプレットは正しいプラグインを使用する必要があります。

キャッシュをクリアするには、次の手順を実行します。

ステップ 1　ブラウザのウィンドウをすべて閉じます。

ステップ 2　Java プラグイン 1.3.*x* がインストールされている場合は、次の手順を実行します。

a. **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.3.x** をクリックします。

b. **Advanced** タブをクリックします。

c. Java Runtime Environment の下で、ドロップダウン メニューから **JRE 1.3.x** を選択します。

d. **Cache** タブをクリックします。

e. **Clear** をクリックします。

ステップ 3　ava プラグイン 1.4.*x* がインストールされている場合は、次の手順を実行します。

a. **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.4.x** をクリックします。

b. **Advanced** タブをクリックします。

c. Java Runtime Environment の下で、ドロップダウン メニューから **JRE 1.3.x** を選択します。

d. **Cache** タブをクリックします。

e. **Browser** タブをクリックします。

f. ブラウザのチェックボックスをすべて選択解除します。

g. **Clear Cache** をクリックします。

ステップ 4　temp ファイルを削除し、ブラウザ内の履歴をクリアします。

IDM を起動できない - 分析エンジンがビジー状態

エラー メッセージ `Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.`

考えられる原因　この条件は、センサー内の分析エンジンがタスクを実行する準備のためにビジー状態で、IDM に応答しない場合に発生する可能性があります。

推奨処置　しばらく待ってから、接続を再試行してください。

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできないが、SSH または Telnet（イネーブルの場合）を使用してセンサーの CLI にアクセスできる場合には、次の手順を実行します。

（注） センサーで Telnet をイネーブルまたはディセーブルにする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Enabling and Disabling Telnet」を参照してください。

ステップ 1　ネットワーク コンフィギュレーションが、センサーで設定されている Web サーバ ポートにアクセスできることを確認します。

```
sensor# 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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
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 443
exit
```

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing Web Server Settings」を参照してください。

ステップ 2　ルータ、スイッチ、またはファイアウォールなどのネットワーク　デバイスがセンサーとワークステーションの間にある場合は、これらのデバイスが、ワークステーションによるセンサーの Web サーバ ポートへのアクセスを許可するように設定されていることを確認します。

リモート管理通信はすべてセンサーの Web サーバによって実行されます。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing Web Server Settings」を参照してください。

シグニチャがアラートを生成しない

シグニチャが反応したときにアラートが表示されない場合は、Produce Alert がイベント アクションとして設定されていることを確認してください。

注意　イベント アクションを設定するたびにその他のアクションを追加することはできません。実際には、イベント アクションを設定するたびに、そのリストを置換しているので、イベント アクションを設定するたびに必ず Produce Alert を選択してください。

たとえば、Produce Alert を選択したが、-後から別のイベント アクションを追加し、Produce Alert を新規コンフィギュレーションに追加しないと、アラートはイベント ストアに送信されません。

アラートを確実に受け取るようにするには、仮想センサーとイベント ストアの統計情報を使用します。

IDSM-2 のトラブルシューティング

IDSM-2 のソフトウェア アーキテクチャは、4200 シリーズのセンサーと同じです。P.C-5 の「4200 シリーズ アプライアンスのトラブルシューティング」で説明されているのと同じトラブルシューティング ツールを使用できます。

この項では特に IDSM-2 のトラブルシューティングについて説明します。取り上げる事項は次のとおりです。

- IDSM-2 問題の診断（P.C-46）
- トラブルシューティング用の switch コマンド（P.C-47）
- ステータス LED がオフになっている（P.C-47）
- ステータス LED がオンだが IDSM-2 がオンラインにならない（P.C-50）
- IDSM-2 コマンド / コントロール ポートと通信できない（P.C-51）
- TCP リセット インターフェイスの使用方法（P.C-52）
- シリアル ケーブルを IDSM-2 に接続する（P.C-53）

IDSM-2 問題の診断

次のリストに照らし合せて、IDSM-2 問題を診断します。

- IDSM-2 とマザーボードの間のリボン ケーブルがゆるくなっています。

  モジュールを物理的に処理しているときに、コネクタがベース カードから外れ、ドーター カードとベース カードの接触が失われる場合があります。コネクタのリボン ケーブルがゆるむと、ポート 7 と 8 でオンライン診断エラーが発生します。この条件が存在する場合、モジュールは動作できません。

  詳細については、Partner Field Notice 52816 を参照してください。

- IDSM-2 の中に、出荷時に障害のある DIMM が同梱されているものがありました。

  IDSM-2 のメモリに問題があるかどうかを確認する手順については、Partner Field 52563 を参照してください。

- ハードディスク ドライブが読み取りまたは書き込みを実行できません。

  ハードディスク ドライブを長期（2 週間以上）にわたって連続使用すると、次のようないくつかの症状が現れる場合があります。

  — ログインできない

  — 読み取り / 書き込み操作の実行時のコンソールへの I/O エラー（**ls** コマンド）

  — コマンドが正しく実行されない（実行可能ファイルへのパスが見つからない）

  スイッチはモジュールが良好であることを報告しますが、サービス アカウントにログインしてコマンドを実行しようとすると、問題が存在することが表示されます。4.1(4) サービス パックを使用すると、この問題は軽減されますが、4.1(4) アプリケーション パーティション イメージで IDSM-2 のイメージを再作成する場合は、4.1(4b) パッチを適用する必要があります。詳細については、CSCef12198 を参照してください。

- ストリームベースのシグニチャ（1300 シリーズ）に対して IP ロギングをイネーブルにすると、SensorApp はクラッシュするか、CPU の 99% を消費します。回避策については、CSCed32093 を参照してください。

- IDSM-2 はロックアップされると思われます。リモート アクセスは禁止されます（SSH、Telnet、IDM、イベント サーバ、制御トランザクション サーバ、および IP ログ サーバ）。

  この障害は、SWAP の使用に関連しています。IDSM-2 は ping に応答します。この問題を解決するには、4.1(4) サービス パックを適用します。詳細については、CSCed54146 を参照してください。

- IDSM-2 をアップグレードした直後、またはシグニチャを VMS で調整した直後に、IDSM-2 が応答しなくなり、多くの場合、SensorApp コア ファイルを生成します。この問題を修正するには、4.1(4b) パッチを適用します。

- サポートされるコンフィギュレーションが IDSM-2 にあることを確認します。

  『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Supported IDSM-2 Configurations」を参照してください。

IDSM-2 に上記の問題のいずれも発生していないことを確認し、それでも応答しないように見える場合、たとえば、SSH または Telnet からログインできない場合やスイッチに対してセッションを開始することができない場合などは、IDSM-2 が ping に応答するかどうかと、サービス アカウントからログインできるかどうかを確認してください。ログインできる場合は、cidDump およびコア ファイルを取得して、TAC に連絡してください。

トラブルシューティング用の switch コマンド

IDSM-2 のトラブルシューティングには、次の switch コマンドが役に立ちます。

- **show module**（Cisco Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show version**（Cisco Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show port**（Cisco Catalyst ソフトウェア）
- **show trunk**（Cisco Catalyst ソフトウェア）
- **show span**（Cisco Catalyst ソフトウェア）
- **show security acl**（Cisco Catalyst ソフトウェア）
- **show intrusion-detection module**（Cisco IOS ソフトウェア）
- **show monitor**（Cisco IOS ソフトウェア）
- **show vlan access-map**（Cisco IOS ソフトウェア）
- **show vlan filter**（Cisco IOS ソフトウェア）

ステータス LED がオフになっている

IDSM-2 のステータス インジケータがオフになっている場合は、電源を入れて IDSM-2 をオンにする必要があります。

IDSM-2 のステータスを判別するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　IDSM-2 がオンラインであることを確認します。

Catalyst ソフトウェアの場合、次のように入力します。

```
cat6k> enable

Enter password:
cat6k> (enable) show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- -------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE     yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC          no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45       no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX       no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC       no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2         yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- -------------------------------------- ------ ---------- ----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
cat6k> (enable)
```

Cisco IOS ソフトウェアの場合

```
cat6k#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0   7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model               Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A    2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
cat6k#
```

(注) IDSM-2　を初めて取り付けたときに、ステータスが　other　を示すのは正常な動作です。IDSM-2 が診断ルーチンを完了してオンラインになった後で、ステータスは ok を示します。IDSM-2 がオンラインになるまでの時間としては、最長で 5 分間みてください。

ステップ 3　ステータスが ok でない場合は、モジュールをオンにします。

```
router# set module power up module_number
```

ステータス LED がオンだが IDSM-2 がオンラインにならない

ステータス インジケータがオンになっているが、IDSM-2 がオンラインにならないという場合は、次のトラブルシューティング ヒントを試してください。

- IDSM-2 をリセットします。
- IDSM-2 がスイッチに適切にインストールされていることを確認します。
- ハードディスク ドライブのステータスが失敗した場合は、アプリケーション パーティションのイメージを再作成します。

IDSM-2 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　コンソールにログインします。

ステップ 2　IDSM-2 がイネーブルになっていることを確認します。

```
router# show module
```

ステップ 3　ステータスが ok でない場合は、IDSM-2 をイネーブルにします。

```
router# set module enable module_number
```

ステップ 4　IDSM-2 がそれでもオンラインにならない場合は、リセットしてください。

```
router# reset module_number
```

IDSM-2 がオンラインになるまで 5 分ほど待ってください。

ステップ 5　IDSM-2 がそれでもオンラインにならない場合は、ハードウェアとオペレーティング システムが良好であることを確認してください。

```
router# show test module_number
```

ステップ 6　port ステータスが fail の場合は、IDSM-2 がスイッチ内でしっかり接続されていることを確認します。

ステップ 7　hdd ステータスが fail の場合は、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必要があります。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

IDSM-2 コマンド / コントロール ポートと通信できない

IDSM-2 コマンド / コントロール ポートと通信できない場合は、コマンド / コントロール ポートが正しい VLAN に配置されていない可能性があります。

IDSM-2 のコマンド / コントロール ポートと通信するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　その他のシステムからコマンド ポートを ping できることを確認します。

ステップ 3　IP アドレス、マスク、およびゲートウェイ設定が正しいことを確認します。

```
router# show configuration
```

ステップ 4　コマンド / コントロール ポートが正しい VLAN に置かれていることを確認します。

Catalyst ソフトウェアの場合

```
cat6k> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                      -  Enable                  No Change

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49

Idle Detection
--------------
   --
cat6k> (enable)
```

Cisco IOS ソフトウェアの場合

```
cat6k#show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


cat6k#
```

ステップ 5　コマンド / コントロール ポートが正しい VLAN に置かれていない場合は、正しい VLAN に置いてください。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring the Catalyst 6500 Series Switch for Command and Control Access to the IDSM-2」を参照してください。

TCP リセット インターフェイスの使用方法

IDSM-2 には TCP リセット インターフェイス（ポート 1）があります。IDSM-2 は、センシング ポートに TCP リセットを送信できないので、専用の TCP リセット インターフェイスが用意されています。

IDSM-2 において TCP リセット上の問題が発生した場合は、次の手順を試してください。

- センシング ポートがアクセス ポート（1 つの VLAN）である場合、TCP リセット ポートが同じ VLAN に存在するように設定する必要があります。
- センシング ポートが dot1q トランク ポート（マルチ VLAN）である場合、このセンシング ポートと TCP リセット ポートはすべて同じネイティブ VLAN を持つ必要があり、TCP リセット ポートは両方のセンシング ポートによってトランク接続されている VLAN すべてにトランク接続されている必要があります。

シリアル ケーブルを IDSM-2 に接続する

シリアル ケーブルを IDSM-2 のシリアル コンソール ポートに直接接続することはできません。直接接続すると、スイッチおよびモジュールのネットワーク インターフェイスがバイパスされます。

IDSM-2 にシリアル ケーブルを接続するには、次の手順を実行します。

ステップ 1　IDSM-2 で 2 つの RJ-45 ポートを見つけます。

マザー ボードの中央あたりにあります。モジュールの前面プレートを見ている場合は、右側の RJ-45 ポートがシリアル コンソール ポートです。

ステップ 2　IDSM-2 で右側のポートにストレート ケーブルを接続してから、端末サーバ ポートにケーブルのもう一方の端を接続します。

ステップ 3　端末サーバ ポートを 19200 ボー、8 ビット、パリティなしに設定します。

これで、IDSM-2 に直接ログインできるようになります。

（注）　ケーブルはシャーシの前面から出てくる必要があるので、シリアル ケーブルを IDSM-2 に接続するのは、スイッチ シャーシ内で IDSM-2 の上にモジュールがない場合だけです。

AIP SSM のトラブルシューティング

AIP SSM のソフトウェア アーキテクチャは、4200 シリーズのセンサーと同じです。P.C-5 の「4200 シリーズ アプライアンスのトラブルシューティング」で説明されているのと同じトラブルシューティング ツールを使用できます。

次の項では、AIP SSM のトラブルシューティングに特有のコマンドを示します。

AIP SSM の一般的な健全性情報を確認するには、**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 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

出力には AIP SSM がアップとして示されます。ステータスが Down の場合は、**hw-module module 1 reset** コマンドを使用して AIP SSM をリセットすることができます。

```
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(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
**************************************************
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

AIP SSM のリカバリで問題が生じた場合は、**debug module-boot** コマンドを使用して AIP SSM の起動時の出力を確認できます。TFTP サーバの IP アドレスが正しいことと、TFTP サーバ上のファイルが正しいことを確認します。その後、**hw-module module 1 recover** コマンドを使用して、再度、AIP SSM をリカバリします。

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
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 2005
Slot-1 141> Platform ASA-SSM-10
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=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.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-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
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 2005
Slot-1 161> Platform ASA-SSM-10
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=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.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-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

情報の収集

問題が発生した場合には、次の CLI コマンドとスクリプトを使用して、情報を収集し、センサーの状態を診断できます。**show tech-support** コマンドを使用してすべてのセンサーの情報を収集することもできれば、この項にリストしたその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。

この項で取り上げる事項は次のとおりです。

- テクニカル サポート情報（P.C-56）
- バージョン情報（P.C-59）
- 統計情報（P.C-61）
- インターフェイスの情報（P.C-71）
- イベント情報（P.C-72）
- cidDump スクリプト（P.C-76）
- Cisco FTP サイトのファイルのアップロードとアクセス（P.C-77）

テクニカル サポート情報

すべてのセンサーのステータスおよびコンフィギュレーション情報を取得する場合は、**show tech-support** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-56）
- テクニカル サポート情報の表示（P.C-57）
- Tech Support コマンドの出力（P.C-58）

概要

show tech-support コマンドは、センサーのステータスおよびコンフィギュレーション情報をすべて収集します。収集した情報には、現在のコンフィギュレーション、バージョン情報、および cidDump 情報が含まれます。出力が 1 MB を超えるなど、大きい可能性があります。出力はリモート システムに転送できます。出力をリモート システムにコピーする手順については、P.C-57 の「テクニカル サポート情報の表示」を参照してください。

（注） Monitoring > Support Information > System Information をクリックすることによって、IDM から同じ情報を収集できます。

（注） TAC に問い合せる前に、必ず、**show tech-support** コマンドを実行してください。

テクニカル サポート情報の表示

show tech-support [**page**] [**password**] [**destination-url** *destination-url*] コマンドを使用して、システム情報を画面に表示したり、特定の URL へ送信したりすることができます。この情報は、TAC で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 ページずつ、情報の出力を表示します。

  次の出力行を表示するには **Enter** キーを押し、次のページの情報を表示するには Space キーを押します。
- **password**：パスワードとその他のセキュリティ情報を出力に残します。
- **destination-url**：情報を HTML としてフォーマットし、このコマンドの後に続く宛先に送信するよう指示します。このキーワードを使用した場合、出力は画面に表示されません。
- *destination-url*：情報を HTML としてフォーマットすることを示します。URL は、情報の送信先を指定します。このキーワードを使用しない場合は、情報が画面に表示されます。

テクニカル 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　管理者特権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　画面に出力を表示します。

```
sensor# show tech-support page
```

システム情報が、一度に 1 ページずつ画面に表示されます。次のページを表示するには Space キーを押し、プロンプトへ戻るには **Ctrl+C** キーを押します。

ステップ 3　ファイルへ出力を送信する（HTML 形式で）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入力します。

```
sensor# show tech-support destination-url destination-url
```

次の宛先タイプを指定できます。

- **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、ファイル `/absolute/reports/sensor1Report.html` へテクニカル サポート出力を送信するには、次の手順を実行します。

```
sensor# 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。

Tech Support コマンドの出力

次は、**show tech-support** コマンドの出力例です。

(注) この出力例は、コマンドの最初の部分と、インターフェイス、ARCm および cidDump サービスに関する情報を示しています。

```
sensor# show tech-support page

System Status Report
This Report was generated on Fri Feb 21 03:33:52 2003.
Output from 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 = 2208534
   Total Bytes Received = 157390286
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239437
   Total Bytes Transmitted = 107163351
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0

Output from show statistics networkAccess
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = true
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
```

```
State
   BlockEnable = true

Output from cidDump

cidDiag
CID Diagnostics Report Fri Feb 21 03:33:54 UTC 2003
5.0(1)
<defaultVersions>
<defaultVersion aspect="S">
<version>149.0</version>
<date>2005-03-04</date>
</defaultVersion>
</defaultVersions>
1.1 - 5.0(1)S149
Linux version 2.4.26-IDS-smp-bigphys (csailer@mcq) (gcc version 2.96 20000731 (R
ed Hat Linux 7.3 2.96-112)) #2 SMP Fri Mar 4 04:11:31 CST 2005
 03:33:54 up 21 days, 23:15,  3 users,  load average: 0.96, 0.86, 0.78
--MORE--
```

バージョン情報

センサーの一般的な健全性情報を確認するには、**show version** コマンドが役に立ちます。この項で取り上げる事項は次のとおりです。

- 概要（P.C-59）
- バージョン情報の表示（P.C-59）

概要

show version コマンドは、センサーの一般的な健全性情報を表示し、障害が発生している場所を示すことができます。次の情報を提供します。

- どのアプリケーションが実行中か
- 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使用量
- アプリケーションのアップグレード履歴

（注）**Monitoring > Support Information > Diagnostics Report** をクリックすることで、IDM または ASDM から同じ情報を収集できます。

バージョン情報の表示

show version コマンドを使用して、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、およびシステム上で稼働している IPS プロセスのバージョン情報を表示することができます。システム全体のコンフィギュレーションを表示するには、**more current-config** コマンドを使用します。

バージョンとコンフィギュレーションを表示するには、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。

```
sensor# show version
```

次の例に、アプライアンスと NM-CIDS のバージョン出力のサンプルを示します。

アプライアンスのバージョン出力のサンプル

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(0.29)S135.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 5 days.
Using 722145280 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.3M out of 166.8M bytes of available disk space (23%
usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


Upgrade History:

  IDS-K9-maj-5.0-0.29-S91-0.29-.pkg   03:00:00 UTC Mon Feb 16 2004

Recovery Partition Version 1.1 - 5.0(0.29)S91(0.29)

sensor#
```

NM-CIDS のバージョン出力のサンプル

```
nm-cids# show version
Application Partition:
Cisco Intrusion Prevention System, Version 5.0(0.27)S129.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: NM-CIDS
Serial Number: JAD06490681
No license present
Sensor up-time is 1 day.
Using 485675008 out of 509448192 bytes of available memory (95% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 31.1M out of 166.8M bytes of available disk space (20%
usage)
boot is using 39.5M out of 68.6M bytes of available disk space (61% usage)
application-log is using 529.6M out of 2.8G bytes of available disk space (20% usage)


MainApp          2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
AnalysisEngine   2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
CLI              2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600


Upgrade History:

  IDS-K9-maj-5.0-0.27-S91-0.27-.pkg   03:00:00 UTC Thu Feb 05 2004

Recovery Partition Version 1.1 - 5.0(0.27)S91(0.27)

nm-cids#
```

（注） --MORE-- プロンプトが表示されたら、Space キーを押して次の情報を表示するか、**Ctrl+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　コンフィギュレーション情報を表示します。

（注） **more current-config** または **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Version 5.0(0.26)
! Current configuration last modified Wed Feb 16 03:20:54 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on banner login.
exit
time-zone-settings
--MORE--
```

統計情報

センサーのサービスの状態を調べるには、**show statistics** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-61）
- 統計情報の表示（P.C-62）

概要

show statistics コマンドは、センサーのサービスの状態のスナップショットを提供します。次の統計情報を提供します。

- 分析エンジン
- 認証
- 拒否された攻撃者
- イベント サーバ
- イベント ストア

- ホスト
- ロガー
- 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
- 仮想センサー
- Web サーバ

（注） **Monitoring > Support Information > Statistics** をクリックすることによって、IDM から同じ情報を収集できます。

統計情報の表示

show statistics virtual-sensor [**clear**] コマンドを使用して、仮想サーバの統計情報を表示できます。**show statistics [analysis-engine** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **host** | **logger** | **network-access** | **notification** | **sdee-server** | **transaction-server** | **transaction-source** | **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生成できます。

（注） **clear** オプションは、分析エンジン、ホスト、またはネットワーク アクセス アプリケーションには使用できません。

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　仮想センサーの統計情報を表示します。

```
sensor# 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 = fe0_1
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1675
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 241
         Total IP packets processed since reset = 12
         Total packets that were not IP processed since reset = 229
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 12
         Total packets that were not TCP, UDP, or ICMP processed since reset = 0
         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 = 22513
```

```
   The rate of packets per second since reset = 0
   The rate of bytes per second since reset = 13
   The average bytes per packet since reset = 93
Denied Address Information
   Number of Active Denied Attackers = 0
   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 = 0
Denied Attackers 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 = 28
      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 = 6
   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 constraints
      TCP nodes keyed on both IP addresses and both ports = 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 = 491
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 6
   Number of FireOnce Intermediate Alerts = 480
   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 = 491
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-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
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
   Actions Filtered
      deny-attacker-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
SigEvent Action Handling Stage Statistics.
   Number of Alerts received to Action Handling Processor = 491
   Number of Alerts where produceAlert was forced = 0
   Number of Alerts where produceAlert was off = 0
   Actions Performed
      deny-attacker-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 = 11
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 5
      request-snmp-trap = 0
      reset-tcp-connection = 0
   Deny Actions Requested in Promiscuous Mode
      deny-packet not performed = 0
```

```
            deny-connection not performed = 0
            deny-attacker not performed = 0
            modify-packet not performed = 0
         Number of Alerts where deny-connection was forced for deny-packet action = 0
         Number of Alerts where deny-packet was forced for non-TCP deny-connection
action = 0
      Per-Signature SigEvent count since reset
         Sig 2004 = 5
         Sig 2156 = 486
sensor#
```

ステップ 3　分析エンジンの統計情報を表示します。

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1999
   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 = 13
   Receiver Statistics
      Total number of packets processed since reset = 290
      Total number of IP packets processed since reset = 12
   Transmitter Statistics
      Total number of packets transmitted = 290
      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 = 491
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 11
sensor#
```

ステップ 4　認証の統計情報を表示します。

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 2
   failedAuthenticationAttempts = 0
sensor#
```

ステップ 5　システム内で拒否された攻撃者の統計情報を表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
sensor#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
sensor# 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
sensor#
```

ステップ 8　ホストの統計情報を表示します。

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05  Thu Feb 10 2005
   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 = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
sensor#
```

ステップ 9　ロギング アプリケーションの統計情報を表示します。

```
sensor# 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
sensor#
```

ステップ 10 ARC の統計情報を表示します。

```
sensor# 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-des
   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 =
sensor#
```

ステップ 11 通知アプリケーションの統計情報を表示します。

```
sensor# 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
sensor#
```

ステップ 12 SDEE サーバの統計情報を表示します。

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

ステップ 13 トランザクション サーバの統計情報を表示します。

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

ステップ 14 トランザクション ソースの統計情報を表示します。

```
sensor# show statistics transaction-source
General
   totalControlTransactions = 0
   failedControlTransactions = 0
sensor#
```

ステップ 15 Web サーバの統計情報を表示します。

```
sensor# 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
sensor#
```

ステップ 16 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するには、次の手順を実行します。

```
sensor# 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
```

統計情報が検出され、クリアされました。

ステップ 17 統計情報がクリアされたことを確認します。

```
sensor# 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
sensor#
```

統計情報はすべて 0 から始まります。

インターフェイスの情報

検知インターフェイス、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には、**show interfaces** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-71）
- インターフェイス コマンドの出力（P.C-72）

概要

show interfaces コマンドを使用して、次の情報を学習できます。

- インターフェイスが起動しているか停止しているか
- パケットが表示されているかどうかと、どのインターフェイスに表示されているか
- パケットが SensorApp によってドロップされているかどうか
- パケットのドロップにつながるエラーがインターフェイスによって報告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、個別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*）、検知インターフェイス（**show interfaces** *interface_name*）のそれぞれの統計情報を表示することもできます。

インターフェイス コマンドの出力

次は、**show interfaces** コマンドの出力例です。

```
sensor# 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
sensor#
```

イベント情報

show events コマンドを使用して、SensorApp によって生成されたアラートと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。

この項で取り上げる事項は次のとおりです。

- センサー イベント（P.C-73）
- 概要（P.C-73）
- 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 イベント

イベントには、次の 5 つのタイプがあります。

- evAlert：侵入検知アラート
- evError：アプリケーション エラー
- evStatus：IP ログを作成中など、ステータスの変化
- evLogTransaction：各センサー　アプリケーションによって処理される制御トランザクションのレコード
- evShunRqst：ブロック要求

イベントは、新しいイベントに上書きされるまでイベント ストア内に残ります。

概要

イベント ビューアやセキュリティ モニタでイベントが表示されないなどのイベント取り込み問題をトラブルシューティングする場合には、**show events** コマンドが役に立ちます。**show events** コマンドを使用すると、センサー上でどのイベントが生成されたかを判断し、生成されたイベントと障害がモニタリング側にあることを確認できます。

clear events コマンドを使用して、イベント ストアのすべてのイベントをクリアできます。

show events コマンドのパラメータは次のとおりです。

```
sensor# 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***]] | **error** [warning] [error] [fatal] | **log** | **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できます。

開始時刻から、イベントが表示されます。開始時刻を指定しない場合は、現在時刻から、イベントが表示されます。イベント タイプを指定しない場合は、すべてのイベントが表示されます。

（注） イベントは、**Ctrl+C** キーを押して要求をキャンセルするまで、ライブ フィードとして表示されます。

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こと、または攻撃が試みられたことを示している可能性のある不審なアクティビティを通知します。

  レベル（informational、low、medium、または high）が選択されていない場合は、すべてのアラート イベントが表示されます。
- **include-traits**：指定した特性を持つアラートを表示します。

- **exclude-traits**：指定した特性を持つアラートを表示しません。
- **traits**：10 進数（0 ～ 15）で表した特性ビットの位置。
- **error**：エラー イベントを表示します。エラー イベントは、エラー条件が発生したときにサービスによって生成されます。
- **log**：ログ イベントを表示します。ログ イベントは、トランザクションが受信され、アプリケーションの応答があったときに生成されます。トランザクションの要求、応答、および成功または失敗に関する情報が含まれています。
- **NAC**：ARC（ブロック）要求を表示します。
- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、分数、秒数の間に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、指定されたイベントが使用可能になるまで待機します。**Ctrl+C** キーを押して終了するまで、イベントの待機と表示は継続します。

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　現在開始されているすべてのイベントを表示します。

```
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2003/01/07 04:41:45 2003/01/07 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: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

フィードは、**Ctrl+C** キーを押すまですべてのイベントを表示し続けます。

ステップ 3　2005 年 2 月 9 日の午前 10 時から、ブロック要求を表示します。

```
sensor#@ show events NAC 10:00:00 Feb 9 2005
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2005/02/09 10:33:31 2004/08/09 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
sensor#
```

ステップ 4　2005 年 2 月 9 日の午前 10 時から、警告レベルのエラーを表示します。

```
sensor# show events error warning 10:00:00 Feb 9 2005
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2003/01/07 04:49:25 2003/01/07 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。

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2005/03/02 14:15:59 2005/03/02 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　過去 30 秒間に始まったイベントを表示します。

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2003/01/08 02:41:00 2003/01/08 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: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

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　管理者特権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。

```
sensor# 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 または CLI へのアクセス権限がない場合は、root としてログインして /usr/cids/idsRoot/bin/cidDump を実行することによって、基盤となるスクリプト cidDump をサービス アカウントから実行できます。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、設定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 サービス アカウントにログインします。

ステップ 2　su と入力し、サービス アカウント パスワードを使用して root になります。

ステップ 3　cidDump /usr/cids/idsRoot/bin/cidDump と入力します。

ステップ 4　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　問題が発生した場合は、結果として生成される HTML ファイルを TAC または IPS 開発者に送信します。

手順については、P.C-77 の「Cisco FTP サイトのファイルのアップロードとアクセス」を参照してください。

Cisco FTP サイトのファイルのアップロードとアクセス

サイズの大きいファイル、たとえば、cidDump.html、show tech-support コマンドの出力、コア ファイルなどを ftp-sj サーバにアップロードできます。

Cisco FTP サイトでファイルのアップロードやアクセスを実行するには、次の手順を実行します。

ステップ 1　anonymous として ftp-sj.cisco.com にログインします。

ステップ 2　/incoming ディレクトリに移動します。

ステップ 3　ファイルをアップロードするには、**put** コマンドを使用します。

バイナリ転送タイプを使用していることを確認します。

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 にサポートされたホストとしてログインします。

ステップ 5　/auto/ftp/incoming ディレクトリに移動します。

A

aaa
認証、認可、アカウンティング（authentication, authorization, and accounting）。Cisco IOS ソフトウェアと PIX ファイアウォールのコマンドで、ユーザがルータまたは PIX ファイアウォールにログインする方法を制御します。

AAA
認証、認可、アカウンティング（authentication, authorization, and accounting）。「トリプルエー」と発音します。

ACE
アクセス コントロール エントリ（Access Control Entry）。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（acknowledgement）。何かのイベントが発生した場合に、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（メッセージの受信など）。

ACL
アクセス コントロール リスト（Access Control List）。ルータ経由のデータ フローを制御する 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。

AIC エンジン
Application Inspection and Control エンジン。Web トラフィックの詳細な分析を行います。HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。たとえばインスタント メッセージや、gotomypc などのトンネリング アプリケーションなど、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。

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。ASA を参照。

API
アプリケーション プログラミング インターフェイス（Application Programming Interface）。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を行うために使用するインターフェイス。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しないでアプリケーション 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の割り込み、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、または他のプログラム間の通信）。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。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。

ARP
アドレス レゾリューション プロトコル（Address Resolution Protocol）。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。RFC 826 で定義されています。

ASA
適応型セキュリティ アプライアンス（Adaptive Security Appliance）。ASA は、ファイアウォール、VPN コンセントレータ、侵入防御ソフトウェアの機能を 1 つのソフトウェア イメージに結合します。シングルモードまたはマルチモードのいずれでも ASA を設定できます。

ASDM
Adaptive Security Device Manager。ASA 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。

ATOMIC エンジン
ATOMIC エンジンは、2 種類あります。ATOMIC.IP は IP プロトコルおよび関連付けられているレイヤ 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。

AuthenticationApp
IPS のコンポーネントの 1 つ。ユーザが、CLI、IDM、または RDEP のアクションを実行するための適切な権限を持っていることを確認します。

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。

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
ブリッジ プロトコル データ ユニット（Bridge Protocol Data Unit）。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機関です。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。

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、設定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ます。

CIDS ヘッダー
IPS システム内の各パケットに付けられるヘッダー。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、中央集中型で統合され自動化されたインストレーションおよびインターネットワークの管理を可能にするだけでなく、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（Command Line Interface）。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。

Cookie
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。

D

Database Processor
「DBP」を参照。

DBP
データベース プロセッサ（Database Processor）。シグニチャ状態とフロー データベースを管理します。

DCE データ回線終端装置（data circuit-terminating equipment）（ITU-T 拡張）。ユーザからネットワークへのインターフェイスのネットワーク終端を構成する、通信ネットワークのデバイスおよび接続。DCE はネットワークへの物理的接続を提供し、トラフィックを転送し、DCE デバイスと DTE デバイスとの間のデータ伝送の同期に使用するクロック信号を提供します。DCE には、モデムやインターフェイス カードなどがあります。

DDoS 分散 DoS（Distributed Denial of Service）。脆弱性が生じた複数のシステムが単一の対象を攻撃した結果、対象になったシステムのユーザがサービスを拒絶されること。対象システムが受信する大量のメッセージによってシステムが強制的にシャットダウンすることにより、正当なユーザのシステムへのサービスが拒絶されます。

Deny Filters Processor 「DFP」を参照。

DES データ暗号規格（Data Encryption Standard）。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。

DFP Deny Filters Processor。拒否攻撃者機能を処理します。拒否された送信元 IP アドレスのリストを管理します。

DIMM デュアル インライン メモリ モジュール（Dual In-line Memory Modules）。

DMZ 非武装地帯（demilitarized zone）。プライベート ネットワーク（内部）とパブリック ネットワーク（外部）と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 サービス拒絶（Denial of Service）。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（dynamic random-access memory）。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。

E

ESD 静電放電（Electrostatic discharge）。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。

Ethereal Ethereal 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。Ethereal 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.ethereal.com を参照してください。

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

false negative 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。

false positive 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。

Flood エンジン ホストおよびネットワークを宛先とする ICMP および UDP フラッドを検出します。

Fragment Reassembly Processor 「FRP」を参照。

FRP Fragment Reassembly Processor。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。

FTP ファイル転送プロトコル（File Transfer Protocol）。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 プロトコルで、ネットワーク ノード間のファイル転送に使用されます。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 スイッチにインストールできるモジュール。**shun** コマンドを使用してブロックを行います。シングルモードまたはマルチモードのいずれでも FWSM を設定できます。

G

GMT グリニッジ標準時（Greenwich Mean Time）。経度 0 の時間帯。現在では、世界標準時（UTC）と呼ばれます。

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。実際に、H.225.0 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を定めています。

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ます。

HTTP ハイパーテキスト転送プロトコル（Hypertext Transfer Protocol）。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 インターネット制御メッセージ プロトコル（Internet Control Message Protocol）。ネットワーク層のインターネット プロトコルで、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 で定義されています。

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（サービス拒絶攻撃）。

IDAPI 侵入検知アプリケーション プログラミング インターフェイス（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 Configurarion。侵入検知システムおよび侵入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規格です。

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。Netscape または Internet Explorer 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。

IDSM-2 侵入検知システム モジュール（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。

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。

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 log EventAction が選択されている場合に作成されます。iplog は、Ethereal または 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（Intrusion Prevention System）。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 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 version 6。現在のバージョンの IP（version 4）に置き換えられます。IPv6 では、パケット ヘッダー内のフロー ID がサポートされます。これは、フローを識別するために使用されます。以前の名称は、IPng（next generation）です。

IP アドレス TCP/IP を使用しているホストに割り当てられる 32 ビットのアドレス。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、サブネット番号（オプション）、およびホスト番号で構成されます。ネットワーク番号とサブネットワーク番号は、ともにルーティングに使用され、ホスト番号はネットワークまたはサブネットワーク内の個々のホストのアドレス指定に使用されます。サブネット マスクは、IP アドレスからネットワーク情報およびサブネットワーク情報を取り出すために使用されます。

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。

L

L2P Layer 2 Processor。レイヤ 2 関連イベントを処理します。また、異常形式のパケットを識別し、処理パスから削除します。

Layer 2 Processor 「L2P」を参照。

LOKI リモート アクセスのバック ドア型トロイの木馬。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、悪質なコードによって小さなペイロードの ICMP 応答の送信に使用する 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。

MD5
Message Digest 5。128 ビット ハッシュを作成する一方向のハッシュ アルゴリズム。MD5 と Secure Hash Algorithm（SHA）は、MD4 のバリエーションで、MD4 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 フレームワーク内の認証にハッシュを使用しています。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は、通信の整合性を確認し、発信元を認証して、適時性をチェックします。

MEG
Mega Event Generator。META エンジンに基づいたシグニチャ。META エンジンは、アラームをパケットではなく入力と見なします。

Meta エンジン
スライドする時間間隔内で、関連する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（Management Information Base）。SNMP または 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管理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、通常 GUI ネットワーク管理システムから SNMP または CMIP コマンドを使用して変更または取得できます。MIB オブジェクトは、public（標準）ブランチおよび private（独自仕様）ブランチを含むツリー構造で構成されています。

MIME
多目的インターネット メール拡張（Multipurpose Internet Mail Extension）。インターネット メールで非テキスト データ（プレーン ASCII コードでは表現できないデータ）を伝送する場合の標準。たとえば、バイナリ、外国語テキスト（ロシア語、中国語など）、オーディオ、ビデオなどのデータがあります。MIME は、RFC 2045 で定義されています。

MSFC、MSFC2
Multilayer Switch 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、スイッチの L3 ルーティングを実行します。

MSRPC
マイクロソフト リモート プロシージャ コール（Microsoft Remote Procedure Call）。

N

NAC
Network Access Controller。ARC を参照。

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
次の営業日。Cisco サービス契約に従った交換用ハードウェアの到着。

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（Network Interface Card）。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。

NM-CIDS
IPS の機能を支社のルータに統合するネットワーク モジュール。

NMS
ネットワーク管理システム（network management system）。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。一般に、NMS にはエンジニアリング ワークステーションなど、十分に高機能なコンピュータを使用します。NMS はエージェントと通信して、ネットワークの統計情報やリソース情報を把握します。

Normalizer エンジン
IP および TCP の正規化エンジンがどのように機能するかを設定し、IP および TCP の正規化エンジンに関連するシグニチャ イベントの設定を行います。

NSDB Network Security Database。IPS が使用するシグニチャと、そのシグニチャの根拠となっている脆弱性を説明したセキュリティ情報のデータベースです。NSDB には、センサーで検出可能な各攻撃シグニチャの説明が含まれます。

NTP ネットワーク タイム プロトコル（Network Timing Protocol）。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。

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 不揮発性読み取り / 書き込みメモリ（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（online insertion and removal）。システムの電源を切ったり、コンソール コマンドを入力したり、他のソフトウェアまたはインターフェイスをシャットダウンしないで、カードの追加、交換、または取り外しを可能にする機能です。

P

PASC 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 以外のポートに接続しようとする試み。これは、認証されていない接続を開始することにより、ファイアウォールが FTP 227（パッシブモードに入る）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（Port Address Translation）。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。

PCI 周辺コンポーネント インターフェイス（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（protocol data unit）。OSI の用語で、パケットを表します。「BPDU」、「パケット」も参照。

PEP Cisco Product Evolution Program。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（packed encoding rules）。PER は、一般的なスタイルを使用して同じ方法ですべてのタイプを符号化するのではなく、日付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リングをサポートします。

PID Product Identifier。注文可能な製品の識別番号。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。ICMP の echo メッセージとその応答。ネットワーク デバイスへの到達状況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。

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 公開鍵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。

POST パワーオン セルフテスト（Power-On Self Test）。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、保持、および終了のシグナリングを行う ITU-T の仕様。

R

RAM ランダムアクセス メモリ（random-access memory）。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。

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の間で使用されるプロトコル。RAS シグナリング機能は、登録、許可、帯域幅の変更、ステータス、および VoIP ゲートウェイとゲートキーパー間の接続解除手順を実行します。

RDEP2 Remote Data Exchange Protocol version 2。コマンド / コントロール ネットワーク上で HTTP と TLS を使用してリモート データ交換を行うための公開仕様です。

regex 「正規表現」を参照。

ROMMON 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（remote-procedure call）。クライアント / サーバ コンピューティングの技術的基盤。RPC は、クライアントで生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。

RR リスク評価（Risk Rating）。RR 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、0 から 100 の間の数値で表した評価です。

RSM Router Switch Module。Catalyst 5000 スイッチにインストールされているルータ 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 リアルタイム転送プロトコル（Real-Time Transport Protocol）。一般に、IP ネットワークで使用されます。RTP は、オーディオ、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、タイムスタンプの付加、およびリアルタイム アプリケーションへのモニタリング送信などのサービスを提供します。

RU ラック単位。ラックは、ラック単位で測定します。1 RU は、44 mm つまり 1.75 インチです。

S

SAP
Signature Analysis Processor。ストリーム ベースでなく、処理中のパケットのために設定されているインスペクタにパケットを送信します。

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、シスコシステムズの 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。

SDEE
Security Device Event Exchange。セキュリティ デバイス イベントの通信を行うための、製品に依存しない標準。RDEP の拡張です。各種のセキュリティ デバイスによって生成された通信イベントに必要な拡張機能を追加します。SDEE プロトコルの詳細については、http://www.icsalabs.com/html/communities/ids/sdee/index.shtml を参照してください。

SDP
Slave Dispatch Processor。

SEAF
シグニチャ イベント アクション フィルタ（signature event action filter）。シグニチャ イベントのシグニチャ ID、アドレス、および RR に基づいてアクションを削除します。SEAF へ入力するのは、SEAO 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。

SEAH
シグニチャ イベント アクション ハンドラ（signature event action handler）。要求されたアクションを実行します。SEAH 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。

SEAO
シグニチャ イベント アクション オーバーライド（signature event action override）。RR 値に基づいて、アクションを追加します。SEAO は、設定済みの RR しきい値の範囲に該当するすべてのシグニチャに適用されます。各 SEAO 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。

SEAP
Signature Event Action Processor。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 リスク評価（RR）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。

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、およびレポート実行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。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探します。パケットは、プロセッサのパイプラインを通過します。このパイプラインは、設計者が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します。Sensorapp は、分析エンジンを実行するスタンドアロンの実行ファイルです。

Service エンジン
DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SL、NTP、RPC、SMB、SNMP、および SSH など、特定のプロトコルを処理します。

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。

shun コマンド
新しい接続を防止し、既存の全接続からのパケットを許可しないことにより、攻撃中のホストへの動的な対応を可能にします。PIX ファイアウォールによるブロッキング時に ARC によって使用されます。

Signature Analysis Processor
「SAP」を参照。

signature event action filter
「SEAF」を参照。

signature event action handler
「SEAH」を参照。

signature event action override
「SEAO」を参照。

Signature Event Action Processor 「SEAP」を参照。

Slave Dispatch Processor 「SDP」を参照。

SMB サーバ メッセージ ブロック（Server Message Block）。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 マネージャおよび同様の NOS が使用するファイル システム プロトコル。

SMTP シンプル メール転送プロトコル（Simple Mail Transfer Protocol）。電子メール サービスを提供するインターネット プロトコル。

SN シリアル番号（Serial Number）。UDI の一部。SN は、ご使用のシスコ製品のシリアル番号です。

SNMP 簡易ネットワーク管理プロトコル（Simple Network Management Protocol）。TCP/IP ネットワークでほとんど独占的に使用されているネットワーク管理プロトコル。SNMP は、ネットワーク デバイスのモニタリングおよび制御、コンフィギュレーション、統計情報の収集、パフォーマンス、セキュリティの管理を行う手段を提供します。

SNMP2 SNMPv2。ネットワーク管理プロトコルのバージョン 2。SNMP2 は、中央集中型および分散型のネットワーク管理戦略をサポートし、SMI、プロトコル操作、管理アーキテクチャ、およびセキュリティにおいて改善されています。

SP Statistics Processor。パケットのカウントや、パケットの到達率など、システム統計情報を継続して追跡します。

SPAN スイッチド ポート アナライザ（Switched Port Analyzer）。Catalyst 5000 スイッチの機能。既存のネットワーク アナライザの監視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監視できます。

SQL 構造化照会言語（Structured Query Language）。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。

SRAM RAM の一種。電源が供給されている限り、内容を保持します。SRAM は、DRAM のように定期的なリフレッシュは必要ありません。

SRP Stream Reassembly Processor。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。正規化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有効または無効にできます。

SSH Secure Shell。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。

Statistics Processor 「SP」を参照。

Stream Reassembly Processor 「SRP」を参照。

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。シスコが強化した専用の Terminal Access Controller Access Control System（TACACS）。認証、認可、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（Transmission Control Protocol）。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。

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。

TCP リセット インターフェイス　TCP リセットを送信できる、IDS-4250-XL および IDSM-2 上のインターフェイス。ほとんどのセンサーでは、パケットが監視されるセンシング 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、IDS-4250-XL と 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。IDS-4250-XL では、オンボードの 10/100/100 TX インターフェイスが TCP リセット インターフェイスになります。このインターフェイスは、通常、XL カードが存在しない場合に IDS-4250-TX アプライアンスで使用されます。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。

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。

TFN2K　Tribe Flood Network 2000。一般的なタイプの DoS 攻撃。偽造した送信元 IP アドレスを利用するか、または送信元 IP アドレスを素早く変更して、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。

Time Processor　「TP」を参照。

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。

TP　Time Processor。タイムスライス カレンダ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 エントリを廃棄し、時間に依存する統計を計算することです。

TPKT　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 RFC 1006 によって定義された方式。

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、および DDOS など、非標準の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、非標準のプロトコルからのトラフィックを分析します。

trusted certificate 検証テストを行わずに証明書ユーザが有効であることを示す証明書。特に公開鍵証明書は、認証パスの最初の公開鍵を提供するために使用されます。

trusted key ユーザが信頼する公開鍵。特に、認証パスで最初の公開鍵として使用される公開鍵。

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 ID PROM に保存されています。

UDP ユーザ データグラム プロトコル（User Datagram Protocol）。TCP/IP プロトコル スタックにおけるコネクションレス型トランスポート層プロトコル。UDP は、確認応答や配信保証を行わずにデータグラムを交換するシンプルなプロトコルで、エラー処理や再送信は他のプロトコルによって行う必要があります。UDP は RFC 768 で定義されています。

UPS 無停電電源（Uninterruptable Power Source）。

UTC 世界標準時（Coordinated Universal Time）。経度 0 の時間帯。以前は、グリニッジ標準時（GMT）およびズールー時（Zulu time）と呼ばれていました。

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）をフィルタリングする ACL。セキュリティ ACL とも言います。

VID バージョンの識別番号（Version identifier）。UDI の一部。

VLAN バーチャル LAN（Virtual Local Area Network）。1 つまたは複数の LAN 上にある設定済みのデバイスのグループ（管理ソフトウェアを使用して設定）。VLAN によって、これらが実際は複数の異なる LAN セグメントに配置されていても、同一のワイヤ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いており、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。通常のテレフォニー型音声を、POTS に類似した機能、信頼性、および音声品質を保持して、IP ベースのインターネットで伝送する機能。VoIP は、IP ネットワーク上でルータが音声トラフィック（たとえば、電話による通話やファックス）を伝送できるようにします。VoIP では、DSP が音声信号をフレームにセグメント化し、2 つからなるグループにカップリングしてボイス パケットに格納します。これらのボイス パケットは、ITU-T 仕様 H.323 に準拠する IP を使用して伝送されます。

VPN バーチャル プライベート ネットワーク（Virtual Private Network(ing)）。ネットワークからネットワークへのすべてのトラフィックを暗号化することにより、IP トラフィックが安全にパブリック TCP/IP ネットワーク上を送信されるようにします。VPN は「トンネリング」を使用して IP レベルのすべての情報を暗号化します。

W

WAN ワイドエリア ネットワーク（wide-area network）。広い地域にいるユーザ間を接続するデータ通信ネットワークで、多くの場合コモン キャリアによって提供される伝送デバイスを使用します。WAN の例としては、フレーム リレー、SMDS、および X.25 などがあります。

Web サーバ IPS のコンポーネントの 1 つ。

X

X.509 証明書に含まれる情報を定義する規格。

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。

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。可能なアクションには、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 パケットの取り込みなどがあります。

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。

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。

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使用を表します。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、受信したイベントごとにアラートを生成することです。

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。

暗号化鍵 クリア テキスト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化鍵が使用される場合を対称と言います。暗号化鍵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 サーバ IPS のコンポーネントの 1 つ。

イベント ストア IPS のコンポーネントの 1 つ。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。

インターフェイス グループ　センシング インターフェイスの論理的なグループ。1 つの論理インターフェイス グループに複数のセンシング インターフェイスを割り当てることができます。シグニチャのパラメータは、論理インターフェイス グループごとに調整されます。

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は、センサーを経由する必要があります。

う

ウイルス　コンピュータ ソフトウェアの隠された自己複製可能なセクション。通常は悪意のあるロジックになっており、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。

え

エスケープ表現　正規表現で使用されます。文字は 16 進値で表現できます。たとえば、\x61 は「a」に相当するため、\x61 は文字「a」を表すエスケープ表現になります。

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。プライベートに所有および管理されるという点で、WAN とは異なります。

か

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。IPS 5.x では、1 つの仮想センサーだけがサポートされます。

き

ギガビット イーサネット　高速イーサネットの標準。1996 年に、IEEE（Institute of Electrical and Electronics Engineers）802.3z 標準化委員会で承認されました。

こ

攻撃　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。

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 において、同一の管理ドメイン内にある管理対象デバイスと NMS の論理グループ。

混合モード　ネットワーク セグメントのパケットを監視する受動インターフェイス。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。

コンソール　センサーの監視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またがる攻撃です。たとえば、FTP、Telnet、およびほとんどの Regex ベース攻撃などの大部分の対話型攻撃が、これに該当します。

さ

サービス パック　新しい機能強化を伴わないバグ フィックスのリリースに使用されます。サービス パックは、ベース バージョンのリリース（マイナーまたはメジャー）の後で、複数のプログラムが累積した形で提供されるものです。

再構成　送信元または中間ノードのいずれかでフラグメント化された IP データグラムを、宛先でまとめること。

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、広い範囲のシグニチャをさらに詳しく定義します。

し

しきい値　アラーム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　IPS のシグニチャ分析エンジン（SensorApp）と NSDB をアップデートする実行可能イメージ。IPS シグニチャ アップデートの適用は、ウイルス スキャン プログラムでのウイルス定義の更新と似ています。シグニチャ アップデートは単独でリリースされ、独自のバージョン体系になっています。

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から構成されます。各エンジンには、許容可能な範囲または値のセットからなる有効パラメータのセットがあります。

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。

出トラフィック　ネットワークから出るトラフィック。

証明書　ユーザまたはデバイスの属性をデジタルに表現したもの。認証可能な秘密鍵とともに署名される公開鍵などがあります。

侵入検知システム　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ことを目的として、システム イベントの監視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、およびフラッドするネットワーク デバイス。このスイッチは、OSI モデルのデータリンク層で動作します。

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。

せ

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 マッチングのために、正規表現では任意のパターンを簡潔に記述できます。

制御インターフェイス NAC では、ネットワーク デバイスと Telnet セッションまたは 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 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には、*start*、*stop*、*getConfig* などがあります。

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 つ以上のアトリビュート。

セキュア シェル プロトコル Transmission Control Protocol（TCP; 伝送制御プロトコル）アプリケーションを通じて、ルータに安全なリモート接続を提供するプロトコル。

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。

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 セグメントを監視する、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、監視したセグメント上では見えません。

全二重 送信端末と受信端末との間で、同時にデータを伝送する機能。

そ

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。

た

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。

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。

て

データグラム
事前にバーチャル サーキットを確立することなく、伝送メディアを介してネットワーク レイヤ単位として送信される情報を論理的にグループ化すること。IP データグラムは、インターネットの主な情報単位です。また、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は、OSI 参照モデルやさまざまな技術領域の各種レイヤで、論理的にグループ化した情報を説明するために使用されます。

と

トポロジ
エンタープライズ ネットワーク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、または端末に送信されるメッセージ。特別に定義された条件に合致する、またはしきい値に到達するなど、重大なイベントの発生を示します。

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、送信元と宛先（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。

トランザクション サーバ
IPS のコンポーネントの 1 つ。

トランザクション ソース
IPS のコンポーネントの 1 つ。

トリプル DES
トリプル データ暗号規格（Triple 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。

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する機能を持つデバイス。ネットワーク デバイスには、Cisco ルータや PIX ファイアウォールなどがあります。

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。

は

バイパス モード
センサーに障害が発生した場合でも、センサーを通じてパケットのフローを継続するモード。バイパス モードは、インラインで組み合されたインターフェイスに対してのみ適用されます。

パケット
制御情報および（通常は）ユーザ データを含むヘッダーなどの情報を論理的にグループ化したもの。パケットは、ネットワーク レイヤ単位のデータを参照するために最も多く使用されます。また、データグラム、フレーム、メッセージ、およびセグメントという用語は、OSI 参照モデルやさまざまな技術領域の各種レイヤで、論理的にグループ化した情報を説明するために使用されます。

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。

パッシブ フィンガープリント
ネットワークのインタラクション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。

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。

半二重
送信端末と受信端末との間で、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例です。

ふ

ファースト イーサネット
100 Mbps イーサネット仕様の任意の数値。ファースト イーサネットは、10BaseT イーサネット仕様の 10 倍の速度を提供し、フレーム形式、MAC メカニズム、および MTU などの品質を維持します。このように 10BaseT と類似しているため、既存の 10BaseT アプリケーションやネットワーク管理ツールをファースト イーサネット ネットワークで使用できます。IEEE 802.3 仕様の拡張をベースにしています。

ファイアウォール
ルータまたはアクセス サーバ、あるいは複数のルータまたはアクセス サーバ。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ます。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。

フラグメンテーション
元のサイズのパケットを維持できないネットワーク メディア上を伝送する際に、より小さい単位にパケットを分割する処理。

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。

フラッディング
スイッチおよびブリッジが使用するトラフィック転送技術のことで、あるインターフェイスで受信されたトラフィックは、そのデバイスにおいて情報を最初に受信したインターフェイス以外のすべてのインターフェイスに送出されます。

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。

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プし、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プします。パケット分析とアラート検知を実行します。

へ

平面設置
平らな面に設置する場合は、センサー底部にゴム製脚を取り付けます。ゴム製脚を使用すると、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。

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 バージョン アップグレードは、ベース バージョン リリースです。

ほ

ホスト ブロック
ARC が特定 IP アドレスからのすべてのトラフィックをブロックすること。

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。

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 イメージ
IDSM-2 のメンテナンス パーティションのイメージの再作成に使用される IPS の完全なイメージ。

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できるカード。AIP SSM、IDSM-2、および NM-CIDS 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 パーティション イメージ
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 イメージ。センサーで復旧に使用されます。

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。

ろ

ロガー
IPS のコンポーネントの 1 つ。

ロギング
ログ ファイル内に、発生したアクションを収集します。セキュリティ情報のロギングは、イベント（IPS のコマンド、エラー、およびアラート）のロギングと、個々の IP セッション情報のロギングという 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、完全に動作するバージョンのプログラムを、ネットワークの他のホストに増殖させることができ、コンピュータ リソースを非常に多く消費します。

A

ACL
- Post-Block 8-27, 8-28
- Pre-Block 8-27, 8-28
- 説明 8-3

Active Host Blocks パネル
- 設定 8-16, 8-44, 11-6, 11-13
- 説明 8-42, 11-4
- フィールド定義 8-42, 11-4
- ボタンの機能 8-42, 11-4
- ユーザのロール 8-42, 11-4

Add Active Host Block ダイアログボックス
- フィールド定義 8-43, 11-5
- ボタンの機能 8-43, 11-5

Add Allowed Host ダイアログボックス
- ユーザのロール 2-5

Add Authorized Key ダイアログボックス
- ユーザのロール 2-9

Add Blocking Device ダイアログボックス
- ユーザのロール 8-22

Add Cat 6K Blocking Device Interface ダイアログボックス
- ユーザのロール 8-34

Add Device Login Profile ダイアログボックス
- ユーザのロール 8-18

Add Event Action Filter ダイアログボックス
- ユーザのロール 7-22

Add Event Action Overrides ダイアログボックス
- ユーザのロール 7-17

Add Event Variable ダイアログボックス
- ユーザのロール 7-11

Add Interface Pair ダイアログボックス
- フィールド定義 3-15
- ボタンの機能 3-15
- ユーザのロール 3-14

Add Known Host Key ダイアログボックス
- ユーザのロール 2-12

Add Master Blocking Sensor ダイアログボックス
- ユーザのロール 8-38

Add Never Block Address ダイアログボックス
- ユーザのロール 8-9

Add Router Blocking Device Interface ダイアログボックス
- ユーザのロール 8-29

Add Signature Variable ダイアログボックス
- ユーザのロール 5-3

Add Signature ダイアログボックス
- ユーザのロール 5-6

Add SNMP Trap Destination ダイアログボックス
- ユーザのロール 9-5

Add Target Value Rating ダイアログボックス
- ユーザのロール 7-14

Add Trusted Host ダイアログボックス
- フィールド定義 2-18
- ボタンの機能 2-18
- ユーザのロール 2-17

Add User ダイアログボックス
- ユーザのロール 2-29

Add/Edit Allowed Host ダイアログボックス
- フィールド定義 2-6
- ボタンの機能 2-6

Add/Edit Authorized Key ダイアログボックス
- フィールド定義 2-10
- ボタンの機能 2-10

Add/Edit Cat 6K Blocking Device Interface ダイアログボックス
- フィールド定義 8-35
- ボタンの機能 8-35

Add/Edit Event Action Overrides ダイアログボックス
- フィールド定義 7-18
- ボタンの機能 7-18

Add/Edit Interface Pair ダイアログボックス
- フィールド定義 3-15
- ボタンの機能 3-15

Add/Edit IP Logging ダイアログボックス
フィールド定義 11-17
ボタンの機能 11-17
Add/Edit Known Host Key ダイアログボックス
フィールド定義 2-13
ボタンの機能 2-13
Add/Edit Target Value Rating ダイアログボックス
フィールド定義 7-15
ボタンの機能 7-15
Add/Edit User ダイアログボックス
フィールド定義 2-30
ボタンの機能 2-30
Add/Edit Event Action Filters dialog boxes
フィールド定義 7-24
ボタンの機能 7-24
Advanced Alert Behavior ウィザード
Alert Dynamic Response Fire Once ウィンドウ
フィールド定義 6-20
ボタンの機能 6-20
Alert Dynamic Response Fire All ウィンドウ
フィールド定義 6-20
ボタンの機能 6-20
Alert Dynamic Response Summary ウィンドウ
フィールド定義 6-19
ボタンの機能 6-19
Alert Summarization ウィンドウ
フィールド定義 6-19
ボタンの機能 6-19
Event Count and Interval ウィンドウ
フィールド定義 6-18
ボタンの機能 6-18
Global Summarization ウィンドウ
フィールド定義 6-21
ボタンの機能 6-21
Server Certificate パネル
証明書
生成 2-20
表示 2-20
説明 2-19
フィールド定義 2-20
ボタンの機能 2-20
ユーザのロール 2-20
AIC
エンジン 5-29
AIC FTP エンジン
パラメータ（表） B-10
AIC HTTP エンジン
パラメータ（表） B-10
AIC エンジン
AIC FTP B-9
AIC HTTP B-9
機能 B-9
定義 B-9
AIP SSM
時刻源 2-22
復旧 C-55
リセット C-54
Allowed Hosts パネル
設定 2-6
説明 2-5
フィールド定義 2-6
ボタンの機能 2-6
ARC
ACL 8-27, A-14
Catalyst 6000 シリーズ スイッチ
VACL A-19
VACL コマンド A-19
Catalyst スイッチ
VACL A-16
VLAN A-16
nac.shun.txt ファイル A-17
NAT アドレッシング A-15
postblock ACL A-16
preblock ACL A-16
SSH A-13
Telnet A-13
VACL A-14
以前の Network Access Controller 8-1, 8-4
インターフェイス A-14
管理対象デバイス 8-8
機能 8-2, A-12, A-13
最大ブロック 8-2
サポートされているデバイス A-15
状態の維持 A-16
シングル ポイント制御 A-15
図 A-12
ステータスの確認 8-3
設計 8-2
説明 A-3
前提条件 8-5
デバイス
サポート対象 8-6

認証 A-15
ファイアウォール
AAA A-18
NAT A-19
postblock ACL A-16
preblock ACL A-16
shun コマンド A-18
TACACS+ A-19
接続ブロッキング A-18
ネットワーク ブロッキング A-18
ブロッキング
接続ベース A-17
無条件のブロッキング A-17
ブロッキング アプリケーション 8-2
ブロック応答 A-13
ブロック数 A-15
マスター ブロッキング センサー A-14
レート制限 8-4, 11-11
Assign Actions ダイアログボックス
フィールド定義 5-16
ボタンの機能 5-16
Atomic ARP エンジン
説明 B-11
パラメータ（表） B-11
Atomic IP エンジン
説明 B-11
パラメータ（表） B-11
Attack Response Controller
ARC を参照
以前の Network Access Controller A-3
説明 A-3
AuthenticationApp
安全な通信 A-22
機能 A-20
説明 A-3
センサーのコンフィギュレーション A-21
方式 A-21
ユーザの認証 A-21
ログイン試行の制限 A-21
Authorized Keys パネル
RSA 鍵生成ツール 2-10
RSA 認証 2-8
設定 2-10
説明 2-8
フィールド定義 2-9
ボタンの機能 2-9
Auto Update パネル
設定 10-3
説明 10-2
フィールド定義 10-2
ボタンの機能 10-2
ユーザのロール 10-2

B

BackOrifice
プロトコル B-41
Blocking Devices パネル
ssh host-key コマンド 8-16, 8-24, 8-44, 8-47, 11-6, 11-9, 11-13
設定 8-24
説明 8-22
フィールド定義 8-23
ボタンの機能 8-23
Blocking Properties パネル
設定 8-11
説明 8-8
フィールド定義 8-9
ボタンの機能 8-9
Bypass パネル
フィールド定義 3-22
ボタンの機能 3-22
ユーザのロール 3-21

C

Cat 6K Blocking Device Interfaces パネル
VACL
Post-Block 8-33
Pre-Block 8-33
設定 8-35
説明 8-33
フィールド定義 8-34
ボタンの機能 8-34
CIDEE
IPS の拡張 A-37
サポートされている IPS イベント A-37
定義 A-37
プロトコル A-37
例 A-38
Cisco Intrusion Prevention Alert Center
概要 12-14

Cisco IOS
レート制限 8-4, 11-11
Cisco Services for IPS
サービス契約 1-24
サポートされている製品 1-24
Cisco.com
IDS ソフトウェア 12-2
アクティブなアップデート通知 12-15
暗号化アクセス 12-8
ソフトウェア アップデートのダウンロード 12-8
ソフトウェアへのアクセス 12-2
Cisco.com アカウント 12-8
Cisco.com への暗号化アクセス 12-8
clear events コマンド 2-27, C-76
CLI A-29
説明 A-3, A-29
CLI の動作 A-31
大文字と小文字の区別 A-32
再呼び出し A-31
タブ補完 A-31
表示オプション A-32
プロンプト A-31
ヘルプ A-31
Clone Signature ダイアログボックス
ユーザのロール 5-6
Configure Summertime ダイアログボックス
フィールド定義 2-24
ボタンの機能 2-24
copy license-key コマンド 12-11
CtlTransSource
図 A-11
説明 A-2, A-11
Ctrl+N A-31
Ctrl+P A-31
Custom Signature Wizard
Alert Behavior ウィンドウ
ボタンの機能 6-18
Alert Response ウィンドウ
フィールド定義 6-17
ボタンの機能 6-17
Atomic IP Engine Parameters ウィンドウ
フィールド定義 6-7
ボタンの機能 6-7
ICMP Traffic Type ウィンドウ
フィールド定義 6-15
ボタンの機能 6-15
Inspect Data ウィンドウ
フィールド定義 6-17
ボタンの機能 6-17
MSRPC Engine Parameters ウィンドウ
フィールド定義 6-9
ボタンの機能 6-9
Protocol Type ウィンドウ
フィールド定義 6-6
ボタンの機能 6-6
Service HTTP Engine Parameters ウィンドウ
フィールド定義 6-8
ボタンの機能 6-8
Service RPC Engine Parameters ウィンドウ
フィールド定義 6-10
ボタンの機能 6-10
Service Type ウィンドウ
フィールド定義 6-16
ボタンの機能 6-16
Signature Identification ウィンドウ
フィールド定義 6-7
ボタンの機能 6-7
State Engine Parameters ウィンドウ
フィールド定義 6-11
ボタンの機能 6-11
String ICMP Engine Parameters ウィンドウ
フィールド定義 6-11
ボタンの機能 6-11
String TCP Engine Parameters ウィンドウ
フィールド定義 6-12
ボタンの機能 6-12
String UDP Engine Parameters ウィンドウ
フィールド定義 6-13
ボタンの機能 6-13
Sweep Engine Parameters ウィンドウ
フィールド定義 6-14
ボタンの機能 6-14
TCP Sweep Type ウィンドウ
フィールド定義 6-16
ボタンの機能 6-16
TCP Traffic Type ウィンドウ
フィールド定義 6-15
ボタンの機能 6-15
UDP Sweep Type ウィンドウ
フィールド定義 6-16
ボタンの機能 6-16

UDP Traffic Type ウィンドウ
フィールド定義 6-15
ボタンの機能 6-15
Welcome ウィンドウ
フィールド定義 6-5
ボタンの機能 6-5
シグニチャ エンジン シーケンス 6-3
シグニチャ エンジンなしのシーケンス 6-4
説明 6-2
プロトコル 6-6
ユーザのロール 6-5

D

DDOS プロトコル B-40
debug-module-boot コマンド C-55
Denied Attackers パネル
使用 11-3
説明 11-2
フィールド定義 11-2
ボタンの機能 11-2
ユーザのロール 11-2
Device Login Profiles パネル
設定 8-20
説明 8-18
フィールド定義 8-18
ボタンの機能 8-18
Diagnostics Report パネル
使用 10-13
説明 10-12
ボタンの機能 10-12
ユーザのロール 10-12

E

Edit Allowed Host ダイアログボックス
ユーザのロール 2-5
Edit Authorized Key ダイアログボックス
ユーザのロール 2-9
Edit Blocking Device ダイアログボックス
ユーザのロール 8-22
Edit Cat 6K Blocking Device Interface ダイアログボックス
ユーザのロール 8-34
Edit Device Login Profile ダイアログボックス
ユーザのロール 8-18
Edit Event Action Filter ダイアログボックス
ユーザのロール 7-22
Edit Event Action Overrides ダイアログボックス 7-17
Edit Interface Pair ダイアログボックス
フィールド定義 3-15
ボタンの機能 3-15
ユーザのロール 3-14
Edit Interface ダイアログボックス
フィールド定義 3-12
ボタンの機能 3-12
ユーザのロール 3-11
Edit Known Host Key ダイアログボックス
ユーザのロール 2-12
Edit Master Blocking Sensor ダイアログボックス
ユーザのロール 8-38
Edit Never Block Address ダイアログボックス
ユーザのロール 8-9
Edit Router Blocking Device Interface ダイアログボックス
ユーザのロール 8-29
Edit Signature Variable ダイアログボックス
ユーザのロール 5-3
Edit Signature ダイアログボックス
ユーザのロール 5-6
Edit SNMP Trap Destination ダイアログボックス
ユーザのロール 9-5
Edit Target Value Rating ダイアログボックス
ユーザのロール 7-14
Edit User ダイアログボックス
ユーザのロール 2-29
Edit Virtual Sensor ダイアログボックス
ユーザのロール 4-2
Event Action Filters パネル
設定 7-26
説明 7-22
フィールド定義 7-22
ボタンの機能 7-22
Event Action Overrides パネル
設定 7-20
説明 7-17
フィールド定義 7-17
ボタンの機能 7-17
Event Variables パネル
設定 7-12
説明 7-11
フィールド定義 7-12
ボタンの機能 7-12

Event Viewer ページ
フィールド定義 7-34
ボタンの機能 7-34
Events パネル
設定 7-35
説明 7-33
フィールド定義 7-33
ボタンの機能 7-33
ユーザのロール 7-33

F

Flood Host エンジン
パラメータ（表） B-13
FLood Net エンジン
パラメータ（表） B-13
Flood エンジン
説明 B-13

G

General Settings パネル
設定 7-31
ユーザのロール 7-30
Global Variables パネル
説明 4-5
フィールド定義 4-5
ボタンの機能 4-5
ユーザのロール 4-5

H

H.225.0 プロトコル B-21
H.323 プロトコル B-21
HTTP 解読
ASCII 正規化 6-34, B-24
説明 6-34, B-24
hw-module module 1 reset コマンド C-54

I

IDAPI A-33
機能 A-33
図 A-33
説明 A-3
通信 A-3, A-33
IDCONF
RDEP2 A-36
XML A-36
説明 A-36
例 A-36
IDIOM
定義 A-36
メッセージ A-36
IDM
Cookie 1-17
GUI 1-2
Java プラグイン 1-4, C-41
Signature Wizard
サポートされるシグニチャ エンジン 6-2, 6-22
TLS および SSL 1-18
Web ブラウザ 1-2
暗号化製品 1-2
エラー メッセージ
分析エンジンがビジー状態 C-44
概要 1-2
勧告 1-2
検証
Internet Explorer の証明書フィンガープリント 1-19
Mozilla の証明書フィンガープリント 1-22
Netscape の証明書フィンガープリント 1-21
システム要件 1-3
証明書 1-18
前提条件 1-16
メモリ 1-4, C-41
ユーザ インターフェイス 1-2
ロードしない
Java キャッシュのクリア C-43
ログイン 1-16
IDM がロードしない
Java キャッシュのクリア C-43
IDSM-2 がオンラインにならない C-51
IDSM-2
時刻源 2-21
IDSM-2 コマンド / コントロール ポート C-51
inline on a stick
説明 3-4
Interface Pairs パネル
設定 3-15
説明 3-14

フィールド定義　3-14
ボタンの機能　3-14
InterfaceApp
説明　A-3
Interfaces パネル
設定　3-13
説明　3-10
フィールド定義　3-11
ボタンの機能　3-11
Internet Explorer
証明書フィンガープリントの検証　1-19
IP Logging パネル
設定　11-17
説明　11-15
フィールド定義　11-16
ボタンの機能　11-16
ユーザのロール　11-16
IP フラグメント再構成
シグニチャ（表）　5-37
説明　5-37
パラメータ（表）　5-37
IP ロギング
イベント アクション　11-15
システム パフォーマンス　11-15
説明　5-44, 11-15
IP ログ
Ethereal　11-15
TCP Dump　11-15
循環バッファ　11-15
状態　11-15
表示　11-17
IPS
外部通信　A-34
内部通信　A-33
IPS アプリケーション
XML 形式　A-2
表　A-39
要約　A-39
IPS イベント
タイプ　A-9
リスト　A-9
IPS ソフトウェア
Linus OS　A-2
アップデート　A-4
アプリケーション リスト　A-2
シグニチャの調整　A-4
使用可能なファイル　12-2
新機能　A-4
セキュリティ機能　A-5
ディレクトリ構造　A-38
データの取得　A-5
デバイスのパラメータ設定　A-4
入手　12-2
バージョン管理方式　12-4
プラットフォームに依存するリリースの例　12-6
ユーザによる対話操作　A-4
IPS データ
XML 文書　A-8
タイプ　A-8

J

Java プラグイン
Linux　1-5, C-42
Solaris　1-5, C-42
Windows　1-4, C-41

K

Known Host Keys パネル
設定　2-13
説明　2-12
フィールド定義　2-12
ボタンの機能　2-12

L

Licensing パネル
設定　1-26, 12-10
説明　1-23, 12-9
フィールド定義　1-25
ボタンの機能　1-25
ユーザのロール　1-25
LogApp
syslog メッセージ　A-20
機能　A-20
説明　A-3, A-20
LOKI プロトコル　B-40

M

MainApp A-6
show version コマンド A-6
アプリケーション A-6
機能 A-6
説明 A-2
ホストの統計情報 A-6
Master Blocking Sensor パネル
設定 8-39
説明 8-37
フィールド定義 8-38
ボタンの機能 8-38
Master エンジン
alert-frequency B-5
アラート頻度パラメータ（表） B-5
イベント アクション B-6
混合デルタ B-5
定義 B-4
汎用パラメータ B-4
汎用パラメータ（表） B-4
MBS が適切にセットアップされていない C-26
Mega Event Generator
説明 7-30
Meta エンジン
説明 5-45, B-14
パラメータ（表） B-14
Miscellaneous パネル
設定
IP フラグメント再構成 5-39
IP ロギング 5-44
TCP ストリーム再構成 5-43
アプリケーション ポリシー 5-35
説明 5-27
フィールド定義 5-28
ボタンの機能 5-28
ユーザのロール 5-27
Mozilla
証明書フィンガープリントの検証 1-22
Multi String エンジン
説明 B-15

N

Netscape
証明書フィンガープリントの検証 1-21
Network Access Controller
機能 A-12
Network Blocks パネル
設定 8-47, 11-9
説明 8-46, 11-8
フィールド定義 8-46, 11-8
ボタンの機能 8-46, 11-8
ユーザのロール 8-46, 11-8
Network パネル
TLS/SSL 2-3
設定 2-3
フィールド定義 2-2
ボタンの機能 2-2
説明 2-2
ユーザのロール 2-2
NM-CIDS
時刻源 2-22
Normalizer エンジン
IP フラグメント再構成 B-16
TCP ストリーム再構成 B-16
説明 B-16
パラメータ（表） B-17
NotificationApp
SNMP get A-9
SNMP トラップ A-9
アラート情報 A-9
機能 A-9
システムの健全性情報 A-10
説明 A-3
統計情報 A-11
NSDB
概要 12-16
NTP
時刻同期 2-21
説明 2-21

P

Post-Block ACL 8-27, 8-28
Pre-Block ACL 8-27, 8-28

Q

Q.931 プロトコル
SETUP メッセージ B-21
説明 B-21

R

Rate Limits パネル
説明 8-14
フィールド定義 8-15, 11-12
ボタンの機能 8-15, 11-12
RDEP2 A-34
機能 A-34
メッセージ A-34
RDEP2 を使用したイベントの取得
図 A-34
RDEP2 を使用したコマンドの送信
図 A-35
Reboot Sensor パネル
設定 10-7
説明 10-6
ボタンの機能 10-6
ユーザのロール 10-6
Restore Defaults パネル
設定 10-5
説明 10-5
ボタンの機能 10-5
ユーザのロール 10-5
Router Blocking Device Interfaces パネル
設定 8-31
説明 8-28
フィールド定義 8-30
ボタンの機能 8-30
RPC ポートマッパー B-28
RR
計算 7-2
例 7-10

S

SDEE
HTTP A-37
定義 A-37
プロトコル A-37
SDEE サーバ
要求 A-37
SEAF
説明 7-5, A-26
パラメータ 7-5, A-26
SEAO
説明 7-4, A-26
SEAP
アラーム チャネル 7-4, A-26
機能 7-4, A-26
コンポーネント 7-4, A-26
シグニチャ イベントのフロー 7-5, A-26
図 7-5, A-26
説明 A-24
Sensor Key パネル
説明 2-15
センサー SSH 鍵
生成 2-15
表示 2-15
フィールド定義 2-15
ボタンの機能 2-15
ユーザのロール 2-15
SensorApp
IP の正規化 A-28
RR A-28
SEAP A-24
TCP の正規化 A-28
アラーム チャネル A-25
イベント アクションのフィルタリング A-28
インライン パケット処理 A-27
機能 A-24
新機能 A-27
説明 A-3
パケット フロー A-25
プロセッサ A-24
分析エンジン A-25
ホールドダウン タイマー A-28
Service DNS エンジン B-18
パラメータ（表） B-18
Service Generic エンジン
説明 B-20
パラメータ（表） B-21
Service H225 エンジン
ASN.1PER 検証 B-22
TPKT 検証 B-22
機能 B-22
説明 B-21
パラメータ（表） B-23
Service HTTP エンジン
カスタム シグニチャ 6-34
説明 6-34, B-24
パラメータ（表） B-24
Service HTTP シグニチャの例 6-34

Service IDENT エンジン
説明 B-26
パラメータ（表） B-26
Service MSRPC エンジン
DCS/RPC protocol B-26
説明 B-26
パラメータ（表） B-27
Service MSSQL エンジン
MSSQL protocol B-27
説明 B-27
Service NTP エンジン
説明 B-28
パラメータ（表） B-28
Service RPC エンジン
RPC ポートマッパー B-28
説明 B-28
パラメータ（表） B-28
Service SMB エンジン
説明 B-29
パラメータ（表） B-29
Service SNMP エンジン
説明 B-31
パラメータ（表） B-31
Service SSH エンジン
説明 B-32
Service FTP エンジン
説明 B-20
パラメータ（表） B-20
SERVICE.MSSQL エンジン
パラメータ（表） B-27
SERVICE.SSH エンジン
パラメータ（表） B-32
setup コマンド 1-6, 2-1
SFR
説明
show events コマンド C-73
show interfaces コマンド C-71
show module 1 details コマンド C-54
show statistics virtual-sensor コマンド C-62
show statistics コマンド C-61, C-62
show tech-support コマンド C-56, C-57
出力 C-58
show version コマンド C-59
説明 C-59
Shut Down Sensor パネル
設定 10-8
説明 10-8
ボタンの機能 10-8
ユーザのロール 10-8
Signature Configuration パネル
アクションの割り当て 5-24
シグニチャ
アクティブ 5-23
イネーブル化 5-22
チューニング 5-21
追加 5-17
ディセーブル化 5-22
複製 5-19
リタイア 5-23
説明 5-6
フィールド定義 5-7
ボタンの機能 5-7
Signature Event Action Processor
「SEAP」を参照
Signature Variables パネル
設定 5-4
フィールド定義 5-3
ボタンの機能 5-3
Signature Wizard
サポートされるシグニチャ エンジン 6-2, 6-22
SNMP
Get 9-2
GetNext 9-2
Set 9-2
Trap 9-2
概要 9-2
設定 9-4
SNMP General Configuration パネル
設定 9-4
説明 9-3
フィールド定義 9-3
ボタンの機能 9-3
ユーザのロール 9-3
SNMP Traps Configuration パネル
設定 9-6
説明 9-5
フィールド定義 9-5
ボタンの機能 9-5
SNMP トラップ
概要 9-2
設定 9-6
SPAN ポートの問題 C-12

SSH
概要 2-8
セキュリティ 2-8
SSH サーバ
公開鍵 A-22
秘密鍵 A-22
State エンジン
Cisco Login B-33
LPR Format String B-33
SMTP B-33
説明 B-33
パラメータ（表） B-33
Statistics パネル
使用 10-15
説明 10-14
ボタンの機能 10-14
ユーザのロール 10-14
String ICMP エンジン
パラメータ（表） B-35
String TCP エンジン
カスタム シグニチャ 6-29
パラメータ（表） B-36
String TCP シグニチャの例 6-29
String エンジン
説明 6-29, B-35
STRING.UDP エンジン
パラメータ（表） B-37
Summarizer
説明 7-30
Summary パネル
概要 3-9
フィールド定義 3-9
ボタンの機能 3-9
Sweep エンジン
説明 B-38
パラメータ（表） B-38
System Information パネル
使用 10-16
説明 10-16
ボタンの機能 10-16
ユーザのロール 10-16

T

TAC
show tech-support コマンド C-57
サービス アカウント A-30
Target Value Rating パネル
設定 7-15
フィールド定義 7-14
ボタンの機能 7-14
TCP ストリーム再構成
シグニチャ（表） 5-40
説明 5-40
パラメータ（表） 5-40
TCP リセット インターフェイス
条件 3-10
TFN2K プロトコル B-40
Time パネル
フィールド定義 2-23
設定 2-25
説明 2-21
フィールド定義 2-24
ボタンの機能 2-23
ユーザのロール 2-23
TLS
概要 1-18
証明書 1-18
説明 2-3
ハンドシェイク 1-18
Traffic Flow Notifications パネル
設定 3-23
説明 3-23
フィールド定義 3-23
ボタンの機能 3-23
ユーザのロール 3-23
Traffic ICMP エンジン
DDOS B-40
LOKI B-40
TFN2K B-40
説明 B-40
パラメータ（表） B-40
Transport Layer Security
「TLS」を参照
Tribe Flood Net 2000 プロトコル B-40
Trojan エンジン
BO2K B-41
説明 B-41
TrojanN エンジン
TFN2K B-41
Trusted Hosts パネル
設定 2-18

説明　2-17
フィールド定義　2-17
ボタンの機能　2-17
TVR
設定　7-15
説明　7-14

U

Update Sensor パネル
設定　10-10
説明　10-9
フィールド定義　10-9
ボタンの機能　10-9
ユーザのロール　10-9
Users パネル
設定　2-30
説明　2-28
フィールド定義　2-29
ボタンの機能　2-29
ユーザのロール　2-28

V

VACL
Post-Block　8-33
Pre-Block　8-33
説明　8-3
Virtual Sensor パネル
設定　4-3
説明　4-2
フィールド定義　4-3
ボタンの機能　4-3
VLAN Pairs パネル
概要　3-17
設定　3-19
フィールド定義　3-18
ボタンの機能　3-18
VLAN ペア
設定　3-19

W

Web サーバ
HTTP 1.0 および 1.1 のサポート　A-23
RDEP2 サポート　A-23
公開鍵　A-22
説明　A-3, A-23
秘密鍵　A-22

あ

アクセス
Cisco Intrusion Prevention Alert Center　12-14
IPS ソフトウェア　12-2
アクセス リストの設定の誤り　C-8
アップグレード
4.1 から 5.0　12-7
最低限必要なバージョン　12-7
アップデート
Cisco.com　10-9
FTP サーバ　10-9
アプライアンス
時刻源　2-21
アプリケーション
XML 形式　A-2
アプリケーション パーティション
説明　A-3
アラーム チャネル
説明　7-4, A-26
暗号化製品
IDM　1-2

い

一般的な設定値
説明　7-30
イベント アクション
説明　7-7, B-6
イベント アクション オーバーライド
概要　7-3
設定　7-20
イベント アクション（表）　7-7, B-6
イベント アクション フィルタ
概要　7-3
設定　7-26
イベント アクション ルール
概要　7-2
機能　7-2
例　7-9

イベント ストア
　イベントのクリア　2-27
　データ構造　A-8
イベント タイプ　C-73
イベント ストア
　機能　A-7
　説明　A-3
　タイムスタンプ　A-7
　例　A-7
イベント変数
　設定　7-12
　例　7-11
インストール
　センサーのライセンス　1-26, 12-10
　ライセンス キー　12-12
インターフェイス
　設定　3-13
　設定上の制限　3-7
　有効な組み合せ　3-7
インターフェイス サポート（表）　3-5
インターフェイス ペア
　設定　3-15
　説明　3-14
インターフェイスの仮想センサーへの割り当て　4-3
インライン VLAN ペア
　サポートしているセンサー　3-4
　説明　3-2, 3-4
インライン インターフェイス ペア
　説明　3-2
インライン インターフェイス モード
　説明　3-2
インライン モード
　概要　3-3

え

エンジン
　AIC　5-29

お

オペレータ
　特権　A-29

か

概要
　SSH　2-8
　センサー上の時刻　2-21
　バイパス モード　3-21
確認
　センサーの初期化　1-12
　センサーのセットアップ　1-12
カスタム シグニチャ
　MEG シグニチャ　5-45
仮想センサー
　インターフェイスの割り当て　4-3
勧告
　暗号化製品　1-2
監視
　イベント　7-35
管理者
　特権　A-29

き

偽のホストに対する手動ブロック　C-25
拒否された攻撃者
　ヒット カウント　11-2
　ヒット カウントのリセット　11-3
　リストのクリア　11-3

く

クリア
　イベント　C-76
　統計情報　C-62

こ

攻撃の重大度評価
　「SFR」を参照
構文
　大文字と小文字の区別　A-32
コマンド
　clear events　2-27, C-76
　copy license-key　12-11
　debug module-boot　C-55
　hw-module module 1 reset　C-54
　show events　C-73

show module 1 details C-54
show statistics C-62
show statistics virtual-sensor C-62
show tech-support C-57
show version C-59
セットアップ 1-6, 2-1
混合モード
説明 3-2

さ

サービス
特権 A-30
サービス アカウント
TAC A-30
説明 A-30
特権 A-30
トラブルシューティング A-30
サービス ロール 2-28, A-30
再呼び出し
使用 A-31
ヘルプおよびタブ補完 A-31
作成
MEG シグニチャ 5-45
カスタム シグニチャ
Service HTTP 6-34
String TCP 6-29
シグニチャ エンジンの使用 6-3
シグニチャ エンジンを使用しない 6-4

し

時間
センサー上での修正 2-27
シグニチャ
false positive 5-2
カスタム 5-2
サブシグニチャ 5-2
説明 5-2
チューニング済み 5-2
デフォルト 5-2
レート制限 8-4, 11-11
シグニチャ エンジン
AIC B-9
Atomic B-11
Atomic ARP B-11
Atomic IP B-11
Flood B-13
Flood Host B-13
FLood Net B-13
IDM によってサポートされる 6-2, 6-22
Meta 5-45, B-14
Multi String B-15
Normalizer B-16
Service DNS B-18
Service Generic B-20
Service H225 B-21
Service HTTP 6-34, B-24
Service IDENT B-26
Service MSRPC B-26
Service MSSQL B-27
Service NTP エンジン B-28
Service RPC B-28
Service SMB B-29
Service SNMP B-31
Service SSH エンジン B-32
Service FTP B-20
String 6-29, B-35
Sweep B-38
Traffic ICMP B-40
Trojan B-41
カスタム シグニチャの作成 6-3
ステート B-33
定義 B-2
リスト B-2
シグニチャ忠実度評価
「SFR」を参照
シグニチャ変数
説明 5-3
時刻源
AIP SSM 2-22
IDSM-2 2-21
NM-CIDS 2-22
アプライアンス 2-21
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-2
ディレクトリ構造 A-38
システム コンポーネント
IDAPI A-33
システム情報
表示 10-16
システムの設計（図） A-2

システム要件
IDM 1-3
自動アップデートの適用 C-38
自動更新
Cisco.com 10-2
サーバ
FTP 10-2
SCP 10-2
出力
現在の行のクリア A-32
表示 A-32
使用
TCP リセット インターフェイス 3-10
障害リカバリ C-3
使用不可
ブロッキング 8-8
証明書
Internet Explorer 1-19
Mozilla 1-22
Netscape 1-21
初期化
確認 1-12
診断
レポート 10-13
診断レポートの生成 10-13

せ

制御トランザクション
特性 A-8
要求のタイプ A-8
制限事項
同時 CLI セッション 1-16
セキュリティ
SSH 2-8
設定
Cat 6K ブロッキング デバイス インターフェイス 8-35
IP フラグメント再構成パラメータ 5-38
IP ロギング 11-17
SNMP 9-4
SNMP トラップ 9-6
TCP フラグメント再構成パラメータ 5-42
TVR 7-15
VLAN ペア 3-19
アクティブなホスト ブロック 8-16, 8-44, 11-6, 11-13
アプリケーション ポリシー 5-36
イベント 7-35
イベント アクション オーバーライド 7-20
イベント アクション フィルタ 7-26
イベント アクション ルールの一般的な設定値 7-31
イベント変数 7-12
インターフェイス 3-13
インターフェイス ペア 3-15
ターゲットの価値評価 7-15
デバイス ログイン プロファイル 8-20
トラフィック フロー通知 3-23
ネットワーク ブロック 8-47, 11-9
ブロッキング デバイス 8-24
ブロッキング プロパティ 8-11
マスター ブロッキング センサー 8-39
ルータのブロッキング デバイス インターフェイス 8-31
レート制限デバイス 8-24
説明 B-18, C-73
センサー
NTP 時刻同期 2-21
setup コマンド 1-6, 2-1
アップデート 10-3, 10-10
イメージの再作成 12-7
インターフェイス サポート 3-5
時刻源 2-21
システム イメージの復旧 12-7
システム情報 10-16
シャットダウン 10-8
初期化 1-6, 2-1
診断レポート 10-13
セットアップ 2-1
デフォルト設定の復元 10-5
統計情報 10-15
パーティション A-3
自らをブロッキング 8-8
ライセンス 1-26, 12-10
リブート 10-7
センサーがパケットを検出しない C-16
センサー上の時刻の修正 2-27
センサー処理が動作しない C-11
センサーにアクセスできない C-5
センサーの更新 10-10
センサーのシャットダウン 10-8

センサーの初期化　1-6, 2-1
センサーのセットアップ　2-1
センサーのリブート　10-7

そ

ソフトウェア アーキテクチャ
　ARC（図）　A-12
　IDAPI（図）　A-33
　RDEP2（図）　A-34
ソフトウェア アップデートの適用　C-37

た

ターゲットの価値評価
　「TVR」を参照
　設定　7-15
代替 TCP リセット インターフェイス
　設定上の制限　3-7
タブ補完
　使用　A-31

ち

重複する IP アドレス　C-9

て

データ構造
　例　A-8
デバイス　8-24
デバイス アクセスの問題　C-22
デバッグ ロギングのイネーブル化　C-28
デバッグ ロギングの使用　C-28
デフォルト
　復元　10-5

と

統計情報
　表示　10-15
統計情報の表示　10-15
トラフィック フロー通知
　設定　3-23
トラブルシューティング　C-1
AIP SSM
　デバッグ　C-55
　復旧　C-55
　リセット　C-54
AIP SSM コマンド　C-54
cidDump スクリプト　C-77
FTP サイト上のファイルへのアクセス　C-77
FTP サイトへのファイルのアップロード　C-77
IDM がセンサーにアクセスできない　C-44
IDM がロードしない　C-43
IDSM-2
　switch コマンド　C-47
　TCP リセット ポート　C-52
　オンラインにならない　C-51
　コマンド / コントロール ポート　C-51
　シリアル ケーブル　C-53
　問題の診断　C-46
MBS が適切にセットアップされていない　C-26
NTP　C-35
show events コマンド　C-72
show interfaces コマンド　C-71
show statistics コマンド　C-61
show tech-support コマンド　C-56
show tech-support コマンド出力　C-58
show version コマンド　C-59
SPAN ポートの問題　C-12
syslog への cidLog メッセージ　C-33
アクセス リストの設定の誤り　C-8
アラートが表示されない　C-14
偽のホストに対する手動ブロック　C-25
自動アップデートの適用　C-38
障害リカバリ　C-3
情報の収集　C-56
センサー イベント　C-73
センサーがパケットを検出しない　C-16
センサー処理が動作しない　C-11
センサーにアクセスできない　C-5
ソフトウェア アップグレード　C-37
　IDS-4235　C-37
　IDS-4250　C-37
　センサー内　C-39
ソフトウェア アップデートの適用　C-37
重複する IP アドレス　C-9
通信　C-5
デバイス アクセスの問題　C-22
デバッグ ロギングのイネーブル化　C-28

デバッグ ロギングの使用　C-28
デバッグ ログ ゾーン名（表）　C-33
破損した SensorApp コンフィギュレーション　C-18
物理接続の問題　C-12
ブロックがシグニチャに対して実行されない　C-25
分析エンジンがビジー状態　C-44
問題のある DIMM　C-18
予防保守　C-2
リセットがシグニチャに対して実行されない　C-35
トラブルシューティング用の switch コマンド　C-47

ね

ネットワーク タイム プロトコル
「NTP」を参照

は

パーティション
アプリケーション　A-3
メンテナンス　A-3
リカバリ　A-3
バイパス モード　3-21
概要　3-21
機能　3-2
パスワード
サービス アカウント　1-7
バック ドア型トロイの木馬
BO2K　B-41

ひ

ビューア
特権　A-29
表示
IP ログ　11-17
イベント　C-74
システム情報　10-16
テクニカル サポート情報　C-57
統計情報　10-15, C-62
バージョン　C-59

ふ

復元
デフォルト　10-5
復旧
AIP SSM　C-55
物理接続の問題　C-12
プラットフォーム
同時 CLI セッション　1-16
ブロッキング
サポートされているデバイス　8-6
使用不可　8-8
説明　8-2
前提条件　8-5
タイプ　8-2
必要な情報　8-3
マスター ブロッキング センサー　8-37
ブロッキングの前提条件　8-5
ブロックがシグニチャに対して実行されない　C-25
ブロックしない
ネットワーク　8-8
ホスト　8-8
プロトコル
Custom Signature Wizard　6-6
プロンプト
デフォルト入力　A-31
分析エンジン
仮想センサー　4-2
グローバル変数　4-5
説明　4-1
分析エンジンがビジー状態
IDM の終了　C-44

へ

ヘルプ
疑問符　A-31
使用　A-31

ま

マスター ブロッキング センサー　8-37
説明　8-37

め

メモリ
IDM 1-4, C-41
メモリの変更
Linux での Java プラグイン 1-5, C-42
Solaris での Java プラグイン 1-5, C-42
Windows での Java プラグイン 1-4, C-41
メンテナンス パーティション
説明 A-3

も

モード
インライン 3-3
インライン VLAN ペア 3-2
インライン インターフェイス 3-2
混合 3-2
バイパス 3-2, 3-21
モニタリング
ビューア特権 A-29

ゆ

ユーザのロール
オペレータ A-29
管理者 A-29
サービス A-29
ビューア A-29

よ

要約
Engine.META 7-4
Fire All 7-4
Fire Once 7-4
Global Summarization 7-4
Summary 7-4
説明 7-3

ら

ライセンス
IPS デバイスのシリアル番号 1-23, 12-9
説明 1-23, 12-9
ライセンス キー
インストール 12-12

り

リカバリ パーティション
説明 A-3
リスク評価
「RR」を参照
リセット
AIP SSM C-54
リセットがシグニチャに対して実行されない C-35

れ

レート制限
ACL 8-28
サービス ポリシー 8-28
サポートされているシグニチャ 8-4, 11-11
説明 8-4, 11-11
ルータ 8-4, 11-11

ろ

ログイン
IDM 1-16