コマンドライン インターフェイスによる Cisco Intrusion Prevention System Sensor 5.1 の設定

Text Part Number: OL-8676-01-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。

CCIP、Cisco Arrow のロゴ、Cisco Powered Network のマーク、Cisco Systems Verified のロゴ、Cisco Unity、Follow Me Browsing、FormShare、Internet Quotient、iQ Breakthrough、iQ Expertise、iQ FastTrack、iQ のロゴ、iQ Net Readiness Scorecard、Networking Academy、ScriptShare、SMARTnet、TransPath、および Voice LAN は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、Discover All That’s Possible、The Fastest Way to Increase Your Internet Quotient、および iQuick Study は、Cisco Systems, Inc. のサービスマークです。Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco IOS のロゴ、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherSwitch、Fast Step、GigaStack、IOS、IP/TV、LightStream、MGX、MICA、Networkers のロゴ、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、RateMUX、Registrar、SlideCast、StrataView Plus、Stratm、SwitchProbe、TeleRouter、および VCO 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。（0206R）

コマンドライン インターフェイスによる Cisco Intrusion Prevention System Sensor 5.1 の設定
Copyright © 2005 Cisco Systems, Inc.
All rights reserved.

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

CHAPTER 1
CLI コンフィギュレーション ガイドの概要 1-1
概要 1-2
センサーのコンフィギュレーション タスクのフロー 1-2
ユーザ ロール 1-4
CLI の動作 1-5
コマンドライン編集 1-7
IPS コマンド モード 1-8
正規表現の構文 1-9
汎用 CLI コマンド 1-11
CLI のキーワード 1-12

CHAPTER 2
センサーへのログイン 2-1
概要 2-2

サポートされるユーザ ロール 2-2
アプライアンスへのログイン 2-3
ターミナル サーバのセットアップ 2-4
IDSM-2 へのログイン 2-6
NM-CIDS へのログイン 2-7
AIP SSM へのログイン 2-9
センサーへのログイン 2-10

CHAPTER 3 センサーの初期化 3-1
概要 3-2
System Configuration Dialog 3-2
センサーの初期化 3-3
初期化の確認 3-9

CHAPTER 4 初期コンフィギュレーション タスク 4-1
ネットワーク設定の変更 4-2
ホスト名の変更 4-2
IP アドレス、ネットマスク、およびゲートウェイの変更 4-4
Telnet のイネーブル化とディセーブル化 4-5
アクセス リストの変更 4-6
FTP タイムアウトの変更 4-8
ログイン バナーの追加 4-10
Web サーバ設定の変更 4-12
ユーザ パラメータの設定 4-14
ユーザの追加と削除 4-14
パスワード リカバリ 4-16
サービス アカウントの作成 4-16
パスワードの設定 4-18
ユーザの特権レベルの変更 4-18
ユーザのステータスの表示 4-19
アカウントのロックの設定 4-20
時刻の設定 4-22
時刻源およびセンサー 4-22
センサー上の時刻の修正 4-24
センサーでの時刻の設定 4-24
システム クロック 4-24
サマータイムの設定 4-26
時間帯の設定 4-31
NTP の設定 4-32

Cisco ルータの NTP サーバとしての設定 4-32
センサーで NTP 時刻源を使用するための設定 4-33
SSH の設定 4-36
SSH について 4-36
既知のホスト リストへのホストの追加 4-36
SSH 許可公開鍵の追加 4-38
新しい SSH サーバ鍵の生成 4-40
TLS の設定 4-41
TLS について 4-41
TLS の信頼できるホストの追加 4-42
サーバ証明書の表示と生成 4-44
ライセンス キーのインストール 4-45
概要 4-45
IPS 製品のサービス プログラム 4-45
ライセンス キーの入手とインストール 4-47

CHAPTER 5 インターフェイスの設定 5-1
インターフェイスの説明 5-2
コマンド / コントロール インターフェイス 5-2
センシング インターフェイス 5-3
インターフェイス サポート 5-4
TCP リセット インターフェイス 5-5
代替 TCP リセット インターフェイスについて 5-5
代替 TCP リセット インターフェイスの指定 5-6
コンフィギュレーション シーケンス 5-7
インターフェイスのコンフィギュレーションの制約事項 5-7
物理インターフェイスの設定 5-9
混合モード 5-13
混合モードについて 5-13
混合モードの設定 5-13
インライン インターフェイス モード 5-14
インライン インターフェイス モードについて 5-14
インライン インターフェイス モードの設定 5-14
インライン VLAN ペア モード 5-17
インライン VLAN ペア モードについて 5-17
インライン VLAN ペアの設定 5-17
インライン バイパス 5-23
インライン バイパスについて 5-23
バイパス モードの設定 5-23

仮想センサーへのインターフェイスの割り当て 5-25
インターフェイスの通知の設定 5-27

CHAPTER 6 イベント アクション ルールの設定 6-1
イベント アクション ルールについて 6-2
Signature Event Action Processor 6-2
イベント アクション 6-4
イベント アクション ルールを設定するためのタスク リスト 6-7
イベント アクション変数 6-7
イベント アクション変数について 6-7
イベント アクション変数の設定 6-8
ターゲットの価値評価 6-9
リスク評価の計算 6-9
ターゲットの価値評価の設定 6-9
イベント アクション オーバーライド 6-11
イベント アクション オーバーライドについて 6-11
イベント アクション オーバーライドの設定 6-11
イベント アクション フィルタ 6-14
イベント アクション フィルタについて 6-14
イベント アクション フィルタの設定 6-14
汎用設定 6-20
汎用設定について 6-20
イベント アクションの要約について 6-20
イベント アクションの集約について 6-20
インラインの攻撃者拒否イベント アクションについて 6-21
汎用設定 6-21
拒否された攻撃者リストのモニタリングとクリア 6-23
イベント アクション ルールの例 6-25
イベントのモニタリング 6-26
イベントの表示 6-26
イベント ストアからのイベントのクリア 6-29

CHAPTER 7 シグニチャの定義 7-1
シグニチャについて 7-2
シグニチャ変数 7-3
シグニチャ変数について 7-3
シグニチャ変数の設定 7-3
シグニチャの設定 7-5
シグニチャの汎用パラメータの設定 7-5

アラート頻度の設定 7-6
アラート重大度の設定 7-8
イベント カウンタの設定 7-9
シグニチャ忠実度評価の設定 7-11
シグニチャのステータスの設定 7-12
シグニチャへのアクションの割り当て 7-13
AIC シグニチャの設定 7-15
概要 7-15
アプリケーション ポリシーの設定 7-16
AIC 要求メソッド シグニチャ 7-18
AIC MIME 定義コンテンツ タイプ シグニチャ 7-19
AIC 転送符号化シグニチャ 7-22
AIC FTP コマンド シグニチャ 7-22
IP フラグメント再構成 7-23
概要 7-23
IP フラグメント再構成シグニチャと設定可能なパラメータ 7-24
IP フラグメント再構成パラメータの設定 7-24
IP フラグメント再構成の方法の設定 7-25
TCP ストリーム再構成の設定 7-26
概要 7-26
TCP ストリーム シグニチャと設定可能なパラメータ 7-27
TCP ストリーム再構成シグニチャの設定 7-28
TCP ストリーム再構成のモードの設定 7-29
IP ロギングの設定 7-30
カスタム シグニチャの作成 7-32
カスタム シグニチャの作成シーケンス 7-32
String TCP シグニチャの例 7-32
Service HTTP シグニチャの例 7-36
MEG シグニチャの例 7-39
AIC MIME タイプ シグニチャ 7-43

CHAPTER 8
IP ロギングの設定 8-1
IP ロギングについて 8-2
自動 IP ロギングの設定 8-3
特定の IP アドレスの手動 IP ロギングの設定 8-5
アクティブな IP ログの停止 8-7
IP ログ ファイルのコピーと表示 8-9

CHAPTER 9 インターフェイスのライブ トラフィックの表示と取り込み 9-1
パケットの表示と取り込みについて 9-2
インターフェイスのライブ トラフィックの表示 9-3
インターフェイスのライブ トラフィックの取り込み 9-6
パケット ファイルのコピー 9-8
パケット ファイルの消去 9-9

CHAPTER 10 ブロッキングとレート制限のための ARC の設定 10-1
ブロッキングについて 10-2
レート制限について 10-4
ARC を設定する前の作業 10-5
サポートされているデバイス 10-6
ブロッキング プロパティの設定 10-8
センサーによる自らのブロックの許可 10-8
ブロッキングのディセーブル化 10-10
最大ブロック数の設定 10-12
ブロック時間の設定 10-14
ACL ロギングのイネーブル化 10-16
NVRAM への書き込みのイネーブル化 10-17
すべてのブロック イベントとエラーのロギング 10-19
ブロッキング インターフェイスの最大数の設定 10-20
ブロックしないアドレスの設定 10-22
ユーザ プロファイルの設定 10-24
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 10-26
センサーがデバイスを管理するしくみ 10-26
センサーで Cisco ルータを管理するための設定 10-27
ルータと ACL 10-27
センサーで Cisco ルータを管理するための設定 10-28
センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定 10-30
スイッチと VACL 10-30
センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定 10-31
センサーで Cisco ファイアウォールを管理するための設定 10-33
センサーをマスター ブロッキング センサーとして使用するための設定 10-35
手動ブロッキングの設定 10-38
ブロックされたホストと接続のリストの入手 10-40

CHAPTER 11 SNMP の設定 11-1
SNMP の概要 11-2
SNMP の設定 11-3
SNMP トラップの設定 11-6
サポートされている MIB 11-8

CHAPTER 12 コンフィギュレーション ファイルの処理 12-1
現在のコンフィギュレーションの表示 12-2
現在のサブモード コンフィギュレーションの表示 12-4
現在のコンフィギュレーション出力のフィルタリング 12-13
現在のサブモード コンフィギュレーション出力のフィルタリング 12-16
論理ファイルの内容の表示 12-18
リモート サーバを使用したコンフィギュレーション ファイルのコピーおよび復元 12-20
バックアップ コンフィギュレーション ファイルの作成および使用 12-22
コンフィギュレーション ファイルの消去 12-23

CHAPTER 13 センサーの管理タスク 13-1
バナー ログインの作成 13-2
CLI セッションの終了 13-3
ターミナル プロパティの変更 13-4
イベント 13-5
イベントの表示 13-5
イベント ストアからのイベントのクリア 13-8
システム クロック 13-9
システム クロックの表示 13-9
手動によるクロック設定 13-10
拒否された攻撃者のリストのクリア 13-11
統計情報の表示 13-13
テクニカル サポート情報の表示 13-22
バージョン情報の表示 13-23
シリアル接続への出力の転送 13-25
ネットワーク接続性の診断 13-26
アプライアンスのリセット 13-27
コマンド履歴の表示 13-28
ハードウェア インベントリの表示 13-29
IP パケットのルートのトレース 13-30
サブモード設定の表示 13-31

CHAPTER 14 AIP SSM コンフィギュレーション タスク 14-1
コンフィギュレーション シーケンス 14-2
AIP SSM 初期化の確認 14-3
AIP SSM へのトラフィックの送信 14-4
概要 14-4
IPS トラフィックを AIP SSM に送信するための ASA の設定 14-4
AIP SSM のリロード、シャットダウン、リセット、および復旧 14-7

CHAPTER 15 IDSM-2 の設定 15-1
コンフィギュレーション シーケンス 15-2
IDSM-2 取り付けの確認 15-3
サポートされている IDSM-2 の設定 15-5
IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定 15-6
Catalyst ソフトウェア 15-6
Cisco IOS ソフトウェア 15-7
IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定 15-9
TCP リセット インターフェイスの使用方法 15-9
SPAN の設定 15-10
Catalyst ソフトウェア 15-10
Cisco IOS ソフトウェア 15-12
VACL の設定 15-14
Catalyst ソフトウェア 15-14
Cisco IOS ソフトウェア 15-16
mls ip ids コマンドの設定 15-18
Catalyst ソフトウェア 15-18
Cisco IOS ソフトウェア 15-19
IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定 15-21
Catalyst ソフトウェア 15-21
Cisco IOS ソフトウェア 15-22
EtherChanneling の設定 15-25
概要 15-25
EtherChanneling のイネーブル化 15-25
EtherChanneling のディセーブル化 15-28
EtherChanneling の確認 15-28
IDSM-2 の管理タスク 15-30
全メモリ テストのイネーブル化 15-30
Catalyst ソフトウェア 15-30

Cisco IOS ソフトウェア 15-31
IDSM-2 のリセット 15-31
Catalyst ソフトウェア 15-31
Cisco IOS ソフトウェア 15-32
Catalyst および Cisco IOS ソフトウェアのコマンド 15-33
Catalyst ソフトウェア 15-33
サポートされているスーパーバイザ エンジン コマンド 15-33
サポートされていないスーパーバイザ エンジン コマンド 15-34
Cisco IOS ソフトウェア 15-35
EXEC コマンド 15-35
コンフィギュレーション コマンド 15-36

CHAPTER 16
NM-CIDS の設定 16-1
コンフィギュレーション シーケンス 16-2
IDS センサー インターフェイスのルータへの設定 16-3
NM-CIDS セッションの確立 16-5
NM-CIDS に対するセッションの開始 16-5
NM-CIDS への Telnet 接続 16-6
パケット キャプチャの設定 16-7
管理タスク 16-9
NM-CIDS のシャットダウン、リロード、およびリセット 16-9
Cisco IPS ソフトウェアのステータスの確認 16-10
サポートされている Cisco IOS コマンド 16-11

CHAPTER 17
システム イメージのアップグレード、ダウングレード、およびインストール 17-1
概要 17-2
センサーのアップグレード 17-3
概要 17-3
アップグレード コマンドおよびオプション 17-3
アップグレード コマンドの使用方法 17-4
リカバリ パーティションのアップグレード 17-5
自動アップグレードの設定 17-7
概要 17-7
自動アップグレード コマンドおよびオプション 17-7
自動アップグレード コマンドの使用方法 17-8
センサーのダウングレード 17-10
アプリケーション パーティションの復旧 17-11
概要 17-11
復旧コマンドの使用方法 17-11

システム イメージのインストール 17-13
概要 17-13
IDS-4215 システム イメージのインストール 17-13
IDS-4215 BIOS および ROMMON のアップグレード 17-16
IPS-4240 および IPS-4255 システム イメージのインストール 17-18
リカバリ / アップグレード CD の使用方法 17-22
NM-CIDS システム イメージのインストール 17-23
概要 17-23
NM-CIDS システム イメージのインストール 17-24
ブート ローダーのアップグレード 17-27
IDSM-2 システム イメージのインストール 17-31
システム イメージのインストール 17-31
メンテナンス パーティションの設定 17-34
メンテナンス パーティションのアップグレード 17-42
AIP SSM システム イメージのインストール 17-44

CHAPTER 18
ソフトウェアの入手方法 18-1
Cisco IPS ソフトウェアの入手方法 18-2
IPS ソフトウェアのバージョン管理 18-4
IPS ソフトウェア イメージの命名規則 18-4
5.x ソフトウェア リリースの例 18-6
Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード 18-7
暗号化アクセスが可能な Cisco.com アカウントの申し込み 18-8
Cisco.com からのライセンス キーの取得 18-9
概要 18-9
IPS 製品のサービス プログラム 18-9
ライセンス キーの入手とインストール 18-11
IDM の使用方法 18-11
CLI の使用方法 18-12
Cisco Intrusion Prevention Alert Center 18-15
Cisco IPS のアクティブなアップデート通知 18-16
Network Security Database 18-17
IPS ドキュメントへのアクセス 18-18

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 のファイル構造 A-39
IPS 5.1 アプリケーションの要約 A-40

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-12
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-22
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-36
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-5
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 でセンサー 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 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
アラートを表示できない 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クリーン アップ C-18
IDS-4250-XL の不良メモリ 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の確認 C-20
ARC 接続がアクティブであることの確認 C-21
デバイス アクセスの問題 C-22
ネットワーク デバイス上のインターフェイスおよび方向の確認 C-24
ネットワーク デバイスへの SSH 接続のイネーブル化 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 コンフィギュレーションの確認 C-26
ロギング C-28
デバッグ ロギングのイネーブル化 C-28
ゾーン名 C-33
cidLog メッセージの SysLog への転送 C-33
センサーが NTP サーバに同期していることの確認 C-34
TCP リセットがシグニチャに対して実行されない C-35
ソフトウェア アップグレード C-37
ソフトウェア アップグレード中に IDS-4235 および IDS-4250 が停止する C-37
適用するアップデートとその前提条件 C-37
自動アップデートでの問題 C-38
センサーに保存されているアップデートによるセンサーのアップデート 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 サイズの増加 C-41
Windows での Java プラグイン C-41
Linux および Solaris での Java プラグイン C-42
IDM を起動できない：Java アプレットをロードできない C-43
IDM を起動できない：分析エンジンがビジー状態 C-43
IDM、リモート マネージャ、またはセンシング インターフェイスがセンサーにアクセスできない C-44
アラートを表示しないシグニチャ C-45
IDSM-2 のトラブルシューティング C-46
IDSM-2 の問題の診断 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 C-47
ステータス LED はオンであるが、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
IDSM-2 へのシリアル ケーブルの接続 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
テクニカル サポート 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-62
概要 C-62
統計情報の表示 C-62
インターフェイス情報 C-71
概要 C-71
インターフェイス コマンド出力 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-77
Cisco FTP サイトでのファイルのアップロードおよびアクセス C-77

GLOSSARY 用語集

INDEX 索引

このマニュアルについて

このマニュアルでは、IPS 5.1 CLI を使用してセンサーを設定する方法について説明します。

この章の構成は次のとおりです。

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

対象読者

このマニュアルは、次の操作を行う管理者を対象としています。

- CLI を使用してセンサーの侵入防御設定を行う。
- 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

このマニュアルでは、次の表記法を使用しています。

- ユーザが入力するファイル名、ディレクトリ名、および引数は、イタリック体で表します。
- ^ 記号は、Control キーを表します。たとえば、画面に表示される ^z というキーの組み合せは、Control キーを押しながら、Z キーを押すことを意味します。
- コマンド、ボタン、およびキーワードは、太字で表します。
- コマンド文は、太字でイタリック体の screen フォントで表します。
- コマンド構文の説明に使用する変数は、イタリック体で表します。コマンドのオプションは、角カッコで入力します。縦線で区切られたパラメータは、1 つのパラメータだけを入力します。縦線で区切られていないパラメータは除きます。
- 画面に表示される情報は、screen フォントで表します。
- ユーザが入力する情報は、太字の screen フォントで表します。
- ユーザが値を指定する変数は、イタリック体の screen フォントで表します。
- メニュー項目（または画面）の選択手順は、screen > screen 2 > screen 3 のように表します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参考資料などを紹介しています。

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

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/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*
- *Installing and Using Cisco Intrusion Prevention System Device Manager Version 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

CLI コンフィギュレーション ガイドの概要

この章では、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の概要を説明します。この章は、次の項で構成されています。

- 概要（P.1-2）
- センサーのコンフィギュレーション タスクのフロー（P.1-2）
- ユーザ ロール（P.1-4）
- CLI の動作（P.1-5）
- コマンドライン編集（P.1-7）
- IPS コマンド モード（P.1-8）
- 正規表現の構文（P.1-9）
- 汎用 CLI コマンド（P.1-11）
- CLI のキーワード（P.1-12）

概要

このマニュアルは、IPS 5.1 CLI のタスクベースのコンフィギュレーション ガイドです。このマニュアルでは、IDSM-2、NM-CIDS、AIP SSM など、特定のアプライアンスやモジュールに限定した手順の説明を除いて、すべてのモデルのセンサーに対して「センサー」という用語を使用しています。

すべての IPS コマンドのアルファベット順のリストについては、『*Command Reference for Cisco Intrusion Prevention System 5.1*』を参照してください。Cisco.com にある IPS 5.1 のすべてのマニュアルの場所を確認するには、センサーに付属の『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1* 』を参照してください。

センサーは、IPS マネージャを使用して設定することもできます。IDM と ASDM の使用方法を説明したマニュアルにアクセスする方法については、センサーに付属の『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1* 』を参照してください。

センサーのコンフィギュレーション タスクのフロー

センサーを設定するには、次のタスクを実行します。

1. センサーにログインします。

   手順については、第 2 章「センサーへのログイン」を参照してください。

2. センサーを初期化します。

   setup コマンドを実行してセンサーを初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

3. センサーの初期化を確認します。

   手順については、P.3-9 の「初期化の確認」を参照してください。

4. サービス アカウントを作成します。

   サービス アカウントは、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、P.4-16 の「サービス アカウントの作成」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。

5. センサーのライセンスを設定します。

   手順については、P.4-45 の「ライセンス キーのインストール」を参照してください。

6. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

7. 必要に応じてインターフェイスのコンフィギュレーションを変更します。

   手順については、第 5 章「インターフェイスの設定」を参照してください。

(注)　インターフェイスは、初期化時に設定します。

8. イベント アクション ルールを設定します。

   手順については、第 6 章「イベント アクション ルールの設定」を参照してください。

9. 侵入防御用のシグニチャを設定します。

   手順については、第 7 章「シグニチャの定義」を参照してください。

10. IP ロギングを設定します。

    手順については、第 8 章「IP ロギングの設定」を参照してください。

11. ブロッキングを設定します。

    手順については、第 10 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。

12. SNMP を設定します（使用する場合）。

    手順については、第 11 章「SNMP の設定」を参照してください。

13. センサーの円滑な実行を維持するための各種のタスクを実行します。

    手順については、第 13 章「センサーの管理タスク」を参照してください。

14. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

    詳細については、第 18 章「ソフトウェアの入手方法」を参照してください。

15. 必要に応じて、アプリケーション パーティションとメンテナンス パーティションのイメージを再作成します。

    手順については、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

各モジュールに固有の手順については、次の各章を参照してください。

- 第 14 章「AIP SSM コンフィギュレーション タスク」
- 第 15 章「IDSM-2 の設定」
- 第 16 章「NM-CIDS の設定」

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。

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

- 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。

コマンドライン編集

表 1-1 に、CLI で提供されるコマンドライン編集機能を示します。

表 1-1　コマンドライン編集

キー	説明
Tab	部分的に入力されたコマンド名を補完します。一意な文字のセットを入力して Tab キーを押すと、コマンド名が補完されます。複数のコマンドを示す可能性のある文字のセットを入力すると、エラーを示すビープ音が発生します。コマンドの一部を入力した直後（スペースなし）に疑問符（?）を入力します。これにより、その文字列で始まるコマンドのリストが表示されます。
Back Space	カーソルの左側の文字を消去します。
Enter	コマンドラインで Enter キーを押すと、コマンドが処理されます。ターミナル画面の `---More---` プロンプトで Enter キーを押すと、行がスクロールされます。
Space	ターミナル画面でさらに出力を表示できます。画面に `---More---` の行が表示されているときに Space キーを押すと、次の画面が表示されます。
左矢印（←）	カーソルを 1 文字左に移動します。1 行を超えるコマンドを入力するときには、繰り返し←キーを押し、スクロールしてシステム プロンプトまで戻り、コマンド入力の先頭を確認することができます。
右矢印（→）	カーソルを 1 文字右に移動します。
上矢印（↑）または Ctrl+P	最も新しいコマンドを先頭に、履歴バッファ内のコマンドを再呼び出しします。このキー シーケンスを繰り返すと、より古いコマンドが順に再呼び出しされます。
下矢印（↓）または Ctrl+N	上矢印（↑）キーまたは Ctrl+P キーでコマンドの再呼び出しを行った後で、履歴バッファ内のより新しいコマンドに戻ります。このキー シーケンスを繰り返すと、より新しいコマンドが順に再呼び出しされます。
Ctrl+A	カーソルを行の先頭に移動します。
Ctrl+B	カーソルを 1 文字前に戻します。
Ctrl+D	カーソル位置の文字を削除します。
Ctrl+E	カーソルをコマンドラインの最後に移動します。
Ctrl+F	カーソルを 1 文字先に進めます。
Ctrl-K	カーソル位置からコマンドラインの最後までのすべての文字を削除します。
Ctrl+L	画面をクリアし、システム プロンプトとコマンドラインを再表示します。
Ctrl+T	カーソルの左側の文字とカーソル位置の文字を入れ替えます。
Ctrl+U	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+V	この直後のキー ストロークを編集キー*ではなく*、コマンド入力として扱うようにシステムに指示するコードを挿入します。
Ctrl+W	カーソルの左側の語を削除します。
Ctrl+Y	削除バッファ内の最新のエントリを再呼び出しします。削除バッファには、最後に削除または切り取りを行った 10 項目が含まれています。
Ctrl+Z	コンフィギュレーション モードを終了し、EXEC プロンプトに戻ります。
Esc+B	カーソルを 1 語前に戻します。

表 1-1　コマンドライン編集（続き）

キー	説明
Esc+C	カーソル位置の語を大文字にします。
Esc+D	カーソル位置から語の最後までを削除します。
Esc+F	カーソルを 1 語先に進めます。
Esc+L	カーソル位置の語を小文字にします。
Esc+U	カーソル位置から語の最後までを大文字にします。

IPS コマンド モード

IPS CLI には次のコマンド モードがあります。

- 特権 EXEC：CLI インターフェイスにログインした場合に入るモード。
- グローバル コンフィギュレーション：特権 EXEC モードから **configure terminal** を入力して入るモード。

  コマンド プロンプトは `sensor(config)#` です。
- サービス モード コンフィギュレーション：グローバル コンフィギュレーション モードから **service** *service-name* を入力して入るモード。

  コマンド プロンプトは `sensor(config-ser)#` です。`ser` はサービス名の最初 3 文字です。
- マルチインスタンス サービス モード：グローバル コンフィギュレーション モードから **service** *service-name log-instance-name* を入力して入るモード。

  コマンド プロンプトは `sensor(config-log)#` です。`log` はログ インスタンス名の最初の 3 文字です。システム内のマルチインスタンス サービスは、シグニチャ定義とイベント アクション ルールだけです。

正規表現の構文

正規表現は、文字列の照合に使用されるテキスト パターンです。正規表現では、プレーン テキストと特殊文字を組み合せてどのような照合を実行するかを指示します。たとえば、数字を検索する場合は、検索用の正規表現は「[0-9]」になります。角カッコは、比較対象の文字が角カッコで囲まれた文字のいずれかに一致する必要があることを示します。0 と 9 の間のダッシュ（-）は、0 ～ 9 の範囲を示します。したがって、この正規表現では、0 ～ 9 の任意の文字、つまり任意の数字に一致します。

特定の特殊文字を検索する場合は、その特殊文字の前にバックスラッシュを使用する必要があります。たとえば、1 文字の正規表現「*」は、1 つのアスタリスクと一致します。

この項で定義されている正規表現は、POSIX 拡張正規表現定義のサブセットと類似しています。特に、「[..]」、「[==]」、および「[::]」の表現はサポートされません。また、1 つの文字を表すエスケープ表現はサポートされます。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。

表 1-2 に、特殊文字を示します。

表 1-2　正規表現の構文

文字	説明
^	文字列の先頭。「^A」という表現は、文字列の先頭の「A」だけに一致します。
^	左の角カッコ（[）の直後。角カッコ内の残りの文字をターゲット文字列の照合から除外します。「[^0-9]」という表現は、ターゲット文字が数字ではないことを示します。
$	文字列の最後に一致します。「abc$」という表現は、文字列の最後にある場合にだけ「abc」というサブ文字列に一致します。
|	この記号のいずれか一方の側にある表現とターゲット文字列を照合します。「a|b」という表現は、「a」にも「b」にも一致します。
.	任意の文字に一致します。
*	表現内のアスタリスクの左側の文字の 0 回以上の出現に一致することを示します。
+	* と似ていますが、表現内の + 記号の左側の文字の 1 回以上の出現に一致します。
?	この記号の左側の文字の 0 回または 1 回の出現に一致します。
()	パターン評価の順序に影響します。また、一致したサブ文字列を別の表現で置き換える場合のタグ付き表現にも使用されます。
[]	一連の文字を囲み、囲まれた文字のいずれかがターゲット文字と一致することを示します。
\	この記号を使用しない場合に特殊文字と解釈される文字を指定することができます。 \xHH は、16 進数の文字 [0-9A-Fa-f] で (HH) と表現された値と同じ値を表します。この値は 0 以外である必要があります。 BEL と \x07、BS と \x08、FF と \x0C、LF と \x0A、CR と \x0D、TAB と \x09、VT と \x0B は、それぞれ同じです。 その他のすべての文字では、「c」と「\c」は「c」と同じで、エスケープ文字がなくても特殊文字と解釈されることはありません。

次に、特殊文字の使用例を示します。

- `a*` は、文字 a が一度も出現しない場合も含めて、a の任意の回数の出現に一致します。
- `a+` では、一致する文字列内に文字 a が少なくとも 1 回出現する必要があります。
- `ba?b` は、文字列 bb または bab に一致します。
- `\**` は、任意の個数のアスタリスク（*）に一致します。

複数文字からなるパターンとともに複数回の出現を指定する記号を使用するには、そのパターンを丸カッコで囲みます。

- `(ab)*` は、複数文字からなる文字列 ab の任意の回数の出現に一致します。
- `([A-Za-z][0-9])+` は、アルファベットと数字のペアの 1 回以上の出現に一致しますが、0 回には一致しません（空文字列では一致しません）。

複数回の出現を指定する記号（*、+、または ?）を使用した照合は、長い構造のものから順に行われます。ネストした構造の場合は、外側から内側の順に照合されます。連結された構造の場合は、左側から照合が開始されます。したがって、この正規表現は、A9b3 に一致しますが、9Ab3 には一致しません。これは、文字が数字より前に指定されているからです。

また、丸カッコを使用して 1 つまたは複数の文字からなるパターンを囲むことにより、ソフトウェアにそのパターンを記憶させ、正規表現内の別の場所で使用することができます。

以前に記憶したパターンを再呼び出しする正規表現を作成するには、丸カッコを使用して特定のパターンを記憶するように指示し、バックスラッシュ（\）に続けて数字を指定して、記憶したパターンを再利用します。この数字は、その正規表現パターン内でのその丸カッコの出現場所を示します。正規表現内で記憶したパターンが複数存在する場合は、\1 が最初に記憶したパターンを示し、\2 が 2 番目に記憶したパターンとなり、以下同様に続きます。

次の正規表現では、丸カッコを使用して次のように再呼び出しを行っています。

- **a(.)bc(.)\1\2** は、1 つの *a*、任意の文字、*bc*、任意の文字、最初に出現した*任意の*文字（2 回目）、2 番目に出現した*任意の*文字（2 回目）の順に並んだ文字列に一致します。

  たとえば、この正規表現は aZbcTZT に一致します。ソフトウェアでは、最初の文字と 2 番目の文字としてそれぞれ Z と T を記憶し、その後正規表現内で Z と T を再び使用しています。

汎用 CLI コマンド

次の CLI コマンドは、IPS 5.1 の汎用コマンドです。

- **configure terminal**：グローバル コンフィギュレーション モードに入ります。

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

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

- **service**：analysis-engine、authentication、event-action-rules、host、interface、logger、network-access、notification、signature-definition、ssh-known-hosts、trusted-certificates、web-server の各コンフィギュレーション サブモードに入ります。

（注） event-action-rules と signature-definition の各サブモードは、複数インスタンスに対応したサービスです。どちらの場合も、事前定義済みの 1 つのインスタンスだけが許可されます。event-action-rules では、インスタンス名 rules0 だけがサポートされます。signature-definition では、インスタンス名 sig0 だけがサポートされます。

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

- **end**：コンフィギュレーション モードまたは任意のコンフィギュレーション サブモードを終了します。これにより、トップレベルの EXEC メニューに戻ります。

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

- **exit**：任意のコンフィギュレーション モードを終了するか、アクティブなターミナル セッションを閉じて、EXEC モードを終了します。これにより、直前のメニュー セッションに戻ります。

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

CLI のキーワード

一般に、特定の機能をディセーブルにするには、コマンドの **no** 形式を使用します。ディセーブルになっていた機能をイネーブルにするには、キーワード **no** を付けずに該当のコマンドを使用します。たとえば、コマンド **ssh host-key** *ipaddress* を使用すると、既知のホスト テーブルにエントリが追加され、コマンド **no ssh host-key** *ipaddress* では既知のホスト テーブルからエントリが削除されます。個々のコマンドの **no** 形式で実行される内容については、各コマンドの詳細情報を参照してください。

サービス コンフィギュレーション コマンドにもデフォルト形式を指定できます。コマンドの設定をデフォルトに戻すには、コマンドの **default** 形式を使用します。このキーワードは、アプリケーションの設定に使用される **service** サブメニュー コマンドに適用されます。コマンドとともに **`default`** と入力することにより、パラメータがデフォルト値にリセットされます。**default** キーワードは、コンフィギュレーション ファイルでデフォルト値を指定するコマンドだけで使用することができます。

センサーへのログイン

この章では、センサーにログイン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。

- 概要（P.2-2）
- サポートされるユーザ ロール（P.2-2）
- アプライアンスへのログイン（P.2-3）
- ターミナル サーバのセットアップ（P.2-4）
- IDSM-2 へのログイン（P.2-6）
- NM-CIDS へのログイン（P.2-7）
- AIP SSM へのログイン（P.2-9）
- センサーへのログイン（P.2-10）

概要

同時 CLI セッション数には、プラットフォームごとに制限があります。IDS-4210、IDS-4215、および NM-CIDS では、同時 CLI セッションは 3 つまで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。

サポートされるユーザ ロール

ユーザは、次の特権でログインできます。

- 管理者
- オペレータ
- ビューア
- サービス

  サービス 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センサー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。

アプライアンスへのログイン

アプライアンスには、コンソール ポートからログインするか、モニタとキーボードをセンサーに接続してログインすることができます。

（注） コンソールからセンサーを初期化（**setup** コマンドを実行）する必要があります。ネットワークが設定された後、SSH および Telnet が使用可能になります。手順については、P.2-10 の「センサーへのログイン」を参照してください。

アプライアンスにログインするには、次の手順を実行します。

ステップ 1　アプライアンスにログインします。

- コンソール ポートをセンサーに接続します。
  手順については、P.2-4 の「ターミナル サーバのセットアップ」を参照してください。
- センサーにモニタとキーボードを接続します。

ステップ 2　ログイン プロンプトでユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードは、どちらも **cisco** です。最初にアプライアンスにログインすると、これらを変更するように求められます。まず UNIX パスワードとして、**cisco** を入力します。次に、新規パスワードを 2 度入力する必要があります。

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

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

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

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
ips-4240#
```

ターミナル サーバのセットアップ

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- IDS-4215、IPS-4240、および IPS-4255 の場合は、次の操作を行います。
  - RJ-45 接続の場合、180/ ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
  - ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- その他のアプライアンスの場合は、すべて M.A.S.H. アダプタ（部品番号 29-4077-01）をアプライアンスの COM1 に接続して、次の操作を行います。
  - RJ-45 接続の場合、180/ ロールオーバー ケーブルを M.A.S.H. アダプタからターミナル サーバのポートに接続します。
  - ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルを M.A.S.H. アダプタからターミナル サーバのポートに接続します。

ステップ 2　次のようにターミナル サーバ上にラインおよびポートを設定します。

a. イネーブル モードでは、次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

b. IDS-4215、IPS-4240、または IPS-4255 用にターミナル サーバを設定する場合は、ステップ 3 に進みます。

それ以外の場合は、サポートしている他のすべてのアプライアンスに対して、すべての出力をターミナル サーバに送ります。CLI にログインして、次のコマンドを入力します。

```
sensor# configure terminal
sensor(config)# display-serial
```

出力は、シリアル ポートに送られます。**no display-serial** コマンドを使用して、出力をキーボードとモニタにリダイレクトします。

（注） ターミナル サーバをセットアップし、**display-serial** コマンドを使用して、アプライアンスからの出力すべてをシリアル ポートに送ることができます。このオプションを使用すると、ブート処理中でも、シリアル ポートに接続したコンソールにシステム メッセージを表示できます。このオプションを使用する場合、出力はすべてシリアル ポートに送られ、ローカルのキーボードおよびモニタ接続はディセーブルにされます。ただし、BIOS メッセージと POST メッセージは、ローカルのキーボードおよびモニタ上に表示されます。手順については、P.13-25 の「シリアル接続への出力の転送」を参照してください。

（注） IDS-4215、IPS-4240、および IPS-4255 には、コンソール ポートが 1 つしかありません。したがって、**display-serial** および **no display-serial** コマンドは、これらのプラットフォームには適用されません。

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションが正常に閉じられていることを確認してください。

ターミナル セッションが正常に終了していない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号を受信していない場合、ターミナル セッションは開いたままです。ターミナル セッションが正常に終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証は実行されません。

注意 接続を確立するために使用したアプリケーションを終了する前に、常にセッションを終了してログイン プロンプトに戻ります。

注意 偶発的に接続が切れたり終了したりした場合は、接続を再確立し、正常に終了して、アプライアンスに対する不正なアクセスを防ぎます。

IDSM-2 へのログイン

スイッチから IDSM-2 にログインすることができます。

（注） スイッチからセンサーを初期化（**setup** コマンドを実行）する必要があります。ネットワークが設定された後、SSH および Telnet が使用可能になります。

IDSM-2 に対してセッションを開始するには、次の手順を実行します。

ステップ 1　次のように入力して、スイッチから IDSM-2 に対してセッションを開始します。

- Catalyst ソフトウェアの場合

  `cat6k>(enable) session slot_number`

- Cisco IOS ソフトウェアの場合

  `switch# session slot_number processor 1`

ステップ 2　ログイン プロンプトでユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。最初に IDSM-2 にログインすると、これらを変更するように求められます。まず UNIX パスワードとして、**cisco** を入力します。次に、新規パスワードを 2 度入力する必要があります。

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

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

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

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
idsm-2#
```

NM-CIDS へのログイン

session コマンドを使用してルータ経由で NM-CIDS にアクセスするには、まず内部管理ポートに IP アドレスを割り当てる必要があります。これには、IDS インターフェイスに対して直接 IP アドレスを割り当てるか、番号を持たないループバック インターフェイスを割り当てます。NM-CIDS に対してセッションを開始する前に IP アドレスを設定しておかないと、エラー メッセージが表示されます。

IP アドレスの割り当て後は、ルータのコンソールから NM-CIDS にログインすることができます。

（注） ルータからセンサーを初期化（**setup** コマンドを実行）する必要があります。ネットワークが設定された後、SSH および Telnet が使用可能になります。

NM-CIDS に対してセッションを開始するには、次の手順を実行します。

ステップ 1　次の手順で管理ポートに IP アドレスを割り当てます。

a. IDS インターフェイスに直接 IP アドレスを割り当てます。

```
router(config)# interface IDS-Sensor1/0
router(config-if)# ip unnumbered Loopback0
router(config-if)# exit
```

b. 番号を持たないループバック インターフェイスを割り当てます。

```
router(config)# interface Loopback0
router(config-if)# ip address 1.2.3.4 255.255.255.255
router(config-if)# exit
```

ネットワーク内の他の場所で使用されていないものであれば、任意のアドレスを IP アドレスとして使用できます。

ステップ 2　ルータのコンソールから NM-CIDS に対してセッションを開始します。

```
service-module IDS-Sensor slot_number/0 session
```

ステップ 3　ログイン プロンプトでユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。最初に NM-CIDS にログインすると、これらを変更するように求められます。まず UNIX パスワードとして **cisco** を入力します。次に、新規パスワードを 2 度入力する必要があります。

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

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

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

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

ステップ 4　ルータに対してセッションを開始していた場合は、**Ctrl+Shift+6** キーを押してから **x** キーを押して、ルータのプロンプトに戻ります。

AIP SSM へのログイン

ASA から AIP SSM にログインすることができます。

（注） ASA からセンサーを初期化（**setup** コマンドを実行）する必要があります。ネットワークが設定された後、SSH および Telnet が使用可能になります。

ASA から AIP SSM にログインするには、次の手順を実行します。

ステップ 1　ASA にログインします。

（注） ASA がマルチモードで動作している場合は、**change system** コマンドを使用してシステム レベルのプロンプトに変更してから手順を続行してください。

ステップ 2　AIP SSM に対してセッションを開始します。

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

60 秒以内にログインしないと、セッションがタイムアウトします。

ステップ 3　ログイン プロンプトでユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。最初に AIP SSM にログインすると、これらを変更するように求められます。まず UNIX パスワードとして **cisco** を入力します。次に、新規パスワードを 2 度入力する必要があります。

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

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

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

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

ステップ 4　セッションから抜けて ASA プロンプトに戻るには、次のいずれかを実行します。

- **exit** と入力します。
- **Ctrl+Shift+6** キーを押してから **x** キーを押します（**CTRL^X** と表現されます）。

センサーへのログイン

setup コマンドを使用してセンサーを初期化し、Telnet をイネーブルにしたら、SSH または Telnet を使用してセンサーにログインできます。

ステップ 1　SSH または Telnet を使用してネットワーク経由でセンサーにログインするには、次のコマンドを実行します。

```
ssh sensor_ip_address
telnet sensor_ip_address
```

ステップ 2　ログイン プロンプトでユーザ名とパスワードを入力します。

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

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

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

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

センサーの初期化

この章では、**setup** コマンドを使用してセンサーを初期化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。

- 概要（P.3-2）
- System Configuration Dialog（P.3-2）
- センサーの初期化（P.3-3）
- 初期化の確認（P.3-9）

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。

System Configuration Dialog

setup コマンドを入力すると、システムのコンソール画面に System Configuration Dialog という対話型のダイアログが表示されます。この System Configuration Dialog によって、設定プロセスの手順が示されます。

現在の値は、各プロンプトの横のカッコ内に表示されます。

変更するオプションに到達するまで System Configuration Dialog 全体を実行する必要があります。変更しない項目のデフォルト設定を使用するには、**Enter** キーを押します。

変更を行わず、System Configuration Dialog 全体を実行しないで EXEC プロンプトに戻るには、**Ctrl+C** キーを押します。

System Configuration Dialog では、各プロンプトのヘルプ テキストを表示できます。ヘルプ テキストにアクセスするには、プロンプトで疑問符（?）を押します。

変更が完了したら、セットアップ セッション中に作成した設定が System Configuration Dialog に表示されます。また、この設定を使用するかどうかを尋ねるメッセージが表示されます。**yes** を入力すると、その設定が保存されます。**no** を入力すると、設定は保存されずに、プロセスが再度開始されます。このプロンプトにはデフォルトはありません。**yes** または **no** を入力する必要があります。

サマータイムは、recurring モードまたは date モードのいずれかで設定できます。recurring モードを選択すると、開始日および終了日は、週、日、月、および時間がベースになります。date モードを選択すると、開始日および終了日は、月、日、年、および時間がベースになります。Disable を選択すると、サマータイムがオフになります。

System Configuration Dialog では、デフォルトの仮想センサー vs0 を編集できます。仮想センサーには、混合モードとインライン ペアの両方またはどちらかを割り当てることができます。またこれは、割り当てられたインターフェイスを使用可能にします。セットアップが完了すると、仮想センサーはトラフィックを監視するように設定されています。

（注） システムがアプライアンスで NTP を使用していない場合は、System Configuration Dialog で日付と時間を設定するだけで済みます。

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 に対してセッションを開始します。
  - 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

    ```
    switch# session slot slot_number processor 1
    ```

- NM-CIDS に対してセッションを開始します。

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

- AIP SSM に対してセッションを開始します。

  ```
  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、管理者特権を持つ別のユーザがいないときは、センサー イメージの再作成が必要になることがあります（第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照）。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、P.4-16 の「サービス アカウントの作成」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、「_」、および「-」は有効ですが、スペースは入力できません。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 形式で表わされます。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、P.4-33 の「センサーで NTP 時刻源を使用するための設定」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:
    GigabitEthernet0/0
    GigabitEthernet2/1
    GigabitEthernet2/0
  Promiscuous:
    None
  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 ～ 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、**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 ～ d を繰り返してこのインターフェイスに別のインライン VLAN ペアを追加するか、**Enter** キーを押して次のオプションに進みます。

ステップ 18 別のインターフェイスを分割するには、**yes** を入力します。インライン VLAN ペアの追加を完了するには、**no** を入力するか、**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.18-2 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

setup コマンドを実行した後で、センサーが正しく初期化されたことを確認する必要があります。

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、第 2 章「センサーへのログイン」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 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 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 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+biULJG95hbTF1qO+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。

初期コンフィギュレーション タスク

この章では、初期設定タスクの手順について説明します。初期設定タスクには、センサーのセットアップ情報の変更、ユーザの追加と削除、時刻と NTP の設定、サービス アカウントの作成、SSH と TLS の設定、ライセンス キーのインストールなどがあります。

（注） このような設定のほとんどは、**setup** コマンドを使用してセンサーを初期化したときに行われています。

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変更（P.4-2）
- Web サーバ設定の変更（P.4-12）
- ユーザ パラメータの設定（P.4-14）
- 時刻の設定（P.4-22）
- SSH の設定（P.4-36）
- TLS の設定（P.4-41）
- ライセンス キーのインストール（P.4-45）

ネットワーク設定の変更

センサーの初期化後に、**setup** コマンドを実行したときに行ったネットワーク設定の一部を変更しなければならない場合があります。

この項では、次のトピックについて説明します。

- ホスト名の変更（P.4-2）
- IP アドレス、ネットマスク、およびゲートウェイの変更（P.4-4）
- Telnet のイネーブル化とディセーブル化（P.4-5）
- アクセス リストの変更（P.4-6）
- FTP タイムアウトの変更（P.4-8）
- ログイン バナーの追加（P.4-10）

ホスト名の変更

setup コマンドの実行後にセンサーのホスト名を変更するには、サービス ホスト サブモードで、**host-name** *host_name* コマンドを使用します。デフォルトは sensor です。

（注） 現在のセッションおよびその他の既存セッションの CLI プロンプトに表示されるホスト名は、新しいホスト名にはなりません。その後の CLI ログイン セッションでは、プロンプトに新しいホスト名が反映されます。

センサーのホスト名を変更するには、次の手順を実行します。

ステップ 1　管理者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 2　ネットワーク設定サブモードに入ります。

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

ステップ 3　センサーのホスト名を変更します。

```
sensor(config-hos-net)# host-name firesafe
```

ステップ 4　新しいホスト名を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1 default:
      10.1.9.201/24,10.1.9.1
      host-name: firesafe default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

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

```
sensor(config-hos-net)# default host-name
```

ステップ 6　デフォルトのホスト名である sensor に変更されたことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1 default:
      10.1.9.201/24,10.1.9.1
      host-name: sensor <defaulted>
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

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

ステップ 8　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。

IP アドレス、ネットマスク、およびゲートウェイの変更

setup コマンドの実行後に、IP アドレス、ネットマスク、およびデフォルト ゲートウェイを変更するには、サービス ホスト サブモードで、**host-ip** *ip_address/netmask,default_gateway* コマンドを使用します。デフォルトは、10.1.9.201/24,10.1.9.1 です。

host-ip 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 はネットマスクのビット数です。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。

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

ステップ 1　管理者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 2　ネットワーク設定モードに入ります。

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

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

```
sensor(config-hos-net)# host-ip 10.89.146.110/24,10.89.146.254
```

（注）　デフォルト ゲートウェイは、センサーの IP アドレスと同じサブネット内に存在する必要があります。そうでない場合はエラーが発生し、センサーはコンフィギュレーションの変更を受け入れません。

ステップ 4　新しい情報を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.146.110/24,10.89.146.254
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
```

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

```
sensor(config-hos-net)# default host-ip
```

ステップ 6　ホストの IP がデフォルトの 10.1.9.201/24,10.1.9.1 になったことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

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

ステップ 8　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。

Telnet のイネーブル化とディセーブル化

センサーへのリモート アクセス用に Telnet をイネーブルにするには、サービス ホスト サブモードで、**telnet-option [enabled | disabled]** コマンドを使用します。デフォルトは disable です。

注意　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。

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

ステップ 1　管理者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 2　ネットワーク設定モードに入ります。

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

ステップ 3　Telnet サービスをイネーブルにします。

```
sensor(config-hos-net)# telnet-option enabled
sensor(config-hos-net)#
```

ステップ 4　Telnet がイネーブルになったことを確認します。

```
sensor(config-hos-net)# show settings
  network-settings
  ------------------------------------------------
    host-ip: 10.89.130.108/23,10.89.130.1
    default: 10.1.9.201/24,10.1.9.1
    host-name: sensor default: sensor
    telnet-option: enabled default: disabled
    access-list (min: 0, max: 512, current: 1)
    ------------------------------------------------
       network-address: 0.0.0.0/0
       ------------------------------------------------
    ------------------------------------------------
    ftp-timeout: 300 seconds <defaulted>
    login-banner-text: <defaulted>
------------------------------------------------
sensor(config-hos-net)#
```

ステップ 5　ネットワーク設定モードを終了します。

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

ステップ 6　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。

(注)　センサーに Telnet で接続するには、Telnet をイネーブルにし、Telnet クライアントが接続できるようにアクセス リストを設定します。手順については、P.4-6 の「アクセス リストの変更」を参照してください。

アクセス リストの変更

アクセス リストを設定するには、サービス ホスト サブモードで、`access-list` *ip_address/netmask* コマンドを使用します。アクセス リストは、センサーへのアクセスを許可するホストまたはネットワークのリストです。リストからエントリを削除するには、このコマンドの **no** 形式を使用します。デフォルトのアクセス リストは空です。

アクセス リストには、次のホストのエントリが存在する必要があります。

- センサーに Telnet で接続する必要のあるホスト。
- センサーに対して SSH を使用する必要のあるホスト。
- Web ブラウザからセンサーにアクセスする必要のある、IDM などのホスト。
- センサーにアクセスする必要のある、VMS などの管理ステーション。
- 該当のセンサーがマスター ブロッキング センサーの場合、リストにはブロッキング転送センサーの IP アドレスのエントリが必要です。

アクセス リストを変更するには、次の手順を実行します。

ステップ 1　管理者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 2　ネットワーク設定モードに入ります。

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

ステップ 3　アクセス リストにエントリを追加します。

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

1 つのホストのネットマスクは 32 です。

ステップ 4　アクセス リストに対して行った変更を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ----------------------------------------------
      host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
      host-name: sensor <defaulted>
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      ---------------------------------------------
         network-address: 10.1.9.0/24
         ---------------------------------------------
         network-address: 10.89.146.110/32
         ---------------------------------------------
      ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ----------------------------------------------
```

ステップ 5　アクセス リストからエントリを削除します。

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

ステップ 6　エントリが削除されたことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ----------------------------------------------
      host-ip: 10.1.9.201/24,10.1.9.1 <defaulted>
      host-name: sensor <defaulted>
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ---------------------------------------------
         network-address: 10.1.9.0/24
         ---------------------------------------------
      ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ----------------------------------------------
sensor(config-hos-net)#
```

ホストはリストに存在していません。

ステップ 7　値をデフォルトに戻します。

```
sensor(config-hos-net)# default access-list
```

ステップ 8　値がデフォルト設定に戻ったことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor <defaulted>
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
sensor(config-hos-net)#
```

リストにはホストもネットワークも存在しません。

ステップ 9　ネットワーク設定モードを終了します。

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

ステップ 10　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。

FTP タイムアウトの変更

センサーと FTP サーバとの通信中に FTP クライアントがタイムアウトになるまでに待つ時間（秒単位）を変更するには、サービス ホスト サブモードで **ftp-timeout** コマンドを使用します。デフォルトは 300 秒です。

（注）　FTP クライアントは、FTP サーバから更新やコンフィギュレーション ファイルをダウンロードする際に使用することができます。

FTP タイムアウトを変更するには、次の手順を実行します。

ステップ 1　管理者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 2　ネットワーク設定モードに入ります。

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

ステップ 3　FTP タイムアウトの時間（秒単位）を変更します。

```
sensor(config-hos-net)# ftp-timeout 500
```

ステップ 4　FTP タイムアウトの変更を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
       ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
    ------------------------------------------------
      ftp-timeout: 500 seconds default: 300
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

ステップ 5　値をデフォルトに戻します。

```
sensor(config-hos-net)# default ftp-timeout
```

ステップ 6　値がデフォルト設定に戻ったことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

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

ステップ 8　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。

ログイン バナーの追加

ユーザのログイン時に表示されるログイン バナーを追加するには、**login-banner-text** *text_message* コマンドを使用します。デフォルトはありません。

メッセージ内で新しい行を開始する場合は、**Ctrl+V+Enter** キーを押します。

ログイン バナーを追加するには、次の手順を実行します。

ステップ 1　管理者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 2　ネットワーク設定モードに入ります。

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

ステップ 3　ログイン バナー テキストを入力します。

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

ステップ 4　ログイン バナー テキスト メッセージを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ---------------------------------------------
         network-address: 0.0.0.0/0
         ---------------------------------------------
    ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: This is the banner login text message. default:
   -----------------------------------------------
sensor(config-hos-net)#
```

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

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

ステップ 6　ログイン テキストが削除されたことを確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.130.108/23,10.89.130.1
      default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 1)
      ------------------------------------------------
         network-address: 0.0.0.0/0
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: default:
   ------------------------------------------------
sensor(config-hos-net)#
```

ステップ 7　ネットワーク設定モードを終了します。

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

ステップ 8　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。

Web サーバ設定の変更

setup コマンドの実行後に、Web サーバ設定を変更することができます。変更できる設定は、Web サーバ ポート、TLS 暗号化を使用するかどうか、および HTTP サーバ ヘッダー メッセージです。

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

HTTP は、Web クライアントが Web ブラウザから要求を行う場合に使用するプロトコルです。HTTP の仕様では、サーバは各応答で自らの ID を示す必要があります。攻撃者は、このプロトコルの機能を悪用して偵察を行う場合があります。IPS Web サーバが推測可能な応答を返すことによって自らの ID を示していると、攻撃者が IPS センサーの存在に気付く可能性があります。

IPS センサーの存在が攻撃者にわからないようにすることをお勧めします。特に、Web サーバがインターネットから使用可能になっている場合は、情報がまったく漏れないような **server-id** に変更してください。

たとえば、センサーをリモートで監視できるようにポートをファイアウォール経由で転送する場合は、**server-id** を設定する必要があります。

Web サーバ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　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 2　Web サーバ モードに入ります。

```
sensor# configure terminal
sensor(config)# service web-server
```

ステップ 3　ポート番号を変更します。

```
sensor(config-web)# port 8080
```

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

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

ステップ 4　TLS をイネーブルまたはディセーブルにします。

```
sensor(config-web)# enable-tls [true | false]
```

TLS をディセーブルにすると、次のメッセージが表示されます。

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

ステップ 5　HTTP サーバ ヘッダーを変更します。

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

ステップ 6　Web サーバの変更を確認します。

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

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

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

ステップ 8　デフォルトに置換されたことを確認します。

```
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)#
```

ステップ 9　Web サーバ モードを終了します。

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

ステップ 10　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。

（注）　ポートや TLS のイネーブル化の設定を変更した場合は、センサーをリセットして、新しい設定が Web サーバで使用されるようにする必要があります。

ユーザ パラメータの設定

次の項では、サービス アカウントとユーザの作成、パスワードの変更、特権レベルの指定、ユーザリストの表示の各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。

- ユーザの追加と削除（P.4-14）
- パスワード リカバリ（P.4-16）
- サービス アカウントの作成（P.4-16）
- パスワードの設定（P.4-18）
- ユーザの特権レベルの変更（P.4-18）
- ユーザのステータスの表示（P.4-19）
- アカウントのロックの設定（P.4-20）

ユーザの追加と削除

ローカル システムでユーザを作成するには、**username** コマンドを使用します。新規ユーザの追加、特権レベル（管理者、オペレータ、ビューア）の設定、および新規ユーザのパスワードの設定を実行することができます。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。この形式を使用すると、CLI と Web アクセスからユーザが削除されます。

注意　**username** コマンドは、ログインだけを目的としたユーザ名とパスワード認証を提供します。システムにログインしているユーザをこのコマンドで削除することはできません。このコマンドを使用して、コマンドの発行者自身をシステムから削除することはできません。

パスワードを指定しないと、指定するように求められます。既存ユーザのパスワードを変更するには、**password** コマンドを使用します。既存ユーザの特権を変更するには、**privilege** コマンドを使用します。

有効なパスワードの長さは 6 ～ 32 文字です。スペースと「?」を除くすべての文字を使用できます。

有効なパスワードを作成しないと、次のエラー メッセージが表示されます。

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

（注）　**privilege** コマンドを使用してユーザ サービス特権を与えることはできません。既存のユーザ サービス特権を使用する場合は、そのユーザを削除してから、**username** コマンドを使用してサービス アカウントを作成する必要があります。手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

ユーザを追加または削除するには、次の手順に従います。

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　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　ユーザのパラメータを指定します。

```
sensor(config)# username username password password privilege
administrator/operator/viewer
```

(注)　有効な username には 1 ～ 64 の英数字が含まれます。ユーザ名には下線（_）またはダッシュ（-）を使用することもできます。有効なパスワードの長さは 6 ～ 32 文字です。スペースと「?」を除くすべての文字を使用できます。

たとえば、管理者特権レベルを持ち、パスワードが「testpassword」であるユーザ「tester」を作成するには、次のコマンドを入力します。

(注)　パスワードをクリア テキストで表示しないようにするには、パスワード プロンプトを待ちます。パスワードをユーザ名と特権とともに入力しないでください。

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

(注)　ユーザの特権レベルを指定しない場合、ユーザにはデフォルトの viewer 特権が割り当てられます。

ステップ 4　ユーザが追加されたことを確認します。

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

ユーザのリストが表示されます。

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

```
sensor# configure terminal
sensor(config)# no username jsmith
```

ステップ 6　ユーザが削除されたことを確認します。

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

ユーザ jsmith が削除されました。

(注)　このコマンドを使用して、コマンドの発行者自身をシステムから削除することはできません。

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、P.4-16 の「サービス アカウントの作成」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、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

サービス アカウントの作成

TAC がトラブルシューティングの際に使用するサービス アカウントを作成することができます。センサーには複数のユーザがアクセスできますが、1 つのセンサーでサービス特権を持つユーザは 1 人だけです。サービス アカウントは、サポート専用です。

注意　TAC の指示がない限り、サービス アカウントを使用してセンサーを変更しないでください。サービス アカウントを使用してセンサーを設定した場合、そのコンフィギュレーションは TAC でサポートされません。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、その他の IPS サービスの適切なパフォーマンスと機能に影響が出ます。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。

(注)　サービス アカウントが作成されると、root ユーザのパスワードはサービス アカウントのパスワードに同期化されます。root でアクセスするには、サービス アカウントでログインしてから **su - root** コマンドを使用して root ユーザに切り替える必要があります。

注意　サービス アカウントを作成するかどうかは慎重に検討してください。サービス アカウントは、システムへのシェル アクセスを提供します。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　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　サービス アカウントのパラメータを指定します。

```
sensor(config)# user username privilege service
```

有効な username には 1 ～ 64 の英数字が含まれます。ユーザ名には下線（_）またはダッシュ（-）を使用することもできます。

ステップ 4　プロンプトが表示されたら、パスワードを指定します。

該当のセンサーにすでにサービス アカウントが存在する場合は、次のエラーが表示され、サービス アカウントは作成されません。

```
Error: Only one service account allowed in UserAccount document
```

ステップ 5　コンフィギュレーション モードを終了します。

```
sensor(config)# exit
sensor#
```

サービス アカウントを使用して CLI にログインすると、次の警告が表示されます。

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

パスワードの設定

ローカル センサーでパスワードを更新するには、**password** コマンドを使用します。また、このコマンドを使用して、既存ユーザのパスワードを変更したり、ロックされたアカウントのパスワードをリセットしたりすることができます。

有効なパスワードの長さは 6 ～ 32 文字です。スペースと「?」を除くすべての文字を使用できます。

パスワードを変更するには、次の手順を実行します。

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

a. 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。

b. コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

c. 特定のユーザのパスワードを変更します。

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

（注） この例では、ユーザ「tester」のパスワードを変更しています。

ステップ 2　パスワードを変更するには、次の手順を実行します。

a. CLI にログインします。

b. コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

c. パスワードを変更します。

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

ユーザの特権レベルの変更

ユーザの特権レベル（管理者、オペレータ、ビューア）を変更するには、**privilege** コマンドを使用します。

（注） **privilege** コマンドを使用してユーザ サービス特権を与えることはできません。既存のユーザ サービス特権を使用する場合は、そのユーザを削除してから、**username** コマンドを使用してサービス アカウントを作成する必要があります。サービス特権を持つユーザは 1 人だけです。手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

ユーザの特権レベルを変更するには、次の手順を実行します。

ステップ 1　管理者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　ユーザ *jsmith* の現在の特権を確認します。

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

ステップ 3　特権レベルをビューアからオペレータに変更します。

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

ステップ 4　ユーザの特権が変更されたことを確認します。

```
sensor(config)# exit
sensor# show users all

    CLI ID   User       Privilege
*   13491    cisco      administrator
             jsmith     operator
             operator   operator
             service    service
             viewer     viewer
sensor#
```

ユーザ `jsmith` の特権が `viewer` から `operator` に変更されました。

ステップ 5　自分の現在の特権レベルを表示します。

```
sensor# show privilege
Current privilege level is administrator
```

ユーザのステータスの表示

センサーにログインしているすべてのユーザのユーザ名と特権の情報、および、ログインのステータスとは関係なく、センサー上に存在しているすべてのユーザ アカウントを表示するには、**show users** コマンドを使用します。

* は、現在のユーザを示します。アカウントがロックされている場合は、ユーザ名が丸カッコで囲まれます。ロックされたアカウントは、そのユーザが、設定されている試行回数を超えて正しいパスワードの入力に失敗したことを示します。

（注） 同時 CLI セッション数は、プラットフォームごとに制限されています。IDS-4210、IDS-4215、および NM-CIDS では、同時セッションは 3 つまでに制限されています。その他のすべてのプラットフォームでは、10 セッションが許可されます。

ユーザ情報を表示するには、次の手順を実行します。

ステップ 1　管理者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　センサーにログインしているユーザを確認します。

```
sensor# show users
    CLI ID   User       Privilege
*   13491    cisco      administrator
sensor#
```

ステップ 3　すべてのユーザを確認します。

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

ユーザ jsmith のアカウントは、ロックされています。

ステップ 4　jsmith のアカウントをアンロックするには、パスワードをリセットします。

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

アカウントのロックの設定

ユーザが一定回数の試行に失敗した後でそれ以上ログインの試行を続けることができないようにアカウントをロックするには、認証サブモードで **attemptLimit** *number* コマンドを使用します。デフォルトは 0 で、認証の試行回数に制限はありません。セキュリティ上の理由から、この回数は変更する必要があります。

アカウントのロックを設定するには、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センサーにログインします。

ステップ 2　サービス認証モードに入ります。

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

ステップ 3　ユーザがアカウントにログインするための試行回数を設定します。

```
sensor(config-aut)# attemptLimit 3
```

ステップ 4　新しい設定を確認します。

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

ステップ 5　値をシステムのデフォルト設定に戻すには、次のコマンドを実行します。

```
sensor(config-aut)# default attemptLimit
```

ステップ 6　設定がデフォルトに戻ったことを確認します。

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

ステップ 7　アカウントがロックされているユーザがいるかどうかを確認します。

(注)　attemptLimit にゼロ以外の値が含まれるコンフィギュレーションを適用すると、SSH サーバに変更が加えられ、その後のセンサーへの接続機能に影響が出る可能性があります。attemptLimit がゼロ以外である場合、SSH サーバに対してクライアントはチャレンジ / レスポンス認証をサポートする必要があります。SSH クライアントが接続してからパスワードのプロンプトが出るまでの間に問題が発生する場合は、チャレンジ / レスポンス認証をイネーブルにする必要があります。手順については、SSH クライアントのマニュアルを参照してください。

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

ユーザ jsmith のアカウントは、丸カッコで囲まれているのでロックされています。

ステップ 8　jsmith のアカウントをアンロックするには、パスワードをリセットします。

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

時刻の設定

この項では、信頼できる時刻源をセンサーに設定することの重要性について説明します。取り上げる事項は次のとおりです。

- 時刻源およびセンサー（P.4-22）
- センサー上の時刻の修正（P.4-24）
- センサーでの時刻の設定（P.4-24）
- NTP の設定（P.4-32）

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、第 3 章「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、P.13-10 の「手動によるクロック設定」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。P.4-32 の「Cisco ルータの NTP サーバとしての設定」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。P.4-32 の「Cisco ルータの NTP サーバとしての設定」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。P.4-32 の「Cisco ルータの NTP サーバとしての設定」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。P.4-32 の「Cisco ルータの NTP サーバとしての設定」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。

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。センサーの最初のセットアップ中に、時刻を 8:00 a.m. と指定するところを 8:00 p.m. と誤って設定した場合、エラーを修正すると、修正した時刻は過去にさかのぼって設定されます。このため、新しいイベントの時刻が、古いイベントの時刻よりも以前になる場合があります。

たとえば、初期セットアップ中に、サマータイムをイネーブルにして中部時間にセンサーを設定し、現地時間が 8:04 p.m. である場合、時刻は 20:04:37 CDT と表示され、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統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、P.4-32 の「Cisco ルータの NTP サーバとしての設定」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。

センサーでの時刻の設定

この項では、イベントに正しくタイムスタンプが記録されるようにセンサーで時刻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。

- システム クロック（P.4-24）
- サマータイムの設定（P.4-26）
- 時間帯の設定（P.4-31）

システム クロック

この項では、アプライアンスのシステム クロックを表示し、手動で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。

- システム クロックの表示（P.4-24）
- システム クロックの手動設定（P.4-25）

システム クロックの表示

システム クロックを表示するには、**show clock** [**detail**] コマンドを使用します。**detail** オプションを使用して、クロック ソース（NTP またはシステム）と現在のサマータイム設定（ある場合）を示すことができます。

システム クロックは、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックが NTP などの時刻源によって設定されている場合は、フラグが設定されます。

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

システム クロックを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
sensor# show clock
22:39:21 UTC Sat Jan 25 2003
```

ステップ 3　システム クロックを詳細に表示します。

```
sensor# show clock detail
22:39:21 CST Sat Jan 25 2003
Time source is NTP
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、センサーが NTP から時間を取得していることと、設定および同期されていることを示しています。

```
sensor# show clock detail
*12:19:22 CST Sat Dec 04 2004
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、時刻源が設定されていないことを示しています。

システム クロックの手動設定

アプライアンスのクロックを手動で設定するには、**clock set** *hh:mm [:ss] month day year* コマンドを使用します。その他の時刻源を使用できない場合は、このコマンドを使用します。

（注）　センサーが NTP クロック ソースなど有効な外部の時刻メカニズムと同期している場合、システム クロックを設定する必要はありません。

NTP の設定手順については、P.4-32 の「NTP の設定」を参照してください。有効な時刻源をセンサーに設定することの重要性については、P.4-22 の「時刻源およびセンサー」を参照してください。クロックを誤って設定した場合の対処方法については、P.4-24 の「センサー上の時刻の修正」を参照してください。

clock set コマンドは、次のプラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- AIP SSM 10
- AIP SSM 20

アプライアンスに手動でクロックを設定するには、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 CLI にログインします。

ステップ 2　クロックを手動で設定します。

```
sensor# clock set 13:21 July 29 2004
```

（注）　時刻形式は 24 時間です。

サマータイムの設定

センサーの初期化時にサマータイムを設定しなかった場合でも、サマータイムを設定できます。また、初期化後にこれらの設定を変更することもできます。

（注）　サマータイムとは、Daylight Saving Time（夏時間）のことです。

この項では、次のトピックについて説明します。

- 定期的なサマータイムの設定（P.4-26）
- 一度のみのサマータイムの設定（P.4-29）

定期的なサマータイムの設定

定期的にサマータイム設定に切り替わるようにセンサーを設定するには、**summertime-option recurring** コマンドを使用します。デフォルトは recurring です。

定期的にサマータイム設定に切り替わるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者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 2　recurring summertime サブモードに入ります。

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

ステップ 3　start summertime サブモードに入ります。

```
sensor(config-hos-rec)# start-summertime
```

ステップ 4　start summertime パラメータを設定します。

d. サマータイム設定の開始曜日を入力します。

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

e. サマータイム設定の開始月を入力します。

```
sensor(config-hos-rec-sta)# month april
```

f. サマータイム設定の開始時刻を入力します。

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

形式は hh:mm:ss です。

g. サマータイム設定の開始週を入力します。

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

値は 1 番目から 5 番目、または最後です。

h. 設定を確認します。

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

ステップ 5　end summertime サブモードに入ります。

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

ステップ 6　end summertime パラメータを設定します。

a. サマータイム設定の終了曜日を入力します。

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

b. サマータイム設定の終了月を入力します。

```
sensor(config-hos-rec-end)# month october
```

c. サマータイム設定の終了時刻を入力します。

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

形式は hh:mm:ss です。

d. サマータイム設定の終了週を入力します。

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

値は 1 番目から 5 番目、または最後です。

e. 設定を確認します。

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

ステップ 7　サマータイム中に使用するローカル時間帯を指定します。

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

ステップ 8　オフセットを指定します。

```
sensor(config-hos-rec)# offset 60
```

ステップ 9　設定を確認します。

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

ステップ 10　recurring summertime サブモードを終了します。

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

ステップ 11　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。

一度のみのサマータイムの設定

一度だけサマータイム設定に切り替わるようにセンサーを設定するには、**summertime-option non-recurring** コマンドを使用します。デフォルトは recurring です。

一度だけサマータイム設定に切り替わるようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者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 2　non-recurring summertime サブモードに入ります。

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

ステップ 3　start summertime サブモードに入ります。

```
sensor(config-hos-non)# start-summertime
```

ステップ 4　start summertime パラメータを設定します。

a.　サマータイム設定の開始日を指定します。

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

形式は yyyy-mm-dd です。

b.　サマータイム設定の開始時刻を入力します。

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

形式は hh:mm:ss です。

c.　設定を確認します。

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

ステップ 5　end summertime サブモードに入ります。

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

ステップ 6　end summertime パラメータを設定します。

a.　サマータイム設定の終了日を入力します。

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

形式は yyyy-mm-dd です。

b.　サマータイム設定の終了時刻を入力します。

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

形式は hh:mm:ss です。

c. 設定を確認します。

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

ステップ 7　サマータイム中に使用するローカル時間帯を指定します。

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

ステップ 8　オフセットを指定します。

```
sensor(config-hos-non)# offset 60
```

ステップ 9　設定を確認します。

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

ステップ 10　non-recurring summertime サブモードを終了します。

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

ステップ 11　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。

時間帯の設定

センサーの時間帯を設定するには、**time-zone-settings** コマンドを使用します。設定には、サマータイム設定が有効でない場合にセンサーが表示する時間帯の名前やオフセットなどがあります。

センサーの時間帯を設定するには、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センサーにログインします。

ステップ 2　時間帯設定サブモードに入ります。

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

ステップ 3　サマータイム設定が有効でない場合に表示される時間帯名を設定します。

デフォルトは UTC です。

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

ステップ 4　オフセットを分単位で設定します。

オフセットは、現地時間を得るために UTC に足す時間（分単位）です。デフォルトは 0 です。

```
sensor(config-hos-tim)# offset -360
```

ステップ 5　設定を確認します。

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

ステップ 6　時間帯設定サブモードを終了します。

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

ステップ 7　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。

NTP の設定

この項では、Cisco ルータを NTP サーバとして設定する方法、および NTP サーバを時刻源として使用するようにセンサーを設定する方法について説明します。

この項では、次のトピックについて説明します。

- Cisco ルータの NTP サーバとしての設定（P.4-32）
- センサーで NTP 時刻源を使用するための設定（P.4-33）

Cisco ルータの NTP サーバとしての設定

センサーが NTP サーバを時刻源として使用する場合、センサーと NTP サーバの間には認証された接続が必要になります。センサーは、鍵の暗号化に MD5 ハッシュ アルゴリズムだけをサポートします。Cisco ルータをアクティブにして NTP サーバとして動作するようにし、その内部クロックを時刻源として使用するには、次の手順を実行します。

注意　センサー NTP 機能は、NTP サーバとして動作する Cisco ルータと互換性があるように設計されています。センサーはその他の NTP サーバとともに動作しますが、テストやサポートはされていません。

（注）　NTP サーバの鍵 ID と鍵値を忘れないでください。これらの情報は、NTP サーバを時刻源として使用するようにセンサーを設定する際に、NTP サーバの IP アドレスとともに必要になります。この手順については、P.4-33 の「センサーで NTP 時刻源を使用するための設定」を参照してください。

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

ステップ 1　ルータにログインします。

ステップ 2　コンフィギュレーション モードに入ります。

```
router# configure terminal
```

ステップ 3　鍵 ID と鍵値を作成します。

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

鍵 ID には、1 ～ 65535 までの数値を指定できます。鍵値はテキストです（数字または文字）。この値は後で暗号化されます。

例

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

（注）　センサーは、MD5 鍵だけをサポートします。

（注） 鍵は、すでにルータ上に存在しているものでもかまいません。他の鍵を確認するには、**show running configuration** コマンドを使用します。これらの値は、ステップ 4 で trusted key として使用することができます。

ステップ 4　ステップ 3 で作成した鍵を trusted key として指定します（既存の鍵を使用してもかまいません）。

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

trusted key の ID は、ステップ 3 の鍵 ID と同じ数字です。

例

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

ステップ 5　センサーが通信するルータ上のインターフェイスを指定します。

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

例

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

ステップ 6　センサーに割り当てる NTP マスター ストラタム番号を指定します。

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

例

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

NTP マスター ストラタム番号は、NTP 階層内でのサーバの相対的な位置を示します。1 ～ 15 の数字を選択できます。どの番号を選択しても、センサーではそれほど重要ではありません。

センサーで NTP 時刻源を使用するための設定

センサーには、一貫性のある時刻源が必要です。NTP サーバを使用することをお勧めします。NTP サーバを時刻源として使用するようにセンサーを設定するには、次の手順を実行します。

注意　センサー NTP 機能は、NTP サーバとして動作する Cisco ルータと互換性があるように設計されています。センサーはその他の NTP サーバとともに動作しますが、テストやサポートはされていません。

（注） NTP サーバから、NTP サーバの IP アドレス、NTP サーバの鍵 ID、および鍵値を取得する必要があります。詳細については、P.4-32 の「Cisco ルータの NTP サーバとしての設定」を参照してください。

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

ステップ 1　管理者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　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　サービス ホスト モードに入ります。

```
sensor(config)# service host
```

ステップ 4　NTP コンフィギュレーション モードに入ります。

```
sensor(config-hos)# ntp-option enable
```

ステップ 5　NTP サーバの IP アドレスと鍵 ID を入力します。

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

鍵 ID は 1 ～ 65535 の数字です。この数字は、NTP サーバで設定済みの鍵 ID です。P.4-32 の「Cisco ルータの NTP サーバとしての設定」のステップ 3 を参照してください。

例

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

ステップ 6　NTP サーバの鍵値を入力します。

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

鍵値はテキストです（数字または文字）。この値は、NTP サーバで設定済みの鍵値です。P.4-32 の「Cisco ルータの NTP サーバとしての設定」のステップ 3 を参照してください。

例

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

ステップ 7　NTP 設定を確認します。

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

ステップ 8　NTP コンフィギュレーション モードを終了します。

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

ステップ 9　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。

SSH の設定

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

- SSH について（P.4-36）
- 既知のホスト リストへのホストの追加（P.4-36）
- SSH 許可公開鍵の追加（P.4-38）
- 新しい SSH サーバ鍵の生成（P.4-40）

SSH について

SSH は、安全でないチャネル上で強力な認証と安全な通信を可能にします。

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。

- パスワード
- ユーザ RSA 公開鍵

SSH は、次の攻撃に対する防御を可能にします。

- 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。

既知のホスト リストへのホストの追加

SSH の既知ホスト リストにホストを追加して、そのホストが SSH を使用して通信可能であることをセンサーが認識できるようにする必要があります。このようなホストには、センサーがアップグレードやファイルのコピーのために接続する必要のある SSH サーバのほか、センサーがブロッキングのために接続する、Cisco ルータ、PIX Firewall、Catalyst スイッチなどのホストがあります。

既知のホスト リストにエントリを追加するには、**ssh host-key** *ip-address* [*key-modulus-length public-exponent public-modulus*] コマンドを使用します。係数、指数、長さの値がわからない場合は、要求された IP アドレスの MD5 フィンガープリントと Bubble Babble が表示されます。その後、鍵をリストに追加することができます。

注意　**ssh host-key** *ip-address* コマンドを使用すると、要求された鍵をネットワーク経由で入手するために、指定された IP アドレスの SSH サーバに対して接続が行われます。指定したホストは、コマンドが発行されるときにアクセス可能である必要があります。ホストに到達できない場合は、このコマンドの完全な形式である、**ssh host-key** *ip-address* [*key-modulus-length public-exponent public-modulus*] を使用して、表示された鍵のフィンガープリントを確認し、攻撃者の鍵を受け入れないように防御する必要があります。

(注)　IP アドレスの鍵を変更するには、エントリを削除してから再作成する必要があります。エントリを削除するには、このコマンドの **no** 形式を使用します。

SSH の既知ホスト リストに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　管理者特権またはオペレータ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　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　既知ホスト リストにエントリを追加します。

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

MD5 フィンガープリントが表示されます。これを既知ホスト リストに追加するように求めるメッセージが表示されます。

コマンドを発行したときにホストにアクセスできない場合は、次のメッセージが表示されます。

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

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

ステップ 5　ホストが追加されたことを確認します。

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

ステップ 6　特定の IP アドレスの鍵を表示します。

```
sensor# show ssh host-keys 10.16.0.0
1024 35
139306213541835240385332922253968814685684523520064131997839905113640120217816869696 70
872170463132284429207385173056504487908267067755415793705848520399557211463129660455 21
613097126010686148127499695935137405983313931548849883023021829223533351526538605891 63
651944997842874583627883277460138506084043415861927
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

ステップ 7　エントリを削除します。

```
sensor(config)# no ssh host-key 10.16.0.0
```

SSH の既知ホスト リストからホストが削除されます。

ステップ 8　ホストが削除されたことを確認します。

```
sensor(config)# exit
sensor# show ssh host-keys
```

IP アドレスはリストに表示されません。

SSH 許可公開鍵の追加

SSH サーバへのログインで RSA 認証の使用を許可されたクライアント用の公開鍵を定義するには、**ssh authorized-key** コマンドを使用します。

次のオプションが適用されます。

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

センサーにログインできる各ユーザは、許可公開鍵のリストを持ちます。対応する RSA 秘密鍵のいずれかにアクセスできる SSH クライアントは、パスワードを入力しなくても、ユーザとしてセンサーにログインすることができます。

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（係数の長さ、公開指数、公開係数）のセットとして表示し、これらの数字を **ssh authorized-key** コマンドのパラメータとして入力します。

（注）　SSH 許可鍵のリストは、各自設定します。管理者がセンサー上の他のユーザの SSH 許可鍵のリストを管理することはできません。

（注） SSH 許可鍵を使用すると、秘密鍵が適切に保護されていれば、パスワードより優れたセキュリティを実現できます。最も推奨される方法は、秘密鍵が使用されるホストと同じホストに秘密鍵を作成し、ローカル ファイルシステム上にパス フレーズを使用して鍵を保管することです。パスワードまたはパス フレーズのプロンプトを最小限にするには、鍵エージェントを使用します。

（注） 許可鍵を変更するには、エントリを削除してから再作成する必要があります。エントリを削除するには、このコマンドの **no** 形式を使用します。ユーザが作成および削除できるのは、自分の鍵だけです。

現在のユーザの SSH 許可鍵のリストに鍵エントリを追加するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在のユーザの許可鍵のリストに鍵を追加します。

```
sensor# configure terminal
sensor(config)# ssh authorized-key system1 1023 37
66022272955660983338089706716372943357082868686000817201780243492180421420781303592082
95091017013584805250399939321125031474527683786209111899866537160898131479220860447399
11341369642870682319361928148521864094557416306138786468335115835910404940213136954353
39616344979349705016792583146548622146467421997057
sensor(config)#
```

ステップ 3　鍵が追加されたことを確認します。

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

ステップ 4　特定の ID の鍵を表示します。

```
sensor# show ssh authorized-keys system1
1023 37 66022272955660983338089706716372943357082868686000817201780243492180421 4
2078130359208295091017013584805250399939321125031474527683786209111899866537160 8
98131479220860447399113413696428706823193619281485218640945574163061387864683351
15835910404940213136954353396163449793497050167925831465486221464674219970 57
sensor#
```

ステップ 5　SSH 許可鍵のリストからエントリを削除します。

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

SSH 許可鍵のリストから鍵が削除されます。

ステップ 6　エントリが削除されたことを確認します。

```
sensor(config)# exit
sensor# show ssh authorized-keys
```

鍵の system1 はリストに表示されなくなります。

以前の ID を入力すると、エラー メッセージが表示されます。

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

新しい SSH サーバ鍵の生成

SSH サーバ ホスト鍵を変更するには、**ssh generate-key** コマンドを使用します。リモート クライアントが SSH 1.5 を使用している場合、表示されるフィンガープリントは、その後のセンサーとの接続でリモート SSH クライアントに表示されるフィンガープリントと同じです。

新しい SSH サーバ ホスト鍵を生成するには、次の手順を実行します。

ステップ 1　管理者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　新しいサーバ ホスト鍵を生成します。

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

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。リモート システムの既知のホスト テーブルは、**ssh host-key** コマンドを使用して更新できます。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 3　現在の SSH サーバ ホスト鍵を表示します。

```
sensor# show ssh server-key
1024 35
137196765426571419509124895787229630062726389801071715581921573847280637533000158590028
79807438582486718433236475889995967537052387960937617481217922841521578294902918396220
78407317716458035098372594754214772124597971708065107160775560107531693126750238604749
87441651041217710152766990480431898217878170000647
MD5: 93:F5:51:58:C7:FD:40:8C:07:26:5E:29:13:C8:33:AE
Bubble Babble: ximal-sudez-kusot-gosym-levag-fegoc-holez-cakar-kunel-nylis-kyxox
sensor#
```

TLS の設定

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

- TLS について（P.4-41）
- TLS の信頼できるホストの追加（P.4-42）
- サーバ証明書の表示と生成（P.4-44）

TLS について

IPS 5.1 には、IDM を実行する Web サーバが含まれます。VMS などの管理ステーションは、この Web サーバに接続します。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、最初は IDM が提示する証明書を拒否します。これは、Certificate Authority（CA; 認証局）を信用しないためです。

（注）　IDM は、デフォルトで TLS と SSL を使用するようにイネーブルになっています。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。

TLS の信頼できるホストの追加

特定の状況では、センサーは TLS/SSL を使用して、リモート Web サーバとの間に確立したセッションを保護します。これらのセッションを man-in-the-middle 攻撃から保護するには、リモート Web サーバの TLS 証明書の信頼を確立する必要があります。信頼できる各リモート ホストの TLS 証明書のコピーは、信頼できるホストのリストに保存されます。

信頼できるホストのリストに信頼できるホストを追加するには、**tls trusted-host ip-address** *ip-address* [**port** *port*] コマンドを使用します。このコマンドでは、指定されたホストおよびポートから TLS 証明書が取得され、そのフィンガープリントが表示されます。追加を要求しているホストから直接取得した情報に基づいて、このフィンガープリントを受け入れるか、拒否することができます。デフォルトのポートは 443 です。

各証明書は、識別子フィールド（**id**）とともに保存されます。IP アドレスとデフォルト ポートの場合、識別子フィールドは **ipaddress** です。IP アドレスと特定のポートの場合、識別子フィールドは **ipaddress:port** になります。

注意　要求されたフィンガープリントをネットワーク経由で入手するために、指定された IP アドレスの TLS に対して接続が行われます。指定したホストは、コマンドが発行されるときにアクセス可能である必要があります。別の方法を使用してフィンガープリントを確認し、攻撃者の証明書を受け入れないように防御してください。

信頼できるホストのリストに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　管理者特権またはオペレータ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　信頼できるホストを追加します。

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

MD5 および SHA1 のフィンガープリントが表示されます。信頼できるホストを追加するように求めるメッセージが表示されます。

接続を確立できない場合、トランザクションは失敗します。

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

ステップ 3　**yes** を入力してフィンガープリントを受け入れます。

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

ホストが TLS の信頼できるホストのリストに追加されました。コマンドが成功すると、要求された証明書用に保存された証明書 ID が表示されます。

ステップ 4　ホストが追加されたことを確認します。

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

ステップ 5　特定のホストのフィンガープリントを表示します。

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

ステップ 6　信頼できるホストのリストからエントリを削除します。

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

信頼できるホストのリストからホストが削除されます。

ステップ 7　信頼できるホストのリストからエントリが削除されたことを確認します。

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

この IP アドレスはリストに表示されなくなります。

サーバ証明書の表示と生成

TLS 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。サーバの新しい自己署名 X.509 証明書を生成するには、**tls generate-key** コマンドを使用します。

（注） 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 アドレスを変更すると、新しい証明書が自動的に生成されます。

注意 新しい証明書で既存の証明書が置換されるため、以後の接続が成功するようにリモート システムの信頼できるホストのリストを新しい証明書で更新する必要があります。リモート IPS センサーの信頼できるホストのリストは、**tls trusted-host** コマンドを使用して更新できます。手順については、P.4-42 の「TLS の信頼できるホストの追加」を参照してください。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要求を送信するリモート センサーにある信頼できるホストのリストを更新する必要があります。

新しい TLS 証明書を生成するには、次の手順を実行します。

ステップ 1　管理者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　新しい証明書を生成します。

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

ステップ 3　鍵が生成されたことを確認します。

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

ライセンス キーのインストール

この項では、IPS のライセンス キーとそのインストール方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.4-45）
- IPS 製品のサービス プログラム（P.4-45）
- ライセンス キーの入手とインストール（P.4-47）

概要

センサーはライセンス キーなしでも動作しますが、シグニチャ アップデートを入手するには、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、Cisco Services for IPS 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.4-45 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。手順については、P.4-47 の「ライセンス キーの入手とインストール」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、または 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

すべての IPS 製品では、ライセンス キーをダウンロードし、IPS シグニチャ アップデートを入手するために、Cisco Services for IPS サービス契約が必要です。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 サービス契約は、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 の追加が必要になり、ASA-SSM-AIP-10-K9 を購入した場合は、この時点で 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.4-45 の「ライセンス キーのインストール」を参照してください。

注意　お使いの製品で Return Materials Authorization（RMA）を実行した場合、シリアル番号は変更されます。その後、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。

ライセンス キーの入手とインストール

センサーにライセンス キーをコピーするには、**copy** *source-url license_file_name* **license-key** コマンドを使用します。

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.4-36 の「既知のホスト リストへのホストの追加」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.4-42 の「TLS 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。

(注) ライセンス キーを申し込む前に、Cisco Services for IPS サービス契約が必要です。詳細については、P.4-45 の「IPS 製品のサービス プログラム」を参照してください。

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 5.1(1)S182.0

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-5.1-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.1(1)S182


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#
```

インターフェイスの設定

この章では、センサー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。インターフェイスは、**setup** コマンドを使用してセンサーを初期化したときに設定されていますが、インターフェイス コンフィギュレーションへの変更や追加を行う必要がある場合は、次の手順を実行します。インターフェイスを設定する最も簡単な方法については、P.3-3 の「センサーの初期化」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。

- インターフェイスの説明（P.5-2）
- 物理インターフェイスの設定（P.5-9）
- 混合モード（P.5-13）
- インライン インターフェイス モード（P.5-14）
- インライン VLAN ペア モード（P.5-17）
- インライン バイパス（P.5-23）
- 仮想センサーへのインターフェイスの割り当て（P.5-25）
- インターフェイスの通知の設定（P.5-27）

インターフェイスの説明

センサーのインターフェイスには、最高速度とインターフェイスの物理的な場所に従って名前が付けられています。物理的な場所は、ポート番号とスロット番号で構成されます。センサーに組み込みのインターフェイスはすべてスロット 0 にあり、PCI 拡張スロットは、一番下にあるスロット 1 から順に、上に行くほどスロット番号が大きくなります。各スロットのインターフェイスでは、一番右にあるポート　0　から順に、左に行くほどポート番号が大きくなります。たとえば、GigabitEthernet2/1 は 1 ギガビットの最高速度をサポートする、下から 2 番目の PCI 拡張スロットの右から 2 番目のインターフェイスです。IPS-4240 と IPS-4255 には、このルールは当てはまりません。これらのセンサーのコマンド / コントロール インターフェイスは、GigabitEthernet0/0 ではなく、Management0/0 と呼ばれます。

各物理インターフェイスは、コマンド / コントロール、センシング、および代替 TCP リセットの 3 つのいずれかの役割を果たします。

この項では、次のトピックについて説明します。

- コマンド / コントロール インターフェイス（P.5-2）
- センシング インターフェイス（P.5-3）
- インターフェイス サポート（P.5-4）
- TCP リセット インターフェイス（P.5-5）
- コンフィギュレーション シーケンス（P.5-7）
- インターフェイスのコンフィギュレーションの制約事項（P.5-7）

コマンド / コントロール インターフェイス

コマンド / コントロール インターフェイスは、IP アドレスを持ち、センサーの設定に使用されます。このインターフェイスは、センサーからセキュリティ イベントとステータス イベントを受信し、センサーに統計情報を問い合せます。

コマンド / コントロール インターフェイスは、常にイネーブルです。このインターフェイスは特定の物理インターフェイス（センサーのモデルによって異なる）に常時マッピングされています。コマンド / コントロール インターフェイスをセンシング インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。

表 5-1 に、各センサーのコマンド / コントロール インターフェイスのリストを示します。

表 5-1　コマンド / コントロール インターフェイス

センサー	コマンド / コントロール インターフェイス
IDS-4210	FastEthernet0/1
IDS-4215	FastEthernet0/0
IDS-4235	GigabitEthernet0/1
IDS-4250	GigabitEthernet0/1
IPS-4240	Management0/0
IPS-4255	Management0/0
NM-CIDS	FastEthernet0/0
AIP SSM 10	GigabitEthernet0/0
AIP SSM 20	GigabitEthernet0/0
IDSM-2	GigabitEthernet0/2

センシング インターフェイス

センシング インターフェイスは、セキュリティ違反がないかどうかについてトラフィックを分析するために、センサーによって使用されます。センサーには 1 つ以上のセンシング インターフェイスがあり、この数はセンサーによって異なります。各センサーで使用可能なセンシング インターフェイスの数とタイプについては、P.5-4 の「インターフェイス サポート」を参照してください。

センシング インターフェイスは、混合モードで個別に動作させるか、ペアにして、インライン センシング モード用のインライン インターフェイスを作成することができます。詳細については、P.5-13 の「混合モードについて」、P.5-14 の「インライン インターフェイス モードについて」、および P.5-17 の「インライン VLAN ペア モードについて」を参照してください。

(注) アプライアンスでは、すべてのセンシング　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。これらのインターフェイスを使用するには、イネーブルにする必要があります。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す。

一部のアプライアンスでは、センサーにセンシング インターフェイスを追加するオプションの PCI インターフェイス カードをサポートしています。これらのオプション カードの挿入と取り外しは、センサーの電源が切れているときに行う必要があります。センサーは、サポートしているインターフェイス カードの追加または削除を検出します。オプションの PCI カードを取り外すと、速度、二重、説明用の文字列、インターフェイスのイネーブル / ディセーブルの状態、インライン インターフェイスのペア情報（存在する場合）など、いくつかのインターフェイス コンフィギュレーションが削除されます。カードを再び取り付けると、これらの設定はデフォルト設定で復元されます。ただし、分析エンジンに割り当てられた混合モード インターフェイスおよびインライン インターフェイスは、分析エンジンのコンフィギュレーションから削除されません。これらの設定は、該当のカードが再び挿入され、インライン インターフェイス ペアを再作成するまでの間、無視されます。詳細については、P.5-25 の「仮想センサーへのインターフェイスの割り当て」を参照してください。

インターフェイス サポート

表 5-2 に、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 5-2　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 5-2　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。

TCP リセット インターフェイス

この項では、TCP リセット インターフェイスと、このインターフェイスを使用する場合について説明します。取り上げる事項は次のとおりです。

- 代替 TCP リセット インターフェイスについて（P.5-5）
- 代替 TCP リセット インターフェイスの指定（P.5-6）

代替 TCP リセット インターフェイスについて

攻撃者のホストと攻撃のターゲット ホストとの間のネットワーク接続をリセットするために、TCP リセット パケットを送信するようにセンサーを設定することができます。一部のインストールでは、インターフェイスが混合モードで動作している場合に、攻撃を検出したセンシング インターフェイスと同じインターフェイスでセンサーが TCP リセット パケットを送信できない場合があります。このような場合には、センシング インターフェイスを代替 TCP リセット インターフェイスに関連付け、混合モードで動作している場合に通常はセンシング インターフェイスで送信されるすべての TCP リセットを、関連付けられている代替 TCP リセット インターフェイスで送信することができます。詳細については、P.5-6 の「代替 TCP リセット インターフェイスの指定」を参照してください。

センシング インターフェイスが代替 TCP リセット インターフェイスに関連付けられている場合、その関連付けは、センサーが混合モードで設定されている場合には適用されますが、センシング インターフェイスがインライン モードで設定されている場合は無視されます。

IDSM-2 を除いて、すべてのセンシング インターフェイスは別のセンシング 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なることができます。IDSM-2 の代替 TCP リセット インターフェイスは、ハードウェアの制限があるために固定されています。

表 5-3 に、代替 TCP リセット インターフェイスのリストを示します。

表 5-3　代替 TCP リセット インターフェイス

センサー	代替 TCP リセット インターフェイス
IDS-4210	なし[1]
IDS-4215	任意のセンシング インターフェイス
IDS-4235	任意のセンシング インターフェイス
IDS-4250	任意のセンシング インターフェイス
IPS-4240	任意のセンシング インターフェイス
IPS-4255	任意のセンシング インターフェイス
NM-CIDS	なし[2]
AIP SSM 10	なし[3]
AIP SSM 20	なし[4]
IDSM-2	System0/1[5]

1. IDS-4210 上にあるセンシング インターフェイスは 1 つだけです。
2. NM-CIDS 上にあるセンシング インターフェイスは 1 つだけです。
3. AIP SSM 10 上にあるセンシング インターフェイスは 1 つだけです。
4. AIP SSM 20 上にあるセンシング インターフェイスは 1 つだけです。
5. Catalyst バックプレーン上に 1 つの内部インターフェイスがあります。

代替 TCP リセット インターフェイスの指定

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。

コンフィギュレーション シーケンス

センサーで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。

1. インターフェイスの物理的な設定（速度、二重、および管理状態）を行います。

   手順については、P.5-9 の「物理インターフェイスの設定」を参照してください。

2. インライン インターフェイスまたはインライン VLAN サブインターフェイス（またはその両方）を作成し、インライン バイパス モードを設定します。

   詳細については、P.5-14 の「インライン インターフェイス モード」、P.5-17 の「インライン VLAN ペア モード」、および P.5-23 の「インライン バイパス」を参照してください。

3. 仮想センサーに、物理インターフェイス、サブインターフェイス、およびインライン インターフェイスを割り当てます。

   手順については、P.5-25 の「仮想センサーへのインターフェイスの割り当て」を参照してください。

インターフェイスのコンフィギュレーションの制約事項

センサーでのインターフェイスの設定には、次の制約事項があります。

- 物理インターフェイス
  - 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。
  - 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 の 1000-SX および XL）の場合、有効な速度設定は 1000 Mbps と自動です。
  - ギガビット銅インターフェイス（IDS-4235、IDS-4250、IPS-4240、および IPS-4255 の 1000-TX）の場合、有効な速度設定は 10 Mbps、100 Mbps、1000 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（銅またはファイバ）インターフェイスでは、速度が 1000 Mbps に設定されている場合、有効な二重設定は自動だけになります。
  - コマンド / コントロール インターフェイスをセンシング インターフェイスとして使用することはできません。
- インライン インターフェイス ペア
  - 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、異なるメディア タイプ、速度、および二重設定のインターフェイスをペアにすることについては、完全にテストまたはサポートされていません。詳細については、P.5-4 の「インターフェイス サポート」を参照してください。
  - コマンド/コントロール インターフェイスをインライン インターフェイス ペアのメンバー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、1 つのインライン インターフェイス ペアのメンバーにすることしかできません。
  - 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。

- 物理インターフェイスは、その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** である場合以外は、インライン インターフェイス ペアのメンバーにすることはできません。

- インライン VLAN インターフェイス ペア
  - 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 インターフェイスでは、VLAN は 1 つのインライン VLAN ペアのメンバーにすることしかできません。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。
  - 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。
- 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。コマンド / コントロール 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で **none** に設定され、センシング インターフェイス以外のすべてのインターフェイスから保護されています。
  - 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。
  - コマンド / コントロール インターフェイスをセンシング インターフェイスの代替 TCP インターフェイスとして使用することはできません。
  - センシング インターフェイスは、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）。

物理インターフェイスの設定

混合モード インターフェイスを設定するには、サービス インターフェイス サブモードで、**physical-interfaces** *interface name* コマンドを使用します。インターフェイス名は FastEthernet または GigabitEthernet です。センサーで設定可能なインターフェイスのリストについては、P.5-4 の「インターフェイス サポート」を参照してください。

（注） AIP SSM は、IPS の CLI からではなく、ASA の CLI から混合モードに設定されます。手順については、P.14-4 の「AIP SSM へのトラフィックの送信」を参照してください。

次のオプションが適用されます。

- **admin-state [enabled | disabled]**：インターフェイスがイネーブルかディセーブルかを示すインターフェイスの管理リンク状態。

  （注） すべてのモジュール（IDSM-2 NM-CIDS および AIP SSM）のすべてのバックプレーン センシング インターフェイスで、**admin-state** は enabled に設定され、保護されています（この設定は変更できません）。**admin-state** は、コマンド / コントロール インターフェイスには影響を及ぼしません（保護されています）。これは、センシング インターフェイスにのみ影響を及ぼします。コマンド / コントロール インターフェイスは監視できないので、イネーブルにする必要はありません。

- **alt-tcp-reset-interface**：このインターフェイスが混合モードでモニタリングに使用され、シグニチャの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に、代替インターフェイスで TCP リセットを送信します。代替 TCP リセット インターフェイスの詳細については、P.5-5 の「代替 TCP リセット インターフェイスについて」およびP.5-6 の「代替 TCP リセット インターフェイスの指定」を参照してください。

  （注） 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。

  （注） このオプションは、モジュール（IDSM-2、NM-CIDS、および AIP SSM）、およびセンシング インターフェイスが 1 つしかないアプライアンス（追加の NIC カードを搭載していない IDS-4210、IDS-4215、IDS-4235、および IDS-4250）では保護されています。

  - **interface-name**：このインターフェイスが混合モードでモニタリングに使用され、シグニチャの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に、TCP リセットを送信するインターフェイスの名前。この設定は、このインターフェイスがインライン インターフェイスのメンバーである場合は無視されます。
  - **none** ：代替 TCP リセット インターフェイスの使用をディセーブルにします。混合モードでリセット アクションによってトリガーされた TCP リセットは、このインターフェイスから送信されます。

- **default**：値をシステム デフォルト設定に戻します。
- **description**：混合モード インターフェイスの説明。

- **duplex**：インターフェイスの二重通信設定。
  - **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。

（注） **duplex** オプションはすべてのモジュールで保護されています。

- **no**：エントリまたは選択設定を削除します。
- **speed**：インターフェイスの速度設定。
  - **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**：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**：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）。

（注） **speed** オプションはすべてのモジュールで保護されています。

センサーで混合モード 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　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　インターフェイス サブモードに入ります。

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

ステップ 3　使用可能なインターフェイスのリストを表示します。

```
sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
sensor(config-int)# physical-interfaces
```

ステップ 4　混合モード用のインターフェイスを選択します。

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

ステップ 5　インターフェイスをイネーブルにします。

```
sensor(config-int-phy)# admin-state enabled
```

インターフェイスを仮想センサーに割り当て（P.5-25 の「仮想センサーへのインターフェイスの割り当て」を参照してください）、トラフィックの監視をイネーブルにする必要があります。

ステップ 6　このインターフェイスの説明を追加します。

```
sensor(config-int-phy)# description INT1
```

ステップ 7　二重通信設定を設定します。

```
sensor(config-int-phy)# duplex full
```

このオプションはモジュールでは使用できません。

ステップ 8　速度を設定します。

```
sensor(config-int-phy)# speed 1000
```

このオプションはモジュールでは使用できません。

ステップ 9　必要に応じて、このインターフェイスの TCP リセットをイネーブルにします。

```
sensor(config-int-phy)# alt-tcp-reset-interface interface-name GigabitEthernet2/0
```

ステップ 10　混合モード インターフェイスとして指定するその他のインターフェイスがあれば、インターフェイスごとにステップ 4 ～ 9 を繰り返します。

ステップ 11　設定を確認します。

（注）　subinterface-type がデフォルトの *none* になっていることを確認してください。**subinterface-type** コマンドは、インライン VLAN ペアを設定する場合に使用します。詳細については、P.5-17 の「インライン VLAN ペアの設定」を参照してください。

```
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/2
   ----------------------------------------------
      media-type: tx <protected>
      description: INT1 default:
      admin-state: enabled default: disabled
      duplex: full default: auto
      speed: 1000 default: auto
     alt-tcp-reset-interface
     ---------------------------------------------
        interface-name: GigabitEthernet2/0
     ---------------------------------------------
     subinterface-type
     ---------------------------------------------
        none
        ---------------------------------------------
        ---------------------------------------------
     ---------------------------------------------
  ----------------------------------------------
sensor(config-int-phy)#
```

ステップ 12 インターフェイスから TCP リセットを削除するには、次の手順を実行します。

```
sensor(config-int-phy)# alt-tcp-reset-interface none
```

ステップ 13 設定を確認します。

```
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/0
   ----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: disabled <protected>
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      ----------------------------------------------
         none
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
sensor(config-int-phy)#
```

ステップ 14 インターフェイス サブモードを終了します。

```
sensor(config-int-phy)# exit
sensor(config-int)# 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。

混合モード

この項では、センサーの混合モードについて説明します。取り上げる事項は次のとおりです。

- 混合モードについて（P.5-13）
- 混合モードの設定（P.5-13）

混合モードについて

混合モードでは、パケットはセンサー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センサー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ことを、センサーが阻止できないという短所があります。混合モードのセンサー デバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に対応するには、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 アタックでは、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。

混合モードの設定

デフォルトでは、すべてのセンシング インターフェイスは混合モードです。インターフェイスをインライン モードから混合モードに変更するには、該当のインターフェイスを含むすべてのインライン インターフェイスを削除し、インターフェイスのコンフィギュレーションから、そのインターフェイスのすべてのインライン VLAN ペアのサブインターフェイスを削除します。

インライン インターフェイス モード

この項では、センサーのインライン モードについて説明します。取り上げる事項は次のとおりです。

- インライン インターフェイス モードについて（P.5-14）
- インライン インターフェイス モードの設定（P.5-14）

インライン インターフェイス モードについて

インライン インターフェイス モードで運用する場合は IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。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。これにより、センサーは、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ドロップして攻撃を阻止し、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。

（注） ペアになっているインターフェイスが同じスイッチに接続されている場合は、それらのインターフェイスをスイッチ上で 2 つのアクセス ポートとして設定し、それぞれが異なる VLAN アクセスを持つようにします。このようにしないと、トラフィックはインライン インターフェイスを通過しません。

インライン インターフェイス モードの設定

インライン インターフェイスを設定するには、サービス インターフェイス サブモードで **inline-interfaces** コマンドを使用します。

（注） AIP SSM は、IPS の CLI からではなく、ASA の CLI からインライン インターフェイス モードに設定されます。手順については、P.14-4 の「AIP SSM へのトラフィックの送信」を参照してください。

次のオプションが適用されます。

- **inline-interfaces**：論理インライン インターフェイス ペアの名前。
- **default**：値をシステム デフォルト設定に戻します。
- **description**：インライン インターフェイス ペアの説明。
- **interface1**：インライン インターフェイス ペアの最初のインターフェイス。
- **interface2**：インライン インターフェイス ペアの 2 番目のインターフェイス。
- **no**：エントリまたは選択設定を削除します。

インライン 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　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　インターフェイス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

ステップ 3　インライン インターフェイスでペアにする両方の物理インターフェイスで、サブインターフェイス モードが「none」であることを確認します。

```
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 2)
   ----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
         subinterface-type
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
```

ステップ 4　インライン ペアの名前を指定します。

```
sensor(config-int)# inline-interfaces PAIR1
```

ステップ 5　使用可能なインターフェイスを表示します。

```
sensor(config-int)# interface1?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet0/2     GigabitEthernet0/2 physical interface.
GigabitEthernet0/3     GigabitEthernet0/3 physical interface.
Management0/0          Management0/0 physical interface.
```

ステップ 6　2 つのインターフェイスをペアとして設定します。

```
sensor(config-int-inl)# interface1 GigabitEthernet0/0
sensor(config-int-inl)# interface2 GigabitEthernet0/1
```

ステップ 7　インターフェイス ペアの説明を追加します。

```
sensor(config-int-inl)# description pairs interfaces Gig0/0 and Gig0/1
```

ステップ 8　インライン インターフェイス ペアとして設定するその他のインターフェイスがあれば、インターフェイスごとにステップ 4 ～ 7 を繰り返します。

ステップ 9　設定を確認します。

```
sensor(config-int-inl)# show settings
   name: PAIR1
   -----------------------------------------------
      description: PAIR1 = Gig0/0 & Gig0/1 default:
      interface1: GigabitEthernet0/0
      interface2: GigabitEthernet0/1
   -----------------------------------------------
```

ステップ 10　インライン インターフェイス ペアを削除してインターフェイスを混合モードに戻すには、次の手順を実行します。

```
sensor(config-int-inl)# exit
sensor(config-int)#
```

ステップ 11　インターフェイス ペアに割り当てられたインターフェイスをイネーブルにします。

```
sensor(config-int)# physical-interfaces GigabitEthernet0/0
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# exit
sensor(config-int)#
```

ステップ 12　インターフェイス コンフィギュレーション サブモードを終了します。

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

ステップ 13　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。

インライン VLAN ペア モード

この項では、インライン VLAN ペア モード、およびインライン 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。

- インライン VLAN ペア モードについて（P.5-17）
- インライン VLAN ペアの設定（P.5-17）

インライン VLAN ペア モードについて

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」と呼ばれます。ペアの一方の VLAN で受信したパケットが分析され、ペアのもう一方の VLAN に転送されます。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すべての VLAN で受信したすべてのパケットを破棄します。

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、サービス インターフェイス サブモードで、**physical-interfaces** *interface name* コマンドを使用します。インターフェイス名は FastEthernet または GigabitEthernet です。

次のオプションが適用されます。

- **admin-state [enabled | disabled]**：インターフェイスがイネーブルかディセーブルかを示すインターフェイスの管理リンク状態。

（注）すべてのモジュール（IDSM-2 NM-CIDS および AIP SSM）のすべてのバックプレーン センシング インターフェイスで、**admin-state** は enabled に設定され、保護されています（この設定は変更できません）。**admin-state** は、コマンド / コントロール インターフェイスには影響を及ぼしません（保護されています）。これは、センシング インターフェイスにのみ影響を及ぼします。コマンド / コントロール インターフェイスは監視できないので、イネーブルにする必要はありません。

- **default**：値をシステム デフォルト設定に戻します。
- **description**：インターフェイスの説明。
- **duplex**：インターフェイスの二重通信設定。
  - **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。

（注）　**duplex** オプションはすべてのモジュールで保護されています。

- **no**：エントリまたは選択設定を削除します。
- **speed**：インターフェイスの速度設定。
  - **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**：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**：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）。

（注）　**speed** オプションはすべてのモジュールで保護されています。

- **subinterface-type**：インターフェイスがサブインターフェイスであることを示し、定義するサブインターフェイスのタイプを指定します。
  - **inline-vlan-pair**：サブインターフェイスをインライン VLAN ペアとして定義します。
  - **none**：サブインターフェイスを定義しません。
- **subinterface**：サブインターフェイスをインライン VLAN ペアとして定義します。
  - **vlan1**：インライン VLAN ペアの最初の VLAN。
  - **vlan2**：インライン VLAN ペアの 2 番目の VLAN。

センサーでインライン 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 CLI にログインします。

ステップ 2　インターフェイス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)#
```

ステップ 3　インライン インターフェイスが存在するかどうかを確認します（インライン インターフェイスが設定されていなければ、サブインターフェイス タイプに「none」と表示されます）。

```
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 5)
   ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      <protected entry>
      name: GigabitEthernet0/2 <defaulted>
      ------------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
         subinterface-type
         ------------------------------------------------
            none
            ------------------------------------------------
            ------------------------------------------------
         ------------------------------------------------
```

```
      ---------------------------------------------
      <protected entry>
      name: GigabitEthernet0/3 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      <protected entry>
      name: Management0/0 <defaulted>
      ---------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
         subinterface-type
         ---------------------------------------------
            none
            ---------------------------------------------
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
   command-control: Management0/0 <protected>
   inline-interfaces (min: 0, max: 999999999, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   bypass-mode: auto <defaulted>
   interface-notifications
   ---------------------------------------------
      missed-percentage-threshold: 0 percent <defaulted>
      notification-interval: 30 seconds <defaulted>
      idle-interface-delay: 30 seconds <defaulted>
   ---------------------------------------------
sensor(config-int)#
```

ステップ 4　この物理インターフェイスを使用しているインライン インターフェイスが存在する場合は、削除します。

```
sensor(config-int)# no inline-interfaces interface_name
```

ステップ 5　使用可能なインターフェイスのリストを表示します。

```
sensor(config-int)# physical-interfaces ?
GigabitEthernet0/0      GigabitEthernet0/0 physical interface.
GigabitEthernet0/1      GigabitEthernet0/1 physical interface.
GigabitEthernet0/2      GigabitEthernet0/2 physical interface.
GigabitEthernet0/3      GigabitEthernet0/3 physical interface.
Management0/0           Management0/0 physical interface.
sensor(config-int)# physical-interfaces
```

ステップ 6　インターフェイスを選択します。

```
sensor(config-int)# physical-interfaces GigabitEthernet0/2
```

ステップ 7　インターフェイスをイネーブルにします。

```
sensor(config-int-phy)# admin-state enabled
```

インターフェイスを仮想センサーに割り当て（P.5-25 の「仮想センサーへのインターフェイスの割り当て」を参照してください）、トラフィックの監視をイネーブルにする必要があります。

ステップ 8　このインターフェイスの説明を追加します。

```
sensor(config-int-phy)# description INT1
```

ステップ 9　二重通信設定を設定します。

```
sensor(config-int-phy)# duplex full
```

このオプションはモジュールでは使用できません。

ステップ 10　速度を設定します。

```
sensor(config-int-phy)# speed 1000
```

このオプションはモジュールでは使用できません。

ステップ 11　インライン VLAN ペアを設定します。

```
sensor(config-int-phy)# subinterface-type inline-vlan-pair
sensor(config-int-phy-inl)# subinterface 1
sensor(config-int-phy-inl-sub)# vlan1 52
sensor(config-int-phy-inl-sub)# vlan2 53
```

ステップ 12　インライン VLAN ペアの説明を追加します。

```
sensor(config-int-phy-inl-sub)# description pairs vlans 52 and 53
```

ステップ 13 インライン VLAN ペアの設定を確認します。

```
sensor(config-int-phy-inl-sub)# show settings
   subinterface-number: 1
   ----------------------------------------------
      description: VLANpair1 default:
      vlan1: 52
      vlan2: 53
   ----------------------------------------------
sensor(config-int-phy-inl-sub)#
```

ステップ 14 インターフェイス サブモードを終了します。

```
sensor(config-int-phy-inl-sub)# exit
sensor(config-int-phy-inl)# exit
sensor(config-int-phy)# exit
sensor(config-int)# 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。

インライン バイパス

この項では、インライン インターフェイスおよびインライン VLAN ペアとして設定された、センサーのインライン バイパスについて説明します。取り上げる事項は次のとおりです。

- インライン バイパスについて（P.5-23）
- バイパス モードの設定（P.5-23）

インライン バイパスについて

インライン バイパスは、診断ツールおよびフェールオーバーの保護メカニズムとして使用できます。通常、パケットの分析はセンサーの分析エンジンが実行します。インライン バイパスをアクティブにすると、分析エンジンがバイパスされ、トラフィックが検査されずにインライン インターフェイスとインライン VLAN ペアを通過します。インライン バイパスを使用すると、センサーのプロセスがアップグレードのために一時的に停止している場合や、センサーのモニタリング プロセスが失敗した場合にも、パケットが継続してセンサーを通過します。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）　インライン バイパス機能はソフトウェアで実装されているため、オペレーティング システムが実行されている場合にだけ機能します。センサーの電源を切ったり、センサーをシャットダウンしたりすると、インライン バイパスが機能しなくなり、トラフィックはセンサーを通過しなくなります。

バイパス モードの設定

バイパス モードを設定するには、サービス インターフェイス サブモードで **bypass-mode** コマンドを使用します。

次のオプションが適用されます。

- **off**：インライン バイパスをオフにします。インライン データ トラフィックに対してパケット検査が実行されます。ただし、分析エンジンが停止すると、インライン トラフィックが中断されます。
- **on**：インライン バイパスをオンにします。トラフィックに対してパケット検査は実行されません。インライン トラフィックは分析エンジンが停止しても流れ続けます。
- **auto**：分析エンジンによるパケット処理が停止した場合に、自動的にインライン パケット検査のバイパスを開始します。これにより、インライン インターフェイスでのデータの中断が防止されます。これがデフォルトの方法です。

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　インターフェイス サブモードに入ります。

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

ステップ 3　バイパス モードを設定します。

```
sensor(config-int)# bypass-mode off
```

ステップ 4　設定を確認します。

```
sensor(config-int)# show settings
-----------------------------------------------
 bypass-mode: off default: auto
 interface-notifications
 ----------------------------------------------
    missed-percentage-threshold: 0 percent <defaulted>
    notification-interval: 30 seconds <defaulted>
    idle-interface-delay: 30 seconds <defaulted>
 ----------------------------------------------
sensor(config-int)#
```

ステップ 5　インターフェイス サブモードを終了します。

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

ステップ 6　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。

仮想センサーへのインターフェイスの割り当て

仮想センサーに混合モード インターフェイスを割り当てるには、仮想センサー サブモードで、**physical-interface** *interface_name* コマンドを使用します。仮想センサーにインライン VLAN ペアを持つサブインターフェイスを割り当てるには、仮想センサー サブモードで、**physical-interface** *interface_name* **subinterface-number** *subinterface_number* コマンドを実行します。仮想センサーにインライン インターフェイス ペアを割り当てるには、仮想センサー サブモードで、**logical-interface** *inline_interface_pair_name* コマンドを使用します。

仮想センサーにインライン インターフェイス ペアまたはインライン VLAN ペアを割り当てる前に、それらが作成されていることを確認してください。

仮想センサーにインターフェイスを割り当てるには、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　仮想センサー サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)# virtual-sensor vs0
```

ステップ 3　使用可能なインターフェイスのリストを表示します。

```
sensor(config-ana-vir)# physical-interfaces ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet2/0     GigabitEthernet2/0 physical interface.
GigabitEthernet2/1     GigabitEthernet2/1 physical interface.
sensor(config-ana-vir)# physical-interfaces
```

ステップ 4　仮想センサーに混合モード インターフェイスを割り当てます。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0
```

すべての混合モード インターフェイスでステップ 4 を繰り返します。

ステップ 5　センサーにインライン インターフェイス ペアを割り当てます。

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

すべてのインライン インターフェイス ペアのインターフェイスでステップ 5 を繰り返します。

ステップ 6　仮想センサーにインライン VLAN ペアを持つサブインターフェイスを割り当てます。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

インライン VLAN ペアを持つすべてのサブインターフェイスでステップ 6 を繰り返します。

ステップ 7　分析エンジンモードを終了します。

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

ステップ 8　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。

インターフェイスの通知の設定

特定のインターフェイスを通過するパケットのフローを監視して、指定された間隔内でフローに変化（開始または停止）があった場合に通知を送信するようにセンサーを設定することができます。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。

トラフィックの通知を設定するには、サービス インターフェイス サブモードで **interface-notifications** コマンドを使用します。

次のオプションが適用されます。

- **default**：値をシステム デフォルト設定に戻します。
- **idle-interface-delay**：インターフェイスがどれだけの間アイドル状態になっていると通知が送信されるかを示す時間（秒単位）。有効な範囲は 5 ～ 3600 です。デフォルトは 30 秒です。
- **missed-percentage-threshold**：指定された間隔内でどれだけのパケットを受け取れない場合に通知が送信されるかを示すパケットの比率。有効な範囲は 1 ～ 100 です。デフォルトは 0 です。
- **notification-interval**：受信できなかったパケットの比率を確認する間隔。有効な範囲は 5 ～ 3600 です。デフォルトは 30 秒です。

インターフェイスの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 CLI にログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　インターフェイス サブモードに入ります。

```
sensor(config)# service interface
```

ステップ 4　インターフェイス通知サブモードに入ります。

```
sensor(config-int)# interface-notifications
```

ステップ 5　idle-interface-delay を設定します。

```
sensor(config-int-int)# idle-interface-delay 60
```

ステップ 6　missed-percentage-threshold を設定します。

```
sensor(config-int-int)# missed-percentage-threshold 1
```

ステップ 7　notification-interval を設定します。

```
sensor(config-int-int)# notification-interval 60
```

ステップ 8　設定を確認します。

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

ステップ 9　インターフェイス通知サブモードを終了します。

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

ステップ 10　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。

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。

- イベント アクション ルールについて（P.6-2）
- Signature Event Action Processor（P.6-2）
- イベント アクション（P.6-4）
- イベント アクション ルールを設定するためのタスク リスト（P.6-7）
- イベント アクション変数（P.6-7）
- ターゲットの価値評価（P.6-9）
- イベント アクション オーバーライド（P.6-11）
- イベント アクション フィルタ（P.6-14）
- 汎用設定（P.6-20）
- イベント アクション ルールの例（P.6-25）
- イベントのモニタリング（P.6-26）

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

Signature Event Action Processor

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.6-9 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）

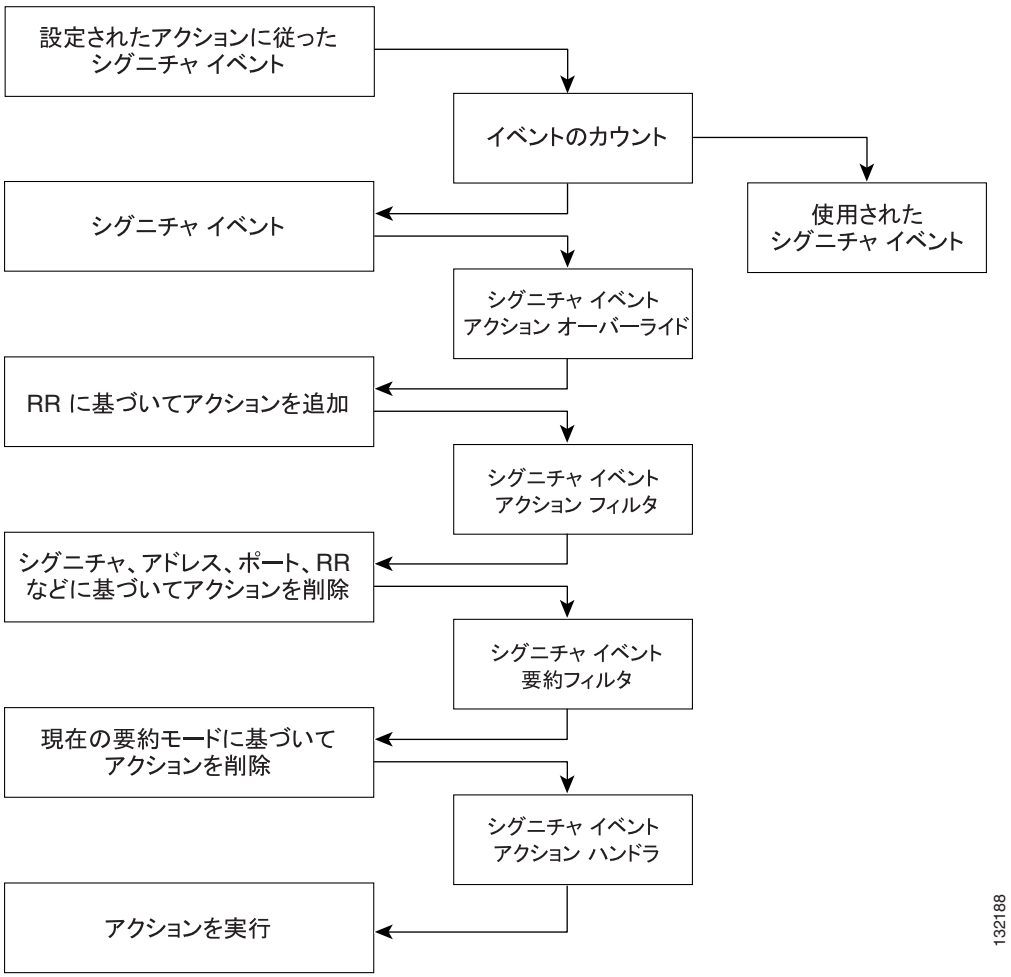
- ストップ ビットまたは継続ビット
- アクション フィルタ行をイネーブルにするビット

- 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 6-1 に、SEAP を通過するシグニチャ イベントの論理的なフローと、このイベントのアクションで実行される操作を示します。これは、アラーム チャネルで受信された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 6-1　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 6-1 は、イベント アクションについて説明しています。

表 6-1　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.6-23 の「拒否された攻撃者リストのモニタリングとクリア」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.6-21 の「汎用設定」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 6-1　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 10 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 10 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.6-21 の「汎用設定」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 10 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 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 11 章「SNMP の設定」を参照してください。

表 6-1　イベント アクション（続き）

イベント アクション名	説明
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 ルールを設定するためのタスク リスト

IPS のイベント アクション ルール用コンポーネントを設定する場合は、次の手順を実行します。

1. イベント アクション フィルタで使用するすべての変数を作成します。
2. Target Value Rating（TVR; ターゲットの価値評価）を作成します。

   RR を計算できるように、ネットワーク資産に TVR を割り当てます。
3. RR 値に基づいてアクションを追加するためのオーバーライドを作成します。

   各イベント アクション タイプに RR を割り当てます。
4. フィルタを作成します。

   シグニチャの ID、IP アドレス、および RR に基づいてアクションを削除するためのフィルタを割り当てます。
5. 汎用設定を行います。

   Summarizer、Meta Event Generator を使用するかどうかを指定します。または、拒否された攻撃者のパラメータを設定します。

イベント アクション変数

この項では、イベント アクション変数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 アクション変数について（P.6-7）
- イベント アクション変数の設定（P.6-8）

イベント アクション変数について

イベント アクション変数を作成して、その変数をイベント アクション フィルタ内で使用することができます。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、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。編集できる変数は一度に 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。

- 10.90.1.1
- 10.89.10.10-10.89.10.23
- 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。このような場合に、この技術グループの IP アドレス空間として変数を設定します。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。

イベント アクション変数の設定

イベント アクション変数を設定するには、サービス イベント アクション ルール サブモードで、**variables** *variable_name* **address** *ip_address* コマンドを使用します。IP アドレスには、1 つのアドレス、1 つの範囲、またはカンマで区切った複数の範囲を指定できます。

イベント アクション変数を設定するには、次の手順を実行します。

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

ステップ 2　イベント アクション ルール サブモードに入ります。

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

ステップ 3　変数を作成します。

```
sensor(config-rul)# variables variable1 address 10.89.130.108
```

address の有効な値は、A.B.C.D-A.B.C.D [,A.B.C.D-A.B.C.D] です。

ステップ 4　作成した変数を確認します。

```
sensor(config-rul)# show settings
   variables (min: 0, max: 256, current: 2)
   ----------------------------------------------
      variableName: variable1
      ---------------------------------------------
         address: 10.89.130.108 default: 0.0.0.0-255.255.255.255
      ---------------------------------------------
   ----------------------------------------------
```

ステップ 5　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 6　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。

ターゲットの価値評価

この項では、リスク評価（RR）、および RR を使用したターゲットの価値評価（TVR）の設定方法について説明します。この項では、次のトピックについて説明します。

- リスク評価の計算（P.6-9）
- ターゲットの価値評価の設定（P.6-9）

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; 攻撃の重大度評価）**：脆弱性の不正利用が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。
- **Signiture Fidelity Rating（SFR; シグニチャの忠実度評価）**：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; ターゲットの価値評価）**：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。

ターゲットの価値評価の設定

ネットワーク資産に TVR を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。

ネットワーク資産の TVR を設定するには、サービス イベント アクション ルール サブモードで、**target-value target-value-setting** [**zerovalue** | **low** | **medium** | **high** | **mission-critical**] **target-address** *ip_address* コマンドを使用します。デフォルトは medium です。

次のオプションが適用されます。

- **target-address** *ip_address*：IP アドレスの範囲のセット（複数も可）。
- **target-value-setting**：次のいずれかを選択します。
  - **zerovalue**：このターゲットに値はありません。
  - **low**：このターゲットの低い値。
  - **medium**：このターゲットの通常の値。
  - **high**：このターゲットの高い値。
  - **mission-critical**：このターゲットの最高の値。

ネットワーク資産の TVR を設定するには、次の手順を実行します。

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

ステップ 2　イベント アクション ルール サブモードに入ります。

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

ステップ 3　ネットワーク資産に TVR を割り当てます。

```
sensor(config-rul)# target-value target-value-setting mission-critical target-address
10.89.130.108
```

ステップ 4　TVR の設定内容を確認します。

```
sensor(config-rul)# show settings
----------------------------------------------
   target-value (min: 0, max: 5, current: 1)
   ----------------------------------------------
      target-value-setting: mission-critical
      target-address: 10.89.130.108 default: 0.0.0.0-255.255.255.255
   ----------------------------------------------
sensor(config-rul)#
```

ステップ 5　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 6　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。

イベント アクション オーバーライド

この項では、イベント アクション オーバーライドについて説明します。取り上げる事項は次のとおりです。

- イベント アクション オーバーライドについて（P.6-11）
- イベント アクション オーバーライドの設定（P.6-11）

イベント アクション オーバーライドについて

イベント アクション オーバーライドを追加すると、特定のイベントに関連付けられたアクションを、そのイベントの RR に基づいて変更することができます。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 以上のすべてのイベントで SNMP トラップを生成する場合は、Request SNMP Trap の RR 範囲を 85 ～ 100 に設定します。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 オーバーライドの設定

イベント アクション オーバーライドのパラメータを設定するには、サービス イベント アクション ルール サブモードで、**overrides** [**request-block-connection** | **request-block-host** | **deny-attacker-inline** | **deny-packet-inline** | **deny-attacker-service-pair-inline** | **deny-attacker-victim-pair-inline** | **deny-connection-inline** | **log-attacker-packets** | **log-victim-packets** | **log-pair-packets** | **reset-tcp-connection** | **produce-alert** | **produce-verbose-alert** | **request-rate-limit** | **request-snmp-trap**] コマンドを使用します。

すべてのイベント アクションの説明については、P.6-4 の「イベント アクション」を参照してください。

次のオプションが適用されます。

- **no**：エントリまたは選択設定を削除します。
- **override-item-status** [**enabled** | **disabled**]：このオーバーライド項目の使用をイネーブルまたはディセーブルにします。デフォルトは enabled です。
- **risk-rating-range**：このオーバーライド項目の RR 値の範囲。デフォルトは 1 ～ 100 です。
- **show**：システム設定または履歴情報（あるいはその両方）を表示します。

イベント アクション オーバーライドを追加するには、次の手順を実行します。

ステップ 1　管理者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 アクション ルール サブモードに入ります。

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

ステップ 3　オーバーライドでのパケットの処理方法を設定するには、次の手順を実行します。

a. 攻撃者の送信元 IP アドレスからのパケットを拒否する場合

```
sensor(config-rul)# overrides deny-attacker-inline
sensor(config-rul-ove)#
```

b. アラートの原因となっている単一のパケットを送信しないようにする場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides deny-packet-inline
sensor(config-rul-ove)#
```

c. 指定された TCP 接続のパケットを送信しないようにする場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides deny-connection-inline
sensor(config-rul-ove)#
```

d. TCP RST パケットを送信して接続を終了する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides reset-tcp-connection
sensor(config-rul-ove)#
```

ステップ 4　ブロックを要求するオーバーライドを設定するには、次の手順を実行します。

a. 接続のブロックを要求する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides request-block-connection
sensor(config-rul-ove)#
```

b. 攻撃者のホストのブロックを要求する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides request-block-host
sensor(config-rul-ove)#
```

ステップ 5　オーバーライドでパケットをログに記録するには、次の手順を実行します。

a. 攻撃者の IP アドレスからのパケットをログに記録する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides log-attacker-packets
sensor(config-rul-ove)#
```

b. 被害先の IP アドレスからのパケットをログに記録する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides log-victim-packets
sensor(config-rul-ove)#
```

c. 攻撃者と被害先の IP アドレスからのパケットをログに記録する場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides log-pair-packets
sensor(config-rul-ove)#
```

ステップ 6　イベント ストアにアラートを書き込むには、次の手順を実行します。

a.　イベント ストアにアラートを書き込む場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides produce-alert
sensor(config-rul-ove)#
```

b.　イベント ストアに詳細なアラートを書き込む場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides produce-verbose-alert
sensor(config-rul-ove)#
```

c.　SNMP トラップを要求するイベントをイベント ストアに書き込む場合

```
sensor(config-rul-ove)# exit
sensor(config-rul)# overrides request-snmp-trap
sensor(config-rul-ove)#
```

ステップ 7　このオーバーライド項目の RR を設定するには、次の操作を実行します。

```
sensor(config-rul-ove)# risk-rating-range 85-100
```

(注)　デフォルトの RR 範囲は 0 ～ 100 です。85 ～ 100 などの別の範囲に設定してください。

ステップ 8　このオーバーライド項目をイネーブルまたはディセーブルにするには、次のコマンドを実行します。

```
sensor(config-rul-ove)# override-item-status [enabled | disabled]
```

デフォルトは enabled です。

ステップ 9　設定を確認します。

```
sensor(config-rul-ove)# show settings
   action-to-add: deny-attacker-inline default: produce-alert
   ----------------------------------------------
      override-item-status: Enabled default: Enabled
      risk-rating-range: 85-100 default: 0-100
   ----------------------------------------------
```

ステップ 10　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul-ove)# exit
sensor(config-rul)#
Apply Changes:?[yes]:
```

ステップ 11　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。

イベント アクション フィルタ

この項では、イベント アクション フィル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。

- イベント アクション フィルタについて（P.6-14）
- イベント アクション フィルタの設定（P.6-14）

イベント アクション フィルタについて

イベント アクション フィルタは、順に並べられたリストで処理されます。フィルタはリスト内で上下に移動することができます。

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したり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 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と、イベントから特定のアクションを削除したり、イベント全体を廃棄したりすることにより、センサーがそれ以上処理しないようにすることができます。フィルタでは、アドレスをグループ化するために定義したイベント アクション変数を使用できます。イベント アクション変数の設定手順については、P.6-8 の「イベント アクション変数の設定」を参照してください。

（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。

イベント アクション フィルタを設定するには、サービス イベント アクション ルール サブモードで、**filters [edit | insert | move] name1 [begin | end | inactive | before | after]** コマンドを使用します。

次のオプションが適用されます。

- **actions-to-remove**：このフィルタ項目で削除するイベント アクション。
  - **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、このパケットおよび将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
  - **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
- **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（切り捨てられている可能性があります）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。
- **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。
- **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。
- **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。
- **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。
- **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。

- **attacker-address-range**：この項目に対応する攻撃者アドレスの範囲のセット（10.20.1.0-10.20.1.255,10.20.5.0-10.20.5.255 など）。
- **attacker-port-range**：この項目に対応する攻撃者ポートの範囲のセット（147-147,8000-10000 など）。
- **default**：値をシステム デフォルト設定に戻します。
- **deny-attacker-percentage**：攻撃者拒否機能で拒否するパケットの比率。有効な範囲は 1 ～ 100 です。デフォルトは 100 です。
- **filter-item-status** [**enabled** | **disabled**]：このフィルタ項目の使用をイネーブルまたはディセーブルにします。
- **no**：エントリまたは選択設定を削除します。
- **risk-rating-range**：このフィルタ項目の RR の範囲。
- **signature-id-range**：この項目に対応するシグニチャ ID の範囲のセット（1000-2000,3000-3000 など）。
- **stop-on-match**：このフィルタ項目に一致した場合に、フィルタの評価を継続するか中止するかの指定。
- **subsignature-id-range**：この項目に対応するサブシグニチャ ID の範囲のセット（0-2,5-5 など）。
- **user-comment**：このフィルタ項目に関するコメントを追加できます。
- **victim-address-range**：この項目に対応する被害先アドレスの範囲のセット（10.20.1.0-10.20.1.255,10.20.5.0-10.20.5.255 など）。
- **victim-port-range**：この項目に対応する被害先ポートの範囲のセット（147-147,8000-10000 など）。

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　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードに入ります。

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

ステップ 3　フィルタ名を作成します。

```
sensor(config-rul)# filters insert name1 begin
```

複数のイベント アクション フィルタに名前を付ける場合は、*name1*、*name2* の順に使用し、以下同様に続きます。フィルタの挿入場所の指定には、**begin | end | inactive | before | after** キーワードを使用します。

ステップ 4　フィルタの値を設定します。

a. シグニチャ ID の範囲を設定します。

```
sensor(config-rul-fil)# signature-id-range 1000-1005
```

デフォルトは 900 ～ 65535 です。

b. サブシグニチャ ID の範囲を設定します。

```
sensor(config-rul-fil)# subsignature-id-range 1-5
```

デフォルトは 0 ～ 255 です。

c. 攻撃者アドレスの範囲を設定します。

```
sensor(config-rul-fil)# attacker-address-range 10.89.10.10-10.89.10.23
```

デフォルトは 0.0.0.0 ～ 255.255.255.255 です。

d. 被害先アドレスの範囲を指定します。

```
sensor(config-rul-fil)# victim-address-range 192.56.10.1-192.56.10.255
```

デフォルトは 0.0.0.0 ～ 255.255.255.255 です。

e. 被害先ポートの範囲を指定します。

```
sensor(config-rul-fil)# victim-port-range 0-434
```

デフォルトは 0 ～ 65535 です。

f. リスク評価の範囲を指定します。

```
sensor(config-rul-fil)# risk-rating-range 85-100
```

デフォルトは 0 ～ 100 です。

g. 削除するアクションを設定します。

```
sensor(config-rul-fil)# actions-to-remove reset-tcp-connection
```

h. 拒否アクションのフィルタリングを行う場合は、拒否アクションの比率を設定します。

```
sensor(config-rul-fil)# deny-attacker-percentage 90
```

デフォルトは 100 です。

i. フィルタのステータスをディセーブルまたはイネーブルに設定します。

```
sensor(config-rul-fil)# filter-item-status [enabled | disabled]
```

デフォルトは enabled です。

j. stop-on-match パラメータを設定します。

```
sensor(config-rul-fil)# stop-on-match [true | false]
```

true を指定すると、この項目に一致した場合にセンサーは処理を中止します。**false** を指定すると、この項目に一致してもセンサーは処理を継続します。

k. フィルタを説明する任意のコメントを追加します。

```
sensor(config-rul-fil)# user-comments
```

ステップ 5　フィルタの設定を確認します。

```
sensor(config-rul-fil)# show settings
   NAME: name1
   ----------------------------------------------
      signature-id-range: 1000-10005 default: 900-65535
      subsignature-id-range: 1-5 default: 0-255
      attacker-address-range: 10.89.10.10-10.89.10.23 default: 0.0.0.0-255.255.255.255
      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 1-343 default: 0-65535
      risk-rating-range: 85-100 default: 0-100
      actions-to-remove: reset-tcp-connection default:
      deny-attacker-percentage: 90 default: 100
      filter-item-status: Enabled default: Enabled
      stop-on-match: True default: False
      user-comment: This is a new filter. default:
   ----------------------------------------------
ssenor(config-rul-fil)#
```

ステップ 6　既存のフィルタを編集するには、次のコマンドを実行します。

```
sensor(config-rul)# filters edit name1
```

ステップ 7　パラメータを編集します（ステップ 4a ～ 4k を参照）。

ステップ 8　フィルタ リストでフィルタを上下に移動するには、次のコマンドを実行します。

```
sensor(config-rul-fil)# exit
sensor(config-rul)# filters move name5 before name1
```

ステップ 9　フィルタが移動したことを確認します。

```
sensor(config-rul-fil)# exit
sensor(config-rul)# show settings
   ----------------------------------------------
   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)
   ----------------------------------------------
   ACTIVE list-contents
   ----------------------------------------------
      NAME: name5
      ----------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ----------------------------------------------
      ----------------------------------------------
      NAME: name1
      ----------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ----------------------------------------------
      ----------------------------------------------
      NAME: name2
      ----------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   INACTIVE list-contents
   ----------------------------------------------
----------------------------------------------
sensor(config-rul)#
```

ステップ 10　フィルタを非アクティブ リストに移動するには、次のコマンドを実行します。

```
sensor(config-rul)# filters move name1 inactive
```

ステップ 11 フィルタが非アクティブ リストに移動したことを確認します。

```
sensor(config-rul-fil)# exit
sensor(config-rul)# show settings
   ----------------------------------------------
   INACTIVE list-contents
   ----------------------------------------------
      ----------------------------------------------
      NAME: name1
      ----------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ----------------------------------------------
      ----------------------------------------------
sensor(config-rul)#
```

ステップ 12 イベント アクション ルール サブモードを終了します。

```
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 13 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。

汎用設定

この項では、汎用設定について説明します。取り上げる事項は次のとおりです。

- 汎用設定について（P.6-20）
- イベント アクションの要約について（P.6-20）
- イベント アクションの集約について（P.6-20）
- インラインの攻撃者拒否イベント アクションについて（P.6-21）
- 汎用設定（P.6-21）
- 拒否された攻撃者リストのモニタリングとクリア（P.6-23）

汎用設定について

イベント アクション ルールに適用する汎用設定を指定できます。汎用設定には、Summarizer や Meta Event Generator を使用するかどうかなどがあります。Summarizer は、イベントを 1 つのアラートにグループ化することによって、センサーが送出するアラートの数を減らします。Meta Event Generator は、コンポーネント イベントを処理します。これにより、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。

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。

イベント アクションの要約について

要約は、複数のイベントを 1 つのアラートにまとめる基本的な集約を実行することにより、センサーから送出されるアラートの量を減らします。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。

アラートを生成するその他のアクションのいずれかを選択し、そのアクションをフィルタリングで排除しない場合は、Produce Alert を選択していなくてもアラートが生成されます。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。これにより、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 アクションの集約について

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、アラートは、ヒットのしきい値を超えるまでは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発生します。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、シグニチャが最初にトリガーされるとアラートが発生します。その後は、サマリー間隔の期間ごとにそのシグニチャの追加のアラートが要約されます。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、サマリー間隔ごとに 1 つのアラートが発生します。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 1 つのアラートが発生します。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。

インラインの攻撃者拒否イベント アクションについて

インラインの攻撃者拒否イベント アクションの一定の特性を設定することができます。インラインで攻撃者拒否を実行する時間（秒単位）を設定したり、システム内で同時に拒否する攻撃者の数を制限したりすることができます。

汎用設定

イベント アクション ルールの汎用設定を行うには、サービス イベント アクション ルール サブモードで次の各コマンドを使用します。

- **global-block-timeout**：ホストまたは接続をブロックする時間（分単位）。

  有効な範囲は 0 ～ 10000000 です。デフォルトは 30 分です。
- **global-deny-timeout**：インラインで攻撃者を拒否する時間（秒単位）。

  有効な範囲は 1 ～ 518400 です。デフォルトは 3600 です。
- **global-filters-status** [**enabled | disabled]**：フィルタの使用をイネーブルまたはディセーブルにします。

  デフォルトは enabled です。
- **global-metaevent-status [enabled | disabled]**：Meta Event Generator の使用をイネーブルまたはディセーブルにします。

  デフォルトは enabled です。
- **global-overrides-status** [**enabled | disabled]**：オーバーライドの使用をイネーブルまたはディセーブルにします。

  デフォルトは enabled です。
- **global-summarization-status [enabled | disabled]**：Summarizer の使用をイネーブルまたはディセーブルにします。

  デフォルトは enabled です。
- **max-denied-attackers**：システム内で同時に拒否できる攻撃者数を制限します。

  有効な範囲は 1 ～ 100000000 です。デフォルトは 10000 です。

イベント アクションの汎用設定を行うには、次の手順を実行します。

ステップ 1　管理者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 アクション ルール サブモードに入ります。

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

ステップ 3　汎用サブモードに入ります。

```
sensor(config)# general
```

ステップ 4　Meta Event Generator をイネーブルまたはディセーブルにするには、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-metaevent-status [enabled | disabled]
```

デフォルトは enabled です。

ステップ 5　Summarizer をイネーブルまたはディセーブルにするには、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-summarization-status [enabled | disabled]
```

デフォルトは enabled です。

ステップ 6　インラインの拒否攻撃者イベント アクションを設定するには、次の操作を実行します。

a.　システム内で同時に拒否される攻撃者数を制限するには、次のコマンドを実行します。

```
sensor(config-rul-gen)# max-denied-attackers 100
```

デフォルトは 1000 です。

b.　システムで攻撃者を拒否する時間（秒単位）を設定するには、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-deny-timeout 1000
```

デフォルトは 3600 秒です。

ステップ 7　ホストまたは接続をブロックする時間（分単位）を設定するには、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-block-timeout 20
```

デフォルトは 30 分です。

ステップ 8　設定したすべての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、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-overrides-status [enabled | disabled]
```

デフォルトは enabled です。

ステップ 9　設定したすべてのフィルタをイネーブルまたはディセーブルにするには、次のコマンドを実行します。

```
sensor(config-rul-gen)# global-filters-status [enabled | disabled]
```

デフォルトは enabled です。

ステップ 10 汎用サブモードの設定を確認します。

```
sensor(config-rul-gen)# show settings
   general
   ----------------------------------------------
      global-overrides-status: Enabled default: Enabled
      global-filters-status: Enabled default: Enabled
      global-summarization-status: Enabled default: Enabled
      global-metaevent-status: Enabled default: Enabled
      global-deny-timeout: 1000 default: 3600
      global-block-timeout: 20 default: 30
      max-denied-attackers: 100 default: 10000
   ----------------------------------------------
sensor(config-rul-gen)#
```

ステップ 11 イベント アクション ルール サブモードを終了します。

```
sensor(config-rul-gen)# exit
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 12 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。

拒否された攻撃者リストのモニタリングとクリア

拒否された攻撃者のリストを表示するには、**show statistics denied-attackers** コマンドを使用します。拒否された攻撃者のリストを削除して仮想センサーの統計情報をクリアするには、サービス イベント アクション ルール サブモードで、**clear denied-attackers** コマンドを使用します。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。シグニチャを設定すると、インライン モードでパケット、接続、および攻撃者を拒否することができます。これは、センサーが単一パケット、接続、および特定の攻撃者を検出したときにそれらを拒否する、つまり送信しないことを意味します。

シグニチャが起動すると、攻撃者は拒否され、リストに入れられます。センサー管理の一環として、リストの削除やリスト内の統計情報のクリアを実行することもできます。

拒否された攻撃者リストの表示、リストの削除、および統計情報のクリアを実行するには、次の手順を実行します。

ステップ 1 管理者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 拒否された IP アドレスのリストを表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

今回 2 つの IP アドレスが拒否されたことが統計情報に示されています。

ステップ 3　拒否された攻撃者のリストを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of
attackers currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力してリストをクリアします。

ステップ 5　リストをクリアしたことを確認します。

```
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 = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

`Denied Attackers and hit count for each` カテゴリの情報がなくなっています。

ステップ 6　統計情報だけをクリアするには、次の手順を実行します。

```
sensor# show statistics virtual-sensor clear
```

ステップ 7　統計情報をクリアしたことを確認します。

```
JWK-4255# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

`Number of Active Denied Attackers` と `Number of exec Clear commands during uptime` のカテゴリ以外の統計情報がクリアされています。リストがクリアされたかどうかを認識していることが重要です。

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相互に影響し合い、どのような動作にな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、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 Produce Alert と Request SNMP Trap が追加されますが、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 ポリシーによってアラート アクションが強制されます。
- RR が 89 の場合は、イベント アクション オーバーライド コンポーネントによって Request SNMP Trap と Request Block Connection が追加されます。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り、Deny Attacker Inline と Request Block Connection を除くすべてのアクションが追加され、イベント アクション フィルタによって削除されるアクションはありません。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。

イベントのモニタリング

この項では、イベント ストアからイベントを表示およびクリア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。

- イベントの表示（P.6-26）
- イベント ストアからのイベントのクリア（P.6-29）

イベントの表示

イベント ストアからイベントを表示するには、**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**：Attack Response Controller（ARC）要求を表示します。

  （注） ARC は、以前は Network Access Controller（NAC）と呼ばれていました。この名前の変更は、IDM および CLI for IPS 5.1 で完全には反映されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、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の間、イベントの待機と表示が続きます。

イベント ストアから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 ストアからのイベントのクリア

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 ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者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。

シグニチャの定義

この章では、シグニチャを定義および作成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。

- シグニチャについて（P.7-2）
- シグニチャ変数（P.7-3）
- シグニチャの設定（P.7-5）
- カスタム シグニチャの作成（P.7-32）

シグニチャについて

攻撃またはその他のネットワーク リソースの不正使用は、ネットワークへの侵入として定義付けることができます。シグニチャベースのテクノロジーを使用するセンサーは、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

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

- シグニチャ変数について（P.7-3）
- シグニチャ変数の設定（P.7-3）

シグニチャ変数について

複数のシグニチャで同じ値を使用する場合、変数を使用します。変数の値を変更すると、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。編集できる変数は一度に 1 つだけです。

シグニチャ変数の設定

変数を作成するには、シグニチャ定義サブモードで **variables** コマンドを使用します。

次のオプションが適用されます。

- *variable-name*：この変数に割り当てる名前を定義します。
  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。
- **ip-addr-range**：IP アドレスをグループ化するためのシステム定義変数。
  有効な値は、A.B.C.D-A.B.C.D[,A.B.C.D-A.B.C.D] です。
- **web-ports**：HTTP トラフィックを探すポート用のシステム定義変数。
  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。

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 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
```

ステップ 3　IP アドレスのグループ用のシグニチャ変数を作成します。

```
sensor(config-sig)# variables IPADD ip-addr-range 10.1.1.1-10.1.1.24
```

ステップ 4　Web ポート用のシグニチャ変数を編集します。

```
sensor(config-sig)# variables WEBPORTS web-ports 80,3128,8000
```

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 5　変更を確認します。

```
sensor(config-sig)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variable-name: IPADD
      ----------------------------------------------
         ip-addr-range: 10.1.1.1-10.1.1.24
      ----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
      ----------------------------------------------
         web-ports: 80,3128,8000 default: 80-80,3128-3128,8000-8000,8010-8010,80
80-8080,8888-8888,24326-24326
      ----------------------------------------------
```

ステップ 6　シグニチャ定義サブモードを終了します。

```
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

シグニチャの設定

この項では、シグニチャのパラメー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。

- シグニチャの汎用パラメータの設定（P.7-5）
- アラート頻度の設定（P.7-6）
- アラート重大度の設定（P.7-8）
- イベント カウンタの設定（P.7-9）
- シグニチャ忠実度評価の設定（P.7-11）
- シグニチャのステータスの設定（P.7-12）
- シグニチャへのアクションの割り当て（P.7-13）
- AIC シグニチャの設定（P.7-15）
- IP フラグメント再構成（P.7-23）
- TCP ストリーム再構成の設定（P.7-26）
- IP ロギングの設定（P.7-30）

シグニチャの汎用パラメータの設定

特定のシグニチャの汎用パラメータの設定では、次のオプションが適用されます。

- **alert-frequency**：アラートをグループ化するためのサマリー オプションを設定します。

  手順については、P.7-6 の「アラート頻度の設定」を参照してください。
- **alert-severity**：アラートの重大度を設定します。

  手順については、P.7-8 の「アラート重大度の設定」を参照してください。
- **engine**：シグニチャ エンジンを指定します。エンジン サブモードでは、アクションを割り当てることができます。

  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。アクションを割り当てる手順については、P.7-13 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。
- **event-counter**：イベントのカウンタを設定します。

  手順については、P.7-9 の「イベント カウンタの設定」を参照してください。
- **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。

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、混合デルタによって特定のアラートの RR が低くなります。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 RR より）低く設定しておくと役立ちます。そうすることで、管理者は優先順位の高い RR 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可されなかったため、RR 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シグニチャ以外では、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。

- **sig-description**：シグニチャの説明。

- **sig-fidelity-rating**：シグニチャの忠実度の評価。
  手順については、P.7-11 の「シグニチャ忠実度評価の設定」を参照してください。
- **status**：シグニチャのステータスをイネーブルまたはリタイアに設定します。
  手順については、P.7-12 の「シグニチャのステータスの設定」を参照してください。

アラート頻度の設定

シグニチャのアラート頻度を設定するには、シグニチャ定義サブモードで **alert-frequency** コマンドを使用します。

次のオプションが適用されます。

- *sig-id*：このシグニチャに割り当てられた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。
- *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。
  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-frequency**：シグニチャの反応中にセンサーがアラートを生成する頻度。
  次のパラメータをシグニチャに指定します。
  - **summary-mode**：センサーでアラートをグループ化する方法。
    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：すべてのアラートを要約します。
  - **summary-interval**：各サマリー アラートを生成する間隔（秒単位）。
    値は 1 ～ 65535 です。
  - **summary-key**：シグニチャの要約に使用されるストレージ タイプ。
    Axxx：攻撃者のアドレス。
    Axxb：攻撃者のアドレスと被害先のポート。
    AxBx：攻撃者と被害先のアドレス。
    AaBb：攻撃者と被害先のアドレスとポート。
    xxBx：被害先のアドレス。
  - **specify-global-summary-threshold [yes | no]**：グローバル サマリーしきい値（オプション）を設定するかどうかを指定します。
  - **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。

シグニチャのアラート頻度パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　設定するシグニチャを指定します。

```
sensor(config-sig)# signatures 9000 0
```

ステップ 4　アラート頻度サブモードに入ります。

```
sensor(config-sig-sig)# alert-frequency
```

ステップ 5　シグニチャのアラート頻度を設定します。

a.　たとえば、サマリー モードを fire-once に設定します。

```
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3000
sensor(config-sig-sig-ale-fir-yes)# summary-interval 5000
```

b.　サマリー キーを設定します。

```
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# summary-key AxBx
```

c.　設定を確認します。

```
sensor(config-sig-sig-ale-fir)# show settings
   fire-once
   ----------------------------------------------
      summary-key: AxBx default: Axxx
      specify-global-summary-threshold
      ---------------------------------------------
         yes
         ---------------------------------------------
            global-summary-threshold: 3000 default: 120
            summary-interval: 5000 default: 15
         ---------------------------------------------
      ---------------------------------------------
   ----------------------------------------------
sensor(config-sig-sig-ale-fir)#
```

ステップ 6　アラート頻度サブモードを終了します。

```
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

アラート重大度の設定

シグニチャの重大度を設定するには、シグニチャ定義サブモードで **alert-severity** コマンドを使用します。

次のオプションが適用されます。

- *sig-id*：このシグニチャに割り当てられた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。
- *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。
  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**：アラートの重大度。
  - **high** ：危険なアラート。
  - **medium**：中レベルのアラート。
  - **low**：低レベルのアラート。
  - **informational**：情報アラート。
    これがデフォルトの方法です。

アラート重大度を設定するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　設定するシグニチャを選択します。

```
sensor(config-sig)# signatures 9000 0
```

ステップ 4　アラート重大度を割り当てます。

```
sensor(config-sig-sig)# alert-severity medium
```

ステップ 5　設定を確認します。

```
sensor(config-sig-sig)# show settings
   <protected entry>
   sig-id: 9000
   subsig-id: 0
   ----------------------------------------------
      alert-severity: medium default: informational
      sig-fidelity-rating: 75 <defaulted>
      promisc-delta: 0 <defaulted>
      sig-description
      ----------------------------------------------
         sig-name: Back Door Probe (TCP 12345) <defaulted>
         sig-string-info: SYN to TCP 12345 <defaulted>
         sig-comment: <defaulted>
         alert-traits: 0 <defaulted>
         release: 40 <defaulted>
      ----------------------------------------------
      engine
      ----------------------------------------------
         atomic-ip
         ----------------------------------------------
            event-action: produce-alert <defaulted>
            fragment-status: any <defaulted>
            specify-l4-protocol
            ----------------------------------------------
--MORE--
```

ステップ 6　シグニチャ サブモードを終了します。

```
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

イベント カウンタの設定

センサーでのイベントのカウント方法を設定するには、シグニチャ定義サブモードで **event-counter** コマンドを使用します。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 回反応した場合にだけ、センサーがアラートを送信するように指定できます。

次のオプションが適用されます。

- **event-count**：アラートを生成するまでのイベントの発生回数。有効な範囲は 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。
  - **Axxx**：攻撃者のアドレス。
  - **AxBx**：攻撃者と被害先のアドレス。
  - **Axxb**：攻撃者のアドレスと被害先のポート。
  - **xxBx**：被害先のアドレス。
  - **AaBb**：攻撃者と被害先のアドレスとポート。
- **specify-alert-interval [yes | no]**：アラートの間隔をイネーブルにします。
  - **alert-interval**：イベント カウントをリセットするまでの時間（秒単位）。デフォルトは 60 です。

イベント カウンタを設定するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　イベント カウンタを設定するシグニチャを選択します。

```
sensor(config-sig)# signatures 9000 0
```

ステップ 4　イベント カウンタ サブモードに入ります。

```
sensor(config-sig-sig)# event-counter
```

ステップ 5　アラートを生成するまでのイベントの発生回数を設定します。

```
sensor(config-sig-sig-eve)# event-count 2
```

ステップ 6　このシグニチャのイベントのカウントに使用するストレージ タイプを設定します。

```
sensor(config-sig-sig-eve)# event-count-key AxBx
```

ステップ 7　（オプション）アラート間隔をイネーブルにします。

```
sensor(config-sig-sig-eve)# specify-alert-interval yes
```

ステップ 8　（オプション）イベント カウントをリセットするまでの時間（秒単位）を指定します。

```
sensor(config-sig-sig-eve-yes)# alert-interval 30
```

ステップ 9　設定を確認します。

```
sensor(config-sig-sig-eve-yes)# exit
sensor(config-sig-sig-eve)# show settings
   event-counter
   ----------------------------------------------
      event-count: 2 default: 1
      event-count-key: AxBx default: Axxx
      specify-alert-interval
      ---------------------------------------------
         yes
         ---------------------------------------------
            alert-interval: 30 default: 60
         ---------------------------------------------
      ---------------------------------------------
   ----------------------------------------------
sensor(config-sig-sig-eve)#
```

ステップ 10 シグニチャ サブモードを終了します。

```
sensor(config-sig-sig-eve)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 11 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。

シグニチャ忠実度評価の設定

シグニチャのシグニチャ忠実度評価を設定するには、シグニチャ定義サブモードで **sig-fidelity-rating** コマンドを使用します。

次のオプションが適用されます。

- **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指定します。

  有効な値は 0 ～ 100 です。

シグニチャのシグニチャ忠実度評価を設定するには、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 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
```

ステップ 3 設定するシグニチャを選択します。

```
sensor(config-sig)# signatures 12000 0
```

ステップ 4 シグニチャの忠実度評価を設定します。

```
sensor(config-sig-sig)# sig-fidelity-rating 50
```

ステップ 5　設定を確認します。

```
sensor(config-sig-sig)# show settings
   <protected entry>
   sig-id: 12000
   subsig-id: 0
   ----------------------------------------------
      alert-severity: low <defaulted>
      sig-fidelity-rating: 50 default: 85
      promisc-delta: 15 <defaulted>
      sig-description
      ----------------------------------------------
         sig-name: Gator Spyware Beacon <defaulted>
         sig-string-info: /download/ User-Agent: Gator <defaulted>
         sig-comment: <defaulted>
         alert-traits: 0 <defaulted>
         release: 71 <defaulted>
      ----------------------------------------------
```

ステップ 6　シグニチャ サブモードを終了します。

```
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

シグニチャのステータスの設定

特定のシグニチャのステータスを指定するには、シグニチャ定義モードで **status** コマンドを使用します。

次のオプションが適用されます。

- **status**：シグニチャがイネーブル、ディセーブル、リタイアのどの状態であるかを指定します。
  - **enabled [true | false]**：シグニチャをイネーブルにします。
  - **retired [true | false]**：シグニチャをリタイアにします。

注意　シグニチャのアクティブ化とリタイアには 30 分以上かかる場合があります。

シグニチャのステータスを変更するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　設定するシグニチャを選択します。

```
sensor(config-sig)# signatures 12000 0
```

ステップ 4　シグニチャのステータスを変更します。

```
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
```

ステップ 5　設定を確認します。

```
sensor(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true default: false
      retired: false <defaulted>
   -----------------------------------------------
sensor(config-sig-sig-sta)#
```

ステップ 6　シグニチャ サブモードを終了します。

```
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

シグニチャへのアクションの割り当て

シグニチャが反応したときにセンサーが実行するアクションを設定するには、シグニチャ定義サブモードで **event-action** コマンドを使用します。

次のオプションが適用されます。

- **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、このパケットおよび将来のパケットを送信しません。
- **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
- **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
- **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（切り捨てられている可能性があります）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。
- **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。
- **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。
- **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 コマンドに送信します。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。
- **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。
- **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。

シグニチャのイベント アクションを設定するには、次の手順を実行します。

ステップ 1　管理者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　シグニチャ定義モードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

ステップ 3　設定するシグニチャを選択します。

```
sensor(config-sig)# signatures 1200 0
```

ステップ 4　Normalizer エンジンを入力します。

```
sensor(config-sig-sig)# engine normalizer
```

ステップ 5　イベント アクションを設定します。

```
sensor(config-sig-sig-nor)# event-action produce-alert|request-snmp-trap
```

（注）　シグニチャのイベント アクションを設定するたびに、前の設定が上書きされます。たとえば、シグニチャが反応したら必ずアラートを生成するには、その他の必要なイベント アクションとともにそのアクションを設定する必要があります。複数のイベント アクションを追加する場合は、| 記号を使用して、**product-alert|deny-packet-inline|request-snmp-trap** のようにします。

ステップ 6　設定を確認します。

```
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-snmp-trap default:
produce-alert|deny-packet-inline
```

ステップ 7　イベント アクション 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 8　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。

AIC シグニチャの設定

この項では、AIC シグニチャ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.7-15）
- アプリケーション ポリシーの設定（P.7-16）
- AIC 要求メソッド シグニチャ（P.7-18）
- AIC MIME 定義コンテンツ タイプ シグニチャ（P.7-19）
- AIC 転送符号化シグニチャ（P.7-22）
- AIC FTP コマンド シグニチャ（P.7-22）

概要

AIC は 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。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か、カスタム シグニチャでポリシーを作成することができます。

（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

  シグニチャの ID と説明については、P.7-18 の「AIC 要求メソッド シグニチャ」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

  シグニチャの ID と説明については、P.7-19 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 シグニチャの作成手順については、P.7-43 の「AIC MIME タイプ シグニチャ」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。

  シグニチャの ID と説明については、P.7-22 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。シグニチャの ID と説明については、P.7-22 の「AIC FTP コマンド シグニチャ」を参照してください。

アプリケーション ポリシーの設定

Web AIC 機能をイネーブルにするには、シグニチャ定義サブモードで **application-policy** コマンドを使用します。レイヤ 4 ～レイヤ 7 のパケット検査を実行するようにセンサーを設定して、Web および FTP サービスに関連した悪意のある攻撃を防ぐことができます。

次のオプションが適用されます。

- **ftp-enable [true | false]**：FTP サービスの保護をイネーブルにします。センサーで FTP トラフィックの検査を必須にするには、true に設定します。

  デフォルトは false です。
- **http-policy**：HTTP トラフィックの検査をイネーブルにします。
  - **aic-web-ports**：AIC トラフィックを探すポート用の変数。

    有効な範囲は、0 ～ 65535 です。a-b[,c-d] 形式で指定された、0 ～ 65535 の整数から成る範囲の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。

    デフォルトは、80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,24326-24326 です。
  - **http-enable [true | false]**：Web サービスに対応する保護をイネーブルにします。センサーで HTTP トラフィックが RFC に準拠しているかどうかの検査を必須にするには、true に設定します。

    デフォルトは false です。

－ **max-outstanding-http-requests-per-connection**：接続ごとに許可される HTTP 要求の最大数。有効な値は 1 ～ 16 です。デフォルトは 10 です。

アプリケーション ポリシーを設定するには、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 CLI にログインします。

ステップ 2　アプリケーション ポリシー サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# application-policy
```

ステップ 3　FTP トラフィックの検査をイネーブルにします。

```
sensor(config-sig-app)# ftp-enable true
```

ステップ 4　HTTP アプリケーション ポリシーを設定します。

a. HTTP アプリケーション ポリシー サブモードに入ります。

```
sensor(config-sig-app)# http-policy
```

b. HTTP アプリケーション ポリシーの実施をイネーブルにします。

```
sensor(config-sig-app-htt)# http-enable true
```

c. 各接続で、サーバからの応答を受信していない未完了の状態が許可される、未完了 HTTP 要求の数を指定します。

```
sensor(config-sig-app-htt)# max-outstanding-http-requests-per-connection 5
```

d. AIC ポートを編集します。

```
sensor(config-sig-app-htt)# aic-web-ports 80-80,3128-3128
```

ステップ 5　設定を確認します。

```
sensor(config-sig-app)# show settings
   application-policy
   ----------------------------------------------
      http-policy
      ---------------------------------------------
         http-enable: true default: false
         max-outstanding-http-requests-per-connection: 5 default: 10
         aic-web-ports: 80-80,3128-3128 default: 80-80,3128-3128,8000-8000,8010-
8010,8080-8080,8888-8888,24326-24326
      ---------------------------------------------
      ftp-enable: true default: false
   ----------------------------------------------
sensor(config-sig-app)#
```

ステップ 6　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-app)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

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 7-1 に、事前定義済みの定義要求メソッド シグニチャを示します。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.7-12 の「シグニチャのステータスの設定」を参照してください。

表 7-1　要求メソッド シグニチャ

シグニチャ ID	定義要求メソッド
12676	要求メソッドは認識されていない
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（定義コンテンツ タイプ）。
  - 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 7-2 に、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.7-12 の「シグニチャのステータスの設定」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.7-43 の「AIC MIME タイプ シグニチャ」を参照してください。

表 7-2　定義コンテンツ タイプ シグニチャ

シグニチャ ID	シグニチャの説明
12621	コンテンツ タイプ image/gif のメッセージ長が無効です。
12622 2	コンテンツ タイプ image/png の検証に失敗しました。
12623 0 12623 1 12623 2	コンテンツ タイプ image/tiff のヘッダー チェック。 コンテンツ タイプ image/tiff のメッセージ長が無効です。 コンテンツ タイプ image/tiff の検証に失敗しました。
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。 無効なメッセージ長のコンテンツ タイプ audio/midi 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 7-2　定義コンテンツ タイプ シグニチャ（続き）

シグニチャ ID	シグニチャの説明
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 7-2　定義コンテンツ タイプ シグニチャ（続き）

シグニチャ ID	シグニチャの説明
12655 0 12655 1 12655 2	コンテンツ タイプ video/x-mng のヘッダー チェック。 コンテンツ タイプ video/x-mng のメッセージ長が無効です。 コンテンツ タイプ video/x-mng の検証に失敗しました。
12656 0 12656 1 12656 2	コンテンツ タイプ application/x-msvideo のヘッダー チェック。 コンテンツ タイプ application/x-msvideo のメッセージ長が無効です。 コンテンツ タイプ application/x-msvideo の検証に失敗しました。
12658 0 12658 1	コンテンツ タイプ application/ms-word のヘッダー チェック。 コンテンツ タイプ application/ms-word のメッセージ長が無効です。
12659 0 12659 1	コンテンツ タイプ application/octet-stream のヘッダー チェック。 コンテンツ タイプ application/octet-stream のメッセージ長が無効です。
12660 0 12660 1 12660 2	コンテンツ タイプ application/postscript のヘッダー チェック。 コンテンツ タイプ application/postscript のメッセージ長が無効です。 コンテンツ タイプ application/postscript の検証に失敗しました。
12661 0 12661 1	コンテンツ タイプ application/vnd.ms-excel のヘッダー チェック。 コンテンツ タイプ application/vnd.ms-excel のメッセージ長が無効です。
12662 0 12662 1	コンテンツ タイプ application/vnd.ms-powerpoint のヘッダー チェック。 コンテンツ タイプ application/vnd.ms-powerpoint のメッセージ長が無効です。
12663 0 12663 1 12663 2	コンテンツ タイプ application/zip のヘッダー チェック。 コンテンツ タイプ application/zip のメッセージ長が無効です。 コンテンツ タイプ application/zip の検証に失敗しました。
12664 0 12664 1 12664 2	コンテンツ タイプ application/x-gzip のヘッダー チェック。 コンテンツ タイプ application/x-gzip のメッセージ長が無効です。 コンテンツ タイプ application/x-gzip の検証に失敗しました。
12665 0 12665 1	コンテンツ タイプ application/x-java-archive のヘッダー チェック。 コンテンツ タイプ application/x-java-archive のメッセージ長が無効です。
12666 0 12666 1	コンテンツ タイプ application/x-java-vm のヘッダー チェック。 コンテンツ タイプ application/x-java-vm のメッセージ長が無効です。
12667 0 12667 1 12667 2	コンテンツ タイプ application/pdf のヘッダー チェック。 コンテンツ タイプ application/pdf のメッセージ長が無効です。 コンテンツ タイプ application/pdf の検証に失敗しました。
12668 0 12668 1	コンテンツ タイプ unknown のヘッダー チェック。 コンテンツ タイプ unknown のメッセージ長が無効です。
12669 0 12669 1	コンテンツ タイプ image/x-bitmap のヘッダー チェック。 コンテンツ タイプ image/x-bitmap のメッセージ長が無効です。
12673 0	認識されるコンテンツ タイプ。

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 7-3 に、事前定義済みの転送符号化シグニチャを示します。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.7-12 の「シグニチャのステータスの設定」を参照してください。

表 7-3　転送符号化シグニチャ

シグニチャ ID	転送符号化メソッド
12686	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 7-4 に、事前定義済みの FTP コマンド シグニチャを示します。必要な事前定義 FTP コマンドを持つシグニチャをイネーブルにします。シグニチャをイネーブルにする手順は、P.7-12 の「シグニチャのステータスの設定」を参照してください。

表 7-4　FTP コマンド シグニチャ

シグニチャ ID	FTP コマンド
12900	認識されていない 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 7-4　FTP コマンド シグニチャ（続き）

シグニチャ ID	FTP コマンド
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

IP フラグメント再構成

この項では、IP フラグメント再構成について説明します。ここでは、IP フラグメント再構成シグニチャと設定可能なパラメータを示し、それらのパラメータの設定方法と IP フラグメント再構成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.7-23）
- IP フラグメント再構成シグニチャと設定可能なパラメータ（P.7-24）
- IP フラグメント再構成パラメータの設定（P.7-24）
- IP フラグメント再構成の方法の設定（P.7-25）

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することができます。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ため、または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シグニチャと設定可能なパラメータ

表 7-5 に、IP フラグメント再構成シグニチャと、このシグニチャに設定可能なパラメータを示します。IP フラグメント再構成シグニチャは、Normalizer エンジンの一部です。

表 7-5　IP フラグメント再構成シグニチャ

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パラメータの設定

特定のシグニチャの IP フラグメント再構成パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　IP フラグメント再構成シグニチャの ID とサブシグニチャ ID を指定します。

```
sensor(config-sig)# signatures 1200 0
```

ステップ 4　エンジンを指定します。

```
sensor(config-sig-sig)# engine normalizer
```

ステップ 5　編集デフォルト シグニチャ サブモードに入ります。

```
sensor(config-sig-sig-nor)# edit-default-sigs-only default-signatures-only
```

ステップ 6　任意の IP フラグメント再構成パラメータをイネーブルにし、必要に応じてデフォルト設定を変更します。たとえば、シグニチャ 1200 の最大フラグメント数を指定します。

```
sensor(config-sig-sig-nor-def)# specify-max-fragments yes
sensor(config-sig-sig-nor-def-yes)# max-fragments 20000
```

ステップ 7　設定を確認します。

```
sensor(config-sig-sig-nor-def-yes)# show settings
   yes
   ----------------------------------------------
      max-fragments: 20000 default: 10000
   ----------------------------------------------
sensor(config-sig-sig-nor-def-yes)#
```

ステップ 8　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-nor-def-yes)# exit
sensor(config-sig-sig-nor-def)# exit
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

IP フラグメント再構成の方法の設定

センサーがフラグメントの再構成に使用する方法を設定するには、シグニチャ定義サブモードで **fragment-reassembly** コマンドを使用します。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。

次のオプションが適用されます。

- **ip-reassemble-mode**：センサーがフラグメントの再構成に使用する方法を、オペレーティングシステムで指定します。
  - **nt**：Windows システム
  - **solaris**：Solaris システム
  - **linux**：GNU/Linux システム
  - **bsd**：BSD UNIX システム

    デフォルトは nt です。

IP フラグメント再構成を設定するには、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 CLI にログインします。

ステップ 2　フラグメント再構成サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# fragment-reassembly
```

ステップ 3　センサーで IP フラグメント再構成に使用するオペレーティング システムを設定します。

```
sensor(config-sig-fra)# ip-reassemble-mode linux
```

ステップ 4　設定を確認します。

```
sensor(config-sig-fra)# show settings
   fragment-reassembly
   -----------------------------------------------
      ip-reassemble-mode: linux default: nt
   -----------------------------------------------
sensor(config-sig-fra)#
```

ステップ 5　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-fra)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 6　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。

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。取り上げる事項は次のとおりです。

- 概要（P.7-26）
- TCP ストリーム シグニチャと設定可能なパラメータ（P.7-27）
- TCP ストリーム再構成シグニチャの設定（P.7-28）
- TCP ストリーム再構成のモードの設定（P.7-29）

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、ハンドシェー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 シグニチャと設定可能なパラメータ

表 7-6 に、TCP ストリーム再構成シグニチャと、TCP ストリーム再構成で設定可能なパラメータを示します。TCP ストリーム再構成シグニチャは、Normalizer エンジンの一部です。

表 7-6　TCP ストリーム再構成シグニチャ

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
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

表 7-6　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
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、Normalizer 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、Normalizer 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

特定のシグニチャに TCP ストリーム再構成を設定するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　TCP ストリーム再構成シグニチャの ID とサブシグニチャ ID を指定します。

```
sensor(config-sig)# signatures 1313 0
```

ステップ 4　エンジンを指定します。

```
sensor(config-sig-sig)# engine normalizer
```

ステップ 5　編集デフォルト シグニチャ サブモードに入ります。

```
sensor(config-sig-sig-nor)# edit-default-sigs-only default-signatures-only
```

ステップ 6　シグニチャ 1313 の最大 MSS パラメータをイネーブルにし、必要に応じてデフォルト設定を編集します。

```
sensor(config-sig-sig-nor-def)# specify-tcp-max-mss yes
sensor(config-sig-sig-nor-def-yes)# tcp-max-mss 1380
```

（注）　このパラメータをデフォルトの 1460 から 1380 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。

ステップ 7　設定を確認します。

```
sensor(config-sig-sig-nor-def-yes)# show settings
   yes
   -----------------------------------------------
      tcp-max-mss: 1380 default: 1460
   -----------------------------------------------
sensor(config-sig-sig-nor-def-yes)#
```

ステップ 8　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-nor-def-yes)# exit
sensor(config-sig-sig-nor-def)# exit
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

TCP ストリーム再構成のモードの設定

センサーが TCP セッションの再構成に使用するモードを設定するには、シグニチャ定義サブモードで **stream-reassembly** コマンドを使用します。

次のオプションが適用されます。

- **tcp-3-way-handshake-required [true | false]**：センサーが 3 ウェイ ハンドシェイクの完了したセッションだけを追跡するように指定します。

  デフォルトは true です。
- **tcp-reassembly-mode**：センサーが TCP セッションの再構成に使用するモードを指定します。
  - **strict**：シーケンスで次に予想されるものだけが許可されます。
  - **loose**：シーケンスに途切れがあっても許可されます。
  - **asym**：非同期トラフィックの再構成を許可します。

    デフォルトは strict です。

注意　非同期オプションを使用すると、TCP ウィンドウの回避チェックがディセーブルになります。

TCP ストリームの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 CLI にログインします。

ステップ 2　TCP ストリーム再構成サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# stream-reassembly
```

ステップ 3　センサーが 3 ウェイ ハンドシェイクの完了したセッションだけを追跡するように指定します。

```
sensor(config-sig-str)# tcp-3-way-handshake-required true
```

ステップ 4　センサーが TCP セッションの再構成に使用するモードを指定します。

```
sensor(config-sig-str)# tcp-reassembly-mode strict
```

ステップ 5　設定を確認します。

```
sensor(config-sig-str)# show settings
   stream-reassembly
   ----------------------------------------------
      tcp-3-way-handshake-required: true default: true
      tcp-reassembly-mode: strict default: strict
   ----------------------------------------------
sensor(config-sig-str)#
```

ステップ 6　TCP ストリーム再構成サブモードを終了します。

```
sensor(config-sig-str)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

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。

IP ロギングを設定するには、シグニチャ定義サブモードで **ip-log** コマンドを使用します。

次のオプションが適用されます。

- **ip-log-bytes**：ログに記録する最大バイト数を指定します。
  有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。
- **ip-log-packets**：ログに記録するパケット数を指定します。
  有効な値は 0 ～ 65535 です。デフォルトは 0 です。
- **ip-log-time**：センサーでログを記録する期間を指定します。
  有効な値は 30 ～ 300 秒です。デフォルトは 30 秒です。

（注）　センサーは、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。

IP ロギング パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者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 CLI にログインします。

ステップ 2　IP ログ サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# ip-log
```

ステップ 3　IP ロギング パラメータを指定します。

a. ログに記録する最大バイト数を指定します。

```
sensor(config-sig-ip)# ip-log-bytes 200000
```

b. ログに記録するパケット数を指定します。

```
sensor(config-sig-ip)# ip-log-packets 150
```

c. センサーでログを記録する期間を指定します。

```
sensor(config-sig-ip)# ip-log-time 60
```

ステップ 4　設定を確認します。

```
sensor(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 150 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 200000 default: 0
   -----------------------------------------------
sensor(config-sig-ip)#
```

ステップ 5　IP ログ サブモードを終了します。

```
sensor(config-sig-ip)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 6　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。

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。

- カスタム シグニチャの作成シーケンス（P.7-32）
- String TCP シグニチャの例（P.7-32）
- Service HTTP シグニチャの例（P.7-36）
- MEG シグニチャの例（P.7-39）

カスタム シグニチャの作成シーケンス

カスタム シグニチャを作成する場合は、次の手順に従います。

ステップ 1　シグニチャ エンジンを選択します。

ステップ 2　シグニチャの識別子を割り当てます。

- 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。

ステップ 6　変更を適用します。

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。

次の例は、カスタム String TCP シグニチャの作成方法を示しています。

（注）この手順は、String UDP シグニチャおよび String ICMP シグニチャにも当てはまります。

String TCP エンジンには、次のパラメータが適用されます。

- **default**：値をシステム デフォルト設定に戻します。
- **direction**：トラフィックの方向。
  - **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。
- **event-action**：アラートがトリガーされたときに実行するアクション。
  - **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、このパケットおよび将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
  - **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
  - **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（切り捨てられている可能性があります）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。
  - **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。
  - **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。
  - **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 コマンドに送信します。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。
  - **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。
  - **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。
- **no**：エントリまたは選択設定を削除します。
- **regex-string**：単一の TCP パケット内で検索する正規表現。

- **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。

  有効な範囲は、0 ～ 65535 です。a-b[,c-d] 形式で指定された、0 ～ 65535 の整数から成る範囲の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。
- **specify-exact-match-offset [yes | no]**：（オプション）完全一致オフセットをイネーブルにします。
- **specify-min-match-length [yes | no]**：（オプション）最小一致長をイネーブルにします。
- **strip-telnet-options**：検索の前にデータから Telnet オプション文字を削除します。
- **swap-attacker-victim [true | false]**：アラーム メッセージでアドレス（およびポート）ソースと宛先をスワップするかどうかを示します。デフォルトは、スワッピングなしを意味する false です。

String TCP エンジンに基づいてシグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。

```
sensor(config-sig)# signatures 60025 0
```

カスタム シグニチャの範囲は 60000 ～ 65000 です。

ステップ 4　シグニチャ説明サブモードに入ります。

```
sensor(config-sig-sig)# sig-description
```

ステップ 5　新しいシグニチャの名前を指定します。

```
sensor(config-sig-sig-sig)# sig-name This is my new name
```

また、**sig-comment** コマンドを使用してシグニチャの追加コメントを指定したり、**sig-string-info** コマンドを使用してシグニチャに関する追加情報を指定したりすることもできます。

ステップ 6　シグニチャ説明サブモードを終了します。

```
sensor(config-sig-sig-sig)# exit
```

ステップ 7　String TCP エンジンを指定します。

```
sensor(config-sig-sig)# engine string-tcp
```

ステップ 8　サービス ポートを指定します。

```
sensor(config-sig-sig-str)# service-ports 23
```

ステップ 9　方向を指定します。

```
sensor(config-sig-sig-str)# direction to-service
```

ステップ 10　TCP パケット内で検索する正規表現文字列を指定します。

```
sensor(config-sig-sig-str)# regex-string This-is-my-new-Sig-regex
```

ステップ 11　必要れあれば、**event-action** コマンドを使用して、セキュリティ ポリシーに従ってイベント アクションを変更することができます。デフォルトのイベント アクションは **produce-alert** です。

ステップ 12　このカスタム String TCP シグニチャでは、次のオプション パラメータを変更することができます。

- **specify-exact-match-offset**
- **specify-min-match-length**
- **strip-telnet-options**
- **swap-attacker-victim**

ステップ 13　設定を確認します。

```
sensor(config-sig-sig-str)# show settings
   string-tcp
   -----------------------------------------------
      event-action: produce-alert <defaulted>
      strip-telnet-options: false <defaulted>
      specify-min-match-length
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      regex-string: This-is-my-new-Sig-regex
      service-ports: 23
      direction: to-service default: to-service
      specify-exact-match-offset
      -----------------------------------------------
         no
         -----------------------------------------------
            specify-max-match-offset
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-min-match-offset
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      swap-attacker-victim: false <defaulted>
   -----------------------------------------------
sensor(config-sig-sig-str)#
```

ステップ 14 シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-str)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# 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。

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お勧めします。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。

次の例は、カスタム Service HTTP シグニチャの作成方法を示しています。

Service HTTP エンジンには、次のオプションが適用されます。

- **de-obfuscate [true | false]**：検索の前に反回避解読を適用します。
- **default**：値をシステム デフォルト設定に戻します。
- **event-action**：アラートがトリガーされたときに実行するアクション。
  - **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、このパケットおよび将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
  - **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
- **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（切り捨てられている可能性があります）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。
- **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。
- **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。
- **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 コマンドに送信します。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。
- **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。
- **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。

- **max-field-sizes**：最大フィールド サイズのグループ。
  - **specify-max-arg-field-length [yes | no]**：max-arg-field-length をイネーブルにします（オプション）。
  - **specify-max-header-field-length [yes | no]**：max-header-field-length をイネーブルにします（オプション）。
  - **specify-max-request-length [yes | no]**：max-request-length をイネーブルにします（オプション）。
  - **specify-max-uri-field-length [yes | no]**：max-uri-field-length をイネーブルにします（オプション）。
- **no**：エントリまたは選択設定を削除します。
- **regex**：正規表現のグループ。
  - **specify-arg-name-regex**：arg-name-regex をイネーブルにします（オプション）。
  - **specify-header-regex**：header-regex をイネーブルにします（オプション）。
  - **specify-request-regex**：request-regex をイネーブルにします（オプション）。
  - **specify-uri-regex**：uri-regex をイネーブルにします（オプション）。
- **service-ports**：ターゲット サービスが常駐することのできるポートまたはポート範囲のカンマ区切りリスト。
- **swap-attacker-victim [true | false]**：アラーム メッセージでアドレス（およびポート）ソースと宛先をスワップするかどうかを示します。デフォルトは、スワッピングなしを意味する false です。

Service HTTP エンジンに基づいてカスタム シグニチャを作成するには、次の手順を実行します。

ステップ 1　管理者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 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
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。

```
sensor(config-sig)# signatures 63000 0
```

カスタム シグニチャの範囲は 60000 ～ 65000 です。

ステップ 4　シグニチャ説明モードに入ります。

```
sensor(config-sig-sig)# sig-description
```

ステップ 5　シグニチャ名を指定します。

```
sensor(config-sig-sig-sig)# sig-name myWebSig
```

ステップ 6　アラートの特性を指定します。

```
sensor(config-sig-sig-sig)# alert-traits 2
```

有効な範囲は 0 ～ 65535 です。

ステップ 7　シグニチャ説明サブモードを終了します。

```
sensor(config-sig-sig-sig)# exit
```

ステップ 8　アラート頻度を割り当てます。

```
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-all
sensor(config-sig-sig-ale-fir)# summary-key Axxx
sensor(config-sig-sig-ale-fir)# specify-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# summary-threshold 200
```

ステップ 9　アラート頻度サブモードを終了します。

```
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
```

ステップ 10　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。

```
sensor(config-sig-sig)# engine service-http
sensor(config-sig-sig-ser)# de-obfuscate true
```

ステップ 11 正規表現パラメータを設定します。

```
sensor(config-sig-sig)# engine service-http
sensor(config-sig-sig-ser)# regex
sensor(config-sig-sig-ser-reg)# specify-uri-regex yes
sensor(config-sig-sig-ser-reg-yes)# uri-regex [Mm][Yy][Ff][Oo][Oo]
```

ステップ 12 正規表現サブモードを終了します。

```
sensor(config-sig-sig-ser-reg-yes)# exit
sensor(config-sig-sig-ser-reg-)# exit
```

ステップ 13 シグニチャ変数 WEBPORTS を使用するサービス ポートを設定します。

```
sensor(config-sig-sig-ser)# service-ports $WEBPORTS
```

ステップ 14 シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-ser)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# 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。

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.6-2 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。

(注) Meta 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。

Meta シグニチャ エンジンには、次のオプションが適用されます。

- **component-list**：Meta コンポーネントのリスト。
  - **edit**：リスト内の既存のエントリを編集します。
  - **insert** *name1*：リストに新しいエントリを挿入します。
  - **move**：リスト内のエントリを移動します。
  - **begin**：エントリをアクティブ リストの先頭に配置します。
  - **end**：エントリをアクティブ リストの終わりに配置します。
  - **inactive**：エントリを非アクティブ リストに配置します。
  - **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。
- **component-count**：このコンポーネントが満たされるまでにコンポーネントが反応する回数。
- **component-sig-id**：このコンポーネントを照合するシグニチャのシグニチャ ID。
- **component-subsig-id**：このコンポーネントを照合するシグニチャのサブシグニチャ ID。
- **component-list-in-order [true | false]**：コンポーネント リストの順に反応するかどうかの指定。
- **event-action**：アラートがトリガーされたときに実行するアクション。
  - **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、このパケットおよび将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
  - **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
  - **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（切り捨てられている可能性があります）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。
  - **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。
  - **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。
  - **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 コマンドに送信します。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。

- **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。
- **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。

- **meta-key**：Meta シグニチャのストレージ タイプ。
  - **AaBb**：攻撃者と被害先のアドレスとポート。
  - **AxBx**：攻撃者と被害先のアドレス。
  - **Axxx**：攻撃者のアドレス。
  - **xxBx**：被害先のアドレス。
- **meta-reset-interval**：Meta シグニチャをリセットする間隔（秒単位）。
  有効な範囲は 0 ～ 3600 秒です。デフォルトは 60 秒です。

（注） シグニチャ 64000 のサブシグニチャ 0 は、同じ送信元アドレスのシグニチャ 2000 のサブシグニチャ 0 およびシグニチャ 3000 のサブシグニチャ 0 からのアラートを認識すると反応します。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。

Meta 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。

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 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
```

ステップ 3　シグニチャのシグニチャ ID とサブシグニチャ ID を指定します。

```
sensor(config-sig)# signatures 64000 0
```

カスタム シグニチャの範囲は 60000 ～ 65000 です。

ステップ 4　シグニチャ エンジンを指定します。

```
sensor(config-sig-sig)# engine meta
```

ステップ 5　リストの先頭に MEG シグニチャ（名前は c1）を挿入します。

```
sensor(config-sig-sig-met)# component-list insert c1 begin
```

ステップ 6　このコンポーネントを照合するシグニチャのシグニチャ ID を指定します。

```
sensor(config-sig-sig-met-com)# component-sig-id 2000
```

ステップ 7　コンポーネント リスト サブモードを終了します。

```
sensor(config-sig-sig-met-com)# exit
```

ステップ 8　別の MEG シグニチャ（名前は c2）をリストの最後に挿入します。

```
sensor(config-sig-sig-met)# component-list insert c2 end
```

ステップ 9　このコンポーネントを照合するシグニチャのシグニチャ ID を指定します。

```
sensor(config-sig-sig-met-com)# component-sig-id 3000
```

ステップ 10　設定を確認します。

```
sensor(config-sig-sig-met-com)# exit
sensor(config-sig-sig-met)# show settings
   meta
   ----------------------------------------------
      event-action: produce-alert <defaulted>
      meta-reset-interval: 60 <defaulted>
      component-list (min: 1, max: 8, current: 2 - 2 active, 0 inactive)
      ----------------------------------------------
      ACTIVE list-contents
      ----------------------------------------------
         NAME: c1
         ----------------------------------------------
            component-sig-id: 2000
            component-subsig-id: 0 <defaulted>
            component-count: 1 <defaulted>
         ----------------------------------------------
         ----------------------------------------------
         NAME: c2
         ----------------------------------------------
            component-sig-id: 3000
            component-subsig-id: 0 <defaulted>
            component-count: 1 <defaulted>
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      meta-key
      ----------------------------------------------
         Axxx
         ----------------------------------------------
            unique-victims: 1 <defaulted>
         ----------------------------------------------
      ----------------------------------------------
      component-list-in-order: false <defaulted>
   ----------------------------------------------
sensor(config-sig-sig-met)#
```

ステップ 11　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-met)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 12　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。

AIC MIME タイプ シグニチャ

次の例は、AIC エンジンに基づいて MIME タイプ シグニチャを作成する方法を示しています。

次のオプションが適用されます。

- **event-action**：アラートがトリガーされたときに実行するアクション。
  - **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、このパケットおよび将来のパケットを送信しません。
  - **deny-attacker-service-pair-inline**：（インラインのみ）指定された期間、攻撃者アドレスと被害先のポートのペアで、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**：（インラインのみ）指定された期間、攻撃者 / 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。
  - **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**：攻撃者のアドレスを含むパケットの IP ロギングを開始します。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-pair-packets**：攻撃者と被害先のアドレスのペアを含むパケットの IP ロギングを開始します。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パケットの IP ロギングを開始します。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。
  - **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（切り捨てられている可能性があります）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。
  - **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。
  - **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。
  - **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 コマンドに送信します。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。
  - **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。
  - **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。
- **no**：エントリまたは選択設定を削除します。
- **signature-type**：目的のシグニチャ タイプ。
  - **content-types**：コンテンツ タイプ。
  - **define-web-traffic-policy**：Web トラフィック ポリシーの定義。
  - **max-outstanding-requests-overrun**：多数の未完了 HTTP 要求の検査。
  - **msg-body-pattern**：メッセージ本体のパターン。
  - **request-methods**：要求メソッドを処理するシグニチャ タイプ。

— **transfer-encodings**：転送符号化を処理するシグニチャ タイプ。

MIME タイプ ポリシーのシグニチャを定義するには、次の手順を実行します。

ステップ 1　管理者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 CLI にログインします。

ステップ 2　アプリケーション ポリシー実施サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 60001 0
sensor(config-sig-sig)# engine application-policy-enforcement-http
```

ステップ 3　イベント アクションを指定します。

```
sensor(config-sig-sig-app)# event-action produce-alert|log-pair-packets
```

ステップ 4　シグニチャ タイプを定義します。

```
sensor(config-sig-sig-app)# signature-type content-type define-content-type
```

ステップ 5　コンテンツ タイプを定義します。

```
sensor(config-sig-sig-app-def)# name MyContent
```

ステップ 6　設定を確認します。

```
sensor(config-sig-sig-app-def)# show settings
-> define-content-type
   ----------------------------------------------
      name: MyContent
*---> content-type-details
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
sensor(config-sig-sig-app-def)#
```

ステップ 7　シグニチャ サブモードを終了します。

```
sensor(config-sig-sig-app-def)# exit
sensor(config-sig-sig-app)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 8　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。

IP ロギングの設定

この章では、センサーで IP ロギングを設定する方法について説明します。この章は、次の項で構成されています。

- IP ロギングについて（P.8-2）
- 自動 IP ロギングの設定（P.8-3）
- 特定の IP アドレスの手動 IP ロギングの設定（P.8-5）
- アクティブな IP ログの停止（P.8-7）
- IP ログ ファイルのコピーと表示（P.8-9）

IP ロギングについて

IP アドレスで指定したホストに関連付けられている IP トラフィックをすべて取り込むように、センサーを手動で設定することができます。IP トラフィックのログを記録する期間、記録する IP パケット数、および記録するバイト数を指定できます。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。

また、特定のシグニチャが反応するたびに、IP パケットをログに記録するようセンサーを設定することもできます。センサーで IP トラフィックのログを記録する期間、および記録する IP パケット数とバイト数を指定できます。

注意　IP ロギングをオンにすると、システムのパフォーマンスが低下します。

（注）　IP ログ ファイルは、削除したり、管理したりすることはできません。**no iplog** コマンドでは、該当の IP ログにそれ以上パケットが記録されないようになるだけで、IP ログは削除されません。IP ログは、一杯になることのない循環バッファに格納されます。これは、新しい IP ログが古いログを上書きするためです。

IP ログをセンサーからコピーして、libpcap 形式のパケット ファイルを読み取る Ethereal や tcpdump などのツールで分析することができます。

（注）　各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

自動 IP ロギングの設定

センサーで自動 IP ロギング パラメータを設定するには、**ip-log-packets** *number*、**ip-log-time** *number*、**ip-log-bytes** *number* の各コマンドを使用します。

次のオプションが適用されます。

- **ip-log-packets**：ログに記録するパケット数を指定します。
  有効な値は 0 ～ 65535 です。デフォルトは 0 です。
- **ip-log-time**：センサーでログを記録する期間を指定します。
  有効な値は 0 ～ 65535 分です。デフォルトは 30 分です。
- **ip-log-bytes**：ログに記録する最大バイト数を指定します。
  有効な値は 0 ～ 2147483647 です。デフォルトは 0 です。

（注） 自動 IP ログは、これらのパラメータのいずれかに達するまでパケットの取り込みを継続します。

パラメータをリセットするには、**default** キーワードを使用します。IP ログ ファイルのコピーと表示については、P.8-9 の「IP ログ ファイルのコピーと表示」を参照してください。

自動 IP ロギングは、シグニチャ単位で設定するか、イベント アクション オーバーライドとして設定します。自動 IP ロギングは、次のアクションによってトリガーされます。

- log-attacker-packets
- log-victim-packets
- log-pair-packets

詳細については、第 6 章「イベント アクション ルールの設定」を参照してください。

自動 IP ロギング パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者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 CLI にログインします。

ステップ 2　シグニチャ IP ログ コンフィギュレーション サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# ip-log
```

ステップ 3　センサーでログに記録するパケット数を設定します。

```
sensor(config-sig-ip)# ip-log-packets 200
```

ステップ 4　センサーでパケットをログに記録する期間を設定します。

```
sensor(config-sig-ip)# ip-log-time 60
```

ステップ 5　ログに記録するバイト数を設定します。

```
sensor(config-sig-ip)# ip-log-bytes 5024
```

ステップ 6　設定を確認します。

```
sensor(config-sig-ip)# show settings
   ip-log
   -----------------------------------------------
      ip-log-packets: 200 default: 0
      ip-log-time: 60 default: 30
      ip-log-bytes: 5024 default: 0
   -----------------------------------------------
sensor(config-sig-ip)#
```

ステップ 7　IP ロギング モードを終了します。

```
sensor(config-sig-ip)# exit
sensor(config-sig)# exit
Apply Changes?:[yes]:
```

ステップ 8　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。

特定の IP アドレスの手動 IP ロギングの設定

特定の IP アドレスの仮想センサーで IP パケットを手動でログに記録するには、**iplog** *name ip-address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*] コマンドを使用します。

次のオプションが適用されます。

- *name*：ロギングを開始および停止する仮想センサー。

（注） IPS 5.0 バージョン 0 では仮想センサーは 1 つだけです。

- *ip-address*：指定された送信元 IP アドレスまたは宛先 IP アドレス（あるいはその両方）を含むパケットをログに記録します。
- *minutes*：ロギングをアクティブにする期間。
  有効な範囲は 1 ～ 60 分です。デフォルトは 10 分です。
- *numPackets*：ログに記録する最大パケット数。
  有効な範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。
- *numBytes*：ログに記録する最大バイト数。
  有効な範囲は 0 ～ 4294967295 です。値 0 はバイト数に制限がないことを示します。

（注） *minutes*、*numPackets*、および *numBytes* の各パラメータはオプションです。3 つすべてを指定する必要はありません。ただし、2 つ以上のパラメータを指定した場合、センサーは最初のしきい値に達するまでしかロギングを継続しません。たとえば、期間を 5 分、パケット数を 1000 と指定した場合、センサーは 2 分しか経過していなくても、1000 番目のパケットを取り込んだ後でロギングを停止します。

特定の IP アドレスの IP パケットのロギングを停止する場合は、P.8-7 の「アクティブな IP ログの停止」を参照してください。IP パケットをシグニチャに関連付けられたイベントとしてログに記録する場合は、P.8-3 の「自動 IP ロギングの設定」を参照してください。IP ログ ファイルのコピーと表示については、P.8-9 の「IP ログ ファイルのコピーと表示」を参照してください。

特定の IP アドレスの仮想センサーでパケットを手動でログに記録するには、次の 3 つ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 CLI にログインします。

ステップ 2　特定の IP アドレスの IP ロギングを開始します。

```
sensor# iplog vs0 10.16.0.0 duration 5
Logging started for virtual sensor vs0, IP address 10.16.0.0, Log ID 1
Warning: IP Logging will affect system performance.
sensor#
```

この例では、センサーが IP アドレス 10.16.0.0 で送受信されるすべての IP パケットを 5 分間ログに記録しています。

（注） 後で参照するときのために、ログ ID をメモしておいてください。

ステップ 3　**iplog-status** コマンドで、IP ログのステータスを監視します。

```
sensor# iplog-status
Log ID:              1
IP Address 1:        10.16.0.0
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
sensor#
```

（注）　各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

アクティブな IP ログの停止

`started` 状態のログのロギングを停止したり、`added` 状態のログを削除したりするには、**no iplog** [**log-id** *log-id* | **name** *name*] コマンドを使用します。

（注） added の状態の IP ログに対して **no iplog** コマンドを使用すると、IP ログが停止します。added の状態は、その IP ログが空のままである（パケットがない）ことを意味します。パケットが存在しない状態での停止は、空の IP ログの停止ということです。空のログは、停止すると削除されます。

（注） **no iplog** コマンドでは、IP ログは削除されません。このコマンドは、センサーに対してその IP ログでの追加パケットの取り込みを停止するようにシグナルを送信するだけです。

次のオプションが適用されます。

- *log-id*：停止するロギング セッションのログ ID。ログ ID を検索するには、**iplog-status** コマンドを使用します。
- *name*：ロギングを開始または停止する仮想センサー。

（注） IPS 5.0 バージョン 0 では仮想センサーは 1 つだけです。

1 つまたはすべての IP ロギング セッションを停止するには、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 CLI にログインします。

ステップ 2　特定の IP ロギング セッションを停止するには、次の手順を実行します。

a. **iplog-status** コマンドを使用して、停止するセッションのログ ID を検索します。

```
sensor# iplog-status
Log ID:              1
IP Address 1:        10.16.0.0
Virtual Sensor:      vs0
Status:              added
Event ID:            0
Bytes Captured:      0
Packets Captured:    0
sensor#
```

（注） 各アラートは、そのアラートのために作成された IP ログを参照します。複数のアラートにより同一の IP アドレスに対して IP ログが作成される場合は、すべてのアラートについて IP ログが 1 つだけ作成されます。各アラートは、同一の IP ログを参照します。しかし、IP ログ ステータスの出力は、IP ログをトリガーした最初のアラートのイベント ID だけを表示します。

b. IP ログ セッションを停止します。

```
sensor# no iplog log-id 137857512
```

ステップ 3　仮想センサー上のすべての IP ロギング セッションを停止するには、次のコマンドを実行します。

```
sensor# no iplog name vs0
```

ステップ 4　IP ロギングが停止したことを確認します。

```
sensor# iplog-status
Log ID:             1
IP Address 1:       10.16.0.0
Virtual Sensor:     vs0
Status:             completed
Event ID:           0
Bytes Captured:     0
Packets Captured:   0
sensor#
```

ログが停止すると、ステータスに completed と表示されます。

IP ログ ファイルのコピーと表示

IP ログ ファイルを FTP サーバまたは SCP サーバにコピーして、Ethereal や tcpdump などのスニフィング ツールで表示できるようにするには、**copy iplog** *log-id destination-url* コマンドを使用します。

次のオプションが適用されます。

- *log-id*：ロギング セッションのログ ID。ログ ID は、**iplog-status** コマンドを使用して取得できます。
- *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。

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 サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

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

  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。

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

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

FTP または SCP プロトコルを使用する場合は、パスワードの入力を求められます。

IP ログ ファイルを FTP サーバまたは SCP サーバにコピーするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コピーするログ ファイルのログ ID のステータスが completed と表示されるまで、**iplog-status** コマンドを使用して IP ログのステータスを監視します。

```
sensor# iplog-status
Log ID:              2425
IP Address:          10.1.1.2
Virtual Sensor:      vs0
Status:              started
Start Time:          2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured:    1039438

Log ID:              2342
IP Address:          10.2.3.1
Virtual Sensor:      vs0
Status:              completed
Event ID:            209348
Start Time:          2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:            2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

ステップ 3　IP ログを FTP サーバまたは SCP サーバにコピーします。

```
sensor# copy iplog 2342 ftp://root@10.16.0.0/user/iplog1
Password: ******** Connected to 10.16.0.0 (10.16.0.0). 220 linux.machine.com FTP
server (Version wu-2.6.0(1) Mon Feb 28 10:30 :36 EST 2000) ready. ftp> user (username)
root 331 Password required for root. Password:230 User root logged in. ftp> 200 Type
set to I. ftp> put iplog.8518.tmp iplog1 local: iplog.8518.tmp remote: iplog1 227
Entering Passive Mode (2,4,6,8,179,125) 150 Opening BINARY mode data connection for
iplog1. 226 Transfer complete. 30650 bytes sent in 0.00246 secs (1.2e+04 Kbytes/sec)
ftp>
```

ステップ 4　Ethereal や tcpdump などのスニファ プログラムを使用して IP ログを開きます。

Ethereal の詳細については、http://www.ethereal.com を参照してください。tcpdump の詳細については、http://www.tcpdump.org/ を参照してください。

インターフェイスのライブ トラフィックの表示と取り込み

この章では、パケット ファイルの表示、取り込み、コピー、および消去の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。

- パケットの表示と取り込みについて（P.9-2）
- インターフェイスのライブ トラフィックの表示（P.9-3）
- インターフェイスのライブ トラフィックの取り込み（P.9-6）
- パケット ファイルのコピー（P.9-8）
- パケット ファイルの消去（P.9-9）

パケットの表示と取り込みについて

インターフェイスからライブ トラフィックの表示や取り込みを行い、ライブ トラフィックや以前に取り込んだファイルを直接画面に表示することができます。保存できるのは 1 つのローカル ファイルだけであるため、後続の取り込み要求によって既存のファイルは上書きされます。保存ファイルのサイズは、プラットフォームによって異なります。要求された数のパケットが取り込まれる前に最大ファイル サイズに達すると、メッセージが表示される場合があります。

（注） インターフェイスからライブ　トラフィックを取り込んでも、センサーの機能が中断されることはありません。

注意 インターフェイスのコンフィギュレーションを変更すると、そのインターフェイスで実行中のすべての **packet** コマンドが異常終了します。

注意 **packet display** コマンドまたは **packet capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックの表示

インターフェイスのライブ トラフィックを直接画面に表示するには、**packet display** *interface-name* [**snaplen** *length*] [**count** *count*] [**verbose**] [**expression** *expression*] コマンドを使用します。

（注） ライブ表示を終了するには、**Ctrl+C** キーを押します。

次のオプションが適用されます。

- *interface-name*：論理インターフェイス名。
  システム内に存在するインターフェイス名だけを使用できます。
- **snaplen**：各パケットに取り込まれる最大バイト数（オプション）。
  有効な範囲は、68 ～ 1600 です。デフォルトは 0 です。値 0 は、パケット全体を取り込むために必要な長さを使用することを意味します。
- **count**：取り込みパケットの最大数（オプション）。
  有効な範囲は 1 ～ 10000 です。

  （注） このオプションを指定しない場合は、最大ファイル サイズまで取り込まれると、取り込みが終了します。

- **verbose**：1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します（オプション）。
- **expression**：パケット表示フィルタの式。
  この式は直接 tcpdump に渡されます。これは、tcpdump 式の構文と合っている必要があります。

  （注） この式の構文の説明は、tcpdump の man ページにあります。

- **file-info**：保存されたパケット ファイルに関する情報を表示します。
  File-info は、次の情報を表示します。
  Captured by: *user:id*, Cmd: *cliCmd*
  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress
  各変数の内容は次のとおりです。
  user = 取り込みを開始するユーザの名前
  id = ユーザの CLI ID
  cliCmd = 取り込みを実行するために入力されたコマンド

注意 **packet display** コマンドを実行すると、パフォーマンスが大幅に低下します。

インターフェイスのライブ トラフィックを画面に表示するようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者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センサーにログインします。

ステップ 2　目的のインターフェイス、たとえば GigabitEthernet0/1 のライブ トラフィックを表示します。

```
sensor# packet display GigabitEthernet0/1
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:43:05.691883 IP (tos 0x10, ttl  64, id 55460, offset 0, flags [DF], length: 100)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 4233955485:4233955533(48) ack
1495691730 win 8576 <nop,nop,timestamp 44085169 226014949>
03:43:05.691975 IP (tos 0x10, ttl  64, id 55461, offset 0, flags [DF], length: 164)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 48:160(112) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.691998 IP (tos 0x10, ttl  64, id 53735, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 48 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693165 IP (tos 0x10, ttl  64, id 53736, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693351 IP (tos 0x10, ttl  64, id 55462, offset 0, flags [DF], length: 316)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 160:424(264) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693493 IP (tos 0x10, ttl  64, id 55463, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 424:664(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693612 IP (tos 0x10, ttl  64, id 55464, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 664:904(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.693628 IP (tos 0x10, ttl  64, id 53737, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 424 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693654 IP (tos 0x10, ttl  64, id 53738, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 664 win 11704
<nop,nop,timestamp 226014949 44085169>
03:43:05.693926 IP (tos 0x10, ttl  64, id 55465, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 904:1144(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694043 IP (tos 0x10, ttl  64, id 55466, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1144:1384(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694163 IP (tos 0x10, ttl  64, id 55467, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1384:1624(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014949>
03:43:05.694209 IP (tos 0x10, ttl  64, id 53739, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 1384 win 11704
<nop,nop,timestamp 226014950 44085169>
03:43:05.694283 IP (tos 0x10, ttl  64, id 55468, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1624:1864(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694402 IP (tos 0x10, ttl  64, id 55469, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 1864:2104(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694521 IP (tos 0x10, ttl  64, id 55470, offset 0, flags [DF], length: 292)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2104:2344(240) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
03:43:05.694690 IP (tos 0x10, ttl  64, id 53740, offset 0, flags [DF], length: 52)
10.89.147.50.41805 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 2344 win 11704
<nop,nop,timestamp 226014950 44085169>
03:43:05.694808 IP (tos 0x10, ttl  64, id 55471, offset 0, flags [DF], length: 300)
10.89.147.31.22 > 10.89.147.50.41805: P [tcp sum ok] 2344:2592(248) ack 1 win 8576
<nop,nop,timestamp 44085169 226014950>
```

ステップ 3　**expression** オプションを使用すると、表示する内容を制限できます。たとえば、TCP パケットだけを表示することができます。

（注） tcpdump の man ページで説明されているように、プロトコル識別子である tcp、udp、および icmp はキーワードでもあるため、2 つのバックスラッシュ（\\）を使用してエスケープする必要があります。

```
sensor# packet display GigabitEthernet0/1 verbose expression ip proto \\tcp
Warning: This command will cause significant performance degradation
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
03:42:02.509738 IP (tos 0x10, ttl  64, id 27743, offset 0, flags [DF], length: 88)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 3449098782:3449098830(48) ack
3009767154 win 8704
03:42:02.509834 IP (tos 0x10, ttl  64, id 27744, offset 0, flags [DF], length: 152)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 48:160(112) ack 1 win 8704
03:42:02.510248 IP (tos 0x0, ttl 252, id 55922, offset 0, flags [none], length: 40)
64.101.182.54.47039 > 10.89.147.31.22: . [tcp sum ok] 1:1(0) ack 160 win 8760
03:42:02.511262 IP (tos 0x10, ttl  64, id 27745, offset 0, flags [DF], length: 264)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 160:384(224) ack 1 win 8704
03:42:02.511408 IP (tos 0x10, ttl  64, id 27746, offset 0, flags [DF], length: 248)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 384:592(208) ack 1 win 8704
03:42:02.511545 IP (tos 0x10, ttl  64, id 27747, offset 0, flags [DF], length: 240)
10.89.147.31.22 > 64.101.182.54.47039: P [tcp sum ok] 592:792(200) ack 1 win 8704
```

ステップ 4　パケット ファイルに関する情報を表示するには、次のコマンドを実行します。

```
sensor# packet display file-info
Captured by: cisco:25579, Cmd: packet capture GigabitEthernet0/1
Start: 2003/02/03 02:56:48 UTC, End: 2003/02/03 02:56:51 UTC
sensor#
```

インターフェイスのライブ トラフィックの取り込み

インターフェイスのライブ トラフィックを取り込むには、**packet capture** *interface-name* [**snaplen** *length*] [**count** *count*] [**expression** *expression*] コマンドを使用します。

同時に **packet capture** コマンドを使用できるユーザは 1 人だけです。2 番目のユーザが要求を出すと、現在取り込みを実行しているユーザについての情報を含むエラー メッセージが表示されます。

注意　**packet capture** コマンドを実行すると、パフォーマンスが大幅に低下します。

packet capture コマンドを実行すると、ローカル ファイルに libpcap の出力が取り込まれます。

ローカル ファイルを表示するには、**packet display packet-file** [**verbose**] [**expression** *expression*] コマンドを使用します。

ローカル ファイルが存在する場合、そのファイルに関する情報を表示するには、**packet display file-info** を使用します。

次のオプションが適用されます。

- *interface-name*：論理インターフェイス名。
  システム内に存在するインターフェイス名だけを使用できます。
- **snaplen**：各パケットに取り込まれる最大バイト数（オプション）。
  有効な範囲は 68 ～ 1600 です。デフォルトは 0 です。
- **count**：取り込みパケットの最大数（オプション）。
  有効な範囲は 1 ～ 10000 です。

  （注）　このオプションを指定しない場合は、最大ファイル サイズまで取り込まれると、取り込みが終了します。

- **expression**：パケット取り込みフィルタの式。
  この式は直接 tcpdump に渡されます。これは、tcpdump 式の構文と合っている必要があります。

  （注）　この式の構文の説明は、Ethereal の man ページにあります。

- **file-info**：保存されたパケット ファイルに関する情報を表示します。
  File-info は、次の情報を表示します。
  Captured by: *user:id*, Cmd: *cliCmd*
  Start: yyyy/mm/dd hh:mm:ss zone, End: yyyy/mm/dd hh:mm:ss zone or in-progress
  各変数の内容は次のとおりです。
  user = 取り込みを開始するユーザの名前
  id = ユーザの CLI ID
  cliCmd = 取り込みを実行するために入力されたコマンド
- **verbose**：1 行のサマリーではなく、各パケットのプロトコル ツリーを表示します。このパラメータはオプションです。

インターフェイスのライブ トラフィックを取り込むようにセンサーを設定するには、次の手順を実行します。

ステップ 1　管理者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センサーにログインします。

ステップ 2　目的のインターフェイス、たとえば GigabitEthernet0/1 のライブ トラフィックを取り込みます。

```
sensor# packet capture GigabitEthernet0/1
Warning: This command will cause significant performance degradation
tcpdump: WARNING: ge0_1: no IPv4 address assigned
tcpdump: listening on ge0_1, link-type EN10MB (Ethernet), capture size 65535 bytes
125 packets captured
126 packets received by filter
0 packets dropped by kernel
```

ステップ 3　取り込んだパケット ファイルを表示するには、次のコマンドを実行します。

```
sensor# packet display packet-file
reading from file /usr/cids/idsRoot/var/packet-file, link-type EN10MB (Ethernet)
03:03:13.216768 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:13.232881 IP 64.101.182.244.1978 > 10.89.130.108.23: . ack 3266153791 win
64328
03:03:13.232895 IP 10.89.130.108.23 > 64.101.182.244.1978: P 1:157(156) ack 0 wi
n 5840
03:03:13.433136 IP 64.101.182.244.1978 > 10.89.130.108.23: . ack 157 win 65535
03:03:13.518335 IP 10.89.130.134.42342 > 255.255.255.255.42342: UDP, length: 76
03:03:15.218814 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:15.546866 IP 64.101.182.244.1978 > 10.89.130.108.23: P 0:2(2) ack 157 win
65535
03:03:15.546923 IP 10.89.130.108.23 > 64.101.182.244.1978: P 157:159(2) ack 2 wi
n 5840
03:03:15.736377 IP 64.101.182.244.1978 > 10.89.130.108.23: . ack 159 win 65533
03:03:17.219612 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.218535 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:19.843658 IP 64.101.182.143.3262 > 10.89.130.23.445: P 3749577803:37495778
56(53) ack 3040953472 win 64407
03:03:20.174835 IP 161.44.55.250.1720 > 10.89.130.60.445: S 3147454533:314745453
3(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:21.219958 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:21.508907 IP 161.44.55.250.1809 > 10.89.130.61.445: S 3152179859:315217985
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:23.221004 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:23.688099 IP 161.44.55.250.1975 > 10.89.130.63.445: S 3160484670:316048467
0(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:25.219054 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:25.846552 IP 172.20.12.10.2984 > 10.89.130.127.445: S 1345848756:134584875
6(0) win 64240 <mss 1460,nop,nop,sackOK>
03:03:26.195342 IP 161.44.55.250.2178 > 10.89.130.65.445: S 3170518052:317051805
2(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.222725 802.1d config TOP_CHANGE 8000.00:04:9a:66:35:01.8025 root 8000.0
0:04:6d:f9:e8:82 pathcost 8 age 2 max 20 hello 2 fdelay 15
03:03:27.299178 IP 161.44.55.250.2269 > 10.89.130.66.445: S 3174717959:317471795
9(0) win 65520 <mss 1260,nop,nop,sackOK>
03:03:27.308798 arp who-has 161.44.55.250 tell 10.89.130.66
03:03:28.383028 IP 161.44.55.250.2349 > 10.89.130.67.445: S 3178636061:317863606
1(0) win 65520 <mss 1260,nop,nop,sackOK>
--MORE--
```

ステップ 4　パケット ファイルに関する任意の情報を表示するには、次のコマンドを実行します。

```
sensor# packet display file-info
Captured by: cisco:8874, Cmd: packet capture GigabitEthernet0/1
Start: 2003/01/07 00:12:50 UTC, End: 2003/01/07 00:15:30 UTC
sensor#
```

パケット ファイルのコピー

パケット ファイルを保存したり、Ethereal や tcpdump などの他のツールでさらに分析したりするために、ファイルを FTP サーバまたは SCP サーバにコピーするには、**copy packet-file** *destination-url* コマンドを使用します。

次のオプションが適用されます。

- **packet-file**：**packet capture** コマンドを使用して取り込み、ローカルに保存した libpcap ファイル。
- *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。

（注）　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。

- ftp:：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。
  ftp:[//[username@] location]/relativeDirectory]/filename
  ftp:[//[username@]location]//absoluteDirectory]/filename
- scp:：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、次のとおりです。
  scp:[//[username@] location]/relativeDirectory]/filename
  scp:[//[username@] location]//absoluteDirectory]/filename

（注）　FTP または SCP プロトコルを使用する場合は、パスワードの入力を求められます。

パケット ファイルを FTP サーバまたは SCP サーバにコピーするには、次の手順を実行します。

ステップ 1　管理者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　パケット ファイルを FTP サーバまたは SCP サーバにコピーします。

```
sensor# copy packet-file scp://jbrown@64.101.182.20/work/
Password: *********
packet-file               100% 1670     0.0KB/s   00:00
sensor#
```

ステップ 3　Ethereal または tcpdump でパケット ファイルを表示します。

パケット ファイルの消去

パケット ファイルを消去するには、**erase packet-file** コマンドを使用します。

パケット ファイルは 1 つだけです。この 16 MB のファイルは、**packet capture** コマンドを使用するたびに上書きされます。

パケット ファイルを消去するには、次の手順を実行します。

ステップ 1　現在取り込まれているパケット ファイルに関する情報を表示します。

```
sensor# packet display file-info
Captured by: cisco:1514, Cmd: packet capture GigabitEthernet0/1
Start: 2005/02/15 03:55:00 CST, End: 2005/02/15 03:55:05 CST
sensor#
```

ステップ 2　パケット ファイルを消去します。

```
sensor# erase packet-file
sensor#
```

ステップ 3　パケット ファイルが消去されたことを確認します。

```
sensor# packet display file-info
No packet-file available.
sensor#
```

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。この名前は IPS 5.1 で変更されましたが、CLI には現在も **nac** や **network-access** などの用語が存在します。

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.10-2）
- レート制限について（P.10-4）
- ARC を設定する前の作業（P.10-5）
- サポートされているデバイス（P.10-6）
- ブロッキング プロパティの設定（P.10-8）
- ユーザ プロファイルの設定（P.10-24）
- 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.10-26）
- センサーをマスター ブロッキング センサーとして使用するための設定（P.10-35）
- 手動ブロッキングの設定（P.10-38）
- ブロックされたホストと接続のリストの入手（P.10-40）

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 ファイアウォール、FWSM、および ASA でブロックを開始および停止します。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、新しいブロックに対するアクション応答を 4 ～ 7 秒以内に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、そのアクションをすべての設定済みイベント アクション オーバーライドに追加する必要があります。この操作により、SensorApp はそのシグニチャがトリガーされたときに ARC にブロック要求を送信することができます。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 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.7-13 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、特定のリスク評価のアラームに Request Block Host または Request Block Connection イベント アクションを追加するオーバーライドを設定する手順については、P.6-11 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 を適用することによって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** および **no shun** コマンドが使用されます。

注意

ARC が作成する ACL 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.10-26 の「センサーがデバイスを管理するしくみ」を参照してください。

ARC でデバイスを管理するには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）
- ログイン パスワード
- イネーブル パスワード（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）

  この情報は、PIX Firewall、FWSM、および ASA には適用されません。これらはブロックに 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。これにより、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 のステータスを表示します。

（注）ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されていますが、IDM と CLI には Network Access Controller を指す **nac** や **network-access** などの表記が存在します。

レート制限について

レート制限により、センサーはネットワーク デバイス上の指定されたトラフィック クラスのレートを制限することができます。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.10-26 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、P.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」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.13-13 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、レート制限イベントの生成を許可されたシグニチャのいずれかに一致する、プロトコル、宛先 IP アドレス、およびデータ値の組み合せを指定します。また、アクションを Request Rate Limit に設定し、該当のシグニチャの比率を指定する必要があります。表 10-1 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 10-1　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 を設定する前の作業

ブロッキングやレート制限を実行するように ARC を設定する前に、必ず次の作業を実行してください。

- ネットワーク トポロジを分析して、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。この状況が必要な場合は、一方のセンサーを、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。それにより、もう一方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できます。手順については、P.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」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 250 までのデバイスをサポートします。ARC によるブロッキングがサポートされるデバイスは、次のとおりです。

（注） ARC は、新しいブロックに対するアクション応答を 4 ～ 7 秒以内に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。

- バージョン 6.0 以降の PIX Firewall（**shun** コマンド）
  - 501
  - 506E
  - 515E
  - 525
  - 535
- バージョン 7.0 以降の ASA（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ACL、VACL、**shun** コマンドのいずれかを使用してブロッキングを設定できます。すべてのファイアウォールおよび ASA モデルは **shun** コマンドをサポートします。

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

デフォルトのブロッキング プロパティを変更することができます。デフォルトのプロパティを使用することをお勧めしますが、変更する必要がある場合は、次の手順を実行します。

- センサーによる自らのブロックの許可（P.10-8）
- ブロッキングのディセーブル化（P.10-10）
- 最大ブロック数の設定（P.10-12）
- ブロック時間の設定（P.10-14）
- ACL ロギングのイネーブル化（P.10-16）
- NVRAM への書き込みのイネーブル化（P.10-17）
- すべてのブロック イベントとエラーのロギング（P.10-19）
- ブロッキング インターフェイスの最大数の設定（P.10-20）
- ブロックしないアドレスの設定（P.10-22）

センサーによる自らのブロックの許可

センサーが自らをブロックするように設定するには、サービス ネットワーク アクセス サブモードで **allow-sensor-block [true | false]** コマンドを使用します。

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。

センサーが自らをブロックできるようにするには、次の手順を実行します。

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

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　センサーが自らをブロックするように設定します。

```
sensor(config-net-gen)# allow-sensor-block true
```

デフォルトでは、この値は **false** です。

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: true default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 6　センサーが自らをブロックしないように設定します。

```
sensor(config-net-gen)# allow-sensor-block false
```

ステップ 7　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

ブロッキングのディセーブル化

センサーでのブロッキングをイネーブルまたはディセーブルにするには、サービス ネットワーク アクセス サブモードで **block-enable [true | false]** コマンドを使用します。

（注）　ブロッキングが動作するためには、デバイスがブロッキングを実行するように設定する必要があります。手順については、P.10-27 の「センサーで Cisco ルータを管理するための設定」、および P.10-30 の「センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定」を参照してください。

センサーでは、デフォルトでブロッキングがイネーブルになっています。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。デバイスまたは ARC（またはその両方）がクラッシュするおそれがあります。

注意　デバイスのメンテナンスのためにブロッキングをディセーブルにする場合は、メンテナンスの完了後必ずブロッキングをイネーブルにしてください。これを忘れると、本来ブロックされる攻撃に対してネットワークが脆弱になります。

（注）　ブロッキングがディセーブルの間も、ARC はブロックを受信し続け、アクティブなブロックの時間を把握していますが、管理対象デバイスに対する新しいブロックの適用やブロックの削除は行いません。ブロッキングが再びイネーブルになると、デバイスのブロックが更新されます。

ブロッキングまたはレート制限をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　センサーでのブロッキングをディセーブルにします。

```
sensor(config-net-gen)# block-enable false
```

デフォルトでは、この値は **true** です。

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: false default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 6　センサーでのブロッキングをイネーブルにします。

```
sensor(config-net-gen)# block-enable true
```

ステップ 7　設定がデフォルトに戻ったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 11.11.11.11
         ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ------------------------------------------------
         ip-address: 12.12.0.0/16
         ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

最大ブロック数の設定

最大ブロック数を設定するには、サービス ネットワーク アクセス サブモードで **block-max-entries** コマンドを使用します。

同時に維持できるブロックの数を設定することができます（1 ～ 65535）。デフォルト値は 250 です。

注意　250 を超える最大ブロック数を設定することはお勧めしません。一部のデバイスでは、ACL または shun のエントリが多くなると問題が発生する場合があります。この数を増やす前に、各デバイスのマニュアルを参照し、制限を確認してください。

（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。

ブロックの最大数を変更するには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロックの最大数を変更します。

```
sensor(config-net-gen)# block-max-entries 100
```

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 6　デフォルト値である 250 ブロックに戻すには、次のコマンドを実行します。

```
sensor(config-net-gen)# default block-max-entries
```

ステップ 7　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 12.12.0.0/16
         ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
--MORE--
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

ブロック時間の設定

自動ブロックが継続する時間を変更するには、サービス イベント アクション ルール サブモードで **global-block-timeout** コマンドを使用します。デフォルトは 30 分です。

（注）　デフォルトのブロック時間を変更すると、シグニチャのパラメータを変更することになるので、すべてのシグニチャが影響を受けます。

（注）　手動ブロックの時間は、ブロックの要求時に設定されます。

デフォルトのブロック時間を変更するには、次の手順を実行します。

ステップ 1　管理者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 アクション ルール サブモードに入ります。

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

ステップ 3　汎用サブモードに入ります。

```
sensor(config-rul)# general
```

ステップ 4　ブロック時間を設定します。

```
sensor(config-rul-gen)# global-block-timeout 60
```

値は、ブロック イベントの分単位の継続期間です（0 ～ 10000000）。

ステップ 5　設定を確認します。

```
sensor(config-rul-gen)# show settings
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 60 default: 30
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
sensor(config-rul-gen)#
```

ステップ 6　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul-gen)# exit
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

（注）　シグニチャが更新される間、時間遅延が発生します。

ACL ロギングのイネーブル化

ACL ロギングをイネーブルにするには、サービス ネットワーク アクセス サブモードで **enable-acl-logging [true | false]** コマンドを使用します。ACL ロギングをイネーブルにすると、ARC は ACL または VACL のブロック エントリにログ パラメータを追加します。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。ACL ロギングのイネーブル化は、ルータとスイッチだけに適用されます。デフォルトは disable です。

ACL ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ACL ロギングをイネーブルにします。

```
sensor(config-net-gen)# enable-acl-logging true
```

ステップ 5　ACL ロギングがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: true default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　ACL ロギングをディセーブルにするには、**false** キーワードを使用します。

```
sensor(config-net-gen)# enable-acl-logging false
```

ステップ 7　ACL ロギングがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

NVRAM への書き込みのイネーブル化

ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定するには、**enable-nvram-write [true | false]** コマンドを使用します。enable-nvram-write がイネーブルの場合は、ACL が更新されるたびに NVRAM に書き込みが行われます。デフォルトは disable です。

NVRAM 書き込みをイネーブルにすると、ブロッキングに関するすべての変更が NVRAM に書き込まれます。ルータがリブートされても、正しいブロックがアクティブに保たれます。NVRAM 書き込みがディセーブルの場合は、ルータのリブート後、短時間ですがブロッキングの存在しない状態になります。NVRAM 書き込みをイネーブルにしない場合は、NVRAM の寿命が長くなり、新しいブロックの設定にかかる時間が短くなります。

NVRAM への書き込みをイネーブルにするには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　NVRAM への書き込みをイネーブルにします。

```
sensor(config-net-gen)# enable-nvram-write true
```

ステップ 5　NVRAM への書き込みがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: true default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　NVRAM への書き込みをディセーブルにします。

```
sensor(config-net-gen)# enable-nvram-write false
```

ステップ 7　NVRAM への書き込みがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

すべてのブロック イベントとエラーのロギング

ブロックの開始から終了までのイベントをログに記録するようにセンサーを設定するには、サービス ネットワーク アクセス サブモードで **log-all-block-events-and-errors [true | false]** コマンドを使用します。たとえば、デバイスにブロックを追加したり、デバイスからブロックを削除したりすると、1 つの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。**log-all-block-events-and-errors** をディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトは enabled です。

ブロック イベントとエラーのロギングをディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロック イベントとエラーのロギングをディセーブルにします。

```
sensor(config-net-gen)# log-all-block-events-and-errors false
```

ステップ 5　ロギングがディセーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: false default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
```

ステップ 6　ブロック イベントとエラーのロギングをイネーブルにします。

```
sensor(config-net-gen)# log-all-block-events-and-errors true
```

ステップ 7　ロギングがイネーブルになったことを確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

ブロッキング インターフェイスの最大数の設定

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するには、**max-interfaces** コマンドを使用します。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。デフォルトは 250 です。

ブロッキング インターフェイスの最大数を設定するには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　インターフェイスの最大数を設定します。

```
sensor(config-net-gen)# max-interfaces 50
```

ステップ 5　インターフェイスの最大数を確認します。

```
sensor(config-net-gen)# show settings
   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 50 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 6　設定をデフォルトの 250 に戻します。

```
sensor(config-net-gen)# default max-interfaces
```

ステップ 7　デフォルト設定を確認します。

```
sensor(config-net-gen)# show settings

   general
   -----------------------------------------------
      log-all-block-events-and-errors: true default: true
      enable-nvram-write: false default: false
      enable-acl-logging: false default: false
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
```

ステップ 8　ネットワーク アクセス モードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

ブロックしないアドレスの設定

ブロックしないホストとネットワークを設定するには、サービス ネットワーク アクセス サブモードで **never-block-hosts** コマンドおよび **never-block-networks** コマンドを使用します。

次のオプションが適用されます。

- *ip_address*：ブロックしないデバイスの IP アドレス。
- *ip_address/netmask*：ブロックしないネットワークの IP アドレス。形式は、A.B.C.D./nn です。

手動であっ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。これは、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。

1 つのホストまたはネットワーク全体を指定できます。

ブロッキング デバイスでブロックしないアドレスを設定するには、次の手順を実行します。

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

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 4　ブロックしないアドレスを定義します。

- 1 つのホストの場合

  ```
  sensor(config-net-gen)# never-block-hosts 10.16.0.0
  ```

- ネットワーク全体の場合

  ```
  sensor(config-net-gen)# never-block-networks 10.0.0.0/8
  ```

ステップ 5　設定を確認します。

```
sensor(config-net-gen)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false default: false
      block-enable: true default: true
      block-max-entries: 100 default: 250
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 2)
      ----------------------------------------------
         ip-address: 10.16.0.0
         ----------------------------------------------
         ip-address: 11.11.11.11
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 2)
      ----------------------------------------------
         ip-address: 10.0.0.0/8
         ----------------------------------------------
         ip-address: 12.12.0.0/16
--MORE--
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

ユーザ プロファイルの設定

センサーで管理する他のデバイスのユーザ プロファイルを設定するには、サービス ネットワーク アクセス サブモードで **user-profiles** *profile_name* コマンドを使用します。ユーザ プロファイルには、ユーザ ID、パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同じパスワードとユーザ名を使用するルータはすべて 1 つのユーザ プロファイルの下にまとめることができます。

(注) デバイスへのログインにユーザ名やパスワードが不要である場合は、値を設定しないでください。

(注) ブロッキング デバイスを設定する前に、ユーザ プロファイルを作成する必要があります。

ユーザ 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　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ネットワーク アクセス モードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ユーザ プロファイル名を作成します。

```
sensor(config-net)# user-profiles PROFILE1
```

ステップ 4　このユーザ プロファイルのユーザ名を入力します。

```
sensor(config-net-use)# username username
```

ステップ 5　ユーザのパスワードを指定します。

```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```

ステップ 6　ユーザのイネーブル パスワードを指定します。

```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```

ステップ 7　設定を確認します。

```
sensor(config-net-use)# show settings
   profile-name: PROFILE1
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   ----------------------------------------------
sensor(config-net-use)#
```

ステップ 8　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-use)# exit
sensor(config-net)# exit
Apply Changes:?[yes]:
```

ステップ 9　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。

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、センサーがブロックやレート制限に使用するデバ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。

- センサーがデバイスを管理するしくみ（P.10-26）
- センサーで Cisco ルータを管理するための設定（P.10-27）
- センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定（P.10-30）
- センサーで Cisco ファイアウォールを管理するための設定（P.10-33）

センサーがデバイスを管理するしくみ

ARC は、Cisco ルータおよびスイッチ上の ACL を使用してこれらのデバイスを管理します。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 NAT アドレス（指定されている場合）を記述した **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） 一致しなかったすべてのパケットを許可する場合は、ACL の最後の行を必ず **permit ip any any** にしてください。

   - **permit ip any any**（Post-Block ACL が指定されている場合は使用されません）

ARC は、2 つの ACL を使用してデバイスを管理します。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.10-8 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.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」を参照してください。

センサーで Cisco ルータを管理するための設定

この項では、センサーを設定して Cisco ルータ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。

- ルータと ACL（P.10-27）
- センサーで Cisco ルータを管理するための設定（P.10-28）

ルータと ACL

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。

センサーで Cisco ルータを管理するための設定

センサーを設定して Cisco ルータを管理し、ブロッキングやレート制限を実行するには、次の手順を実行します。

ステップ 1　管理者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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたルータの IP アドレスを設定します。

```
sensor(config-net)# router-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成した論理デバイス名を入力します。

```
sensor(config-net-rou)# profile-name user_profile_name
```

何を入力しても ARC によって受け入れられます。ユーザ プロファイルが存在するかどうはチェックされません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-rou)# communication [telnet | ssh-des | ssh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

(注)　DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-rou)# nat-address nat_address
```

(注)　これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　ルータで、ブロッキングまたはレート制限（あるいはその両方）を実行するかどうかを指定します。

(注)　デフォルトはブロッキングです。ルータでブロッキングだけを実行する場合は、応答機能を設定する必要はありません。

a.　レート制限だけの場合は、次のコマンドを実行します。

```
sensor(config-net-rou)# response-capabilities rate-limit
```

b.　ブロッキングとレート制限の両方を実行する場合は、次のコマンドを実行します。

```
sensor(config-net-rou)# response-capabilities block|rate-limit
```

ステップ 8　インターフェイス名と方向を設定します。

```
sensor(config-net-rou)# block-interfaces interface_name [in | out]
```

注意　インターフェイスの名前は、インターフェイスの完全な名前か、**interface** コマンドで使用したときにルータで認識される省略名である必要があります。

ステップ 9　（オプション）Pre-ACL 名を追加します（ブロッキングのみ）。

```
sensor(config-net-rou-blo)# pre-acl-name pre_acl_name
```

ステップ 10（オプション）Post-ACL 名を追加します（ブロッキングのみ）。

```
sensor(config-net-rou-blo)# post-acl-name post_acl_name
```

ステップ 11 設定を確認します。

```
sensor(config-net-rou-blo)# exit
sensor(config-net-rou)# show settings
   ip-address: 10.89.127.97
   ----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      ---------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         ---------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         ---------------------------------------------
      ---------------------------------------------
      response-capabilities: block|rate-limit default: block
   ----------------------------------------------
sensor(config-net-rou)#
```

ステップ 12 ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-rou)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 13 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。

センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定

この項では、センサーを設定して Cisco スイッチ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。

- スイッチと VACL（P.10-30）
- センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定（P.10-31）

スイッチと VACL

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。

ルータの ACL を使用したブロッキングについては、P.10-27 の「センサーで Cisco ルータを管理するための設定」を参照してください。

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。

Pre-Block VACL と Post-Block VACL は、スイッチ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 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。

センサーで Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するための設定

センサーを設定して Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータを管理するには、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　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたルータの IP アドレスを設定します。

```
sensor(config-net)# cat6k-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成したユーザ プロファイル名を入力します。

```
sensor(config-net-cat)# profile-name user_profile_name
```

（注）　何を入力しても ARC によって受け入れられます。これは、論理デバイスが存在するかどうかをチェックしません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-cat)# communication [telnet | ssh-des/ | sh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

（注）　DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-cat)# nat-address nat_address
```

（注）　これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　VLAN 番号を指定します。

```
sensor(config-net-cat)# block-vlans vlan_number
```

ステップ 8　（オプション）Pre-VACL 名を追加します。

```
sensor(config-net-cat-blo)# pre-vacl-name pre_vacl_name
```

ステップ 9　（オプション）Post-VACL 名を追加します。

```
sensor(config-net-cat-blo)# post-vacl-name post_vacl_name
```

ステップ 10　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-cat-blo)# exit
sensor(config-net-cat)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 11　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。

センサーで Cisco ファイアウォールを管理するための設定

センサーを設定して Cisco ファイアウォールを管理するには、次の手順を実行します。

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

ステップ 2　ネットワーク アクセス サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3　ARC によって制御されたファイアウォールの IP アドレスを設定します。

```
sensor(config-net)# firewall-devices ip_address
```

ステップ 4　P.10-24 の「ユーザ プロファイルの設定」で作成したユーザ プロファイル名を入力します。

```
sensor(config-net-fir)# profile-name user_profile_name
```

（注）　何を入力しても ARC によって受け入れられます。これは、論理デバイスが存在するかどうかをチェックしません。

ステップ 5　センサーにアクセスするために使用する方法を指定します。

```
sensor(config-net-fir)# communication [telnet | ssh-des | sh-3des]
```

指定しない場合は、SSH 3DES が使用されます。

（注） DES または 3DES を使用している場合は、コマンド **ssh host-key** *ip_address* を使用して鍵を受け入れる必要があります。そうしないと、ARC はデバイスに接続できません。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 6　センサーの NAT アドレスを指定します。

```
sensor(config-net-fir)# nat-address nat_address
```

（注） これによって ACL の最初の行の IP アドレスがセンサーのアドレスから NAT アドレスへ変更されます。これは、管理対象のサービスで設定された NAT アドレスではありません。センサーは、中間デバイスによってこのアドレスに変換されます。つまり、これは、センサーと管理対象デバイスの間のアドレスです。

ステップ 7　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-fir)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 8　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。

センサーをマスター ブロッキング センサーとして使用するための設定

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。この状況が必要な場合は、一方のセンサーを、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。それにより、もう一方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。

マスター ブロッキング センサーを設定するには、サービス ネットワーク アクセス サブモードで `master-blocking-sensors` *mbs_ip_address* コマンドを使用します。

次のオプションが適用されます。

- *mbs_ip_address*：ブロック要求を転送するセンサーの IP アドレス。
- **password**：ブロック要求を転送するセンサーのアカウント パスワード。
- **port**：ブロック要求を転送するセンサーのポート。
- **tls [true | false]**：リモート センサーで TLS が必要な場合は true に設定し、そうでない場合は false に設定します。
- **username**：ブロック要求を転送するセンサーのアカウント名。

センサーの ARC がマスター ブロッキング センサーにブロックを転送するように設定するには、次の手順を実行します。

ステップ 1　マスター ブロッキング センサーとブロッキング転送センサーの両方で管理者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　両方のセンサーで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　必要に応じて TLS を設定します。

a. マスター ブロッキング センサーで、TLS が必要かどうかと、使用されるポート番号を確認します。

```
sensor(config)# service web-server
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)#
```

`enable-tls` が true の場合は、ステップ b に進みます。

b. ブロッキング転送センサーで、このセンサーがマスター ブロッキング センサーの X.509 証明書を受け入れるように設定します。

```
sensor(config-web)# exit
sensor(config)# tls trusted-host ip-address mbs_ip_address port port_number
```

例

```
sensor(config)# tls trusted-host ip-address 10.0.0.0 port 8080
Certificate MD5 fingerprint is
F4:4A:14:BA:84:F4:51:D0:A4:E2:15:38:7E:77:96:D8Certificate SHA1 fingerprint is
84:09:B6:85:C5:43:60:5B:37:1E:6D:31:6A:30:5F:7E:4D:4D:E8:B2
Would you like to add this to the trusted certificate table for this host?[yes]:
```

(注)　証明書のフィンガープリントに基づいて証明書を受け入れるよう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 センサーのホストでセンサーにログインし、**show tls fingerprint** コマンドを入力して、このホストの証明書のフィンガープリントと一致することを確認することによって、ホスト センサーの証明書を検証することができます。

ステップ 4　`yes` を入力して、マスター ブロッキング センサーの証明書を受け入れます。

ステップ 5　ネットワーク アクセス モードに入ります。

```
sensor(config)# service network-access
```

ステップ 6　汎用サブモードに入ります。

```
sensor(config-net)# general
```

ステップ 7　マスター ブロッキング センサーのエントリを追加します。

```
sensor(config-net-gen)# master-blocking-sensors mbs_ip_address
```

ステップ 8　マスター ブロッキング センサー ホストの管理アカウントのユーザ名を指定します。

```
sensor(config-net-gen-mas)# username username
```

ステップ 9　ユーザのパスワードを指定します。

```
sensor(config-net-gen-mas)# password
Enter password []: *****
Re-enter mbs-password []: *****
sensor(config-net-gen-mas)#
```

ステップ 10　ホストの HTTP 通信用のポート番号を指定します。

```
sensor(config-net-gen-mas)# port port_number
```

指定しない場合、デフォルトは 80/443 になります。

ステップ 11　ホストが TLS/SSL を使用するかどうかのステータスを設定します。

```
sensor(config-net-gen-mas)# tls [true | false]
sensor(config-net-gen-mas)
```

(注)　この値を true に設定する場合は、コマンド **tls trusted-host ip-address** *mbs_ip_address* を使用する必要があります。

ステップ 12　ネットワーク アクセス サブモードを終了します。

```
sensor(config-net-gen-mas)# exit
sensor(config-net-gen)# exit
sensor(config-net)# exit
sensor(config)# exit
Apply Changes:?[yes]:
```

ステップ 13　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 14 マスター ブロッキング センサーで、アクセス リストにブロック転送センサーの IP アドレスを追加します。手順については、P.4-6 の「アクセス リストの変更」を参照してください。

手動ブロッキングの設定

ホストまたはネットワークを手動でブロックするには、サービス ネットワーク アクセス サブモードで **block-hosts** コマンドおよび **block-networks** コマンドを使用します。手動ブロックを設定する前に、ブロッキングを設定しておく必要があります。また、ブロックされているホストとネットワークのリストを表示することもできます。

(注) CLI での手動ブロックでは実際にコンフィギュレーションが変更されるため、ブロックは永続的です。期間を限定した手動ブロックを実行することはできません。CLI で作成したブロックを IPS マネージャを使用して削除することはできません。手動ブロックは CLI で削除する必要があります。

注意 手動ブロッキングは、使用するとしても最小限にすることをお勧めします。

ホストまたはネットワークを手動でブロックするには、次の手順を実行します。

ステップ 1 管理者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 ネットワーク アクセス モードに入ります。

```
sensor# configuration terminal
sensor(config)# service network-access
sensor(config-net)#
```

ステップ 3 汎用モードに入ります。

```
sensor (config-net)# general
sensor(config-net-gen)#
```

ステップ 4 手動ブロックを開始します。

a. ホストの IP アドレスの場合

```
sensor(config-net-gen)# block-hosts ip_address
```

b. ネットワークの IP アドレスの場合

```
sensor(config-net-gen)# block-networks ip_address/netmask
```

ip_address/netmask の形式は、A.B.C.D/nn です。

例

```
sensor (config-net-gen)# block-networks 10.0.0.0/8
```

（注） 手動ブロックは、CLI で終了しない限り永続します。

ステップ 5　手動ブロックを終了するには、次の操作を実行します。

```
sensor (config-net-gen)# no block-hosts ip_address
```

ステップ 6　ネットワーク アクセス サブモードを終了します。

```
sensor (config-net-gen)# exit
sensor (config-net)# exit
sensor(config)# exit
sensor#
```

ブロックされたホストと接続のリストの入手

ブロックされたホストとブロックされた接続のリストを入手するには、**show statistics** コマンドを使用します。

ブロックされたホストと接続のリストを入手するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を確認します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.1.1.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.1.1.1
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   BlockedAddr
      Host
         IP = 192.168.1.1
         Vlan =
         ActualIp =
         BlockMinutes = 80
         MinutesRemaining = 76
```

`Host` エントリに、ブロックされているホストと、ブロックされている時間が示されます。

SNMP の設定

この章では、SNMP の設定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.7-13 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 の概要（P.11-2）
- SNMP の設定（P.11-3）
- SNMP トラップの設定（P.11-6）
- サポートされている MIB（P.11-8）

SNMP の概要

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

SNMP の汎用パラメータをサービス通知サブモードで設定します。

（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.7-13 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。

次のオプションが適用されます。

- **default**：値をシステム デフォルト設定に戻します。
- **enable-set-get [true | false]**：Object Identifier（OID; オブジェクト ID）の取得および設定をイネーブルにします。
- **no**：エントリまたは選択設定を削除します。
- **read-only-community**：SNMP エージェントの読み取り専用コミュニティ名。
  デフォルトは public です。
- **read-write-community**：SNMP エージェントの読み取り / 書き込みコミュニティ名。
  デフォルトは private です。
- **snmp-agent-port**：SNMP エージェントが受信するポート。
  デフォルト SNMP ポート番号は 161 です。
- **snmp-agent-protocol**：SNMP エージェントが通信に使用するプロトコル。
  デフォルト プロトコルは UDP です。
- **system-contact**：このセンサーの接続情報。
  system-contact オプションでは、SNMPv2-MIB::sysContact.0 値が変更されます。
- **system-location**：センサーの場所。
  system-location オプションでは、SNMPv2-MIB::sysLocation.0 値が変更されます。

SNMP の汎用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 CLI にログインします。

ステップ 2　通知サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)#
```

ステップ 3　SNMP をイネーブルにして、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します。

```
sensor(config-not)# enable-set-get true
```

ステップ 4　SNMP エージェント パラメータを設定します。

次の値で、センサー SNMP エージェントにコミュニティ名を設定します。コミュニティ名はプレーンテキストのパスワード メカニズムで、SNMP クエリーの weak 認証を行うのに使用されます。

a. 読み取り専用コミュニティ ストリングを割り当てます。

```
sensor(config-not)# read-only-community PUBLIC1
```

読み取り専用コミュニティ名で、SNMP エージェントに対するクエリーのパスワードを指定します。

b. 読み取り / 書き込みコミュニティ ストリングを割り当てます。

```
sensor(config-not)# read-write-community PRIVATE1
```

読み取り / 書き込みコミュニティ名で、SNMP エージェントに対するセットのパスワードを指定します。

(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から発行された要求において、コミュニティ ストリングがセンサー上の内容と一致しない場合、センサーによって要求が拒否されます。

c. センサー接続ユーザ ID を割り当てます。

```
sensor(config-not)# system-contact BUSINESS
```

d. センサーの場所を入力します。

```
sensor(config-not)# system-location AUSTIN
```

e. センサー SNMP エージェントのポートを入力します。

```
sensor(config-not)# snmp-agent-port 161
```

(注) ポートまたはプロトコルを変更する場合はセンサーをリブートする必要があります。

f. センサー SNMP エージェントが使用するプロトコルを選択します。

```
sensor(config-not)# snmp-agent-protocol udp
```

(注) ポートまたはプロトコルを変更する場合はセンサーをリブートする必要があります。

ステップ 5　設定を確認します。

```
sensor(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: public <defaulted>
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
sensor(config-not)#
```

ステップ 6　通知サブモードを終了します。

```
sensor(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 7　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。

SNMP トラップの設定

SNMP トラップをサービス通知サブモードで設定します。

（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.7-13 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。

次のオプションが適用されます。

- **enable-detail-traps [true | false]**：詳細トラップの送信をサイズ制限なしでイネーブルにします。このオプションを設定しない場合、トラップは希薄モード（484 バイト未満）で送信されます。
- **enable-notifications [true | false]**：イベント通知をイネーブルにします。
- **error-filter [warning | error | fatal]**：SNMP トラップを生成するエラーを決定します。SNMP トラップは、フィルタに一致する evError イベントすべてに対して生成されます。デフォルトは、error および fatal です。
- **trap-community-name**：トラップの宛先を定義したときに名前が指定されていなかった場合に、トラップ送信に際して使用されるコミュニティ名。
- **trap-destinations**：シグニチャ アクションで生成されたエラー イベントおよびアラート イベントを送信する宛先を定義します。
  - **trap-community-name**：トラップを送信するときに使用されるコミュニティ名。コミュニティ名が指定されていない場合、汎用トラップ コミュニティ名が使用されます。
  - **trap-port**：SNMP トラップの送信先ポート番号。

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 CLI にログインします。

ステップ 2　通知サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)#
```

ステップ 3　SNMP トラップをイネーブルにします。

```
sensor(config-not)# enable-notifications true
```

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。

```
sensor(config-not)# error-filter [error | warning | fatal]
```

（注） **error-filter [error | warning | fatal]** コマンドには、エラー トラップ、警告トラップ、および重大トラップがあります。重大度に基づいて、トラップをフィルタリングして組み込みます（フィルタリングして排除ではない）。

b. 詳細 SNMP トラップが必要であるかどうかを選択します。

```
sensor(config-not)# enable-detail-traps true
```

c. 詳細トラップに組み込むコミュニティ ストリングを入力します。

```
sensor(config-not)# trap-community-name TRAP1
```

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. SNMP 管理ステーションの IP アドレスを入力します。

```
sensor(config-not)# trap-destinations 10.1.1.1
```

b. SNMP 管理ステーションの UDP ポートを入力します。

```
sensor(config-not-tra)# trap-port 162
```

デフォルトは 162 です。

c. トラップ コミュニティ ストリングを入力します。

```
sensor(config-not-tra)# trap-community-name AUSTIN_PUBLI
```

(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。

ステップ 6　設定を確認します。

```
sensor(config-not-tra)# exit
sensor(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 1)
   -----------------------------------------------
      ip-address: 10.1.1.1
      ---------------------------------------------
         trap-community-name: AUSTIN_PUBLIC default:
         trap-port: 161 default: 162
      ---------------------------------------------
   -----------------------------------------------
   error-filter: warning|error|fatal default: error|fatal
   enable-detail-traps: true default: false
   enable-notifications: true default: false
   enable-set-get: true default: false
   snmp-agent-port: 161 default: 161
   snmp-agent-protocol: udp default: udp
   read-only-community: PUBLIC1 default: public
   read-write-community: PRIVATE1 default: private
   trap-community-name: PUBLIC1 default: public
   system-location: AUSTIN default: Unknown
   system-contact: BUSINESS default: Unknown
sensor(config-not)#
```

ステップ 7　通知サブモードを終了します。

```
sensor(config-not)# exit
Apply Changes:?[yes]:
```

ステップ 8　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。

サポートされている MIB

次のプライベート MIB がセンサーでサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

これらのプライベート Cisco MIB は、次の URL の見出し SNMP v2 MIBs から取得できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

センサーでサポートされている管理 MIB は、rfc1213 (mib-2) です。

この mib-2 は、たとえば http://rfc.net/rfc1213.html のようなパブリック ドメインから取得できます。

コンフィギュレーション ファイルの処理

この章では、コンフィギュレーション ファイルを表示、コピー、および消去するコマンドの使用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。

- 現在のコンフィギュレーションの表示（P.12-2）
- 現在のサブモード コンフィギュレーションの表示（P.12-4）
- 現在のコンフィギュレーション出力のフィルタリング（P.12-13）
- 現在のサブモード コンフィギュレーション出力のフィルタリング（P.12-16）
- 論理ファイルの内容の表示（P.12-18）
- リモート サーバを使用したコンフィギュレーション ファイルのコピーおよび復元（P.12-20）
- バックアップ コンフィギュレーション ファイルの作成および使用（P.12-22）
- コンフィギュレーション ファイルの消去（P.12-23）

現在のコンフィギュレーションの表示

現在のコンフィギュレーションの内容を表示するには、**show configuration** コマンドまたは **more current-config** コマンドを使用します。

現在のコンフィギュレーションの内容を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在のコンフィギュレーションを表示します。

```
sensor# show configuration
! ------------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ------------------------------
display-serial
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
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
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
user-profiles test
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 60000 0
alert-severity medium
sig-fidelity-rating 75
sig-description
sig-name My Sig
sig-string-info My Sig Info
sig-comment Sig Comment
exit
engine string-tcp
```

```
event-action produce-alert
direction to-service
regex-string My Regex String
service-ports 23
exit
event-counter
event-count 1
event-count-key Axxx
specify-alert-interval no
exit
alert-frequency
summary-mode summarize
summary-interval 15
summary-key Axxx
specify-global-summary-threshold yes
global-summary-threshold 75
exit
exit
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
sensor#
```

現在のサブモード コンフィギュレーションの表示

サブモードの現在のコンフィギュレーションを表示するには、そのサブモードで **show settings** コマンドを使用します。

サブモードの現在の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　サービス分析エンジン サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)# show settings
   global-parameters
   ---------------------------------------------
      ip-logging
      ---------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      ---------------------------------------------
   ---------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   ---------------------------------------------
      <protected entry>
      name: vs0 <defaulted>
      ---------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         physical-interface (min: 0, max: 999999999, current: 0)
         ---------------------------------------------
         ---------------------------------------------
         logical-interface (min: 0, max: 999999999, current: 0)
         ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ---------------------------------------------
sensor(config-ana)# exit
sensor(config)# exit
sensor#
```

ステップ 3　サービス認証サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service authentication
sensor(config-aut)# show settings
   attemptLimit: 0 <defaulted>
sensor(config-aut)# exit
sensor(config)# exit
sensor#
```

ステップ 4　サービス イベント アクション ルール サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# show settings
   variables (min: 0, max: 256, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   overrides (min: 0, max: 12, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
   -----------------------------------------------
   general
   -----------------------------------------------
      global-overrides-status: Enabled <defaulted>
      global-filters-status: Enabled <defaulted>
      global-summarization-status: Enabled <defaulted>
      global-metaevent-status: Enabled <defaulted>
      global-deny-timeout: 3600 <defaulted>
      global-block-timeout: 30 <defaulted>
      max-denied-attackers: 10000 <defaulted>
   -----------------------------------------------
   target-value (min: 0, max: 5, current: 0)
   -----------------------------------------------
   -----------------------------------------------
sensor(config-rul)# exit
sensor(config)# exit
sensor# exit
```

ステップ 5　サービス ホスト サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.149.27/25,10.89.149.126 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 2)
      ---------------------------------------------
         network-address: 10.0.0.0/8
         -------------------------------------------
         network-address: 64.0.0.0/8
         -------------------------------------------
      ---------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
   time-zone-settings
   -----------------------------------------------
      offset: 0 minutes default: 0
      standard-time-zone-name: UTC default: UTC
   -----------------------------------------------
   ntp-option
   -----------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
   -----------------------------------------------
   summertime-option
   -----------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
```

```
   ----------------------------------------------
   auto-upgrade-option
   ----------------------------------------------
      disabled
      ---------------------------------------------
      ---------------------------------------------
   ----------------------------------------------
   crypto
   ----------------------------------------------
      key (min: 0, max: 10, current: 2)
      ---------------------------------------------
         <protected entry>
         name: realm-cisco.pub <defaulted>
         type
         ---------------------------------------------
            rsa-pubkey
            ---------------------------------------------
               length: 2048 <defaulted>
               exponent: 65537 <defaulted>
               modulus: 2444218998935774708387485533523262884359996893419855964 8
630199473878411519325039111726689401947545491553904076580203933306118912925083 00
859403040311860144996325688124280680580895816141963373996230606249900570491030 55
901539559350860600086797768080736401860634357232523755752931263045580687043018 63
805621144374392890694566709220749958273902847616105915157520084051402436730831 89
778224699649345983670103893898882974908028841185437300762935897035359121619933 19
470931302986888300125472155726463496235394688386410649153139478068529040823519 55
132172731380999653830397161301532707152200465671078281289241976924173320339117 04
3 <defaulted>
            ---------------------------------------------
         ---------------------------------------------
         <protected entry>
         name: realm-trend.pub <defaulted>
         type
         ---------------------------------------------
            rsa-pubkey
            ---------------------------------------------
               length: 2048 <defaulted>
               exponent: 65537 <defaulted>
               modulus: 2176556142257302131415985535141872303162509338077705369 6
638172895270605709325510654898181907137456721482605270300606672083666066038026 79
304390667241433906264954793005501016181795846372870529364656921465726126513759 69
203545215856442216029442035208044042129754019708951199037567696011338536732967 66
452897957779734919840565870452145148200633669507313464000443084915946264347069 99
476086688228140148300633995342046470695090524434395253637065272552245107711222 35
801811504605447832514984814327059910100698443685257548784136694276397529508017 67
999053092352324562955800867242032979140959842243284443915822231384237991008381 91
9 <defaulted>
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
   ----------------------------------------------
sensor(config-hos)# exit
sensor(config)# exit
sensor#
```

ステップ 6　サービス インターフェイス サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# show settings
   physical-interfaces (min: 0, max: 999999999, current: 4)
   ----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/0 <defaulted>
      ----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
         subinterface-type
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      <protected entry>
      name: GigabitEthernet0/1 <defaulted>
      ----------------------------------------------
         media-type: tx <protected>
         description: <defaulted>
         admin-state: disabled <protected>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
         subinterface-type
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      <protected entry>
      name: GigabitEthernet2/0 <defaulted>
      ----------------------------------------------
         media-type: xl <protected>
         description: <defaulted>
         admin-state: disabled <defaulted>
         duplex: auto <defaulted>
         speed: auto <defaulted>
         alt-tcp-reset-interface
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
         ----------------------------------------------
         subinterface-type
         ----------------------------------------------
            none
            ----------------------------------------------
            ----------------------------------------------
```

```
            ----------------------------------------------
         ---------------------------------------------
         <protected entry>
         name: GigabitEthernet2/1 <defaulted>
         ---------------------------------------------
            media-type: xl <protected>
            description: <defaulted>
            admin-state: disabled <defaulted>
            duplex: auto <defaulted>
            speed: auto <defaulted>
            alt-tcp-reset-interface
            ----------------------------------------------
               none
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            subinterface-type
            ----------------------------------------------
               none
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      command-control: GigabitEthernet0/1 <protected>
      inline-interfaces (min: 0, max: 999999999, current: 0)
      ---------------------------------------------
      ---------------------------------------------
      bypass-mode: auto <defaulted>
      interface-notifications
      ---------------------------------------------
         missed-percentage-threshold: 0 percent <defaulted>
         notification-interval: 30 seconds <defaulted>
         idle-interface-delay: 30 seconds <defaulted>
      ---------------------------------------------
sensor(config-int)# exit
sensor(config)# exit
sensor#
```

ステップ 7　サービス ロガー サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: false <defaulted>
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)# exit
sensor(config)# exit
sensor#
```

ステップ 8　サービス ネットワーク アクセス サブモードの現在のコンフィギュレーションを表示します。

```
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>
      rate-limit-max-entries: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ----------------------------------------------
      profile-name: test
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: <defaulted>
      ----------------------------------------------
   ----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ----------------------------------------------
   ----------------------------------------------
   router-devices (min: 0, max: 250, current: 0)
   ----------------------------------------------
   ----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ----------------------------------------------
   ----------------------------------------------
sensor(config-net)# exit
sensor(config)# exit
sensor#
```

ステップ 9　通知サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service notification
sensor(config-not)# show settings
   trap-destinations (min: 0, max: 10, current: 0)
   -----------------------------------------------
   -----------------------------------------------
   error-filter: error|fatal <defaulted>
   enable-detail-traps: false <defaulted>
   enable-notifications: false <defaulted>
   enable-set-get: false <defaulted>
   snmp-agent-port: 161 <defaulted>
   snmp-agent-protocol: udp <defaulted>
   read-only-community: public <defaulted>
   read-write-community: private <defaulted>
   trap-community-name: public <defaulted>
   system-location: Unknown <defaulted>
   system-contact: Unknown <defaulted>
sensor(config-not)# exit
sensor(config)# exit
sensor#
```

ステップ 10　シグニチャ定義サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings
   variables (min: 0, max: 256, current: 1)
   ----------------------------------------------
      <protected entry>
      variable-name: WEBPORTS
      ----------------------------------------------
         web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,2432
6-24326 <defaulted>
      ----------------------------------------------
   ----------------------------------------------
   application-policy
   ----------------------------------------------
      http-policy
      ----------------------------------------------
         http-enable: false <defaulted>
         max-outstanding-http-requests-per-connection: 10 <defaulted>
         aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
      ----------------------------------------------
      ftp-enable: false <defaulted>
   ----------------------------------------------
   fragment-reassembly
   ----------------------------------------------
      ip-reassemble-mode: nt <defaulted>
   ----------------------------------------------
   stream-reassembly
   ----------------------------------------------
--MORE--
```

ステップ 11 SSH の既知のホスト サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service ssh-known-hosts
sensor(config-ssh)# show settings
   rsa1-keys (min: 0, max: 500, current: 0)
   -----------------------------------------------
   -----------------------------------------------
sensor(config-ssh)# exit
sensor(config)# exit
sensor#
```

ステップ 12 trusted certificate サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service trusted-certificate
sensor(config-tru)# show settings
   trusted-certificates (min: 0, max: 500, current: 1)
   -----------------------------------------------
      common-name: 10.89.130.108
      certificate: MIICJDCCAY0CCPbSkgXUchJIMA0GCSqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTA
lVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwEAYDVQQLEwlTU00tSVBTMjAxFjAUBgNVB
AMTDTEwLjg5LjEzMC4xMDgwHhcNMDMwMTAzMDE1MjEwWhcNMDUwMTAzMDE1MjEwWjBXMQswCQYDVQQGE
wJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESMBAGA1UECxMJU1NNLUlQUzIwMRYwFAYDV
QQDEw0xMC44OS4xMzAuMTA4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzldqLFG4MT4bfgh3mJ
fP/DCilnnaLfzHK9FdnhmWI4FY+9MVvAI7MOhAcuV6HYfyp6n6cYvH+Eswzl9uv7H5nouID9St9GI3Yr
SUtlIQAJ4QVL2DwWP230x6KdHrYqcj+Nmhc7AnnPypjidwGSfF+VetIJLEeRFh/mI2JcmwF2QIDAQABM
A0GCSqGSIb3DQEBBQUAA4GBAAUI2PLANTOehxvCfwd6UAFXvy8uifbjqKMC1jrrF+f9KGkxmR+XZvUaG
OS83FYDXlXJvB5Xyxms+Y01wGjzKKpxegBoan8OB8o193Ueszdpvz2xYmiEgywCDyVJRsw3hAFMXWMS5
XsBUiHtw0btHH0j7ElFZxUjZv12fGz8hlnY
   -----------------------------------------------
sensor(config-tru)# exit
sensor(config)# exit
sensor#
```

ステップ 13 Web サーバ サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor(config)# service web-server
sensor(config-web)# show settings
   enable-tls: true <defaulted>
   port: 443 <defaulted>
   server-id: HTTP/1.1 compliant <defaulted>
sensor(config-web)# exit
sensor(config)# exit
sensor#
```

現在のコンフィギュレーション出力のフィルタリング

現在のコンフィギュレーションの内容の出力を検索またはフィルタリングするには、**show configuration | [begin | exclude | include]** *regular-expression* コマンドを使用します。

（注） オペレータ特権またはビューア特権を持つユーザが検索またはフィルタリングできるのは、**current-config** だけです。

次のオプションが適用されます。

- **|**：パイプ記号は、出力処理の指定がこの後に続くことを示します。
- **begin**：指定した正規表現を含む最初の行で、**show configuration** コマンドのフィルタリングしない出力を開始します。
- **exclude**：指定した正規表現を含む行を **show configuration** コマンドの出力から除外します。
- **include**：指定した正規表現を含む行だけを **show configuration** コマンドの出力に含めます。
- *regular-expression*：**show configuration** コマンド出力にある任意の正規表現。

（注） *regular-expression* オプションには大文字と小文字の区別があり、複雑なマッチング要件に対応しています。

現在のコンフィギュレーションの内容の出力を検索またはフィルタリングするには、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　例として、正規表現「ssh」で始まるコンフィギュレーション出力を検索します。

（注） **show configuration | begin** *regular-expression* コマンドは、指定された正規表現を含む最初の行で、**show** コマンドのフィルタリングされない出力を開始します。

```
sensor# show configuration | begin ssh
communication ssh-3des
profile-name test1
block-vlans 234
pre-vacl-name aaaa
post-vacl-name bbbb
exit
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2200 0
engine service-generic
specify-payload-source yes
payload-source l2-header
exit
```

```
exit
exit
signatures 12300 0
status
enabled true
retired true
--MORE--
```

（注） 出力を中止して CLI プロンプトに戻るには、**Ctrl+C** キーを押します。

ステップ 3　現在のコンフィギュレーションをフィルタリングして、正規表現、たとえば、「service」を含む行を除外します。

```
sensor# show configuration | exclude service
! ------------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ------------------------------
display-serial
! ------------------------------
exit
! ------------------------------
exit
! ------------------------------
exit
! ------------------------------
exit
! ------------------------------
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
exit
time-zone-settings
offset 0
standard-time-zone-name UTC!
--MORE--
```

（注） 出力を中止して CLI プロンプトに戻るには、**Ctrl+C** キーを押します。

ステップ 4　現在のコンフィギュレーションをフィルタリングして、正規表現、たとえば、「service」を含む行を表示します。

```
sensor# show configuration | include service
service analysis-engine
service authentication
service event-action-rules rules0
service host
service interface
service logger
service network-access
service notification
service signature-definition sig0
engine service-generic
service ssh-known-hosts
service trusted-certificates
service web-server
sensor#
```

現在のサブモード コンフィギュレーション出力のフィルタリング

サブモード コンフィギュレーションの内容の出力を検索またはフィルタリングするには、**show settings | [begin | exclude | include]** *keyword* コマンドを対象のサブモードで使用します。

次のオプションが適用されます。

- **|**：パイプ記号は、出力処理の指定がこの後に続くことを示します。
- **begin**：指定した正規表現を含む最初の行で、**show settings** コマンドのフィルタリングしない出力を開始します。
- **exclude**：指定した正規表現を含む行を **show settings** コマンドの出力から除外します。
- **include**：指定した正規表現を含む行だけを **show settings** コマンドの出力に含めます。
- *regular-expression*：**show settings** コマンド出力にある任意の正規表現。

（注） *regular-expression* オプションには大文字と小文字の区別があり、複雑なマッチング要件に対応しています。

サブモード コンフィギュレーションの内容の出力を検索またはフィルタリングするには、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　例として、正規表現「filters」のイベント アクション ルール設定の出力を検索します。

```
sensor# configure terminal
sensor(config)# service event-action-rules
sensor(config-rul)# show settings | begin filters
filters (min: 0, max: 4096, current: 0 - 0 active, 0 inactive)
 ----------------------------------------------
 general
 ----------------------------------------------
    global-overrides-status: Enabled <defaulted>
    global-filters-status: Enabled <defaulted>
    global-summarization-status: Enabled <defaulted>
    global-metaevent-status: Enabled <defaulted>
    global-deny-timeout: 3600 <defaulted>
    global-block-timeout: 15 default: 30
    max-denied-attackers: 10000 <defaulted>
 ----------------------------------------------
 target-value (min: 0, max: 5, current: 0)
 ----------------------------------------------
 ----------------------------------------------
sensor(config-rul)#
```

ステップ 3　ネットワーク アクセス設定の出力をフィルタリングして、正規表現を除外します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings | exclude false
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true default: true
      block-enable: true default: true
      block-max-entries: 11 default: 250
      max-interfaces: 13 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 1)
      ----------------------------------------------
         ipaddress: 10.89.149.124
         ----------------------------------------------
            password: <hidden>
            port: 443 default: 443
            tls: true default: true
            username: cisco default:
         ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 10.89.146.112
         ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 1)
      ----------------------------------------------
         ip-address: 88.88.88.0/24
--MORE--
```

ステップ 4　ホスト設定の出力をフィルタリングして、正規表現「ip」を含めます。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# show settings | include ip
      host-ip: 10.89.149.185/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
sensor(config-hos)#
```

論理ファイルの内容の表示

論理ファイル（現在のシステム コンフィギュレーションや保存されているバックアップ システム コンフィギュレーションなど）の内容を表示するには、**more** *keyword* コマンドを使用します。

次のオプションが適用されます。

- *keyword*：current-config または backup-config のどちらか。
  - **current-config**：現在の実行コンフィギュレーション。これらのコマンドが入力されると、このコンフィギュレーションは永続的になります。
  - **backup-config**：コンフィギュレーションのバックアップ ファイルの保管場所。

（注） オペレータおよびビューアは、現在のコンフィギュレーションしか表示できません。パスワードのような非表示フィールドを表示できるのは管理者だけです。

more current-config または **more backup-config** で more プロンプトをディセーブルにするには、**terminal length 0** コマンドを使用してターミナル長にゼロを設定します。これで、**more** コマンドでファイル内容全体が一時停止せずに表示されます。**terminal** コマンドの使用手順については、P.13-4 の「ターミナル プロパティの変更」を参照してください。

論理ファイルの内容を表示するには、次の手順を実行します。

ステップ 1　管理者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　現在のコンフィギュレーション ファイルの内容を表示します。

```
sensor# more current-config
Generating current config:
```

現在のコンフィギュレーションが表示されます。

```
! ------------------------------
! Version 5.1(0.7)
! Current configuration last modified Thu Jul 14 21:49:58 2005
! ------------------------------
display-serial
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
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
exit
```

```
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
user-profiles test
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 60000 0
alert-severity medium
sig-fidelity-rating 75
sig-description
sig-name My Sig
sig-string-info My Sig Info
sig-comment Sig Comment
exit
engine string-tcp
event-action produce-alert
direction to-service
regex-string My Regex String
service-ports 23
exit
event-counter
event-count 1
event-count-key Axxx
specify-alert-interval no
exit
alert-frequency
summary-mode summarize
summary-interval 15
summary-key Axxx
specify-global-summary-threshold yes
global-summary-threshold 75
exit
exit
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
sensor#
```

リモート サーバを使用したコンフィギュレーション ファイルのコピーおよび復元

コンフィギュレーション ファイルをリモート サーバにコピーするには、**copy** [**/erase**] *source-url destination-url* **keywords** コマンドを使用します。これで、リモート サーバから現在のコンフィギュレーションを復元できます。まず、現在のコンフィギュレーションをバックアップすることが求められます。

（注） アップグレードする前に、現在のコンフィギュレーション ファイルをリモート サーバにコピーすることを推奨します。

次のオプションが適用されます。

- **/erase**：コピーする前にコピー先のファイルを消去します。

  このキーワードは current-config にのみ適用されます。backup-config は常に上書きされます。このキーワードがコピー先 current-config に指定されている場合、コピー元コンフィギュレーションはシステム デフォルトのコンフィギュレーションに適用されます。コピー先 current-config に指定されていない場合、コピー元コンフィギュレーションは current-config とマージされます。
- *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。

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 プロトコルを使用する場合は、パスワードの入力が求められます。

次のキーワードは、センサー上のファイルの場所を指定するために使用されます。

- **current-config**：現在の実行コンフィギュレーション。これらのコマンドが入力されると、コンフィギュレーションは永続的になります。
- **backup-config**：コンフィギュレーションのバックアップの保管場所。

注意　センシング インターフェイスと仮想センサーが同じに設定されていない場合に、別のセンサーからコンフィギュレーション ファイルをコピーすると、エラーになることがあります。

現在のコンフィギュレーションをバックアップおよび復元するには、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 CLI にログインします。

ステップ 2　現在のコンフィギュレーションをリモート　サーバにバックアップするには、次のように入力します。

```
sensor# copy current-config ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.cfg
Password: ********
```

ステップ 3　リモート サーバにコピーしたコンフィギュレーション ファイルを復元するには、次のように入力します。

```
sensor# copy ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable
state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 4　コンフィギュレーション ファイルをコピーする場合は **Enter** キーを押し、中止する場合は **no** と入力します。

バックアップ コンフィギュレーション ファイルの作成および使用

コンフィギュレーションを保護するには、現在のコンフィギュレーションをバックアップしてから、それを表示して保存するコンフィギュレーションであることを確認します。このコンフィギュレーションを復元する必要がある場合は、バックアップ コンフィギュレーション ファイルを現在のコンフィギュレーションとマージするか、または現在のコンフィギュレーション ファイルをバックアップ コンフィギュレーション ファイルで上書きします。

現在のコンフィギュレーションをバックアップするには、次の手順を実行します。

ステップ 1　管理者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　現在のコンフィギュレーションを保存します。

```
sensor# copy current-config backup-config
```

現在のコンフィギュレーションがバックアップ ファイルに保存されます。

ステップ 3　バックアップ コンフィギュレーション ファイルを表示します。

```
sensor# more backup-config
```

バックアップ コンフィギュレーション ファイルが表示されます。

ステップ 4　バックアップ コンフィギュレーションと現在のコンフィギュレーションをマージするか、または現在のコンフィギュレーションに上書きできます。

- バックアップ コンフィギュレーションを現在のコンフィギュレーションにマージするには、次のように入力します。

  ```
  sensor# copy backup-config current-config
  ```

- 現在のコンフィギュレーションをバックアップ コンフィギュレーションで上書きするには、次のように入力します。

  ```
  sensor# copy /erase backup-config current-config
  ```

コンフィギュレーション ファイルの消去

論理ファイルを削除するには、**erase** [**backup-config** | **current-config**] コマンドを使用します。

次のオプションが適用されます。

- **current-config**：現在の実行コンフィギュレーション。これらのコマンドが入力されると、コンフィギュレーションは永続的になります。
- **backup-config**：コンフィギュレーションのバックアップの保管場所。

現在のコンフィギュレーションを消去してすべての設定をデフォルトに戻すには、次の手順を実行します。

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

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset
to default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no
username" command.
Continue? []:
```

ステップ 2　続行する場合は **Enter** キーを押し、中止する場合は **no** と入力します。

センサーの管理タスク

この章では、センサーの管理面で役立つ手順について説明します。この章は、次の項で構成されています。

- バナー ログインの作成（P.13-2）
- CLI セッションの終了（P.13-3）
- ターミナル プロパティの変更（P.13-4）
- イベント（P.13-5）
- システム クロック（P.13-9）
- 拒否された攻撃者のリストのクリア（P.13-11）
- 統計情報の表示（P.13-13）
- テクニカル サポート情報の表示（P.13-22）
- バージョン情報の表示（P.13-23）
- シリアル接続への出力の転送（P.13-25）
- ネットワーク接続性の診断（P.13-26）
- アプライアンスのリセット（P.13-27）
- コマンド履歴の表示（P.13-28）
- ハードウェア インベントリの表示（P.13-29）
- IP パケットのルートのトレース（P.13-30）
- サブモード設定の表示（P.13-31）

バナー ログインの作成

ユーザおよびパスワードのログイン プロンプトの前に表示されるバナー ログインを作成するには、**banner login** コマンドを使用します。メッセージの最大長は 2500 文字です。バナーを削除するには、**no banner login** コマンドを使用します。

バナー ログインを作成するには、次の手順を実行します。

ステップ 1　管理者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　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
```

ステップ 3　バナー ログインを作成します。

```
sensor(config)# banner login
Banner[]:
```

ステップ 4　メッセージを入力します。

```
Banner[]: This message will be displayed on banner login. ^M Thank you
sensor(config)#
```

(注)　メッセージに ? または復帰を使用するには、**Ctrl+V+?** キーまたは **Ctrl+V+Enter** キーを押します。これらの記号は ^M で表されます。

完成したバナー ログインの例を次に示します。

```
This message will be displayed on login.
Thank you
login: cisco
Password:****
```

ステップ 5　バナー ログインを削除するには、次のように入力します。

```
sensor(config)# no banner login
```

バナーがログイン時に表示されなくなります。

CLI セッションの終了

別の CLI セッションを終了するには、**clear line** *cli-id* [**message**] コマンドを使用します。**message** キーワードを使用すると、受信ユーザに終了要求とともにメッセージを送信できます。メッセージの最大長は 2500 文字です。

次のオプションが適用されます。

- *cli-id*：ログイン セッションに関連付けられている CLI ID 番号。CLI ID 番号を見つけるには、**show users** コマンドを使用します。
- **message**：受信ユーザに送信するメッセージ。

注意　**clear line** コマンドでは、CLI ログイン セッションしかクリアできません。このコマンドでは、サービス ログインはクリアできません。

管理者がログインしようとしたときに最大セッション数に達していたときは、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, would you like to
terminate one of the open sessions? [no]
```

オペレータまたはビューアがログインしようとしたときに最大セッション数がオープンしていたときは、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

CLI セッションを終了するには、次の手順を実行します。

ステップ 1　管理者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　ログイン セッションに関連付けられている CLI ID 番号を見つけます。

```
sensor# show users
    CLI ID   User    Privilege
*   13533    jtaylor administrator
    15689    jsmith  operator
    20098    viewer  viewer
```

ステップ 3　jsmith の CLI セッションを終了します。

```
sensor# clear line cli_id message
Message[]:
```

例

```
sensor# clear line 15689 message
Message{}: Sorry! I need to terminate your session.
sensor#
```

ステップ 4　ユーザ jsmith は、管理者 jtaylor から次のメッセージを受信します。

```
sensor#
***
***
*** Termination request from jtaylor
***
Sorry! I need to terminate your session.
```

ターミナル プロパティの変更

ログイン セッションのターミナル プロパティを変更するには、**terminal [length]** *screen length* コマンドを使用します。*screen length* オプションを指定すると、画面に設定した行数が表示され、その後に `--more--` プロンプトが表示されるようにすることができます。値が 0 の場合、出力は一時停止しません。デフォルト値は 24 行です。

(注)　ターミナル セッションの中には、画面の行数を指定する必要のないタイプがあります。これは、一部のリモート ホストでは、指定された画面の行数が分かるためです。

ターミナル プロパティを変更するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　複数画面の出力間で一時停止しないようにするには、*screen length* 値として 0 を使用します。

```
sensor# terminal length 0
```

(注)　画面の行数は、ログイン セッション間では保存されません。

ステップ 3　10 行ごとに CLI を一時停止して、`--more--` プロンプトを表示するには、*screen length* 値として 10 を使用します。

```
sensor# terminal length 10
```

イベント

この項では、イベント ストアからイベントを表示およびクリア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。

- イベントの表示（P.13-5）
- イベント ストアからのイベントのクリア（P.13-8）

イベントの表示

イベント ストアからイベントを表示するには、**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。

  （注） ARC は、以前は Network Access Controller（NAC）と呼ばれていました。この名前の変更は、IDM および CLI for IPS 5.1 で完全には反映されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、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。待機し、イベントを表示している状態は、Ctrl+C キーを押して終了するまで継続します。

イベント ストアから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 ストアからのイベントのクリア

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 ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者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。

システム クロック

この項では、システム クロックを表示および手動で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。

- システム クロックの表示（P.13-9）
- 手動によるクロック設定（P.13-10）

システム クロックの表示

システム クロックを表示するには、**show clock** [**detail**] コマンドを使用します。**detail** オプションを使用して、クロック ソース（NTP またはシステム）と現在のサマータイム設定（ある場合）を示すことができます。

システム クロックは、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックが NTP などの時刻源によって設定されている場合は、フラグが設定されます。

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

システム クロックを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
sensor# show clock
22:39:21 UTC Sat Jan 25 2003
```

ステップ 3　システム クロックを詳細に表示します。

```
sensor# show clock detail
22:39:21 CST Sat Jan 25 2003
Time source is NTP
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、センサーが NTP から時間を取得していることと、設定および同期されていることを示しています。

```
sensor# show clock detail
*12:19:22 CST Sat Dec 04 2004
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、時刻源が設定されていないことを示しています。

手動によるクロック設定

アプライアンスのクロックを手動で設定するには、**clock set** *hh:mm [:ss] month day year* コマンドを使用します。その他の時刻源を使用できない場合は、このコマンドを使用します。

(注) センサーが NTP クロック ソースなど有効な外部の時刻メカニズムと同期している場合、システム クロックを設定する必要はありません。

NTP の設定手順については、P.4-32 の「NTP の設定」を参照してください。センサーに有効な時刻源が必要であることの重要性の説明については、P.4-22 の「時刻源およびセンサー」を参照してください。クロックを誤って設定した場合の処置の説明については、P.4-24 の「センサー上の時刻の修正」を参照してください。

clock set コマンドは、次のプラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- AIP SSM 10
- AIP SSM 20

クロックをアプライアンスに手動で設定するには、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 CLI にログインします。

ステップ 2　クロックを手動で設定します。

```
sensor# clock set 13:21 July 29 2004
```

(注) 時刻形式は 24 時間です。

拒否された攻撃者のリストのクリア

拒否された攻撃者のリストを削除して、仮想センサーの統計情報をクリアするには、サービス イベント アクション ルール サブモードで **clear denied-attackers** コマンドを使用します。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。シグニチャを設定すると、インライン モードでパケット、接続、および攻撃者を拒否することができます。これは、センサーが単一パケット、接続、および特定の攻撃者を検出したときにそれらを拒否する、つまり送信しないことを意味します。

シグニチャが起動すると、攻撃者は拒否され、リストに入れられます。センサー管理の一環として、リストの削除やリスト内の統計情報のクリアを実行することもできます。

拒否された攻撃者のリストを削除して、統計情報をクリアするには、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　拒否された IP アドレスのリストを表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

今回 2 つの IP アドレスが拒否されたことが統計情報に示されています。

ステップ 3　拒否された攻撃者のリストを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of
attackers currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力してリストをクリアします。

ステップ 5　リストをクリアしたことを確認します。

```
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 = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

`Denied Attackers and hit count for each` カテゴリの下には情報がなくなりました。

ステップ 6　統計情報だけをクリアするには、次の手順を実行します。

```
sensor# show statistics virtual-sensor clear
```

ステップ 7　統計情報をクリアしたことを確認します。

```
JWK-4255# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

統計情報は、`Number of Active Denied Attackers` カテゴリおよび `Number of exec Clear commands during uptime` カテゴリを除いて、すべてクリアされました。リストがクリアされたかどうかを認識していることが重要です。

統計情報の表示

仮想センサーの統計情報を表示するには、**show statistics virtual-sensor** [**clear**] コマンドを使用します。各センサー アプリケーションごとに統計情報を生成するには、**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。

テクニカル サポート情報の表示

システム情報を画面に表示するか、または特定の URL に送信するには、**show tech-support** [**page**] [**password**] [**destination-url** *destination-url*] コマンドを使用します。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。

バージョン情報の表示

インストール済みのすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで動作中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の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。

バージョンおよび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 5.1(0.16)S185.0

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-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005

Recovery Partition Version 1.1 - 5.1(0.16)

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 5.1(0.16)S185.0

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-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005

Recovery Partition Version 1.1 - 5.1(0.16)

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** コマンドまたは **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Version 5.1(0.16)
! Current configuration last modified Wed Oct 31 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--
```

シリアル接続への出力の転送

シリアル接続にすべての出力を転送するには、**display-serial** コマンドを使用します。このコマンドを使用すると、ブート処理中でも、リモート コンソール（シリアル ポートを使用）にシステム メッセージを表示できます。この選択が有効である限り、ローカル コンソールは使用できません。出力をローカル ターミナルにリセットするには、**no display-serial** コマンドを使用します。

注意　シリアル ポートに接続している場合は、Linux が完全にブートされてシリアル接続のサポートがイネーブルになるまで、フィードバックは取得できません。

display-serial コマンドは、次の IPS プラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- IDS-4215
- IPS-4240
- IPS-4255
- AIP SSM 10
- AIP SSM 20

シリアル ポートに出力を転送するには、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　シリアル ポートへの出力を指示します。

```
sensor# configure terminal
sensor(config)# display-serial
```

デフォルトでは、出力はシリアル接続に転送されません。

ステップ 3　リセットして、ローカル コンソールへ出力するようにします。

```
sensor(config)# no display-serial
```

ネットワーク接続性の診断

基本的なネットワーク接続性を診断するには、**ping** ip-*address* [**count**] コマンドを使用します。

注意　このコマンドには、コマンド割り込みは使用できません。最後まで実行する必要があります。

基本的なネットワーク接続性を診断するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　対象のアドレスを ping します。

```
sensor# ping ip-address count
```

count は、送信するエコー要求の数です。数を指定しない場合は、要求が 4 回送信されます。範囲は 1 ～ 10,000 です。

正常な ping の例

```
sensor# ping 10.89.146.110 6
PING 10.89.146.110 (10.89.146.110): 56 data bytes
64 bytes from 10.89.146.110: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 10.89.146.110: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=5 ttl=61 time=0.2 ms

--- 10.89.146.110 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

正常でない ping の例

```
sensor# ping 172.21.172.1 3
PING 172.21.172.1 (172.21.172.1): 56 data bytes

--- 172.21.172.1 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

アプライアンスのリセット

アプライアンスで動作中のアプリケーションを適切にシャットダウンしてアプライアンスをリブートするには、**reset [powerdown]** コマンドを使用します。**powerdown** オプションを指定すると、アプライアンスの電源を切るか（可能な場合）、またはアプライアンスを、電源を切ることができる状態にしておくことができます。

（注） モジュールのリセットについては、P.15-31 の「IDSM-2 のリセット」、P.16-9 の「NM-CIDS のシャットダウン、リロード、およびリセット」、および P.14-7 の「AIP SSM のリロード、シャットダウン、リセット、および復旧」にあるそれぞれの手順を参照してください。

コマンドを実行すると、即座にシャットダウン（アプライアンスの停止）が開始されます。シャットダウンには少し時間がかかることがあり、この間に CLI コマンドにアクセスできますが、セッションは警告なしに終了します。

アプライアンスをリセットするには、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 CLI にログインします。

ステップ 2　すべてのアプリケーションを停止してアプライアンスをリブートするには、次のステップを実行します。あるいは、アプライアンスの電源を切って、ステップ 4 に進みます。

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

ステップ 3　**yes** を入力してリセットを続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

ステップ 4　すべてのアプライアンスを停止して、アプライアンスの電源を切るには、次のように入力します。

```
sensor# reset powerdown
Warning: Executing this command will stop all applications and power off the node if
possible. If the node can not be powered off it will be left in a state that is safe
to manually power down.
Continue with reset? []:
```

ステップ 5　**yes** を入力して、リセットおよび電源切断を続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

コマンド履歴の表示

現在のメニューに入力したコマンドのリストを表示するには、**show history** コマンドを使用します。リスト内の最大コマンド数は 50 です。

最近使用したコマンドのリストを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　EXEC モードで使用したコマンドの履歴を表示します。

```
sensor# show history
clear line
configure terminal
show history
```

ステップ 3　ネットワーク アクセス モードで使用したコマンドの履歴を表示します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show history
show settings
show settings terse
show settings | include profile-name|ip-address
exit
show history
sensor (config-net)#
```

ハードウェア インベントリの表示

PEP 情報を表示するには、**show inventory** コマンドを使用します。このコマンドは、センサーの PID、VID、および SN から構成される UDI 情報を表示します。

PEP 情報によって、CLI を使用してハードウェア バージョンおよびシリアル番号を容易に知ることができるようになります。

show inventory コマンドは、次のプラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- IDS-4210
- IDS-4215
- IDS-4235
- IDS-4250

PEP 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　PEP 情報を表示します。

```
sensor# show inventory

Name: "Chassis", DESCR: "IPS 4255 Intrusion Prevention Sensor"
PID: IPS-4255-K9, VID: V01 , SN: JAB0815R017

Name: "Power Supply", DESCR: ""
PID: ASA-180W-PWR-AC, VID: V01 , SN: 123456789AB
sensor#

sensor# show inventory

Name: "Module", DESCR: "ASA 5500 Series Security Services Module-20"
PID: ASA-SSM-20, VID: V01 , SN: JAB0815R036
sensor#

sensor-4240# show inventory

Name: "Chassis", DESCR: "IPS 4240 Appliance Sensor"
PID: IPS-4240-K9, VID: V01 , SN: P3000000653
sensor-4240#
```

TAC とやり取りする際に、この情報が使用できます。

IP パケットのルートのトレース

宛先までの IP パケットのルートを表示するには、**trace** *ip_address count* コマンドを使用します。*ip_address* オプションは、ルートをトレースする宛先のシステムのアドレスです。*count* オプションに、使用するホップ数を定義できます。デフォルトは 4 です。有効な値は 1 ～ 256 です。

注意　このコマンドには、コマンド割り込みは使用できません。最後まで実行する必要があります。

IP パケットのルートをトレースするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　対象の IP パケットのルートを表示します。

```
sensor# trace 10.1.1.1
traceroute to 10.1.1.1 (10.1.1.1), 4 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.267 ms  0.262 ms  0.236 ms
 2  10.89.128.17 (10.89.128.17)  0.24 ms *  0.399 ms
 3  * 10.89.128.17 (10.89.128.17)  0.424 ms *
 4  10.89.128.17 (10.89.128.17)  0.408 ms *  0.406 ms
sensor#
```

ステップ 3　ルートでデフォルトの 4 より多くのホップを使用するようにするには、*count* オプションを使用します。

```
sensor# trace 10.1.1.1 8
traceroute to 10.1.1.1 (10.1.1.1), 8 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.35 ms  0.261 ms  0.238 ms
 2  10.89.128.17 (10.89.128.17)  0.36 ms *  0.344 ms
 3  * 10.89.128.17 (10.89.128.17)  0.465 ms *
 4  10.89.128.17 (10.89.128.17)  0.319 ms *  0.442 ms
 5  * 10.89.128.17 (10.89.128.17)  0.304 ms *
 6  10.89.128.17 (10.89.128.17)  0.527 ms *  0.402 ms
 7  * 10.89.128.17 (10.89.128.17)  0.39 ms *
 8  10.89.128.17 (10.89.128.17)  0.37 ms *  0.486 ms
sensor#
```

サブモード設定の表示

現在のコンフィギュレーションの内容を表示するには、サブモードで **show settings** [**terse**] コマンドを使用します。

サブモードの現在のコンフィギュレーション設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC サブモードの現在のコンフィギュレーションを表示します。

```
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 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ----------------------------------------------
      profile-name: 2admin
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      ----------------------------------------------
      profile-name: r7200
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ----------------------------------------------
      profile-name: insidePix
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      ----------------------------------------------
      profile-name: qatest
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      ----------------------------------------------
```

```
   profile-name: fwsm
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ----------------------------------------------
   profile-name: outsidePix
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ----------------------------------------------
   profile-name: cat
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username:  <defaulted>
   ----------------------------------------------
   profile-name: rcat
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ----------------------------------------------
   profile-name: nopass
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username:  <defaulted>
   ----------------------------------------------
   profile-name: test
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ----------------------------------------------
   profile-name: sshswitch
   ----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ----------------------------------------------
-----------------------------------------------
cat6k-devices (min: 0, max: 250, current: 1)
-----------------------------------------------
   ip-address: 10.89.147.61
   ----------------------------------------------
      communication: telnet default: ssh-3des
      nat-address: 0.0.0.0 <defaulted>
      profile-name: cat
      block-vlans (min: 0, max: 100, current: 1)
      ----------------------------------------------
         vlan: 1
         ----------------------------------------------
            pre-vacl-name:  <defaulted>
            post-vacl-name:  <defaulted>
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
-----------------------------------------------
router-devices (min: 0, max: 250, current: 1)
-----------------------------------------------
   ip-address: 10.89.147.54
   ----------------------------------------------
      communication: telnet default: ssh-3des
      nat-address: 0.0.0.0 <defaulted>
      profile-name: r7200
      block-interfaces (min: 0, max: 100, current: 1)
      ----------------------------------------------
```

```
            interface-name: fa0/0
            direction: in
            ----------------------------------------------
               pre-acl-name:  <defaulted>
               post-acl-name:  <defaulted>
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ----------------------------------------------
      ip-address: 10.89.147.10
      ----------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: insidePix
      ----------------------------------------------
      ip-address: 10.89.147.82
      ----------------------------------------------
         communication: ssh-3des <defaulted>
         nat-address: 0.0.0.0 <defaulted>
         profile-name: f1
      ----------------------------------------------
   ----------------------------------------------
sensor (config-net)#
```

ステップ 3　ARC 設定を簡略モードで表示します。

```
sensor(config-net)# show settings terse
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ----------------------------------------------
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
```

```
   ----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   ----------------------------------------------
      ip-address: 10.89.147.61
   ----------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ----------------------------------------------
      ip-address: 10.89.147.54
   ----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ----------------------------------------------
      ip-address: 10.89.147.10
      ip-address: 10.89.147.82
   ----------------------------------------------
sensor(config-net)#
```

ステップ 4　**include**　キーワードを使用すると、フィルタリングされた出力で設定が表示できます。たとえば、ARC コンフィギュレーション内のプロファイル名および IP アドレスのみが表示できます。

```
sensor(config-net)# show settings | include profile-name|ip-address
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
      ip-address: 10.89.147.61
         profile-name: cat
      ip-address: 10.89.147.54
         profile-name: r7200
      ip-address: 10.89.147.10
         profile-name: insidePix
      ip-address: 10.89.147.82
         profile-name: test
sensor(config-net)#
```

AIP SSM コンフィギュレーション タスク

この章では、AIP SSM の設定に固有の手順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。

- コンフィギュレーション シーケンス（P.14-2）
- AIP SSM 初期化の確認（P.14-3）
- AIP SSM へのトラフィックの送信（P.14-4）
- AIP SSM のリロード、シャットダウン、リセット、および復旧（P.14-7）

コンフィギュレーション シーケンス

AIP SSM を設定するには、次のタスクを実行します。

1. AIP SSM にログインします。

   手順については、P.2-9 の「AIP SSM へのログイン」を参照してください。

2. AIP SSM を初期化します。

   setup コマンドを実行して、AIP SSM を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

3. AIP SSM 初期化を確認します。

   手順については、P.14-3 の「AIP SSM 初期化の確認」を参照してください。

4. IPS トラフィックを AIP SSM に送信するように ASA を設定します。

   手順については、P.14-4 の「AIP SSM へのトラフィックの送信」を参照してください。

5. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

6. 侵入防御を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 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。

7. 各種タスクを実行して、AIP SSM が円滑に動作し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」を参照してください。

8. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、第 18 章「ソフトウェアの入手方法」を参照してください。

9. 必要に応じて、AIP SSM のイメージを再作成します。

   手順については、P.17-44 の「AIP SSM システム イメージのインストール」を参照してください。

AIP SSM 初期化の確認

show module *slot* **details** コマンドを使用すると、AIP SSM を初期化したことと、正しいソフトウェア バージョンを使用していることが確認できます。

初期化を確認するには、次の手順を実行します。

ステップ 1　ASA にログインします。

ステップ 2　AIP SSM の詳細を取得します。

```
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(0.05)S179.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   false
asa#
```

ステップ 3　情報を確認します。修正が必要な場合は、P.14-2 の「コンフィギュレーション シーケンス」を参照してください。

AIP SSM へのトラフィックの送信

この項では、AIP SSM を設定して、ASA から IPS トラフィックを受信する方法（インライン モードまたは混合モード）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.14-4）
- IPS トラフィックを AIP SSM に送信するための ASA の設定（P.14-4）

概要

ASA は、パケットが出力インターフェイスを出る直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）、および他のファイアウォール ポリシーが適用された後に、パケットを AIP SSM に転送します。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM を設定すると、インライン モードまたは混合モード、およびフェールオープン モードまたはフェールオーバー モードでトラフィックが検査できます。

ASA で、AIP SSM に転送されて、AIP SSM によって検査されるトラフィックを識別するには、次の手順を実行します。

1. **class-map** コマンドを使用して、IPS トラフィック クラスを定義します。
2. **policy-map** コマンドを使用して、トラフィック クラスを 1 つまたは複数のアクションに関連付けることよって IPS ポリシー マップを作成します。
3. **service-policy** コマンドを使用して、ポリシー マップを 1 つまたは複数のインターフェイスに関連付けることによって IPS セキュリティ ポリシーを作成します。

   IPS トラフィック検査を設定するには、ASA CLI または ASDM が使用できます。

IPS トラフィックを AIP SSM に送信するための ASA の設定

（注） このためのコマンドの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の第 18 章「Using Modular Policy Framework」を参照してください。

次のオプションが適用されます。

- **access-list** *word*：アクセス コントロール要素を設定します。*word* はアクセス リスト識別子です（最大 241 文字）。
- **access-group** *word*：access-list をインターフェイスにバインドしてトラフィックをフィルタリングします。*word* はアクセス リスト識別子です（最大 241 文字）。
- **class-map** *class_map_name*：IPS トラフィック クラスを定義します。
- **match**：トラフィック クラスに含まれるトラフィックを定義します。

  トラフィック クラス マップには、**match** コマンドが含まれます。パケットをクラス マップと照合してマッチングをとる場合、マッチング結果は一致または不一致です。

  — **access-list**：アクセス リストのマッチングをとります。

  — **any**：すべてのパケットのマッチングをとります。
- **policy-map** *policy_map_name*：トラフィック クラスを 1 つまたは複数のアクションに関連付けることよって IPS ポリシー マップを作成します。
- **ips [inline | promiscuous][fail-close | fail-open]**：トラフィックを AIP SSM に割り当てます。

  — **inline**：AIP SSM をトラフィック フローに直接置きます。

トラフィックは、まず AIP SSM を通過し、これによって検査されないと ASA を通過し続けることができません。このモードは、すべてのパケットが分析された後に通過を許可されるので、最も安全です。また AIP SSM は、パケットごとにブロッキング ポリシーを実装することもできます。ただし、このモードはスループットに影響を及ぼすことがあります。

- **promiscuous**：トラフィックの重複したストリームを AIP SSM に送信します。

  このモードは安全性は低くなりますが、トラフィックのスループットにはほとんど影響を及ぼしません。インライン モードとは異なり、AIP SSM がトラフィックをブロックできるのは、ASA にトラフィックをブロックするように指示した場合、または ASA 上の接続をリセットした場合だけです。さらに、AIP SSM がトラフィックを分析している間に、AIP SSM がブロックする前に少量のトラフィックが ASA を通過する場合があります。

- **fail-close**：AIP SSM が使用不能の場合は、すべてのトラフィックをブロックするように ASA を設定します。
- **fail-open**：AIP SSM が使用不能の場合は、検査しないで、すべてのトラフィックの通過を許可するように ASA を設定します。

• **service-policy** *service_policy_name* [**global** | **interface** *interface_name*]：ポリシー マップを 1 つまたは複数のインターフェイスに関連付けることによって IPS セキュリティ ポリシーを作成します。

- **global**：ポリシー マップをすべてのインターフェイスに適用します。

  1 つのグローバル ポリシーのみが許可されます。インターフェイス上のグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで無効にできます。各インターフェイスには 1 つのポリシー マップしか適用できません。

- **interface**：1 つのインターフェイスにポリシーを適用します。

ASA から AIP SSM にトラフィックを送信して IPS が検査できるようにするには、次の手順を実行します。

ステップ 1　ASA 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。

```
asa# configure terminal
```

ステップ 3　IPS アクセス リストを作成します。

```
asa(config)# access-list IPS permit ip any any
```

ステップ 4　アクセス リストをインターフェイスおよびトラフィック方向に適用するには、アクセス グループを使用します。

```
asa(config)# access-group IPS [in|out] interface [DMZ|inside|mgmt|outside]
```

ステップ 5　IPS トラフィック クラスを定義します。

```
asa(config)# class-map class_map_name
asa(config-cmap)# match [access-list | any]
```

ステップ 6　IPS ポリシー マップを定義します。

```
asa(config-cmap)# policy-map policy_map_name
```

ステップ 7　アクションを割り当てる、ステップ 5 からのクラス マップを指定します。

```
asa(config-pmap)# class class_map_name
```

ステップ 8　トラフィックを AIP SSM に割り当てます。

```
asa(config-pmap-c)# ips [inline | promiscuous] [fail-close | fail-open]
```

ステップ 9　IPS サービス ポリシーを定義します。

```
asa(config-pmap-c)# service-policy policymap_name [global | interface interface_name]
```

ステップ 10　設定を確認します。

```
asa(config-pmap-c)# show running-config
!
class-map my_ips_class
class-map my-ips-class
 match access-list IPS
class-map all_traffic
 match access-list all_traffic
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map my-ids-policy
 class my-ips-class
  ips promiscuous fail-close
!
service-policy my-ids-policy global
```

ステップ 11　コンフィギュレーションを終了して保存します。

```
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)# exit
asa#
```

次の例は、すべての IP トラフィックを混合モードで AIP SSM に転送し、何らかの理由で AIP SSM に障害が発生したらすべての IP トラフィックをブロックします。

```
hostname(config)# access-list IPS permit ip any any
asa(config)# access-group IPS in interface inside
asa(config)# access-group IPS in interface outside
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ids-policy global
```

AIP SSM のリロード、シャットダウン、リセット、および復旧

ASA から AIP SSM を直接、リロード、シャットダウン、リセット、および復旧するには、次のコマンドを使用します。

（注）

hw-module コマンドは、特権 EXEC モードまたはグローバル コンフィギュレーション モードで入力できます。このコマンドは、シングル ルーテッド モードおよびシングル透過モードで入力できます。マルチモード（ルーテッド マルチモードまたは透過マルチモード）で動作する適応型セキュリティ デバイスの場合は、**hw-module** コマンドは、（管理者コンテキストやユーザ コンテキストからではなく）システム コンテキストから実行できるだけです。

- **hw-module module 1 reload**

  このコマンドは、ハードウェアをリセットせずに、AIP SSM にソフトウェアをリロードします。AIP SSM が Up 状態の場合にのみ有効です。

- **hw-module module 1 shutdown**

  このコマンドは、AIP SSM 上のソフトウェアをシャットダウンします。AIP SSM が Up 状態の場合にのみ有効です。

- **hw-module module 1 reset**

  このコマンドは、AIP SSM のハードウェア リセットを実行します。カードが Up/Down/Unresponsive/Recover 状態の場合に適用できます。

- **hw-module module 1 recover [boot | stop | configure]**

  recover コマンドは、復旧パラメータの設定用または変更用の対話型オプション セットを表示します。パラメータを変更することも Enter キーを押して既存の設定を保持することもできます。

  AIP SSM の復旧の手順については、P.17-44 の「AIP SSM システム イメージのインストール」を参照してください。

  — **hw-module module 1 recover boot**

    このコマンドは、AIP SSM の復旧を開始します。AIP SSM が Up 状態の場合にのみ適用できます。

  — **hw-module module 1 recover stop**

    このコマンドは、AIP SSM の復旧を停止します。AIP SSM が Recover 状態の場合にのみ適用できます。

注意

AIP SSM 復旧を停止する必要がある場合は、**hw-module module 1 recover stop** コマンドを AIP SSM 復旧の開始後 30 ～ 45 秒以内に発行する必要があります。これ以上待つと、予期しない結果となる場合があります。たとえば、AIP SSM が Unresponsive 状態になることがあります。

  — **hw-module module 1 recover configure**

    このコマンドは、モジュール復旧のためのパラメータを設定する場合に使用します。不可欠なパラメータは、IP アドレスと復旧イメージ TFTP URL の場所です。

IDSM-2 の設定

この章では、IDSM-2 の設定に固有の手順について説明します。

(注) Catalyst 6500 シリーズ スイッチは、6500 シリーズ スイッチおよび 7600 シリーズ ルータの両方を指す一般名として使用されます。

この章は、次の項で構成されています。

- コンフィギュレーション シーケンス（P.15-2）
- IDSM-2 取り付けの確認（P.15-3）
- サポートされている IDSM-2 の設定（P.15-5）
- IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定（P.15-6）
- IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定（P.15-9）
- IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定（P.15-21）
- IDSM-2 の管理タスク（P.15-30）
- Catalyst および Cisco IOS ソフトウェアのコマンド（P.15-33）

コンフィギュレーション シーケンス

IDSM-2 を設定するには、次のタスクを実行します。

1. IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定します。

   手順については、P.15-6 の「IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定」を参照してください。

2. IDSM-2 にログインします。

   IDSM-2 に対してセッションを開始する手順については、P.2-6 の「IDSM-2 へのログイン」を参照してください。

3. IDSM-2 を初期化します。

   setup コマンドを実行して、IDSM-2 を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

4. トラフィックを取り込んで侵入分析を行うように IDSM-2 を設定します。

   手順については、P.15-9 の「IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定」および P.15-21 の「IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定」を参照してください。混合モードまたはインライン モードで実行するように IDSM-2 を設定する手順については、第 5 章「インターフェイスの設定」を参照してください。TCP リセット インターフェイスの詳細については、P.15-9 の「TCP リセット インターフェイスの使用方法」を参照してください。Cisco IOS ソフトウェアを使用して IDSM-2 のロード バランスを設定するための手順については、P.15-25 の「EtherChanneling の設定」を参照してください。

5. サービス アカウントを作成します。

   手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

6. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

7. 侵入防御を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 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。

8. 各種タスクを実行して、IDSM-2 が円滑に実行し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」および P.15-30 の「IDSM-2 の管理タスク」を参照してください。

9. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

10. 必要に応じて、アプリケーション パーティションとメンテナンス パーティションのイメージを再作成します。

    手順については、P.17-31 の「IDSM-2 システム イメージのインストール」を参照してください。

IDSM-2 取り付けの確認

スイッチが IDSM-2 を認識し、オンラインにしたことを確認します。

取り付けを確認するには、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　Catalyst ソフトウェアの場合、次のように入力します。

```
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)
```

ステップ 3　Cisco IOS ソフトウェアの場合、次のように入力します。

```
switch# 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
  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
 10    3  Anomaly Detector Module                WS-SVC-ADM-1-K9    SAD084104JR
 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
  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
 10  000b.fcf8.2ca8 to 000b.fcf8.2caf   0.101 7.2(1)        4.0(0.25)    Ok
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)     5.0(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
--- --------------------------- ------------------ ------------ ------- -------
  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
  6 Pass
  7 Pass
  9 Unknown
 10 Not Applicable
 11 Pass
 13 Pass
switch#
```

（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。

IDSM-2 の取り付け確認後、全メモリ テストをイネーブルにするための詳細については、P.15-30 の「全メモリ テストのイネーブル化」を参照してください。

サポートされている IDSM-2 の設定

表 15-1 にサポートされている IDSM-2 の設定を示します。

表 15-1　サポートされている設定

スーパーバイザ	SPAN/ RSPAN	VACL キャプチャ	VACL ブロッキング	RACL ブロッキング	Catalyst ソフトウェア	Cisco IOS ソフトウェア
スーパーバイザ 1A	X	—	—	—	7.5(1)	—
PFC1 組み込みのスーパーバイザ 1A	X	X	X	—	7.5(1)	—
PFC1 または MSFC1 組み込みのスーパーバイザ 1A	X	X	X[1]	X	7.5(1)	[2]
スーパーバイザ 1A-PFC2 または MSFC2	X	X	X[3]	X	7.5(1)	12.1(19)E1
PFC2 組み込みのスーパーバイザ 2	X	X	X	—	7.5(1)	—
PFC2 または MSFC2 組み込みのスーパーバイザ 2	X	X	X[4]	X	7.5(1)	12.1(19)E、12.2(14)SY
スーパーバイザ 720（PFC3 および MSFC3 統合）	X	X	[5]	X	—	12.2(14)SX1

1. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
2. Cisco IOS は PFC1 または MSFC1 組み込みのスーパーバイザ 1A でサポートされています。しかし、IDSM-2 はこの設定ではサポートされていません。
3. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
4. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
5. Cisco IOS 組み込みのスーパーバイザ 720 は VACL の deny 文をサポートしています。しかし、IDSM-2 は、Cisco IOS 形式の VACL でブロックを実行できません。

注意　スーパーバイザ 1A と PFC2 の組み合せはサポートされていません。PFC2 または MSFC2 が組み込まれていないスーパーバイザ 2 は、Catalyst ソフトウェアや Cisco IOS ソフトウェアではサポートされていません。

IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定

IDSM-2 にコマンド / コントロール アクセスを行うように Catalyst 6500 シリーズ スイッチを設定する必要があります。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-6）
- Cisco IOS ソフトウェア（P.15-7）

Catalyst ソフトウェア

IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定するには、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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　コマンド / コントロール ポートを正しい VLAN に置きます。

```
cat6k> (enable) set vlan command_and_control_vlan_number
idsm2_slot_number/command_and_control_port_number
```

例

```
cat6k> (enable) set vlan 147 6/2
VLAN 147 modified.
VLAN 146 modified.
VLAN  Mod/Ports
---- ------------------------
147   2/5,2/16-18
      6/2
```

コマンド / コントロール ポート番号は、常に 2 です。

ステップ 4　IDSM-2 に対してセッションを開始し、ネットワーク IP アドレスを ping します。

```
cat6k> session slot_number
idsm-2# ping network_ip_address
```

例

```
console> (enable) session 6
Trying IDS-6...
Connected to IDS-6.
Escape character is '^]'.

login: cisco
Password:
Last login: Thu Mar 3 09:40:53 from 127.0.0.11
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco
cryptographic products does not imply third-party authority to import, export,
distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable to comply with
U.S. and local laws, return this product immediately.

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

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

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a
license.
idsm-2# ping 10.89.149.126
PING 10.89.149.126 (10.89.149.126): 56 data bytes
64 bytes from 10.89.149.126: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=3 ttl=255 time=0.3 ms
--- 10.89.149.126 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
idsm-2# exit
cat6k> (enable)
```

ステップ 5　IDSM-2 を初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

ステップ 6　IDSM-2 のデフォルト ルータを ping します。

ステップ 7　管理ステーションが IDSM-2 に対して ping、SSH または Telnet 接続、および Web ブラウザでの参照ができることを確認します。

Cisco IOS ソフトウェア

IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定するには、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　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　コマンド / コントロール ポートを正しい VLAN に置きます。

```
switch (config)# intrusion-detection module module_number management-port access-vlan
vlan_number
```

例

```
switch (config)# intrusion-detection module 11 management-port access-vlan 146
```

ステップ 4　IDSM-2 に対してセッションを開始し、ネットワーク IP アドレスを ping して、接続できることを確認します。

```
switch# session slot module_number processor 1
idsm-2# ping network_ip_address
```

例

```
switch# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

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

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

If you require further assistance please contact us by sending email to
export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
idsm-2# ping 10.89.149.254
PING 10.89.149.254 (10.89.149.254): 56 data bytes
64 bytes from 10.89.149.254: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=3 ttl=255 time=0.2 ms
--- 10.89.149.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
idsm-2# exit
[Connection to 127.0.0.91 closed by foreign host]
switch#
```

ステップ 5　IDSM-2 をまだ初期化していない場合は、初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定

トラフィックは、SPAN または VACL キャプチャを使用して、IDSM-2 上での混合分析のために取り込まれます。ポート 1（GigabitEthernet0/1）は TCP リセット ポートとして、ポート 2（GigabitEthernet0/2）はコマンド / コントロール ポートとして、およびポート 7 とポート 8（GigabitEthernet0/7 と GigabitEthernet0/8）はモニタリング ポートとして、それぞれ使用されます。両方のモニタリング ポートを、SPAN 宛先ポートまたは VACL キャプチャ ポートのいずれかとして設定できます。

注意　両方のポートをモニタリング ポートに設定する場合は、必ずこれらのポートが別のトラフィックを監視するように設定してください。

注意　IDSM-2 はトラフィックを受信しないので、IDSM-2 データ ポートを SPAN 宛先ポートと VACL キャプチャ ポートの両方として設定しないでください。このデュアル コンフィギュレーション（SPAN および VACL）を行うと、スイッチで問題が発生し、トラフィックが適切に送信されなくなります。

この項では、次のトピックについて説明します。

- TCP リセット インターフェイスの使用方法（P.15-9）
- SPAN の設定（P.15-10）
- VACL の設定（P.15-14）
- mls ip ids コマンドの設定（P.15-18）

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、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、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。

SPAN の設定

IDSM-2 はイーサネットまたはファースト イーサネット SPAN ソース ポートからのイーサネット VLAN トラフィックを分析できます。つまり、イーサネット VLAN を SPAN ソースとして指定できます。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-10）
- Cisco IOS ソフトウェア（P.15-12）

Catalyst ソフトウェア

IDSM-2 に対して SPAN をイネーブルにするには、特権モードで **set span** コマンドを使用します。

（注） IDSM-2 ポート番号は、7 または 8 に限られます。

次のオプションが適用されます。

- **disable**：ポート モニタリングをディセーブルにします。
- *module/port*：送信元モジュール番号およびポート番号。
- *vlan*：送信元 VLAN 番号。
- *module/port*：宛先モジュール番号およびポート番号。
- **both**：トラフィックの受信および転送の両方。
- **filter**：VLAN にフィルタを適用します。
- **inpkts**：宛先ポートへのパケット着信をイネーブル / ディセーブルにします。
- **learning**：MAC アドレス ラーニングをイネーブル / ディセーブルにします。
- **multicast**：マルチキャスト トラフィックをイネーブル / ディセーブルにします。
- **rx**：トラフィックの受信。
- **session**：SPAN セッションのセッション番号。
- **tx**：トラフィックの送信。

IDSM-2 上の SPAN 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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　IDSM-2 に対して SPAN をイネーブルにします。

- 送信元ポートから

```
cat6k> (enable) set span 3/3 13/7
Destination     : Port 13/7
Admin Source    : Port 3/3
Oper Source     : Port 3/3
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -

Session Number  : 1

cat6k> (enable)
```

（注） 送信元トランク ポートで特定の VLAN のトラフィックを監視するには、**filter** キーワードを使用します。

- VLAN から

```
cat6k> (enable) set span 650 13/7 rx

Destination : Port 13/7
Admin Source : VLAN 650
Oper Source : Port 11/1,13/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -

Session Number : 1

cat6k> (enable)
```

ステップ 4　SPAN セッションを表示します。

```
cat6k> (enable) show span

Destination     : Port 13/7
Admin Source    : VLAN 650
Oper Source     : Port 11/1,13/1
Direction       : receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -

Session Number  : 1

Total local span sessions:  1
cat6k> (enable)
```

ステップ 5　IDSM-2 にトラフィックを送信している SPAN セッションをディセーブルにするには、次のように入力します。

```
cat6k> (enable) set span disable session 1
This command will disable your span session.
Do you want to continue (y/n) [n]? y
Disabled Port 13/7 to monitor receive traffic of VLAN 650
cat6k> (enable)
```

（注）　SPAN の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

Cisco IOS ソフトウェア

IDSM-2 上で SPAN をイネーブルにするには、グローバル コンフィギュレーション モードで **monitor session** コマンドを使用します。

（注）　IDSM-2 データ ポート番号には、1 または 2 を使用します。

次のオプションが適用されます。

- **interface**：SPAN 送信元インターフェイス
- **remote**：SPAN 送信元リモート
- **vlan**：SPAN 送信元 VLAN
- **GigabitEthernet**：ギガビット イーサネット IEEE 802.3z
- **Port-channel**：インターフェイスのイーサネット チャネル
- **,**：インターフェイスの別の範囲を指定
- **--**：インターフェイスの範囲を指定
- **both**：受信および送信トラフィックを監視
- **rx**：受信トラフィックのみを監視
- **tx**：送信トラフィックのみを監視
- **intrusion-detection-module**：SPAN 宛先侵入検出モジュール
- **destination**：SPAN 宛先インターフェイスまたは VLAN
- **filter**：SPAN フィルタ VLAN
- **source**：SPAN 送信元インターフェイス、VLAN
- **type**：モニタ セッションのタイプ

IDSM-2 上の SPAN 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　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　モニタ セッションの送信元インターフェイスを設定します。

```
switch (config)# monitor session (session_number) source interface
interface/port_number [, | - | rx | tx | both]
```

例

```
switch (config)# monitor session 1 source interface GigabitEthernet2/23 both
```

ステップ 4　IDSM-2 データ ポートを SPAN 宛先としてイネーブルにします。

```
switch (config)# monitor session (session_number) destination
intrusion-detection-module module_number data-port data_port_number
```

例

```
switch (config)# monitor session 1 destination intrusion-detection-module 9 data-port
1
```

ステップ 5　（オプション）モニタ セッションをディセーブルにするには、次のように入力します。

```
switch (config)# no monitor session session_number
```

ステップ 6　（オプション）スイッチ ポート トランクから特定の VLAN のみが見えるように SPAN セッションをフィルタリングするには、次のように入力します。

```
switch (config)# monitor session (session_number) {filter vlan {vlan_ID} [, | - ]}
```

例

```
switch (config)# monitor session 1 filter vlan 146
```

ステップ 7　コンフィギュレーション モードを終了します。

```
switch (config)# exit
```

ステップ 8　現在のモニタ セッションを表示するには、次のように入力します。

```
switch # show monitor session session_number
```

例

```
switch # show monitor session 1
    Session 1
    ---------
    Type                    : Local Session
    Source Ports            :
        Both                : Gi2/23
    Destination Ports       : intrusion-detection-module 9 data-port 1
```

（注）SPAN の詳細については、『*Catalyst 6500 Series Cisco IOS Command Reference*』を参照してください。

VACL の設定

Cisco IOS ソフトウェアを使用している場合、1 つの VLAN または複数の VLAN から、あるいは 7600 ルータの FLexWAN2 ポートから IPS 用のトラフィックを取り込むように VACL を設定できます。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-14）
- Cisco IOS ソフトウェア（P.15-16）

Catalyst ソフトウェア

（注）ポート 1 は、TCP リセット ポートとして設定されます。ポート 7 および 8 は、センシング ポートで、セキュリティ ACL キャプチャ ポートとして設定できます。Catalyst Software 8.4(1) 以前のリリースでは、デフォルトで、ポート 7 および 8 はトランク ポートとして設定され、セキュリティ ACL にキャプチャ機能が適用されたすべての VLAN にトランク接続します。特定の VLAN からのトラフィックだけを監視する場合は、監視しない VLAN をクリアして、ポート 7 および 8 にトランク接続されないようにする必要があります。

セキュリティ ACL キャプチャ ポートを設定するには、**set security acl** コマンドを使用します。

次のオプションが適用されます。

- **ACL**：セキュリティ ACL 機能を設定します。
  - **capture-port**：ACL キャプチャ用のポートを設定します。
  - **cram**：セキュリティ ACL クラムを設定します。
  - **ip**：IP セキュリティ ACL 機能を設定します。
  - **ipx**：IPX セキュリティ ACL 機能を設定します。
  - **mac**：MAC セキュリティ ACL 機能を設定します。
  - **map**：セキュリティ ACL を VLAN マッピングに設定します。
- **permit**：転送するパケットを指定します。
- **deny**：拒否するパケットを指定します。
- **redirect**：ポートに転送するパケットを指定します。

- **before**：編集バッファ内の指定された ACE の前に ACE を挿入します。
- **capture**：このフローのコピーをキャプチャ ポートに作成します。
- **modify**：編集バッファ内の指定された ACE を変更します。

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　トラフィックを取り込むために VACL を作成します。許可、拒否、および取り込むトラフィックを指定します。

```
cat6k> (enable) set security acl ip acl_name permit ip [permit (...) | deny (...)]
capture
```

(注)　許可したトラフィックのみを取り込むことができます。トラフィックを許可するが、取り込まない場合は、**capture** キーワードを使用しないでください。

例

```
console> (enable) set security acl ip CAPTUREALL permit ip any any capture
CAPTUREALL editbuffer modified. Use 'commit' command to apply changes.
```

ステップ 4　VACL を適用します。

```
console> (enable) commit security acl CAPTUREALL
ACL commit in progress.
```

VACL を適用すると、VACL および関連 ACE が NVRAM に書き込まれます。

ステップ 5　VACL を VLAN にマッピングします。

```
console> (enable) set security acl map acl_name vlan_number
```

例

```
console> (enable) set security acl map CAPTUREALL 650
Mapping in progress.

ACL CAPTUREALL successfully mapped to VLAN 650.
```

ステップ 6　IDSM-2 ポート（ポート 7 または 8）をキャプチャ ポートとして設定します。

```
console> (enable) set security acl capture module_number/port_number
```

例

```
console> (enable) set security acl capture 2/13
Successfully set 2/13 to capture ACL traffic.
```

(注) トランク ポートおよび ACL の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

Cisco IOS ソフトウェア

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、次のコマンドを使用します。

次のオプションが適用されます。

- **ip access-list**：名前付きアクセス リスト
  - **extended**：拡張アクセス リスト
  - **hardware**：ハードウェア フラグメント処理のイネーブル化
  - **log-update**：アクセス リスト ログのアップデートの制御
  - **logging**：アクセス リストのロギングの制御
  - **resequence**：アクセス リストの再シーケンス
  - **standard**：標準アクセス リスト

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、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　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　ACL を定義します。

```
switch (config)# ip access-list [standard | extended] acl_name
```

例

```
switch(config)# ip access-list standard CAPTUREALL
switch(config-std-nacl)# exit
```

ステップ 4　VLAN アクセス マップを定義します。

```
switch(config)# vlan access-map map_name [0-65535]
```

ステップ 5　VLAN アクセス マップ シーケンスに match 句を設定します。

```
switch (config-access-map)# match [ip address {1-199 | 1300-2699 | acl_name}]
```

ステップ 6　VLAN アクセス マップ シーケンスに action 句を設定して、先行する match 句に付加します。

```
switch(config-access-map)# action forward capture
```

ステップ 7　VLAN アクセス マップを指定された VLAN に適用します。

```
switch (config)# vlan filter map_name vlan-list vlan_list
```

ステップ 8　取り込まれたフラグ付きトラフィックを取り込むように IDSM-2 データ ポートを設定します。

```
switch (config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```

(注)　スイッチでトラフィックをルーティングしている場合は、ルーティングされる VLAN すべてを監視するように IDSM-2 を設定します。VACL を FlexWan2 ポートに適用する場合は、すべての VLAN を監視するように IDSM-2 を設定する必要があります。

ステップ 9　IDSM-2 上のキャプチャ機能をイネーブルにします。

```
switch (config)# intrusion-detection module module_number data-port data_port_number
capture
```

次の例は、**show run** コマンドの出力を示します。

```
switch# show run
intrusion-detection module 4 data-port 1 capture allowed-vlan 450,1002-1005
intrusion-detection module 4 data-port 1 capture
.
.
.
vlan access-map CAPTUREALL 10
match ip address MATCHALL
action forward capture
.
.
.
ip access-list extended MATCHALL
permit ip any any
switch#
```

mls ip ids コマンドの設定

この項では、**mls ip ids** コマンドを使用して IPS トラフィックを取り込む方法について説明します。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-18）
- Cisco IOS ソフトウェア（P.15-19）

Catalyst ソフトウェア

MSFC で Cisco IOS ファイアウォールを動作させている場合は、VACL を使用して IDSM-2 のトラフィックを取り込むことはできません。これは、Cisco IOS ファイアウォールの IP 検査ルールを適用した VLAN には VACL が適用できないからです。しかし、**mls ip ids** コマンドを使用して、取り込むパケットを指定することはできます。ACL によって許可されたパケットが取り込まれます。ACL によって拒否されたパケットは取り込まれません。permit/deny パラメータは、宛先ポートへのパケットの転送に影響を与えません。そのルータ インターフェイスに到着するパケットが IPS ACL に照らしてチェックされ、それらを取り込むかどうかが判断されます。**mls ip ids** コマンドは、スーパーバイザ コンフィギュレーションではなく、MSFC コンフィギュレーションの一部として適用されます。**mls ip ids** コマンドでは、着信トラフィックのみが取り込まれます。**mls ip ids** コマンドは、クライアント側のルータ インターフェイスとサーバ側のルータ インターフェイスの両方で使用する必要があります。これにより、接続の両方向で取り込まれるようになります。

mls ip ids コマンドを使用して IPS トラフィックを取り込むには、次の手順を実行します。

ステップ 1　MSFC にログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 4　ACL を設定して、取り込むパケットを指定します。

```
switch(config)# ip access-list extended word
```

ステップ 5　取り込んだパケットを伝送するインターフェイスを選択します。

```
switch(config)# interface interface_name
```

ステップ 6　ステップ 4 で作成した ACL を、ステップ 5 で選択したインターフェイスに適用します。

```
switch(config-if)# mls ip ids word
```

ステップ 7　スーパーバイザ エンジンにログインします。

ステップ 8　特権モードに入ります。

```
cat6k> enable
```

ステップ 9　スーパーバイザ エンジンで、IDSM-2 モニタ ポート（ポート 7 または 8）を VACL キャプチャ リストに追加します。

```
cat6k> (enable) set security acl capture module_number/port_number
```

注意　IDSM-2 が、**mls ip ids** コマンドによってマークが付けられたパケットすべてを取り込むには、IDSM-2 のポート 7 または 8 が、パケットのルーティング先の VLAN すべてのメンバーでなければなりません。

Cisco IOS ソフトウェア

ポートを、スイッチ ポートではなく、ルータ インターフェイスとして使用している場合は、VACL を適用する VLAN はありません。

mls ip ids コマンドを使用すると、取り込むパケットを指定することができます。ACL によって許可されたパケットが取り込まれます。ACL によって拒否されたパケットは取り込まれません。permit/deny パラメータは、宛先ポートへのパケットの転送に影響を与えません。そのルータ インターフェイスに到着するパケットが IPS ACL に照らしてチェックされ、それらを取り込むかどうかが判断されます。

mls ip ids コマンドを使用して IDS トラフィックを取り込むには、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　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　ACL を設定して、取り込むパケットを指定します。

```
switch(config)# ip access-list extended word
```

ステップ 4　取り込んだパケットを伝送するインターフェイスを選択します。

```
switch(config)# interface interface_name
```

ステップ 5　キャプチャ VLAN を指定します。

```
switch(config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```

例

```
switch(config)# intrusion-detection module 4 data-port 1 capture allowed-vlan 165
```

ステップ 6　ステップ 4 で作成した ACL を、ステップ 5 で選択したインターフェイスに適用します。

```
switch(config-if)# mls ip ids word
```

注意　IDSM-2 が、**mls ip ids** コマンドによってマークされたすべてのパケットを取り込むには、IDSM-2 のデータ ポート 1 または 2 が、パケットのルーティング先の VLAN すべてのメンバーでなければなりません。

IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定

IDM または CLI を使用して、2 つの離れた VLAN（IDM-2 の両側それぞれに 1 つの VLAN）の間でインライン モードで動作するように IDSM-2 を設定できます。インライン モード用の IDSM-2 を準備するには、スイッチと IDSM-2 を設定する必要があります。まずスイッチを設定して、その後インライン モード用の IDSM-2 インターフェイスを設定します。混合モードまたはインライン モードで動作するように IDSM-2 を設定するための手順については、第 5 章「インターフェイスの設定」を参照してください。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-21）
- Cisco IOS ソフトウェア（P.15-22）

Catalyst ソフトウェア

IDSM-2 モニタリング ポートを、Supervisor Engine 1a、Supervisor Engine 2、Supervisor Engine 32、または Supervisor Engine 720 を備えた Catalyst ソフトウェア 8.4(1) 以上に対するインライン動作用のトランク ポートとして設定します。ネイティブ VLAN はトランク接続される唯一の VLAN と同じであるので、トラフィックは 802.1q カプセル化されていません。

注意　IDSM-2 ポート 7 および 8 のデフォルト コンフィギュレーションでは、すべての VLAN 1 ～ 4094 をトランク接続します。IDSM-2 コンフィギュレーションをクリアすると（**clear configuration** *module_number*）、IDSM-2 はすべての VLAN をトランク接続します。IDSM-2 インターフェイスがインライン用に設定されている場合、スパニング ツリー ループが作成されてストームが発生する可能性があります。ストームとは数多くのパケットのループであり、それらのパケットが宛先に到達することはありません。

IDSM-2 上にインライン モード用のモニタリング ポートを設定するには、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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　各 IDSM-2 モニタリング ポートにネイティブ VLAN を設定します。

```
cat6k (enable)> set vlan vlan_number slot_number/port_number
```

例

```
cat6k (enable)> set vlan 651 9/7
cat6k (enable)> set vlan 652 9/8
```

ステップ 4　各 IDSM-2 モニタリング ポートからすべての VLAN をクリアします。ただし、各ポートのネイティブ VLAN（ポート 7 の場合は 651、ポート 8 の場合は 652）は除きます。

```
cat6k (enable)> clear trunk slot_number/port_number vlan_range
```

例

```
cat6k (enable)> clear trunk 9/7 1-650,652-4094
cat6k (enable)> clear trunk 9/8 1-651,653-4094
```

ステップ 5　IDSM-2 モニタリング ポートの Bpdu スパンツリー フィルタリングをイネーブルにします。

```
cat6k (enable)> set spantree bpdu-filter 6/7-8 enable
```

（注）　IPS 5.0(2) の場合は、このステップは省略します。

Cisco IOS ソフトウェア

（注）　Supervisor Engine 720 を備えた Cisco IOS ソフトウェア 12.2(18)SXE は、2 つの VLAN 間では 1 つの IDSM-2 インラインのみをサポートします。

IDSM-2 モニタリング ポートをインライン動作用のアクセス ポートとして設定します。

（注）　Etherchannelling インライン IDSM-2 は、Cisco IOS ではまだサポートされていません。

インライン VLAN を設定するには、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　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　インライン IDSM-2 のそれぞれの側に 1 つずつ、2 つの VLAN を作成します。

```
switch(config)# vlan vlan_number
switch(config)# name vlan_name
switch(config)# exit
switch# exit
```

ステップ 4　各インライン VLAN 上の各インターフェイスに IOS アクセス ポートをまだ設定していない場合は、設定します。

a. グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

b. 設定する IOS インターフェイスを選択します。

```
switch(config)# interface interface_name
```

c. インターフェイスの目的が分かるように説明を入力します。

```
switch(config-if)# description description
```

d. インターフェイスをレイヤ 2 スイッチ ポートとして設定します。

```
switch(config-if)# switchport
```

e. アクセス モード VLAN を設定します。

```
switch(config-if)# switchport access vlan vlan_number
```

f. アクセス ポートとするインターフェイス / ポートを設定します。

```
switch(config-if)# switchport mode access
```

g. グローバル コンフィギュレーション モードを終了します。

```
switch(config-if)# exit
switch# exit
```

ステップ 5　ステップ 3 で作成した 2 つの VLAN それぞれの上に 1 つの IDSM-2 データ ポートを設定します。

```
switch# configure terminal
switch(config)# intrusion-detection module slot_number data-port data_port_number
access-vlan vlan_number
switch(config)# exit
```

ステップ 6　コンフィギュレーションを確認します。

（注）　次の例では、スロット 13 の IDSM-2 は、VLAN 661 および 662 の間でインラインです。IDSM-2 データ ポート 1 は VLAN 661 上にあり、データ ポート 2 は VLAN 662 上にあります。

a. IDSM-2 侵入検出設定を確認します。

```
switch# show run | include intrusion-detection
intrusion-detection module 13 management-port access-vlan 147
intrusion-detection module 13 data-port 1 access-vlan 661
intrusion-detection module 13 data-port 2 access-vlan 662
switch#
```

b. IDSM-2 データ ポート 1 が VLAN 661 上のアクセス ポートであることを確認します。

```
switch# show intrusion-detection module slot_number data-port data_port_number
state
```

例

```
switch# show intrusion-detection module 13 data-port 1 state
Intrusion-detection module 13 data-port 1:

Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation:
native Negotiation of Trunking: Off Access Mode VLAN: 661 (inline-vlan-1) Trunking
Native Mode VLAN: 1 (default) Trunking VLANs Enabled: NONE Pruning VLANs Enabled:
2-1001 Vlans allowed on trunk:661 Vlans allowed and active in management domain:
661 Vlans in spanning tree forwarding state and not pruned: 661
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: <empty>
```

c. VLAN 番号を確認します。

```
switch# show vlan id vlan_number
```

例

```
switch# show vlan id 661
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
661  ward-attack3                     active    Gi3/2, Gi13/d1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
661  enet  100661     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
switch#
```

EtherChanneling の設定

この項では、IDSM-2 に Cisco IOS ソフトウェア用の EtherChanneling 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.15-25）
- EtherChanneling のイネーブル化（P.15-25）
- EtherChanneling のディセーブル化（P.15-28）
- EtherChanneling の確認（P.15-28）

概要

Catalyst 6500 シリーズ シャーシのスーパーバイザ エンジンは、IPS 5.0 を EtherChannel デバイスとして実行している IDSM-2 デバイスを認識します。これによって、最大 8 個の IDSM-2 デバイスを同一シャーシに取り付けることができます。

Catalyst 6500 シリーズ スイッチの IDSM-2 には、8 個の内部ポートがあります。これらのポートのうち、4 個のみが使用されます。ポート 1 は、TCP/IP リセット ポートです。ポート 2 は、コマンド / コントロール ポートです。ポート 7 および 8 は Catalyst ソフトウェア用のセンシング ポートで、データ ポート 1 および 2 は Cisco IOS ソフトウェア用です。その他のポートは使用されません。

バックプレーンは 1000 Mbps です。これが、IDSM-2 は約 600 Mbps のパフォーマンスしか処理できない場合でも、IDSM-2 が 1000 Mbps を示す理由です。EtherChannel 機能により、最大 8 台の IDSM-2 デバイスが、ポート 7 または 8 のいずれかのロード バランシングに参加できるようになります。

（注） IDSM-2 の EtherChannel ロード バランシングは、Cisco IOS ソフトウェアでのみサポートされています。Cisco Catalyst ソフトウェア用の EtherChannel ロード バランシングを IDSM-2 に設定するための手順については、これをサポートする Catalyst リリースが使用可能になるときに提供されます。

EtherChanneling のイネーブル化

（注） EtherChannel ロード バランシングを IDSM-2 に設定するには、Cisco IOS 12.2(18)SXE をインストールし、Supervisor Engine 720 を装備する必要があります。Cisco IOS は、VACL キャプチャ（SPAN でも監視でもない）を使用する混合 DSM-2 EtherChanneling のみをサポートします。

EtherChannel は、フレーム内のアドレスから形成されるバイナリ パターンの部分を、チャネル内のリンクの 1 つを選択する数値に縮小して、EtherChannel 内のリンクを越えてトラフィック ロードをバランスさせます。

EtherChannel ロード バランシングでは、MAC アドレス、IP アドレス、またはレイヤ 4 ポート番号が使用できます。アドレスまたはポートは、送信元または宛先のアドレスまたはポートでも、送信元および宛先の両方のアドレスまたはポートでもかまいません。選択されたモードがスイッチに設定されている EtherChannel すべてに適用されます。EtherChannel ロード バランシングでは、MPLS レイヤ 2 情報も使用できます。

使用しているコンフィギュレーションにおいて非常に多様なバランス基準を与えるオプションが使用できます。たとえば、EtherChannel 上のトラフィックが 1 つの MAC アドレスだけに送信され、その宛先 MAC アドレスを EtherChannel ロード バランシングの基準とする場合、EtherChannel は常にその EtherChannel 内の同じリンクを選択します。送信元アドレスまたは IP アドレスを使用すると、ロード バランシングが向上する場合があります。

EtherChanneling の詳細については、『*Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*』を参照してください。

EtherChannel ロード バランシングを IDSM-2 に設定するには、次の手順を実行します。

ステップ 1　混合動作用に各 IDSM-2 を設定します。

手順については、第 5 章「インターフェイスの設定」を参照してください。

（注）　IDSM-2 EtherChanneling を設定する前に、IDSM-2 VACL キャプチャ、あるいは SPAN またはモニタ コンフィギュレーションの行がすべて、削除されていることを確認します。

ステップ 2　コンソールにログインします。

ステップ 3　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 4　VACL を作成します。

```
switch(config)# ip access-list extended vacl_name
```

ステップ 5　任意のアクセス コントロール エントリ（たとえば、`permit any any`）を追加します。

```
switch(config-ext-nacl)# permit ip any any
```

ステップ 6　少なくとも 1 つの VLAN アクセス マップ シーケンスを作成します。

```
switch(config-ext-nacl)# vlan access-map vlan_access_map_name sequence_number
switch(config-access-map)# match ip address vacl_name
switch(config-access-map)# action forward capture
```

ステップ 7　VLAN アクセス マップを VLAN に適用します。

```
switch(config-access-map)# vlan filter vlan_access_map_name vlan-list vlan_list
```

ステップ 8　各 IDSM-2 に対して、目的のデータ ポートを目的の EtherChannel に追加します。

```
switch(config)# intrusion-detection module module_number data-port data_port_number
channel-group channel_number
```

各 EtherChannel には、番号付きのポート チャネル インターフェイスがあります。最大 64 個のポート チャネル インターフェイス（1 ～ 256 の番号を付けて）を設定できます。

ステップ 9　EtherChannel ロード バランシングを設定します。

```
switch(config)# port-channel load-balance [dst-ip | dst-mac | dst-port | mpls |
src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port]
```

次のオプションが適用されます。

- **dst-ip**：宛先 IP アドレス
- **dst-mac**：宛先 MAC アドレス
- **dst-port**：宛先 TCP/UDP ポート
- **mpls**：MPLS パケットのロード バランシング
- **src-dst-ip**：送信元および宛先 IP アドレス
- **src-dst-mac**：送信元および宛先 MAC アドレス
- **src-dst-port**：送信元および宛先 TCP/UDP ポート
- **src-ip**：送信元 IP アドレス
- **src-mac**：送信元 MAC アドレス
- **src-port**：送信元 TCP/UDP ポート

  デフォルトは **src-dst-ip** です。これは、EtherChannel が、配布方法として、送信元と宛先の IP アドレスの組み合せを使用することを意味します。

ステップ 10　ロード バランシングを確認します。

```
cat6k# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
  MPLS: Label or IP
```

ステップ 11　取り込む VLAN を EtherChannel に設定します。

```
switch(config)# intrusion-detection port-channel channel_number capture allowed-vlan
vlan_list
```

ステップ 12　EtherChannel に対してキャプチャをイネーブルにします。

```
switch(config)# intrusion-detection port-channel channel_number capture
```

ステップ 13　グローバル コンフィギュレーション モードを終了します。

```
switch(config)# exit
```

ステップ 14 変更内容を保存するには、次のように入力します。

```
switch# write memory
```

EtherChanneling のディセーブル化

IDSM-2 EtherChanneling をディセーブルにするには、次の手順を実行します。

ステップ 1 コンソールにログインします。

ステップ 2 グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3 EtherChannel から 1 つの IDSM-2 を削除するには、次のように入力します。

```
switch(config)# no intrusion-detection module module_number data-port
data_port_number channel-group channel_number
```

ステップ 4 EtherChannel 全体を削除するには、次のように入力します。

（注） IDSM-2 用の VACL キャプチャ コマンドは残ります。

```
switch(config)# no intrusion-detection module port-channel channel_number
```

EtherChanneling の確認

IDSM-2 EtherChannel 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 コンソールにログインします。

ステップ 2 すべての EtherChannel を表示するには、次のように入力します。

```
switch# show etherchannel
                Channel-group listing:
                ----------------------

Group: 10
----------
Group state = L2
Ports: 0   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:    -

cat6k#
```

ステップ 3　特定の EtherChannel のステータスを表示するには、次のように入力します。

```
switch# show etherchannel 1 [summary | detail | port | port-channel | protocol]
```

例

```
switch# show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        u - unsuitable for bundling
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------

switch#
```

ステップ 4　EtherChannel ロード バランスの設定を表示するには、次のように入力します。

```
switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip
        mpls label-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
  MPLS: Label or IP
switch#
```

ステップ 5　IDSM-2 データ ポート情報を表示するには、次のように入力します。

```
switch# show intrusion-detection module module_number data-port data_port_number state
Intrusion-detection module 11 data-port 2:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 662 (ward-victim3)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:none
Vlans allowed and active in management domain: none
Vlans in spanning tree forwarding state and not pruned:
   none
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: empty
```

IDSM-2 の管理タスク

この項では、IDSM-2 の管理タスクに役立つ手順について説明します。取り上げる事項は次のとおりです。

- 全メモリ テストのイネーブル化（P.15-30）
- IDSM-2 のリセット（P.15-31）

全メモリ テストのイネーブル化

IDSM-2 を最初にブートするときに、デフォルトでは部分的なメモリ テストが実行されます。Catalyst ソフトウェアおよび Cisco IOS ソフトウェアで全メモリ テストをイネーブルにできます。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-30）
- Cisco IOS ソフトウェア（P.15-31）

Catalyst ソフトウェア

全メモリ テストをイネーブルにするには、**set boot device** *boot_sequence module_number* **mem-test-full** コマンドを使用します。全メモリ テストには約 12 分かかります。

全メモリ テスト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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　全メモリ テストをイネーブルにします。

```
cat6k> (enable) set boot dev cf:1 3 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable) set boot dev hdd:1 3 mem-test-full
Device BOOT variable = hdd:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
cat6k> (enable)
```

set boot device コマンドには、**cf:1** または **hdd:1** を指定できます。

ステップ 4　IDSM-2 をリセットします。

手順については、P.15-31 の「IDSM-2 のリセット」を参照してください。

全メモリ テストを実行します。

（注）　全メモリ テストは、部分的なメモリ テストよりも完了に時間がかかります。

Cisco IOS ソフトウェア

全メモリ テストをイネーブルにするには、**hw-module module** *module_number* **reset mem-test-full** コマンドを使用します。全メモリ テストには約 12 分かかります。

全メモリ テスト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　全メモリ テストをイネーブルにします。

```
switch# hw-module module 9 reset mem-test-full
    Device BOOT variable for reset = <empty>
    Warning: Device list is not verified.

    Proceed with reload of module?[confirm]
    % reset issued for module 9
switch#
```

ステップ 3　IDSM-2 をリセットします。

手順については、P.15-31 の「IDSM-2 のリセット」を参照してください。

全メモリ テストを実行します。

（注）　全メモリ テストは、部分的なメモリ テストよりも完了に時間がかかります。

IDSM-2 のリセット

何らかの理由で、SSH、Telnet、またはスイッチの **session** コマンドを使用して IDSM-2 と通信できない場合は、スイッチ コンソールから IDSM-2 をリセットする必要があります。リセット処理には数分かかります。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-31）
- Cisco IOS ソフトウェア（P.15-32）

Catalyst ソフトウェア

CLI から IDSM-2 をリセットするには、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　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　アプリケーション パーティションまたはメンテナンス パーティションに IDSM-2 をリセットします。

```
cat6k> (enable) reset module_number [hdd:1 | cf:1]
```

(注)　アプリケーション パーティション（hdd:1 デフォルト）もメンテナンス パーティション（cf:1）も指定しないと、IDSM-2 はブート デバイス変数を使用します。

次の例は、**reset** コマンドの出力を示します。

```
cat6k> (enable) reset 3
2003 Feb 01 00:18:23 %SYS-5-MOD_RESET: Module 3 reset from console//
Resetting module 3... This may take several minutes.
2003 Feb 01 00:20:03 %SYS-5-MOD_OK: Module 3 is online.
cat6k> (enable)
```

注意　IDSM-2 を先にシャットダウンしないでスイッチ シャーシから取り外した場合、またはシャーシの電源が切れた場合は、IDSM-2 のリセットを複数回行うことが必要な場合があります。リセット操作を 3 回繰り返しても IDSM-2 が反応しない場合は、メンテナンス パーティションをブートし、アプリケーション パーティションの復元手順を実行してください。手順については、P.17-31 の「IDSM-2 システム イメージのインストール」を参照してください。

Cisco IOS ソフトウェア

(注)　リセット処理には数分かかります。

CLI から IDSM-2 をリセットするには、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 をリセットします。

```
switch# hw-module module module_number reset [hdd:1 | cf:1]
```

(注)　アプリケーション パーティション（hdd:1 デフォルト）もメンテナンス パーティション（cf:1）も指定しないと、IDSM-2 はブート デバイス変数を使用します。

次の例は、**reset** コマンドの出力を示します。

```
switch# hw-module module 8 reset
Device BOOT variable for reset =
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 8
switch#
```

Catalyst および Cisco IOS ソフトウェアのコマンド

この項では、IDSM-2 に関係する Catalyst ソフトウェアおよび Cisco IOS ソフトウェアのコマンドを示します。

（注） Catalyst および Cisco IOS ソフトウェア コマンドの詳細については、Cisco.com にあるコマンド リファレンスを参照してください。これらの文書の検索方法については、IDSM-2 に付属する『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1*』を参照してください。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-33）
- Cisco IOS ソフトウェア（P.15-35）

Catalyst ソフトウェア

この項では、サポートされている Catalyst ソフトウェア コマンドとサポートされていない Catalyst ソフトウェア コマンドを示します。取り上げる事項は次のとおりです。

- サポートされているスーパーバイザ エンジン コマンド（P.15-33）
- サポートされていないスーパーバイザ エンジン コマンド（P.15-34）

サポートされているスーパーバイザ エンジン コマンド

IDSM-2 は、次のスーパーバイザ エンジン CLI コマンドもサポートしています。このコマンドの詳細は、Catalyst 6500 シリーズのコマンド リファレンスに記載されています。

- **clear config** *module_number*

  指定された IDSM-2 に関連付けられたスーパーバイザ エンジンのコンフィギュレーションをクリアします。
- **clear log** *module_number*

  指定された IDSM-2 に関するエラー ログのエントリをすべて削除します。
- **session** *slot_number*

  スイッチ コンソールから IDSM-2 のコンソールにログインします。
- **set module** コマンド（他のすべての **set module** コマンドはエラー メッセージを返します）。
  - **set module name** *module_number*

    モジュールの名前を設定します。
  - **set module power** *module_number* **[up | down]**

    指定された IDSM-2 の電源をイネーブルまたはディセーブルにします。

- **set port name** *module_number*

  指定された IDSM-2 ポートの名前を設定します。
- **set span**

  ポート 1 を SPAN 宛先ポートとして設定します。IDSM-2 上のポート 1 は、SPAN 発信元ポートとして使用できません。
- **set trunk**

  トランク ポートを設定します。
- **set vlan**

  VLAN キャプチャ ポートを設定します。
- **show config**

  スーパーバイザ エンジン NVRAM コンフィギュレーションを表示します。
- **show log**

  指定された IDSM-2 のエラー ログを表示します。
- **show mac** *module_number*

  指定された IDSM-2 の MAC カウンタを表示します。
- **show module** *module_number*

  IDSM-2 が取り付けられている場合は、Module-Type に「Intrusion Detection System Module」が表示されます。
- **show port** *module_number*

  指定された IDSM-2 のポート ステータスを表示します。
- **show port capabilities** [*module* | *module_number*]

  モジュールおよびポートの機能を表示します。
- **show test**

  SPAN ポート（ポート 1）および管理ポート（ポート 2）の両方の診断テストから報告されたエラーと、BIOS および CMOS のブート結果を表示します。

サポートされていないスーパーバイザ エンジン コマンド

次のスーパーバイザ エンジン CLI コマンドは、IDSM-2 ではサポートされていません。

- **set module** [**enable** | **disable**] *module_number*
- **set port broadcast**
- **set port channel**
- **set port cops**
- **set port disable**
- **set port enable**
- **set port flowcontrol**
- **set port gmrp**
- **set port gvrp**
- **set port host**
- **set port inlinepower**
- **set port jumbo**
- **set port membership**
- **set port negotiation**
- **set port protocol**

- **set port qos**
- **set port rsvp**
- **set port security**
- **set port speed**
- **set port trap**
- **set protocolfilter**
- **set rgmp**
- **set snmp**
- **set spantree**
- **set udld**
- **set vtp**

Cisco IOS ソフトウェア

この項では、IDSM-2 がサポートしている Cisco IOS ソフトウェア コマンドを示します。これらのコマンドは、モードに従ってグループ化されています。

この項では、次のトピックについて説明します。

- EXEC コマンド（P.15-35）
- コンフィギュレーション コマンド（P.15-36）

EXEC コマンド

次のコマンドはすべて、EXEC モードで実行されます。

- **clock read-calendar**

  クロック時刻をカレンダ時刻にアップデートします。
- **clock set** *time date*

  現在の時刻と日付を設定します。
- **clock update-calendar**

  カレンダ時刻をクロック時刻にアップデートします。
- **hw-module module** *slot_number* **reset**

  IDSM-2 を、ブート デバイス変数で指定されたパーティションにリセットします。ブート デバイス変数が設定されていなかった場合、IDSM-2 はデフォルトでアプリケーション パーティションにリセットされます。ブート デバイス変数の現在の設定を表示するには、**show boot device module** *module_number* コマンドを使用します。
- **hw-module module** *slot_number* **reset cf:1**

  モジュールをメンテナンス パーティションにリセットします。
- **hw-module module** *slot_number* **shutdown**

  モジュールをシャットダウンして、シャーシから安全に取り外しできるようにします。
- **reload**

  スイッチ全体をリロードします。
- **session slot** *slot_number* **processor** *processor_number*

  スイッチ コンソールから IDSM-2 のコンソールにログインします。
- **show intrusion-detection module** *module_number* **data-port** *data_port_number* **state**

  指定された IDSM-2 データ ポートの状態を表示します。

- **show intrusion-detection module** *module_number* **data-port** *data_port_number* **traffic**
  IDSM-2 データ ポート トラフィックのトラフィック統計情報を表示します。
- **show intrusion-detection module** *module_number* **management-port state**
  IDSM-2 管理ポートの状態を表示します。
- **show intrusion-detection module** *module_number* **management-port traffic**
  IDSM-2 管理ポートのトラフィック統計情報を表示します。
- **show ip access-lists**
  現在のアクセス リストを表示します。
- **show module**
  取り付けられているモジュール、バージョン、および状態を表示します。
- **show running-config**
  現在動作しているコンフィギュレーションを表示します。
- **show startup-config**
  保存されているコンフィギュレーションを表示します。
- **show vlan access-map**
  現在の VLAN アクセス マップをすべて表示します。

コンフィギュレーション コマンド

次のコンフィギュレーション コマンドはすべて、グローバル コンフィギュレーション モード、インターフェイス コンフィギュレーション モード、または VACL コンフィギュレーション サブモードのいずれかで実行されます。

- グローバル コンフィギュレーション モード
  - **clock calendar valid**
    現在のカレンダ時刻をブートのスイッチ時刻として設定します。
  - **clock summer-time** *zone* **recurring**
    サマータイム設定を使用するようにスイッチを設定します。
  - **clock timezone** *zone offset*
    スイッチ /IDSM-2 の時間帯を設定します。
  - **intrusion-detection module** *module_number* **management-port access-vlan** *access_vlan_number*
    IDSM-2 コマンド / コントロール ポートのアクセス VLAN を設定します。
  - **intrusion-detection module** *module_number* **data-port** *data_port_number* **capture allowed-vlan** *allowed_capture_vlan(s)*
    VACL キャプチャ用の VLAN を設定します。
  - **intrusion-detection module** *module_number* **data-port** *data_port_number* **capture**
    指定された IDSM-2 データ ポートの VACL キャプチャをイネーブルにします。
  - **ip access-list extended** *word*
    VACL マップで使用するアクセス リストを作成します。
  - **monitor session** *session* {**destination** {**interface** *interface interface-number*} [, | -] {**vlan** *vlan-id*}}
    SPAN セッションの宛先を設定します。
  - **monitor session** *session* {**source** {**interface** *interface interface-number*} | {**vlan** *vlan-id*}} [, | - | **rx** | **tx** | **both**]
    SPAN セッションの送信元を設定します。
  - **no power enable module** *slot_number*
    IDSM-2 をシャットダウンして、電源を切ります。

- **power enable module** *slot_number*
  IDSM-2 の電源がまだオンでない場合は、オンにします。
- **vlan access-map** *map_name_sequence*
  VACL マップを作成します。
- **vlan filter** *map_name* **vlan-list** *vlans*
  VACL マップを VLAN にマッピングします。

• インターフェイス コンフィギュレーション モード
  - **switchport**
    インターフェイスをスイッチ ポートとして設定します。
  - **switchport access vlan** *vlan*
    インターフェイスのアクセス VLAN を設定します。
  - **switchport capture**
    インターフェイスをキャプチャ ポートとして設定します。
  - **switchport mode access**
    インターフェイスをアクセス ポートとして設定します。
  - **switchport mode trunk**
    インターフェイスをトランク ポートとして設定します。
  - **switchport trunk allowed vlan** *vlans*
    トランク用の許可された VLAN を設定します。
  - **switchport trunk encapsulation dot1q**
    dot1q をカプセル化タイプとして設定します。
  - **switchport trunk native vlan** *vlan*
    トランク ポート用のネイティブ VLAN を設定します。

• VACL コンフィギュレーション サブモード
  - **action forward capture**
    一致したパケットを取り込むことを指定します。
  - **match ip address** [*1-199* | *1300-2699* | *acl_name*]
    VACL でのフィルタリングを指定します。

NM-CIDS の設定

この章では、NM-CIDS をセットアップして、トラフィックの受信を準備するために実行する必要のあるタスクについて説明します。これを行うと、侵入検出を設定できるようになります。

(注) NM-CIDS はインライン モードでは動作せず、混合モードでのみ動作します。したがって、侵入防御は設定できません。

この章は、次の項で構成されています。

- コンフィギュレーション シーケンス（P.16-2）
- IDS センサー インターフェイスのルータへの設定（P.16-3）
- NM-CIDS セッションの確立（P.16-5）
- パケット キャプチャの設定（P.16-7）
- 管理タスク（P.16-9）
- サポートされている Cisco IOS コマンド（P.16-11）

コンフィギュレーション シーケンス

NM-CIDS を設定するには、次のタスクを実行します。

1. ルータに IDS インターフェイスを設定します。

   手順については、P.16-3 の「IDS センサー インターフェイスのルータへの設定」を参照してください。

2. NM-CIDS にログインします。

   手順については、P.16-5 の「NM-CIDS セッションの確立」を参照してください。

3. NM-CIDS を初期化します。

   setup コマンドを実行して NM-CIDS を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

4. トラフィックを取り込んで侵入検出分析を行うように NM-CIDS を設定します。

   手順については、P.16-7 の「パケット キャプチャの設定」を参照してください。

5. サービス アカウントを作成します。

   手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

6. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

7. 侵入検出を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 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。

8. 管理タスクを実行して NM-CIDS が円滑に動作し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」および 第 16 章「管理タスク」を参照してください。

9. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

10. 必要に応じて、ブート ヘルパーとブート ローダーのイメージを再作成します。

    手順については、P.17-23 の「NM-CIDS システム イメージのインストール」を参照してください。

IDS センサー インターフェイスのルータへの設定

NM-CIDS には外部コンソール ポートはありません。NM-CIDS へのコンソール アクセスは、ルータで **service-module ids-module** *slot_number*/**0 session** コマンドを発行した場合、または NM-CIDS スロットに対応するポート番号でルータへの Telnet 接続を開始した場合にイネーブルになります。外部コンソール ポートがないことは、初期ブートアップ コンフィギュレーションはルータ経由でのみ可能であることを意味します。

service-module ids-sensor *slot_number*/**0 session** コマンドを発行する場合は、NM-CIDS とのコンソール セッションを作成します。NM-CIDS で、どのような IPS コンフィギュレーション コマンドでも発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドは、IDS センサー インターフェイスの IP アドレスを使用して、逆 Telnet 接続を開始します。IDS センサー インターフェイスは、NM-CIDS とルータの間のインターフェイスです。**session** コマンドを起動するには、事前に IDS センサー インターフェイスに IP アドレスを割り当てておく必要があります。ルーティング可能な IP アドレスを割り当てると、ID センサー インターフェイス自体が攻撃に対して脆弱になります。この脆弱性に対処するために、ループバック IP アドレスを IDS センサー インターフェイスに割り当てます。

NM-CIDS 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　NM-CIDS スロット番号をルータに設定します。

```
router # show interfaces ids-sensor slot_number/0
```

（注）　**show run** コマンドを使用することもできます。「IDS-Sensor」とスロット番号を検索します。

（注）　Cisco IOS では、NM-CIDS に「IDS-Sensor」という名前が付けられています。この例では、スロット番号は 1 で、ポートは 1 つしかないので、ポート番号は 0 です。

ステップ 2　CEF スイッチング パスをイネーブルにします。

```
router# configuration terminal
router(config)# ip cef
router(config)# exit
```

ステップ 3　ループバック インターフェイスを作成します。

```
router# configure terminal
router(config)# interface loopback 0
```

ステップ 4　IP アドレスとネットマスクをループバック インターフェイスに割り当てます。

```
router(config-if)# ip address 10.16.0.0 255.255.0.0
```

（注） NM-CIDS の内部インターフェイスに IP アドレスを割り当てて、NM-CIDS に対してセッションを開始する必要があります。ルータにある他のインターフェイスに割り当てられているネットワークと重複しないネットワークを選択します。このアドレスは NM-CIDS へのアクセスに使用しないので、実 IP アドレスである必要はありません。

ステップ 5　番号未指定のループバック インターフェイスを IDS センサー インターフェイスに割り当てます。この例では、スロット 1 を使用します。

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered loopback 0
```

ステップ 6　ポートをアクティブにします。

```
router(config-if)# no shutdown
```

ステップ 7　コンフィギュレーション モードを終了します。

```
router(config-if)# end
```

ステップ 8　コンフィギュレーションを NVRAM に書き込みます。

```
router# write memory
Building configuration
[OK]
```

NM-CIDS セッションの確立

この項では、ルータと NM-CID 間にセッションを確立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。

- NM-CIDS に対するセッションの開始（P.16-5）
- NM-CIDS への Telnet 接続（P.16-6）

NM-CIDS に対するセッションの開始

ルータから NM-CIDS へのセッションを確立するには、**session** コマンドを使用します。**Ctrl+Shift+6** キーを押し、その後 **x** キーを押して、セッション プロンプトをルータ プロンプトに戻します。つまり、NM-CIDS プロンプトからルータ プロンプトに戻ります。空白行で **Enter** キーを押して、セッション プロンプト、つまり NM-CIDS プロンプトに戻ります。ルータ コマンドを実行後、セッションに戻る場合は、NM-CIDS へのセッションを中断するだけにします。NM-CIDS セッションに戻る予定がない場合は、セッションを中断するのではなく、セッションを閉じます。

セッションを閉じると、NM-CIDS CLI から完全にログアウトされて、新規セッションを接続するには、ログインするためにユーザ名とパスワードが必要です。セッションの中断では、CLI にログインした状態のままになっています。**session** コマンドで接続すると、同じ CLI に戻ることができ、ユーザ名もパスワードも指定する必要はありません。

（注） Telnet クライアントはさまざまです。場合によっては、**Ctrl+6+x** キーを押す必要があります。制御文字は ^^、Ctrl+^、または ASCII 値 30（16 進数 1E）として指定されます。

注意 **disconnect** コマンドを使用してセッションをそのままにしておくと、セッションは動作状態のままです。開いているセッションは、まだ動作中の接続を利用しようと考える人物によって、不正利用される可能性があります。

NM-CIDS へのセッションをオープンおよびクローズするには、次の手順を実行します。

ステップ 1　ルータから NM-CIDS へのセッションを開きます。

```
router# service-module ids-sensor 1/0 session
Trying 10.16.0.0, 2033 ... Open
```

ステップ 2　**Ctrl+Shift+6** キーを押し、その後 **x** キーを押して、ルータ プロンプトに戻って、NM-CIDS セッションを中断します。

ステップ 3　空白行で **Enter** キーを押して、NM-CIDS プロンプトに戻ります。

ステップ 4　NM-CIDS セッションを終了します。

```
nm-cids# exit
```

（注） IPS CLI のサブモードにいる場合は、すべてのサブモードを終了する必要があります。センサー ログイン プロンプトが表示されるまで、**exit** を入力します。

セッションを適切に閉じることができないと、まだ動作中の接続が他人に不正利用される可能性があります。`Router#` プロンプトで必ず **exit** と入力して、Cisco IOS セッションを完全に閉じてください。

ステップ 5　NM-CIDS へのセッションを中断して閉じるには、**Ctrl+Shift** キーを押した状態で **6** キーを押します。すべてのキーを放してから、**x** キーを押します。

（注） セッションを終了したら、ルータに戻って、セッション（IPS アプリケーション）と監視するルータ インターフェイスとの間の関連付けを確立する必要があります。

ステップ 6　ルータから切断します。

```
router# disconnect
```

ステップ 7　**Enter** キーを押して切断を確認します。

```
router# Closing connection to 10.16.0.0 [confirm] <Enter>
```

NM-CIDS への Telnet 接続

NM-CIDS スロットに対応するポート番号で、直接ルータに Telnet で接続することもできます。P.16-3 の「IDS センサー インターフェイスのルータへの設定」でループバック 0 インターフェイスを設定するときに割り当てたアドレスを使用します。

ポート番号は、「2001 + 32 × スロット番号」という式で決定されます。

たとえば、スロット 1 の場合、ポート番号は 2033、スロット 2 の場合は 2065、などとなります。

Telnet を使用してポート 2033 へのセッションを起動するには、次のように入力します。

```
router# telnet 10.16.0.0 2033
```

パケット キャプチャの設定

パケット モニタリングには、ルータ上で目的のインターフェイス（サブインターフェイスを含む）をイネーブルにする必要があります。監視対象のインターフェイスまたはサブインターフェイスは必要な数だけ選択できます。これらのインターフェイスで送信されるパケットおよび受信されるパケットは、検査のために NM-CIDS に転送されます。インターフェイスは、ルータ CLI（Cisco IOS）を使用してイネーブルまたはディセーブルにします。

（注） ルータで暗号化を行っている場合、NM-CIDS は、ルータに着信するパケットは復号化後、およびルータから発信するパケットは暗号化前に、受信します。

NM-CIDS にパケット キャプチャを設定するには、次の手順を実行します。

ステップ 1　ルータ コンソールにログインします。

ステップ 2　インターフェイス コンフィギュレーションを表示します。

```
router# show run
```

ステップ 3　監視するインターフェイスまたはサブインターフェイス（たとえば、FastEthernet0/0）を確認します。

（注） 監視するインターフェイスまたはサブインターフェイスは複数選択できますが、一度に編集できるインターフェイスは 1 つだけです。

ステップ 4　グローバル コンフィギュレーション モードに入ります。

```
router# configure terminal
```

ステップ 5　インターフェイスまたはサブインターフェイスを指定します。

```
router(config)# interface FastEthernet0/0
```

（注） トラフィックは、ルータの 1 つのインターフェイスから着信します。

ステップ 6　ネットワーク トラフィックを NM-CIDS にコピーするようにインターフェイスを設定します。

```
router(config-if)# ids-service-module monitoring
```

（注） モニタリングを停止するには、**no ids-service-module monitoring** コマンドを使用します。

ステップ 7　インターフェイス モードを終了します。

```
router(config-if)# exit
```

ステップ 8　監視するインターフェイスまたはサブインターフェイスそれぞれに対して、ステップ 3～ 6 を繰り返します。

ステップ 9　グローバル コンフィギュレーション モードを終了します。

```
router(config)# exit
```

ステップ 10　NM-CIDS がネットワーク トラフィックを分析していることを確認します。

a.　NM-CIDS 上の外部インターフェイスに対して Telnet セッションまたは SSH セッションを開きます。

（注）　SSH　には、許可されたホストが必要です。手順については、P.4-36 の「既知のホストリストへのホストの追加」を参照してください。

b.　NM-CIDS にログインします。

c.　インターフェイス統計情報を表示して、モニタリング インターフェイスが動作していることを確認します。

```
nm-cids# show interface clear
nm-cids# show interface
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 = 23
   Total Bytes Received = 1721
   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 = 2
   Total Bytes Transmitted = 120
   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
```

d.　ステップ c を繰り返して、カウンタが徐々に増加していることを確認します。増加していることは、NM-CIDS がネットワーク トラフィックを受信していることを示します。

カウンタが増加しない場合は、ステップ 3 ～ 6 を適切に実行し、**setup** コマンドで NM-CIDS を初期化したときに、FastEthernet0/0 が仮想センサーに追加されていることを確認します。

管理タスク

この項では、NM-CIDS のリブート方法および Cisco IPS ソフトウェアのステータスの確認方法について説明します。

この項では、次のトピックについて説明します。

- NM-CIDS のシャットダウン、リロード、およびリセット（P.16-9）
- Cisco IPS ソフトウェアのステータスの確認（P.16-10）

NM-CIDS のシャットダウン、リロード、およびリセット

Cisco IOS には、NM-CIDS を制御する **shutdown** コマンド、**reload** コマンド、および **reset** コマンドが用意されています。

- **shutdown**：オペレーティング システムを適切に終了させます。

```
router# service-module ids-sensor slot_number/0 shutdown
```

注意　ルータから NM-CIDS を取り外す前に、必ず **shutdown** コマンドを実行してください。**shutdown** コマンドを実行せずに NM-CIDS を取り外すと、データの消失、またはハードディスク ドライブの破損を招く可能性があります。

- **reload**：NM-CIDS 上のオペレーティング システムを適切に停止してリブートします。

```
router# service-module ids-sensor slot_number/0 reload
```

- **reset**：NM-CIDS　のハードウェアをリセットします。通常、このコマンドは、シャットダウンから回復するために使用されます。

```
router# service-module ids-sensor slot_number/0 reset
```

次の警告が表示されます。

```
router# service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

注意　ハードディスク ドライブのデータが失われるのは、最初に NM-CIDS をシャットダウンせずに **reset** コマンドを発行した場合だけです。NM-CIDS がまだ正常に動作している場合は、**reset** コマンドでなく、**reload** コマンドを使用します。その他の状況の場合は、**reset** コマンドを使用しても安全です。

Cisco IPS ソフトウェアのステータスの確認

ルータで動作している Cisco IPS のステータスを確認するには、**status** コマンドを使用します。

```
router# service-module ids-sensor slot_number/0 status
```

表示される出力の例を次に示します。

```
Router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait..
Service Module Version information received,
Major ver = 1, Minor ver= 1
Cisco Systems Intrusion Detection System Network Module
Software version: 5.0(1)S42
Model: NM-CIDS
Memory: 254676 KB
Mgmt IP addr:     xx.xx.xx.xx
Mgmt web ports:    443
Mgmt TLS enabled: true
```

サポートされている Cisco IOS コマンド

service-module ids-sensor *slot_number*/**0** Cisco IOS コマンドが新しく NM-CIDS をサポートするようになりました。スロット番号は異なることがありますが、ポートは常に 0 です。

次のオプションが適用されます。

- 特権モード EXEC
  - **service-module ids-sensor** *slot_number*/**0 reload**

    オペレーティング システムを NM-CIDS にリロードします。
  - **service-module ids-sensor** *slot_number*/**0 reset**

    NM-CIDS に対してハードウェア リセットを行います。
  - **service-module ids-sensor** *slot_number*/**0 session**

    session コマンドを使用して、IPS コンソールにアクセスできるようになります。
  - **service-module ids-sensor** *slot_number*/**0 shutdown**

    NM-CIDS で動作している IPS アプリケーションをシャットダウンします。

注意　シャットダウンを正常に行わずに NM-CIDS を取り外すと、ハードディスク ドライブの破損を招く可能性があります。NM-CIDS アプリケーションが正常にシャットダウンされると、NM-CIDS の取り外しが可能になったことを示すメッセージが Cisco IOS によって表示されます。

  - **service-module ids-sensor** *slot_number*/**0 status**

    Cisco IPS ソフトウェアのステータスに関する情報を提供します。
- インターフェイス モードの設定 (`config-if`)
  - **ids-service-module monitoring**

    指定したインターフェイス（またはサブインターフェイス）上で IPS モニタリングをイネーブルにできます。指定したインターフェイス上の着信パケットと発信パケットの両方が、モニタリングのために転送されます。

システム イメージのアップグレード、ダウングレード、およびインストール

この章では、システム イメージのアップグレード、ダウングレード、およびインストールの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。

- 概要（P.17-2）
- センサーのアップグレード（P.17-3）
- 自動アップグレードの設定（P.17-7）
- センサーのダウングレード（P.17-10）
- アプリケーション パーティションの復旧（P.17-11）
- システム イメージのインストール（P.17-13）

概要

センサー上のソフトウェアをアップグレードおよびダウングレードできます。アップグレードは、サービス パック、シグニチャ アップデート、マイナー バージョン、メジャー バージョン、またはリカバリ パーティション ファイルに適用されます。ダウングレードでは、最後に適用されたアップグレードをセンサーから削除します。

注意

downgrade コマンドを使用して 5.0 から 4.x へ移行することはできません。4.x へ戻るには、センサーのイメージを再作成する必要があります。5.0(1) 以降のリリースには **downgrade** コマンドを使用できます。

センサーのアプリケーション パーティション イメージが使用できなくなった場合、それを復旧することができます。**recover** コマンドを使用すると、ホスト設定は保持できますが、その他の設定は出荷時のデフォルトに戻ります。

新規のシステム イメージをセンサーにインストールするには、使用するプラットフォームに応じて、リカバリ / アップグレード CD、ROMMON、ブート ローダー / ヘルパー ファイル、またはメンテナンス パーティションを使用します。

新規のシステム イメージをセンサーにインストールすると、すべてのアカウントが削除され、デフォルトの cisco アカウントは、デフォルトのパスワード「cisco」を使用するようにリセットされます。システム イメージをインストールした後に、センサーを再度初期化する必要があります。手順については、P.3-3 の「センサーの初期化」を参照してください。

センサーは、イメージを再作成し、初期化した後、最新のサービス パック、シグニチャ アップデート、マイナー バージョン、メジャー バージョン、およびリカバリ パーティション ファイルでアップグレードする必要があります。Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

センサーのアップグレード

この項では、**upgrade** コマンドを使用して、センサー上のソフトウェアをアップグレード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.17-3）
- アップグレード コマンドおよびオプション（P.17-3）
- アップグレード コマンドの使用方法（P.17-4）
- リカバリ パーティションのアップグレード（P.17-5）

概要

センサーは、次のファイルでアップグレードできます。これらのファイルにはすべて、拡張子 .pkg が付いています。

- シグニチャ アップデート（たとえば、IPS-sig-S150-minreq-5.0-1.pkg）
- メジャー アップデート（たとえば、IPS-K9-maj-6.0-1-pkg）
- マイナー アップデート（たとえば、IPS-K9-min-5.1-1.pkg）
- サービス パック アップデート（たとえば、IPS-K9-sp-5.0-2.pkg）
- リカバリ パーティション アップデート（たとえば、IPS-K9-r-1.1-a-5.0-1.pkg）

センサーをアップグレードすると、センサーのソフトウェア バージョンが変更されます。

アップグレード コマンドおよびオプション

サービス ホスト サブモードで **auto-upgrade-option enabled** コマンドを使用して、自動アップグレードを設定します。

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **directory**：ファイル サーバ上でアップグレード ファイルが置かれているディレクトリ。
  先頭の「/」はこれが絶対パスであることを示しています。
- **file-copy-protocol**：ファイル　サーバからのファイルのダウンロードに使用されるファイル　コピー プロトコル。有効な値は **ftp** または **scp** です。

（注） SCP を使用する場合は、センサーが SSH を介してサーバと通信できるよう、**ssh host-key** コマンドを使用してサーバを SSH の既知ホストに追加する必要があります。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

- **ip-address**：ファイル サーバの IP アドレス。
- **password**：ファイル サーバ上の認証用のユーザ パスワード。
- **schedule-option**：自動アップグレードが実行されたときにスケジュールされます。カレンダのスケジューリングでは、特定の日の特定の時刻にアップグレードが開始されます。定期スケジューリングでは、特定の間隔でアップグレードが開始されます。
  - **calendar-schedule**：自動アップグレードを実行する曜日と時刻を設定します。
    days-of-week：自動アップグレードを実行する曜日。複数の曜日を選択できます。*sunday* から *saturday* までが有効な値です。
    no：エントリまたは選択設定を削除します。

times-of-day：自動アップグレードを開始する時刻。複数の時刻を選択できます。有効な値は *hh:mm[:ss]* です。

– **periodic-schedule**：最初の自動アップグレードが実行される時刻と、各自動アップグレード間の間隔を設定します。

interval：各自動アップグレード間の時間数。有効な値は 0 ～ 8760 です。

start-time：最初の自動アップグレードを開始する時刻。有効な値は *hh:mm[:ss]* です。

- **user-name**：ファイル サーバ上の認証用のユーザ名。

アップグレード コマンドの使用方法

センサーをアップグレードするには、次の手順を実行します。

ステップ 1　メジャー アップデート ファイル（たとえば、IPS-K9-maj-6.0-1-pkg）を、センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

（注） ファイルをダウンロードするには、暗号化特権を持つアカウントを使用して Cisco.com にログインする必要があります。ファイル名は変更しないでください。アップデートを受け入れるには、センサーの元のファイル名を保持する必要があります。暗号化特権を持つアカウントの入手手順については、『*Release Notes for Cisco Intrusion Prevention System 5.1*』を参照してください。

ステップ 2　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 3　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 4　センサーをアップグレードします。

```
sensor# configure terminal
sensor(config)# upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-6.0-1-pkg
```

ステップ 5　プロンプトが表示されたら、パスワードを入力します。

```
Enter password: ********
Re-enter password: ********
```

ステップ 6　**yes** を入力してアップグレードを完了します。

（注） メジャー アップデート、マイナー アップデート、およびサービス パックによって、IPS プロセスの再起動が強制されることがあります。または、インストールを完了するためにセンサーのリブートが強制されることもあります。

ステップ 7　新しいセンサーのバージョンを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(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 5 days.
Using 490110976 out of 1984704512 bytes of available memory (24% 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   Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-maj-6.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 6.0(1)S149

sensor#
```

リカバリ パーティションのアップグレード

リカバリ パーティションを最新のバージョンでアップグレードするには、**upgrade** コマンドを使用します。これによって、センサーのアプリケーション パーティションを復旧する必要がある場合の準備ができます。

(注)　リカバリ パーティション イメージはメジャーおよびマイナー ソフトウェア リリースのために生成され、サービス パックまたはシグニチャ アップデートのために生成されるという状況はごくまれにしかありません。

(注)　リカバリ パーティションをアップグレードするには、センサーでバージョン 5.0(1) 以上がすでに動作している必要があります。

センサーのリカバリ パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-K9-r-1.1-a-5.1-1.pkg）を、センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

注意　一部のブラウザでは、ファイル名に拡張子が付加されます。保存されたファイルのファイル名は、ダウンロード ページに表示されているファイル名と一致する必要があります。一致しないと、そのファイルは、リカバリ パーティションのアップグレードに使用できません。

ステップ 2　管理者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 3　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 4　リカバリ パーティションをアップグレードします。

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-5.1-1.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-5.1-1.pkg
```

ステップ 5　サーバ パスワードを入力します。

アップグレード処理が始まります。

（注）　この手順では、リカバリ パーティションのイメージしか再作成しません。アプリケーション パーティションは、このアップグレードでは変更されません。リカバリ パーティションの後にアプリケーション パーティションのイメージを再作成するには、**recover application-partition** コマンドを使用します。手順については、P.17-11 の「復旧コマンドの使用方法」を参照してください。

自動アップグレードの設定

この項では、アップグレード ディレクトリにあるアップグレード ファイルを自動的に検索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。取り上げる事項は次のとおりです。

- 概要（P.17-7）
- 自動アップグレード コマンドおよびオプション（P.17-7）
- 自動アップグレード コマンドの使用方法（P.17-8）

概要

アップグレード ディレクトリにある新しいアップグレード ファイルを自動的に検索するようにセンサーを設定することができます。

センサーが自動アップグレード ファイルをポーリングするには、ソフトウェア アップグレードを Cisco.com からダウンロードして、アップグレード ディレクトリにコピーしておく必要があります。Cisco.com でソフトウェアの場所を特定する手順については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

自動アップグレード コマンドおよびオプション

サービス ホスト サブモードで **auto-upgrade-option enabled** コマンドを使用して、自動アップグレードを設定します。

次のオプションが適用されます。

- **default**：値をシステムのデフォルト設定に戻します。
- **directory**：ファイル サーバ上でアップグレード ファイルが置かれているディレクトリ。
  先頭の「/」はこれが絶対パスであることを示しています。
- **file-copy-protocol**：ファイル　サーバからのファイルのダウンロードに使用されるファイル　コピー プロトコル。有効な値は **ftp** または **scp** です。

（注） SCP を使用する場合は、センサーが SSH を介してサーバと通信できるよう、**ssh host-key** コマンドを使用してサーバを SSH の既知ホストに追加する必要があります。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

- **ip-address**：ファイル サーバの IP アドレス。
- **password**：ファイル サーバ上の認証用のユーザ パスワード。
- **schedule-option**：自動アップグレードが実行されたときにスケジュールされます。カレンダのスケジューリングでは、特定の日の特定の時刻にアップグレードが開始されます。定期スケジューリングでは、特定の間隔でアップグレードが開始されます。
  - **calendar-schedule**：自動アップグレードを実行する曜日と時刻を設定します。

    days-of-week：自動アップグレードを実行する曜日。複数の曜日を選択できます。*sunday* から *saturday* までが有効な値です。

    no：エントリまたは選択設定を削除します。

    times-of-day：自動アップグレードを開始する時刻。複数の時刻を選択できます。有効な値は *hh:mm[:ss]* です。

— **periodic-schedule**：最初の自動アップグレードが実行される時刻と、各自動アップグレード間の間隔を設定します。

interval：各自動アップグレード間の時間数。有効な値は 0 ～ 8760 です。

start-time：最初の自動アップグレードを開始する時刻。有効な値は *hh:mm[:ss]* です。

- **user-name**：ファイル サーバ上の認証用のユーザ名。

自動アップグレード コマンドの使用方法

自動アップグレードをスケジューリングするには、次の手順を実行します。

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

ステップ 2　アップグレード ディレクトリにある新しいアップグレード ファイルを自動的に検索するようにセンサーを設定します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade-option enabled
```

ステップ 3　スケジューリングを指定します。

a.　カレンダのスケジューリングでは、特定の日の特定の時刻にアップグレードが開始されます。

```
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal# days-of-week sunday
sensor(config-hos-ena-cal# times-of-day 12:00:00
```

b.　定期スケジューリングでは、特定の間隔でアップグレードが開始されます。

```
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
sensor(config-hos-ena-per)# start-time 13:00:00
```

ステップ 4　ファイル サーバの IP アドレスを指定します。

```
sensor(config-hos-ena-per)# exit
sensor(config-hos-ena)# ip-address 10.1.1.1
```

ステップ 5　ファイル サーバ上でアップグレード ファイルが置かれているディレクトリを指定します。

```
sensor(config-hos-ena)# directory /tftpboot/update/5.1_dummy_updates
```

ステップ 6　ファイル サーバ上の認証用ユーザ名を指定します。

```
sensor(config-hos-ena)# user-name tester
```

ステップ 7　ユーザのパスワードを指定します。

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

ステップ 8　ファイル サーバ プロトコルを指定します。

```
sensor(config-hos-ena)# file-copy-protocol ftp
```

(注)　SCP を使用する場合は、センサーが SSH を介してサーバと通信できるよう、**ssh host-key** コマンドを使用してサーバを SSH の既知ホストに追加する必要があります。手順については、P.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

ステップ 9　設定を確認します。

```
sensor(config-hos-ena)# show settings
   enabled
   ----------------------------------------------
      schedule-option
      ---------------------------------------------
         periodic-schedule
         ---------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
         ---------------------------------------------
      ---------------------------------------------
      ip-address: 10.1.1.1
      directory: /tftpboot/update/5.0_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   ----------------------------------------------
sensor(config-hos-ena)#
```

ステップ 10　自動アップグレード サブモードを終了します。

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

ステップ 11　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。

センサーのダウングレード

最後に適用されたアップグレードをセンサーから削除するには、**downgrade** コマンドを使用します。

注意　**downgrade** コマンドを使用して 5.0 から 4.x へ移行することはできません。4.x へ戻るには、センサーのイメージを再作成する必要があります。5.0(1) 以降のリリースには **downgrade** コマンドを使用できます。

最後に適用されたアップグレードをセンサーから削除するには、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センサーにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　センサーをダウングレードします。

```
sensor(config)# downgrade
Warning: Executing this command will reboot the system and downgrade to
IPS-K9-sp.5.0-2.pkg. Configuration changes made since the last upgrade will be lost
and the system may be rebooted.
Continue with downgrade?:
```

ステップ 4　**yes** を入力してダウングレードを続行します。

ステップ 5　最近適用されたサービス パックまたはシグニチャ アップデートがない場合、**downgrade** コマンドは使用できません。

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

アプリケーション パーティションの復旧

この項では、アプリケーション パーティションの復旧方法について説明します。取り上げる事項は次のとおりです。

- 概要（P.17-11）
- 復旧コマンドの使用方法（P.17-11）

概要

アプライアンスのアプリケーション パーティション イメージは、使用できなくなった場合は、復旧することができます。この方法を使用すると、一部のネットワーク コンフィギュレーション情報は保持されます。これによって、復旧を実行した後、ネットワークにアクセスできます。

リカバリ パーティションをブートするには、**recover application-partition** コマンドを使用します。このコマンドにより、アプライアンス上のアプリケーション パーティションが自動的に復旧されます。

（注） アプリケーション パーティション イメージを復旧する前に、リカバリ パーティションを最新のバージョンにアップグレードしている場合は、最新のソフトウェア イメージをインストールできます。リカバリ パーティションを最新バージョンにアップグレードする手順については、P.17-11 の「復旧コマンドの使用方法」を参照してください。

recover application-partition コマンドは、Telnet 接続または SSH 接続を使用して実行できるので、リモート ロケーションにインストールされているセンサーを復旧するのに使用することを推奨します。

（注） アプライアンスでサポートされている場合は、リカバリ / アップグレード CD を使用して、リカバリ パーティションとアプリケーション パーティションの両方を再インストールすることもできます。手順については、P.17-22 の「リカバリ / アップグレード CD の使用方法」を参照してください。

（注） 復旧後にセンサーに再接続する場合は、デフォルトのユーザ名とパスワード `cisco` を使用してログインする必要があります。

復旧コマンドの使用方法

アプリケーション パーティション イメージを復旧するには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-K9-r-1.1-a-5.0-2.pkg）を、センサーからアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

（注） センサーのイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　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 3　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 4　アプリケーション パーティション イメージを復旧します。

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 5.0(0.27)S91(0.27). All configuration changes except for network settings will
be reset to default.
Continue with recovery? []:
```

ステップ 5　**yes** を入力して続行します。

recover コマンドを実行すると、即座にシャットダウンが開始されます。シャットダウンには少し時間がかかることがあり、この間に CLI にアクセスできますが、アクセスは警告なしに終了します。

アプリケーション パーティションのイメージは、リカバリ パーティションに保存されているイメージを使用して再作成されます。ここで、**setup** コマンドを使用してアプライアンスを初期化する必要があります。手順については、P.3-3 の「センサーの初期化」を参照してください。

（注） IP アドレス、ネットマスク、アクセス リスト、時間帯、およびオフセットは、保存され、そしてイメージが再作成されたアプリケーション パーティションに適用されます。**recover application-partition** コマンドをリモートで実行すると、デフォルトのユーザ名およびパスワード（cisco/cisco）を使用してセンサーに SSH 接続し、**setup** コマンドでセンサーを再度初期化できます。Telnet は、デフォルトでディセーブルになっているので、センサーを初期化するまでは、使用できません。

recover application-partition コマンドを実行するために CLI にアクセスできない場合は、センサーをリブートして、ブート処理中にブート メニューからオプションを選択します。これによって、リカバリ パーティションにブートして、アプリケーション パーティションのイメージを再作成できます。**recovery** コマンドをこの方法で実行するには、コンソールまたはキーボード、およびセンサーへのモニタ アクセスが必要です。これは、アプライアンスおよび NM-CIDS では実行できますが、IDSM-2 または ASA-SSM では実行できません。

システム イメージのインストール

この項では、システム イメージをアプライアンスおよびモジュールにインストールする手順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.17-13）
- IDS-4215 システム イメージのインストール（P.17-13）
- IDS-4215 BIOS および ROMMON のアップグレード（P.17-16）
- IPS-4240 および IPS-4255 システム イメージのインストール（P.17-18）
- リカバリ / アップグレード CD の使用方法（P.17-22）
- NM-CIDS システム イメージのインストール（P.17-23）
- IDSM-2 システム イメージのインストール（P.17-31）
- AIP SSM システム イメージのインストール（P.17-44）

概要

注意　システム イメージをインストールすると、ユーザ コンフィギュレーション設定はすべて失われます。システム イメージをインストールしてセンサーを復旧する前に、**recover application-partition** コマンドを使用するか、またはセンサーのブート中にリカバリ パーティションを選択して、復旧を試みてください。手順については、P.17-11 の「アプリケーション パーティションの復旧」を参照してください。

一部の TFTP サーバでは、転送可能な最大サイズが約 32 MB に制限されています。したがって、次の TFTP サーバを推奨します。

- Windows の場合

  Tftpd32 バージョン 2.0。次のサイトから入手可能です。

  http://tftpd32.jounin.net/
- UNIX の場合

  Tftp-hpa シリーズ。次のサイトから入手可能です。

  http://www.kernel.org/pub/software/network/tftp/

IDS-4215 システム イメージのインストール

アプライアンス上の ROMMON を使用してコンパクト フラッシュ デバイスにシステム イメージを TFTP 転送することにより、IDS-4215 システム イメージをインストールできます。

注意　システム イメージをインストールする前に、アップグレード ユーティリティ ファイル IDS-4215-bios-5.1.7-rom-1.4.bin を使用して、まず IDS-4215 BIOS をバージョン 5.1.7 に、ROMMON をバージョン 1.4 にアップグレードする必要があります。手順については、P.17-16 の「IDS-4215 BIOS および ROMMON のアップグレード」を参照してください。

IDS-4215 システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IDS-4215 システム イメージ ファイル（IPS-4215-K9-sys-1.1-a-5.0-1.img）を、IDS-4215 からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

IDS-4215 のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IDS-4215 をブートします。

ステップ 3　システムのブート時に、次のプロンプトで **Ctrl+R** キーを押します。

```
Evaluating Run Options...
```

（注）　5 秒間 **Ctrl+R** キーを押し続けます。

コンソールの表示は次のようなものになります。

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.7 02/23/04 15:50:39.31
Compiled by dnshep
Evaluating Run Options ...
Cisco ROMMON (1.4) #3: Mon Feb 23 15:52:45 MST 2004
Platform IDS-4215

Image Download Memory Sizing
Available Image Download Space: 510MB

0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)

Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.0001.0001
Use ? for help.
rommon>
```

ステップ 4　IDS-4215 で BIOS バージョン 5.1.7 以上および ROMMON バージョン 1.4 以上が動作していることを確認します。

（注）　IDS-4215 が BIOS および ROMMON の正しいバージョンを使用していない場合は、イメージを再作成する前に、BIOS および ROMMON をアップグレードする必要があります。手順については、P.17-16 の「IDS-4215 BIOS および ROMMON のアップグレード」を参照してください。

現在のバージョンは、ステップ 3 で確認されるコンソール表示情報に示されています。

ステップ 5　必要に応じて、TFTP のダウンロードに使用するポートを変更します。

```
rommon> interface port_number
```

使用中のポートが rommon プロンプトの直前に示されます。例では、`Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.0001.0001` というテキストに示されているとおり、ポート 1 が使用されています。

（注） TFTP ダウンロードに使用されるデフォルトのポートは、ポート 1 です。このポートは、IDS-4215 のコマンド / コントロール インターフェイスに対応します。

（注） ポート 0（モニタリング インターフェイス）およびポート 1（コマンド / コントロール インターフェイス）は、シャーシの背面にラベルで表示されています。

ステップ 6　IDS-4215 上のローカル ポートの IP アドレスを指定します。

```
rommon> address ip_address
```

（注） IDS-4215 に割り当てられているのと同じ IP アドレスを使用します。

ステップ 7　TFTP サーバの IP アドレスを指定します。

```
rommon> server ip_address
```

ステップ 8　ゲートウェイの IP アドレスを指定します。

```
rommon> gateway ip_address
```

ステップ 9　ローカルのイーサネット ポートから ping コマンドを使用することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　イメージのダウンロード元である TFTP ファイル サーバ上のパスおよびファイル名を指定します。

```
rommon> file path/filename
```

UNIX の例：

```
rommon> file /system_images/IDS-4215-K9-sys-1.1-a-5.0-1.img
```

（注） このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリを基準とした相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージには、ファイルの場所にディレクトリ名もスラッシュも指定されていません。

Windows の例

```
rommon> file C:\tftp_directory\IDS-4215-K9-sys-1.1-a-5.0-1.img
```

ステップ 11 システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

(注) IDS-4215　は、イメージの再作成処理中に、数回リブートします。アップデート処理中は IDS-4215 の電源を切らないでください。電源を切ると、アップグレードが失敗する場合があります。

IDS-4215 BIOS および ROMMON のアップグレード

BIOS/ROMMON アップグレード ユーティリティ（IDS-4215-bios-5.1.7-rom-1.4.bin）は、IDS-4215 の BIOS をバージョン 5.1.7 に、ROMMON をバージョン 1.4 にアップグレードします。

IDS-4215 の BIOS および ROMMON をアップグレードするには、次の手順を実行します。

ステップ 1 BIOS ROMMON アップグレード ユーティリティ（IDS-4215-bios-5.1.7-rom-1.4.bin）を、IDS-4215 からアクセス可能な TFTP サーバの TFTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

(注) IDS-4215 イーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2 IDS-4215 をブートします。

リブートの間、IDS-4215 は、BIOS POST を実行します。POST の完了後、コンソールに「`Evaluating Run Options ...`」というメッセージが約 5 秒間表示されます。

ステップ 3 このメッセージが表示されている間に **Ctrl+R** キーを押して、ROMMON メニューを表示します。

コンソールの表示は次のようなものになります。

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.3 05/12/03 10:18:14.84
Compiled by ciscouser
Evaluating Run Options ...
Cisco ROMMON (1.2) #0: Mon May 12 10:21:46 MDT 2003
Platform IDS-4215
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01
Use ? for help.
rommon>
```

ステップ 4　必要に応じて、TFTP のダウンロードに使用するポート番号を変更します。

```
rommon> interface port_number
```

使用中のポートが rommon プロンプトの直前に示されます。`Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01` というテキストに示されているとおり、ポート 1（デフォルト ポート）が使用されています。

（注）　ポート 0（モニタリング ポート）およびポート 1（コマンド / コントロール ポート）は、シャーシの背面にラベルで表示されています。

ステップ 5　IDS-4215 上のローカル ポートの IP アドレスを指定します。

```
rommon> address ip_address
```

（注）　IDS-4215 に割り当てられているのと同じ IP アドレスを使用します。

ステップ 6　TFTP サーバの IP アドレスを指定します。

```
rommon> server ip_address
```

ステップ 7　ゲートウェイの IP アドレスを指定します。

```
rommon> gateway ip_address
```

ステップ 8　ローカルのイーサネット ポートから ping コマンドを使用することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 9　イメージのダウンロード元である TFTP ファイル サーバ上のファイル名を指定します。

```
rommon> file filename
```

例

```
rommon> file IDS-4215-bios-5.1.7-rom-1.4.bin
```

（注）　ファイルの場所の構文は、使用している TFTP のタイプに応じて異なります。上記の形式でうまくいかない場合は、システム管理者またはネットワーク管理者に適切な構文を問い合せてください。

ステップ 10 アップデート ユーティリティをダウンロードして実行します。

```
rommon> tftp
```

ステップ 11 アップデート プロンプトで **y** を入力すると、アップデートが実行されます。

IDS-4215 は、アップデートが終了するとリブートします。

注意 アップデート プロセスの間は IDS-4215 の電源を切らないでください。電源を切ると、アップグレードが失敗する場合があります。アップグレードが失敗した場合、IDS-4215 は使用できなくなり、RMA が必要になります。

IPS-4240 および IPS-4255 システム イメージのインストール

アプライアンス上の ROMMON を使用してシステム イメージをコンパクト フラッシュ デバイスに TFTP 転送することにより、IPS-4240 および IPS-4255 システム イメージをインストールできます。

（注） この手順は IPS-4240 用ですが、IPS-4255 にも適用できます。IPS-4255 用のシステム イメージには、ファイル名に「4255」が付いています。

IPS-4240 および IPS-4255 システム イメージをインストールするには、次の手順を実行します。

ステップ 1 IPS-4240 システム イメージ ファイル（IPS-4240-K9-sys-1.1-a-5.0-1.img）を、IPS-4240 からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

（注） IPS-4240 のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2 IPS-4240 をブートします。

コンソールの表示は次のようなものになります。

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  PCI-to-PCI Bridge
00  03  00   8086   257B  PCI-to-PCI Bridge
00  1C  00   8086   25AE  PCI-to-PCI Bridge
00  1D  00   8086   25A9  Serial Bus         11
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  PCI-to-PCI Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS-4240-K9
Management0/0

MAC Address: 0000.c0ff.ee01
```

ステップ 3　システムのブート中に、次のプロンプトで **Break** キーまたは **Esc** キーを押して、ブートを中断します。ブートを即座に開始するには、スペースバーを押します。

（注）　10 秒間 **Break** キーまたは **Esc** キーを押し続けます。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

システムが ROMMON モードになります。`rommon>` プロンプトが表示されます。

ステップ 4　現在のネットワーク設定を確認します。

```
rommon> set
```

設定済みのシステムでの出力は、次のようなものになります。

```
ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
      CONFIG=
```

変数には、次が定義されています。

- アドレス：IPS-4240 のローカル IP アドレス
- サーバ：アプリケーション イメージが保存されている TFTP サーバの IP アドレス
- ゲートウェイ：IPS-4240 によって使用されるゲートウェイ IP アドレス
- ポート：IPS-4240 管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのまま）
- イメージ：システム イメージ ファイル / パス名
- コンフィギュレーション：これらのプラットフォームでは使用されない

（注） ネットワーク接続を確立するには、すべての値が必要というわけではありません。アドレス、サーバ、ゲートウェイ、およびイメージの値は必須です。使用するローカル環境に必要な設定が不明の場合は、システム管理者に問い合せてください。

ステップ 5　必要に応じて、TFTP のダウンロードに使用するインターフェイスを変更します。

（注） TFTP ダウンロードに使用されるデフォルトのインターフェイスは Management0/0 です。これは、IDS-4240 の MGMT インターフェイスに対応します。

```
rommon> PORT=interface_name
```

ステップ 6　必要に応じて、IDS-4240 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注） IPS-4240 に割り当てられているのと同じ IP アドレスを使用します。

ステップ 7　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 8　必要に応じて、ゲートウェイの IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 9　ローカルのイーサネット ポートから次のいずれかのコマンドで ping することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスおよびファイル名を指定します。

```
rommon> IMAGE=path/file_name
```

UNIX の例：

```
rommon> IMAGE=/system_images/IPS-4240-K9-sys-4.1-4-S91.img
```

（注）　このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリを基準とした相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージには、IMAGE 指定にディレクトリ名もスラッシュも指定されていません。

Windows の例

```
rommon> IMAGE=C:\system_images\IPS-4240-K9-sys-4.1-4-S91.img
```

ステップ 11　**set** と入力し、**Enter** キーを押して、ネットワーク設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定を NVRAM に保存して、ブートしても維持されるようにできます。維持されるようにしないと、ROMMON からイメージをブートするたびに、この情報を入力する必要があります。

ステップ 12　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を避けるために、システム イメージのインストール中は、IPS-4240 の電源を切らないでください。

（注）　ネットワーク設定が正しい場合、指定されたイメージが IPS-4240 にダウンロードされてブートされます。必ず IPS-4240 イメージを使用してください。

リカバリ / アップグレード CD の使用方法

CD-ROM ドライブが装備されたアプライアンス（IDS-4210、IDS-4235、および IDS-4250 など）では、リカバリ / アップグレード CD が使用できます。リカバリ / アップグレード CD では、リカバリ パーティションおよびアプリケーション パーティションの両方のイメージが再作成されます。

注意　新しいソフトウェア イメージをインストールしようとしています。すべてのコンフィギュレーション データが上書きされます。

リカバリ / アップグレード CD でシステム イメージをインストールした後、**setup** コマンドを使用してアプライアンスを初期化する必要があります。コンフィギュレーション情報が必要です。この情報は、IDM を使用して診断レポートを生成することにより入手できます。

シグニチャ アップデートは、約 1 週間ごとに行われますが、必要な場合は、さらに頻繁に行われます。最新のシグニチャ アップデートは、アプライアンスに付属するリカバリ / アップグレード CD には組み込まれていません。システム イメージを復旧した後、最新のシグニチャ アップデートをダウンロードして適用します。

リカバリ / アップグレード CD でシステム イメージを復旧するには、次の手順を実行します。

ステップ 1　IDM からコンフィギュレーション情報を入手します。

- **a.** IDM にアクセスするには、アップグレード中のアプライアンスをブラウザで参照します。
- **b.** **Monitoring** > **Diagnostics** を選択します。

  Diagnostics パネルが表示されます。
- **c.** **Run Diagnostics** をクリックします。

  診断の実行には少し時間がかかる場合があります。
- **d.** **View Results** をクリックします。

  結果がレポートに表示されます。
- **e.** 診断レポートを保存するには、ブラウザの **Menu** > **Save As** を選択します。

ステップ 2　リカバリ / アップグレード CD を CD-ROM ドライブに挿入します。

ステップ 3　アプライアンスの電源を切って、再度電源を入れます。

ブート メニューが表示され、これに重要な注意事項とブート オプションがリストされています。

ステップ 4　キーボードからインストールする場合は **k**、シリアル接続からインストールする場合は **s** と入力します。

（注）　ファイルが CD からアプライアンスにコピーされている間、何もステータス メッセージが表示されないで、青い画面が数分間表示されます。

ステップ 5　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） 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 6　デフォルトの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。

（注） 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。

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 7　**setup** コマンドを入力して、アプライアンスを初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

ステップ 8　最新のサービス パックおよびシグニチャ アップデートをインストールします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

NM-CIDS システム イメージのインストール

この項では、NM-CIDS システム イメージのインストール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.17-23）
- NM-CIDS システム イメージのインストール（P.17-24）
- ブート ローダーのアップグレード（P.17-27）

概要

NM-CIDS のイメージを再作成するには、システム イメージ ファイル（IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.pkg）を使用します。システム イメージ ファイルを使用するには、事前に次のいずれかの方法でブート ローダーをアップグレードしておく必要があります。

（注） NM-CIDS ですでにバージョン 5.0 が動作している場合、ブート ローダーはアップグレードされています。ブート ローダーをアップグレードする必要があるのは、4.x から 5.0 にアップグレードする場合のみです。

- システム イメージをインストールする代わりに、**upgrade** コマンドで、メジャー アップグレード ファイル（IPS-K9-maj-5.0-1-S149.rpm.pkg）を使用して、4.x から 5.0 にアップグレードします。

  5.0 へのアップグレードでは、ブート ローダーも新規のブート ローダー ファイル（servicesengine-boot-1.0-17-1_dev.bin）でアップデートし、その後ハードディスク ドライブのイメージを新規イメージで再作成します。

  upgrade コマンドを使用することを推奨します。

- ブート ローダーを手動でアップグレードします。

  最初に古いヘルパー ファイルをブートする必要があります。ヘルパー メニューにブート ローダーをアップデートするオプションがあります。その後、ハードディスク ドライブをリブートしてイメージを再作成します。4.x のマニュアルを参照してください。

注意 5.0 のシステム イメージは、古いブート ローダーでは動作しません。

ヘルパーをブートして、5.0 システム イメージをロードする必要はなくなりました。5.0 システム イメージには、NM-CIDS のイメージの再作成に必要なものがすべて含まれています。

新しいブート ローダーは 4.x システム イメージで動作しますが、ロードするにはヘルパーをブートする必要があります。

注意 ブート ローダーをアップグレードする場合は、正しいファイルを使用していることを確認してください。NM-CIDS は、正しいファイルを使用していることを確認しません。間違ったファイルでアップグレードすると、リブートしたときに、NM-CIDS がアクセス不能になり、RMA を実行する必要があります。

NM-CIDS システム イメージのインストール

注意 5.0 システム イメージ ファイルをインストールするには、NM-CIDS ブート ローダーが 1.0.17-1 になっている必要があります。必要な場合、手順については、P.17-27 の「ブート ローダーのアップグレード」を参照してください。

（注） ブート ローダーには 10 分のタイムアウトがあります。そのため、低速の WAN リンクでのイメージの再作成は失敗します。この状況を避けるため、ブート ローダー ファイルをローカル TFTP サーバにダウンロードして、ローカル TFTP サーバから NM-CIDS のイメージを再作成します。

NM-CIDS のイメージを再作成するには、次の手順を実行します。

ステップ 1 NM-CIDS システム イメージ ファイル（IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.pkg）を、NM-CIDS からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

（注） NM-CIDS のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2 ルータにログインします。

ステップ 3　イネーブル モードに入ります。

```
router# enable
router(enable)#
```

ステップ 4　NM-CIDS に対してセッションを開始します。

```
router(enable)# service-module IDS-Sensor slot_number/0 session
```

(注)　NM-CIDS スロット番号を判別するには、**show configuration | include interface IDS-Sensor** コマンドを使用します。

ステップ 5　**Shift+Ctrl+6 X** キーを押してセッションを中断します。

`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、**Ctrl+6 X** キーを押してください。

ステップ 6　NM-CIDS をリセットします。

```
router(enable)# service-module IDS-Sensor slot_number/0 reset
```

reset コマンドを確認するよう求めるプロンプトが表示されます。

ステップ 7　**Enter** キーを押して確認します。

ステップ 8　**Enter** キーを押して、中断されたセッションを再開します。

バージョンが表示された後、ブート ローダーによってこのプロンプトが 15 秒間、表示されます。

```
Please enter '***' to change boot configuration:
```

ステップ 9　この 15 秒の遅延時間の間に ******* と入力します。

ブート ローダー プロンプトが表示されます。

ステップ 10　ブート ローダー コンフィギュレーションが表示されます。

```
ServicesEngine boot-loader> show config
```

注意　ブート ローダーのバージョンが 1.0.17-1 でない場合は、5.0 をインストールする前に、ブート ローダーをアップグレードする必要があります。手順については、P.17-27 の「ブート ローダーのアップグレード」を参照してください。

ステップ 11　ブート ローダー パラメータを設定します。

```
ServicesEngine boot-loader> config
```

ステップ 12 行ごとに各値のプロンプトが表示されます。

a. IP アドレスを指定します。これは、NM-CIDS 上の外部ファースト イーサネット ポートです。

これは、ネットワーク上の実際の IP アドレスである必要があります。

b. サブネット マスクを指定します。これは、NM-CIDS 上の外部ファースト イーサネット ポートです。

これは、ネットワーク上の実際の IP アドレスである必要があります。

c. TFTP サーバの IP アドレスを指定します。この TFTP サーバの IP アドレスから NM-CIDS システム イメージがダウンロードされます。

d. ゲートウェイ IP アドレスを指定します。これは、サブネット上のホスト用のデフォルト ゲートウェイの IP アドレスです。

e. デフォルト ヘルパー ファイルを指定します。これは、ブートするヘルパー イメージの名前です。

NM-CIDS ヘルパー ファイルは、ブート ヘルパー IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img です。

(注) 4.x には別のヘルパー ファイル NM-CIDS-K9-helper-1.0-1.bin がありますが、5.0 では、システム イメージ ファイルが、それ自体のヘルパー ファイルです。

f. イーサネット インターフェイスを指定します。イーサネット インターフェイスは常に **external** に設定されます。

g. デフォルト ブート デバイスを指定します。デフォルト ブート デバイスは常に **disk** に設定されます。

h. デフォルト ブート ローダーを指定します。デフォルト ブート ローダーは常に **primary** に設定されます。

変更を加えた場合、ブート ローダーはそれらを永続的に保存します。ブート ローダー コマンドのプロンプトが表示されます。

注意 次のステップで、NM-CIDS ハードディスク ドライブからすべてのデータが消去されます。

ステップ 13 システム イメージをブートします。

```
ServicesEngine boot-loader> boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img
```

ブート ローダーによって、TFTP サーバからシステム イメージをロードする際にスピニング行が表示されます。システム イメージは、ロードされると、ブートされます。システム イメージは、NM-CIDS 上に IPS 5.0(1) をインストールします。インストールが完了すると、NM-CIDS がリブートします。システムが、デフォルト設定に復元されます。ユーザ アカウントとパスワードは `cisco` に設定されます。

setup コマンドを使用して NM-CIDS を初期化する必要があります。手順については、P.3-3 の「センサーの初期化」を参照してください。

ブート ローダーのアップグレード

NM-CIDS ブート ローダーは、BIOS がその POST を完了すると、ただちに実行されます。最初に NM-CIDS に付属していたブート ローダーは 1.0.5 です。このバージョンは IPS 5.0(1) を起動できません。

（注） NM-CIDS を 5.0(1) にアップグレードするには、5.0(1) アップグレード パッケージ（IPS-K9-maj-5.0-1-S149.rpm.pkg）を適用することを推奨します。アップグレード パッケージが適用されると、コンフィギュレーションが移行されて、ブート ローダーがバージョン 1.0.17-1 にアップグレードされます。**upgrade** コマンドを使用する手順については、P.17-3 の「センサーのアップグレード」を参照してください。アップグレード ファイルで NM-CIDS をアップグレードすれば、将来は、システム アップグレードを実行する前に、ブート ローダーをアップグレードする必要がなくなります。

NM-CIDS システム イメージ（IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img）は、既存のコンフィギュレーションの移行もブート ローダーのアップグレードも行いません。したがって、まずブート ローダー バージョン 1.0.17-1 を手動でインストールする必要があります。

1.0.17-1 ブート ローダーは、1.0.5 ブート ローダーと下位互換性があります。これは、IDS 4.1 イメージをブート ローダーのバージョン 1.0.17-1 でブートできることを意味します。

（注） ブート ローダーには 10 分のタイムアウトがあります。そのため、低速の WAN リンクでのイメージの再作成は失敗します。この状況を避けるため、ブート ローダー ファイルをローカル TFTP サーバにダウンロードして、ローカル TFTP サーバから NM-CIDS のイメージを再作成します。

ブート ローダーをアップグレードするには、次の手順を実行します。

ステップ 1　ブート ローダー ファイル（servicesengine-boot-1.0-17-1_dev.bin）とヘルパー ファイル（NM-CIDS-K9-helper-1.0-1.bin）を、NM-CIDS からアクセスできる TFTP サーバの TFTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

（注） NM-CIDS のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　ルータにログインします。

ステップ 3　イネーブル モードに入ります。

```
router# enable
router(enable)#
```

ステップ 4　NM-CIDS に対してセッションを開始します。

```
router(enable)# service-module IDS-Sensor slot_number/0 session
```

NM-CIDS のスロット番号を判別するには、**show configuration | include interface IDS-Sensor** コマンドを使用します。

ステップ 5　**Shift+Ctrl+6 X** キーを押してセッションを中断します。

`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、**Ctrl+6 X** キーを押してください。

ステップ 6　NM-CIDS をリセットします。

```
router(enable)# service-module IDS-Sensor slot_number/0 reset
```

reset コマンドを確認するよう求めるプロンプトが表示されます。

ステップ 7　**Enter** キーを押して確認します。

ステップ 8　**Enter** キーを押して、中断されたセッションを再開します。

バージョンが表示された後、ブート ローダーによってこのプロンプトが 15 秒間、表示されます。

```
Please enter '***' to change boot configuration:
```

ステップ 9　この 15 秒の遅延時間の間に *** と入力します。ブート ローダー プロンプトが表示されます。

ステップ 10　ブート ローダー コンフィギュレーションが表示されます。

```
ServicesEngine boot-loader> show config
```

ステップ 11　ブート ローダー パラメータを設定します。

```
ServicesEngine boot-loader> config
```

ステップ 12　行ごとに各値のプロンプトが表示されます。

a. IP アドレスを指定します。これは、NM-CIDS 上の外部ファースト イーサネット ポートです。

これは、ネットワーク上の実際の IP アドレスである必要があります。

b. サブネット マスクを指定します。これは、NM-CIDS 上の外部ファースト イーサネット ポートです。

これは、ネットワーク上の実際の IP アドレスである必要があります。

c. TFTP サーバの IP アドレスを指定します。この TFTP サーバの IP アドレスから NM-CIDS システム イメージがダウンロードされます。

d. ゲートウェイ IP アドレスを指定します。これは、サブネット上のホスト用のデフォルト ゲートウェイの IP アドレスです。

e. デフォルト ヘルパー ファイルを指定します。これは、ブートするヘルパー イメージの名前です。

NM-CIDS ヘルパー ファイルは NM-CIDS-K9-helper-1.0-1.bin です。

f. イーサネット インターフェイスを指定します。イーサネット インターフェイスは常に **external** に設定されます。

g. デフォルト ブート デバイスを指定します。デフォルト ブート デバイスは常に **disk** に設定されます。

h. デフォルト ブート ローダーを指定します。デフォルト ブート ローダーは常に **primary** に設定されます。

変更を加えた場合、ブート ローダーはそれらを永続的に保存します。

ステップ 13 ヘルパー イメージをブートします。

```
ServicesEngine boot-loader># boot helper NM-CIDS-K9-helper-1.0-1.bin
```

ブート ローダーによって、TFTP サーバからヘルパー イメージをロードする際にスピニング行が表示されます。ヘルパーは、ロードされると、ブートされます。NM-CIDS ヘルパーは、起動されると、そのメイン メニューを表示します。

```
Cisco Systems, Inc.
Services engine helper utility for NM-CIDS
Version 1.0.17-1 [200305011547]
——-
Main menu
1 - Download application image and write to HDD
2 - Download bootloader and write to flash
3 - Display software version on HDD
4 - Display total RAM size
5 - Change file transfer method (currently secure shell)
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine
Selection [1234rh]:
```

ステップ 14 転送方法を選択します（デフォルトは SSH です）。

a. SSH の場合は、ステップ 15 に進みます。

b. TFTP の場合は、ステップ 16 と 17 に進みます。

ステップ 15 ブート ローダー イメージをダウンロードして、フラッシュに書き込みます。

a. **2** と入力します。

b. SSH サーバのユーザ名とパスワードを指定します。

c. SSH サーバの IP アドレスを入力します。

d. ルート ディレクトリからのブート ローダー イメージのフル パス名を入力します。

```
Selection [1234rh]:servicesengine-boot-1.0-17-1_dev.bin
Ready to begin
Are you sure? y/n
```

e. **y** を入力して続行します。

```
The operation was successful
```

`Selection [1234rh]:` プロンプトでメイン メニューに戻ります。ステップ 18 へ進みます。

ステップ 16 転送方法として TFTP を設定します。

a. **5** と入力します。

b. **2** を入力して、TFTP に切り替えます。

c. **r** を入力して、メイン メニューに戻ります。

ステップ 17 ブート ローダー イメージをダウンロードして、フラッシュに書き込みます。

a. **2** と入力します。

b. TFTP サーバの IP アドレスを入力します。

c. TFTP ルート ディレクトリからのパスを入力します。

```
Selection [1234rh]:servicesengine-boot-1.0-17-1_dev.bin
Ready to begin
Are you sure? y/n
```

d. **y** を入力して続行します。

`Selection [1234rh]:` プロンプトでメイン メニューに戻ります。ステップ 18 へ進みます。

ステップ 18 **r** を入力して、NM-CIDS をリブートします。

```
Selection [1234rh]: r
About to exit and reset Services Engine.
Are you sure? [y/N]
```

ステップ 19 **y** を入力して確認します。

これで、ブート ローダーがバージョン 1.0.17-1 にアップグレードされました。NM-CIDS システム イメージを今すぐインストールする場合にのみ続行します。

ステップ 20 NM-CIDS での BIOS POST が完了した後、次のメッセージが表示されたら、アスタリスクを 3 つ（***）入力します。

```
Please enter '***' to change boot configuration:
```

注意 次のステップで、NM-CIDS ハードディスク ドライブからすべてのデータが消去されます。

ブート ローダー プロンプトが表示されます。

ステップ 21 NM-CIDS システム イメージをブートします。

```
ServicesEngine boot-loader> boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img
```

ブート ローダーによって、TFTP サーバからシステム イメージをロードする際にスピニング行が表示されます。システム イメージは、ロードされると、ブートされます。システム イメージは、NM-CIDS 上に IPS 5.0(1) をインストールします。インストールが完了すると、NM-CIDS がリブートします。システムが、すべてのデフォルト設定に復元されます。ユーザ アカウントとパスワードは `cisco` に設定されます。

setup コマンドを使用して NM-CIDS を初期化する必要があります。手順については、P.3-3 の「センサーの初期化」を参照してください。

IDSM-2 システム イメージのインストール

IDSM-2 アプリケーション パーティションが使用できなくなった場合、メンテナンス パーティションからイメージを再作成できます。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した後、**setup** コマンドを使用して IDSM-2 を初期化する必要があります。手順については、P.3-3 の「センサーの初期化」を参照してください。

新しいメンテナンス パーティション イメージ ファイルがある場合は、アプリケーション パーティションからメンテナンス パーティションのイメージを再作成できます。

この項では、Catalyst ソフトウェアおよび Cisco IOS ソフトウェア用のアプリケーション パーティションとメンテナンス パーティションのイメージを再作成する方法について説明します。

この項では、次のトピックについて説明します。

- システム イメージのインストール（P.17-31）
- メンテナンス パーティションの設定（P.17-34）
- メンテナンス パーティションのアップグレード（P.17-42）

システム イメージのインストール

この項では、IDSM-2 システム イメージのインストール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。

- Catalyst ソフトウェア（P.17-31）
- Cisco IOS ソフトウェア（P.17-32）

Catalyst ソフトウェア

システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IDSM-2 システム イメージ ファイル（WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz）を、IDSM-2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 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 2　スイッチ CLI にログインします。

ステップ 3　IDSM-2 をメンテナンス パーティションにブートします。

```
cat6k> (enable) reset module_number cf:1
```

ステップ 4　メンテナンス パーティション CLI にログインします。

```
login: guest
Password: cisco
```

（注） IDSM-2　でメンテナンス　パーティションを設定する必要があります。手順については、P.17-34 の「メンテナンス パーティションの設定」を参照してください。

ステップ 5　システム イメージをインストールします。

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
```

ステップ 6　FTP サーバ パスワードを指定します。

アプリケーション パーティション ファイルがダウンロードされた後、続行するかどうかが尋ねられます。

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed
installing it [y|n]:
```

ステップ 7　**y** を入力して続行します。

アプリケーション パーティション ファイルがインストールされると、メンテナンス パーティション CLI に戻ります。

ステップ 8　メンテナンス パーティション CLI を終了してスイッチ CLI に戻ります。

ステップ 9　IDSM-2 をアプリケーション パーティションにリブートします。

```
cat6k> (enable) reset module_number hdd:1
```

ステップ 10　IDSM-2 がリブートされたら、ソフトウェア バージョンを確認します。

手順については、P.15-3 の「IDSM-2 取り付けの確認」を参照してください。

ステップ 11　アプリケーション パーティション CLI にログインして、IDSM-2 を初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

Cisco IOS ソフトウェア

システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IDSM-2 システム イメージ ファイル（WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz）を、IDSM-2 からアクセスできる TFTP サーバの TFTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 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 2　スイッチ CLI にログインします。

ステップ 3　IDSM-2 をメンテナンス パーティションにブートします。

```
switch# hw-module module module_number reset cf:1
```

ステップ 4　メンテナンス パーティション CLI に対してセッションを開始します。

```
switch# session slot slot_number processor 1
```

ステップ 5　メンテナンス パーティション CLI にログインします。

```
login: guest
Password: cisco
```

（注）　IDSM-2　でメンテナンス　パーティションを設定する必要があります。手順については、P.17-34 の「メンテナンス パーティションの設定」を参照してください。

ステップ 6　システム イメージをインストールします。

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_IP_address/directory_path/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
-install
```

ステップ 7　TFTP サーバ パスワードを指定します。

アプリケーション パーティション ファイルがダウンロードされた後、続行するかどうかが尋ねられます。

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

ステップ 8　**y** を入力して続行します。

アプリケーション パーティション ファイルがインストールされると、メンテナンス パーティション CLI に戻ります。

ステップ 9　メンテナンス パーティション CLI を終了してスイッチ CLI に戻ります。

ステップ 10　IDSM-2 をアプリケーション パーティションにリブートします。

```
switch# hw-module module module_number reset hdd:1
```

ステップ 11　IDSM-2 がオンラインで、ソフトウェア バージョンが正しく、ステータスが ok であることを確認します。

```
switch# show module module_number
```

ステップ 12 IDSM-2 アプリケーション パーティション CLI に対してセッションを開始します。

```
switch# session slot slot_number processor 1
```

ステップ 13 IDSM-2 を初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

メンテナンス パーティションの設定

この項では、IDSM-2 にメンテナンス パーティション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。

- Catalyst ソフトウェア（P.17-34）
- Cisco IOS ソフトウェア（P.17-38）

Catalyst ソフトウェア

IDSM-2 メンテナンス パーティションを設定するには、次の手順を実行します。

ステップ 1 スイッチ CLI にログインします。

ステップ 2 特権モードに入ります。

```
cat6k# enable
cat6k(enable)#
```

ステップ 3 IDSM-2 に対してセッションを開始します。

```
cat6k# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.

Cisco Maintenance image
```

（注） IDSM-2 メンテナンス パーティションに Telnet または SSH で接続することはできません。これには、スイッチ CLI からセッションを開始する必要があります。

ステップ 4 ユーザ **guest** とパスワード **cisco** でログインします。

（注） ゲスト パスワードの変更は可能ですが、お勧めしません。メンテナンス パーティションのゲスト パスワードを忘れて、何らかの理由で IDSM-2 アプリケーション パーティションにログインできない場合は、IDSM-2 に対して RMA を実行する必要があります。

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

ステップ 5　IDSM-2 メンテナンス パーティションのホスト コンフィギュレーションを表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 6　IDSM-2 メンテナンス パーティションのホスト コンフィギュレーション（IP アドレス、ゲートウェイ、ホスト名）をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

ステップ 7　メンテナンス パーティションのホスト コンフィギュレーションを設定します。

a.　IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b.　デフォルト ゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c.　ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

ステップ 8　メンテナンス パーティションのホスト コンフィギュレーションを表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 9　アプリケーション パーティションにインストールされているイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       5.0(1)
guest@idsm2.localdomain#
```

ステップ 10　メンテナンス パーティションのバージョンを確認します（BIOS バージョンを含む）。

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

ステップ 11　アプリケーション パーティションをアップグレードします。

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.g
z
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.g
z (unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.
gz is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

ステップ 12　**y** と入力してアップグレードを続行します。

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

ステップ 13 アップグレード ログを表示します。

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.
gz
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several
minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

ステップ 14 アップグレード ログをクリアします。

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

ステップ 15 アップグレード ログを表示します。

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

ステップ 16 別のコンピュータを ping します。

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

ステップ 17 IDSM-2 をリセットします。

（注） メンテナンス パーティションから **reset** コマンドを発行しているときにパーティションを指定することはできません。IDSM-2 は、ブート デバイス変数で指定されたパーティションにブートします。ブート デバイス変数がブランクである場合、IDSM-2 はアプリケーション パーティションにブートします。

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in
progress. Do not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!
cat6k> (enable)
```

Cisco IOS ソフトウェア

IDSM-2 メンテナンス パーティションを設定するには、次の手順を実行します。

ステップ 1 スイッチ CLI にログインします。

ステップ 2 IDSM-2 に対してセッションを開始します。

```
switch# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

（注） IDSM-2 メンテナンス パーティションに Telnet または SSH で接続することはできません。これには、スイッチ CLI からセッションを開始する必要があります。

ステップ 3　ユーザ **guest** とパスワード **cisco** でログインします。

（注）　ゲスト パスワードの変更は可能ですが、お勧めしません。メンテナンス パーティションのゲスト パスワードを忘れて、何らかの理由で IDSM-2 アプリケーション パーティションにログインできない場合は、IDSM-2 に対して RMA を実行する必要があります。

```
login: guest
password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

ステップ 4　メンテナンス パーティションのホスト コンフィギュレーションを表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 5　メンテナンス パーティションのホスト コンフィギュレーション（IP アドレス、ゲートウェイ、ホスト名）をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

ステップ 6　メンテナンス パーティションのホスト コンフィギュレーションを設定します。

a.　IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b.　デフォルト ゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c.　ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

ステップ 7　メンテナンス パーティションのホスト コンフィギュレーションを表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 8　アプリケーション パーティションにインストールされているイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       5.0(1)
guest@idsm2.localdomain#
```

ステップ 9　メンテナンス パーティションのバージョンを確認します（BIOS バージョンを含む）。

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

ステップ 10　アプリケーション パーティションをアップグレードします。

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.g
z
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.g
z (unknown size)
/tmp/upgrade.gz            [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.
gz is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

ステップ 11 **y** と入力してアップグレードを続行します。

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

ステップ 12 アップグレード ログを表示します。

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.
gz
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several
minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

ステップ 13 アップグレード ログをクリアします。

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

ステップ 14 アップグレード ログを表示します。

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

ステップ 15 別のコンピュータを ping します。

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

ステップ 16 IDSM-2 をリセットします。

（注） メンテナンス パーティションから **reset** コマンドを発行しているときにパーティションを指定することはできません。IDSM-2 は、ブート デバイス変数で指定されたパーティションにブートします。ブート デバイス変数がブランクである場合、IDSM-2 はアプリケーション パーティションにブートします。

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
switch#
```

メンテナンス パーティションのアップグレード

この項では、メンテナンス パーティションのアップグレード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。

- Catalyst ソフトウェア（P.17-42）
- Cisco IOS ソフトウェア（P.17-43）

Catalyst ソフトウェア

メンテナンス パーティションをアップグレードするには、次の手順を実行します。

ステップ 1 IDSM-2 メンテナンス パーティション ファイル（c6svc-mp.2-1-1.bin.gz）を、IDSM-2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 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 2　IDSM-2 CLI にログインします。

ステップ 3　コンフィギュレーション モードに入ります。

```
idsm2# configure terminal
```

ステップ 4　メンテナンス パーティションをアップグレードします。

```
idsm2# upgrade ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

続行するかどうかを要求されます。

ステップ 5　**y** を入力して続行します。

これで、メンテナンス パーティション ファイルがアップグレードされました。

Cisco IOS ソフトウェア

メンテナンス パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　IDSM-2 メンテナンス パーティション ファイル（c6svc-mp.2-1-1.bin.gz）を、IDSM-2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

Cisco.com でソフトウェアの場所を確認する方法については、P.18-2 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 2　スイッチ CLI にログインします。

ステップ 3　アプリケーション パーティション CLI に対してセッションを開始します。

```
switch# session slot slot_number processor 1
```

ステップ 4　コンフィギュレーション モードに入ります。

```
idsm2# configure terminal
```

ステップ 5　メンテナンス パーティションをアップグレードします。

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

ステップ 6　FTP サーバ パスワードを指定します。

```
Password: ********
```

続行を求めるプロンプトが表示されます。

```
Continue with upgrade?:
```

ステップ 7　**yes** を入力して続行します。

AIP SSM システム イメージのインストール

AIP SSM のイメージは、次のいずれかの方法で再作成できます。

- ASA から、**hw-module module 1 recover configure/boot** コマンドを使用します。
  次の手順を参照してください。
- **recover application-partition** コマンドを使用して、センサーの CLI からアプリケーション イメージを復旧します。
  手順については、P.17-11 の「アプリケーション パーティションの復旧」を参照してください。
- **upgrade** コマンドを使用して、センサーの CLI からリカバリ イメージをアップグレードします。
  手順については、P.17-5 の「リカバリ パーティションのアップグレード」を参照してください。

AIP SSM システム イメージをインストールするには、次の手順を実行します。

ステップ 1　ASA にログインします。

ステップ 2　イネーブル モードに入ります。

```
asa# enable
```

ステップ 3　AIP SSM 用のリカバリ設定値を設定します。

```
asa (enable)# hw-module module 1 recover configure
```

(注)　ディレクトリ　コンフィギュレーションでエラーが発生した場合は、**hw-module module 1 recover stop** コマンドを使用して、システム イメージの再作成を停止してから、コンフィギュレーションを訂正できます。

ステップ 4　システム イメージの TFTP URL を指定します。

```
Image URL [tftp://0.0.0.0/]:
```

例

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
```

ステップ 5　AIP SSM のコマンド / コントロール インターフェイスを指定します。

```
Port IP Address [0.0.0.0]:
```

例

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

ステップ 6　VLAN ID を 0 にしておきます。

```
VLAN ID [0]:
```

ステップ 7　AIP SSM のデフォルト ゲートウェイを指定します。

```
Gateway IP Address [0.0.0.0]:
```

例

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

ステップ 8　リカバリを実行します。

```
asa# hw-module module 1 recover boot
```

ステップ 9　リカバリが完了するまで、時々確認します。

(注)　ステータスは、リカバリ中は Recovery となり、イメージの再作成が完了すると Up になります。

```
asa# show module 1

Mod Card Type                                      Model              Serial No.
--- ---------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance           ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20    ASA-SSM-20         P1D000004F4

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#
```

(注)　リカバリ処理で発生する可能性のあるエラーをデバッグするには、**debug module-boot** コマンドを使用して、システム イメージの再作成処理のデバッグをイネーブルにします。

ステップ 10　AIP SSM に対してセッションを開始して、**setup** コマンドで AIP SSM を初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

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.18-2）
- IPS ソフトウェアのバージョン管理（P.18-4）
- Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード（P.18-7）
- 暗号化アクセスが可能な Cisco.com アカウントの申し込み（P.18-8）
- Cisco.com からのライセンス キーの取得（P.18-9）
- Cisco Intrusion Prevention Alert Center（P.18-15）
- Cisco IPS のアクティブなアップデート通知（P.18-16）
- Network Security Database（P.18-17）
- IPS ドキュメントへのアクセス（P.18-18）

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、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.18-8 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.18-9 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 にアクセスします。

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.18-4 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、アップデート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、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

（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.18-4）
- 5.x ソフトウェア リリースの例（P.18-6）

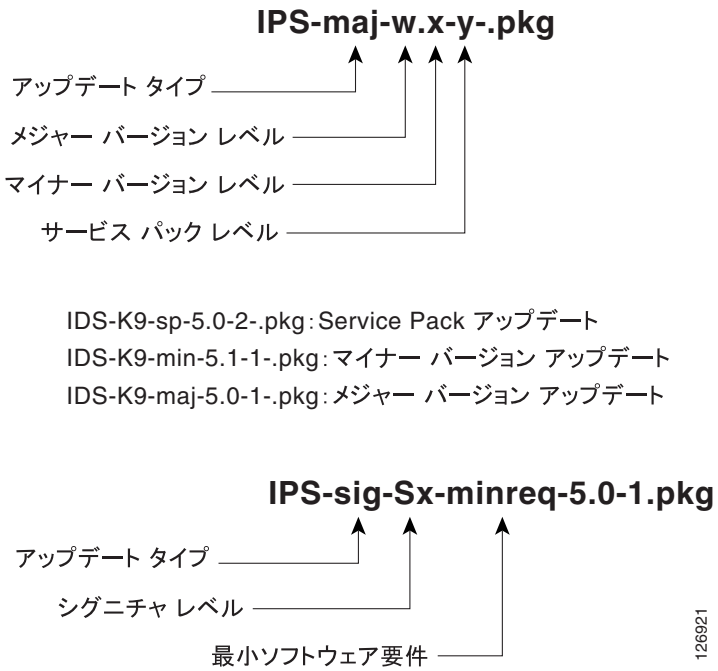
IPS ソフトウェア イメージの命名規則

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 18-1 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 18-1　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　リリースをリストしたテーブルについては、P.18-6 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、および AIP SSM 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 ファイルが存在します。

- システム イメージ ファイル（IDS-4215、IPS-4240、IPS-4255、NM-CIDS、IDSM-2、および AIP SSM）：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 18-1 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.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

表 18-1　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	パッチ	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 18-2 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 18-2　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.18-2 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、P.17-3 の「センサーのアップグレード」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.17-7 の「自動アップグレードの設定」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、P.17-22 の「リカバリ / アップグレード CD の使用方法」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、P.17-11 の「アプリケーション パーティションの復旧」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、P.17-13 の「IDS-4215 システム イメージのインストール」および P.17-18 の「IPS-4240 および IPS-4255 システム イメージのインストール」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、P.17-23 の「NM-CIDS システム イメージのインストール」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、P.17-31 の「IDSM-2 システム イメージのインストール」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、P.17-44 の「AIP SSM システム イメージのインストール」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について説明します。この項では、次のトピックについて説明します。

- 概要（P.18-9）
- IPS 製品のサービス プログラム（P.18-9）
- ライセンス キーの入手とインストール（P.18-11）

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.18-9 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 キーも入手できます。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。

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.18-11 の「ライセンス キーの入手とインストール」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、または 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

IPS 製品には、Cisco Services for IPS サービス契約が必要です。これにより、ライセンス キーをダウンロードして、最新の IPS シグニチャ アップデートが入手できます。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 の追加が必要になり、ASA-SSM-AIP-10-K9 を購入した場合は、この時点で 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.18-11 の「ライセンス キーの入手とインストール」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。

ライセンス キーの入手とインストール

この項では、IDM または CLI を使用してライセンス キーを入手し、インストール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。

- IDM の使用方法（P.18-11）
- CLI の使用方法（P.18-12）

IDM の使用方法

ライセンス キーを入手して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。ライセンスをすでにインストールしている場合は、必要に応じて、**Download** をクリックしてライセンスを保存できます。

ステップ 3　次のいずれかを実行してライセンス キーを取得します。

- Cisco.com 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。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、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.4-36 の「既知のホスト リストへのホストの追加」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.4-42 の「TLS 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。

（注） ライセンス キーを適用する前に、Cisco Services for IPS サービス契約が必要です。詳細については、P.18-9 の「IPS 製品のサービス プログラム」を参照してください。

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 5.1(1)S182.0

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-5.1-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.1(1)S182


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.18-16 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.18-17 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/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

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 のファイル構造（P.A-39）
- IPS 5.1 アプリケーションの要約（P.A-40）

システムの概要

Cisco IPS ソフトウェアは、アプライアンスおよびモジュールという 2 つのプラットフォームにインストールできます（現在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）。

この項では、次のトピックについて説明します。

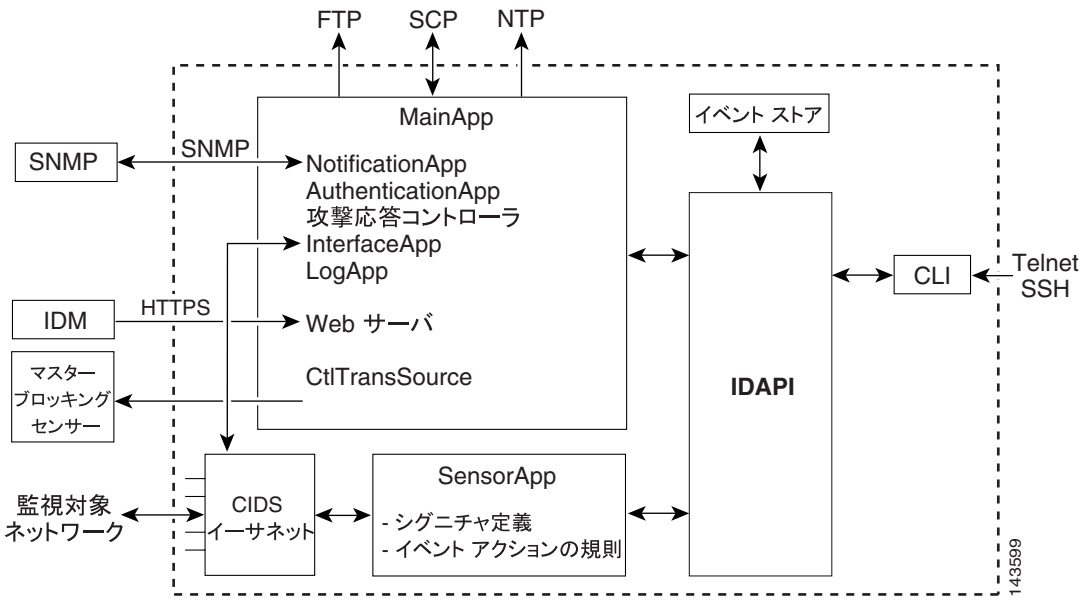
- システムの設計（P.A-2）
- IPS 5.1 の新機能（P.A-4）
- ユーザによる対話操作（P.A-4）
- セキュリティ機能（P.A-5）

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 に、システムの設計を示します。

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、センサーの全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したり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（以前の Network Access Controller）、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。

表 A-1　IPS イベントの例（続き）

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
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

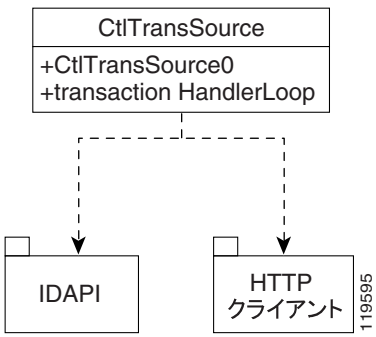
CtlTransSource

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。

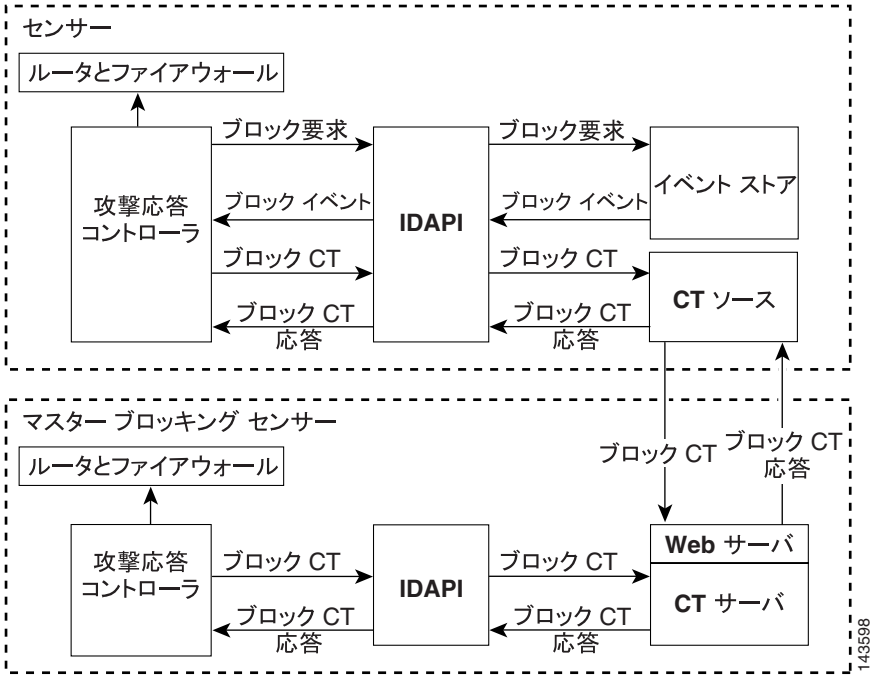
この項では、次のトピックについて説明します。

- ARC について（P.A-12）
- ARC の機能（P.A-13）
- サポートされているブロッキング デバイス（P.A-15）
- ACL と VACL（P.A-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.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」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 を適用したりする（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したり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 アドレスを表示したりする場合

  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したり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たりする場合があります。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.13-22 の「テクニカル サポート情報の表示」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.13-5 の「イベントの表示」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 ロギングのイネーブル化」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。Normalizer 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.6-9 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。

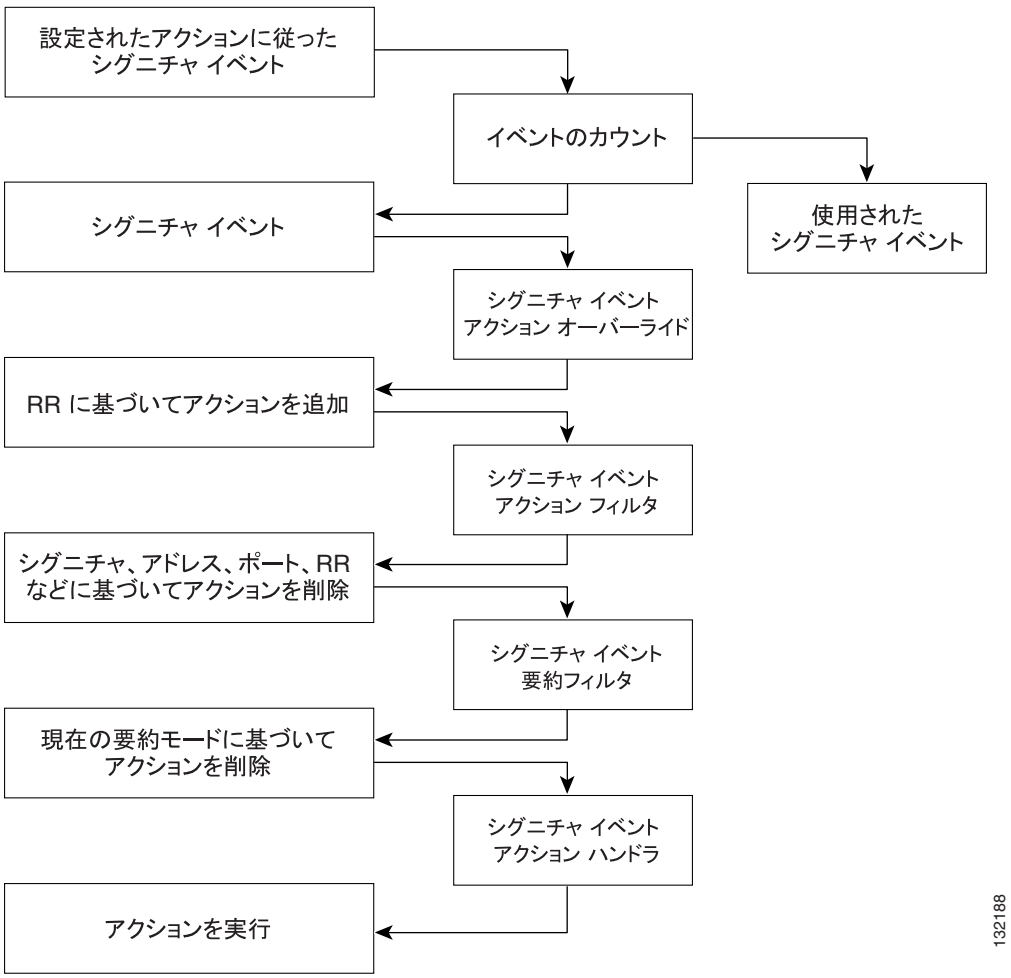
  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート
  - 被害先のアドレス
  - 被害先のポート
  - RR しきい値の範囲
  - 削除するアクション
  - シーケンス識別子（オプション）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット

- 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 に、SEAP を使用したシグニチャ イベントの論理フローと、このイベントに関してアクションで実行される動作を示します。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限り、すべてのパケットは変更されずに転送されます。TCP の正規化により、一部のパケットが適切なカバレッジを確保するために遅延することがあります。ポリシー違反が発生すると、SensorApp はアクションの設定を許可します。パケットの拒否、フローの拒否、攻撃者の拒否など、追加のアクションがインライン モードで使用できるようになっています。

  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ないはずです。上書きが発生する場合は、誰かがセキュリティ ポリシーを意図的に回避しようとしているか、TCP スタックの実装が破損しています。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。

この項では、次のトピックについて説明します。

- 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 アカウントの作成手順については、P.4-16 の「サービス アカウントの作成」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。これにより、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

- 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）

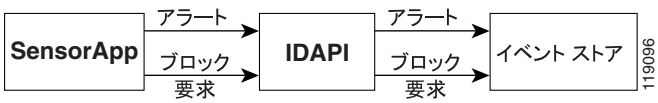
IDAPI

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。

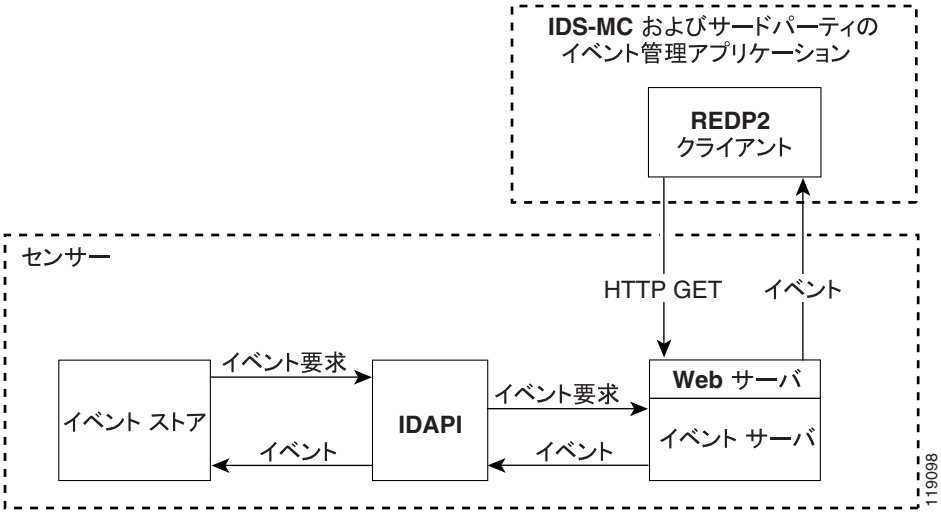
RDEP2 は、業界標準の HTTP、TLS および SSL、および XML を使用して、RDEP2 エージェント間に標準化されたインターフェイスを提供します。RDEP2 プロトコルは HTTP 1.1 プロトコルのサブセットです。すべての RDEP2 メッセージは、有効な HTTP 1.1 メッセージです。RDEP2 は、HTTP のメッセージ形式とメッセージ交換プロトコルを使用して、RDEP2 エージェント間でメッセージを交換します。

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。

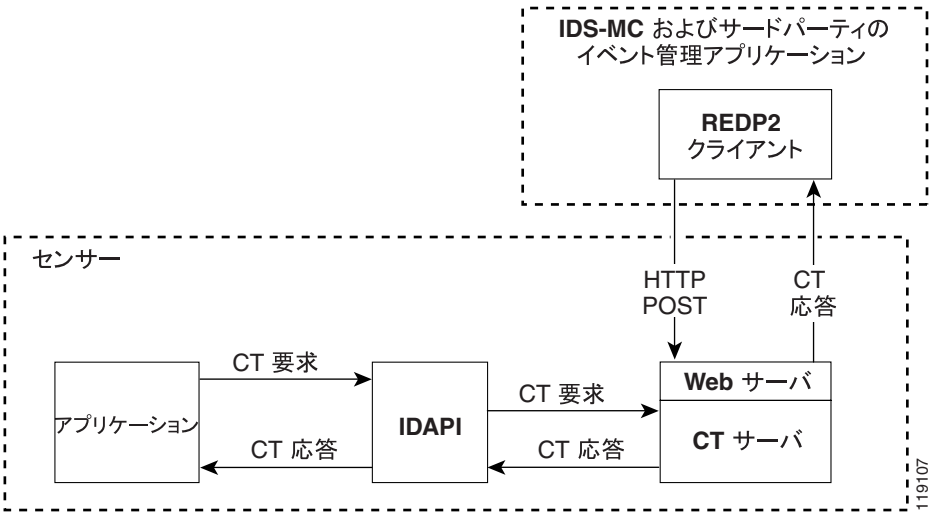
リモート アプリケーションは、RDEP2 を使用してセンサーからイベントを取得します。リモート クライアントが RDEP2 のイベント要求をセンサーの Web サーバに送信すると、Web サーバがそれをイベント サーバに渡します。イベント サーバは IDAPI を使用してイベント ストアをクエリーし、結果を戻します。図 A-6 に、RDEP2 を使用してセンサーからイベントを取得するリモート アプリケーションを示します。

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 を経由して該当するアプリケーションに制御トランザクションを渡し、アプリケーションの応答を待ち、その後結果を返します。図 A-7 に、RDEP2 を使用してコマンドをセンサーに送信するリモート アプリケーションを示します。

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したり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 のファイル構造

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を要約して示します。

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。

表 A-2　アプリケーションの要約（続き）

アプリケーション	説明
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で構成されています。各エンジンにはパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。

（注） 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 シグニチャを設定する方法の詳細については、P.7-15 の「AIC シグニチャの設定」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。そうすることで、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.6-23 の「拒否された攻撃者リストのモニタリングとクリア」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.6-21 の「汎用設定」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 10 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 10 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、第 6 章「汎用設定」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 10 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 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 11 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。事前定義済む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 シグニチャの設定手順については、P.7-15 の「AIC シグニチャの設定」を参照してください。カスタム AIC シグニチャの例については、P.7-43 の「AIC MIME タイプ シグニチャ」を参照してください。

表 B-4 に、AIC HTTP エンジンに固有のパラメータを示します。

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 に、AIC FTP エンジンに固有のパラメータを示します。

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-12）

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 に、Atomic ARP エンジンに固有のパラメータを示します。

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 に、Atomic IP エンジンに固有のパラメータを示します。

表 B-7　Atomic IP エンジンのパラメータ

パラメータ	説明
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 に、Flood Host エンジンに固有のパラメータを示します。

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数のしきい値。	0 ～ 65535[1]
icmp-type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535
dst-ports	UDP プロトコルを選択した場合の宛先ポートを指定します。	0 ～ 65535[2] a-b[,c-d]
src-ports	UDP プロトコルを選択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数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 に、Flood Net エンジンに固有のパラメータを示します。

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数のしきい値。	0 ～ 65535[1]
sampling-interval	トラフィックをサンプリングする間隔。	1 ～ 3600
icmp-type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535

1. 秒あたりのパケット数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.6-2 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 に、Meta エンジンに固有のパラメータを示します。

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 シグニチャの例については、P.7-39 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 に、Multi String エンジンに固有のパラメータを示します。

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：前回の一致か所から、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ないはずです。上書きが発生する場合は、誰かがセキュリティ ポリシーを意図的に回避しようとしているか、TCP スタックの実装が破損しています。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 シグニチャの設定手順については、P.7-23 の「IP フラグメント再構成」および P.7-26 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 に、Normalizer エンジンに固有のパラメータを示します。

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。

この項では、次のトピックについて説明します。

- 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 に、Service DNS エンジンに固有のパラメータを示します。

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 に、Service FTP エンジンに固有のパラメータを示します。

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 に、Service Generic エンジンに固有のパラメータを示します。

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-22）

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 に、Service H225 エンジンに固有のパラメータを示します。

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

表 B-16　Service H.225 エンジンのパラメータ（続き）

パラメータ	説明	値
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お勧めします。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

カスタム Service HTTP シグニチャの例は、P.7-36 の「Service HTTP シグニチャの例」を参照してください。

表 B-17 に、Service HTTP エンジンに固有のパラメータを示します。

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
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

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-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][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 に、Service IDENT エンジンに固有のパラメータを示します。

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 に、Service MSRPC エンジンに固有のパラメータを示します。

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 に、Service MSSQL エンジンに固有のパラメータを示します。

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 に、Service NTP エンジンに固有のパラメータを示します。

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 に、Service RPC エンジンに固有のパラメータを示します。

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 に、Service SMB エンジンに固有のパラメータを示します。

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
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

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-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
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

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
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 に、Service SNMP エンジンに固有のパラメータを示します。

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。	—
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 に、Service SSH エンジンに固有のパラメータを示します。

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 オーバーフローが発生します。 • user-length：ユーザ長 SSH 検査： 　– length：鍵がこれより大きくなると、RSAREF オーバーフローが発生します。	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たりすることができます。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 に、State エンジンに固有のパラメータを示します。

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-36）

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.7-32 の「String TCP シグニチャの例」を参照してください。

表 B-27 に、String ICMP エンジンに固有のパラメータを示します。

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.7-32 の「String TCP シグニチャの例」を参照してください。

表 B-28 に、String TCP エンジンに固有のパラメータを示します。

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.7-32 の「String TCP シグニチャの例」を参照してください。

表 B-29 に、String UDP エンジンに固有のパラメータを示します。

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]

表 B-29　String UDP エンジン（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。

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 に、Sweep エンジンに固有のパラメータを示します。

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 に、Traffic ICMP エンジンに固有のパラメータを示します。

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-5）
- 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、P.12-22 の「バックアップ コンフィギュレーション ファイルの作成および使用」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、P.12-20 の「リモート サーバを使用したコンフィギュレーション ファイルのコピーおよび復元」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、P.4-16 の「サービス アカウントの作成」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、P.12-22 の「バックアップ コンフィギュレーション ファイルの作成および使用」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。センサーの現在のユーザのリストを入手する手順については、P.4-19 の「ユーザのステータスの表示」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。

   アプライアンスおよびモジュールに対する手順については、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

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.3-3 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 バージョンの取得と、そのインストール方法の詳細については、P.18-2 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、P.12-22 の「バックアップ コンフィギュレーション ファイルの作成および使用」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.4-36 の「既知のホスト リストへのホストの追加」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.4-14 の「ユーザ パラメータの設定」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、P.4-16 の「サービス アカウントの作成」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、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

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。

この項では、次のトピックについて説明します。

- 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 サーバに同期していることの確認（P.C-34）
- TCP リセットがシグニチャに対して実行されない（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 でセンサー 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 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 でセンサー 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 をイネーブルおよびディセーブルにする手順は、P.4-5 の「Telnet のイネーブル化とディセーブル化」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。

CLI セッションをセンサーで直接開くためのさまざまな方法については、第 2 章「センサーへのログイン」を参照してください。

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、ステータス行が `Media Type = TX` の、リスト内のインターフェイスです。Link Status が `Down` の場合はステップ 3 に進みます。Link Status が `Up` の場合はステップ 5 に進みます。

ステップ 3　センサーの 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、P.4-4 の「IP アドレス、ネットマスク、およびゲートウェイの変更」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、P.4-6 の「アクセス リストの変更」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、P.4-6 の「アクセス リストの変更」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 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*』内の使用するセンサーに関する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.3-3 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）
- アラートを表示できない（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クリーン アップ（P.C-18）
- IDS-4250-XL の不良メモリ（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 からダウンロードしてください。手順については、P.18-2 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*』内の使用するアプライアンスに関する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*』内の IDSM-2 に関する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、第 5 章「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
```

アラートを表示できない

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。

センサーを適切に取り付けるための詳細については、『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』内の使用するセンサーに関係する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クリーン アップ

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。

メモリに問題があるかどうかに関して IDS-4250-XL をチェック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の確認（P.C-20）
- ARC 接続がアクティブであることの確認（P.C-21）
- デバイス アクセスの問題（P.C-22）
- ネットワーク デバイス上のインターフェイスおよび方向の確認（P.C-24）
- ネットワーク デバイスへの SSH 接続のイネーブル化（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 コンフィギュレーションの確認（P.C-26）

ブロッキングのトラブルシューティング

ARC を設定すると、**show version** コマンドを使用して ARC が正しく動作してい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 で名前が変更されましたが、IDM および CLI ではまだ、Network Access Controller、**nac**、および **network-access** として表示されます。

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の確認」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-21 の「ARC 接続がアクティブであることの確認」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 コンフィギュレーションの確認」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の確認

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 によって `Not Running` と表示される場合、ARC に障害が発生しています。TAC に連絡します。

ARC 接続がアクティブであることの確認

ARC 統計情報の State が `Active` でない場合は、問題があります。

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 からダウンロードしてください。手順については、P.18-2 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 デバイス上のインターフェイスおよび方向の確認」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 接続のイネーブル化」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 デバイス上のインターフェイスおよび方向の確認」を参照してください。

デバイス アクセスの問題

ARC が、管理しているデバイスにアクセスできないことがあります。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 デバイス上のインターフェイスおよび方向の確認」を参照してください。

ネットワーク デバイス上のインターフェイスおよび方向の確認

制御対象デバイスそれぞれのインターフェイスおよび方向が正しいことを確認するには、手動ブロックを偽のホストに送信して、ルータの ACL にブロックされたアドレスの拒否エントリが存在するかどうかをチェックします。

(注)　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　ステップ 1 ～ 4（ただし、ステップ 2 ではコマンドの前に **no** を指定する）を繰り返して、手動ブロックを削除します。

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

ネットワーク デバイスへの SSH 接続のイネーブル化

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ためのプロンプトが表示されたら、**yes** を入力します。

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、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かどうかをチェックします。

特定のシグニチャに対してブロッキングが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）　アラートを受信する場合は、イベント アクションを設定するたびに、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 コンフィギュレーションの確認

マスター ブロッキング センサーが正しくセットアップされていることを確認したり、正しく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には、**show statistics network-access** コマンドを使用します。リモート マスター ブロッキング センサーが 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.10-35 の「センサーをマスター ブロッキング センサーとして使用するための設定」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 ホストの CLI にログインし、**show statistics network-access** コマンドを使用して、ブロックが、マスター ブロッキング センサー ARC の統計情報にも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提案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。

この項では、次のトピックについて説明します。

- デバッグ ロギングのイネーブル化（P.C-28）
- ゾーン名（P.C-33）
- cidLog メッセージの SysLog への転送（P.C-33）

デバッグ ロギングのイネーブル化

注意　デバッグ ロギングをイネーブル化するとパフォーマンスに重大な影響があるので、TAC によって指示された場合に限り行ってください。

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)#
```

各ゾーン名が指す内容のリストについては、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。

cidLog メッセージの SysLog への転送

cidLog メッセージを syslog に転送すると役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. Set [logApp] `enabled=false`

`enabled=false` がデフォルトなので、`enabled=true` をコメント アウトします。

b. Set [drain/main] `type=syslog`

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 サーバに同期していることの確認

IPS 5.1 では、無効な NTP 鍵の値や 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 `Not Synchronized` のままの場合は、NTP サーバ管理者に問い合せて、NTP サーバが正しく設定されていることを確認します。

TCP リセットがシグニチャに対して実行されない

リセットするようにイベント アクションを設定していない場合、特定のシグニチャに対して TCP リセットは実行されません。

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

この項は、ソフトウェア アップグレードのトラブルシューティングに役立ちます。取り上げる事項は次のとおりです。

- ソフトウェア アップグレード中に IDS-4235 および IDS-4250 が停止する（P.C-37）
- 適用するアップデートとその前提条件（P.C-37）
- 自動アップデートでの問題（P.C-38）
- センサーに保存されているアップデートによるセンサーのアップデート（P.C-39）

ソフトウェア アップグレード中に IDS-4235 および IDS-4250 が停止する

IDS-4235 および IDS-4250 の BIOS が A03 の場合、最新の IPS ソフトウェアを適用する前に、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 アップグレード処理中にアプライアンスが停止します。BIOS のアップグレード手順については、『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』内の「Upgrading the BIOS」を参照してください。最新の IPS ソフトウェアの適用手順については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

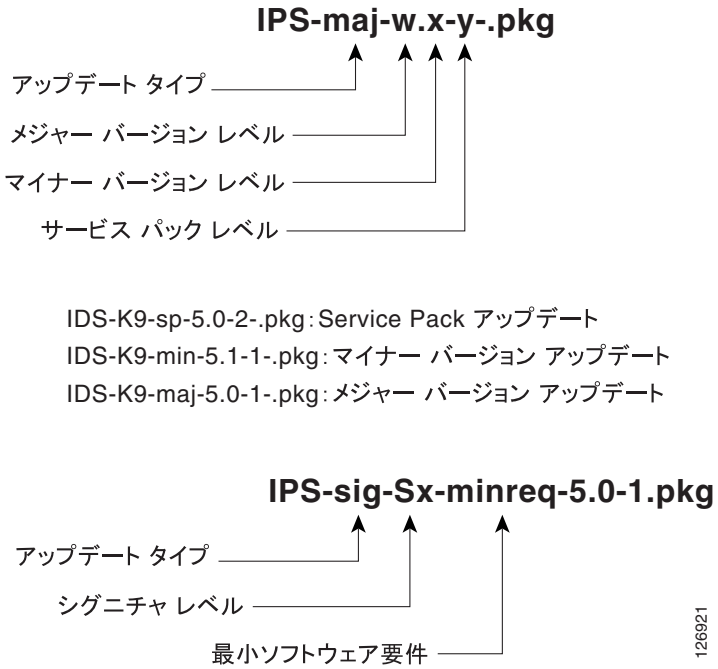
適用するアップデートとその前提条件

ソフトウェアの正しいサービス パックおよびマイナー バージョンとメジャー バージョンが必要です。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 に、IPS ソフトウェア ファイル名の解釈方法を示します。

図 C-1　IPS ソフトウェアのファイル名



自動アップデートでの問題

次のリストに、自動アップデートのトラブルシューティングに関する提案を示します。

- 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、P.4-16 の「サービス アカウントの作成」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、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。
  - 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.4-36 の「既知のホスト リストへのホストの追加」を参照してください。

自動アップデートを試行する前に、手動で **upgrade** コマンドを試行してください。**upgrade** コマンドが動作して、自動アップデートが動作しない場合は、次の操作を試してください。

- センサーの IPS ソフトウェア バージョンを判別します（手順については、P.13-23 の「バージョン情報の表示」を参照）。

  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によるセンサーのアップデート

アップデート パッケージをセンサー上の /var ディレクトリに保存して、必要な場合、そこから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.18-2 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。

この項では、次のトピックについて説明します。

- Java プラグインのメモリ サイズの増加（P.C-41）
- IDM を起動できない：Java アプレットをロードできない（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-43）
- IDM、リモート マネージャ、またはセンシング 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）
- アラートを表示しないシグニチャ（P.C-45）

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、ブラウザに 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。メモリ不足は、**Refresh** をクリックした場合にも発生することがあります。メモリ不足が発生すると常に、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。

この項では、次のトピックについて説明します。

- Windows での Java プラグイン（P.C-41）
- Linux および Solaris での Java 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 用の Windows での 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` と入力して、**OK** をクリックます。

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 Java プラグイン

Linux および Solaris で 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. **Advanced** 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` と入力して、**OK** をクリックます。

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 アプレットをロードできない

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、複数の Java プラグイン（1.4.*x* または 1.3.*x*、あるいは両方）が IDM を起動するマシンにインストールされている場合に発生することがあります。

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　ava 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、またはセンシング 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、またはセンシング インターフェイスはセンサーにアクセスできないが、ユーザが SSH または Telnet を使用して（使用可能な場合）センサーの CLI にアクセスできる場合は、次の手順を実行します。

（注）センサーで Telnet をイネーブルおよびディセーブルにする手順は、P.4-5 の「Telnet のイネーブル化とディセーブル化」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、P.4-12 の「Web サーバ設定の変更」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、P.4-12 の「Web サーバ設定の変更」を参照してください。

アラートを表示しないシグニチャ

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 を選択した場合に、後で別のイベント アクションを追加して、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。

この項では、次のトピックについて説明します。

- IDSM-2 の問題の診断（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（P.C-47）
- ステータス LED はオンであるが、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）
- IDSM-2 へのシリアル ケーブルの接続（P.C-53）

IDSM-2 の問題の診断

IDSM-2 の問題を診断するには、次のリストを使用します。

- 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。

  メモリに問題があるかどうかに関して IDSM-2 をチェック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 / 書き込み動作中に、コンソールに I/O エラーが表示される（**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。

  詳細については、P.15-5 の「サポートされている IDSM-2 の設定」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

次の switch コマンドが、IDSM-2 のトラブルシューティングに役立ちます。

- **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

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

```
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

```
switch#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
switch#
```

（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。

```
switch# set module power up module_number
```

ステータス LED はオンであるが、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 がスイッチにしっかりと接続されていることを確認してください。

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、第 17 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

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 に置か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、P.15-6 の「IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定」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。

IDSM-2 へのシリアル ケーブルの接続

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ができます。これにより、スイッチおよびモジュール ネットワーク インターフェイスをバイパスできます。

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#
```

AIP SSM が動作していることが出力に示されます。ステータスが Down の場合、**hw-module module 1 reset** コマンドを使用して AIP SSM をリセットできます。

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa(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 の復旧で問題がある場合は、**debug module-boot** コマンドを使用して、AIP SSM ブートの出力を確認します。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** コマンドを再度使用して AIP SSM を復旧します。

```
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

問題が発生したときに、情報を収集してセンサーの状態を診断するには、次の CLI コマンドおよびスクリプトが使用できます。すべてのセンサーの情報を収集するには、**show tech-support** コマンドが使用できます。また、特定の情報については、この項にリストされているその他の個別のコマンドが使用できます。

この項では、次のトピックについて説明します。

- 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-62）
- インターフェイス情報（P.C-71）
- イベント情報（P.C-72）
- cidDump スクリプト（P.C-77）
- Cisco FTP サイトでのファイルのアップロードおよびアクセス（P.C-77）

テクニカル サポート情報

show tech-support コマンドは、センサーのステータス情報およびコンフィギュレーション情報をすべて取り込む場合に役立ちます。

この項では、次のトピックについて説明します。

- 概要（P.C-56）
- テクニカル サポート情報の表示（P.C-57）
- テクニカル サポート コマンドの出力（P.C-58）

概要

show tech-support コマンドは、センサー上のすべてのステータス情報およびコンフィギュレーション情報を取り込み、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 情報を組み込みます。出力が 1 MB を超えるなど、大きい可能性があります。出力をリモート 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 に連絡する前に、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

システム情報を画面に表示するか、または特定の URL に送信するには、**show tech-support** [**page**] [**password**] [**destination-url** *destination-url*] コマンドを使用します。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。

テクニカル サポート コマンドの出力

show tech-support コマンドの出力例を次に示します。

（注） 次の出力例は、コマンドの最初の部分で、インターフェイス、Network Access Controller、および cidDump サービスの情報が示されています。

```
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

show version コマンドは、センサーの一般的な健全性の確立に役立ちます。

この項では、次のトピックについて説明します。

- 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て、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によって、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

インストール済みのすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで動作中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の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。

バージョンおよび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** コマンドまたは **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

show statistics コマンドは、センサーのサービスの状態の検査に役立ちます。

この項では、次のトピックについて説明します。

- 概要（P.C-62）
- 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
- Attack Response（以前は Network Access と呼ばれていました）
- 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 から同じ情報が収集できます。

統計情報の表示

仮想センサーの統計情報を表示するには、**show statistics virtual-sensor** [**clear**] コマンドを使用します。各センサー アプリケーションごとに統計情報を生成するには、**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。

インターフェイス情報

show interfaces コマンドは、センシング インターフェイスと、コマンド / コントロール インターフェイスの情報の収集に役立ちます。

この項では、次のトピックについて説明します。

- 概要（P.C-71）
- インターフェイス コマンド出力（P.C-72）

概要

show interfaces コマンドで次の情報が表示できます。

- 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。あるいは、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*）およびセンシング インターフェイス（**show interfaces** *interface_name*）の統計情報が表示できます。

インターフェイス コマンド出力

次の例は、**show interfaces** コマンドの出力を示します。

```
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 = 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 コマンドを使用すると、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が表示できます。

この項では、次のトピックについて説明します。

- 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

show events コマンドは、Event Viewer や Security Monitor でイベントが表示されないというイベント キャプチャの問題をトラブルシューティングする場合に役立ちます。**show events** コマンドを使用すると、センサーで生成されているイベントを判別して、イベントが生成されていて、障害がモニタ側に存在することを確認できます。

イベント ストアからすべてのイベントをクリアするには、**clear events** コマンドを使用します。

次は、**show events** コマンドのパラメータです。

```
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

イベント ストアからイベントを表示するには、**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**：Attack Response Controller（ARC）要求を表示します。

（注） ARC は、以前は Network Access Controller（NAC）と呼ばれていました。この名前の変更は、IDM および CLI for IPS 5.1 で完全には反映されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、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。イベントを表示して待機している状態は、Ctrl+C キーを押して終了するまで継続します。

イベント ストアから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 ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者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　サービス アカウント パスワードを使用して root に切り替えます。

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 サイトでのファイルのアップロードおよびアクセス」を参照してください。

Cisco FTP サイトでのファイルのアップロードおよびアクセス

大規模ファイル（たとえば、cidDump.html、show tech-support コマンドの出力、コアなど）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　**put** コマンドを使用して、ファイルをアップロードします。

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 ビット鍵を基盤とする強化暗号化方式。

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。

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単方向のハッシュ 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、他のソフトウェアやインターフェイスをシャットダウンしたりせずに、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、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。Normalizer 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鍵が使用される場合を対称と言います。暗号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で構成されています。各エンジンには、許容される範囲または値のセットを持つ正当な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　ARC 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

access-list コマンド　4-6
ACL
　Post-Block　10-26, 10-27
　Pre-Block　10-26, 10-27
　説明　10-3
AIC
　エンジン　7-15
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
　hw-module module 1 recover　14-7
　hw-module module 1 reset　14-7
　hw-module module 1 shutdown　14-7
　IPS トラフィックの検査　14-4
　session コマンド　2-9
　show module コマンド　14-3
　インライン モード　14-4
　混合モード　14-4
　時刻源　4-23
　初期化の確認　14-3
　タスクのシーケンス　14-2
　トラフィックの送信　14-4
　復旧　C-55
　モード　14-4
　リセット　C-54
　ログイン　2-9
alert-frequency コマンド　7-6
alert-severity コマンド　7-8
allow-sensor-block コマンド　10-8
application-policy コマンド　7-16
ARC
　ACL　10-26, 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　10-4
　インターフェイス　A-14
　インターフェイスの確認　C-24
　機能　10-2, A-12, A-13
　最大ブロック　10-2, 10-6
　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　10-3
　設計　10-2, 10-6
　説明　A-3
　前提条件　10-5
　デバイス
　　サポート対象　10-6
　動作していることの確認　C-20
　認証　A-15
　非アクティブな状態　C-21
　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 10-2
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 10-4
ARC のトラブルシューティング C-19
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-12
パラメータ（表） B-12
Attack Response Controller
以前の Network Access Controller A-3
機能 A-12
説明 A-3
attemptLimit コマンド 4-20
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
auto-upgrade-option コマンド 17-7

B

BackOrifice
プロトコル B-41
backup-config コマンド 12-18
banner login コマンド 13-2
block-enable コマンド 10-10
block-hosts コマンド 10-38
block-networks コマンド 10-38
bypass-option コマンド 5-23

C

Cat 6K Blocking Device Interfaces パネル
VACL
Post-Block 10-31
Pre-Block 10-31
Catalyst ソフトウェア
IDSM-2
mls ip ids コマンド 15-18
SPAN のイネーブル化 15-10
VACL の設定 15-15
コマンド / コントロール アクセス 15-6
全メモリ テストのイネーブル化 15-30
リセット 15-31
set span コマンド 15-10
コマンド / コントロール アクセス 15-6
スーパーバイザ エンジン コマンド
サポート対象 15-33
サポート対象外 15-34
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
デフォルト パスワード 2-3
デフォルト ユーザ名 2-3
Cisco Intrusion Prevention Alert Center
概要 18-15
Cisco IOS
レート制限 10-4
Cisco IOS ソフトウェア
EXEC コマンド 15-35
IDSM-2
mls ip ids コマンド 15-19
SPAN のイネーブル化 15-12
VACL の設定 15-16
コマンド / コントロール アクセス 15-7
全メモリ テストのイネーブル化 15-31
リセット 15-32
SPAN
オプション 15-12
コンフィギュレーション コマンド 15-36
Cisco Services for IPS
サービス契約 4-45, 18-9

サポートされている製品　4-45, 18-9
Cisco.com
IDS ソフトウェア　18-2
アクティブなアップデート通知　18-16
暗号化アクセス　18-8
ソフトウェア アップデートのダウンロード　18-8
ソフトウェアへのアクセス　18-2
Cisco.com アカウント　18-8
Cisco.com への暗号化アクセス　18-8
class-map コマンド　14-4
clear denied-attackers コマンド　6-23, 13-11
clear events コマンド　4-24, 6-29, 13-8, C-76
clear line コマンド　13-3
CLI　A-29
概要　1-2
コマンド モード　1-8
コマンドライン編集　1-7
正規表現の構文　1-9
説明　A-3, A-29
デフォルト キーワード　1-12
同時セッション　2-2
汎用コマンド　1-11
CLI の動作　1-5, A-31
大文字と小文字の区別　1-6, A-32
再呼び出し　1-5, A-31
タブ補完　1-5, A-31
表示オプション　1-6, A-32
プロンプト　1-5, A-31
ヘルプ　1-5, A-31
clock set コマンド　4-25, 13-10
copy backup-config コマンド　12-20
copy current-config コマンド　12-20
copy iplog コマンド　8-9
copy license-key コマンド　4-47, 18-12
copy packet-file コマンド　9-8
CtlTransSource
図　A-11
説明　A-3, A-11
Ctrl+N　1-5, A-31
Ctrl+P　1-5, A-31
current-config コマンド　12-18

D

DDOS プロトコル　B-40
debug-module-boot コマンド　C-55
display-serial コマンド　13-25
サポートされているプラットフォーム　13-25
downgrade コマンド　17-10

E

enable-acl-logging コマンド　10-16
enable-detail-traps コマンド　11-6
enable-nvram-write コマンド　10-17
erase packet-file コマンド　9-9
erase コマンド　12-23
EtherChanneling
オプション　15-25
確認　15-28
混合モード　15-25
説明　15-25
ディセーブル化　15-28
要件　15-25
ロード バランシング　15-25
event-action コマンド　7-13
event-counter コマンド　7-9

F

filters コマンド　6-14
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
fragment-reassembly コマンド　7-25
ftp-timeout
設定　4-8
ftp-timeout コマンド　4-8

G

global-block-timeout コマンド　6-21, 10-14
global-deny-timeout コマンド　6-21
global-filters-status コマンド　6-21
global-metaevent-status コマンド　6-21
global-overrides-status コマンド　6-21
global-summarization コマンド　6-21

H

H.225.0 プロトコル　B-21
H.323 プロトコル　B-21
host-ip
　設定　4-4
host-ip コマンド　4-4
host-name コマンド　4-2
HTTP 解読
　ASCII 正規化　7-36, B-24
　説明　7-36, B-24
hw-module module 1 recover コマンド　14-7
hw-module module 1 reset コマンド　14-7, C-54
hw-module module 1 shutdown コマンド　14-7

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
　Java プラグイン　C-41
　TLS および SSL　4-41
　エラー メッセージ
　　分析エンジンがビジー状態　C-43
　証明書　4-41
　メモリ　C-41
　ロードしない
　　Java キャッシュのクリア　C-43
IDM がロードしない
　Java キャッシュのクリア　C-43
IDS-4215　17-16
　BIOS アップグレード　17-16
　ROMMON　17-11
　ROMMON アップグレード　17-16
　アップグレード
　　BIOS　17-16
　　ROMMON　17-16
　イメージの再作成　17-13
IDSM-2 がオンラインにならない　C-51
IDSM-2
　Catalyst ソフトウェア
　　インライン モード　15-21
　　コマンド / コントロール アクセス　15-6
　EtherChanneling
　　確認　15-28
　　ディセーブル化　15-28
　　要件　15-25
　IPS トラフィックの取り込み　15-14
　　mls ip ids コマンド　15-18
　　SPAN　15-10
　mls ip ids コマンド
　　Catalyst ソフトウェア　15-18
　　Cisco IOS ソフトウェア　15-19
　set span コマンド　15-10
　TCP リセット ポート　15-9, 15-14
　VACL
　　設定　15-14
　　説明　15-14
　VACL の設定
　　Catalyst ソフトウェア　15-15
　　Cisco IOS ソフトウェア　15-16
　アップグレード
　　メンテナンス パーティション（Catalyst ソフトウェア）　17-42
　　メンテナンス パーティション（Cisco IOS ソフトウェア）　17-43
　イメージの再作成
　　説明　17-31
　インストール
　　システム イメージ（Catalyst ソフトウェア）　17-31
　　システム イメージ（Cisco IOS ソフトウェア）　17-32
　インライン モード
　　Cisco IOS ソフトウェア　15-22
　　説明　15-21
　　要件　15-21
　管理タスク　15-30
　コマンド / コントロール アクセス　15-7
　　説明　15-6
　コマンド / コントロール ポート　15-9

混合モード　15-9
コンフィギュレーション タスク　14-1, 15-2, 16-2
サポートされていないスーパーバイザ エンジン コマンド　15-33, 15-34
サポートされている設定　15-5
時刻源　4-22
設定
EtherChanneling　15-26
mls ip ids コマンド　15-18
SPAN　15-10
インライン モード　15-21, 15-22
コマンド / コントロール アクセス　15-6
シーケンス　15-2
タスク　15-1
メンテナンス パーティション（Catalyst ソフトウェア）　17-34
メンテナンス パーティション（Cisco IOS）　17-38
ロード バランシング　15-26
センシング ポート　15-14
全メモリ テストのイネーブル化
Catalyst ソフトウェア　15-30
Cisco IOS ソフトウェア　15-31
取り付け
確認　15-3
取り付けの確認　15-3
モニタリング ポート　15-9
リセット　15-31
Catalyst ソフトウェア　15-31
Cisco IOS ソフトウェア　15-32
ログイン　2-6
IDSM-2 コマンド / コントロール ポート　C-51
IDSM-2 取り付けの確認　15-3
IDSM-2 のリセット　15-31
inline on a stick
説明　5-17
inline-interfaces コマンド　5-14
InterfaceApp
説明　A-3
interface-notifications コマンド　5-27
IP フラグメント再構成
シグニチャ（表）　7-24
説明　7-23
パラメータ（表）　7-24
IP ロギング
自動　8-3
手動　8-5
設定　8-2
説明　7-30, 8-2
ファイルのコピー　8-9
ip-access-list コマンド　15-16
ip-log コマンド　7-30
iplog コマンド　8-5
ip-log-bytes コマンド　8-3
ip-log-packets コマンド　8-3
ip-log-time コマンド　8-3
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-40
要約　A-40
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　18-2
新機能　A-4
セキュリティ機能　A-5
ディレクトリ構造　A-39
データの取得　A-5
デバイスのパラメータ設定　A-4
入手　18-2
バージョン管理方式　18-4
プラットフォームに依存するリリースの例　18-6
ユーザによる対話操作　A-4
IPS データ
XML 文書　A-9
タイプ　A-8
IPS-4240
ROMMON　17-11
インストール
システム イメージ　17-18
IPS-4255
ROMMON　17-11
インストール
システム イメージ　17-18

J

Java プラグイン
- Linux C-42
- Solaris C-42
- Windows C-41

L

Licensing パネル
- 設定 18-11
- 説明 4-45, 18-9

log-all-block-events-and-errors コマンド 10-19
LogApp
- syslog メッセージ A-20
- 機能 A-20
- 説明 A-3, A-20

logical-interface コマンド 5-25
login-banner-text
- 設定 4-10

login-banner-text コマンド 4-10
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-3
- ホストの統計情報 A-6

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

max-block-entries コマンド 10-12
max-denied-attackers コマンド 6-21
max-interfaces コマンド 10-20
MBS が適切にセットアップされていない C-26
Meta エンジン
- 説明 7-39, B-14
- パラメータ（表） B-14

MIB
- サポート対象 11-8

mls ip ids コマンド 15-18, 15-19
- IDSM-2 15-18

more current-config コマンド 12-2
more コマンド 12-18
Multi String エンジン
- 説明 B-15

N

never-block-hosts コマンド 10-22
never-block-networks コマンド 10-22
NM-CIDS
- reload コマンド 16-9
- reset コマンド 16-9
- session コマンド 16-3
- shutdown コマンド 16-9
- Telnet で接続
  - ルータへ 16-6
- アップグレード
  - ブート ローダー 17-27
- イメージの再作成 17-24
  - 概要 17-23
- サポートされている Cisco IOS コマンド 16-11
- 時刻源 4-23
- システム イメージ ファイル 17-23
- 設定
  - IDS セッション インターフェイス 16-3
  - インターフェイス 16-3
  - パケット取り込み 16-7
- チェック
  - IPS ソフトウェア ステータス 16-10
- パケット モニタリング
  - 説明 16-7
- ブート ローダー
  - 概要 17-27
  - ファイル 17-27
- リブート 16-9
- ログイン 2-7

no iplog コマンド 8-7
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
システム健全性情報 A-10
説明 A-3
統計情報 A-11
NSDB
概要 18-17
NTP
時刻同期 4-22
説明 4-22
センサーの時刻源 4-32, 4-33
NTP サーバ
設定 4-32
NVRAM 書き込みの設定 10-17

O

overrides コマンド 6-11

P

packet capture コマンド 9-6
packet display コマンド 9-3
password コマンド 4-14
PEP 情報
PID 13-29
SN 13-29
VID 13-29
physical-interface コマンド 5-25
physical-interfaces コマンド 5-9, 5-13, 5-17
ping コマンド 13-26
policy-map コマンド 14-4
Post-Block ACL 10-26, 10-27
Pre-Block ACL 10-26, 10-27
privilege
設定 4-19
privilege コマンド 4-14, 4-18

Q

Q.931 プロトコル
SETUP メッセージ B-21
説明 B-21

R

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
recover コマンド 17-11
reset コマンド 13-27
ROMMON
IDS-4215 17-13
RPC ポートマッパー B-28
RR
計算 6-9
例 6-25
RSA 認証
許可鍵 4-38

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 6-2, A-26
パラメータ 6-2, A-26
SEAO
説明 6-2, A-26
SEAP
アラーム チャネル 6-2, A-26
機能 6-2, A-26
コンポーネント 6-2, A-26
シグニチャ イベントのフロー 6-3, A-26
図 6-3, A-26
説明 A-24
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 FTP エンジン
説明　B-20
パラメータ（表）　B-20
Service Generic エンジン
説明　B-20
パラメータ（表）　B-21
サービス 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-22
Service HTTP
シグニチャ　7-36
Service HTTP エンジン
説明　7-36, B-24
パラメータ（表）　B-24
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 プロトコル　B-26
説明　B-26
パラメータ（表）　B-27
Service MSSQL エンジン
MSSQL プロトコル　B-27
説明　B-27
パラメータ（表）　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
パラメータ（表）　B-32
service-policy コマンド　14-4
session コマンド
AIP SSM　2-9
IDSM-2　2-6
NM-CIDS　2-7
set security acl コマンド　15-14
setup コマンド　3-2, 3-3
SFR
説明
show clock コマンド　4-24, 13-9
show configuration コマンド　12-2, 12-13
show events コマンド　6-26, 13-5, C-73
show history コマンド　13-28
show interfaces コマンド　C-71
show inventory コマンド　13-29
show module 1 details コマンド　C-54
show module コマンド　14-3
show settings コマンド　12-4, 12-16, 13-31
show statistics denied-attackers コマンド　6-23
show statistics virtual-sensor コマンド　13-13, C-62
show statistics コマンド　10-40, 13-13, C-62
show tech-support コマンド　13-22, C-56, C-57
出力　C-58
show users コマンド　4-19
show version コマンド　13-23, C-59
説明　C-59
sig-fidelity-rating コマンド　7-11
Signature Event Action Processor
「SEAP」を参照
SNMP
Get　11-2
GetNext　11-2
Set　11-2
Trap　11-2
概要　11-2

サポートされている MIB　11-8
設定
エージェント パラメータ　11-3
トラップ　11-6
汎用パラメータ　11-3
SNMP トラップ
概要　11-2
snmp-agent-port コマンド　11-3
snmp-agent-protocol コマンド　11-3
SPAN
オプション　15-12
設定　15-10
SPAN ポートの問題　C-12
SSH
概要　4-36
セキュリティ　4-36
ホストの追加　4-37
ssh authorized-key コマンド　4-38
ssh generate-key コマンド　4-40
ssh host-key コマンド　4-36
SSH サーバ
公開鍵　A-22
秘密鍵　A-22
SSH サーバ ホスト鍵
生成　4-40
SSH の既知ホスト リスト
ホストの追加　4-36
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
status コマンド　7-12
stream-reassembly コマンド　7-29
String ICMP エンジン
パラメータ（表）　B-35
String TCP エンジン
パラメータ　7-33
パラメータ（表）　B-36
String TCP シグニチャ
例　7-32
String エンジン
説明　7-32, B-35
STRING.UDP エンジン
パラメータ（表）　B-36
subinterface-type コマンド　5-18
summertime-option non-recurring コマンド　4-29
summertime-option recurring コマンド　4-26
Sweep エンジン
説明　B-38
パラメータ（表）　B-38
System Configuration Dialog　3-2

T

TAC
PEP 情報　13-29
show tech-support コマンド　13-22, C-57
サービス アカウント　4-16, A-30
target-value コマンド　6-9
TCP ストリーム再構成
シグニチャ（表）　7-27, 7-28
説明　7-26
パラメータ（表）　7-27, 7-28
TCP リセット インターフェイス
条件　5-6
説明　5-5
リスト　5-6
TCP リセット ポート
IDSM-2　15-9
Telnet
NM-CIDS　16-6
telnet-option
設定　4-5
telnet-option コマンド　4-5
terminal コマンド　13-4
TFN2K プロトコル　B-40
TFTP サーバ
推奨　17-13
UNIX　17-13
Windows　17-13
time-zone-settings コマンド　4-31
TLS
概要　4-41
証明書　4-41
ハンドシェーク　4-41
tls generate-key コマンド　4-44
tls trusted-host コマンド　4-42
TLS 証明書
生成　4-44
trace コマンド　13-30

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
trap-community-name 11-6
trap-destinations コマンド 11-6
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
TVR
概要 6-9
説明

U

upgrade コマンド 17-5, 17-11
username コマンド 4-14
user-profile コマンド 10-24

V

VACL
IDSM-2 15-14
Post-Block 10-31
Pre-Block 10-31
説明 10-3
variables コマンド 6-8, 7-3

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
Web サーバ設定
設定 4-12

あ

アカウントのロック
設定 4-20
アクセス
Cisco Intrusion Prevention Alert Center 18-15
IPS ソフトウェア 18-2
アクセス リスト
設定 4-6
設定の誤り C-8
アップグレード
4.1 から 5.0 18-7
最低限必要なバージョン 18-7
メンテナンス パーティション
IDSM-2（Catalyst ソフトウェア） 17-42
IDSM-2（Cisco IOS ソフトウェア） 17-43
リカバリ パーティション 17-5, 17-11
アプライアンス
アップグレード
リカバリ パーティション 17-5
アプリケーション パーティション イメージ 17-11
時刻源 4-22
ターミナル サーバ 2-4
ターミナル サーバのセットアップ 2-4
復旧
ソフトウェア イメージ 17-22
ログイン 2-3
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
アプリケーション パーティション イメージ
復旧 17-11
アラーム チャネル
説明 6-2, A-26

い

イネーブル化
シグニチャ 7-12
全メモリ テスト
Catalyst ソフトウェア 15-30
Cisco IOS ソフトウェア 15-31
イベント アクション
インラインの攻撃者拒否 6-21

説明　6-4, B-6
イベント アクション オーバーライド
概要　6-11
イベント アクション（表）　6-4, B-6
イベント アクション フィルタ
概要　6-14
イベント アクション ルール
概要　6-2
機能　6-2
タスク リスト　6-7
例　6-25
イベント ストア
イベントのクリア　4-24
機能　A-7
説明　A-3
タイムスタンプ　A-7
データ構造　A-8
例　A-7
イベント タイプ　C-73
イベント変数
説明　6-7
例　6-7
イメージの再作成
IDS-4215
ROMMON　17-13
IDSM-2
説明　17-31
NM-CIDS　17-24
アプライアンス　17-11
説明　17-2
センサー　17-2
インストール
システム イメージ
IPS-4240　17-18
IDSM-2（Catalyst ソフトウェア）　17-31
IDSM-2（Cisco IOS ソフトウェア）　17-32
センサーのライセンス　18-11
ライセンス キー　4-48, 18-13
インターフェイス
TCP リセット　5-5
コマンド / コントロール　5-2
スロット番号　5-2
設定上の制限　5-7
説明　5-2
センシング　5-2, 5-3
代替 TCP リセット　5-2
ポート番号　5-2
ライブ トラフィックの表示　9-3
インターフェイス サポート（表）　5-4
インターフェイスのコンフィギュレーション シーケンス　5-7
インターフェイスの設定
シーケンス　5-7
インライン VLAN ペア
サポートしているセンサー　5-17
設定　5-18
説明　5-17
インライン インターフェイス モード
設定　5-15
インライン モード
概要　5-14

え

エンジン
AIC　7-15

お

オペレータ
特権　1-4, A-29

か

概要
CLI　1-2
SSH　4-36
センサー上の時刻　4-22
バイパス モード　5-23
確認
EtherChanneling　15-28
センサーの初期化　3-9
センサーのセットアップ　3-9
カスタム シグニチャ
MEG シグニチャ　7-39
Service HTTP の例　7-37
String TCP　7-32
コンフィギュレーション シーケンス　7-32
仮想センサー
インターフェイスの割り当て　5-25
管理
スイッチ　10-31

ファイアウォール　10-33
ルータ　10-28
管理者
特権　1-4, A-29

き

キーワード
no　1-12
デフォルト　1-12
偽のホストに対する手動ブロック　C-25
許可鍵
RSA 認証　4-38
定義　4-39

く

クリア
イベント　6-29, 13-8, C-76
拒否された攻撃者の統計情報　6-23, 13-11
統計情報　13-13, C-63

け

現在のコンフィギュレーション
出力の検索　12-13
出力のフィルタリング　12-13
バックアップ　12-22
検索
現在のコンフィギュレーション　12-13
サブモード コンフィギュレーション　12-16

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　1-6, A-32
コピー
IP ロギング ファイル　8-9
パケット ファイル　9-8
コマンド　11-6, 14-3
access-list　4-6
alert-frequency　7-6
alert-severity　7-8
allow-sensor-block　10-8
application-policy　7-16
attemptLimit　4-20
auto-upgrade-option　17-7
backup-config　12-18
banner login　13-2
block-enable　10-10
block-hosts　10-38
block-networks　10-38
bypass-option　5-23
class-map　14-4
clear denied-attackers　6-23, 13-11
clear events　4-24, 6-29, 13-8, C-76
clear line　13-3
clock set　4-25, 13-10
copy backup-config　12-20
copy current-config　12-20
copy iplog　8-9
copy license-key　4-47, 18-12
copy packet-file　9-8
current-config　12-18
debug module-boot　C-55
display-serial　13-25
downgrade　17-10
enable-acl-logging　10-16
enable-detail-traps　11-6
enable-nvram-write　10-17
erase　12-23
erase packet-file　9-9
event-action　7-13
event-counter　7-9
filters　6-14
fragment-reassembly　7-25
ftp-timeout　4-8
global-block-timeout　6-21, 10-14
global-deny-timeout　6-21
global-filters-status　6-21
global-metaevent-status　6-21
global-overrides-status　6-21
global-summarization　6-21
host-ip　4-4
host-name　4-2
hw-module module 1 recover　14-7
hw-module module 1 reset　14-7, C-54
hw-module module 1 shutdown　14-7
inline-interfaces　5-14

interface-notifications 5-27
ip-access-list 15-16
ip-log 7-30
iplog 8-5
ip-log-bytes 8-3
ip-log-packets 8-3
ip-log-time 8-3
log-all-block-events-and-errors 10-19
logical-interface 5-25
login-banner-text 4-10
max-block-entries 10-12
max-denied-attackers 6-21
max-interfaces 10-20
mls ip ids 15-18, 15-19
more 12-18
more current-config 12-2
never-block-hosts 10-22
never-block-networks 10-22
no iplog 8-7
overrides 6-11
packet capture 9-6
packet-display 9-3
password 4-14
physical-interface 5-25
physical-interfaces 5-9, 5-13, 5-17
ping 13-26
policy-map 14-4
privilege 4-14, 4-18
reset 13-27
service-policy 14-4
set security acl 15-14
set span 15-10
setup 3-2, 3-3
show clock 4-24, 13-9
show configuration 12-2, 12-13
show events 6-26, 13-5, C-73
show history 13-28
show inventory 13-29
show module 1 details C-54
show settings 12-4, 12-16, 13-31
show statistics 10-40, 13-13, C-62
show statistics denied-attackers 6-23
show statistics virtual-sensor 13-13, C-62
show tech-support 13-22, C-57
show users 4-19
show version 13-23, C-59
sig-fidelity-rating 7-11
snmp-agent-port 11-3
snmp-agent-protocol 11-3
ssh authorized-key 4-38
ssh generate-key 4-40
ssh host-key 4-36
status 7-12
stream-reassembly 7-29
subinterface-type 5-18
summertime-option non-recurring 4-29
summertime-option recurring 4-26
target-value 6-9
telnet-option 4-5
terminal 13-4
time-zone-settings 4-31
tls generate-key 4-44
tls trusted-host 4-42
trace 13-30
trap-community-name 11-6
trap-destinations 11-6
upgrade 17-5
username 4-14
user-profile 10-24
variables 6-8, 7-3
コマンド モード 1-8
EXEC 1-8
イベント アクション ルールのコンフィギュレーション 1-8
グローバル コンフィギュレーション 1-8
サービス モード コンフィギュレーション 1-8
シグニチャ定義コンフィギュレーション 1-8, 1-9
特権 EXEC 1-8
コマンド / コントロール アクセス
Catalyst ソフトウェア 15-6
Cisco IOS ソフトウェア 15-7
説明 15-6
コマンド / コントロール インターフェイス
説明 5-2
リスト 5-2
コマンドライン編集（表） 1-7
混合モード
EtherChanneling 15-25
設定 5-10, 5-13
説明 5-13
パケット フロー 5-13

コンフィギュレーション シーケンス
AIP SSM 14-2
コンフィギュレーション ファイル
バックアップ 12-22
マージ 12-22

さ

サービス
特権 1-4, A-30
サービス アカウント
TAC A-30
作成 4-17
説明 4-16, A-30
特権 1-4, A-30
トラブルシューティング A-30
サービス ロール 1-4, 2-2, A-30
再呼び出し
使用 1-5, A-31
ヘルプおよびタブ補完 1-5, A-31
削除
拒否された攻撃者のリスト 6-23, 13-11
最後に適用されたアップグレード 17-10
作成
MEG シグニチャ 7-39
Service HTTP シグニチャ 7-37
String TCP シグニチャ 7-34
カスタム シグニチャ 7-32
サービス アカウント 4-17
バナー ログイン 13-2
ユーザ プロファイル 10-24
サブモード コンフィギュレーション
出力の検索 12-16
出力のフィルタリング 12-16
サポートされていないスーパーバイザ エンジン コマンド 15-34
サポートされている Cisco IOS コマンド
NM-CIDS 16-11
サマータイム
設定
non-recurring 4-29
recurring 4-26
センサーがパケットを検出しない C-16

し

時間帯設定
設定 4-31
シグニチャ
false positive 7-2
Service HTTP 7-36
String TCP 7-34
カスタム 7-2
サブシグニチャ 7-2
説明 7-2
チューニング済み 7-2
デフォルト 7-2
レート制限 10-4
シグニチャ エンジン
AIC B-9
Atomic B-11
Atomic ARP B-11
Atomic IP B-12
Flood B-13
Flood Host B-13
FLood Net B-13
Meta 7-39, B-14
Multi String B-15
Normalizer B-16
Service DNS B-18
Service FTP B-20
Service Generic B-20
Service H225 B-21
Service HTTP 7-36, 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
State B-33
String 7-32, B-35
Sweep B-38
Traffic ICMP B-40
Trojan B-41
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 7-3
時刻
センサー上での修正 4-24
時刻源
AIP SSM 4-23
IDSM-2 4-22
NM-CIDS 4-23
アプライアンス 4-22
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-39
システム クロック
設定 4-26, 13-10
表示 4-25, 13-9
システム コンポーネント
IDAPI A-33
システムの設計（図） A-2
自動アップデートの適用 C-38
終了
CLI セッション 13-3
出力
現在の行のクリア 1-6, A-32
表示 1-6, A-32
手動ブロッキング 10-38
使用
TCP リセット インターフェイス 5-6
障害リカバリ C-3
使用可能
SPAN
Cisco IOS ソフトウェア 15-12
消去
現在のコンフィギュレーション 12-23
パケット ファイル 9-9
初期化
AIP SSM
確認 14-3
確認 3-9
診断
ネットワーク接続性 13-26
信頼できるホスト
追加 4-42

す

スーパーバイザ エンジン コマンド
サポート対象 15-33
サポート対象外 15-34
スケジューリング
自動アップグレード 17-8

せ

正規表現の構文 1-9
正規表現の構文（表） 1-9
制御トランザクション
特性 A-9
要求のタイプ A-8
生成
SSH サーバ ホスト鍵 4-40
TLS 証明書 4-44
セキュリティ
SSH 4-36
アカウントのロック 4-20
設定
ACL ロギング 10-16
ftp-timeout 4-8
host-ip 4-4
IP フラグメント再構成 7-25
IP フラグメント再構成パラメータ 7-24, 7-28
IP ロギング 7-30
login-banner-text 4-10
Meta Event Generator 6-21
NTP サーバ 4-32
NTP を使用するセンサー 4-34
privilege 4-19
SFR 7-11
Summarizer 6-21
TCP ストリーム再構成 7-29
telnet-option 4-5
TVR 6-10
Web サーバ設定 4-12
アカウントのロック 4-20
アクセス リスト 4-6
アップグレード 17-4
アプリケーション ポリシー 7-17, 7-44
アラート重大度 7-8
アラート頻度パラメータ 7-6
イベント アクション 7-14

イベント アクション フィルタ　6-16
イベント アクション変数　6-8
イベント カウンタ　7-10
インターフェイス　5-7
　NM-CIDS　16-3
インライン VLAN ペア　5-18
インライン インターフェイス モード　5-15
拒否する攻撃者の最大数　6-21
混合モード　5-10
最大ブロッキング インターフェイス数　10-20
最大ブロック数　10-13
サマータイム
　non-recurring　4-29
　recurring　4-26
時間帯設定　4-31
シグニチャ忠実度評価　7-11
シグニチャ変数　7-3
システム クロック　4-26, 13-10
自動 IP ロギング　8-3
自動アップグレード　17-8
手動 IP ロギング　8-5
ステータス　7-12
すべてのブロック イベントとエラーのロギング　10-19
センサーが自らをブロックする　10-8
トラフィック フロー通知　5-27
ネットワークの手動ブロック　10-38
バイパス モード　5-23
パケット取り込み
　NM-CIDS　16-7
パスワード　4-18
物理インターフェイス　5-25
ブロッキング
　時間　10-14
　スイッチ　10-31
　ファイアウォール　10-33
　ルータ　10-28
ブロックしないネットワーク　10-22
ブロックしないホスト　10-22
ホストの手動ブロック　10-38
ホスト名　4-2
マスター ブロッキング センサー　10-36
メンテナンス パーティション（Catalyst ソフトウェア）　17-34
メンテナンス パーティション（Cisco IOS）　17-38
ユーザ プロファイル　10-24
説明　B-18, C-73
　System Configuration Dialog　3-2
センサー
　NTP 時刻源　4-33
　NTP 時刻源の使用　4-32
　NTP 時刻同期　4-22
　NTP を使用するための設定　4-34
　setup コマンド　3-2, 3-3
　イメージの再作成　17-2, 18-7
　インターフェイス サポート　5-4
　管理
　　スイッチ　10-31
　　ファイアウォール　10-33
　　ルータ　10-28
　コンフィギュレーション タスクの順序　1-2
　時刻源　4-22
　システム イメージの復旧　18-7
　初期化　3-2, 3-3
　ダウングレード　17-10
　パーティション　A-3
　ライセンス　18-11
　ログイン
　　SSH　2-10
　　Telnet　2-10
センサー上の時刻の修正　4-24
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
センサーの初期化　3-2, 3-3
センサーの設定
　タスクのシーケンス　1-2
センシング インターフェイス
　PCI カード　5-3
　説明　5-3
　モード　5-3

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

ターミナル
行数の変更 13-4
ターミナル サーバ
セットアップ 2-4
ターミナル サーバのセットアップ 2-4
ダウングレード
センサー 17-10
タスク
IDSM-2 の設定 15-2
NM-CIDS の設定 16-2
センサーの設定 1-2
タブ補完
使用 1-5, A-31

ち

チェック
IPS ソフトウェア ステータス
NM-CIDS 16-10
重複する IP アドレス C-9

つ

追加
イベント アクション オーバーライド 6-11
信頼できるホスト 4-42
ホストを SSH の既知ホスト リストに 4-36, 4-37
ユーザ 4-14, 4-18, 4-19

て

定義
許可鍵 4-39
停止
IP ロギング 8-7
ディセーブル化
EtherChanneling 15-28
シグニチャ 7-12
ブロッキング 10-10
データ構造
例 A-8
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
パスワード
cisco 2-3
ブロックする時間 10-14
ユーザ名
cisco 2-3
デフォルト キーワード
使用 1-12
転送
シリアル ポートへの出力 13-25

と

トライアル ライセンス キー 4-45, 18-9
トラフィック
AIP SSM 14-4
トラフィック フロー通知
概要 5-27
設定 5-27
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
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-62
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
サービス アカウント　4-16
センサーがパケットを検出しない　C-16
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
正しく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　C-26
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
ARC
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-43
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
取り込み
ライブ トラフィック　9-7
トレース
IP パケットのルート　13-30

に

入手
コマンド履歴　13-28
使用したコマンド リスト　13-28
ブロックされたホストと接続のリスト　10-40

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　5-23
概要　5-23
設定　5-23
パスワード
サービス アカウント　3-3
設定　4-18
変更　4-18
バック ドア型トロイの木馬
BO2K　B-41
バックアップ
現在のコンフィギュレーション　12-21
設定　12-22
汎用コマンド　1-11

ひ

ビューア
特権　1-4, A-29
表示
PEP 情報　13-29
イベント　6-27, 13-6, C-74
現在のコンフィギュレーション　12-2
現在のサブモード コンフィギュレーション　12-4
サブモード設定　13-31
システム クロック　4-25, 13-9
テクニカル サポート情報　13-22, C-57
統計情報　13-13, C-63
バージョン　13-23, C-59
ユーザ情報　4-20
ライブ トラフィック　9-3
論理ファイルの内容　12-18

ふ

フィルタリング
　現在のコンフィギュレーション　12-13
　サブモード コンフィギュレーション　12-16
ブート ローダー
　アップグレード　17-27
　説明　17-27
復元
　現在のコンフィギュレーション　12-21
復旧
　AIP SSM　C-55
　アプリケーション パーティション イメージ　17-11
　リカバリ / アップグレード CD　17-22
物理インターフェイス
　設定　5-25
物理接続の問題　C-12
ブロッキング
　show statistics　10-40
　最大数　10-12
　サポートされているデバイス　10-6
　手動　10-38
　スイッチの管理　10-31
　説明　10-2
　センサーによる自らのブロック　10-8
　前提条件　10-5
　タイプ　10-2
　ディセーブル化　10-10
　必要な情報　10-3
　ファイアウォールの管理　10-33
　ブロックされるホストのリスト　10-40
　ブロック時間　10-14
　ブロックしないアドレス　10-22
　プロパティ　10-8
　マスター ブロッキング センサー　10-35
　ユーザ プロファイル　10-24
　ルータの管理　10-28
ブロッキングの前提条件　10-5
ブロックがシグニチャに対して実行されない　C-25
ブロックされるホストのリスト　10-40
プロンプト
　デフォルト入力　1-5, A-31
分析エンジンがビジー状態
　IDM が終了する　C-43

へ

ヘルプ
　疑問符　1-5, A-31
　使用　1-5, A-31
変更
　ターミナル プロパティ　13-4
　パスワード　4-18

ほ

ホスト名
　設定　4-2

ま

マージ
　コンフィギュレーション ファイル　12-22
マスター ブロッキング センサー　10-35
　説明　10-35

め

メモリ
　IDM　C-41
メモリの変更
　Linux での Java プラグイン　C-42
　Solaris での Java プラグイン　C-42
　Windows での Java プラグイン　C-41
メンテナンス パーティション
　設定（Catalyst ソフトウェア）　17-34
　設定（Cisco IOS）　17-38
　説明　A-3

も

モード
　インライン　5-14
　バイパス　5-23
モジュール
　IDSM-2　15-5
モニタリング
　ビューア特権　1-4, A-29

ゆ

ユーザ
　削除　4-14
　追加　4-14
ユーザ プロファイル　10-24
ユーザのロール
　オペレータ　1-4, A-29
　管理者　1-4, A-29
　サービス　1-4, A-29
　ビューア　A-29, 1-4

よ

要約
　Engine.META　6-20
　Fire All　6-21
　Fire Once　6-21
　Global Summarization　6-21
　サマリー　6-21
　説明　6-20

ら

ライセンス
　IPS デバイスのシリアル番号　4-45, 18-9
　説明　4-45, 18-9
ライセンス キー
　インストール　4-48, 18-13
　ステータス　4-45, 18-9
　トライアル　4-45, 18-9

り

リカバリ パーティション
　アップグレード　17-5
　説明　A-3
リスク評価
　「RR」を参照
リセット
　AIP SSM　C-54
　IDSM-2　15-31
　アプライアンス　13-27
リセットがシグニチャに対して実行されない　C-35
リタイア
　シグニチャ　7-12
リブート
　NM-CIDS　16-9

れ

レート制限
　サポートされているシグニチャ　10-4
　説明　10-4
　ルータ　10-4

ろ

ロード バランシング
　オプション　15-25
ログイン
　AIP SSM　2-9
　IDSM-2　2-6
　NM-CIDS　2-7
　アプライアンス　2-3
　サービス ロール　2-2
　センサー
　　SSH　2-10
　　Telnet　2-10
　ターミナル サーバ　2-4
　ユーザ ロール　2-2
ロックされたアカウント
　リセット　4-18
論理デバイスの設定　10-24

わ

割り当て
　インターフェイスを仮想センサーへ　5-25