
## 数字

**3DES** トリプル DES（Data Encryption Standard）。DES をより強力にしたバージョンで、SSH バージョン 1.5 のデフォルトの暗号化方式。センサーと SSH セッションを確立するときに使用されます。センサーでデバイスを管理しているときに使用できます。

**802.x** LAN プロトコルを定義する一連の IEEE 標準。

## A

**AAA** 認証、許可、アカウンティング。「トリプル A」と読みます。シスコ デバイスの主要な推奨アクセス コントロール方法です。

**ACE** Access Control Entry（アクセス コントロール エントリ）。ACL 内のエントリで、指定されたアドレスまたはプロトコルに関して実行するアクションを記述します。センサーは、ACE を追加または削除してホストをブロックします。

**ACK** 確認応答。1 台のネットワーク デバイスからもう 1 台のネットワーク デバイスに送信される、イベントが発生したこと（メッセージの受信など）を確認する通知。

**ACL** Access Control List（アクセス コントロール リスト）。ルータを経由するデータの流れを制御する ACE のリストです。ルータ インターフェイスごとに、受信データ用と送信データ用の 2 つの ACL があります。1 つの方向で同時にアクティブにできる ACL は 1 つだけです。ACL は、番号または名前で識別されます。ACL は、標準、強化、拡張のいずれかになります。センサーで ACL を管理するように設定できます。

**ACS サーバ** Cisco Access Control Server。ネットワーク ユーザ、ネットワーク管理者、ネットワーク インフラストラクチャ リソースの集中管理ポイントとなる RADIUS セキュリティ サーバ。

**AIC エンジン** Application Inspection および Control エンジン。Web トラフィックを詳細に分析します。HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。インスタント メッセージングなど、指定されたポートを介してトンネリングを試みるアプリケーションや gotomypc などのトンネリング アプリケーションを管理制御できます。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できます。

**alert** 厳密には IPS のイベント タイプの 1 つを指し、evAlert 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使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。

**API** アプリケーション プログラミング インターフェイス。アプリケーション プログラムが通信ソフトウェアと対話する手段。標準化された API では、基礎となる通信手段とは関係なく、アプリケーション プログラムを開発できます。コンピュータ アプリケーション プログラムは、一式の標準ソフトウェア割り込み、呼び出し、およびデータ フォーマットを実行して、他のデバイスとの接続を開始します（ネットワーク サービス、メインフレーム通信プログラム、その他のプログラム間通信）。通常、API を使用すると、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 システムやネットワークと通信するために必要なリンクを簡単に作成できます。

**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** アドレス解決プロトコル。IP アドレスを MAC アドレスにマッピングする際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 5500-X IPS SSP** 侵入防御システム セキュリティ サービス プロセッサ。IPS はサービスとして動作しており、ASA は IPS 間のトラフィックの送受信を制御します。IPS サービス プロセッサは、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行います。不正なアクティビティを検出すると、ASA 5500-X IPS SSP は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。「適応型セキュリティ アプライアンス」も参照してください。

**ASA 5585-X IPS SSP** 侵入防御システム セキュリティ サービス プロセッサ。Cisco ASA 5585-X 適応型セキュリティ アプライアンスの IPS プラグイン モジュール。ASA 5585-X IPS SSP は、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行う IPS サービス プロセッサです。不正なアクティビティを検出すると、ASA 5585-X IPS SSP は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。「適応型セキュリティ アプライアンス」も参照してください。

**ASDM** Adaptive Security Device Manager。適応型セキュリティ デバイスの設定と管理が可能な Web ベースのアプリケーション。

**ASN.1** 抽象構文記法 1。データ プレゼンテーションの標準。

**Atomic エンジン** 2 つの Atomic エンジンがあります。アトミック IP は IP プロトコル パケットとそれに関連付けられたレイヤ 4 トラスポート プロトコルを検査します。アトミック ARP はレイヤ 2 ARP プロトコルを検査します。

**attack relevance rating** ARR。ターゲット OS の関連性に関連付けられた重み。攻撃関連性レーティングは取得値（関連性あり、不明、関連性なし）で、アラート時に決定されます。関連する OS はシグニチャごとに設定されます。

**AuthenticationApp** IPS のコンポーネントの 1 つ。IP アドレス、パスワード、デジタル証明書に基づいてユーザを許可および認証します。

**AV** アンチウイルス。

## B

**backplane** 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 バスおよび配電バス間の物理接続。

**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間の通信を行うプログラム。

**BO** BackOrifice。UDP 上だけで実行された Windows を標的とした最初のバック ドア型トロイの木馬。

**BO2K** BackOrifice 2000。TCP と UDP 上で実行される Windows を標的とするバック ドア型トロイの木馬。

**Bpdu** Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワーク内のブリッジ間で情報を交換するために設定可能な間隔で送出される、スパニングツリー プロトコルの hello パケット。

## C

**CA** 認証局（certification authority）。デジタル証明書（特に X.509 証明書）を発行し、証明書内のデータ項目間のバインディングを保証するエンティティです。センサーは、自己署名証明書を使用します。

**CA 証明書** 別の CA によって発行された、CA の証明書。

**CEF** シスコ エクスプレス フォワーディング。CEF は、高度なレイヤ 3 IP スイッチング テクノロジーです。CEF によって、インターネットや、Web ベースのアプリケーションまたは対話型セッションが集中的に使用されるネットワークなどの、大規模でダイナミックなトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティが最適化されます。

**cidDump** 大量の情報を取り込むためのスクリプト。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。

**CIDEE** Cisco Intrusion Detection Event Exchange。Cisco IPS システムで使用される SDEE への拡張子を指定します。CIDEE 標準では、Cisco IPS システムでサポートされる使用可能なすべての拡張子が指定されています。

**CIDS ヘッダー** IPS システムの各パケットに追加されるヘッダー。パケットの分類、長さ、チェックサムの結果、タイムスタンプ、受信インターフェイスが含まれます。

**Cisco IOS** CiscoFusion アーキテクチャの下で全製品に共通の機能、拡張性、セキュリティを提供するシスコ ソフトウェア。Cisco IOS では、広範なプロトコル、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ながら、インターネットワークのインストールと管理を一元化、統合、および自動化できます。

**CLI** コマンドライン インターフェイス。センサー アプリケーションの設定と制御に使用される、センサーに付属のシェル。

**CollaborationApp** IPS のコンポーネントの 1 つ。グローバル相関データベースを通して他のデバイスと情報を共有し、すべてのデバイスの総合的な有効性を高めます。

**console** センサーのモニタと制御に使用される端末またはラップトップ コンピュータ。

**Control Transaction Server** IPS のコンポーネントの 1 つ。リモート クライアントからの制御トランザクションを受け付け、ローカル制御トランザクションを開始して、リモート クライアントに応答を返します。

**Control Transaction Source** IPS のコンポーネントの 1 つ。リモート アプリケーションに向けられた制御トランザクションを待機し、制御トランザクションをリモート ノードに転送し、応答を発信側に返します。

**Cookie** Web サーバから Web ブラウザに送信される情報。ブラウザはこれを保存し、Web サーバに追加要求を行うたびに Web サーバに送り返します。

**CSA MC** Cisco Security Agent Management Center。CSA MC は、管理する CSA エージェントからホスト ポスチャ情報を受信します。また、ネットワークから隔離する必要があると判断した IP アドレスのウォッチ リストも維持します。

**CSM** Cisco Security Manager。Cisco Self-Defending Network ソリューションのプロビジョニング コンポーネントです。CS-Manager は CS-MARS と完全に統合されています。

**CS-MARS** Cisco Security Monitoring, Analysis, and Response System。Cisco Self-Defending Network ソリューションのモニタリング コンポーネント。CS-MARS は CS-Manager と完全に統合されています。

**CVE** Common Vulnerabilities and Exposures。http://cve.mitre.org/ で管理されている脆弱性および他の情報セキュリティの危険に関する標準化された名前のリスト。

## D

**DCE** データ回線終端装置（ITU-T の拡張）。ユーザとネットワークを結ぶインターフェイスのネットワーク側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、トラフィックの転送を行い、DCE と DTE デバイス間のデータ転送を同期化するためのクロッキング信号を提供します。DCE の例として、モデルとインターフェイス カードがあります。

**DCOM** 分散コンポーネント オブジェクト モデル。ソフトウェア コンポーネントどうしがネットワーク上で直接通信できるようにするプロトコル。Microsoft が開発し、以前はネットワーク OLE と呼ばれた DCOM は、HTTP などのインターネット プロトコルを含む複数のネットワーク転送で使用されるように設計されています。

**DDoS** 分散型サービス拒否攻撃。多数の侵害されたシステムが 1 つのターゲットを攻撃することで、対象のシステムユーザにサービス拒否を発生させる攻撃。ターゲット システムにメッセージが大量に送信されると、基本的にそのシステムが強制的にシャット ダウンされ、システムの正規ユーザへのサービスが拒否されます。

**DES** データ暗号規格。アルゴリズムではなく 56 ビット キーを基盤とする、強力な暗号化方式。

**DIMM** Dual In-line Memory Module（デュアル インライン メモリ モジュール）。

**DMZ** 非武装地帯。プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立地帯に位置する単独のネットワークです。

**DNS** Domain Name System（ドメイン ネーム システム）。インターネット全体にわたるホスト名と IP アドレスのマッピングです。DNS を使用すると、人間が読める形式の名前を、ネットワーク パケットで必要とされる IP アドレスに変換できます。

**DoS** Denial of Service（サービス拒絶）。特定のシステムまたはネットワークの操作を混乱させることを目的とする攻撃です。

**DRAM** ダイナミック RAM。定期的な更新が必要なコンデンサ内に情報を格納する RAM。内容の更新中、プロセッサが DRAM にアクセスできなくなるため、遅延が発生することがあります。ただし、DRAM は SRAM ほど複雑ではなく、大容量です。

**DTE** データ端末機器。RS-232C 接続上のデバイスのロールを指します。DTE はデータを送信回線に書き込み、受信回線からデータを読み取ります。

**DTP** ダイナミック トランキング プロトコル。2 台のデバイスを結ぶリンクでのトランキングや使用するトランキング カプセル化のタイプ（ISL または 802.1q）のネゴシエーションに使用される、VLAN グループのシスコ独自のプロトコル。

## E

**ECLB** イーサネット チャネル ロード バランシング。Catalyst スイッチが、異なる物理パスでトラフィック フローを分岐できるようにします。

**ESD** 静電放電。静電放電は、1 つの物体から別の物体への急速な電荷の移動により、数千ボルトの電荷が発生することを指します。電気的コンポーネントやサーキット カード アセンブリ全体に重大なダメージを引き起こす場合があります。

**event** 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。

**evIdsAlert** イベント ストアに書き込まれる、アラートを表す XML エンティティ。

## F

**Fast Flux** Fast Flux はボットネットで使用される DNS 手法の 1 つで、フィッシング サイトやマルウェア配信サイトを、プロキシとして動作する絶えず変化する侵害されたホスト ネットワークの後ろに隠します。マルウェア ネットワークの検出や対策を困難にするためにピアツーピア ネットワーキング、分散指示管理、Web ベース ロード バランシング、プロキシ リダイレクションを組み合わせる手法を指すこともあります。Storm Worm は、この手法を利用した最新のマルウェアの変異型の 1 つです。

**Flood エンジン** ホストおよびネットワーク宛の ICPM および UDP フラッドを検出します。

**FQDN** 完全修飾名。DNS のツリー階層で正確な場所を指定するドメイン名。ルート ドメインを基準に、トップレベル ドメインを含むすべてのドメイン レベルを指定します。完全修飾ドメイン名は、ネームスペースでこの正確さによって識別されます。

**fragment** 小さな単位に分割された大きなパケットの一部。

**FTP** File Transfer Protocol（ファイル転送プロトコル）。ネットワーク ノード間でファイルを転送するために使用され、TCP/IP プロトコル スタックの一部であるアプリケーション プロトコル。FTP は、RFC 959 で定義されています。

**FTP サーバ** ファイル転送プロトコル（File Transfer Protocol）サーバ。ネットワーク ノード間のファイルの転送に FTP プロトコルを使用するサーバ。

**FWSM** ファイアウォール セキュリティ モジュール。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。ブロックに **shun** コマンドを使用します。FWSM は、シングル モードでもマルチモードでも設定できます。

## G

**GBIC** ギガビット インターフェイス コンバータ。多くの場合、光ケーブルをファイバ インターフェイスに適応させる光ファイバ トランシーバを指します。ファイバ対応スイッチと NIC は、一般に GBIC スロットと SFP スロット、またはそのどちらかを提供します。詳細については、『*Catalyst Switch Cable, Connector, and AC Power Cord Guide*』を参照してください。

**GMT** Greenwich Mean Time（グリニッジ標準時）。経度が 0 度のタイムゾーン。現在は、協定世界時（UTC）と呼ばれます。

**GRUB** Grand Unified Bootloader。ブートローダは、コンピュータを起動すると最初に実行されるソフトウェア プログラムです。オペレーティング システム カーネル ソフトウェアをロードし、制御を渡す役割を果たします。その後、カーネルがオペレーティング システムの残りを初期化します。

## H

**H.225.0** H.225.0 セッションの確立とパケット化を規定する ITU 標準。H.225.0 では、実際には、RAS、Q.931 の使用、RTP の使用など、いくつかの異なるプロトコルが定められています。

**H.245** H.245 エンドポイントの制御を規定する ITU 標準。

**H.323** 異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 は、CODEC の共通セット、コール セットアップとネゴシエーションの手順、および基本的なデータ転送方法を定義しています。

**HTTP** ハイパーテキスト転送プロトコル。IPS アーキテクチャでリモート データ交換に使用される、ステートレスな要求 / 応答メディア転送プロトコルです。

**HTTPS** 標準 HTTP プロトコルを拡張したもので、Web サイトからのトラフィックを暗号化することによって機密保持を可能にします。デフォルトでは、このプロトコルは TCP ポート 443 を使用します。

## I

**ICMP** Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。エラーを報告し、IP パケット処理に関連するその他の情報を提供するネットワーク層のインターネット プロトコル。RFC 792 に規定されています。

**ICMP フラッド** プロトコル実装で処理可能な数よりも多いエコー要求（「ping」）パケットをホストに送信する DoS 攻撃。

**IDAPI** Intrusion Detection Application Programming Interface。IPS アーキテクチャ アプリケーション間に単純なインターフェイスを提供します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。

**IDCONF** 侵入検知設定。侵入検知と予防システムの設定に使用される操作メッセージを定義するデータ形式の標準です。

**IDENT** RFC 1413 で指定された Ident プロトコルは、特定の TCP 接続のユーザの識別に役立つインターネット プロトコルです。

**IDIOM** Intrusion Detection Interchange and Operations Messages。侵入検知システムによって報告されるイベント メッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の標準です。

**IDM** IPS Device Manager。センサーの設定と管理が可能な Web ベースのアプリケーションです。IDM の Web サーバはセンサーに常駐します。この Web サーバには、Internet Explorer や Firefox などの Web ブラウザでアクセスできます。

**IDMEF** Intrusion Detection Message Exchange Format。IETF Intrusion Detection Working Group による標準草案です。

**IME** IPS Manager Express。システムのヘルス モニタリング、イベント モニタリング、レポートおよび最大 10 のセンサーの設定を行うことができるネットワーク管理アプリケーション。

**InterfaceApp** IPS のコンポーネントの 1 つ。バイパスおよび物理設定を処理し、ペアにするインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。

**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 イベント アクションが選択されている場合に作成されます。iplog は、WireShark および TCPDUMP で読み取り可能な libpcap 形式で格納されます。

**IPS** 侵入防御システム。ネットワーク トラフィックの分析技術を使用して、ネットワークへの侵入の存在をユーザに警告するシステムです。

**IPS データまたはメッセージ** IPS アプリケーション間でコマンド / コントロール インターフェイスを介して転送されるメッセージ。

**IPv6** IP バージョン 6。IP の現在のバージョン（バージョン 4）に代わるバージョン。IPv6 ではパケット ヘッダーのフロー ID がサポートされており、フローの識別が可能です。以前は IPng（next generation（次世代））と呼ばれていました。

**IP アドレス** TCP/IP を使用するホストに割り当てられる 32 ビット アドレス。IP アドレスは、5 つのクラス（A、B、C、D、または E）のいずれかに属し、ピリオドで区切られた 4 つのオクテット（ドット付き 10 進形式）で記述されます。各アドレスはネットワーク番号、オプションのサブネットワーク番号、およびホスト番号で構成されます。ルーティングにはネットワーク番号とサブネットワーク番号を組み合わせて使用し、ネットワーク内またはサブネットワーク内の個別のホストのアドレス指定にはホスト番号を使用します。IP アドレスからのネットワーク情報とサブネットワーク情報の抽出には、サブネット マスクを使用します。

**IP スプーフィング** IP スプーフィング攻撃は、ネットワーク外の攻撃者が信頼されたユーザになりすますことによって発生します。攻撃者は、ネットワークの IP アドレス範囲内の IP アドレスを使用するか、信頼され、ネットワーク上の指定されたリソースへのアクセスが可能な、許可された外部 IP アドレスを使用して、このなりすましを行います。攻撃者が IPSec セキュリティ パラメータにアクセスした場合は、その攻撃者が企業ネットワークへのアクセスを許可されたリモート ユーザを偽装する可能性があります。

**ISL** スイッチ間リンク スイッチとルータの間のトラフィック フローとして VLAN 情報を維持するシスコ独自のプロトコル。

## J

**Java Web Start** Java Web Start は、プラットフォームに依存しない、安全で堅牢な展開テクノロジーです。開発者は、アプリケーションを標準 Web サーバで利用可能にすることで、すべての機能を備えたアプリケーションをユーザに展開できます。ユーザは任意の Web ブラウザを使用してアプリケーションを起動し、常に最新バージョンを使用できます。

**JNLP** Java Network Launching Protocol。XML ファイル形式で定義され、Java Web Start アプリケーションの起動方法を指定しています。JNLP は、起動メカニズムを正しく実装する方法を定義したルールのセットで構成されています。

## K

**KB** ナレッジ ベース。異常検出で学習され、ワーム ウイルス検出に使用されるしきい値のセット。

**Knowledge Base** 「KB」を参照してください。

## L

**LACP** リンク集約制御プロトコル。LACP は、LAN ポート間で LACP パケットを交換することで、EtherChannel リンクの自動作成を支援します。このプロトコルは、IEEE 802.3ad で定義されています。

**LAN** ローカルエリア ネットワーク。特定のホストのローカルとなっているレイヤ 2 ネットワーク ドメインを指します。同じ LAN 上の 2 つのホストで交換されるパケットは、レイヤ 3 ルーティングを必要としません。

**LOKI** リモート アクセス、バック ドア 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、悪意のあるコードによってペイロード サイズの小さい ICMP 応答の送信に使用できる ICMP トンネルが作成されます。

## M

**MainApp** IPS のメイン アプリケーション。オペレーティング システムのブート後、センサーで最初に起動するアプリケーションです。設定を読み取ってアプリケーションを起動し、アプリケーションの開始および終了とノードの再起動を扱い、ソフトウェアのアップグレードを処理します。

**MD5** Message Digest 5。128 ビット ハッシュを作成する単方向のハッシュ アルゴリズム。MD5 とセキュア ハッシュ アルゴリズム（SHA）は両方とも MD4 のバリエーションであり、MD4 のハッシュ アルゴリズムのセキュリティを強化するように設計されています。シスコは、IPSec フレームワーク内での認証にハッシュを使用します。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。

**Meta エンジン** スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。

**MIB** 管理情報ベース。SNMP や CMIP などのネットワーク管理プロトコルにより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、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

**MIME** Multipurpose Internet Mail Extension。電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045 で定義されています。

**module** スイッチ、ルータ、またはセキュリティ アプライアンス シャーシのリムーバブル カード。ASA 5585-X IPS SSP は、IPS モジュールです。

**MPF** モジュラ ポリシー フレームワーク。Cisco IOS ソフトウェアのモジュラ QoS CLI と同様の方法でセキュリティ アプライアンスの機能を設定するための手段です。

**MSFC、MSFC2** マルチレイヤ スイッチ フィーチャ カード。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、スイッチの L3 ルーティングを実行します。

**MSRPC** Microsoft Remote Procedure Call。MSRPC は、Microsoft による DCE RPC メカニズムの実装です。Microsoft は、Unicode 文字列、暗黙ハンドル、インターフェイスの継承（DCOM で広く使用される）、および DCE/RPC にすでに存在する可変文字列や構造パラダイムでの複雑な計算のサポートを追加しました。

**MySDN** My Self-Defending Network。IDM および IME のシグニチャ定義セクションの一部。シグニチャに関する詳細情報を提供します。

## N

**NAC** Network Access Controller。「ARC」を参照してください。

**NAS-ID** ネットワーク アクセス ID。クライアントが、認証を試みているサービスのタイプを伝えるためにサーバに送信する識別子。

**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。シスコ サービス契約による交換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。コンピュータ システムとのネットワーク通信機能を提供するボード。

**NMS** Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。NMS は、一般的に適度にパワーのある装備の整ったコンピュータで、エンジニアリング ワークステーションなどです。NMS はエージェントと通信して、ネットワーク統計情報やリソースを追跡し続けるのに役立ちます。

**Normalizer エンジン** IP および TCP ノーマライザが機能する方法を設定し、IP および TCP ノーマライザに関連するシグニチャ イベントに設定を提供します。

**NOS** ネットワーク オペレーティング システム。分散ファイル システムを指すときに使用される総称的な用語。LAN Manager、NetWare、NFS、VINES などが含まれます。

**NotificationApp** IPS のコンポーネントの 1 つ。アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp は、パブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的な状態に関する情報を提供します。

**NTP** ネットワーク タイム プロトコル。インターネット内に置かれているラジオ クロックおよびアトミック クロックを参照することにより、正確な現地時間を維持する TCP 上に構築されたプロトコル。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

**NTP サーバ** ネットワーク タイム プロトコル（Network Timing Protocol）サーバ。NTP を使用するサーバ。NTP は、TCP 上に構築されたプロトコルで、インターネット上にあるラジオおよびアトミック クロックを参照して正確なローカル タイムを維持します。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

**NVRAM** 不揮発性読み取り / 書き込みメモリ。ユニットの電源オフ時に内容を保持する RAM。

## O

**OIR** 活性挿抜 システム電源のオフ、コンソール コマンドの入力、他のソフトウェアやインターフェイスのシャットダウンを伴わずにカードの追加、交換、取り外しを行うことができる機能。

**OPS** Outbreak Prevention Service。

## P

**PAgP** Port Aggregation Control Protocol。PAgP は、LAN ポート間で PAgP パケットを交換することで、EtherChannel リンクの自動作成を支援します。シスコ独自のプロトコルです。

**PAM** アプリケーションに AAA 機能を提供するソフトウェア モジュール。

**PAP** パスワード認証プロトコル。最もよく使用される RADIUS メッセージング プロトコル。

**PASV ポート スプーフィング** 保護された FTP サーバから非 FTP ポートへの接続をファイアウォール経由で開こうとする試み。ファイアウォールが不正接続を開くことによって、FTP 227 **passive** コマンドを誤って解釈したときに発生します。

**PAT** ポート アドレス変換。NAT より制限された変換方式で、1 つの IP アドレスと複数の異なるポートを使用してネットワークのホストを表します。

**PAWS** Protection Against Wrapped Sequence。ハイ パフォーマンス TCP ネットワークでのシーケンス番号のラップに対する保護。RFC 1323 を参照してください。

**PCI** Peripheral Component Interface。Intel ベースのコンピュータで使用される最も一般的な周辺装置拡張バス。

**PDU** プロトコル データ ユニット。パケットの OSI 用語。「BPDU」と「パケット」も参照してください。

**PEP** Cisco Product Evolution Program。PEP は、センサーの PID、VID、および SN で構成される UDI 情報です。PEP は、電子クエリー、製品ラベル、出荷品目を通して、ハードウェア バージョンとシリアル番号を提供します。

**PER** パック済みエンコーディング ルール。PER では、すべてのタイプを同じようにエンコードする一般的なエンコード スタイルを使用せずに、日付タイプに基づいてエンコードを特化して、よりコンパクトな表現を生成します。

**PFC** ポリシー フィーチャ カード（Policy Feature Card）。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、VACL パケットのフィルタ処理をサポートします。

**PID** 製品 ID。UDI の 3 つのパートの 1 つを構成する注文可能製品識別子です。UDI は PEP ポリシーの一部です。

**ping** Packet Internet Groper。ネットワーク デバイスへの到達可能性をテストするために、IP ネットワークでよく使用されます。ターゲット ホストに ICMP エコー要求パケットを送信し、エコー応答返信をリッスンします。

**PIX ファイアウォール** Private Internet Exchange Firewall。シスコのネットワーク セキュリティ デバイスで、プログラミングによってネットワーク間でアドレスとポートをブロックしたり使用可能にしたりできます。

**PKI** 公開キー インフラストラクチャ（Public Key Infrastructure）。クライアントの X.509 証明書を使用した HTTP クライアントの認証です。

**Point-to-Point（P2P; ポイントツーポイント）** ピアツーピア。P2P ネットワークでは、ファイル共有の目的で、同時にクライアントとサーバの両方の機能を果たすノードが使用されます。

**POST** 電源投入時自己診断テスト。ハードウェア デバイスの電源を入れると、そのデバイスで実行されるハードウェア診断のセット。

**Post-ACL** ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの後ろにエントリを入れる ACL を指定します。

**Pre-ACL** ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの前にエントリを入れる ACL を指定します。

## Q

**Q.931** ISDN ネットワーク接続の確立、維持、およびクリアする信号送信に関する ITU-T 仕様。

**QoS** Quality of Service。伝送システムのパフォーマンスをもとに、その送信品質とサービスのアベイラビリティを表します。

## R

**RADIUS** リモート認証ダイヤルイン ユーザ サービス。システムに対して、ネットワーク サービスに接続し、使用するための一元化された AAA 機能を提供するネットワーキング プロトコル。

**RAM** ランダムアクセス メモリ。マイクロプロセッサによる読み書きが可能な揮発性メモリ。

**RAS** Registration, Admission, and Status Protocol。管理機能を実行するためにエンドポイントとゲートキーパー間で使用されるプロトコル。RAS シグナリング機能は、VoIP ゲートウェイとゲートキーパー間で、登録、許可、帯域幅変更、ステータス、および解放手順を実行します。

**RBCP** ルータ ブレード制御プロトコル。RBCP は SCP に基づいていますが、ルータ アプリケーション専用に変更されています。イーサネット インターフェイスで動作し、メッセージに 802.2 SNAP カプセル化を使用するように設計されています。

**regex** 「正規表現」を参照。

**Remote Authentication Dial In User Service** 「RADIUS」を参照してください。

**RMA** 返品許可。不具合のあるハードウェアを返却し、交換品を受け取るシスコ プログラム。

**ROMMON** ROM モニタ（Read-Only-Memory Monitor）。ROMMON は、復旧のためにシステム イメージをセンサーに TFTP 転送できます。

**RPC** リモート プロシージャ コール。クライアント / サーバ コンピューティングの技術的な基礎。RPC は、クライアントで作成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。

**RSM** Router Switch Module。Catalyst 5000 スイッチに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** Real-Time Transport Protocol（リアルタイム転送プロトコル）。一般に、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャストのネットワーク サービスとして、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供するように設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプ処理、配信のモニタリングなどのサービスをリアルタイム アプリケーションに提供します。

**RTT** ラウンドトリップ時間。ネットワークによってホストに課されるパケットを送信してから受信確認を受け取るまでの遅延時間の測定値。

**RU** ラック ユニット。ラックは、ラック ユニットで測定されます。1 RU は、44 mm つまり 1.75 インチです。

## S

**SCEP** Simple Certificate Enrollment Protocol。PKCS#7 および PKCS#10 の使用によって既存のテクノロジーを活用した、シスコの PKI 通信プロトコルです。SCEP は進化した登録プロトコルです。

**SCP** Switch Configuration Protocol。イーサネット上で直接実行されるシスコの制御プロトコル。

**SDEE** Security Device Event Exchange。セキュリティ デバイスのイベントを伝える、製品に依存しない標準。さまざまなタイプのセキュリティ デバイスによって生成されるイベントを伝えるために必要な拡張性機能を追加します。

**SDEE サーバ** リモート クライアントからのイベントの要求を受け入れます。

**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、および報告の機能を提供します。IDS MC とともに使用されます。

**SensorApp** IPS のコンポーネントの 1 つ。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 トラフィックで悪意のあるコンテンツを分析します。パケットは、センサー上のネットワーク インターフェイスからパケットを収集するように設計されたプロデューサによって供給されたプロセッサのパイプラインを通ります。SensorApp は分析エンジンを実行するスタンドアロンの実行可能ファイルです。

**Service エンジン** DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SQL、NTP、P2P、RPC、SMB、SNMP、SSH、TNS などの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。

**SFP** Small Form-Factor Pluggable。多くの場合、光ケーブルをファイバ インターフェイスに適応させる光ファイバ トランシーバを指します。詳細については、GBIC を参照してください。

**shun コマンド** 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。PIX ファイアウォールでブロックしているときに、ARC によって使用されます。

**SMB** サーバ メッセージ ブロック。LAN マネージャおよび同様の NOS で、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使用され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。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** Serial Number（シリアル番号）。UDI に含まれます。SN はシスコ製品のシリアル番号です。

**SNAP** サブネットワーク アクセス プロトコル。サブネットワーク内のネットワーク エンティティとエンドシステム内のネットワーク エンティティ間で動作するインターネット プロトコル。SNAP は、IEEE ネットワーク上で IP データグラムと ARP メッセージをカプセル化する標準方式を指定します。エンド システム内の SNAP エンティティは、サブネットワークのサービスを利用して、3 つの重要な機能（データ転送、接続管理、および QoS 選択）を実行します。

**SNMP** 簡易ネットワーク管理プロトコル。TCP/IP ネットワークでほぼ独占的に使用されているネットワーク管理プロトコル。SNMP を使用すると、ネットワーク デバイスのモニタリングと制御、および設定、統計情報収集、パフォーマンス、セキュリティの管理が可能になります。

**SNMP2** SNMP Version 2。ネットワーク管理プロトコルのバージョン 2。SNMP2 では、集中型および分散型のネットワーク管理方式がサポートされ、SMI、プロトコル動作、管理アーキテクチャ、およびセキュリティが改善されています。

**SPAN** スイッチド ポート アナライザ。Catalyst 5000 スイッチの機能。既存のネットワーク アナライザのモニタリング機能をスイッチ型イーサネット環境に拡張します。SPAN は、1 つのスイッチド セグメントのトラフィックを事前定義済みの SPAN ポートにミラーリングします。SPAN ポートに接続されたネットワーク アナライザで、その他の任意の Catalyst スイッチド ポートからのトラフィックをモニタできます。

**SQL** 構造化照会言語。リレーショナル データベースの定義およびアクセスに使用される国際的な標準言語。

**SRAM** 電源が供給される限り内容を保持する RAM のタイプ。SRAM は、DRAM のように継続的な更新は必要ありません。

**SSH** セキュア シェル。強力な認証と安全な通信を使用してネットワーク上の別のコンピュータにログインするユーティリティ。

**SSL** Secure Socket Layer。e- コマースにおけるクレジットカード番号の転送など、安全なトランザクションを提供するために使用されるインターネット用暗号化テクノロジー。

**Stacheldraht** ICMP プロトコルに依存する DDoS ツール。

**State エンジン** HTTP 文字列のステートフル検索。

**String エンジン** シグニチャ エンジンの 1 つ。正規表現ベースのパターン検査、および、TCP、UDP、ICMP などの複数の転送プロトコルのアラート機能を提供します。

**switch** 各フレームの宛先アドレスに基づいて、フレームのフィルタリング、転送、およびフラッディングを行うネットワーク デバイス。スイッチは、OSI モデルのデータリンク層で動作します。

**SwitchApp** IPS のコンポーネントの 1 つ。IPS 4500 シリーズ センサー。外部モニタリング インターフェイスを提供するスイッチを搭載しています。SwitchApp は InterfaceApp およびセンサーの初期化スクリプトを有効にし、スイッチと通信を行ったり、制御を行ったりします。

**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。世界には、4 つの TAC があります。

**TACACS+** Terminal Access Controller Access Control System Plus（ターミナル アクセス コントローラ アクセス コントロール システム プラス）。シスコが強化した専用の Terminal Access Controller Access Control System（TACACS）。認証、許可、アカウンティングに追加サポートを提供します。

**TCP** 伝送制御プロトコル。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

**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、稼働中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。さまざまなオプションを使用して、各パケットの要約情報と詳細情報を表示できます。詳細については、http://www.tcpdump.org/ を参照してください。

**Telnet** TCP/IP プロトコル スタックにおける標準の端末エミュレーション プロトコル。Telnet はリモート端末接続に使用され、ユーザはこれを使用してリモート システムにログインし、そのリソースを、ローカル システムに接続されているかのように使用することができます。Telnet は RFC 854 で定義されています。

**TFN** Tribe Flood Network。偽装の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタリングしたりする手段を妨げることができる一般的な DoS 攻撃。

**TFN2K** Tribe Flood Network 2000。偽装の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタリングしたりする手段を妨げることができる一般的な DoS 攻撃。

**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。

**threshold** 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。

**TLS** Transport Layer Security。ピアの ID をネゴシエートし、暗号化通信を確立するために、ストリーム転送で使用されるプロトコル。

**TNS** Transparent Network Substrate。データベース アプリケーションに、すべての業界標準ネットワーク プロトコルに対する 1 つの共通インターフェイスを提供します。TNS により、データベース アプリケーションは、異なるプロトコルを使用して他のデータベース アプリケーションにネットワークから接続できます。

**TPKT** トランスポート パケット。RFC 1006 で定義された、パケット内のメッセージの境界を区切る方法。プロトコルでは、TCP の上で ISO トランスポート サービスを使用します。

**traceroute** 多くのシステム上で使用できる、パケットが宛先まで通るパスを追跡するプログラム。ほとんどの場合、ホスト間のルーティングの問題のデバッグに使用されます。traceroute プロトコルは RFC 1393 でも定義されています。

**Traffic ICMP エンジン** TFN2K、LOKI、DDOS などの非標準プロトコルを分析します。

**trap** 特別に定義された状況やしきい値の到達などの重要なイベントの発生を知らせるために、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。

**Trojan エンジン** BO2K や TFN2K などの非標準プロトコルからのトラフィックを分析します。

**trunk** ネットワーク トラフィックが移動する 2 つのスイッチ間の物理および論理接続。バックボーンは多数のトランクで構成されています。

## U

**UDI** Unique Device Identifier。すべてのシスコ製品に一意の ID を提供します。UDI は、PID、VID、および SN で構成されています。UDI は、Cisco IPS ID PROM に格納されます。

**UDLD** 単一方向リンク検出。LAN ポートに接続された光ファイバまたは銅製イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができるシスコ独自のプロトコルです。単一方向のリンクはスパニングツリー トポロジ ループなど、さまざまな問題の原因となる可能性があるため、単一方向のリンクが検出された場合、UDLD は影響を受けた LAN ポートをシャットダウンしてアラートを送信します。

**UDP** ユーザ データグラム プロトコル。TCP/IP プロトコル スタックのコネクションレス型トランスポート層プロトコルです。UDP は、確認応答や配信保証なしでデータグラムを交換する単純なプロトコルです。エラー処理と再送信は、他のプロトコルで処理する必要があります。UDP は RFC 768 で定義されています。

**UPS** 無停電電源装置。

**UTC** 協定世界時。経度が 0 度のタイムゾーン。旧名称はグリニッジ標準時（GMT）およびズールー時。

**UTF-8** 8 ビットの Unicode Transformation Format。Unicode の可変長文字エンコーディング。UTF-8 は、Unicode 文字セットのすべての文字を表すことができ、ASCII と下位互換性があります。

## V

**VACL** VLAN ACL。スイッチを経由して渡されるすべてのパケット（VLAN 内および VLAN 間）をフィルタする ACL。セキュリティ ACL とも言います。

**VID** バージョン ID。UDI に含まれます。

**VIP** Versatile Interface Processor。Cisco 7000 および Cisco 7500 シリーズ ルータで使用されるインターフェイス カード。VIP は、マルチレイヤ スイッチングを行い、Cisco IOS を実行します。VIP の最新バージョンは VIP2 です。

**VLAN** バーチャル LAN（Virtual Local Area Network）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイス グループ。実際には多数の異なる LAN セグメントに配置されている場合でも、同じケーブルに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づいているため、柔軟性がとても高い機能です。

**VMS** CiscoWorks VPN/Security Management Solution。さまざまな Web ベース ツールを組み合わせた、ネットワーク セキュリティ アプリケーション スイート。これらのツールは、エンタープライズ VPN、ファイアウォール、ネットワーク侵入検知システム、およびホストベースの侵入防御システムを構成、管理、およびトラブルシューティングするために使用できます。

**VoIP** Voice over IP。POTS のような機能、信頼性、および音声品質を備えながら、IP ベースのインターネット上で通常のテレフォニー スタイルの音声を伝送する機能。VoIP を使用すれば、ルータから IP ネットワーク上で音声トラフィック（通話や FAX など）を伝送できます。VoIP では、DSP が音声信号をフレームに分割します。その後、フレームは、2 つずつ連結され、音声パケットに保存されます。これらの音声パケットは、ITU-T 仕様の H.323 に従って、IP を使用して送信されます。

**VPN** バーチャル プライベート ネットワーク（ネットワーキング）ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

**VTP** VLAN トランキング プロトコル。ネットワーク全体で VLAN の追加、削除、および名前の変更を管理するシスコのレイヤ 2 メッセージング プロトコル。

**vulnerability** コンピュータやネットワークの悪用パターンが開始されやすい状況を許す、当該コンピュータやネットワークの 1 つ以上の属性。

## W

**WAN** ワイドエリア ネットワーク。広範な地理的領域に分散するユーザにサービスを提供し、多くの場合、共通の通信事業者が提供する送信デバイスを使用するデータ通信ネットワークです。フレームリレー、SMDS、および X.25 が WAN の代表例です。

**Web サーバ** IPS のコンポーネントの 1 つ。リモート HTTP クライアント要求を待機し、適切なサーブレット アプリケーションを呼び出します。

**WHOIS** ドメイン名または IP アドレスの所有者を特定する公式データベースへのクエリーに使用される TCP ベースのクエリー / 応答プロトコル。

**Wireshark** Wireshark は、フリーの Unix および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼働中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。対話的にキャプチャ データをブラウズし、各パケットの要約情報と詳細情報を表示できます。Wireshark には、機能豊富な表示フィルタ言語や TCP セッションの再構築されたストリームの表示機能など、いくつかの強力な機能があります。詳細については、http://www.wireshark.org を参照してください。

## X

**X.509** 証明書に含まれる情報を定義する標準。

**XML** eXtensible Markup Language。異種ホスト間のデータ交換に使用されるテキスト ファイル形式。

**XPI** クロス パケット インスペクション。複数のパケットにわたって検索し、パケットおよびペイロードの再構成を行える、TCP で使用されているテクノロジー。

## Z

**zone** 異常検出で使用される、内部、不正、または外部ゾーンにソートされる宛先 IP アドレスのセット。

## 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。TCP リセット、ホストのブロック、接続のブロック、IP ログ収集、アラート トリガー パケットのキャプチャなどがあります。

**アクティブ ACL** ARC によって作成、管理される ACL。ルータのブロック インターフェイスに適用されます。

**アスペクト バージョン** IDIOM のデフォルト コンフィギュレーション設定と関連付けられたバージョン情報。たとえば、シスコは攻撃シグニチャの標準セットを、S アスペクトのデフォルト設定の集合として公開しています。S アスペクトのバージョン番号は、シグニチャ更新パッケージ ファイル名では S の後ろに表示されます。その他のアスペクトとしては、ウイルス シグニチャ定義を含む V アスペクト、IDIOM 署名キーを含むキーアスペクトがあります。

**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** 1 つのパケット内に含まれる悪用を表します。たとえば、「ping of death」攻撃は、単一の異常に大きな ICMP パケットです。

**アプリケーション** Cisco IPS 環境で動作するように設計された任意のプログラム（プロセス）。

**アプリケーション イメージ** センサーの操作に使用される永続的なストレージ デバイスに格納される完全な IPS イメージ。

**アプリケーション インスタンス** IPS 環境の特定のハードウェアで動作する特定のアプリケーション。アプリケーション インスタンスには、その名前と、ホスト コンピュータの IP アドレスによってアドレス可能です。

**アプリケーション パーティション** IPS ソフトウェア イメージを含むブート可能ディスクまたはコンパクトフラッシュ パーティション。

**アラーム 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、受信した各イベントに対するアラートの生成です。

**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。

**暗号キー** 平文と暗号文の間の変換に使用されるシークレット バイナリ データ。暗号化と復号化に同じ暗号キーが使用される場合を対称と言います。暗号キーが暗号化と復号化のいずれかに使用される（両方ではない）場合を非対称と言います。

**異常検出** AD。正常なネットワーク トラフィックのベースラインを作成し、そのベースラインを使用してワームに感染したホストを検出するセンサー コンポーネント。

**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（30 MB）。

**インライン インターフェイス** センサーが 1 つのインターフェイスで受け取ったすべてのトラフィックをペアの他方のインターフェイスに転送するように設定された物理インターフェイスのペア。

**インライン モード** ネットワークに出入りするすべてのパケットがセンサーを通過する必要があります。

**ウイルス** コンピュータ ソフトウェアの隠された、自己複製セクション。通常、感染によって伝播する悪意のあるロジックです。自分自身のコピーを別のプログラムに挿入し、その一部となります。ウイルスは自力では実行できません。ウイルスをアクティブにするには、ホスト プログラムを実行する必要があります。

**ウイルス更新** 特にウイルスに対応したシグニチャ更新。

**ウォッチ リスト レーティング** WLR。0 ～ 100 の範囲で CSA MC ウォッチ リストに関連付けられる重み（CSA MC は 0 ～ 35 の範囲のみを使用します）。

**エスケープ表現** 正規表現で使用されます。文字を 16 進数値で表すことができます。たとえば、「a」に相当する \x61 を使用した場合、\x61 は文字「a」を表すエスケープ表現です。

**エンジン** センサーのコンポーネントの 1 つ。特定の 1 つのカテゴリで多数のシグニチャをサポートするように設計されています。各エンジンには、シグニチャの作成や既存のシグニチャの調整に使用できるパラメータがあります。

**エンタープライズ ネットワーク** 企業などの組織内で大部分の主要ポイントを接続する、大規模で多様なネットワーク。私的に所有され、保守される点で WAN とは異なります。

## か

**仮想化された検知インターフェイス** 仮想化されたインターフェイスはサブインターフェイスに分割され、各サブインターフェイスは VLAN のグループで構成されます。1 つ以上のサブインターフェイスに 1 つの仮想センサーを関連付け、それらのサブインターフェイスに異なる侵入防止ポリシーを割り当てることができます。物理インターフェイスとインライン インターフェイスの両方を仮想化できます。

**仮想化されていない検知インターフェイス** 仮想化されていない検知インターフェイスは、サブインターフェイスに分割されず、インターフェイス全体を 1 つの仮想センサーだけに関連付けることができます。

**仮想センサー** シグニチャ エンジンのセンシング インターフェイスと設定ポリシー、およびシグニチャ エンジンに適用するアラーム フィルタの論理グループ。つまり、それぞれが異なるシグニチャの動作とトラフィック供給で設定された、同一アプライアンス上で動作する複数の仮想センサーです。

**カットスルー アーキテクチャ** カットスルー アーキテクチャとは、パケットスイッチング システムの設計方法の 1 つです。パケットがスイッチに到達すると、パケット内の最初の数バイトのみを読み取って宛先アドレスを確認し、ほぼ瞬時にパケットの転送を開始します。この手法はパフォーマンスを向上させます。

**偽陰性** 不正なトラフィックが検出されたときにシグニチャが起動されない状態。

**ギガビット イーサネット** 1996 年に IEEE（電気電子学会）802.3z 規格委員会によって承認された、高速イーサネットの規格。

**脅威レーティング** TR。脅威レーティングは、モニタ対象のネットワークでアラートの脅威を示す応答アクションに基づいて、攻撃のリスク レーティングの数値的な減少を表す 0 ～ 100 の値です。

**偽陽性** 正常なトラフィックまたは良好なアクションによってシグニチャが起動される状態。

**共有秘密情報** セキュア通信に関わる当事者のみが知っているデータ。共有秘密には、パスワード、パスフレーズ、大きな数、ランダムに選択したバイトの配列などがあります。

**拒否フィルタ プロセッサ** IPS のプロセッサ。攻撃者拒否機能を処理します。拒否されたソース IP アドレスのリストを維持します。

**グローバル相関** IPS センサーは、グローバル相関データベースを通して他のデバイスと情報を共有し、すべてのデバイスの有効性を総合的に向上させます。

**グローバル相関クライアント** 更新を取得し、ローカル グローバル相関データベースにインストールする CollaborationApp のソフトウェア コンポーネント。

**グローバル相関データベース** IPS センサーなどのコラボレーション デバイスから取得され、これらの間で共有される情報の集合。

**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。

**攻撃重大度レーティング** ASR。脆弱性の悪用が成功した場合の重大度に関連付けられた重み。攻撃重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）から計算されます。攻撃重大度レーティングはシグニチャごとに設定され、検出されたイベントどれだけ危険かを示します。

**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 における、同じ管理ドメイン内の管理対象デバイスと NMS の論理グループ。

**コンソール 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。

## さ

**サービス パック** 不具合の修正のリリースおよび新しいシグニチャ エンジンのサポートに使用されます。サービス パックには、最後のベース バージョン（マイナーまたはメジャー）以降のすべての不具合の修正と新しい不具合の修正が含まれます。

**再構成** ソースまたは中間ノードでフラグメント化された IP データグラムを宛先で元に戻すこと。

**再パッケージ リリース** パッケージングまたはインストーラの不具合に対処したリリース。

**サブシグニチャ** 一般のシグニチャより細分化されたシグニチャ。通常は、より広い範囲のシグニチャをさらに定義します。

**時間プロセッサ** IPS のプロセッサ。タイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、古いデータベース エントリを有効期限切れにすることと時間に依存する統計情報を計算することです。

**シグニチャ** シグニチャはネットワーク情報を抽出し、典型的な侵入アクティビティを示すルール セットと比較します。

**シグニチャ アップデート** ワーム、DDOS、ウイルスなどの悪意のあるネットワーク アクティビティを認識するためのルール セットを含む実行可能ファイル。シグニチャ更新は独立してリリースされ、必要なシグニチャ エンジン バージョンに依存し、独自のバージョニング スキームを持ちます。

**シグニチャ イベント アクション オーバーライド** リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定されたリスク レーティングしきい値の範囲に入るすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立し、アクション タイプごとに別々の設定値を持ちます。

**シグニチャ イベント アクション ハンドラ** 要求されたアクションを実行します。シグニチャ イベント アクション ハンドラからの出力は、実行されているアクションと、イベント ストアに書き込まれる evIdsAlert（ある場合）です。

**シグニチャ イベント アクション フィルタ** シグニチャ イベントのシグニチャ ID、アドレス、リスク レーティングに基づいてアクションを差し引きます。シグニチャ イベント アクション フィルタへの入力は、シグニチャ イベントアクション オーバーライドによって追加された可能性のあるアクションを含むグニチャ イベントです。

**シグニチャ イベント アクション プロセッサ** イベント アクションを処理します。イベント アクションは、イベント リスク レーティングのしきい値と関連付けることができます。アクションが発生するには、この値を上回る必要があります。

**シグニチャ エンジン** センサーのコンポーネントの 1 つ。特定のカテゴリで多数のシグニチャをサポートします。エンジンは、パーサーとインスペクタで構成されています。各エンジンには規定のパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。

**シグニチャ エンジンのアップデート** 新しいシグニチャ アップデートをサポートするバイナリ コードを含む、独自のバージョニング スキームを持つ実行可能ファイル。

**シグニチャ忠実度レーティング** SFR。ターゲットに関する具体的な情報がない場合に、シグニチャをどの程度忠実に実行するかに関連付ける重みを示します。シグニチャ忠実度レーティングはシグニチャごとに設定され、シグニチャが、それが表しているイベントまたは条件をどれだけ正確に検出するかを示します。

**シグニチャ分析プロセッサ** IPS のプロセッサ。処理中のパケットを対象とするように設定された、ストリームベースではないインスペクタにパケットを発送します。

**システム イメージ** センサー全体のイメージの再作成に使用される、IPS アプリケーションとリカバリの完全なイメージ。

**自動ステート** 通常自動ステート モードでは、VLAN 上のポートが少なくとも 1 つアップしていると、レイヤ 3 インターフェイスはアップしたままになります。VLAN 上のポートにロード バランサやファイアウォール サーバなどのアプライアンスが接続されている場合、これらのポートを自動ステート機能から除外するように設定して、これらのポートが非アクティブの場合でも転送 SVI がダウンしないようにすることができます。

**出力** ネットワークを離れるトラフィック。

**証明書** 公開キーなどのユーザまたはデバイス属性のデジタル表現であり、信頼できる秘密キーで署名されています。

**侵入検知システム** IDS。不正な方法によるシステム リソースへのアクセスの試みを発見し、リアルタイムまたはそれに近い形で警告を与えることを目的として、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。

**信頼できるキー** ユーザが信頼する公開キー。特に、認証パスで最初の公開キーとして使用される公開キーです。

**信頼できる証明書** 証明書のユーザが検証テストなしで有効であると信頼する証明書。特に、認証パスで最初の公開キーの提供に使用される公開キー証明書です。

**据え置き** 平らな面に設置する場合にセンサー底部にゴム脚を取り付けます。ゴム脚を使用すると、センサーの周りに適正なエアーフローが確保され、振動を吸収するので、ハードディスク ドライブへの衝撃が軽減されます。

**ストリーム再構成プロセッサ** IPS のプロセッサ。さまざまなストリームベース インスペクタでのパケットが正しい順序で到着するように TCP ストリームの順序を変更します。TCP ストリームの正規化も行います。Normalizer エンジンでは、アラート アクションと拒否アクションをイネーブルまたはディセーブルにできます。

**スニファ インターフェイス** 「センシング インターフェイス」を参照。

**スパニングツリー** ネットワーク トポロジのループのないサブセット。

**スリーウェイ ハンドシェイク** 2 つのプロトコル エンティティが接続の確立中に同期するプロセス。

**スレーブ ディスパッチ プロセッサ** IPS のプロセッサ。デュアル CPU システムで見られるプロセス。

**正規表現** データ ストリームまたはファイル内で指定された文字シーケンスを検索する方法を定義できるメカニズム。正規表現は高機能かつ柔軟な表記法で、テキストを表現するためのミニ プログラミング言語のようなものです。パターン マッチングでは、正規表現によりあらゆる任意のパターンを簡潔に表記できます。

**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** CT。特定のアプリケーション インスタンスに対して出されたコマンドを含む IPS メッセージ。制御トランザクションは、管理アプリケーションと IPS センサー間、または同じ IPS センサー上のアプリケーション間で送信できます。制御トランザクションには、*start*、*stop*、*getConfig* などがあります。

**製造イメージ** 製造によってイメージ センサーに使用される完全な IPS システム イメージ。

**セキュア シェル プロトコル** 伝送制御プロトコル（TCP）アプリケーションを介して、ルータへのセキュア リモート接続を提供するプロトコルです。

**セキュリティ コンテキスト** 1 つの適応型セキュリティ アプライアンスは複数の仮想デバイスに分割できます。これをセキュリティ コンテキストと呼びます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。

**接続ブロック** 特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。

**センサー** 侵入検知エンジンのことです。不正行為の兆候を探してネットワーク トラフィックを分析します。

**センシング インターフェイス** 目的のネットワーク セグメントをモニタする、センサー上のインターフェイス。センシング インターフェイスは、無差別モードです。つまり、IP アドレスを持たず、モニタしたセグメント上では見えません。

**全二重** 送信ステーションと受信ステーション間でデータを同時伝送する機能。

**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。

**ソフトウェア バイパス** 検査なしでトラフィックを IPS システム経由で通過させます。

## た

**ダークネット** ユーザが信頼する人々とのみ接続する仮想プライベート ネットワーク。一般に、ダークネットは通信する人々の閉じた、プライベートな任意のタイプのグループを意味しますが、多くの場合、特にファイル共有ネットワークに使用されます。すべての秘密の通信ネットワークに対して集合的に使用されることもあります。

**ターゲットの価値レーティング** TVR。ターゲットの認識値に関連付けられた重み。ターゲットの価値レーティングはユーザ設定可能な値（zero、low、medium、high、または mission critical）であり、ネットワーク資産の IP アドレスを通じてその重要性を表します。

**ターミナル サーバ** 他のシリアル デバイスに接続された複数の低速な非同期ポートを搭載したルータ。ターミナル サーバは、センサーを含むネットワーク機器をリモートで管理する場合に利用できます。

**単一方向リンク検出** 「UDLD」を参照してください。

**チューニング** 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。

**データグラム** 事前に仮想回線を確立することなく、伝送媒体上のネットワーク層ユニットとして送信される情報の論理的なグループ化。IP データグラムは、インターネットにおける主な情報単位です。セル、フレーム、メッセージ、パケット、セグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

**データベース プロセッサ** IPS のプロセッサ。シグニチャの状態とフロー データベースを管理します。

**適応型セキュリティ アプライアンス** ASA。ファイアウォール、VPN コンセントレータ、および侵入防御ソフトウェア機能が 1 つのソフトウェア イメージに結合されています。適応型セキュリティ アプライアンスは、シングル モードまたはマルチモードで設定できます。

**統計プロセッサ** IPS のプロセッサ。パケット数やパケット到着レートなどのシステム統計情報を記録します。

**トポロジ** 企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

**トラフィック分析** データが暗号化されている場合、または直接使用可能でない場合にも、データ フローの観測可能な特徴から情報を推理すること。このような特徴には、発信元と宛先（複数の場合もある）の ID と場所や、事象の存在、回数、頻度、期間などがあります。

## な

**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。

**ネイバー検索** IPv6 のプロトコル。同じリンク上の IPv6 ノードは、ネイバー探索を使用して相手の存在の検出、相手のリンク層アドレスの特定、ルータの検索、アクティブ ネイバーへのパスに関する到達可能性情報の維持を行います。

**ネットワーク アクセス ID** 「NAS-ID」を参照してください。

**ネットワーク参加** グローバル相関データベースに学習した情報を提供するネットワーク。

**ネットワーク参加クライアント** SensorBase ネットワークにデータを送信する CollaborationApp のソフトウェア コンポーネント。

**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、攻撃元ホストをブロックできるデバイス。ネットワーク デバイスには、Cisco ルータや PIX Firewall などがあります。

**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、アプライアンスまたはルータ。

## は

**ハードウェア バイパス** 物理インターフェイスをペアにする特殊なインターフェイス カード。ソフトウェア エラーが検出されると、物理インターフェイスを直接接続し、トラフィックがペアを通過できるようにするバイパス メカニズムを起動します。ハードウェア バイパスは、ネットワーク インターフェイスでトラフィックを通過させますが、IPS システムへは渡しません。

**バイパス モード** センサーが失敗した場合でも、引き続きセンサーからパケットを通過させるモード。バイパス モードは、インラインペア インターフェイスにのみ適用されます。

**パケット** 情報を論理的にグループ化したもの。制御情報が格納されたヘッダーと、（通常は）ユーザ データが含まれています。パケットは、ほとんどの場合ネットワーク層のデータの単位を表します。データグラム、フレーム、メッセージ、セグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

**パッシブ OS フィンガープリント** センサーは、ネットワークで交換されるパケットの特性を検査することで、ホストのオペレーティング システムを特定します。

**パッシブ フィンガープリント** システムで使用できる OS やサービスをネットワーク対話のパッシブな観察から決定すること。

**パッチ リリース** ソフトウェア リリース（サービス パック、マイナー、またはメジャー更新）のリリース後に更新（マイナー、メジャー、またはサービス パック）バイナリで特定された不具合を解決するリリース。

**ハンドシェイク** 複数のネットワーク デバイス間で、伝送の同期を確認するために交換される一連のメッセージ。

**半二重** 送信ステーションと受信ステーション間で、一度に 1 方向にのみデータ転送できる機能。BSC は、半二重プロトコルの一例です。

**ファイアウォール** 接続されている任意のパブリック ネットワークおよびプライベート ネットワーク間でバッファとして設計された、1 つのルータまたはアクセス サーバ、または複数のルータまたはアクセス サーバ。ファイアウォール ルータは、アクセス リストや他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

**ファスト イーサネット** 各種 100 Mbps イーサネット仕様のいずれか。ファスト イーサネットは、10BASE-T イーサネット仕様の 10 倍の速度を実現し、フレーム フォーマット、MAC メカニズム、MTU などの品質を維持します。その類似性により、ファスト イーサネット ネットワーク上で既存の 10BaseT アプリケーションおよびネットワーク管理ツールを使用できます。IEEE 802.3 仕様の拡張に基づいています。

**ブートローダ** システムの電源投入時に読み込まれるソフトウェアの小セット。（ディスク、ネットワーク、外部のコンパクト フラッシュや外部の USB フラッシュ メモリから）オペレーティング システムをロードし、そのオペレーティング システムが IPS アプリケーションをロード、実行します。AIM IPS では、モジュールをネットワークから起動し、ディザスタ リカバリ、ソフトウェアのインストールなど、モジュールがソフトウェアにアクセスできないときの動作を補助します。

**フェール オープン** ハードウェア障害後にデバイスからトラフィックを通過させます。

**フェール クローズ** ハードウェア障害後にデバイスでのトラフィックをブロックします。

**フォワーディング** インターネットワーキング デバイス経由でフレームを最終宛先に送信するプロセス。

**複合攻撃** 1 つのセッションの複数のパケットにわたって影響します。FTP、Telnet などのほとんどのカンバセーション攻撃とほとんどの正規表現ベースの攻撃が含まれます。

**プラグイン可能な認証モジュール** 「PAM」を参照してください。

**フラグメンテーション** 元のパケット サイズをサポートできないネットワーク メディアを介してパケットを送信するときに、パケットを小さい単位に分割するプロセス。

**フラグメント再構成プロセッサ** IPS のプロセッサ。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行います。

**ブラックホール** ネットワークの一部分の悪条件またはシステム設定の不備により、パケットが入っても現れないインターネットワークの領域を表すルーティング用語。

**フラッディング** スイッチおよびブリッジにより使用されるトラフィック通過手法。インターフェイス上で受信されたトラフィックは、最初に情報を受信したインターフェイスを除き、そのデバイスのすべてのインターフェイスから送信されます。

**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。インターフェイスと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のインターフェイスにマッピングします。パケット分析とアラート検出を実行します。分析エンジン機能は、SensorApp プロセスによって提供されます。

**ベース バージョン** サービス パックやシグニチャ更新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する必要があるソフトウェア リリース。メジャーおよびマイナー更新はベース バージョン リリースです。

**ホスト ブロック** ARC は、特定の IP アドレスからのすべてのトラフィックをブロックします。

**ボットネット** 自立的および自動的に実行されるソフトウェア ロボット、つまりボットの集合。多くの場合、悪意のあるソフトウェアを表す場合に使用される用語ですが、配布されたコンピューティング ソフトウェアを使用するコンピュータのネットワークを指すこともあります。ボットネットという用語は、一般的な指示管理インフラストラクチャで、通常、ワーム、トロイの木馬、バック ドアを通してインストールされたソフトウェアを実行する侵害されたコンピュータ（ゾンビ コンピュータと呼ばれる）の集合を指すときに使用されます。

## ま

**マイナー アップデート** 製品ラインへの小規模な機能強化を含むマイナー バージョン。マイナー アップデートはメジャー バージョンに対する差分であり、サービス パックのベース バージョンです。

**マスター ブロッキング センサー** 1 つ以上のデバイスを制御するリモート センサーです。ブロッキング転送センサーがブロッキング要求をマスター ブロッキング センサーに送信し、マスター ブロッキング センサーがブロッキング要求を実行します。

**マルウェア** 不明なホストにインストールされている悪意のあるソフトウェアです。

**無差別デルタ** PD。シグニチャごとに設定される 0 ～ 30 の重み。無差別モードでは、全体的なリスク レーティングからこの値を差し引くことができます。

**無差別モード** ネットワーク セグメントのパケットをモニタするパッシブ インターフェイス。検知インターフェイスには IP アドレスが割り当てられず、攻撃者に見えません。

**メジャー アップデート** 製品の主要な新機能または大きなアーキテクチャ上の変更を含むベース バージョン。

**メンテナンス パーティション** IDSM2 上のブート可能ディスク パーティション。ここから、アプリケーション パーティションに IPS イメージをインストールできます。IDSM2 がメンテナンス パーティションにブートされている間、IPS 機能は使用できません。

**メンテナンス パーティション イメージ** IDSM2 上のメンテナンス パーティションにインストールされたブート可能ソフトウェア イメージ。メンテナンス パーティション イメージは、アプリケーション パーティションへのブート中にのみインストールできます。

**モニタリング インターフェイス** 「センシング インターフェイス」を参照。

## ら

**ラウンドトリップ時間** 「RTT」を参照してください。

**ラックマウント** センサーを装置ラックに搭載すること。

**リカバリ パッケージ** アプリケーションの完全なイメージとインストーラを含む IPS パッケージ ファイル。センサーで復旧に使用されます。

**リスク レーティング** RR。リスク レーティングとは、ネットワーク上の特定イベントと関連付けられたリスクを数値化した 0 ～ 100 の値です。攻撃のリスクは、攻撃の重大度、忠実度、関連性、および資産価値を表し、応答または軽減アクションではありません。このリスクは、ネットワークに対する障害が大きくなるほど高くなります。

**良性トリガー** シグニチャは正しく起動されたけれどもトラフィックのソースに悪意がない状態。

**レイヤ 2 プロセッサ** IPS のプロセッサ。レイヤ 2 関連イベントを処理します。また、不正な形式のパケットを識別し、処理パスから取り除きます。

**レピュテーション** レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。レピュテーションを使用すると、インストール ベースの IPS センサーは、既存のネットワーク インフラストラクチャと協力してコラボレーションを行うことができるようになります。レピュテーションのあるネットワーク デバイスは、ほとんどが悪意のあるネットワーク デバイスまたは感染した可能性があるネットワーク デバイスです。

**ロガー** IPS のコンポーネントの 1 つ。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、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。

**ロギング** ログ ファイル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** 独立して実行され、自身の完全な動作バージョンをネットワーク上の他のホストに伝播させて、コンピュータ リソースを破壊的に消費することができるコンピュータ プログラム。