GLOSSARY

数字

802.x LAN プロトコルを定義する一連の IEEE（Institute of Electrical and Electronics Engineers）標準。

A

aaa 認証、認可、アカウンティング（authentication, authorization, and accounting）。シスコのデバイスでアクセス コントロールを行うための推奨される第一の方法。

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。

AD 異常検出（Anomaly Detection）。通常のネットワーク トラフィックについてベースラインを作成し、このベースラインを使用してワームに感染したホストを検出するセンサーのコンポーネント。

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。インスタント メッセージやトンネリング アプリケーション（例：gotomypc）など、特定のポート上でトンネリングを行うアプリケーションに対する管理制御を行います。また、FTP トラフィックを検査し、発行されるコマンドを制御します。

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。以前の名称は、Network Access Controller（NAC）。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。

ARR 攻撃関連性評価（Attack Relevance Rating）。

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。

ASN.1 抽象構文記法 1（Abstract Syntax Notation 1）。データ表記の標準。

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。

AV アンチウイルス（Anti-Virus）。

B

BIOS Basic Input/Output System。センサーを起動し、センサー内のデバイスとシステムとの間で通信するプログラムです。

BO BackOrifice。UDP 上だけで実行された Windows のオリジナルのバック ドア型トロイの木馬。

BO2K BackOrifice 2000。TCP および UDP 上で実行される Windows のバック ドア型トロイの木馬。

Bpdu 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、コンフィギュレーション ファイルなどがあります。

CIDEE Cisco Intrusion Detection Event Exchange。Cisco IPS システムが使用する SDEE への拡張を指定します。CIDEE 標準は、Cisco IPS システムがサポートする可能性のあるすべての拡張を指定します。

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。

CSA MC Cisco Security Agent Management Center。CSA MC は、管理対象の CSA エージェントからホストのポスチャ情報を受け取ります。また、ネットワークからの検疫が必要であると決定した IP アドレスのウォッチ リストを保守します。

CSM Cisco Security Manager。シスコの自己防衛型ネットワーク ソリューションのプロビジョニング コンポーネントです。CS-Manager は Cisco Security Monitoring, Analysis and Reporting System（CS-MARS）と完全に統合されています。

CS-Manager 「CSM」を参照。

CS-MARS Cisco Security Monitoring, Analysis and Reporting System。シスコの自己防衛型ネットワーク ソリューションのモニタリング コンポーネントです。CS-MARS は CS-Manager と完全に統合されています。

CVE Common Vulnerabilities and Exposures。脆弱性の標準名およびセキュリティ上の危険性に関するその他の情報のリスト。保守は http://cve.mitre.org/ で行われます。

D

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。

DCOM 分散 COM（Distributed Component Object Model）。ネットワークを経由したソフトウェア コンポーネントの直接通信を可能にするプロトコル。マイクロソフトによって開発され、以前は Network OLE と呼ばれていました。DCOM は、HTTP などのインターネット プロトコルをはじめとする、複数ネットワークにまたがる伝送での利用を目的として設計されています。

DDoS 分散 DoS（Distributed Denial of Service）。脆弱性が生じた複数のシステムが単一の対象を攻撃した結果、対象になったシステムのユーザがサービスを拒絶されること。対象システムが受信する大量のメッセージによってシステムが強制的にシャットダウンすることにより、正当なユーザのシステムへのサービスが拒絶されます。

Deny Filters Processor 「DFP」を参照。

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

DFP Deny Filters Processor。拒否攻撃者機能を処理します。拒否された送信元 IP アドレスのリストを管理します。

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

DMZ 非武装地帯（demilitarized zone）。プライベート ネットワーク（内部）とパブリック ネットワーク（外部）との間の中立地帯にある別個のネットワーク。

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

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

DRAM ダイナミック ランダムアクセス メモリ（dynamic random-access memory）。キャパシタに情報を保存する RAM のことで、定期的にリフレッシュする必要があります。DRAM がコンテンツをリフレッシュするときは、プロセッサがアクセスできないため、遅延が発生します。ただし、DRAM は SRAM に比べて複雑ではなく、容量も大きくなっています。

DTE データ端末装置（Data Terminal Equipment）。RS-232C 接続のデバイスの役割を表します。DTE はデータを送信回線に書き込み、受信回線から読み取ります。

DTP ダイナミック トランキング プロトコル（Dynamic Trunking Protocol）。VLAN グループにおけるシスコの専用プロトコルで、2 台のデバイス間のリンク上でトランキングをネゴシエートし、さらに、使用するトランキング カプセル化のタイプ（Inter-Switch Link（ISL; スイッチ間リンク）または 802.1q）をネゴシエートします。

E

ECLB イーサチャネル ロード バランシング（Ether Channel Load Balancing）。Catalyst スイッチで、さまざまな物理パスを流れるトラフィックを分割します。

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。ブロックするには **shun** コマンドを使用します。シングルモードまたはマルチモードのいずれでも FWSM を設定できます。

G

GBIC ギガビット インターフェイス コンバータ（GigaBit Interface Converter）。多くの場合、ファイバ インターフェイスに光ケーブル接続を適応させる光ファイバ トランシーバを指します。一般に、ファイバ対応のスイッチおよび Network Interface Card（NIC; ネットワーク インターフェイス カード）は、GBIC スロットや Small Form-factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）スロットを備えています。詳細については、『*Catalyst Switch Cable, Connector, and AC Power Cord Guide*』を参照してください。

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。

GRUB Grand Unified Bootloader。

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。

IDENT RFC 1413 で規定された Ident プロトコル。特定の TCP 接続のユーザを識別するのに役立つインターネット プロトコルです。

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

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

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

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 台のセンサーのコンフィギュレーションを管理できます。

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。

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。

ISL スイッチ間リンク（Inter-Switch Link）。VLAN 情報をスイッチとルータの間を流れるトラフィックとして維持するシスコの専用プロトコル。

K

KB 知識ベース（Knowledge Base）。AD がラーニングしたしきい値セットで、ワーム ウイルスの検出に使用します。

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。

LACP リンク集約制御プロトコル（Link Aggregation Control Protocol）。LACP は、LACP パケットを LAN ポート間で交換することにより、イーサチャネル 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（Local Area Network）。特定ホストに対するレイヤ 2 ネットワーク ドメイン ローカルを指します。同じ LAN 上の 2 つのホスト間で交換されたパケットには、レイヤ 3 ルーティングは必要ありません。

Layer 2 Processor 「L2P」を参照。

Logger IPS のコンポーネントの 1 つ。

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 応答を送信するために使用する 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 や CMIP などのネットワーク管理プロトコルによって使用および保守される、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 コマンドや CMIP コマンドを使用して、通常は GUI ネットワーク管理システムを通じ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）。MSRPC はマイクロソフトによる DCE RPC メカニズムの実装です。マイクロソフトは、Unicode 文字列、暗黙の処理、インターフェイスの継承（DCOM で広く使用されています）、および可変長文字列での複雑な計算や、DCE/RPC の既存の構造パラダイムに対するサポートを追加しました。

MySDN My Self-Defending Network。セキュリティ情報レポートと、他のセキュリティ ツールおよび関連リンクがある Cisco.com サイト。

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 翌営業日（Next Business Day）。シスコとのサービス契約に従って交換のハードウェアを配送します。

ND 近隣探索（Neighbor Discovery）。IPv6 の近隣探索プロトコル。同一リンクの IPv6 ノードは近隣探索を使用して、互いの存在の検出、互いのリンク層アドレスの判別、ルータの検出、およびアクティブなネイバーへのパスに関する到達状況情報の保守を行います。

never block アドレス ブロックされることのないように指定したホストおよびネットワーク。

never shun アドレス 「never block アドレス」を参照。

NIC ネットワーク インターフェイス カード（Network Interface Card）。コンピュータ システムとの間でやり取りされるネットワーク通信機能を提供するボード。

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の比較的高性能、高機能のコンピュータが使用されます。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 NORMALIZER がどのように機能するかを設定し、IP および TCP の NORMALIZER に関連するシグニチャ イベントの設定を行います。

NOS ネットワーク OS（Network Operating System）。分散ファイル システムを指すために使用される一般的な用語。LAN Manager、NetWare、NFS、VINES などがあります。

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

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

NVRAM 不揮発性読み取り / 書き込みメモリ（Non-Volatile Read/Write Memory）。RAM は、ユニットの電源が切られた後も内容を保持します。

O

OIR 活性挿抜（online insertion and removal）。システムの電源を切ったり、コンソール コマンドを入力したり、他のソフトウェアまたはインターフェイスをシャットダウンしないで、カードの追加、交換、または取り外しを可能にする機能です。

OPS Outbreak Prevention Service。

P

PAgP ポート集約制御プロトコル（Port Aggregation Control Protocol）。PAgP は、PAgP パケットを LAN ポート間で交換することにより、イーサチャネル リンクの自動作成を支援します。シスコの専用プロトコルです。

PASV ポート スプーフィング ファイアウォールを通過し、保護された FTP サーバを経由して FTP 以外のポート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 **passive** コマンドを誤って解釈した場合に発生します。

PAT ポート アドレス変換（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。

POSFP パッシブ OS フィンガープリント（Passive OS Fingerprinting）。センサーは、ネットワークで交換された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 システムを判別します。

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。

RMA Return Materials Authorization。故障したハードウェアを返却して交換のハードウェアを入手するためのシスコのプログラム。

ROMMON Read-Only-Memory Monitor。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。攻撃のリスクでは、攻撃の重大度、忠実度、関連性、および資産価値が考慮されますが、応答や軽減のアクションは考慮されません。ネットワークが大きな損害を受けるほど、このリスクは高くなります。

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、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ことを目的に設計されています。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 サービスとして転送します。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。

RTT ラウンドトリップ時間（round-trip time）。パケットの送信から受信の確認応答までに、ネットワークによってホストで発生した時間遅延の指標。

RU ラック単位（rack unit）。ラックはラック単位で測定されます。1 RU は 44 Mm または 1.75 インチに相当します。

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 シグニチャ イベント アクション プロセッサ（Signature Event Action Processor）。イベント アクションを処理します。イベント アクションはイベント リスク評価（RR）しきい値と関連付けできます。アクションが実行されるには、このしきい値を超える必要があります。

Security Monitor Monitoring Center for Security。ネットワーク デバイスに、イベントの収集、表示、およびレポート実行の機能を提供します。IDS MC とともに使用されます。

SensorApp IPS のコンポーネントの 1 つ。パケットの取り込みと分析を実行します。SensorApp はネットワーク トラフィックを分析して悪意のあるコンテンツを探します。パケットは、プロセッサのパイプラインを通過します。このパイプラインは、設計者がセンサー上のネットワーク インターフェイスからパケットを収集するように設計します。Sensorapp は、分析エンジンを実行するスタンドアロンの実行ファイルです。

Service エンジン DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SL、NTP、RPC、SMB、SNMP、および SSH など、特定のプロトコルを処理します。

session コマンド ルータとスイッチに対して使用されるコマンドで、ルータまたはスイッチ内のモジュールに対して Telnet またはコンソールのいずれかによるアクセスを提供します。

SFP 着脱可能小型フォーム ファクタ（Small Form-factor Pluggable）。多くの場合、ファイバ インターフェイスに光ケーブル接続を適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 Firewall 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 カウントおよびパケット到着率などのシステム統計情報を追跡します。

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

SQL 構造化照会言語（Structured Query Language）。リレーショナル データベースの定義およびアクセスに使用する国際的な標準言語。

SRAM RAM の一種。電源が供給されている限り、内容を保持します。SRAM は、DRAM のように定期的なリフレッシュは必要ありません。

SRP Stream Reassembly Processor。さまざまなストリームベース インスペクタでパケットが適切な順序で到着するよう、TCP ストリームを並べ替えます。また、TCP ストリームの正規化も行います。正規化エンジンを使用すると、アラートおよび拒否アクションを有効または無効にできます。

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

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

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

State エンジン HTTP ストリングのステートフル検索。

Statistics Processor 「SP」を参照。

Stream Reassembly Processor 「SRP」を参照。

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

SYN フラッド プロトコルの実装で処理可能な数を超える多数の TCP SYN パケット（接続開始時に使用されるシーケンス番号の同期化要求）をホストに送信する DoS 攻撃。

T

TAC Cisco Technical Assistance Center。TAC は、世界中に 4 か所あります。

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。

TFN Tribe Flood Network。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 アドレスをすばやく変更して、攻撃の特定やフィルタリングを攻撃者が阻止できます。

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 アドレスをすばやく変更して、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。

TNS Transparent Network Substrate。すべての業界標準ネットワーク プロトコルに対する 1 つの共通インターフェイスをデータベース アプリケーションに提供します。TNS を使用するデータベース アプリケーションは、異なるプロトコルを使用するネットワークで他のデータベース アプリケーションに接続できます。

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、古いデータベース エントリを有効期限切れにすること、および時間に依存する統計情報を計算することです。

TPKT 転送パケット（Transport Packet）。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。このプロトコルは TCP の最上位にある ISO 転送サービスを使用します。

TR 脅威評価（Threat Rating）。TR は、監視対象ネットワークでのアラートの脅威を表す応答アクションに基づいて、攻撃に関するリスク評価の低下を、0 から 100 の間の数値で表した評価です。

traceroute パケットが宛先に到達するまでに通過するパスをトレースするプログラムのことで、多数のシステムで使用可能です。主に、ホスト間のルーティング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。

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。

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 によってマルチレイヤ スイッチングが可能になり、Cisco IOS が実行されます。VIP の最新バージョンは VIP2 です。

VLAN バーチャル LAN（Virtual Local Area Network）。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。

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

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。たとえば、TCP リセット、ホストのブロック、接続のブロック、IP ロギング、アラート トリガー パケットの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。

アスペクト バージョン IDIOM デフォルト コンフィギュレーションのグループに関連付けられたバージョン情報。たとえば、シスコシステムズでは S アスペクトを使用して、攻撃シグニチャの標準セットをデフォルト設定の集合として公開します。S アスペクトのバージョン番号は、シグニチャ アップデート パッケージ ファイル名の S の後に表示されます。その他のアスペクトとして、V アスペクトのウイルス シグニチャ定義や、キー アスペクトの IDIOM 署名キーがあります。

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 つのパケット内に組み込まれた不正利用を表します。たとえば、「ping of death」攻撃は、異常に大きな単一の ICMP パケットです。

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

アプリケーション イメージ センサーの稼動に使用される永続ストレージ デバイスに格納された完全な IPS イメージ。

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

アラート 厳密には IPS のイベント タイプの 1 つを指し、evidsAlert としてイベント ストアに書き込まれます。一般に、アラートは、ネットワークの不正利用が進行中であるか、潜在的なセキュリティの問題が発生していることを示す IPS メッセージです。アラームとも言います。

アラーム チャネル インスペクタによって生成されたすべてのシグニチャ イベントを処理する IPS ソフトウェア モジュール。主な機能は、受け取った各イベントのアラートを生成することです。

暗号化 データに特殊なアルゴリズムを適用してそのデータの外見を変更し、その情報を読む許可を与えられていないユーザには理解できないようにすること。

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

い

異常検出 「AD」を参照。

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。

インライン インターフェイス センサーがペアの一方のインターフェイスで受信したトラフィックをもう一方のインターフェイスにすべて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

仮想化センシング インターフェイス 仮想化インターフェイスは、サブインターフェイスに分割されています。個々のインターフェイスは VLAN のグループで構成されます。仮想センサーを 1 つ以上のサブインターフェイスに関連付けて、さまざまな侵入防御ポリシーをこれらのサブインターフェイスに割り当てることができます。物理インターフェイスとインライン インターフェイスのどちらも仮想化できます。

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コンフィギュレーション 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。

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。

く

クッキー Web サーバから Web ブラウザに送信される情報で、ブラウザによって保存されます。ブラウザは、Web サーバに対して追加要求を行うときに、Web サーバにこの情報を送り返します。

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ので、攻撃者には表示されません。

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。

コントロール インターフェイス ARC では、ネットワーク デバイスで 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。これがコントロール インターフェイスです。

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 不良箇所の修正をリリースするためと、新しいシグニチャ エンジンをサポートするために使用されます。

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。

再パッケージ リリース パッケージまたはインストーラの不良箇所に対応したリリース。

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、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 ワーム、DDOS、ウイルスなどの悪意のあるネットワーク アクティビティを認識するように設計された一連のルールが含まれる実行可能ファイル。シグニチャ アップデートは単独でリリースされ、必要なシグニチャ エンジン バージョンに依存し、独自のバージョン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 新しいシグニチャ アップデートをサポートするバイナリ コードが含まれる独自のバージョン体系を持つ実行可能ファイル。

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

出トラフィック 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。

信頼できる鍵 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。

信頼できる証明書 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。

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。

据え置き 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。

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。パターン照合では、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、監視対象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。

ゾーン AD が使用する内部ゾーン、無許可ゾーン、または外部ゾーンに分類される宛先 IP アドレスのセット。

ソフトウェア バイパス トラフィックを検査することなく IPS システムを通過させます。

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

知識ベース 「KB」を参照。

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。

適応型セキュリティ アプライアンス 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適応型セキュリティ アプライアンスを設定できます。

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 決められた条件に合致したり、しきい値を超えたりするような重大なイベントがエージェントに発生したことを示すメッセージ。SNMP エージェントから NMS、コンソール、あるいは端末に送られます。

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

ハードウェア バイパス 物理インターフェイスのペアを設定する特殊な NIC。ソフトウェア エラーが検出されると、バイパス メカニズムによって物理インターフェイスが直接接続されて、ペア間をトラフィックが流れるようにすることができます。ハードウェア バイパスはトラフィックをネットワーク インターフェイスに渡します。IPS システムには渡しません。

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。

パッチ リリース ソフトウェア リリース（サービス パック、マイナーまたはメジャー アップグレード）がリリースされた後に、アップデート（マイナー、メジャー、またはサービス パック）バイナリで確認された不良箇所に対応するリリース。

ハンドシェイク 複数のネットワーク デバイス間で、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。

ひ

非仮想化センシング インターフェイス 非仮想化センシング インターフェイスは、サブインターフェイスに分割されていないため、インターフェイス全体を最大 1 つの仮想センサーに関連付けることができます。

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。

フェール オープン ハードウェアに障害が発生した後、デバイスでトラフィックを通過させます。

フェール クローズ ハードウェアに障害が発生した後、デバイスでトラフィックをブロックします。

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 センサーのコンフィギュレーションを処理する 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

ベース バージョン サービス パックやシグニチャ アップデートなどの後続リリースをインストールするために、事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 バージョン アップグレード 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 アップグレードはメジャー 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 バージョン アップグレード 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

ラウンドトリップ時間 「RTT」を参照。

ラックマウント センサーを装置ラックに搭載すること。

り

リカバリ パッケージ アプリケーションの完全なイメージとインストーラを含む IPS パッケージ ファイル。センサーで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。