GLOSSARY

数字

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

802.x LAN プロトコルを定義するための IEEE 標準のセット。

A

AAA 認証、許可、アカウンティング。「トリプル エー」と発音します。シスコ デバイスのアクセス コントロールに使用する、推奨される主要な方法です。

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 Acknowledgement（確認応答）。イベントが発生したこと（たとえば、メッセージの受信）を確認ために、あるネットワーク 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。

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 Secure Access Control Server。ネットワーク ユーザ、ネットワーク管理者、およびネットワーク インフラ リソースを管理する集中コントロール ポイントである、RADIUS セキュリティ サーバ。

AIC エンジン Application Inspection and Control（アプリケーション インスペクションと制御）エンジン。Web トラフィックを詳細に分析します。これは、HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。指定したポートを使用したトンネリングを試行するアプリケーション（インスタント メッセージなど）、およびトンネリング アプリケーション（GoToMyPC など）の管理制御を実現します。また FTP トラフックを検査して、発行中のコマンドを制御することもできます。

AIM の IPS Advanced Integration Module（拡張統合モジュール）。Cisco ルータにインストールされる IPS ネットワーク モジュールのタイプ。

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。AIP SSM は、多数の埋め込み署名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 モジュールです。AIP SSM は、不正なアクティビティを検出すると、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、さらにアラートをデバイス マネージャに送信します。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。

API Application Programming Interface（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通信するための手段。標準化された API では、基盤となる通信方式に関係なくアプリケーション プログラムを開発できます。コンピュータのアプリケーション プログラムは、標準ソフトウェアの割り込み、呼び出し、およびデータ形式のセットを実行して、その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、メインフレーム通信プログラム、またはその他のプログラム間通信）。通常、ソフトウェア開発者は API を使用することで、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必要のあるリンクを簡単に作成できるようになります。

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 / ブロック解除の機能を提供するソフトウェア モジュールです。

ARP Address Resolution Protocol（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こと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。

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

ASN.1 Abstract Syntax Notation 1（抽象構文記法 1）。データ プレゼンテーションの標準です。

ATOMIC エンジン IP プロトコル パケットおよび関連付けられているレイヤ 4 トランスポート プロトコルを検査する Atomic IP と、レイヤ 2 ARP プロトコルを検査する Atomic ARP の 2 種類の ATOMIC エンジンがあります。

attack 知的脅威から発生するシステム セキュリティへの攻撃。セキュリティ サービスを回避してシステムのセキュリティ ポリシーを妨害するために、（特に方法や技術に関して）用意周到に計画したうえで試みられた知的行為を意味します。

AuthenticationApp IPS のコンポーネントの 1 つ。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 Anti-Virus（アンチウイルス）。

B

BIOS Basic Input/Output System。センサーを起動し、センサー内のデバイスとシステムとの間の通信を行うプログラムです。

block 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。

BO BackOrifice。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。

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。

bootloader 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、または外部の USB フラッシュから）オペレーティング システムをロードし、それからオペレーティング システムが IPS アプリケーションをロードして実行します。AIM-IPS の場合、モジュールをネットワークから起動し、ソフトウェアのインストールおよびアップグレード、ディザスタ リカバリなど、モジュールがソフトウェアにアクセスできないときの動作を補助します。

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 Cisco Express Forwarding（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インタラクティブな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拡張性が最適化されます。

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

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

CIDEE Cisco Intrusion Detection Event Exchange。Cisco IPS システムが使用する SDEE への拡張を指定します。CIDEE 規格は、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、拡張性、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ール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 Command-Line Interface（コマンドライン インターフェイス）。センサーに付属のシェルで、センサー アプリケーションの設定と制御に使用されます。

CollaborationApp IPS のコンポーネントの 1 つ。グローバル相関データベースを介して他のデバイスと情報を共用し、すべてのデバイスを組み合わせた効率を向上します。

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。

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、ネットワークから隔離する必要があると判別した IP アドレスのウォッチ リストを維持します。

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

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問題点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 IPS のプロセッサ。シグニチャ状態とフロー データベースを保持します。

DCE Data Circuit-terminating Equipment（データ回線終端装置）（ITU-T の拡張）。ユーザネットワーク インターフェイスのネットワーク端を構成する通信ネットワークのデバイスと接続部。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、モデムとインターフェイス カードがあります。

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

DDoS Distributed Denial of Service（分散型サービス拒否攻撃）。攻撃を受けた多数のシステムが単一のターゲットを攻撃した結果、ターゲットになったシステムのユーザがサービスを拒否されること。ターゲット 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否されます。

Deny Filters Processor IPS のプロセッサ。攻撃者拒否機能を処理します。拒否された送信元 IP アドレスのリストを維持します。

DES Data Encryption Standard（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 Demilitarized Zone（非武装地帯）。ニュートラル ゾーンにある別のネットワークで、プライベート（内部）ネットワークとパブリック（外部）ネットワークの間にあります。

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

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

DRAM Dynamic Random-Access Memory（ダイナミック ランダムアクセス メモリ）。キャパシタに情報を保存する RAM のことで、定期的にリフレッシュする必要があります。DRAM がコンテンツをリフレッシュするときは、プロセッサに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 Data Terminal Equipment（データ端末機器）。RS-232C 接続のデバイスの役割を指します。DTE は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 Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）。VLAN グループにおけるシスコ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（ISL または 802.1q）をネゴシエートします。

E

ECLB Ether Channel Load Balancing（EtherChannel ロード バランシング）。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。

encryption 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。

engine 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。

ESD Electrostatic Discharge（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

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。

FQDN Fully Qualified Domain Name（完全修飾ドメイン名）。DNS ツリー階層内で、正確な位置を指定するドメイン名です。ルート ドメインに関連するすべてのドメイン レベル（トップレベルのドメインも含む）を指定します。完全修飾ドメイン名は、この絶対性により名前空間で区別されています。

Fragment Reassembly Processor 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処理します。

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

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

FWSM Firewall Security Module。Catalyst 6500 シリーズ スイッチにインストールできるモジュールです。ブロックするには **shun** コマンドを使用します。FWSM は、シングルモードまたはマルチモードのいずれでも設定できます。

G

GBIC Gigabit Interface Converter（ギガビット インターフェイス コンバータ）。多くの場合、ファイバ インターフェイスへの光ケーブル接続を適合させるファイバ光トランシーバを指します。一般に、ファイバ対応のスイッチおよび NIC は、GBIC スロットまたは SFP スロット（またはその両方）を備えています。詳細については、『*Catalyst Switch Cable, Connector, and AC Power Cord Guide*』を参照してください。

Gigabit Ethernet 1996 年に IEEE（Institute of Electrical and Electronics Engineers）802.3z 規格委員会によって承認された、高速イーサネットの規格。

GMT Greenwich Mean Time（グリニッジ標準時）。経度ゼロの時間帯。現在では、協定世界時（UTC）と呼ばれています。

GRUB Grand Unified Bootloader。ブート ローダは、コンピュータが起動したときに、最初に実行されるプログラムです。オペレーティング システムのカーネル ソフトウェアをロードし、コントロールをカーネル ソフトウェアに転送します。これに対し、カーネルではオペレーティング システムの残りの部分を初期化します。

H

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

H.245 H.245 エンドポイントの制御を規定する ITU 標準。

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

HTTP Hypertext Transfer Protocol（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および応答メディア転送プロトコルです。

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

I

ICMP Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。ネットワーク層のインターネット プロトコルであり、エラーを報告し、IP パケット処理に関するその他の情報を提供します。RFC 792 に記載されています。

ICMP フラッド プロトコルの実装で処理可能な数を超える多数の ICMP エコー要求（「ping」）パケットをホストに送信する DoS 攻撃。

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

IDCONF Intrusion Detection Configuration。侵入検知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 Web ブラウザでアクセスできます。

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

IDS MC Management Center for IDS Sensors。Web ベースの IDS マネージャで、最大 300 台のセンサーの設定を管理できます。

IDSM2 Intrusion Detection System Module。Catalyst 6500 シリーズ スイッチで侵入検知を実行するスイッチング モジュールです。

IME IPS Manager Express。最大 10 個のセンサーのシステム ヘルス モニタリング、イベント モニタリング、レポート、および設定を提供す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。物理設定とは、速度、デュプレックス、および管理状態です。

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

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

iplog 指定されたアドレスとの間でやり取りされるバイナリ パケットのログ。iplog は、シグニチャに log Event Action が選択されている場合に作成されます。iplog は、WireShark または TCPDUMP で読み取り可能な libpcap 形式で格納されます。

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

IPS SSP Intrusion Prevention System Security Services Processor。Cisco ASA 5585-X 適応型セキュリティ アプライアンスの IPS プラグイン モジュール。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。IPS SSP は、不正なアクティビティを検出すると、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、さらにアラートをデバイス マネージャに送信します。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。

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です。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。

ISL Inter-Switch Link（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導入テクノロジーです。Java Web Start を使用すると、開発者は、標準の Web サーバでアプリケーションを利用できるようにすることで、フル機能のアプリケーションをユーザに展開できます。どの Web ブラウザを使用しても、アプリケーションを起動することができ、いつでも確実に最新バージョンを使用できます。

JNLP Java Network Launching Protocol。XML ファイル形式で定義し、Java Web Start アプリケーションの起動方法を指定します。JNLP は、どの程度厳密に起動メカニズムを実装するかを定義するルール セットで構成されます。

K

KB Knowledge Base（ナレッジ ベース）。異常検出により学習されたしきい値のセットで、ワーム ウイルスの検出に使用されます。

L

LACP Link Aggregation Control Protocol（リンク アグリゲーション制御プロトコル）。LACP では、LAN ポート間で LACP パケットを交換することによる、EtherChannel リンクの自動作成を助けます。このプロトコルは IEEE 802.3ad で定義されています。

LAN Local Area Network（ローカルエリア ネットワーク）。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 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、不正なパケットを識別し、処理パスから削除します。

Logger 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。

Logging 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グ収集は、イベント（IPS のコマンド、エラー、およびアラート）のロギングと、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。

LOKI リモート アクセスのバック ドア型トロイの木馬で、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り、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。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したものです。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、通信の整合性を検証し、発信元を認証し、適時性をチェックします。

Meta エンジン 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 Management Information Base（管理情報ベース）。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維持されるネットワーク管理情報のデータベース。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

MIME Multipurpose Internet Mail Extension（多目的インターネット メール拡張）。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。

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

MSRPC Microsoft Remote Procedure Call。MSRPC は、マイクロソフトによる DCE RPC メカニズムの実装です。マイクロソフトは、Unicode ストリング、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）、可変長ストリングでの複雑な計算、および DCE/RPC の既存の構造パラダイムに対するサポートを追加しました。

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

N

NAC Network Access Controller。「ARC」を参照。

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 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が到着します。

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

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

NIC Network Interface Card（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。

NME IPS Network Module Enhanced。Cisco 2800 および 3800 シリーズ サービス統合型ルータの任意のネットワーク モジュール スロットにインストールできる IPS モジュール。

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、ネットワークの統計やリソースを追跡し続けるのに役立ちます。

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

NotificationApp IPS のコンポーネントの 1 つ。アラート イベントが、ステータス イベントが、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健全性に関する情報を提供します。

NTP Network Timing Protocol（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無線時計および原子時計を参照することにより、正確な現地時間を維持するプロトコル。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

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

NVRAM Non-Volatile Read/Write Memory（不揮発性読み取り / 書き込みメモリ）。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 Online Insertion and Removal（活性挿抜）。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。

OPS Outbreak Prevention Service。

P

PAgP Port Aggregation Control Protocol（ポート集約制御プロトコル）。PAgP では、LAN ポート間で PAgP パケットを交換することによる、EtherChannel リンクの自動作成を助けます。シスコ独自のプロトコルです。

PASV Port Spoof ファイアウォールを通過して、保護された FTP サーバを経由して非 FTP ポートへの接続を開く試み。これは、不正な接続を開くことにより、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起こります。

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

PAWS Protection Against Wrapped Sequence。高性能 TCP ネットワークでのラップされたシーケンス番号に対する保護。RFC 1323 を参照してください。

PCI Peripheral Component Interface。Intel ベースのコンピュータで、最も一般的に使用されているペリフェラル拡張バス。

PDU Protocol Data Unit（プロトコル データ ユニット）。パケットの OSI 用語。「BPDU」および「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 Packed Encoding Rules。PER は、同じ方法ですべてのタイプを符号化する一般的なスタイルの符号化のではなく、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処理をサポートします。

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。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。ICMP エコー要求パケットをターゲット ホストに送信して、エコー応答をリッスンすることで機能します。

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

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

Point-to-Point（P2P; ポイントツーポイント） Peer-to-Peer（ピアツーピア）。P2P ネットワークは、ファイル共有のためにクライアントとサーバの両方として同時に機能できるノードを使用します。

POST Power-On Self Test（電源投入時自己診断テスト）。デバイスに電源が投入されたときに、ハードウェア デバイスで実行されるハードウェア診断のセット。

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

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

Q

Q.931 ISDN ネットワーク接続の確立、保持、および終了のシグナリングを行う ITU-T の仕様。

QoS Quality of Service。伝送システムのパフォーマンスを基に、その伝送品質とサービスのアベイラビリティを表します。

R

RAM Random-Access Memory（ランダムアクセス メモリ）。マイクロプロセッサによる読み取りと書き込みが可能な揮発性メモリ。

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 Router Blade Control Protocol。RBCP は、SCP をベースにしていますが、ルータ アプリケーション用に特別に変更されています。イーサネット インターフェイス上で動作するように設計されており、メッセージには 802.2 SNAP カプセル化を使用します。

Regex 「正規表現」を参照。

RMA Return Materials Authorization（返品許可）。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 ROM モニタ（Read-Only-Memory Monitor）。ROMMON は、リカバリのための TFTP システム イメージをセンサーに転送できます。

RPC Remote-Procedure Call（リモート プロシージャ コール）。クライアント / サーバ コンピューティングの技術的基盤。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 Round-Trip Time（ラウンドトリップ時間）。パケットの送信から受信の確認応答までに、ネットワークによってホストで発生した時間遅延の単位。

RU Rack Unit（ラック ユニット）。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

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

SCP Switch Configuration Protocol。イーサネット上で直接動作するシスコの制御プロトコル。

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。各種セキュリティ 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 Server リモート クライアントからイベントの要求を受け付けます。

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、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ことを目的としたプロデューサが提供する、プロセッサのパイプラインを経由して流れます。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。

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（着脱可能小型フォーム ファクタ）。多くの場合、ファイバ インターフェイスへの光ケーブル接続を適合させるファイバ光トランシーバを指します。詳細については、GBIC を参照してください。

shun コマンド 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。PIX Firewall を使用してブロックする場合に、ARC により使用されます。

SMB Server Message Block（サーバ メッセージ ブロック）。データをパッケージ化し、他のシステムと情報を交換するために LAN マネージャおよび同様の NOS が使用するファイル システム プロトコル。

SMTP Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。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 の一部です。SN は、ご使用のシスコ製品のシリアル番号です。

SNAP Subnetwork Access Protocol（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 Simple Network Management Protocol（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 バージョン 2。ネットワーク管理プロトコルのバージョン 2。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 Switched Port Analyzer（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 Structured Query Language（構造化照会言語）。リレーショナル データベースの定義およびアクセスに使用する国際的な標準言語。

SRAM RAM のタイプ。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。

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

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

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

State エンジン HTTP ストリングのステートフル検索。

Statistics Processor IPS のプロセッサ。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。

Stream Reassembly Processor 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。TCP ストリームの正規化も処理します。ノーマライザ エンジンを使用すると、アラートおよび拒否アクションをイネーブル化またはディセーブル化できます。

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 シスコの Technical Assistance Center。TAC は、世界で 4 拠点あります。

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

TCP リセット インターフェイス TCP リセットを送信できる、IDSM-2 上のインターフェイス。ほとんどのセンサーでは、パケットがモニタされるセンシング インターフェイスと同じインターフェイスで TCP リセットが送信されますが、IDSM-2 では、センシング インターフェイスを TCP リセットの送信に使用することができません。IDSM-2 の場合、TCP リセット インターフェイスは、Catalyst ソフトウェアでポート 1 として指定され、Cisco IOS ソフトウェアのユーザには表示されません。TCP リセット アクションは、TCP ベースのサービスに関連するシグニチャ上のアクションとして選択したときだけ有効なアクションとなります。

TCPDUMP TCPDUMP ユーティリティは、フリーの UNIX および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。さまざまなオプションを使用して、各パケットの要約情報と詳細情報を表示できます。詳細については、http://www.tcpdump.org/ を参照してください。

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

TFN Tribe Flood Network。攻撃者が、偽装されたかすぐに変更される送信元 IP アドレスを活用して、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、一般的なタイプの DoS 攻撃。

TFN2K Tribe Flood Network 2000。攻撃者が、偽装されたかすぐに変更される送信元 IP アドレスを活用して、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、一般的なタイプの 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。

Time Processor 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。

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

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

TPKT Transport Packet（トランスポート パケット）。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 の上位にある ISO トランスポート サービスを使用します。

traceroute パケットが宛先に到達するまでに通過するパスをトレースするプログラムのことで、多数のシステムで使用可能です。主に、ホスト間のルーティング問題をデバッグする際に使用されます。traceroute プロトコルは、RFC 1393 でも定義されています。

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

Trojan エンジン BO2K および TFN2K などの非標準プロトコルを分析します。

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。

UDLD UniDirectional Link Detection（単方向リンク検出）。LAN ポートに接続された光ファイバまたは銅製イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単方向リンクの存在を検出することができるようにするシスコ独自のプロトコル。単方向リンクはスパニング ツリー トポロジ ループなどのさまざまな問題の原因となるため、単方向リンクが検出されたら、UDLD により影響を受ける LAN ポートがシャット ダウンされ、アラートが送信されます。

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

UPS Uninterruptable Power Source（無停電電源）。

UTC Coordinated Universal Time（協定世界時）。経度ゼロの時間帯。以前は、グリニッジ標準時（GMT）およびズールー時と呼ばれていました。

UTF-8 8-bit Unicode Transformation Format。Unicode 用の可変長文字エンコーディング。UTF-8 では、Unicode 文字セットのすべての文字を表現でき、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 Version Identifier（バージョン ID）。UDI の一部です。

VIP Versatile Interface Processor。Cisco 7000 および Cisco 7500 シリーズ ルータで使用されるインターフェイス カード。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）。仮想 LAN は、管理ソフトウェアを使用して設定された 1 つ以上の LAN 上のデバイスのグループで、これらのデバイスは、実際には異なる複数の LAN セグメントに配置されていたとしても、同じケーブルに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づくため、きわめて柔軟です。

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

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

VPN Virtual Private Network（バーチャル プライベート ネットワーク）。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 Trunking Protocol（VLAN トランキング プロトコル）。ネットワーク全体での VLAN の追加、削除、および名前変更を管理するシスコのレイヤ 2 メッセージ プロトコル。

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

W

WAN Wide-Area Network（ワイドエリア ネットワーク）。広大な地理的地域のユーザにサービスを提供し、通常は、コモン キャリアが提供する伝送デバイスを使用するデータ通信ネットワーク。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 TCP ベースのクエリー / 応答プロトコルで、公式データベースをクエリーしてドメイン名または IP アドレスの所有者を判別します。

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

X

X.509 証明書に含まれる情報を定義する規格。

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。

XPI Cross Packet Inspection。TCP の使用するテクノロジーで、パケット全体を検索し、パケットとペイロードの再構成を可能にします。

あ

アーキテクチャ コンピュータまたは通信システムの全体的な構造。アーキテクチャは、システムの機能および制限事項に影響します。

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 デフォルト設定のグループに関連付けられたバージョン情報。たとえば、シスコでは 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まりとして発行しています。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 アスペクト内のウイルス シグニチャ定義、キー アスペクト内の 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 つのパケット内に含まれる不正利用を表します。たとえば、「ping of death」攻撃は異常に大きい 1 つの 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 センサーの動作に使用される永続的ストレージ デバイスに保存される完全な 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 イメージが含まれるブート ディスクまたはコンパクトフラッシュ パーティション。

アラート 厳密には IPS のイベント タイプの 1 つを指し、evidsAlert としてイベント ストアに書き込まれます。一般に、アラートは、ネットワークの不正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。

アラーム チャネル インスペクタにより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して、アラートを生成することです。

暗号キー 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キーが使用される場合を対称と言います。暗号キーが暗号化と復号化のいずれかに使用される（両方ではない）場合を非対称と言います。

い

異常検出 AD。通常のネットワーク トラフィックのベースラインを作成してから、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 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。

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がセンサーを通過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。

ウォッチ リスト評価 WLR。CSA MC ウォッチ リストに関連付けられた、範囲 0 ～ 100 の重み値（CSA MC は範囲 0 ～ 35 だけを使用）。

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。非公開で所有され、保守される点で 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。

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 つの仮想センサーを 1 つ以上のサブインターフェイスに関連付け、さまざまな侵入防御ポリシーをそ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 インターフェイスはどちらも仮想化できます。

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着信すると、スイッチはパケットの最初の数バイトのみを読み込んで宛先アドレスを判別し、ただちにそのパケットを転送します。この技術により、パフォーマンスが向上します。

き

脅威レーティング TR。脅威レーティングは、モニタ対象ネットワークでのアラートの脅威を表す応答アクションに基づいて、攻撃に関するリスク レーティングの低下を、0 ～ 100 の数値で表した評価です。

共有秘密情報 安全な通信に参加する人のみに通知されるデータ。共有秘密は、パスワード、パスフレーズ、大きい値、またはランダムに選択したバイトの配列などです。

く

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

グローバル相関 IPS センサーは、グローバル相関データベースを通じてその他のデバイスと情報を共有し、すべてのデバイスの共同有効性を向上します。

グローバル相関クライアント CollaborationApp のソフトウェア コンポーネントで、ローカルのグローバル相関データベースのアップデートを取得してインストールします。

グローバル相関データベース IP センサーなどのコラボレーション デバイスから取得し、それらのデバイスと共有する包括的な情報。

こ

攻撃関連性レーティング ARR。ターゲット OS の関連性に関連する重み値。攻撃関連性レーティングは、アラート時点に決定される派生値です（relevant、unknown、または not relevant）。関連する OS は、シグニチャごとに設定されます。

攻撃の重大度レーティング ASR。脆弱性の不正利用が成功した場合の重大度に関連する重み値。攻撃の重大度レーティングは、シグニチャの Alert Severity パラメータ（informational、low、medium、または high）から得られます。攻撃の重大度レーティングは、シグニチャごとに設定され、検出されたイベントの危険性を示します。

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。

混合デルタ PD。シグニチャごとに設定されている範囲 0 ～ 30 の重み値。この重み値は、無差別モードでの全体的なリスク レーティングから除外されます。

混合モード ネットワーク セグメントのパケットをモニタリングするパッシブ インターフェイス。センシング インターフェイスには IP アドレスが割り当てられていないため、攻撃者からは見えません。

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

コンソール ポート センサーでコンソール デバイスへの接続に使用される、RJ45 シリアル ポートまたは DB9 シリアル ポート。

コンポジット アタック 単一セッションで複数のパケットにまたがる攻撃です。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 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に対応します。

サービス パック 障害のフィックス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。サービス パックには、最新のベース バージョン（メジャーまたはマイナー）からの障害のフィックスすべてと、新しい障害のフィックスが含まれています。

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具合に対処するリリース。

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。

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引き出して、一般的な侵入アクティビティを示す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ルール セット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 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、設定したリスク 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ており、アクション タイプごとに個別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、実行中のアクションであり、イベント ストアに evIdsAlert が書き込まれる場合があります。

シグニチャ イベント アクション フィルタ シグニチャ イベントのシグニチャ ID、アドレス、およびリスク レーティングに基づいてアクションを除外します。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る可能性のあるアクションを持つシグニチャ イベントです。

シグニチャ イベント アクション プロセッサ イベント アクションを処理します。イベント アクションは、イベント リスク レーティングしきい値と関連付けることができます。このしきい値を上回ることが、アクションを実行する前提になります。

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

シグニチャ エンジン アップデート 新しいシグニチャ アップデートをサポートするバイナリ コードが含まれる独自のバージョン体系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、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。シグニチャの忠実度レーティングは、シグニチャごとに設定され、シグニチャでイベントまたはシグニチャが記述している状態を検出する精度を示します。

シグニチャ分析プロセッサ IPS のプロセッサ。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。

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フル イメージ。

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

出力 ネットワークを出るトラフィック。

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 イベントのモニタ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。

信頼できる証明書 検証テストを行わずにユーザが信頼する証明書。特に公開キー証明書は、認証パスの最初の公開キーを提供するために使用されます。

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。

スニファ インターフェイス 「センシング インターフェイス」を参照。

スパニング ツリー ネットワーク トポロジのループフリーのサブセット。

スリーウェイ ハンドシェイク 接続を確立する間に、2 つのプロトコル エンティティが同期するプロセス。

スレーブ ディスパッチ プロセス IPS のプロセッサ。デュアル CPU システムで見つかる処理。

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 センサーとの間、または同一の IPS センサーに存在するアプリケーション間で送信されます。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 つ以上の属性。

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。

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（セキュリティ コンテキストと呼ばれる）に分割できます。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 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 セグメントをモニタする、センサー上のインターフェイス。センシング インターフェイスは、混合モードです。つまり、IP アドレスを持たず、モニタしたセグメント上では見えません。

全二重 送信側ステーションと受信側ステーションとの間で、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 異常検出によって使用される内部ゾーン、不正ゾーン、または外部ゾーンに分類される宛先 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

ダークネット ユーザが、信頼する相手とのみ接続するバーチャル プライベート ネットワーク。最も一般的な意味としては、ダークネットは通信を行う複数のユーザで構成された、あらゆるタイプの公開されていないプライベート グループを指しますが、この名前は特にファイル共有ネットワークを指す場合に最もよく使用されます。ダークネットは、あらゆる秘密通信ネットワークの総称としても使用されます。

ターゲットの価値レーティング TVR。ターゲットの知覚価値に関連する重み値。ターゲットの価値レーティングは、ネットワーク資産（IP アドレスによる）の重要度を示す、ユーザ設定可能な値です（0、low、medium、high、または mission critical）。

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。

単方向リンク検出 「UDLD」を参照。

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 事前に仮想回線を確立することなく、伝送メディア上のネットワーク層単位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、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。

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。

転送 インターネットワーキング デバイスを介して、最終の宛先に向けてフレームを送信する処理。

と

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

トラップ SNMP エージェントから NMS、コンソール、または端末に送られ、具体的に定義された条件や、しきい値に達したなどの、重要なイベントが発生したことを伝えるメッセージ。

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

トランク ネットワーク トラフィックが通過する 2 つのスイッチ間の物理的および論理的接続。バックボーンは、複数のトランクによって構成されています。

な

ナレッジ ベース 「KB」を参照。

に

認証 ユーザがシステムを使用する権限を持っていることを確認する処理。通常はパスワード キーまたは証明書によって行われます。

ね

ネイバー探索 IPv6 のプロトコル。同一リンクの IPv6 ノードはネイバー探索を使用して、互いの存在の検出、互いのリンク層アドレスの判別、ルータの検出、およびアクティブなネイバーへのパスに関する到着可能性情報の保守を行います。

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デバイス。ネットワーク デバイスには、Cisco ルータや PIX Firewall などがあります。

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

ネットワーク参加クライアント 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。

の

ノード コマンド / コントロール ネットワーク上の物理的な通信要素。たとえば、アプライアンス、IDSM-2、またはルータを指します。

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

は

ハードウェア バイパス 物理インターフェイスのペアを設定する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、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わ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 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。

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 バスおよび電力分散バスとの間の物理的な接続。

パッシブ OS フィンガープリント センサーは、ネットワーク上で交換されるパケットの特性を検査してホスト オペレーティング システムを判別します。

パッシブ フィンガープリント ネットワークのインタラクションを受動的に観察することにより、システムで使用可能な OS またはサービスを判別する動作。

パッチ リリース ソフトウェア リリース（サービス パック、マイナーまたはメジャー アップデート）がリリースされた後に、アップデート（マイナー、メジャー、またはサービス パック）バイナリで確認された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 送信側ステーションと受信側ステーションとの間で、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おらず、インターフェイス全体を最大で 1 個の仮想センサーに関連付けることができます。

ふ

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指定された、1 つのルータまたはアクセス サーバ、または複数のルータまたはアクセス サーバ。ファイアウォール ルータは、アクセス リストや他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

ファスト イーサネット 各種 100 Mbps イーサネット仕様のいずれか。ファスト イーサネットは、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ながら、10BaseT イーサネット仕様の 10 倍の速度を実現します。このように 10BaseT と類似しているため、既存の 10BaseT アプリケーションおよびネットワーク管理ツールをファスト 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。

ファスト フラックス ファスト フラックスは、ボットネットによって使用される DNS 技術の 1 つであり、フィッシングおよびマルウェア配信サイトを、プロキシとして動作する、絶えず変化する攻撃を受けたホストのネットワークの背後に隠します。この用語は、マルウェア ネットワークを見つかりにくくし、対抗策への耐性を高めるために使用される、ピアツーピア ネットワーキング、分散コマンドおよびコントロール、Web ベースのロード バランシング、およびプロキシ リダイレクションの組み合わせも指します。Storm Worm は、この技術を使用した最近のマルウェアの亜種の 1 つです。

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サポート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たもの。

ブラックホール ネットワークのある部分の状態またはシステム設定が不良であるために、パケットは着信するが送信されない状態となっているインターネットワークの領域を指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に向けて送出されます。

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。インターフェイスのマッピングに加えて、この設定済みインターフェイスへのシグニチャおよびアラーム チャネル ポリシーのマッピングも行います。また、パケット分析とアラート検出を実行します。分析エンジンの機能は、SensorApp プロセスにより提供されています。

へ

ベース バージョン サービス パックまたはシグニチャ アップデートなどのフォローアップ リリースをインストールする前にインストールしておく必要のあるソフトウェア リリース。メジャーおよびマイナー アップデートは、ベース バージョン リリースです。

ほ

ホスト ブロック ARC 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 自律的、自動的に実行されるソフトウェア ロボット（ボット）の集まり。この用語は悪意のあるソフトウェアに関連している場合が多いですが、分散コンピューティング ソフトウェアを使用するコンピュータのネットワークも指します。ボットネットという用語は、一般的な指示管理インフラ環境で、通常はワーム、トロイの木馬、またはバックドアによりインストールされたソフトウェアを実行する、攻撃を受けたコンピュータ（ゾンビ コンピュータと呼ばれる）を指す場合に使用されます。

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 システムのフル イメージ。

マルウェア 不明なホストにインストールされている悪意のあるソフトウェア。

め

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

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

メンテナンス パーティション イメージ IDSM2 のメンテナンス パーティションにインストールされるブート可能なソフトウェア イメージ。ユーザがメンテナンス パーティション イメージをインストールできるのは、アプリケーション パーティションにブートされている間だけです。

も

モジュール スイッチ、ルータ、またはセキュリティ アプライアンス シャーシの取り外しできるカード。AIM IPS、AIP SSM、IDSM2、および NME IPS は、IPS モジュールです。

モニタリング インターフェイス 「センシング インターフェイス」を参照。

ら

ラウンドトリップ時間 「RTT」を参照。

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フル イメージとインストーラを含む IPS パッケージ ファイル。センサーでのリカバリに使用されます。

リスク レーティング RR。リスク レーティングは、ネットワーク上の特定のイベントに関連付けられたリスクを、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。ネットワークが受けた損害が大きいほど、このリスクは高くなります。

良性トリガー シグニチャは正しく起動されているが、トラフィックの送信元には悪意がない状態。

れ

レピュテーション

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。既存のネットワーク インフラを使用してコラボレーションを行うには、現場に設置されている IPS センサーのベースをイネーブルにします。レピュテーションが付いているネットワーク デバイスは、ほとんどの場合、悪意があるか感染しています。

わ

ワーム

単独で実行可能なコンピュータ プログラムで、単体で動作するバージョンのプログラム自体を、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。