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。

A

aaa 認証、許可、アカウンティング。Cisco IOS ソフトウェアと PIX Firewall のコマンドで、ユーザがルータまたは PIX Firewall にログインする方法を制御します。

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。

ACE アクセス制御エントリ（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。

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。

AuthenticationApp IPS のコンポーネントの 1 つ。ユーザが、CLI、IDM、または RDEP のアクションを実行するための適切な権限を持っていることを確認します。

B

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

C

CA 認証局。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存在です。センサーは、自己署名証明書を使用します。

CA 証明書 別の CA によって発行された、CA の証明書。

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

CIDMEF Cisco Intrusion Detection System Message Exchange Format。IDS アーキテクチャ データ用の公開メッセージ交換形式です。CIDMEF の仕様は、XML/1.0 スキーマ ドキュメントです。

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。

CTR Cisco Threat Response。「Threat Response」を参照。

D

Database Processor 「DBP」を参照。

DBP 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。

Deny Filters Processor 「DFP」を参照。

DES データ暗号化規格（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。拒否された発信元 IP アドレスのリストを管理します。

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。

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。

E

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

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

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

F

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

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

fileXferd 従来使用されていた専用ファイル転送メカニズム。

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 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。単一モードまたはマルチモードのいずれでも FWSM を設定できます。

G

GMT グリニッジ標準時（Greenwich Mean Time）。経度 0 の時間帯。現在では、Coordinated Universal Time（UTC; 世界標準時）と呼ばれます。

H

HTTP 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 に記載されています。

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。

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

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

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

IPS 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。

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。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やサブネットワーク情報を抽出するために使用されます。

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

L

L2P Layer 2 Processor。レイヤ 2 関連イベントを処理します。また、異常形式のパケットを識別し、処理パスから削除します。

Layer 2 Processor 「L2P」を参照。

Logger IPS のコンポーネントの 1 つ。

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。

managed ネットワーク デバイス（ルータおよびパケット フィルタ）を管理および監視するレガシー サービス。

MBS 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。

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。

N

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。

Network Access Controller 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。

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。

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。

NSDB ネットワーク セキュリティ データベース（Network Security Database）。IPS が使用するシグニチャと、そのシグニチャの根拠となっている脆弱性を説明したセキュリティ情報のデータベースです。NSDB には、センサーで検出可能な各攻撃シグニチャの説明が含まれます。

NTP 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。

P

packetd 侵入検知を提供していたレガシー サービス。packetd は、センサー自体がネットワークから直接パケットを取り込む場合に使用されていました。

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。

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。

PIX Firewall 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。

Post-ACL NAC 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 NAC 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。

R

RDEP Remote Data Exchange Protocol。コマンド / コントロール ネットワーク上で HTTP と TLS を使用してリモート データ交換を行うための公開仕様です。

regex 「正規表現」を参照。

ROMMON ROM モニタ（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。

RR リスク格付け。

RSM Router Switch Module。Catalyst 5000 スイッチにインストールされているモジュール上のルータ。スタンドアロン ルータとまったく同様に機能します。

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。

SDP Slave Displatch Processor。

SEAP Signature Event Action Processor。イベント アクションを処理します。イベント アクションはイベント リスク格付け（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、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。

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

shun コマンド 新しい接続を防止し、既存の全接続からのパケットを許可しないことにより、攻撃中のホストへの動的な対応を可能にします。PIX によるブロッキング時に NAC によって使用されます。

Signature Analysis Processor 「SAP」を参照。

Signature Event Action Processor 「SEAP」を参照。

Slave Displatch Processor 「SDP」を参照。

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。

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 セキュア シェル（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 セキュア ソケット レイヤ（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。

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

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、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（Transmission Control Protocol）。コネクション型のトランスポート層プロトコルで、信頼性の高い全二重のデータ伝送を提供します。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 正規化エンジン TCP ストリームの正規化を処理します。正規化エンジンを使用すると、アラートおよび拒否アクションを有効または無効にできます。

TCP 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。

TFTP トリビアル ファイル転送プロトコル（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。

Threat Response 効率的な侵入保護ソリューションを提供するために Cisco センサーとともに動作します。Threat Response は実質的に、誤ったアラームを削除して本当の攻撃への対処を優先させ、損失の大きい侵入からの修復を支援します。

Time Processor 「TP」を参照。

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

TP Time Processor。タイムスライス カレンダに格納されたイベントを処理します。主なタスクは、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。

U

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のトランスポート層プロトコル。UDP は、確認応答や送達保証を伴わずに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。

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）およびズール一時（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）をフィルタする ACL。セキュリティ ACL とも言います。

VLAN バーチャル LAN（Virtual Local Area Network）。LAN を複数の異なるブロードキャスト ドメインに論理的に分割したものです。

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止システムを構成、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。

W

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、フィルタ処理されない場合にだけ発生します。可能なアクションには、TCP リセット、ホストのブロック、接続のブロック、IP ログ収集、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 NAC 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 イメージ センサーのアプリケーション パーティションのイメージを再作成するために使用される IPS の完全なイメージ。

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、渡され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

イベント　アラート、ブロック要求、ステータス メッセージ、またはエラー メッセージを含む IPS メッセージ。

イベント サーバ　IPS のコンポーネントの 1 つ。

イベント ストア　IPS のコンポーネントの 1 つ。IPS イベントの格納に使用される、固定サイズのインデックス付きストア。

インターフェイス グループ　センシング インターフェイスの論理的なグループ。1 つの論理インターフェイス グループに複数のセンシング インターフェイスを割り当てることができます。シグニチャのパラメータは、論理インターフェイス グループごとに調整されます。

インライン モード　ネットワークに入るかネットワークから出て行く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

ウィルス アップデート　特にウィルスに対処するシグニチャ アップデート。

え

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

エンタープライズ ネットワーク　企業などの組織内で大部分の主要ポイントを接続する、大規模で多様なネットワーク。プライベートに所有および管理されるという点で、WAN とは異なります。

か

仮想センサー　シグニチャ エンジンのセンシング インターフェイスと設定ポリシー、およびシグニチャ エンジンに適用するアラーム フィルタの論理グループ。つまり、それぞれが異なるシグニチャの動作とトラフィック供給で設定された、同一アプライアンス上で動作する複数の仮想センサーです。IPS 5.x では、1 つの仮想センサーだけがサポートされます。

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。

コマンドおよびコントロール 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。

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。モニタリング 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。

さ

サービス パック 新しい機能強化を伴わないバグ フィックスのリリースに使用されます。サービス パックは、ベース バージョンのリリース（マイナーまたはメジャー）の後で、複数のプログラムが累積した形で提供されるものです。

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 アップデート IPS のシグニチャ分析エンジン（SensorApp）と NSDB をアップデートする実行可能イメージ。IPS シグニチャ アップデートの適用は、ウィルス スキャン プログラムでのウィルス定義の更新と似ています。シグニチャ アップデートは単独でリリースされ、独自のバージョン体系になっています。

シグニチャ エンジン センサーのコンポーネントの 1 つ。特定のカテゴリで多数のシグニチャをサポートします。エンジンは、パーサーとインスペクタで構成されています。各エンジンには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メージ。

侵入検知システム 不正な方法によるシステム リソースへのアクセスの試みを発見し、リアルタイムまたはそれに近い形で警告を与えることを目的として、システム イベントの監視と分析を行うセキュリティ サービス。

す

スニファ インターフェイス 「センシング インターフェイス」を参照。

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。

制御インターフェイス NAC では、ネットワーク デバイスと Telnet セッションまたは SSH セッションを開くときに、そのデバイスのルーティング インターフェイスの 1 つがリモート IP アドレスとして使用されます。これが制御インターフェイスです。

制御トランザクション 特定のアプリケーション インスタンスに対して出されたコマンドを含む IPS メッセージ。制御トランザクションには、*start*、*stop*、*getConfig* などがあります。

脆弱性 コンピュータやネットワークの悪用パターンが開始されやすい状況を許す、当該コンピュータやネットワークの 1 つ以上のアトリビュート。

接続ブロック NAC による、特定の発信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックのブロック。

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

センシング インターフェイス 目的のネットワーク セグメントを監視する、センサー上のインターフェイス。センシング インターフェイスは、混合モードです。つまり、IP アドレスを持たず、監視したセグメント上では見えません。

そ

ソース IPS メッセージを生成する、AGM などのアプリケーション。

た

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

ち

調整 シグニチャ パラメータを調整して既存のシグニチャを変更すること。

て

ディスク イメージ IPS アプライアンスのハードディスク ドライブの完全なイメージ。これには、OS、追加ドライバ、サードパーティ製ソフトウェア、IPS ソフトウェアなどが含まれます。

と

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。

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 Firewall などがあります。

の

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

は

バイパス モード センサーに障害があっても、パケットがセンサーを経由してフローし続けることのできるモード。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。

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。

ふ

ファイアウォール ネットワークの境界を保護するセキュリティ デバイス。

複合攻撃 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。

フラグメンテーション IP フラグメンテーションとは、1 つの IP パケットを、すべてがネットワークの最大転送サイズより小さい複数のセグメントに分割することを意味します。

ブロック 指定されたネットワーク ホストまたはネットワークから入ってくるすべてのパケットをネットワーク デバイスが拒否するように指定するセンサーの機能。

ブロック インターフェイス センサーが管理する、ネットワーク デバイス上のインターフェイス。

ブロック解除 それまで適用されていたブロックを削除するようにルータに指示すること。

分析エンジン センサーの設定を処理する IPS ソフトウェア モジュール。インターフェイスをマップし、またシグニチャおよびアラーム チャネル ポリシーを設定済みインターフェイスにマップします。

へ

平面設置 平らな台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。

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 NAC による、特定 IP アドレスからのすべてのトラフィックのブロック。

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。

マニュファクチャリング イメージ イメージ センサーに対するマニュファクチャリングで使用される IPS システムの完全なイメージ。

め

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

メンテナンス パーティション イメージ IDSM-2 のメンテナンス パーティションのイメージの再作成に使用される IPS の完全なイメージ。

も

モニタリング インターフェイス 「センシング インターフェイス」を参照。

ら

ラックマウント センサーを装置ラックに搭載すること。

り

リカバリ パーティション イメージ
アプリケーションの完全なイメージとインストーラを含む IPS イメージ。アプライアンスで復旧に使用されます。

ろ

ロギング
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。