

IPS-1

強固で高精度な侵入防御システム

課題

今日のネットワーク環境は、驚異的速さで変化を続けており、ネットワーク環境の日々の変化、オペレーティング・システムのパッチ提供の遅れ、ハッカーの標的型攻撃による絶え間ない脅威、そして企業や組織内のユーザや社員が不意に悪意のあるプログラムに感染し、ネットワーク中で気づかないうちに攻撃や拡散を開始するワームなど、これらすべてがリアルタイムで企業を危険にさらし、その脆弱性を増大させる要因になっています。今日のネットワーク環境に潜んでいる脆弱性は、ほとんどのネットワーク管理者が追跡できる範囲を超えています。ましてや、ネットワーク内に存在するすべてのデバイスを完璧に管理してすべてを完璧に運用することは、さらに困難です。結果的にネットワークや企業のビジネス環境は、不可避な攻撃に常にさらされているのです。

解決策

Check Point IPS-1™は、ミッション・クリティカルな用途にも対応する、侵入防御 (IPS) 専用のセキュリティ・ソリューションです。IPS-1は、他に類を見ない充実した管理機能と、きめ細かなフォレンジック分析機能を備え、さまざまな導入形態へ柔軟に対応します。IPS-1では、Hybrid Detection Engine™がネットワークの境界で侵入の検知と防御を行い、Dynamic Shielding Architecture™が内部ネットワークを保護する事前の防御機能を提供します。また、侵入防御機能のネットワークへの導入に多大な柔軟性をもたらすConfidence Indexing™により、さらに強固な防御が実現されます。また、IPS-1のこれらの機能はすべて、小規模から大規模に至る、あらゆる規模のネットワークに対応する強力な集中管理環境を利用し管理を行うことが可能になります。

正確できめ細かい攻撃防御

IPS-1システムは、好ましくないネットワーク・トラフィックを素早く確実に遮断できるように設計されており、バックドア型や複合型の脅威 (Code Red、MS Blaster、Nimda、SQL Slammerなどのワーム) だけでなく、SQLインジェクション、コマンド改ざん、多形型バッファ・オーバーフローなどの攻撃を、ネットワークに悪影響を与える前にリアルタイムで防止します。IPS-1は、その中核部分から全体に至るまで、侵入防止のために必要な時間、コスト、および人員を最小限に抑えながら、信頼性の高い侵入防止機能を提供できるように設計されています。

IPS-1の中核を構成するのはHybrid Detection Engine™です。このエンジンには、脆弱性シグネチャ、エクスプロイト・シグネチャ、アノーマリ検出、プロトコル分析、アプリケーションの認識、スマートIP再アセンブリ、オペレーティング・システムやアプリケーションのフィンガープリント、複数要素の相関性、動的なワーム弱体化などを含め、疑わしいトラフィックに対する複数の検出および分析手法が採用されています。広い範囲の脅威をカバーするこの堅牢な検出エンジンにより、IT資産を既知および未知の脅威から確実に保護できます。

IPS-1 Hybrid Detection Engineは、出荷時の標準設定に加え、高性能かつ柔軟なシグネチャ言語も備えています。この言語を使用すると、新しいプロトコル・デコーダやシグネチャを記述したり、既存のデコーダやシグネチャをカスタマイズしたりでき、より精度の高い攻撃検出が可能になります。

製品の概要

Check Point IPS-1™は、ミッション・クリティカルな用途にも対応する、侵入防御 (IPS) 専用のセキュリティ・ソリューションです。IPS-1は、他に類を見ない充実した管理機能と、きめ細かなフォレンジック分析機能を備え、さまざまな導入形態に柔軟に対応します。

製品の特徴

- ネットワーク・レイヤとアプリケーション・レイヤの攻撃を防御するため、複数の検出および分析手法が採用されているHybrid Detection Engine™
- Confidence Indexing™は、セキュリティ実施の指示および調整を行います。
- 高度なフォレンジック分析および報告機能
- すべてのIPS-1センサーをリアルタイムでグラフィカルに表示する集中管理機能
- シグネチャおよびプロトコル・デコーダのカスタマイズを可能にする高性能かつ柔軟なシグネチャ言語

製品の利点

- 既知の攻撃と未知の攻撃の両方からネットワークやITシステムを保護
- 好ましくないネットワーク・トラフィックを素早く確実に遮断
- フォレンジック調査を支援し、攻撃元および攻撃の対象を確実に特定
- IPSを容易に導入および管理可能



IPS-1は、Confidence Indexingという名の便利な機能を備えています。この機能を使用すると、脅威や攻撃を受けているネットワーク・リソースなど、さまざまな要因に応じて防止実施を指示および調整できます。このような方法により、正当なトラフィックのみが通過しているという信頼性を実現し、誤検知の確率を下げています。

認識、適応、対処が可能なセキュリティ

IPS-1は、認識、適応、および対処が可能なセキュリティを提供します。つまり、ネットワーク環境を認識して環境内の変更に適応し、それらの変更を攻撃から保護するための対応策を講じることができます。これにより、ネットワーク・セキュリティの管理を簡素化しつつセキュリティを強化でき、ネットワーク・セキュリティ・チームをより付加価値の高いセキュリティ機能に集中させることができます。

侵入防止における画期的なテクノロジーであるIPS-1 Dynamic Shielding Architectureは、高度な認識、適応、対処が可能なセキュリティを実現する上で鍵となる技術です。IPS-1は、脅威の対象となるポイントを自動的に認識し、それらを不可避な攻撃から動的に保護します。また、致命的な脆弱性やネットワーク内の変更を識別し、脅威の対象となるポイントをセキュリティ・マネージャに警告したり、適切なシグネチャ・セットを自動的に導入して攻撃前に脅威となるポイントを保護することもできます。

高度なフォレンジック分析およびレポート機能

IPS-1は優れた分析機能を備えており、管理者は攻撃データを詳細に分析し、攻撃やイベントの傾向に関するレポートを作成できます。IPS-1 Management Dashboardを使用すると、ドリルダウン形式ですべてのセンサーの全体像をリアルタイムでグラフィカルに表示できるだけでなく、イベントや警告のデータに関する詳細情報を確認したりグループ化したりすることで、攻撃元とその対象を確実に特定できます。また、攻撃グラフと攻撃ベクトル・タイムラインをカスタマイズして、攻撃と防止のアクティビティをリアルタイムに監視できる独自のウィンドウを作成できます。

警告データは一般的なグループに簡単に分類でき、ユーザが設定した条件に基づいてグループをカスタマイズすることで、攻撃元のIP、攻撃タイプ、攻撃対象の脆弱性などのフィールドごとにグループ化できます。



特定の期間に発生した警告を簡単に分析できる直観的なタイムライン・ビュー

レポートのカスタマイズは、Crystal Reportsを使用して簡単に生成できます。あらかじめ定義された各種レポートを選択し、要件に合わせて修正を加えるだけです。

直観的な集中管理機能

IPS-1の集中管理機能は、中小規模環境で利用する場合には簡略さを、大規模環境で利用する場合には直観的で機能性に優れた集中管理とスケラビリティを提供します。

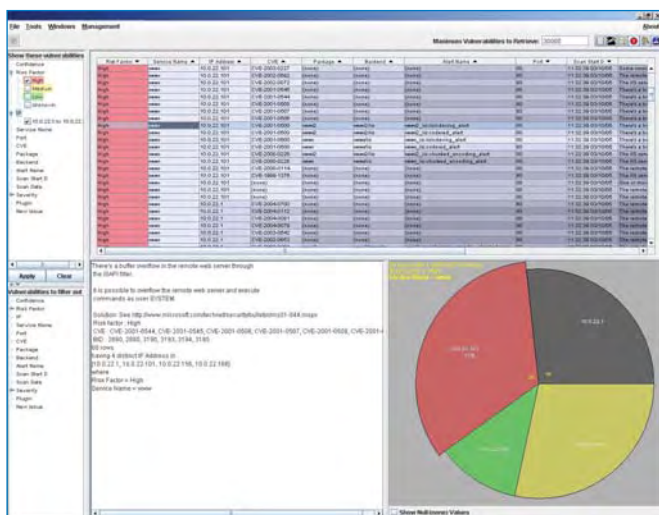
グラフィック機能、自動化機能、ウィザード機能を使用することで、ネットワーク・セキュリティをより直観的、より効率的に管理でき、ネットワーク管理者の作業時間を短縮できます。

リアルタイム監視、ポリシー管理などの主要機能も、ウィザード形式で簡単に設定できます。また、警告を集約する機能も備えており、複合フィールドを含むすべてのフィールドに基づいてイベント・データを集計できます。

IPS-1のアーキテクチャ

IPS-1システムは3層アーキテクチャをベースとしており、小さな設置スペースに小規模に導入して効率的に管理できると同時に、簡単に拡張して何百ものセンサーを使用する大規模な導入をサポートし、利用環境にあわせ柔軟に対応します。各IPS-1システムは、以下のコンポーネントで構成されています。

- **IPS-1 Sensor** - IPS-1 Sensorには、多様な脅威からネットワークを保護するため、複数の検出および分析手法が採用されています。各センサーは、パッシブな侵入検出モードや、インライン・パッシブ、およびインライン・アクティブのIPSモードで動作させることができます。IPS-1 Sensorは、導入環境が必要とする要件やネットワーク上の設置場所に合わせて、さまざまなモデルが用意されています。詳細については、モデルと仕様に関するセクションをご覧ください。
- **IPS-1 Management Server** - IPS-1 Management Serverは、IPS-1 Sensorが生成した警告やイベントのデータを受信、処理、および管理し、IPS-1 Sensorを集中管理するための機能を提供します。

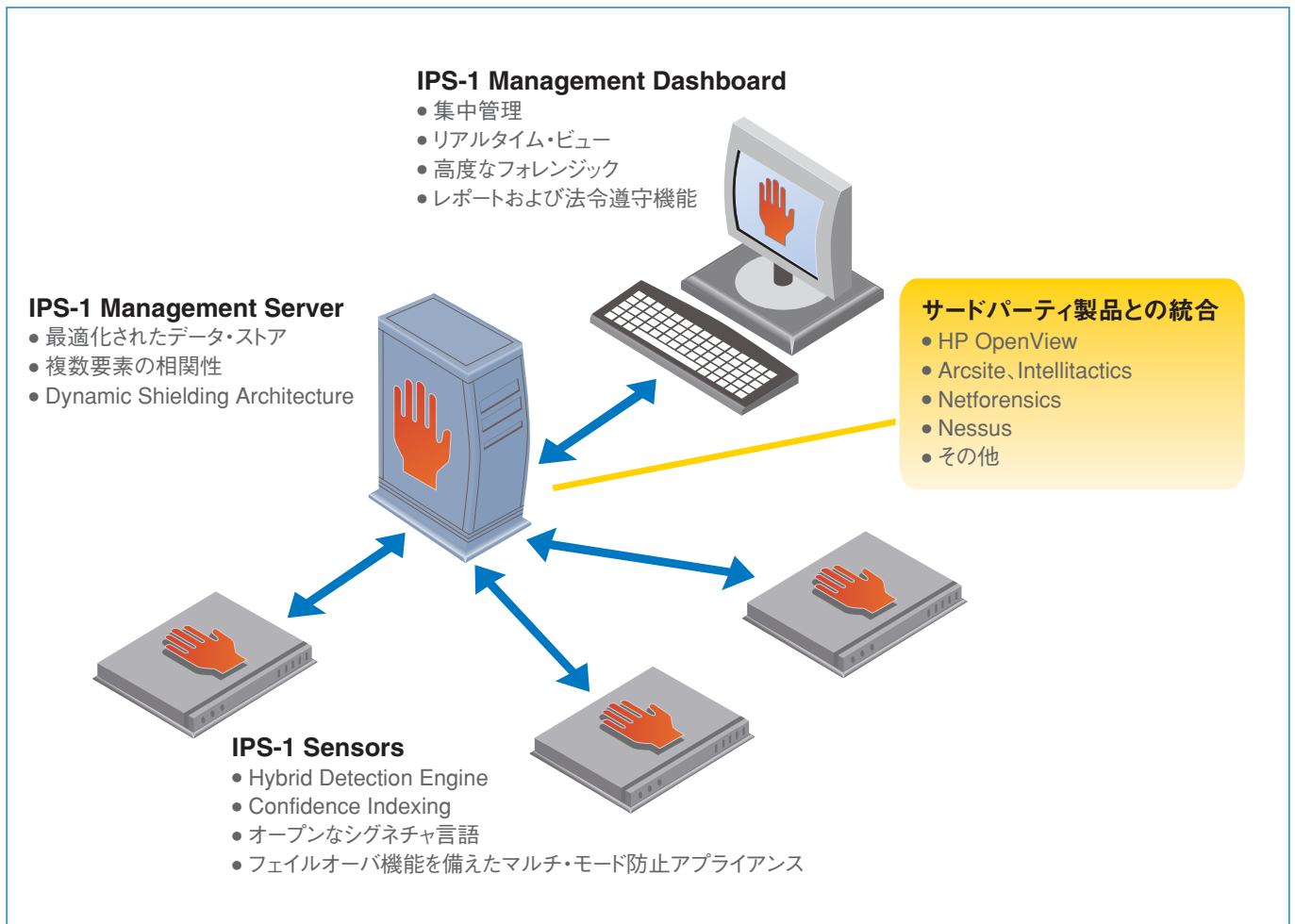


1つのダッシュボードから脆弱性をスキャン、表示、および管理を可能にするIPS-1脆弱性ブラウザ (Vulnerability Browser)

- **IPS-1 Management Dashboard - IPS-1 Management Dashboard**
は、IPS-1の管理コンポーネントです。
IPS-1 Management Dashboardを使用すると、システム内全体で生成された警告を監視し、ハイレベルな分析を行えます。

SmartDefenseサービスによる継続的なセキュリティ・アップデート

他のチェック・ポイントのセキュリティ・ソリューションと同様に、IPS-1システムもチェック・ポイントSmartDefense™サービスによって常に最新のセキュリティ脅威に対応できるようアップデートが行えます。このサービスは、絶えず進化を遂げる脅威の常に一步先を行くセキュリティ・アップデートで、最新脅威に対応するためのアップデートや、設定に関するアドバイスを含み、セキュリティ・アドバイザリをリアルタイムで提供し、チェック・ポイントのセキュリティ・ソリューションを継続的に更新するためのサービスです。チェック・ポイントSmartDefense研究センターのセキュリティ専門家が、最新の脅威からの確実な保護を提供するため、インターネットに出現する新しいエクスプロイトや脆弱性を継続的に監視し、新しい防御機能やシグネチャを迅速に開発して配布しています。



3層アーキテクチャをベースとし、信頼性とスケーラビリティを提供するIPS-1侵入防止システム

IPS-1のモデルおよび仕様

	IPS-1 Sensor 50	IPS-1 Sensor 200	IPS-1 Sensor 500	IPS-1 Power Sensor 1000	IPS-1 Power Sensor 2000
ネットワーク上の導入対象環境	リモート・オフィス/ ネットワークの境界	リモート・オフィス/ ネットワークの境界	ネットワークの境界 (マルチ・セグメント)	ネットワーク・コア (マルチ・セグメント)	ネットワーク・コア (マルチ・セグメント)
パフォーマンス					
スループット (IPS/IDS)	50/75 Mbps	200/250 Mbps	500Mbps/1Gbps	1/2Gbps	2/4Gbps
同時セッション数(定格の最大数)	100,000	200,000	500,000	1,200,000	2,800,000
筐体の仕様					
フォーム・ファクタ	1-RU	1-RU	1-RU	2-RU	2 @ 2-RU
筐体寸法 H x W x D (cm)	4.325 x 42.6 x 37.98	4.325 x 43.0 x 67.2	4.325 x 43.0 x 69.8	8.9 x 43.2 x 57.1	8.9 x 43.2 x 57.1
重量 (kg)	6.8	14.1	15.8	18	2 @ 18
モニタリング・インタフェース	10/100/1000 Mbps copper x 2	10/100/1000 Mbps copper x 2 または1000 Mbps fiber x 2	10/100/1000 Mbps copper x 4 または1000 Mbps fiber x 4	10/100/1000 Mbps copper x 8 または1000 Mbps fiber x 8	10/100/1000 Mbps copper x 8 または1000 Mbps fiber x 8
管理インタフェース	10/100/1000 Mbps copper x 1	10/100/1000 Mbps copper x 1	10/100/1000 Mbps copper x 1	10/100 Mbps copper	10/100 Mbps copper
ロック機構付きフロント・ベゼル	-	あり	あり	-	-
冗長化電源	-	あり	あり	あり	あり
冗長化記憶装置	-	-	-	あり	あり
ハードウェア・レベルでのバイパス	可能	可能	可能	可能 (copperのみ)	可能 (copperのみ)
主要コンポーネントのホットスワップ	-	-	-	可能	可能
データ転送速度のアップグレード	-	-	-	可能	可能
電源					
アンペア	6/3	6.5/3.2	6.7	5	10 (1ボックスあたり5)
電圧 (AC)	110/220	100/127	100/127	110/220	100/240
入力範囲 (AC)	100-240	100-127/200-240	100-127/200-240	-	-
使用環境					
動作温度条件	0°C~40°C	10°C~35°C	10°C~35°C	0°C~40°C (周囲温度)	0°C~40°C (周囲温度)
非動作時温度条件	-20°C~80°C	-40°C~70°C	-40°C~70°C	-	-
湿度条件	10%~90% (結露なきこと)	10%~90% (結露なきこと)	10%~90% (結露なきこと)	10%~90% (結露なきこと)	10%~90% (結露なきこと)
適合規格	FCC Class A デバイス	FCC Class A デバイス	FCC Class A デバイス	FCC Part 15 Class A Subpart B (米国/カナダ)	FCC Part 15 Class A Subpart B (米国/カナダ)

*Sentivist™ Smart Sensor 100C v1.3にてNSS認定を取得



©2003-2007 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

P/N 502334-J 2007.03 ※記載された製品仕様は予告無く変更される場合があります。