

totalsecurity™



Check Point®
SOFTWARE TECHNOLOGIES LTD.



革新的な侵入防御ソリューション

Check Point IPS Software Blade

画期的な価格で画期的なパフォーマンスと保護機能を実現

Contents

本書の内容

妥協不要の新型IPS	3
最高レベルのセキュリティ	3
プロアクティブな脅威制御	3
誤検知の削減	5
リアルタイムのアップデート	5
一貫性のあるセキュリティ・ポリシー	5
トップ・レベルのパフォーマンス	5
画期的なコスト	7
導入コストの低減	7
簡単な導入	7
環境負荷の低減	8
まとめ	9

妥協不要の新型IPS

侵入防御システム (IPS) によるネットワーク保護を導入する場合、これまでは2つの選択肢に迫られていました。1つは高価なIPS専用システムの利用、もう1つはパフォーマンスとセキュリティの面で堅牢性に欠ける統合システムの利用です。また多くの場合、IPSはその性能を最大限発揮するようには使用されていませんでした。つまり、オフラインで設置され、攻撃を未然に防ぐのではなく単に記録するだけの「侵入検知システム」として利用されるケースが多かったのです。この場合、IPSはネットワークを攻撃から保護できていないだけでなく、価値を十分に発揮することができず、投資対効果 (ROI) が損なわれる結果となります。ITセキュリティにおいてIPSが「当然導入すべき」基本コンポーネントになったのであれば、次世代のIPSではより優れたコスト効率の高い導入オプションが提供されるべきとチェック・ポイントでは考えます。

そこでチェック・ポイントは、新しいIPSソリューションを開発しました。チェック・ポイントのIPS Software Bladeは、トップ・レベルのパフォーマンスとトータル・セキュリティを画期的なTCOで実現できる統合ソリューションを提供します。IPS Software Bladeは、チェック・ポイントの柔軟で拡張性の高いSoftware Bladeアーキテクチャを構成するブレードの1つで、マルチ・ギガビットの速度で動作するフル機能の侵入防御をチェック・ポイントのセキュリティ・ゲートウェイに統合します。IPS Software Bladeは、導入や管理が容易な統合ソリューションであるにもかかわらず、IPS専用システムを超えるパフォーマンスを従来のIPSソリューションよりも大幅に低いコストで実現します。

最高レベルのセキュリティ

IPS Software Bladeは、包括的なIPSセキュリティ・ソリューションです。次のような悪意のある、あるいは好ましくないネットワーク・トラフィックに対する幅広い保護機能を提供します。

- マルウェアによる攻撃
- サービス妨害 (DoS) 攻撃および分散サービス妨害攻撃 (DDoS) 攻撃
- アプリケーションやサーバの脆弱性を狙う攻撃
- Microsoft製品の脆弱性を狙う攻撃
- 内部からの脅威
- インスタント・メッセージング (IM) やピアツーピア (P2P) など、好ましくないアプリケーションのトラフィック

プロアクティブな脅威制御

IPS Software Bladeは、以下の最新技術の採用により、完全かつ正確な脅威保護機能を提供します。

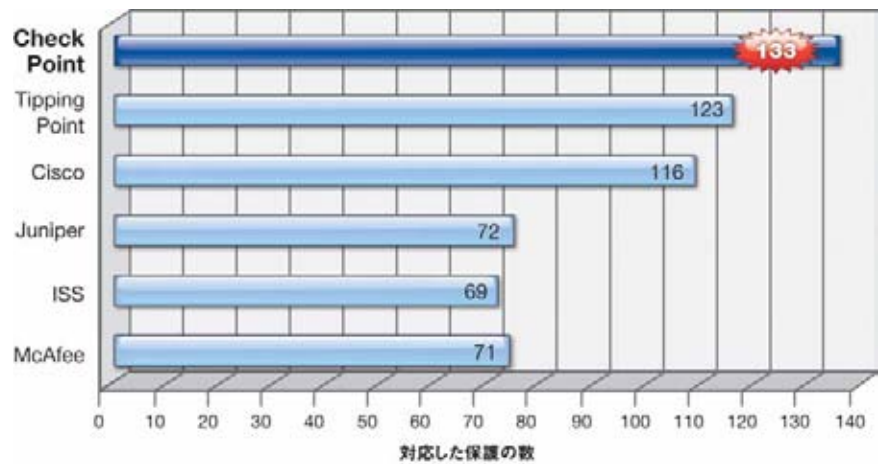
- パッシブ・ストリーミング・ライブラリ
 - IPSの回避およびネットワーク攻撃からの保護
- プロトコル・パーサ (Protocol Parser)
 - プロトコル準拠の確認とアノマリ検出
- パターン照合 (Pattern Matcher)
 - 悪意のあるパケットに共通する特徴を素早く特定
 - 第2段階の解析により攻撃が本物かどうかを確認

チェック・ポイントのIPSの利点：

- ゲートウェイにおける統合化ソリューション
- トータル・セキュリティ
- マルチ・ギガビットの高いパフォーマンス
- 画期的なTCO効果

- 複合シグネチャによる脅威の特定
 - 高度なシグネチャ検査により脅威を正確に特定
 - 複数のプロトコル部分から得られた手がかりをもとに攻撃をピンポイントで特定
- コンテキスト管理インフラストラクチャ
 - トラフィックの解析後、プロトコル内の関係のあるコンテンツだけを検査
- INSPECT v2
 - 既知のコンテキストに基づいて攻撃を特定し、明確に定義されたプロトコルを持たないアプリケーションを検査

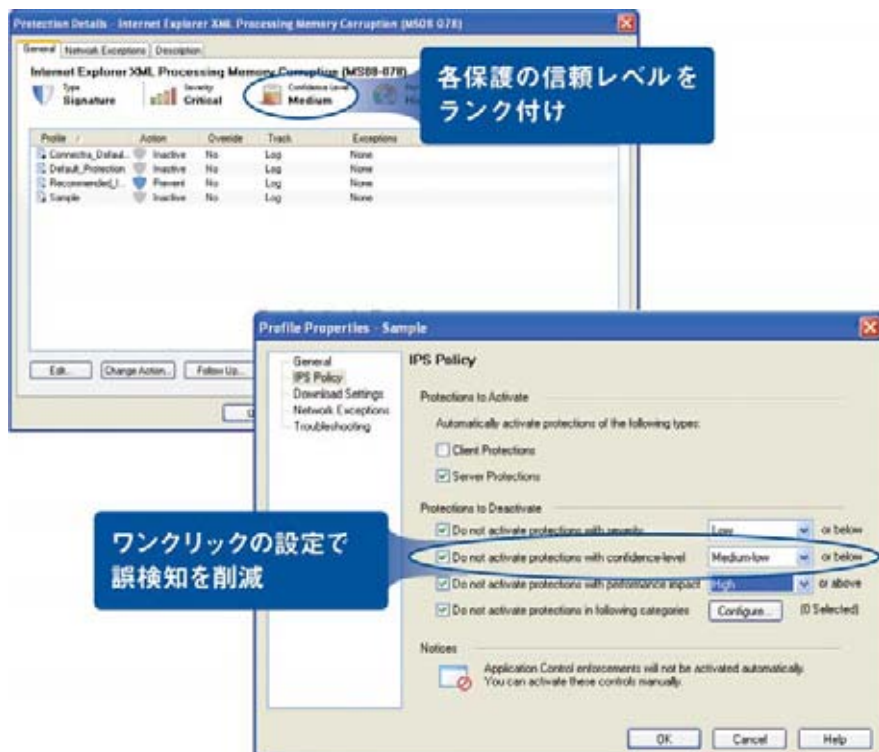
これらの先進技術の採用によって、チェック・ポイントのトップ・レベルの保護機能が実現されています。チェック・ポイントのアップデート・チームは、2008年のMicrosoft製品の脆弱性への対応数で最多を誇っており、2009年もIPS Software Bladeの投入によってそのリードを維持しています。



Microsoft製品の脆弱性の保護 (2008第1四半期~2009年第1四半期)

誤検知の削減

この新型IPSエンジンでは、保護の精度の向上により誤検知が削減されただけでなく、各保護が信頼性レベルに従ってランク付けされるようになりました。ワンクリックの簡単な設定で、信頼性レベルの高い保護のみを有効にすることも可能です。



Check Point R70 Dashboard: ポリシーおよび保護の詳細設定

リアルタイムのアップデート

IPS Software Bladeには保護機能のアップデート・サブスクリプション・サービスが付属するため、製品に加えてサービスを追加購入する必要がありません。チェック・ポイントのアップデート・サービスでは、使いやすい管理インターフェースを通じて最新の保護機能が提供されます。このインターフェースを使用して、新しいアップデートを確実に効率的に管理することができます。IPS Software Bladeでは、最新の脅威に対応するための新しい防御が絶え間なく更新されます。また、誤検知を削減しながら保護性能とパフォーマンスを最大限に引き出すには、それらの更新の設定方法についてもチェック・ポイントは詳しい情報を提供しています。これらのIPS機能の多くは事前対応型であり、脆弱性が発見/公開される前、すなわちその脆弱性を攻撃するコードが出現する前でも脆弱性を保護することが可能です。

一貫性のあるセキュリティ・ポリシー

セキュリティ・ポリシー実施ソリューションのコンポーネントが複数あると、ポリシーやルールの複雑さは増大します。その場合、潜在的なセキュリティ・リスクも倍増します。複雑さが増すと、脅威や攻撃を見逃したりトラフィックを複数回チェックしたりする可能性が高まります。どちらも望ましいことではありません。チェック・ポイントでは、IPSソリューションを完全に統合することにより、1つに集約された一貫性のあるセキュリティ・ポリシーを実現しています。

トップ・レベルのパフォーマンス

IPSをファイアウォールに統合すると、パフォーマンスが劣化してシステムが停止するおそれがあるとの理由から、これまで多くの企業は統合型IPSを避ける傾向にありました。このような心配は、セキュリティを犠牲にすることなく、驚くほど低いコストでトップ・レベルのパフォーマンスを実現できるIPS Software Bladeによって過去のものとなりました。

誤検知の削減:

- 検出精度の向上
- 各保護の信頼レベルをランク付け

リアルタイムのアップデート:

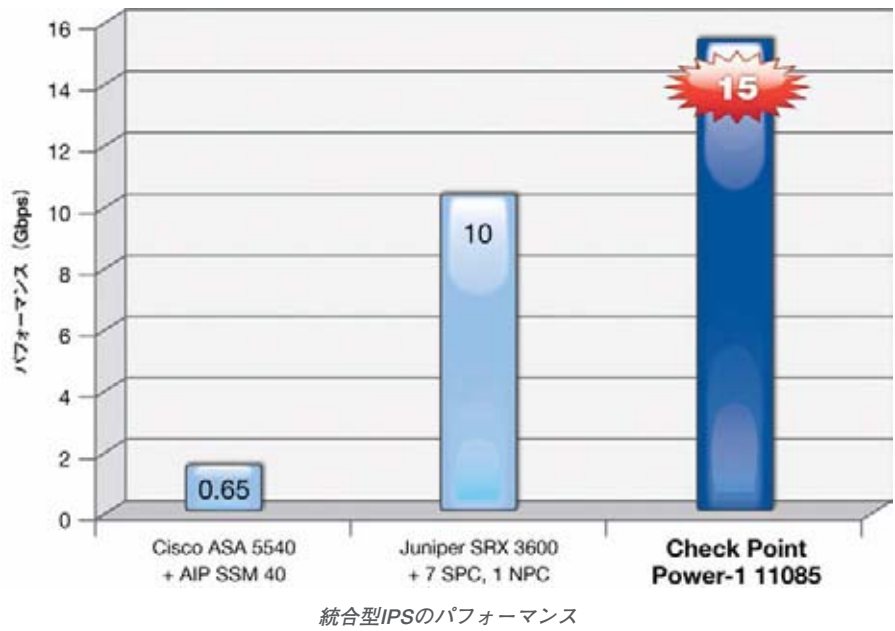
- サービスの追加購入は不要
- 使いやすい管理インターフェース
- 新しい防御機能を常時提供

一貫性のあるセキュリティ・ポリシー:

- 障害点の削減
- トラフィックを1回のみチェック

トップ・レベルの パフォーマンス:

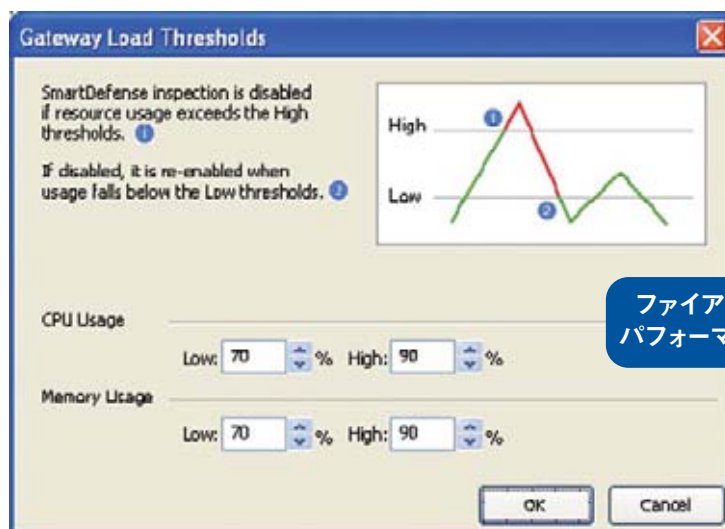
- 新しいアクセラレーション技術
- メモリ使用量の削減
- ファイアウォール・パフォーマンスへの影響はなし



チェック・ポイントの先進技術が、IPS統合ソリューションのパフォーマンスに革新をもたらしました。チェック・ポイントのオープン・パフォーマンス・プラットフォームは、IPS Software Bladeを支える3つのパフォーマンス拡張技術、SecureXL™、CoreXL™、ClusterXL®を基盤としています。これらの技術を組み合わせることで、IPSとファイアウォールの両方を有効にした場合で最大15Gbpsのスループットを実現しました。

チェック・ポイントの統合ソリューションでは、アクセラレーション技術に加え、ファイアウォールとIPSでのトラフィック検査を1回で済ますことでパフォーマンスへの影響を最小限に抑えています。

またIPS Software Bladeでは、ゲートウェイのCPUとメモリの使用率に基づいてパフォーマンスのしきい値を設定することができます。設定されたしきい値をリソース使用率が上回ると、IPSによる分析は自動的に一時停止します。その後、リソース使用率がしきい値を下回るとIPSによる分析が再開します。これによって、ファイアウォールのスループットと実施中のネットワーク・オペレーションが保証されることになります。IPS Software Bladeが原因で、ファイアウォールのパフォーマンスが許容範囲を下回ることを心配する必要はありません。



ゲートウェイに対する負荷のしきい値の設定

チェック・ポイントの先進のパフォーマンス技術の詳細については、技術白書「IPSの統合におけるパフォーマンス上の課題と解決」をご覧ください。

画期的なコスト


複数のセキュリティ・アプライアンスを購入、導入、運用する場合に比べ、IPS Software Bladeのような統合ソリューションを導入するとコストを大幅に削減できます。削減できるコストとしては、アプライアンスの購入をはじめとする機器コストと、トレーニングや継続的な管理のような運用コストが考えられます。セキュリティ機能を1つのゲートウェイに集約することで、ラック・スペース、ケーブル、冷却コスト、消費電力などの継続的な運用コストも削減できます。チェック・ポイントのIPS Software Bladeが提供するソリューションであれば、IPS保護を統合することによるメリットを大幅に低いコストですべて享受できます。

IPS Software Bladeをチェック・ポイントのゲートウェイに追加する場合、必要な運用コストはわずか¥396,000です。IPS Software Bladeでは、ハードウェアやメンテナンス、トレーニングに必要な追加コストやその他の潜在的に必要なコストが発生しません。

導入コストの低減

追加のハードウェアを購入してIPS専用ソリューションをサポートするコストは、思った以上に高額になる可能性があります。チェック・ポイントが提供するファイアウォールとIPSの統合ソリューションは、パフォーマンスを犠牲にすることなく、同程度の専用ソリューションの10%ほどの価格で購入できます。

他の統合ソリューションと比較した場合でも、IPS Software Bladeは数分の1のコストで卓越したパフォーマンスを提供します。

中規模企業	チェック・ポイントのソリューション Power-1 5075にIPS Software Bladeを統合	IBM (ISS) の専用ソリューション IPS Proventia GX 6116
IPSのパフォーマンス (Mbps)	7,500	6,000
追加ハードウェアの価格	-	\$ 188,995
ソリューションの導入価格	\$ 3,000	\$ 188,995
Mbpsあたりのコスト	 \$ 0.40	\$ 31.50
パフォーマンスは向上、コストは1/78!		

IPS Software Bladeと専用ソリューションのコスト比較

簡単な導入

IPSソリューションはコストが高く導入に時間がかかる、というのがこれまでの常識でした。新たに専用のIPSデバイスをネットワーク全体に導入しなければならないだけでなく、まったく異なるシステムを管理できるよう管理者をトレーニングする必要があり、その上管理しなければならないベンダーが1社増えるのです。しかし、このような導入に伴う各種マイナス要因は過去のものとなりました。チェック・ポイントのIPS Software Bladeなら、侵入防御をワンクリックで導入してIPS保護を直ちに実現し、ソリューションへの投資を短期間で回収できます。

昨今の多くのネットワーク環境では既にファイアウォールが導入されているため、それらのファイアウォールにIPS機能を追加することができれば、追加デバイスを購入して導入する場合に比べ、財政面でも人員面でも大幅に負担を軽減できます。チェック・ポイントのセキュリティ・ゲートウェイのユーザであれば、単一の管理コンソールからワンクリックでIPS保護を有効にできます。

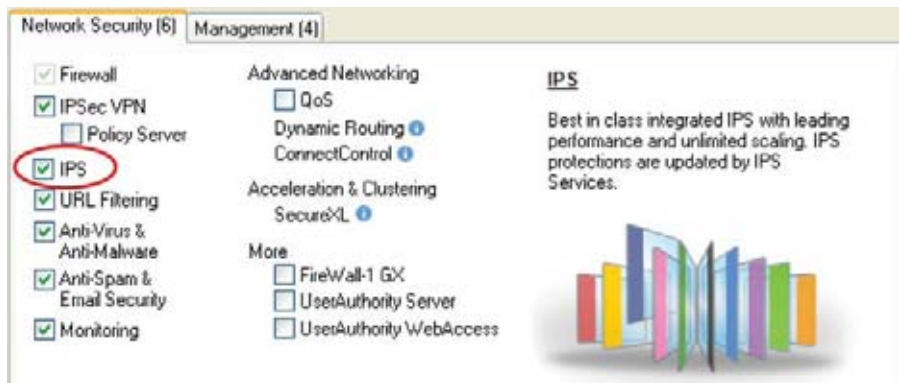
画期的なコスト:

- 資本コストの削減
- 運用コストの削減
- ラック・スペース、ケーブル、冷却コストの削減

必要なコストは 専用ソリューションの1/10

簡単な導入:

- ワン・クリックで導入
- 単一の管理コンソール
- 投資を短期間で回収



Check Point R70 SmartDashboard : IPSの有効化

複数のベンダーから複数のソリューションを導入すると、管理が複雑になりスタッフのトレーニングにもより多くの時間が必要になります。統合ソリューションなら、管理やトレーニングにかかる費用だけでなく、エラーやミスの発生も減らすことができます。ファイアウォール機能とIPS機能のほとんどは同じネットワーク・セキュリティ・グループで管理するのが一般的であるため、ファイアウォールとIPSが統合されたとしても問題なく統合管理が行えます。

環境負荷の低減：

- ケーブルの削減
- 冷却コストの削減
- 消費電力の低減

環境負荷の低減

継続的に発生する運用コストは、時間の経過とともにセキュリティ・ソリューションの総コストの50%以上を占めるようになります。多くの企業は、まずハードウェアの設置に必要なラック・スペースの確保に四苦八苦し、その先何年もの間、電力や冷却コストといった継続的な費用を抱えることとなります。

IPS Software Bladeのような統合ソリューションであれば、ラック・スペース、ケーブル、冷却コスト、消費電力などの継続的な運用コストも削減できます。このことは、組織のコスト削減に寄与するだけでなく、より「グリーン」なセキュリティ・ソリューションを所有することにもつながるのです。



* チェック・ポイントのソリューション: Power-1 11065にIPS Software Bladeを統合
 ** CiscoとIBM (ISS) のIPS専用ソリューション: ASA 5580-40とProventia GX 6116
 *** CiscoとMcAfeeのソリューション: ASA 5580-40とIntruShield M8000

IPS Software Bladeと専用ソリューションの運用コストおよび環境への影響の比較

他の統合システムと比較した場合でも、必要なラック・スペースの小ささ、消費電力や放熱量の少なさなどから見て、チェック・ポイントのソリューションの方が無駄がなくグリーン効果も高いと結論付けることができます。

まとめ

チェック・ポイントの統合型IPS Software Bladeは、IPSとネットワーク・セキュリティのあり方を大きく変える製品です。もはや、価格やパフォーマンス、セキュリティ保護レベルの間のトレードオフを考える必要はありません。

チェック・ポイントの革新的でコスト効率の高い手法であれば、所有するすべてのセキュリティ・ゲートウェイでIPS保護機能を利用できます。画期的なパフォーマンスと最高レベルのセキュリティ機能を誇るIPS技術が、使いやすいソリューションとして手頃な価格で入手できるようになったのです。

IPS Software Bladeは、価格、パフォーマンス、保護機能のあらゆる面で侵入防御に革命をもたらす画期的な製品です。



Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) は、インターネット・セキュリティにおけるトップ企業として、特にネットワーク、データ、およびエンドポイントのトータル・セキュリティを単一の統合管理フレームワークで提供できる唯一のベンダーとして広く認められています。チェック・ポイントは、セキュリティの複雑さと総所有コスト (TCO) を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。2009年には、新たな革新的セキュリティ技術としてSoftware Bladeアーキテクチャを開発しました。Software Bladeアーキテクチャは、導入先にあわせカスタマイズすることで、あらゆる組織、あらゆる環境のセキュリティ・ニーズにも的確でダイナミックに対応できる、安全かつ柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、Fortune 100社の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントのZoneAlarmソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。

© 2003-2009 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, 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, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, puresecurityのロゴ, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, totalsecurityのロゴ, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, 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、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076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。

The New Face of Intrusion Prevention

P/N:600010-J 2009.07

※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。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
 〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500