

Web Intelligence

Web環境全体に対するセキュリティ保護

課題

企業はビジネスを遂行するにあたり、ますますインターネットへの依存度を高めつつあります。企業のLAN上でのみ使用可能であった従来のクライアント・サーバ型のアプリケーションは、現在Webを通じてアクセスできることも珍しくなくなりました。しかしながら、インターネット、イントラネット、およびエクストラネットの急速な融合は、利便性をもたらすばかりではなく、ミッション・クリティカルなデータを攻撃者などに晒すリスクも増大させてしまう危険性もあります。

Web環境は、ネットワーク、オペレーティング・システム、Webサーバ、およびバックエンド・システムに関する全体の視野で考える必要があります。Web用に構築された多くのソフトウェア・アプリケーションは、セキュリティが優先的に考慮されていないのが実状であり、結果的に、Webアプリケーションは、デコードするユニコードからバッファ・オーバーフローの様々な形式におよぶセキュリティ上の欠陥を多く抱えています。

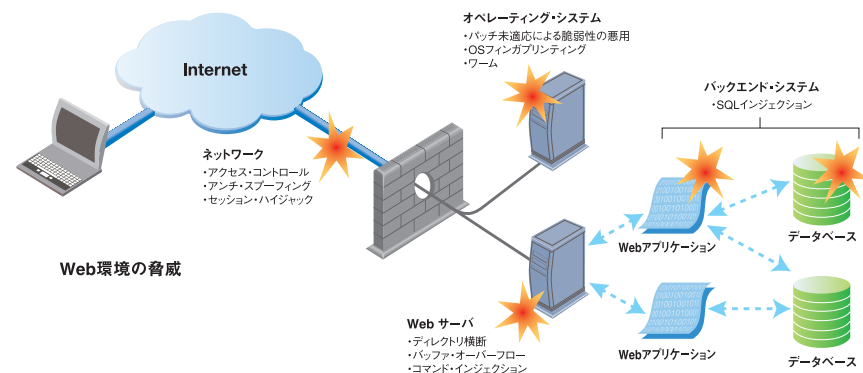
攻撃者は、Web環境の脆弱な部分を悪用する革新的な手法によって絶え間なく攻撃先を探し続けています。Webアプリケーションは利用の機会が広がるにつれて、攻撃者の主要な攻撃目標になってしまっているのが現状です。

企業など各種組織は、Webに対する投資および貴重なデータを確実に保護するための解決策を見出すべく奮闘していますが、そのほとんどの解決策は全体の中の一部分に対してのみ有効なソリューションで、Web環境全体を保護するために完全な解決策を提供することができていません。

解決策

チェック・ポイントのWeb Intelligence™は、Web環境全体に向けた完全なセキュリティ保護を提供する、唯一のWebアプリケーション・ファイアウォール技術です。VPN-1®Power、VPN-1 UTM、UTM-1、およびConnectra™などのチェック・ポイントのセキュリティ・ゲートウェイは、ネットワーク、オペレーティング・システム、Webサーバ、およびバックエンド・システムに対しマルチ・レイヤの防御を提供するためのステートフル・インスペクション技術、Application Intelligence™技術、およびWeb Intelligence™を実装します。

Web Intelligenceは、防御機能のアップデートおよび設定アドバイザリをリアルタイムで提供するSmartDefenseサービスを通じて、最新の脅威にも対応します。



Webインフラストラクチャの各レイヤにおける様々な脆弱性

製品の概要

Web Intelligence™は、Webインフラストラクチャに対する攻撃を検知および防止する先進的な機能です。Web Intelligenceは、ビジネスおよび通信でWebを利用する際に包括的な保護機能を提供します。

製品の特徴

- Malicious Code Protector™
- 悪意のあるコードからの防御機能
- Advanced Streaming Inspection
- 先進のストリーミング検査技術
- 簡単な導入と管理
- チェック・ポイント製品とのシームレスな統合

製品の利点

- バッファ・オーバーフロー攻撃より最も強力に保護
- アプリケーション・レベルのWebセキュリティをワイヤ・スピードで実現
- ヘルプデスクのWebページが挿入可能、エンド・ユーザの利用感を向上
- ミッション・クリティカルなアプリケーションに迅速に導入することが可能
- SmartDefense™サービスにより、新たに出現した脅威にも対応

NGX™

NGXプラットフォームによりチェック・ポイントの統一されたセキュリティ・アーキテクチャを実現します。

Web Intelligence機能

Malicious Code Protector (悪意のあるコードからの防御機能)

チェック・ポイントが特許出願中のMalicious Code Protector™は、Webサーバやアプリケーションを目標とするバッファ・オーバーフロー、ヒープ・オーバーフロー、および悪意のある実行可能なコードについて、シグネチャを必要としない革新的な手法により認識します。Malicious Code Protectorは、チェック・ポイントのApplication Intelligence上に更なる強力な保護機能を提供します。Malicious Code Protectorは、データ・ストリームの中の実行可能なコードの存在を検出するだけでなく、悪意があると推測できる行動を識別することで、Webトラフィックに含まれる悪意のある実行可能なコードを確実に検出します

Malicious Code Protectorは4つの重要なアクションを実行します。

- 潜在的な実行可能なコードを検出するためにWeb通信を監視
- 実行可能なコードの存在を確認
- 実行可能なコードにおける悪意の有無を認識
- 目標ホストに達する前に、悪意のある実行可能なコードをブロック

Malicious Code Protectorの攻撃防御機能は、未知および既知の攻撃を識別します。

最近のテストラボにおける検証結果によると、Malicious Code Protectorは、検出精度が極めて高く、誤検出の発生率が極めて低いことが実証されています。さらに、Malicious Code Protectorは、カーネル・レベルで動作するため、高い検出能力を発揮しつつ、ワイヤ・スピードのスループットを実現するので、保護レベルでパフォーマンスの低下を犠牲にすることはありません。

Advanced Streaming Inspection

(先進のストリーミング検査)

Advanced Streaming Inspectionは、通信データのコンテキスト全体を検査する、チェック・ポイントのカーネル・ベースの技術により実現します。ステートフル・インスペクションおよびApplication Intelligenceと同様に、Advanced Streaming Inspectionは、チェック・ポイントのINSPECT™エンジンを基に行われます。この技術は、セッションおよびアプリケーション情報に基づきリアルタイムでセキュリティ判断を実施できるため、仮に複数のTCPセグメント間にまたがるWeb通信が行われていても、それをWeb Intelligenceで正しく理解することを可能にします。

Web Intelligenceは、アプリケーションに関わる検査プロセスをカーネル・レベルに集約することで、スループット、および接続数を維持しつつ高度な検査を行えます。

Web Intelligenceのパフォーマンス*

スループット : 1.9 Gbps

コネクション・レート : 8,300 HTTPコネクション/sec

*パフォーマンスは、デフォルトのWeb Intelligenceの設定で測定

迅速な対応を実現

Advanced Streaming Inspectionは、Webコネクションの内容をすばやく変更する機能を実現したWeb Intelligenceに含まれるActive Streamingを導入しています。この重要な機能は、いくつかのユニークな利点をチェック・ポイントの顧客にもたらします。

Active Streamingは、HTTPヘッダのスプーフィング機能によりWeb環境における重要なサイト固有の情報を隠すことで、初期段階の防御機能を提供します。

隠蔽できる固有情報には、オペレーティング・システムの名前やバージョン、Webサーバやバックエンド・サーバの識別情報などがあります。これらの情報は、一般ユーザーに有益な情報ではありませんが、攻撃目標について情報収集している攻撃者には非常に有益です。Web Intelligenceは、Webのレスポンスに対しサーバの識別情報を含むか、または完全に隠すかの選択肢を管理者に与えた上、攻撃者を困惑させるための全く異なるストリーミングを流すなどの様々な手段を提供します。

操作性の向上

管理者は、Active Streamingを使用して、カスタマイズ可能なエラー・ページを事前に定義することで、エンド・ユーザーの操作性を向上します。

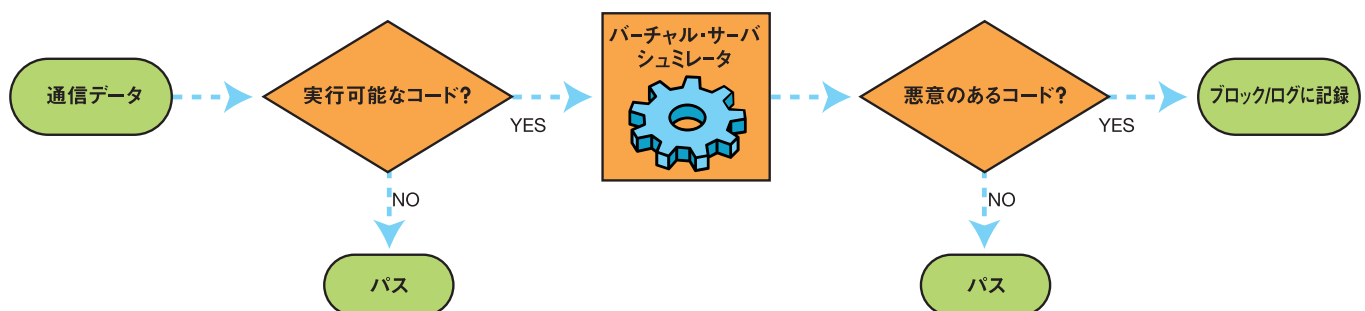
ほとんどのネットワーク・ユーザーにとっては、エラー発生時にWebブラウザで表示される一般的なステータス・コードは無意味です。

Active Streamingでは、エラーが発生した際、管理者が事前に設定した管理者の連絡先やトラブルシューティングの方法が記載されたエラー発生時用のWebページにエンド・ユーザーを転送します。この機能によりエンド・ユーザーに対するサービス・レベルを向上することが可能となります。

簡単な導入と管理

VPN-1とUTM-1に組み込まれたWeb Intelligenceの管理は、SmartCenter™のセキュリティ管理GUIに完全に統合されています。

このユーザー・インターフェイスは、一般的な既知の攻撃に対する防御策があらかじめ定義されています。各攻撃手法に対する防御策は、攻撃名と防御の説明と共に表示されます。右上のスクリーンショットに示すように、「Web Server View」はエンタープライズ・ネットワーク内に存在するWebサーバのためのコマンド・センターで、様々なサーバに適用された保護のタイプの要約に関する情報を提供します。



Malicious Code Protectorは、シグネチャの使用を必要とすることなく、悪意のあるコードを検出およびブロックします。

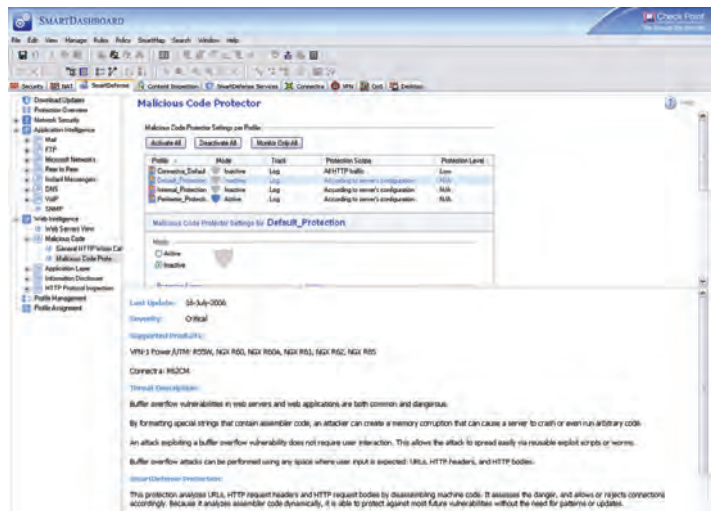
例えば複数のWebサーバが存在する環境で、各Webアプリケーション・サーバに必要なセキュリティ要件が異なる場合、Web Intelligenceは、それぞれ異なるWebアプリケーションやWebサーバのために段階的なセキュリティを設定する機能を備えています。Web Intelligenceを初めて設定する場合、通常2~3分で設定が可能です。

Web Intelligenceは、ミッション・クリティカルな環境に導入する場合などでは、セキュリティ・ポリシーの誤った設定などが原因でアプリケーションの接続がブロックされてしまうリスクを低減するために、一時的に使用するためのモニタ・モードも備えています。

チェック・ポイント製品とのシームレスな統合

Web Intelligenceは、VPN-1 Power、VPN-1 UTM、UTM-1、Connectraゲートウェイと緊密に統合されるため、ハードウェアを追加することなく利用できます。特にVPN-1およびUTM-1を既に利用している環境でWeb Intelligenceを使用する場合、SmartCenterによる管理が可能です。この場合、管理者がSmartCenterのユーザ・インターフェイスに慣れていれば、改めて操作について学習する必要はほとんどありません。また、セキュリティおよび監査のログは、VPN-1およびUTM-1のセキュリティ・ログと統合が可能で、管理者は、SmartCenterが提供する各種ツールにより、セキュリティ問題の兆候などを含む多角的なセキュリティ分析、監査、結果のレポート出力、リアルタイム・モニタリングなど、セキュリティ管理に必須となる様々な分析、解析、診断を行えます。

Web Intelligenceは、チェック・ポイントのセキュリティ・インフラストラクチャの事前防衛的セキュリティを常に最新の状態に維持するSmartDefenseサービスにも対応しています。SmartDefenseサービスは、最新の脅威や攻撃の一步先を行くことを可能にするため、各種のアップデートや、防御機能およびセキュリティ・ポリシーの設定アドバイザリをリアルタイムで提供します。



VPN-1およびUTM-1と統合されたWeb Intelligenceは、SmartCenterによる統合管理が可能で、セキュリティの集中管理、ログの記録、およびモニタリングが可能です。

No.	Date	Time	Origin	Service	Source	Destination	Rule	Curr. Rule No.	Rule Name
44	18Nov2002	15:00:41	California_GW	smtp	California.LAN.hemilton	florida-abc-corp.lbc	4	4-Standard	rule 4
45	18Nov2002	15:06:28	California_GW	smtp	California.LAN.hemilton	florida-abc-corp.lbc	4	4-Standard	rule 4
46	18Nov2002	15:41:28	California_GW	smtp	California.LAN.hemilton	California_GW	4	4-Standard	rule 4
47	18Nov2002	16:43:13	California_GW	web	California.LAN.hemilton	California_GW	3	3-Standard	rule 3
48	18Nov2002	17:45:28	California_GW	web	California.LAN.hemilton	California_GW	3	3-Standard	rule 3
49	18Nov2002	18:35:11	California_GW	smtp	California.LAN.jacobson	oc1.labc-hq.com	10	10-Standard	rule 10
50	18Nov2002	18:35:14	California_GW	smtp	38.12.10.129	38.12.10.129	4	4-Standard	rule 4
51	18Nov2002	18:39:42	Alaska_cluster	http	10.111.254.11	www.ahf.org	12	12-Standard	rule 12
52	20Nov2002	8:10:20	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
53	20Nov2002	8:11:22	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
54	20Nov2002	8:11:30	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
55	20Nov2002	8:12:29	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
56	20Nov2002	8:14:36	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
57	20Nov2002	8:14:38	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
58	30Mar2002	11:14:26	Alaska_cluster	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
59	19Mar2003	1:00:11	Primary_Mana...	ftp	robot.ftps.domain.com	Alaska_DMZ_internal_web	15	15-Standard	rule 15
60	19Mar2003	2:14:36	Alaska_cluster	http	resolved.hosts.com	Alaska_DMZ_internal_web	0	0-Standard	Implied rule
61	19Mar2003	2:19:21	Alaska_cluster	http	Alaska.Fin.Deasel	Alaska_DMZ_internal_web	11	11-Standard	rule 11
62	19Mar2003	10:9:29	Alaska_cluster	http	10.111.254.31	192.168.9.111	12	12-Standard	rule 12
63	19Mar2003	10:9:30	Alaska_cluster	http	10.111.254.31	192.168.9.111	0	0-Standard	Implied rule
64	19Mar2003	10:9:31	Alaska_cluster	http	10.111.254.31	192.168.9.111	0	0-Standard	Implied rule
65	16Mar2003	16:35:31	Alaska_cluster	http	scriptids.inc	Alaska_DMZ_internal_web	14	14-Standard	rule 14
66	16Mar2003	16:35:19	Alaska_cluster	http	scriptids.inc	Alaska_DMZ_internal_web	14	14-Standard	rule 14
67	1Jan2003	22:54:13	Alaska_cluster	http	California.LAN.jacobson	Alaska_cluster	0	0-Standard	Implied rule
68	1Jan2003	22:54:13	Alaska_cluster	http	California.LAN.jacobson	Alaska_cluster	0	0-Standard	Implied rule
69	15Jan2003	22:59:34	California_GW	httpsession	California.LAN.hemilton	Alaska.LAN.Chinella	2	2-Standard	rule 2
70	15Jan2003	22:54:14	California_GW	httpsession	California.LAN.hemilton	Florida.LAN.eucld	2	2-Standard	rule 2
71	29Jan2003	22:53:49	Delaware_clu...	httpsession	California.LAN.hemilton	Alaska.LAN.Chinella	2	2-Standard	rule 2
72	2Feb2003	22:59:35	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
73	2Feb2003	22:54:14	California_GW	http	California.LAN.jacobson	Alaska_cluster	2	2-Standard	rule 2
74	4Feb2003	22:59:35	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
75	12Feb2003	22:54:14	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
76	17Feb2003	22:54:15	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
77	19Mar2003	22:59:36	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
78	19Mar2003	23:23:39	Alaska_cluster	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
79	19Mar2003	23:23:59	Alaska_cluster	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
80	19Mar2003	23:29:21	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
81	19Mar2003	23:24:00	Alaska_cluster	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
82	19Mar2003	23:29:21	California_GW	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
83	19Mar2003	23:29:21	Florida_GW	httpsession	Florida_GW	Alaska_cluster	2	2-Standard	rule 2
84	19Mar2003	23:29:22	California_GW	httpsession	California.DMZ.Lagrange	Alaska.LAN.Chinella	2	2-Standard	rule 2
85	19Mar2003	23:24:01	Alaska_cluster	http	Alaska.Fin.Deasel	Florida.LAN.eucld	2	2-Standard	rule 2
86	19Mar2003	23:24:01	Alaska_cluster	httpsession	Florida.LAN.eucld	Alaska_cluster	2	2-Standard	rule 2

Web IntelligenceのログはSmartCenterで統合が可能です。

Webの保護

悪意のあるコード

- Malicious Code Protector™
- HTTP Worm Catcher (一般的なHTTPワームからの防御)

アプリケーション・レイヤ

- クロス・サイト・スクリプティング攻撃に対する保護
- LDAPインジェクション攻撃に対する保護
- SQLインジェクション攻撃に対する保護
- コマンド・インジェクション攻撃に対する保護
- ディレクトリ横断攻撃に対する保護

情報の公開

- ヘッダ・スプーフィングの実施
- ディレクトリ・リスティングの防止
- エラーの隠蔽

HTTPプロトコルの検査

- HTTPフォーマット・サイズの実施
- ASCII-リクエストのみ実施
- ASCII-レスポンス・ヘッダのみ実施
- ヘッダ拒否の定義
- HTTPメソッドの実施

実施オプション

有効

- ブロックと追跡
- ブロック、追跡、およびHTMLエラー・メッセージの送信

モニタリング専用モード

無効

設定のレベル

個別のサーバをWeb Intelligenceで保護
サーバごとに攻撃に対する保護を有効化
攻撃に対する保護ごとに、個別のサーバに適用するか、すべてのHTTPトラフィックを検査
SmartDefenseのプロファイルは、チェック・ポイントのゲートウェイに個別に関連付けてカスタマイズ可能

保護機能と防御機能のリアルタイム・アップデート

SmartDefense™サービスの加入により対応

ライセンス要件

Web Intelligenceにより保護されるサーバの台数(3台、10台、または無制限)に基づいて、ゲートウェイ単位でWeb Intelligenceのライセンスが必要

システム要件

Web Intelligenceは、関連するチェック・ポイントのゲートウェイと同じシステム要件および設定要件を共有

サポート対象のゲートウェイのバージョン: R55WまたはR60以上
サポート対象の実施ポイント

- FireWall-1®
- VPN-1® Power™
- VPN-1 UTM
- UTM-1
- Connectra™ (購入時にWeb Intelligence機能が導入済み)

Web Intelligenceは、SmartCenter™PowerまたはSmartCenter UTM™による管理が可能

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

Check Point, AlertAdvisor, 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, 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 Protectorm, 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, UTM-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, 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。

P/N 501860-J 2007.08 ※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。



Check Point®

SOFTWARE TECHNOLOGIES LTD.

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