



# Check Point Application Intelligence

# Contents

本書の内容

概要 .....	3
はじめに—アプリケーション層に対する攻撃 .....	4
Application Intelligence 一次世代の脅威に対する防御 .....	4
ネットワーク層とトランスポート層: Application Intelligence の基盤 .....	8
結論 .....	9

## 概要

インターネットが一般的に普及し始めた1994年以来、企業向けファイアウォールは、ネットワーク・レベルおよびトランスポート・レベルのセキュリティ侵害に対して有効に機能してきました。適切にセキュリティ・ポリシーが定義されたファイアウォール — とりわけ最もインテリジェントかつ適応性の高い検査技術であるINSPECT™技術をベースとし、チェック・ポイントが特許を保有するステートフル・インスペクション技術を搭載したファイアウォール — は、この種の攻撃の約9割に対処することが可能です。しかし21世紀に入り、ハッカーの活動は、ネットワーク層やトランスポート層の脆弱性を探し回る程度では済まなくなってきました。高いスキルを備えた今日のハッカーは、主にアプリケーション・レベルで攻撃を行うようになっているのです。例えば、HTTP (TCP 80番ポート) や HTTPS (TCP 443番ポート)、RPC (Remote Procedure Call)、NFS (Network File System) といった重要性の高いサービスが、アプリケーションを不正操作する高度な攻撃の主要ターゲットとなっています。

Application Intelligence™技術を搭載するチェック・ポイントのセキュリティ・ソリューションは、アプリケーション・レベルの攻撃に対する強力な防御機能と遮断機能を備えています。これらの機能により、ネットワーク上の最も重要な資産、すなわちユーザ・データを保護することが可能になります。チェック・ポイントのセキュリティ・ゲートウェイは、Application Intelligence技術と SmartDefense™サービスの組み合わせにより、「標準に適合しているかの妥当性検査」、「プロトコルの利用手順の確認 (プロトコル異常の検出)」、「脅威を与えるデータを運ぶアプリケーションの機能制限」、「アプリケーション層の操作を制御」という4つのメカニズムを用いて攻撃を防御および遮断します。これらのメカニズムによって、VoIP (Voice over Internet Protocol) やインスタント・メッセージ、ピア・ツー・ピア (P2P) ファイル共有、Webサイトでのスクリプト使用、プリンタの共有、FTPによるアップロードといったインターネット・リソース/サービスを安全に利用できるようになります。

また、Application IntelligenceとSmartDefenseサービスは、IPフラグメンテーション攻撃、スマーフ攻撃、非TCPサービス拒否攻撃 (非TCP DoS)、ポート・スキャンなどの攻撃に対する防御機能も備えており、ネットワーク・レベルの攻撃およびトランスポート・レベルの攻撃に対しても、引き続き最高レベルの保護が提供されます。チェック・ポイントのゲートウェイは、真のマルチレイヤ対応セキュリティ・ソリューションとして、急激な進化を遂げるアプリケーション・レベル、ネットワーク・レベル、およびトランスポート・レベルの攻撃に対する、最も包括的で実績のあるセキュリティ機能を提供します。

## はじめに—アプリケーション層に対する攻撃

ファイアウォールは、ネットワーク・セキュリティ・システムの中核として、主にネットワーク・リソースへのアクセスを制御する手段を提供し、ほとんどの大規模ネットワークで大きな成果を上げてきました。ファイアウォールの成功の主な理由は、適切に定義されたセキュリティ・ポリシーを実施するために実施した場合、通常90%以上のネットワーク攻撃をファイアウォールで防ぐことができる点にあります。しかしながら、殆どのファイアウォールが効果的なアクセス制御を提供するにもかかわらず、その多くはアプリケーション層に対する攻撃を検知、防御するようには設計されていません。

この事実を認識して、攻撃者達は企業ファイアウォールで実施されている従来のアクセス制御を回避するように設計した巧妙な攻撃方法を開発しています。今日の経験ある攻撃者は、ファイアウォールのオープン・ポートを探す手法からさらに進歩した、アプリケーション層を直接攻撃するようになって来ています。

今日のインターネット環境で最も深刻な脅威に、アプリケーションの既知の脆弱性に対する攻撃があります。攻撃者が特に注目しているのは、HTTP (TCPポート80) やHTTPS (TCPポート443) などのサービスで、一般的にこれらは多くのネットワークで開かれています。アクセス制御デバイスでは、これらのサービスを狙った悪意のある攻撃を検知するのは容易ではありません。

攻撃者は、アプリケーションを直接ターゲットにして、次のような悪意のある目標のいずれかを達成しようとします。

- 正規ユーザへのサービス拒否 (DoS攻撃)
- サーバまたはクライアントの管理者権限を取得
- バックエンドの情報データベースへのアクセス権限を取得
- セキュリティを回避してアプリケーションへのアクセスを可能にする、“トロイの木馬”のインストール

アプリケーション層に対する攻撃はその性質上巧妙であるため、効果的な防御方法も精巧かつインテリジェントであることが必要とされます。増大するアプリケーション層を利用した攻撃に対処するために、企業ファイアウォールは複数レベルでの包括的セキュリティを提供する必要があります。これらの複数レベルのセキュリティは、ITリソースに対する強固なアクセス制御を提供するかたわら、ネットワーク層ならびにアプリケーション層レベルへの保護も提供しなければなりません。

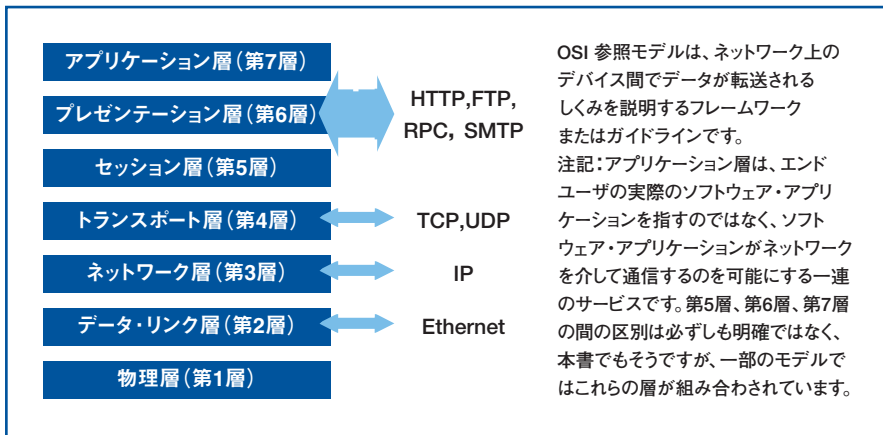
## Application Intelligence—最新の脅威に対する防御

多くのファイアウォール、とりわけチェック・ポイントが特許を保有するステートフル・インスペクション技術が組み込まれたファイアウォールは、ネットワーク攻撃の防衛に成功してきました。この結果、直接ファイアウォールを攻撃対象とするよりも、ネットワーク・アプリケーションの脆弱性につけこむ攻撃の数が増加してきました。このように攻撃手法が大きく変化したため、ファイアウォールはアクセス制御を行ってネットワーク・レベルの攻撃から保護するだけでなく、アプリケーションの振る舞いを理解してアプリケーション層に対する攻撃を阻止する必要があります。業界で最もインテリジェントかつ適応性の高い検査技術であるINSPECT™をベースとするCheckPoint Application Intelligence™は、このような広い視点に基づいたネットワーク・セキュリティ・ソリューションを提供します。

Application Intelligence™ は、  
チェック・ポイント製品  
に統合されている  
一連の高度な機能で、  
アプリケーション層に  
対する攻撃を検知して  
ブロックします。

## Application layer security

### プロトコルの例



### OSI (Open Systems Interconnection) 参照モデル

## アプリケーション層のセキュリティ

アプリケーション層は、いくつかの理由から非常に多くの攻撃を受けます。まず、アプリケーション層には、攻撃者の最終目的である実際のユーザ・データが存在しています。次に、アプリケーション層は多数のプロトコル (HTTP、CIFS、VoIP、SNMP、SMTP、SQL、FTP、DNSなど) をサポートしているため、さまざまな攻撃の対象となるおそれがあります。さらに、この層は他の層に比べて脆弱性が数多く存在するため、アプリケーション層への攻撃の検知と防御は非常に困難です。

Application Intelligenceでは、アプリケーション層におけるセキュリティを完全にするために必要な次の4つの防御戦略に焦点を当てています:

### 1) 標準に適合しているかの妥当性検査

ファイアウォールは通信が適切なプロトコル標準に従っているかどうかを判断する必要があります。標準に沿わない通信は脅威を与えるトラフィックである可能性があります。厳格なプロトコルやアプリケーション標準に従わないトラフィックは、ネットワークへの侵入前に綿密に調べる必要があります。さもなければ、重要なビジネス・アプリケーションが危険にさらされる可能性があります。以下に例を示します。

- **Voice Over IP (VoIP)** — VoIPトラフィックは、通常H.323やSIPなどのプロトコルを使用してサポートされます。これらのプロトコルの動作は複雑になる場合があり、多数の通信ポートによってVoIP通信の確立と維持がサポートされます。これらのプロトコルの処理が不適切な場合、VoIPを使用した結果、次のような危険に曝される恐れがあります。

- 通信のリダイレクション— 指定した受信者宛での通信がリダイレクトされる。
- 通信の盗用— 発信者が別の人物になります。
- DoS— VoIPの正当な使用が妨げられる。

セキュリティ・ゲートウェイは、VoIPコマンドが該当する標準とRFCに完全に準拠し、パケットが構造的に正しく、正しい順番で到着していることを確認する必要があります。さらに、ファイアウォールは許可されているすべてのポートを通過するパケットのコンテンツを検査し、適切な情報が含まれていることを確認する必要があります。

- **HTTPヘッダのバイナリ・データ** — 正式なHTTP標準仕様は、HTTPヘッダへバイナリ・データの組み込みを禁止していますが、この規則は曖昧で、大半のファイアウォールがチェックをしません。その結果、HTTPヘッダに実行可能コードを組み込んで攻撃を開始する攻撃者が大勢います。セキュリティ・ゲートウェイはすべて、HTTPヘッダなしにHTTP要求に含まれるバイナリ・データをブロックするか、フラグを付ける必要があります。

## 2) プロトコルの利用手順の確認

プロトコルを遵守しているかどうかを検査することの重要性に加え、プロトコル内のデータが期待された使用形態であるかを調べることも同様に重要です。すなわち、通信の流れがプロトコル標準に適合していても、プロトコルの使われ方が期待しているものと矛盾している可能性もあるわけです。以下に例を示します。

- **ピア・ツー・ピア (P2P)** — 通信におけるHTTPの利用P2Pは当事者同士が同じ機能を持ち、どちらの当事者も通信セッションを開始できる通信モデルです。P2Pアプリケーションは、主に2種類に分類されます。
  - Instant messaging (IM) — 主な目的は、人々が直接オンライン・コミュニケーションを実施することです。
  - ファイル共有ネットワーク—主な目的は、ストレージなどのリソースを共有することです。

P2P通信では、TCPポート80が頻繁に利用されますが、TCPポート80は通常HTTPトラフィックに使用されるため、内部からの接続に対して開かれています。P2Pに固有のプロトコルが多数あるにも関わらず、P2P通信はHTTPトラフィック内に埋め込まれることがよくあります。このような状況では、プロトコルの準拠のみを調べるファイアウォールは、P2Pセッションを許可してしまいます (セッションに標準HTTPが使用されるため)。一般的に予想されるHTTPの使用法はWebトラフィックに対するものであるため、HTTPトラフィックに埋め込まれたP2P通信はファイアウォールでブロックするか、フラグを付ける必要があります。

セキュリティ、帯域幅、法律上などの理由から、多くの組織がP2Pトラフィックをブロックまたは制限することを希望しています。P2P通信は、ファイアウォール、ウイルス・チェック、ロギング、トラッキングを回避し、ファイル転送、チャット、ゲーム、ボイス、電子メールを許可するように設計されているため、セキュリティ上の問題が生じます。このため、攻撃者はネットワークへの攻撃ベクトルとしてP2Pを使用することがあります。セキュリティ・ゲートウェイは不正なP2Pトラフィックをブロックするか、逆に、認められたP2Pトラフィックを選択的に許可する必要があります。

- **ディレクトリ・トラバーサル** — ディレクトリ・トラバーサル攻撃により、攻撃者は手の届かないところにあるファイルやディレクトリにアクセスすることができるため、アクセス権限のないリソースにアクセスし、好ましくない実行コードをWebサーバで実行する場合があります。これらの攻撃の大半は、ファイル・システム内の“..”表記を利用して行われます。ファイアウォールは、構文に準拠していても予想される使用法と異なるディレクトリ要求がURLに含まれている場合、要求をブロックすべきです。例えば、`http://www.server.com/first/second/../../../../`は、ルート・ディレクトリより深く入り込もうとするものであるため、ブロックする必要があります。
- **長すぎるHTTPヘッダ** — HTTP標準仕様はヘッダの長さを制限していません。しかし、ヘッダが長すぎる場合は、HTTPの通常の使用法や予想される使用法から逸脱しています。長すぎるヘッダは、ブロックするか、フラグを付けてバッファ・オーバーフローの可能性を減らし、オーバーフローを使用して挿入されるコードのサイズを制限する必要があります。

### 3) 脅威を与えるデータを運ぶアプリケーションの機能制限

アプリケーション層の通信がプロトコルを遵守していたとしても、システムに害を与えるデータを持ち込む可能性があります。従って、セキュリティ・ゲートウェイは、アプリケーションが潜在的に危険なデータやコマンドを内部ネットワークに持ち込むことを制限する、あるいは制御する仕組みを持つ必要があります。以下に例を示します。

- クロス・サイト・スクリプティング攻撃** — スクリプトは、アプリケーションに対して攻撃を開始する一般的なメカニズムを提供します。大半のスクリプトは無害ですが、ユーザを疑わずにいると、不正なスクリプトが誤って容易に実行されるおそれがあります。これらのスクリプトは、例えば、電子メール・カードに見せかけるなど、しばしば無害を装ったリンクに隠されている場合があります。
 

良くある不正なスクリプトの例に、クロス・サイト・スクリプティング攻撃 (XSS) があります。クロス・サイト・スクリプティング攻撃は、巧妙に作った URL を使用してユーザと Web サイト間の信頼関係の盲点をつきます。攻撃の目的は、ユーザ ID やクレデンシャルを含むクッキーを盗んだり、クレデンシャルを攻撃者に提供させるようにユーザをだますことです。通常、クロス・サイト・スクリプティング攻撃は、ユーザが信頼しているサイトに無意識に送信する HTTP 要求にスクリプトを埋め込んで開始されます。Web サーバを保護するには、セキュリティ・ゲートウェイが、脅威となるスクリプティング・コードが含まれる HTTP 要求を検知してブロックする必要があります。
- 不正の恐れがある URL を制限またはブロック** — URL に埋め込まれた不正なデータがネットワーク内部に入り込む可能性もあります。例えば、電子メール・クライアントなどのアプリケーションが、HTML が埋め込まれた URL を自動的に実行する場合があります。URL が不正な場合は、ネットワークやユーザ・システムに被害が発生するおそれがあります。不正の可能性のある URL へのアクセスはブロックまたは制限する必要があります。
- 攻撃シグネチャの検知とブロック** — セキュリティ・ゲートウェイは、攻撃やワームなどのデータ・パターンを検知してブロックするために、あらゆるデータ・ストリームに対してコンテンツ・フィルタリングを実行する必要があります。

### 4) アプリケーション層のオペレーション管理

アプリケーション層での通信が、危険なデータをネットワークに持ち込む可能性を持つだけでなく、アプリケーション自身が許可されていないオペレーションを実行する可能性もあります。ネットワーク・セキュリティ・ソリューションには、アクセス制御や正当な使用かどうかのチェックを通じて、このようなオペレーションを認識し制御できる機能が必要です。このレベルのセキュリティにはアプリケーション・オペレーションを細やかに区別できる機能が必要です。以下に例を示します。

- Microsoft Networking Services** — ネットワーク・セキュリティ・ソリューションは、CIFS (Microsoft ベースの Common Internet File System) の多くのパラメータを使用したセキュリティ・ポリシーを実装することができます。CIFS は、ファイル共有およびプリント共有操作の他、さまざまな機能もサポートします。これらの操作を例にとると、セキュリティ・ゲートウェイには、許可されていないユーザやシステムが行うファイル共有操作を識別してブロックする機能が必要です。逆に、同じユーザが行うプリント共有操作は許可および承認してもかまいません。このようにきめ細かなセキュリティ・レベルを提供するには、CIFS を完全に理解し、アプリケーション層のプロトコル・コンポーネントを制御する機能が必要です。
- FTP** — ファイアウォールは、特定のファイル名に接続制限を課し、PUT、GET、SITE、REST、MACB などの危険を伴う可能性のある FTP コマンドを制御する必要があります。例えば、セキュリティ・ポリシーで、“payroll” などの言葉を含むファイルの操作をすべて制限することが必要かもしれません。

## ネットワーク層およびトランスポート層: Application Intelligenceの基盤

Application Intelligenceは、元来、アプリケーション・レベルの防衛に関連付けられています。しかし、実際には、ネットワーク・アプリケーションを標的とする攻撃の多くが、ネットワーク層やトランスポート層をターゲットにします。攻撃者は、アプリケーション層にアクセスする手段としてこれらの下位層をターゲットにし、最終的にはアプリケーションやデータ自体を標的にします。また、下位層をターゲットにすることにより、正当なユーザやアプリケーションへのサービスを中断または拒否することができます (DoS攻撃)。このような理由により、Application Intelligenceなどのネットワーク・セキュリティ・ソリューションは、アプリケーション層だけでなく、ネットワーク層やトランスポート層にも対処する必要があります。

### ネットワーク層のセキュリティ

ネットワーク層のプロトコル (IP、ICMPなど) の悪用を防ぐことは、マルチレベル・セキュリティ・ゲートウェイに欠くことのできない要件です。ネットワーク層への攻撃で最もよく使われる手法は、インターネット・プロトコル (IP) で、そのサービス・セットがネットワーク層にあります。ネットワーク層にひそむ危険や攻撃は多数存在しますが、以下にいくつか例を示します。

- **IPフラグメンテーション**—検知を回避するために、IPフラグメンテーションを使って攻撃を加えたり、攻撃を偽装することができます。この攻撃方法は、IPプロトコル自体 (RFC791およびRFC815) に内在する耐障害メカニズムを利用し、攻撃を意図的に複数のIPパケットに断片化して、IPフラグメントの再構築を行わないファイアウォールを回避します。IPフラグメンテーションは、IPフラグメント再構築デバイスを不完全なフラグメント・シーケンスで溢れさせて、DoS攻撃を開始するために使用することもできます。
- **スマーフィング (スマーフ攻撃)**—ICMPにより、あるネットワーク・ノードから他のネットワーク・ノードにpingすること、すなわちエコー要求を送信することで、動作確認を行うことができます。この機能を利用して、“スマーフ” DoS攻撃が行われます。スマーフ攻撃が可能なのは、標準のICMPが要求と応答を照合しないためです。このため、攻撃者は偽のソースIPアドレスを使って、IPブロードキャスト・アドレスにpingを送信することができます。IPブロードキャスト・アドレスは、指定されたネットワーク内のすべてのIPアドレスにパケットを到達させます。pingを受信したネットワーク内のマシンはすべて、攻撃対象にされた罪のないIPソースにエコー応答を送信します。大量のpingと応答により、攻撃対象となったネットワークが渋滞し、正当なトラフィックによるアクセスが拒否される場合があります。このタイプの攻撃は、チェック・ポイントのStateful ICMPが実行するように、要求と一致しない応答を落としてブロックすることができます。

### トランスポート層のセキュリティ

ネットワーク層と同じように、トランスポート層およびこの層で一般に使用されるプロトコル (TCP、UDP) は、アプリケーションやデータに対する攻撃で頻繁に利用されるアクセス・ポイントになります。以下に、トランスポート層に対する攻撃と脅威の例を示します。

- **非TCP DoS**—非TCP (UDP、ICMPなど) DoS攻撃は、TCPトラフィックを使用する重要なアプリケーション (SMTP、HTTP、FTPなど) を完全に渋滞させることができます。ファイアウォールは、TCP接続のステート・テーブルの専用範囲を予約してこれらの脅威から保護することができます。非TCP接続がリソースを過剰に利用しようとした場合、TCP接続は予約されたシステム・リソース、または専用のシステム・リソースで処理されるため、影響を受けません。
- **ポート・スキャン**—ポート・スキャンはその名のとおりに、攻撃者がターゲット・ホストの一連のポートをスキャンし、実行中のアプリケーションの脆弱性をつきとめることです。ポート・スキャンによる偵察は、攻撃につながるおそれのある危険な行為です。セキュリティ・ゲートウェイには、警告を発生し、スキャン元からの通信をブロックまたは遮断する機能が必要です。

## 結論

ファイアウォールは、ネットワークに対する攻撃をブロックする機能により、ネットワーク・セキュリティ・インフラストラクチャの主要製品としての地位を確立しました。ファイアウォールが成功をおさめた結果、攻撃者はさらに高度な攻撃手法を考案しました。新しいタイプの攻撃は、直接アプリケーションをターゲットとして、アプリケーション自体や通信プロトコルに内在する脆弱性を狙うものです。これらの脅威から企業ネットワークを守るためには、複数レベルにわたりセキュリティを提供する必要があります。また、複数レベルを対象とするセキュリティ・ソリューションは、ITリソースへのアクセスを制御する一方、ネットワーク攻撃とアプリケーション層への攻撃の両方を防御しなければなりません。

Check Point Application Intelligenceは、チェック・ポイント製品に統合されている一連の高度な機能で、アプリケーション・レベルへの攻撃を検知して防御します。チェック・ポイントのソリューションは、ますます増加しつつある重要なアプリケーションに向けられた攻撃に、業界で最も定評のある包括的な答えを提供します。

## 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、世界中の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティおよびVPN市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・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。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

### 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

E-mail : info\_jp@checkpoint.com

Tel : 03 (5367) 2500

<http://www.checkpoint.co.jp/>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, 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, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityのlogo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, 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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, 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。

Check Point Application Intelligence

P/N:500936-J\* 2008.02

※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。

