



Stateful Inspection Technology

ステートフル・インスペクション技術

Contents

本書の内容

セキュリティの必要条件	3
ステートフル・インスペクション技術	3
拡張可能な、チェック・ポイントのステートフル・インスペクション	4
INSPECTエンジン	4
INSPECT仮想マシン	4
ステートフル・インスペクションと従来のファイアウォール・アーキテクチャとの比較	6
パケット・フィルタ	6
アプリケーション・ゲートウェイ	6
ステートフル・インスペクション	7
広範なプロトコルおよびアプリケーションのサポート	8
UDP等のコネクションレス・プロトコルのサポート	8
RPC等のポートが動的に割り当てられる接続のサポート	9
パフォーマンス	9

セキュリティの必要条件

強固なセキュリティを確保するためには、ファイアウォールを通過する通信のフローを監視・制御する必要があります。TCP/IPベースのサービスに対する制御上の判断（通信の接続要求を許可、拒否、認証、暗号化、ログ記録するかどうかといった判断）を下すためには、ファイアウォールは、すべての通信レイヤおよびアプリケーションから導き出される情報を取得、保存、検索、および操作する必要があります。

この際、パケットを個別に調査するだけでは不十分です。新しい通信の接続要求に対する制御上の判断を下すにあたっては、過去の通信およびアプリケーションから導き出される状態情報が必要不可欠な要素となります。接続要求の種類によっては、通信状態（過去の通信から導き出される）とアプリケーション状態（アプリケーションから導き出される）の両方が、制御上の判断を下すうえで重要になる場合もあります。

したがって、最高レベルのセキュリティを実現するためには、ファイアウォールで次のことが可能でなければなりません。

- 通信情報の取得と分析
パケット内の全7層から情報を取得し、分析する必要があります。
- 通信から導き出される状態の取得と分析
過去の通信から導き出される状態を取得し、分析する必要があります。例えば、FTPセッションの外向きPORTコマンドを保存しておくことにより、内向きのFTPデータ接続をそのコマンドと照合できるようになります。
- アプリケーションから導き出される状態の取得と分析
他のアプリケーションから導き出される状態情報を取得し、分析する必要があります。例えば、一度認証を受けたユーザに対しては、許可されたサービスについてのみファイアウォールを介したアクセスを許可するといったことが可能になります。
- 情報の操作
パケットの任意部分のデータに対して、論理演算または算術演算を実行する必要があります。

ステートフル・インスペクション技術

チェック・ポイント・ソフトウェア・テクノロジーズが開発したStateful Inspection™（ステートフル・インスペクション）は、企業向けネットワーク・セキュリティ・ソリューションの業界標準として広く利用されています。ステートフル・インスペクションは上記のセキュリティ要件をすべて満たしますが、パケット・フィルタやアプリケーション・ゲートウェイ等の従来からあるファイアウォール技術では、いくつかの領域においてセキュリティ要件を満たすことができません（P5：表1を参照）。

ステートフル・インスペクションでは、パフォーマンスを向上させるため、パケット・フィルタと同様にネットワーク層でパケットを捕捉しますが、その後すべての通信レイヤから導き出されたデータを分析することにより、セキュリティを向上させています（アプリケーション・ゲートウェイでは第4層～7層が対象）。さらに、通信およびアプリケーションから導き出された状態情報と、動的に保存および更新されるコンテキスト情報を取り入れることによって、より高いレベルのセキュリティを実現します。こうして蓄積されたデータは、それ以降の通信における接続要求を評価する際に利用されます。またステートフル・インスペクションでは、RPCやUDPに代表されるコネクションレス・プロトコル等を追跡するための仮想セッション情報を作成することも可能です。これは、ステートフル・インスペクション以外のファイアウォール技術では実現できないチェック・ポイント独自の機能です。

拡張可能な、チェック・ポイントのステートフル・インスペクション

チェック・ポイントのFireWall-1およびFireWall-1が統合されているVPN-1、UTM-1、UTM-1 Edgeなどチェック・ポイントのゲートウェイ・セキュリティ製品が実装するステートフル・インスペクション・アーキテクチャでは、チェック・ポイントが独自に開発した、特許取得済みのINSPECTエンジンを採用しています。INSPECTエンジンは、ゲートウェイ上で動作し、セキュリティ・ポリシーが実施されます。INSPECTエンジンは、すべての通信層を監視し、適切なデータだけを抽出することにより、極めて効率的なオペレーション、広範なプロトコルおよびアプリケーションのサポート、さらには新しいアプリケーションおよびサービスにも容易に対応可能な拡張性を実現します。

INSPECTエンジンは、チェック・ポイントの強力なINSPECT言語を使用してプログラミングすることが可能で、システムにとって重要な拡張性を高いレベルで実現しています。これにより、チェック・ポイント社のみならず技術パートナー各社やエンド・ユーザは、ソフトウェアを新たにロードすることなく、新しい脅威や新しいアプリケーション、サービス、およびプロトコルに対応することが可能になります。

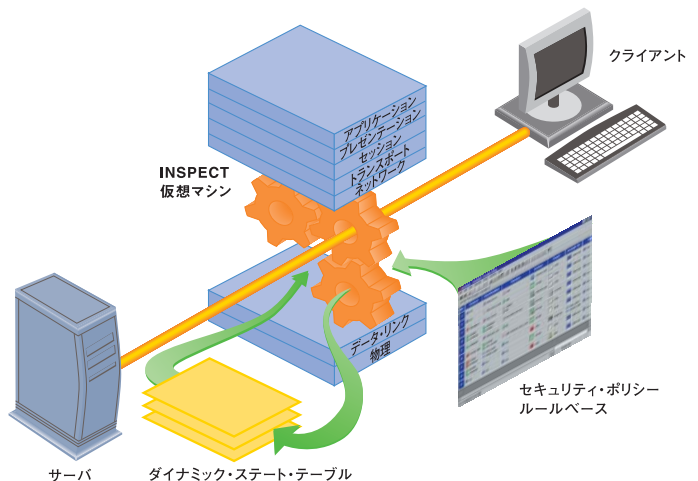
INSPECT™ エンジン

チェック・ポイント ステートフル・インスペクションのINSPECTエンジンは、ゲートウェイにインストールされた場合、ネットワーク間を通過するトラフィックを制御します。INSPECTエンジンは、オペレーティング・システム・カーネルのデータ・リンク層とネットワーク層（第2層と第3層）の間に動的にロードされます。データ・リンク層は物理的なネットワーク・インタフェース・カード（NIC）であり、ネットワーク層はIPなどのプロトコル・スタックの第1層なので、ステートフル・インスペクションは、ソフトウェア層の最下位層に位置することになります。チェック・ポイントのステートフル・インスペクションでは、INSPECTエンジンでこの層を検査することにより、すべてのインタフェース上のすべての着信/発信パケットを捕捉および検査することが可能になります。パケットがどのような通信プロトコルやアプリケーション・プロトコルを使用するものであっても、そのパケットがセキュリティ・ポリシーに適合するものであるとINSPECTエンジンが最初に判断しない限り、いかなるパケットもプロトコル・スタックの上位層で処理されることはありません。

INSPECT仮想マシン

チェック・ポイントのセキュリティ・ゲートウェイ製品に搭載された特許取得済みのINSPECT仮想マシンは、通信がゲートウェイ・マシンのオペレーティング・システムに到達する前にそれらすべてを捕捉・分析・対処することで、ネットワークの完全なセキュリティと保全性を実現します。

INSPECT仮想マシンは、通信状態およびアプリケーション状態から得られた累積データ、ネットワーク構成情報、およびセキュリティ・ルールを使用して、エンタープライズ・セキュリティ・ポリシーを実施します。



ファイアウォールの機能	パケット・フィルタ	アプリケーション・ゲートウェイ	ステートフル・インスペクション
通信情報	一部	一部	あり
通信から導き出される状態	なし	一部	あり
アプリケーションから導き出される状態	なし	あり	あり
情報の操作	一部	あり	あり

表1：ファイアウォール技術の比較

INSPECTエンジンは「生のメッセージ」にアクセスするため、メッセージ内のすべての情報を検査できます。例えば、上位のすべての通信層に関係する情報や、メッセージ・データ自体（通信およびアプリケーションから導き出された状態情報とコンテキスト情報）も検査できます。INSPECTエンジンは、パケットを受理するかどうかを判断するために、定義されているセキュリティ・ポリシーに従ってIPアドレスやポート番号などの必要な情報を検査します。

チェック・ポイント ステートフル・インスペクションのINSPECTエンジンは、IPプロトコル・ファミリの内部構造や、その上に構築されたアプリケーションを認識できます。UDPやRPCといったステートレス・プロトコルに対しては、コンテキスト・データを生成・保存することにより、UDP通信の上に仮想接続を保持します。INSPECTエンジンは、パケットのアプリケーション・コンテンツからデータを抽出し、それを記録しておくことで、アプリケーションがコンテキストを提供しない場合にそのデータを使用できます。さらには、必要に応じて接続を動的に許可・不許可とすることができます。このような動的な機能は、複雑なプロトコルに対して最高レベルのセキュリティを適用するために用意されていますが、不要な場合にはユーザ側で無効にすることもできます。

このように、INSPECTエンジンはパケットの内部を見ることができ、アプリケーション内の一部のコマンドだけを許可し、それ以外のコマンドを拒否することができます。例えば、ICMPのpingを許可する一方でリダイレクトは拒否する、あるいはSNMPのgetを許可する一方でsetは拒否する、といったことが可能です。またINSPECTエンジンは、値をテーブル形式で保存・検索したり（これにより動的なコンテキストが与えられます）、パケットの任意部分のデータに対して論理演算や算術演算を実行したりできます。この際、セキュリティ・ポリシーからコンパイルされた演算を使用する他に、ユーザが独自の演算式を作成することもできます。

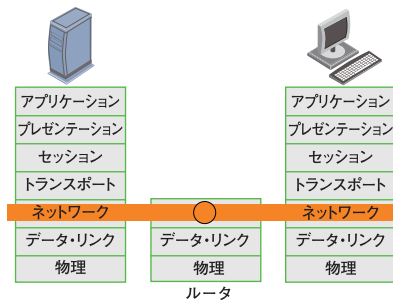
他社のセキュリティ・ソリューションとは異なり、チェック・ポイントのステートフル・インスペクション・アーキテクチャでは、通信がゲートウェイ・マシンのオペレーティング・システムに到達する前にそれらすべてを捕捉・分析・対処することで、ネットワークの完全なセキュリティと保全性を実現します。通信状態およびアプリケーション状態から得られた累積データ、ネットワーク構成情報、およびセキュリティ・ルールを使用して適切なアクションを生成し、その通信を許可、拒否、認証、または暗号化します。デフォルトでは、セキュリティ・ルールによって明示的に許可されなかったトラフィックはすべて破棄されます。また、セキュリティ・アラートとログはリアルタイムに生成され、システム管理者に完全なネットワーク・ステータス情報を提供します。

ステートフル・インスペクションと他のファイアウォール技術との比較

FTPを例とした各ファイアウォール技術の差

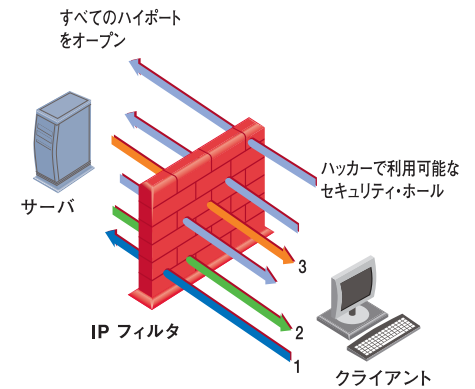
パケット・フィルタ

パケット・フィルタは通常ルータ上に実装され、ユーザ定義のコンテンツ(IPアドレスなど)をフィルタリングします。ネットワーク層でパケットを検査し、アプリケーションに依存しないため、高いパフォーマンスとスケーラビリティを実現できます。ただし、パケット・フィルタはアプリケーションを認識できず、通信のコンテキストを理解することができないため、ハッカーによる侵入に対してそれほど強固とは言えません。ファイアウォールとしては最も安全性が低いタイプです。



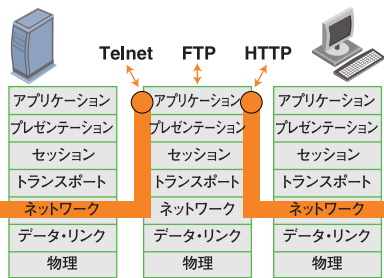
- | | |
|--|--|
| 長所 | 短所 |
| <ul style="list-style-type: none"> ●アプリケーションに非依存 ●パフォーマンスが高い ●スケーラビリティが高い | <ul style="list-style-type: none"> ●セキュリティが低い ●ネットワーク層より上位の層を検査できない(状態情報やアプリケーションのコンテキスト情報を取得できない) |

パケット・フィルタでは、発信FTP接続に関して2つの選択肢があります。1つは、ポートの上位範囲全体(1024以上)をオープンにするというもので、この場合、ファイル転送セッションは動的に割り当てられたポートで実行できます(ただし、内部ネットワークを外部に公開してしまいます)。もう1つは、ポートの上位範囲全体を閉じて内部ネットワークを保護するというもので、この場合、他のサービスもブロックされます。このような、アプリケーションのサポートをとるかセキュリティをとるかといった二者択一的な考え方は、今日のユーザには受け入れられません。



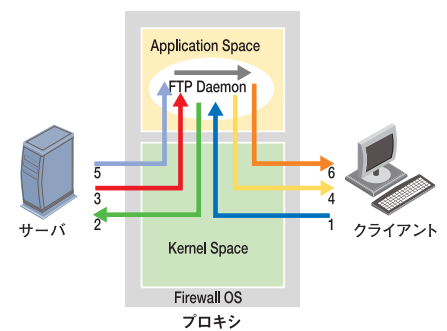
アプリケーション・ゲートウェイ

アプリケーション・ゲートウェイでは、すべてのアプリケーション層を調べ、コンテキスト情報に基づいてパケットの処理方法を判断することでセキュリティを向上させます。ただしこれは、クライアント/サーバ・モデルからは逸脱する結果となります。アプリケーション・ゲートウェイでは、すべてのクライアント/サーバ通信において、クライアントからファイアウォールへの通信、ファイアウォールからサーバへの通信という2つの接続が必要になるためです。また、プロキシごとに別々のアプリケーション・プロセス(デーモン)が必要になるため、スケーラビリティや新しいアプリケーションのサポートという部分に難点があります。



- | | |
|--|--|
| 長所 | 短所 |
| <ul style="list-style-type: none"> ●セキュリティが高い ●アプリケーション層を完全に認識 | <ul style="list-style-type: none"> ●パフォーマンスが低い ●アプリケーションのサポートに制限がある ●スケーラビリティが低い(クライアント/サーバ・モデルを逸脱する) |

アプリケーション・ゲートウェイは、FTPプロキシを使用する際、セッション数を二重にしてクライアントとサーバ間の仲介役を務めます。このアプローチでは、アプリケーション層を認識したうえでパケットの処理方法を判断することによりIPフィルタリングの制限を克服していますが、このために許容できないほどのパフォーマンス低下を招く場合があります。さらに、サービスごとに専用のプロキシが必要となるため、使用可能なサービスの数とスケーラビリティは制限されます。また、このアプローチではオペレーティング・システムが外部の脅威にさらされることになります。

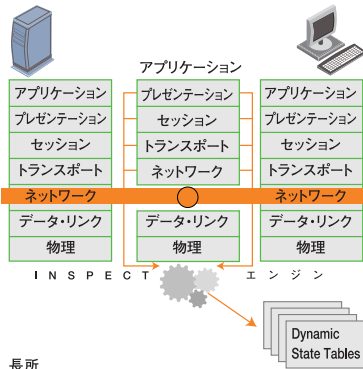


FTPを例とした各ファイアウォール技術の差

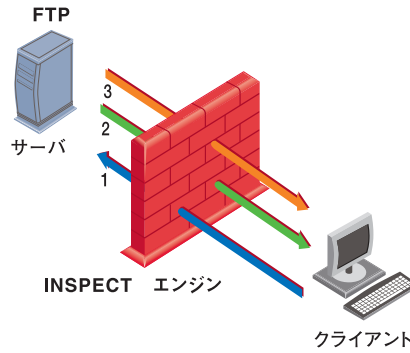
ステートフル・インスペクション

チェック・ポイントのステートフル・インスペクションは、クライアント/サーバ・モデルを逸脱することなくアプリケーション層を完全に認識できるようにすることで、上記2つのアプローチの制限を克服しています。ステートフル・インスペクションでは、パケットはネットワーク層で捕捉されますが、その後の処理はINSPECTエンジンが引き受けます。INSPECTエンジンは、セキュリティ上の判断を下すのに必要な状態情報をすべてのアプリケーション層から抽出し、この情報を動的なステート・テーブルで管理して、それ以降の接続要求の評価に使用します。これにより、高度なセキュリティと、最高レベルのパフォーマンス、スケーラビリティ、および拡張性を提供するソリューションが実現されます。

チェック・ポイントのステートフル・インスペクションは、FTPセッションを追跡してFTPアプリケーション層のデータを検査します。クライアントがサーバに対して逆接続 (FTPのPORTコマンド) を生成するように要求すると、ステートフル・インスペクションは、このリクエストからポート番号を抽出します。このとき、クライアントおよびサーバのIPアドレスとポート番号がFTPデータ保留リクエスト・リストに記録されます。FTPのデータ接続が要求されると、ステートフル・インスペクションは、このリストを調べ、それが有効なリクエストに対する応答であるかどうかを確認します。接続のリストは動的に管理されるので、必要なFTPポートだけがオープンされます。このセッションがクローズされると、これらのポートは直ちにロックされるため、セキュリティは最大限保たれます。



- 長所
- セキュリティが高い
 - アプリケーション層を完全に認識
 - パフォーマンスが高い
 - 拡張性・透過性
 - 動的なステート・テーブル



広範なプロトコルおよびアプリケーションのサポート

チェック・ポイントのステートフル・インスペクションは、業界で最も多くのアプリケーション、サービス、およびプロトコルをサポートしており、その数は数百にもおよびます。主要なインターネット・サービスはすべてサポートされており、例えば、WebブラウザによるHTTPS通信、従来型のインターネット・アプリケーション（電子メール、FTP、Telnetなど）、TCPファミリ全体、コネクションレス・プロトコル（RPCやUDPベースのアプリケーション）がサポートされます。さらに、データベース・アクセスを提供するOracle SQL*Netなどの重要なビジネス・アプリケーションや、各種マルチメディア・アプリケーションおよびSIP、H.323、MGCPなどのVoice over IPアプリケーションもサポートされます。その他、インスタント・メッセージやPeer-to-Peerアプリケーションの利用に対する細やかな制御も可能です。また、次世代のIPプロトコルであるIPv6もサポートされています。

以降の各項、および4～5ページの図で、チェック・ポイントのステートフル・インスペクションで独自にサポートされる複雑なプロトコルについて説明します。

UDP等のコネクションレス・プロトコルのサポート

UDPベースのアプリケーション（DNS、WAIS、Archieなど）を、単純なパケット・フィルタ方式でフィルタリングすることは困難です。というのも、UDPではリクエストと応答は区別されないためです。従来、UDPベースのアプリケーションに対する選択肢としては、UDPセッションを全面的に排除するか、双方向通信を行うUDPパケットの大半を許可し、その結果として内部ネットワークを外部に公開してしまうかのいずれかしかなかった。

チェック・ポイントのステートフル・インスペクションは、UDP通信の上に仮想接続を保持することによって、UDPベースのアプリケーションにセキュリティを適用します。チェック・ポイントのINSPECTエンジンは、ゲートウェイを通過する各セッションの状態情報を保持します。ファイアウォールを通過することを許可された各UDPリクエスト・パケットは記録され、逆方向に流れるUDPパケットはそれらが承認されたコンテキストにあるかどうかを確認するために保留セッションのリストと照合されます。リクエストに対する正規の応答であるパケットは目的地に配送され、それ以外のパケットはすべて破棄されます。応答が指定時間内に到着しない場合、その接続はタイムアウトされます。こうした仕組みにより、攻撃はすべてブロックする一方で、UDPアプリケーションを安全に利用することが可能になります。

アプリケーション				
プレゼンテーション				
セッション				
トランスポート		TCP		UDP
ネットワーク			IP	
データ・リンク				
物理	Ethernet	FDDI	x.25	その他

TCP/IPサービスとOSI参照モデルのマッピング

RPC等のポートが動的に割り当てられる接続のサポート

RPC (リモート・プロシージャ・コール) については、単純にポート番号を追跡するという方法では対応できません。RPCベースのサービスは既定のポート番号を使用しないからです。ポートの割り当ては動的に行われ、多くの場合、時間の経過と共に変化します。チェック・ポイント ステートフル・インスペクションのINSPECTエンジンは、システムのポート・マップを使って動的かつ透過的にRPCポート番号を追跡します。INSPECTエンジンは最初のポート・マップ・リクエストを追跡し、RPCプログラム番号をその関連ポート番号とサーバにマッピングするキャッシュを保持します。INSPECTエンジンは、RPCベースのサービスに関係しているルールを調べるたびにこのキャッシュを参照し、パケット内のポート番号とキャッシュ内のポート番号を比較して、そのポートに割り当てられているプログラム番号がルールで指定されたものであるかどうかを確認します。パケット内のポート番号がキャッシュに存在しない場合—これは、アプリケーションが既知のポート番号を使用し、最初にポート・マップ・リクエストを発行せずに通信を開始したときに発生することがあります—INSPECTエンジンは自らポート・マップにリクエストを発行し、ポートに割り当てられているプログラム番号を確認します。

パフォーマンス

チェック・ポイント ステートフル・インスペクションのINSPECTエンジンは、シンプルかつ効率的な設計により、最高レベルのパフォーマンスを実現しています。

- オペレーティング・システムのカーネル内で動作するため、処理時のオーバーヘッドはほとんど発生しません。コンテキスト・スイッチングは不要で、遅延時間の短縮化を実現しています。
- キャッシングやハッシュ・テーブルといった先進のメモリ管理技術の採用により、複数のオブジェクト・インスタンスの統合、および効率的なデータ・アクセスを可能にします。
- シンプルで汎用的なインスペクション・メカニズムとパケット・インスペクション・オブティマイザとの組み合わせにより、最新のCPUとOS設計を最大限活用することができます。

チェック・ポイント ステートフル・インスペクションがネットワーク・パフォーマンスに与える影響はごくわずかであり、また、先進のアクセラレーション技術により、数Gbpsから数十Gbpsのパフォーマンスを実現します。さらに、チェック・ポイントのステートフル・インスペクションは多様なプラットフォームをサポートしているため、厳しくなる一方の企業ネットワーク要件に合わせてセキュリティ・インフラストラクチャを拡張していくことが可能です。

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 (<http://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、変化し続けるお客様のビジネス・ニーズに応じてカスタマイズ可能なトータル・セキュリティ・ソリューション群を提供しています。統合されたゲートウェイ、単一エージェントによるエンドポイント、および単一の管理アーキテクチャで構成されるこのトータル・セキュリティ・ソリューション群の組み合わせは、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/エンドポイント・セキュリティ、データ・セキュリティ、およびVPN市場におけるリーダーシップと技術革新に基づく独自性を備えています。チェック・ポイントは、情報セキュリティの分野のみに注力するセキュリティの専門企業です。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を保護する、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。また、業界をリードするエンドポイント/データ・セキュリティ・ソリューションである Check Point Endpoint Security 製品ラインナップを通じ、PC やモバイル端末に保存されてい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 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。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。

©2003-2008 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 Cl, 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 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 Cl, 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。

Stateful Inspection Technology

P/N:501798*-J 2008.5

※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

Tel: 03(5367)2500

E-mail: info_jp@checkpoint.com

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