



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

# エンドポイント・ポリシーの実施

確実な企業のトータル・アクセス・プロテクション



Intelligent Security

チェック・ポイントはネットワークのあらゆる環境——境界、内部、Web——に対する確実なセキュリティ保護と、情報リソースの安全性、接続性、管理性を兼ね備えたソリューションを提供します。

# Contents

本書の内容

---

はじめに .....	3
現実的な解決策 .....	4
リモート・アクセス・セキュリティの協調施行(Cooperative Enforcement) .....	4
LANアクセス・セキュリティの実施 .....	5
ゲスト・エンドポイントによるリモート・アクセスの制御 .....	6
協調施行(Cooperative Enforcement)の利点 .....	7
ネットワーク・アクセス・ポリシー実施の展望 .....	8
確実な企業のトータル・アクセス・プロテクション .....	8

## はじめに

理論的な情報セキュリティと実際の情報セキュリティの違いは、ここ数年ではつきりしてきました。データとネットワークの保護のため、また業務の継続と評判のため、企業が信頼してきた一般的なセキュリティ技術は、もはや約束した通りの防御機能を提供できなくなっています。このため、実効性を失う原因となった要因に対応する新しいアプローチが求められています。

- これまで、セキュリティ管理者は、境界ファイアウォールが適切に構成されていれば、企業のネットワークに対する外部からの攻撃にフィルタをかけることができると期待できました。しかし、従業員とゲストのリモート・アクセス、インスタント・メッセージ、ポート80トラフィックや、他の通信形態が存在する今日、効果的な境界セキュリティを達成することがより困難になっています。
- 数年前は、ウィルスから企業を保護するため、一般的にアンチウィルス製品の使用が効果的でした。セキュリティの脆弱性を突いた攻撃の件数が少なく、大流行までに数日または数週間かかっていました。IT部門には準備時間が十分にあり、企業内の多くのPCに感染したり、ネットワーク・パフォーマンスが低下したりする前に、最新のウィルス・シグネチャを導入することができました。  
ところが、最新のワームやウィルスはインターネット上のあらゆる脆弱なホストにあつという間に感染してしまいます。社内のすべてのデスクトップとモバイル・コンピュータで、アンチウィルスのシグネチャが更新される前に、何百万のシステムを攻撃し、企業のネットワークをダウンさせることが可能です。
- 毎週、アプリケーションとオペレーティング・システムの新たな脆弱性が見つかったら、パッチによる対応では効果的な事前保護ができなくなっています。  
正しいパッチのサブセットを適用し、安定性と互換性をテストして、内部およびリモートのコンピュータに配備するという手順は、ハッカーが新たに発見された脆弱性を利用して攻撃するより長い時間を要します。
- 多くの企業では、大量のネットワーク侵入検知システム（IDS）のアラートと「誤検知」のアラームを分析するために必要な技術レベルを持つスタッフが不足しています。  
何百または何千のネットワーク・コンピュータまたは「エンドポイント」からのIDSのログを収集しても、問題を増幅させるばかりです。最も重要なことは、IDSのリアクティブ（事後対処型）技術では、今日の驚異的な速度の攻撃によるダメージを防ぐことができないということです。
- エンドポイント・ファイアウォールとアンチウィルス製品は、今日の巧妙な攻撃の対象となっています。これらの必須防御も、ハッカーによって無効にされた場合、効果を発揮することはできません。エンド・ユーザもまた、デスクトップ・セキュリティ技術を無効にする方法がわかれば、企業のセキュリティ・ポリシーによる制限を回避することができます。
- ネットワーク・ゲスト（受託業者、ビジネス・パートナー、顧客、ホームPCを使用する従業員など）は、通常定期的に企業のWebベースのアプリケーションやポータルへのリモート・アクセス権を付与されます。ITおよびセキュリティの管理者は、これらゲストのエンドポイントのセキュリティ状態をほとんど制御することができません。その結果、感染したゲストPCが、ネットワークの感染または情報の漏えいの原因と特定されることも少なくありません。

データとネットワークの保護のため、また業務の継続と評判のため、企業が信頼してきた一般的なセキュリティ技術は、もはや約束した通りの防御機能を提供できなくなっています。

## 現実的な解決策

セキュリティ・インフラストラクチャの実効性を回復するには、企業リスクの新たな現状に対する解決策が必要です。新たな脆弱性を突いた攻撃、いわゆるゼロ攻撃を最小限に抑えるには、ネットワーク接続されたコンピュータをリアクティブではなくプロアクティブに防御するソリューションが不可欠です。シグネチャまたはヒューリスティックが更新されるのを待つのではなく、デフォルトまたは最小の設定で、脆弱性に対する脅威と攻撃を直ちに阻止できなければなりません。また、エンドポイントが適切に保護されていないために、企業のネットワークを攻撃に晒すようなことも防がなければなりません。このためには、ITセキュリティ・ポリシーに定義されており、ネットワークに接続するすべてのコンピュータが安全な状態であると保障できなければなりません。このポリシーは、LAN接続を許可する前に、すべてのエンドポイントでホスト・ベースのファイアウォールと最新のシグネチャを備えたアンチウィルスを実行するよう強制できます。ネットワーク・アクセスの前に、重要なWindowsパッチと更新されたVPNクライアントのインストールを強制することもあります。ハッカーまたはエンド・ユーザによって改ざんまたは無効にされるのを防ぐため、ソリューションはある程度強化されていなければなりません。最後に、これも重要ですが、ネットワークの製品やオペレーティングス・システムの違いに関わらず、企業ネットワーク環境全体で、ネットワーク・アクセスを保護しなければなりません。これらすべての条件を満たすソリューションがあれば、MS-Blaster、Welchia/Nachi、SoBig.F、MyDoom、Sasser、Netsky、Wittyやその他の最近の攻撃による甚大な被害から無数の組織を守ることができなくなります。

Integrity™は、まさにそのような解決策です。現在最も信頼できる防御により、ネットワーク接続されたPCを守ります。ネットワークにアクセスするすべてのPC（従業員およびゲスト、リモートおよび内部、有線または無線）で確実にポリシーを順守することで、Integrityは企業のトータル・アクセス・プロテクションを実現します。Cooperative Enforcement™技術により、Integrityを数百のネットワーク・ゲートウェイ製品（VPNからスイッチや無線アクセス・ポイントまで）と統合し、ポリシー順守違反のPCを隔離し、ネットワーク・リソースへのアクセスを許可する前に、ポリシーを順守させることができます。このソリューションにより、企業がネットワーク・インフラに使用する製品のメーカーや種類に関係なく、IPベースのすべてのネットワーク環境でポリシーの順守を確実にします。また、Integrityのトータル・クライアント・ロックダウン（Total Client Lockdown）機能は、ユーザまたは攻撃者がエンドポイント・セキュリティを無効にしたり、ネットワーク・アクセス・ポリシーの実施を停止したりするのを防止します。包括的で確実なセキュリティの実現と全社的なポリシーの順守により、Integrityは他のセキュリティやネットワーク・アクセス製品をすり抜けた脅威も撃退することができます。

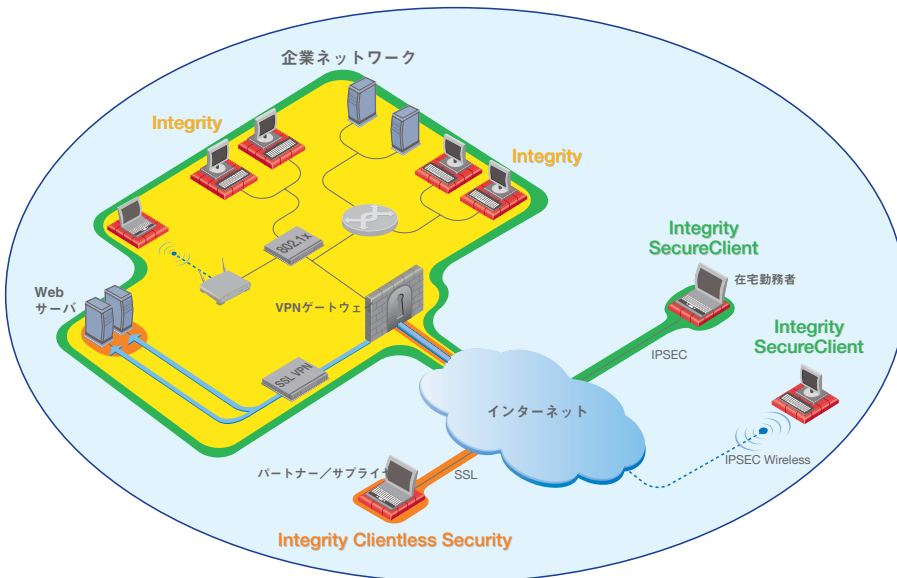
## リモート・アクセス・セキュリティの協調施行（Cooperative Enforcement）

安全なリモート・アクセスが、協調施行（Cooperative Enforcement）の最終目標です。チェック・ポイントのZone Lab部門は、業界をリードするすべてのVPNおよびリモート接続ベンダと連携し、ネットワーク・アクセス権を付与されたすべてのPCの安全性を確保するため、各社のIPSec製品とSSL製品およびサービスをIntegrityに統合しました。

これらの協調施行（Cooperative Enforcement）インテグレーションでは、PCに企業ネットワークへのアクセス権を与える前、およびリモート・アクセス・セッションの間、リモートPCでIntegrityクライアントが実行されていなければなりません。また、PCのセキュリティ状態をチェックし、ネットワーク・アクセス権を与える前に、広範なセキュリティ・ポリシー要素への順守を強制します。Integrityは、エンドポイントに適切なベンダの最新のアンチウィルスを実行することを義務付けることができます。特定のサービス・パックまたはソフトウェア・パッチがインストールされていること、特定のプロセスが実行されている／いないこと、特定のレジストリ・キーがある／ないことを義務付けることができます。

必要なポリシーに対して何らかの順守違反のあるPCを使用するエンド・ユーザは、企業ネットワークへのアクセスを拒否されます。代わりに、それらのユーザは自動サービス修正リソースを提供するサーバにリダイレクトされます。エンド・ユーザがセキュリティ・ポリシーに順守するためのステップを実行すると、Integrityとネットワーク・ゲートウェイは、ユーザに付与されていたアクセス権を自動的に回復します。Integrityをネットワーク・ゲートウェイに統合することで、ネットワークにアクセスするすべてのPCの安全性を確保し、統合されていないアプローチによって企業ポリシーが実施される危険性を排除します。

#### チェック・ポイントのエンドポイントセキュリティ・ソリューション – トータル・アクセス・プロテクション



トータル・アクセス・プロテクションにより、企業はネットワークに接続するPCを、場所、所有者、接続方法にかかわらず、すべて保護することができます。

#### LANアクセス・セキュリティの実施

協調施行 (Cooperative Enforcement) の次のフェーズには2つの目標がありました。1つ目は、個々の製品との統合から、普及しているオープン・スタンダードをベースにした統合に発展させることでした。2つ目の目標は、ポリシーの実施を境界線の内側から有線および無線LANにまで拡張することでした。多くの製品によってサポートされるIEEE 802.1X規格の一部である Extensible Authentication Protocol (EAP) に対する革新的なサポートにより、チェック・ポイントのZone Labs部門はどちらの目標も達成できました。IntegrityおよびCisco、Nortel、Microsoftの製品、その他の先進のエンタープライズ・スイッチ、ルータ、および無線アクセス・ポイント・ベンダは、EAPベースの統合をサポートしています。その結果、Integrityは、カスタム設定をほとんど必要とせず、有線および無線LAN接続の協調施行 (Cooperative Enforcement) を実現できます。802.1X仕様をサポートする他社製品と統合することにより、チェック・ポイントは、協調施行 (Cooperative Enforcement) で、実質的に、企業が使用するどのネットワーク・ベンダの機器とも連携できるようになります。

Integrityは、VPNゲートウェイとの連携と同様の方法で、内部でEAPを使用するゲートウェイと連携してセキュリティ・ポリシーを実施します。Integrityは各エンドポイントのセキュリティ状態をチェックし、各ポリシー要素を順守しているか評価し、その結果をEAPを使用するスイッチ、ルータ、または無線アクセス・ポイントに伝えます。ゲートウェイはIntegrityによってポリシーを順守していると評価されたエンドポイントにLANへのアクセス権を与え、順守していない場合は隔離します。エンドポイントがポリシーを順守する状態に戻ったと判断すると、Integrityはゲートウェイにそれを伝え、エンドポイントのLANへのアクセス権を回復します。

ネットワーク・ゲートウェイと直接統合することにより、企業のポリシーが常時、確実に実施されるようにします。企業ネットワークが完全に802.1Xに対応していない場合、Integrityは、ゲートウェイを統合せずに、独自に包括的なポリシー順守を実行することができます。これは、順守違反を検出した場合に、ユーザのアクセスを一部のネットワーク・リソースに限定するエンドポイント・ファイアウォール・ルールを適用することで実現できます。協調施行 (Cooperative Enforcement) と同じように、Integrity単独の実施でも修正リソースを提供し、ユーザをすばやく簡単に順守状態に戻すことができます。ユーザのエンドポイントがポリシー順守状態に戻ったら、Integrityはユーザの通常のネットワーク・アクセス権限を自動回復します。このスタンドアロン構成では、Integrityクライアントがエンドポイントで実行されていることを確認するゲートウェイがありません。Integrityのトータル・クライアント・ロックダウン (Total Client Lockdown) 機能により、管理者がインストールしたすべてのIntegrityクライアントが常時稼働し、エンドポイント・セキュリティとポリシー順守の両方が確実に実施されるようになります。

包括的な、トータル・アクセス・プロテクションを提供するエンド・ツー・エンドの協調施行 (Cooperative Enforcement) を実現するため、Integrityは、チェック・ポイントの境界、内部およびWebセキュリティ製品のフル・ラインナップを統合します。例えば、Integrityとチェック・ポイントの内部セキュリティ・ゲートウェイであるInterSpect™を連携させて、LAN上の他のPCと通信を行う前に、すべての内部PCの安全を確保します。InterSpectは、ネットワークをセキュリティ・ゾーンにセグメント化し、ダウンしたデバイスを隔離することにより、新しいワームおよび攻撃がLAN全体に蔓延するのを阻止します。Integrityはまた、VPN-1hとの統合をベースに、境界セキュリティ・ポリシーの協調施行 (Cooperative Enforcement) を実現します。

## ゲスト・エンドポイントによるリモート・アクセスの制御

最近まで、エンドポイント・ポリシーの実施のためには、PCにクライアント・ソフトウェアをインストールする必要がありました。クライアント・ベースのセキュリティは、脆弱なエンドポイントに対して最も包括的な防御を提供しますが、ほとんどの場合、企業が自社のネットワークにアクセスするゲストのコンピュータにクライアント・ソフトウェアをインストールすることは不可能です。ビジネス・パートナー、顧客、ホームPCを使用する従業員などのネットワーク・ゲストは、次々に企業のWebベースのアプリケーションやポータルへの接続を許可されます。ネットワーク・ゲストのPCがキーストローク・ロガーやその他のスパイウェアに感染している場合、保護されていない企業資産で発生するのと同じセキュリティ侵害が発生することになります。ゲストPCのアンチウィルスが最新でないか、重要なパッチをインストールしていない、またはその他のエンドポイントのセキュリティ条件を満たしていない場合、感染や機密性違反を引き起こすことにもなります。

Integrity Clientless Securityは、このようなセキュリティ・ホールをふさぐために開発されました。この製品はIT管理者によってクライアント・ソフトウェアをインストールする必要がないので、企業はネットワーク・アクセス保護を制御範囲外だったユーザにも広げることができます。外部ユーザが保護されたWebポータルまたはアプリケーション (企業のWebメール、電子商取引システム、またはSSLVPNゲートウェイなど) のログイン・ページを表示すると、Integrity Clientless Securityブラウザ・プラグインが外部ユーザのPCをスキャンして、キーストローク・ロガー、スパイウェアや、その他の望ましくないプログラムがないかチェックします。何らかのスパイウェア・プロセスを検出すると、Integrity Clientless Securityは直ちにそれらを無効にします。ユーザが他の検出されたソフトウェアを削除するまで、管理者はWebポータルまたはアプリケーションへのアクセスを拒否することもできます。ユーザがログインIDとパスワードを入力する前にキーストローク・ロガーを無効にして、機密データや重要なネットワーク・リソースへの不正アクセスを可能にするクレデンシャルを、侵入者に奪取されることを防ぎます。

スパイウェアを無効にして削除するほか、企業はIntegrity Clientless Securityを使用して、クライアント・ベースのバージョンのIntegrityで実施されるのと同様のネットワーク・アクセス・ルールを実施することができます。クライアントレス・ソリューションは、ゲストにログイン画面へのアクセスを許可する前に、最新のアンチウイルス、パッチ、アプリケーション、レジストリ・キー、その他の条件を満たすように要求できます。また、管理者はユーザに修正リソースを提供するように設定できます。これにより、ユーザは簡単にエンドポイントをセキュリティ・ポリシーに順守させることができます。Integrity Clientless SecurityおよびConnectra™、チェック・ポイントのWeb セキュリティ・ゲートウェイの組み合わせで、企業のWebリソースを脅威から守る包括的な防御機能を提供します。

IT管理者の管理下のないエンドポイントにも、企業所有のエンドポイントと同様のセキュリティ・ポリシーを実施する機能を追加することで、チェック・ポイントは、企業が、今日の実世界の脅威から自らを守るために必要なトータル・アクセス・プロテクションを実現しました。

## 協調施行 (Cooperative Enforcement) の利点

### トータル・アクセス・プロテクション

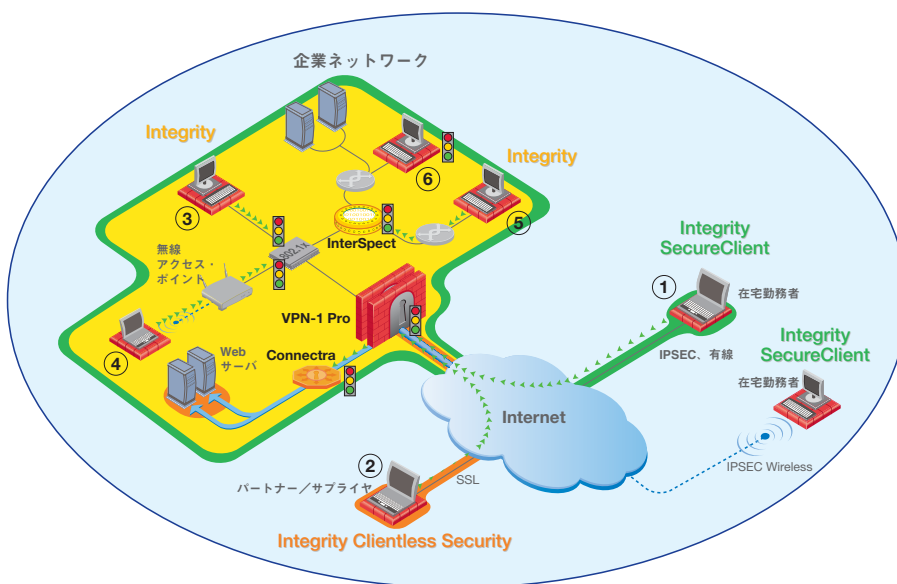
業界初のトータル・アクセス・プロテクションは、企業ネットワークに接続するすべてのPC（従業員およびゲスト、内部およびリモート、有線または無線）にまで、エンドポイント・セキュリティを拡張します。業界をリードするセキュリティを提供し、すべてのエンドポイントでポリシー順守を実施することにより、トータル・アクセス・プロテクションは、ワーム、スパイウェア、その他の脅威が、ビジネスの継続およびデータの機密性に与えるリスクを大幅に軽減します。

### 広範なゲートウェイとの統合

Integrityは、業界をリードする20社以上のネットワーク・ゲートウェイと連携することにより、包括的なエンドポイント・ポリシーの順守を確実にします。Cooperative Enforcement技術により、Integrityは一般的なVPNおよび200種以上のスイッチ、ルータ、無線アクセス・ポイントを介してエンドポイントのセキュリティ状態を検証し、ネットワーク・アクセスを制御することができます。Integrityは、広範な環境におけるネットワーク・アクセスを保護するため、多くの製品に採用されている802.1x規格の主要コンポーネントである（非商標の）Extensible Authentication Protocol (EAP) をサポートした最初の製品です。Integrityは、また、チェック・ポイントの境界、内部およびWebセキュリティ・ソリューションのフル・ラインナップとシームレスに統合します。

### トータル・クライアント・ロックダウン (Total Client Lockdown)

セキュリティ・クライアント・ソフトウェアが改ざんされたり、無効にされると、すべてのネットワーク・アクセス制御が失われます。旧式の内部ゲートウェイが順守違反のエンドポイントを隔離できない環境では、管理者はセキュリティ・クライアントが独自にポリシーを順守することに頼るしかありません。Integrityに組み込まれた高度な自己防御メカニズムは、攻撃者またはエンド・ユーザによって改ざんあるいは無効にされないことを保証します。このため、Integrityは使用しているゲートウェイに関係なく、事実上どのような環境でもネットワーク・アクセスを保護することができます。



- ① VPNリモート・アクセス・ポリシーの実施
- ② Webリモート・アクセス・ポリシーの実施
- ③ 802.1X準拠ゲートウェイによる内部ポリシーの実施
- ④ 802.1X準拠ゲートウェイによる不正アクセスの防止
- ⑤ InterSpectによる内部ポリシーの実施
- ⑥ スタンドアロンでの実施

▶▶▶ 協調施行 (Cooperative Enforcement)  
▶▶▶ スタンドアロンでの実施

### ネットワーク・アクセス・ポリシー実施の展望

企業の通信チャネルと常時接続コンピュータの急増により、ビジネス機会が増加すると同時に、セキュリティ・リスクも増大します。チェック・ポイントには、脅威の進化よりも、企業が常に1歩先を行くための、プロアクティブ（事前予防型）なセキュリティの革新を図った豊富な実績があります。先を展望し、チェック・ポイントは、企業のコンピュータ・リソースに接続するホストの安全と企業ポリシーの順守を保証することに全力を注いでいます。これを、ユーザ、さまざまな種類のデバイス、プラットフォームおよびネットワーク環境に展開することができます。柔軟性に欠ける（単一ベンダのネットワーク装置やオペレーティング・システムをサポートするような）既存のネットワーク・アクセス制御のアプローチでは、顧客の利益となるよりも、むしろ、メーカーの利益となっています。802.1Xのような業界標準を独自に実装する場合にも同様の思惑があるのです。多くの企業は、業界標準の実装によってベンダの制約を受けたり、TCO（総所有コスト）を上昇させたりすることは避けようとしています。

チェック・ポイントは、あらゆる環境でオープンかつ包括的なポリシーの実施を実現するとともに、エンドポイント・セキュリティ・ソリューションの導入と管理に掛かる管理者の負担を最小限に抑えるよう取り組んでいます。標準ベースの技術と管理しやすさから、エンドポイント・セキュリティとITインフラ全般のTCOを可能な限り低く抑えることができます。このようなセキュリティと財務上の利点を提供することで、チェック・ポイントは、企業に常に最善のエンドポイント防御を提供し続けることをお約束します。

## Check Point Software Technologies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 (www.checkpoint.com) はインターネット・セキュリティにおける世界トップ企業として、特に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、およびVPNの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Next Generation製品ラインナップを通じ、インテリジェント性を兼ね備えた境界、内部、およびWeb環境に対するセキュリティ・ソリューションを提供し、エンタープライズ・ネットワークをはじめ、アプリケーション、エンドポイント、支店・支社環境、更にはパートナー各社のエクストラネットなどに対する包括的なセキュリティ保護を実現します。

チェック・ポイントの一部門である Zone Labs(www.zonelabs.com) は、インターネット・セキュリティの分野で高い信頼性を誇るブランドとして数々の賞に輝くエンドポイント・セキュリティ・ソリューションを提供し、世界中で何百万台ものコンピュータをハッカーやスパイウェア、データの盗難などから守っています。

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最高の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・ポイントは世界88ヶ国、2200社を超えるパートナー・ネットワークを通じてソリューションの販売、導入、サービス提供を行っています。

©2004-2005 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd.およびその関連会社の商標、サービス・マーク又は登録商標です。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および6,496,935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 501691-J 2005.05 ※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.

**We Secure the Internet.**

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 建成ビル6F  
http://www.checkpoint.co.jp/ E-mail : info@checkpoint.co.jp Tel : 03(5367)2500