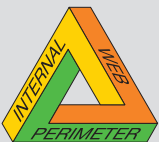


## Best-of-BreedのOPSEC製品による セキュリティ・インフラストラクチャの構築

### 本書の内容

- 1 セキュリティ上の課題を解決するソリューションの導入
- 2 包括的なセキュリティ・ソリューションの構築
- 3 統合セキュリティ管理のフレームワーク
- 4 OPSEC統合ポイント
- 5 チェック・ポイントのOPSECフレームワークの利点



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

## Best-of-BreedのOPSEC製品によるセキュリティ・インフラストラクチャの構築

### セキュリティ上の課題を解決するソリューションの導入

企業は、ビジネス上の重要なデータへのリアルタイムアクセスを求める顧客やサプライヤにインターネットを介して社内ネットワークを解放するという課題に直面しています。しかし、セキュリティの設定を適切に行わなければ、ネットワークのあらゆる部分がハッカーやライバル企業、時には社員の不正な活動の対象となるおそれがあります。従来、セキュリティ上の脅威は、一箇所で制御を行う製品で簡単に追跡し、阻止することができましたが、近年、セキュリティ上の脅威は複雑さを増し、ウイルス、ハッキング、サービス拒否を組み合わせたものになりました。CodeRedやNimdaのような最近の脅威は、短時間でネットワーク全体に広がり、何千億円もの損害を与える場合があります。これら攻撃を組み合わせたものが引き起こす脅威を1つの製品やベンダ1社で根絶することは不可能です。企業は以下のようなセキュリティ上のゴールを効果的に達成するために、複数のセキュリティ製品を導入する必要があります。

- ・内外の攻撃や脅威からネットワークを守る
- ・攻撃や侵入にリアルタイムで対処する
- ・エクストラネットによりパートナーにネットワークやアプリケーションへの選択的なアクセス権を供与する
- ・すべてのセキュリティ・アプリケーションに単一のセキュリティ・ポリシーを配布する
- ・セキュリティを緩めずにパフォーマンス、信頼性、アベイラビリティを確保する
- ・ネットワーク全体に対する包括的なセキュリティ・ポリシーを集中管理する

### 包括的なセキュリティ・ソリューションの構築

#### ファイアウォール— 防衛の第一線

ネットワーク・セキュリティは、ネットワークの境界を保護することから始まります。ファイアウォールは、企業のネットワークやセキュリティの強化を要するサブネットのゲートウェイにインストールします。チェック・ポイントのVPN-1®/FireWall-1®は、主にアクセス制御デバイスとして動作するマルチレイヤ・セキュリティ・アーキテクチャの最初のレイヤです。FireWall-1は、ステートフル・インスペクション技術( [http://www.checkpoint.com/products/downloads/Stateful\\_Inspection.pdf](http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf)を参照)を使用して、トラフィックを検査し、アクセスを許可するかどうかについて高度な判断を行います。ファイアウォールがネットワーク・トラフィックを許可すると、次のレベルの保護を担当する他のセキュリティ・アプリケーションが起動されます。

#### 侵入検知システム

侵入検知システム(IDS)は、ファイアウォールのセキュリティ・ポリシーで許可されたプロトコルの脆弱性を悪用する攻撃から企業を守るために使用します。企業を守るには、ネットワーク型IDSとホスト型IDSという複数レイヤのIDSが必要です。侵入検知システムは、ネットワークを通過するすべてのパケットのコンテンツを検査し、シグネチャ・ベースまたはアノマリ・ベースで攻撃を検知し、ファイアウォールに通知します。ファイアウォールは、即座に不正なトラフィックをブロックし、今後の攻撃から防御するポリシーを再設定します。

#### アンチウイルスおよびコンテンツ・セキュリティ

ウイルスは、システムに感染後急速に増殖するため、最もよく知られている脅威です。Code RedやNimdaなどの最近の脅威から守るために、複数のセキュリティ技術を組み合わせせたセキュリティ対策が必要になってきました。ファイアウォールにより、様々な種類のコンテンツを許可/拒否するポリシーを適用できますが、コンテンツを検査してコンテンツ・セキュリティ・ポリシーを適用するには別のセキュリティ対策が必要です。アンチウイルス製品のベンダは、自社製品をファイアウォールと統合し、企業ネットワークに侵入を試みるあらゆるコンテンツをスキャンし、問題のないコンテンツのみネットワークに入ることを許可します。これにより、一箇所の実施ポイントでネットワーク・インフラストラクチャ上の全てのプラットフォームとレイヤを保護します。



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

企業は、アンチウイルス技術の対象外である電子メールやインターネットの使用に関わるコンテンツ・セキュリティの脅威にさらされています。URLフィルタリングやインスタント・メッセージング・フィルタリングなどのコンテンツ・セキュリティ・システムは、不適切または制限されているコンテンツが組織内に入るのを防ぎます。アンチスパム・ソリューションは、不要な電子メールが電子メール・システムに滞留し、帯域幅やストレージ・リソースを浪費するのを防止します。アンチウイルス製品と同様に、他のコンテンツ・セキュリティ製品は、ファイアウォールに統合されて、好ましくないコンテンツをゲートウェイでブロックします。

### 認証と承認

企業は、インターネットを使用してモバイル社員、ビジネス・パートナー、サプライヤおよび顧客にリソースへの選択的アクセス権を提供します。認証は、ID管理に関するものですが、ユーザやパートナー、アプリケーション、取引を識別する固有の方法は多数あります。堅牢なセキュリティ・インフラストラクチャが構築されていれば、適切なリソースに適切な認証を実行でき、さらに、承認により、ポリシーに基づいてアプリケーション・リソースに対して選択的なアクセス許可を与えることができます。これらのアプリケーションをファイアウォールに統合すると、各リソースにアクセスするたびに認証を行う必要がなくなります。

### レポートと監視

監査ログは、ネットワークに導入されているすべてのセキュリティ・アプリケーションによって生成されます。これらのログは、ネットワークへのアクセスと認証、使用プロトコルと異常フラグ、および企業ネットワークへの不正な侵入の試みなどを追跡します。ログ・データは、セキュリティ・ポリシーの検証と微調整、セキュリティ・インフラストラクチャの健全性の監視にも利用します。ファイアウォールへ統合することにより、ログ・ファイルを一元的に表示し、イベント発生時にインテリジェントな警告を発生し、エスカレーションされるように設定することができます。

### パフォーマンスとアベイラビリティ

ネットワーク・パケットは、目的地に到達するまでに複数のセキュリティ・レイヤを通過する必要があります。ネットワーク・トラフィックが増加し、高度な侵入をブロックするためにファイアウォールでパケットを詳細に検査する必要があると、システム全体のパフォーマンスが低下するおそれがあります。生産性の向上とアップタイムの最大化を実現するには、パフォーマンス向上技術とハイ・アベイラビリティ・システムが必要です。

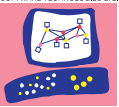
上記のように、企業は包括的なセキュリティ・ソリューションを実現するために、複数のセキュリティ製品を導入する必要があります。企業が装備すべき機能には次のようなものがあります。

- ・ 最高品質の製品群 – セキュリティ全分野にわたり1社で最高のソリューションを継続的に提供するのは極めて困難
- ・ 単一ポリシー・フレームワーク – 瞬時に何千ものネットワーク、システム、アプリケーション、ユーザに対しポリシーを簡単に反映
- ・ 集中管理 – 包括的なソリューションには複数のセキュリティ・ベンダのコンポーネントが含まれる可能性が大
- ・ 業界標準プロトコルのサポート – シームレスな統合と相互運用性を実現

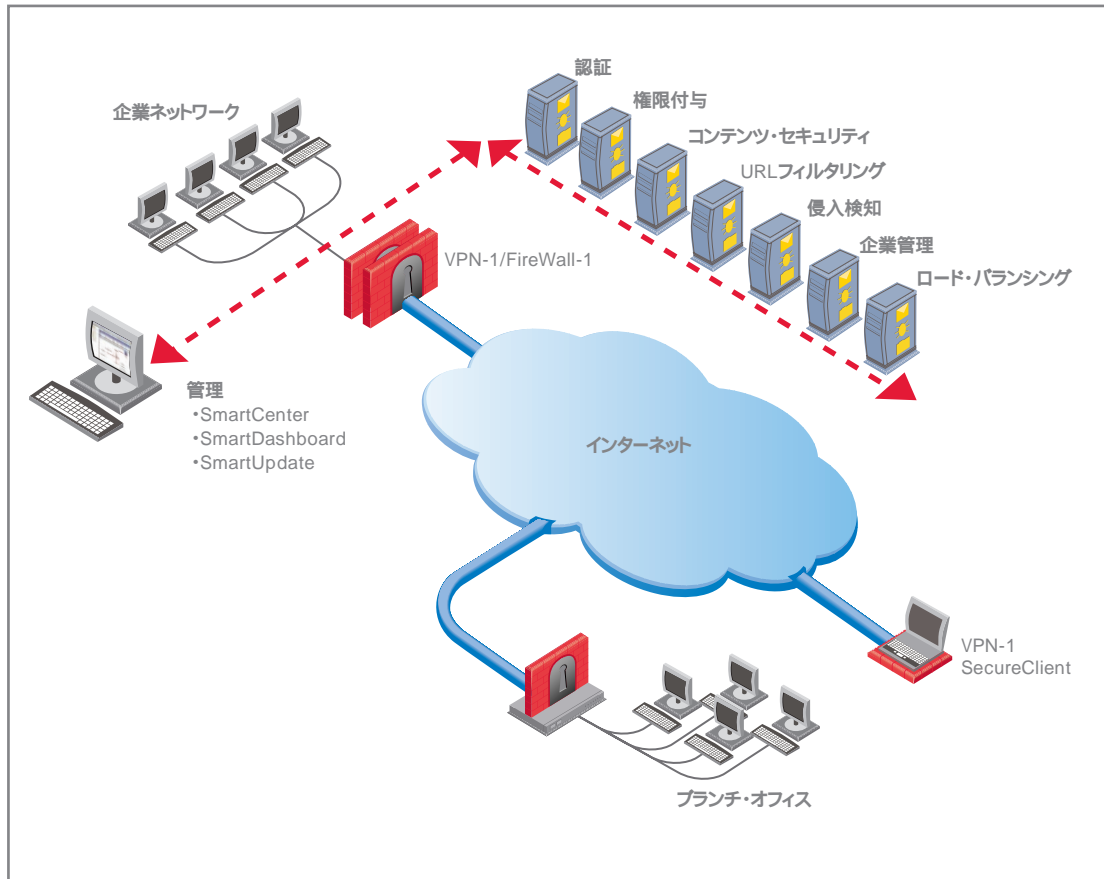
### 統合セキュリティ管理のフレームワーク

1997年にチェック・ポイント社は、相互運用性を可能にする業界全体のオープン・フレームワークとして、セキュリティ・アプリケーションおよびアプライアンス・ベンダ向けにOPSEC( Open Platform for Security )アライアンス・プログラムを設立しました。以来、このプログラムのインタフェースは、業界の他のどのセキュリティ・プラットフォームよりも多くのベンダに使用され、事実上のデファクト・スタンダードになりました。OPSECの広範囲な統合インタフェースは、インターネット・セキュリティ・アーキテクチャのあらゆる分野に対応しています。OPSECフレームワークには、350社のベンダが参加し、175以上の認定製品があるため、顧客は最良のインターネット・セキュリティ・アプリケーションと導入プラットフォームを最も幅広い製品群の中から選択することができます。これらの製品はすべて、1つの統合ネットワーク・セキュリティ・インフラストラクチャとして集中管理および相互運用可能なことが保証されています。OPSECソリューションは、Linux、IPSO、Solaris、Windows、HP-UX、AIXなど、業界をリードする25以上のハードウェア・ベンダによって提供される様々なオペレーション・システムで使用できます。



Check Point  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



## OPSEC統合ポイント

OPSECは、複数のサードパーティ製品をCheck Point VPN-1/FireWall-1と統合するOPSEC Software Development Kit (SDK)により、単一の統合フレームワークを提供します。SDKは、業界標準プロトコルやCheck Pointが提供する独自のAPI (Application Programming Interface) を含む20以上の実績のあるインタフェースを提供します。

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に統合されるサードパーティのセキュリティ製品は、統合テストを行い、テストに合格した場合には、シームレスな相互運用性を保証する"OPSEC認定"を取得します。企業は、"OPSEC認定"を取得したセキュリティ製品を使用することにより、セキュリティ・インフラストラクチャ全体を再構成することなく、新しいセキュリティ技術を最大限に利用し、個々のコンポーネントをアップグレードすることができます。

ハードウェアの認定プログラム、"Secured by Check Point"プログラムにより、チェック・ポイントのセキュリティ・ソリューションは、消費者から小規模オフィス、企業、サービス・プロバイダまであらゆるマーケット・セグメントで使用されている広範囲のハードウェア・アプライアンス・プラットフォーム上で展開されます。

以下のAPIは、コード・サンプルとともに、OPSEC Software Development Kit (SDK)に含まれているため、チェック・ポイントのインフラストラクチャと自社製品の統合を希望するベンダや組織はこれを利用できます。



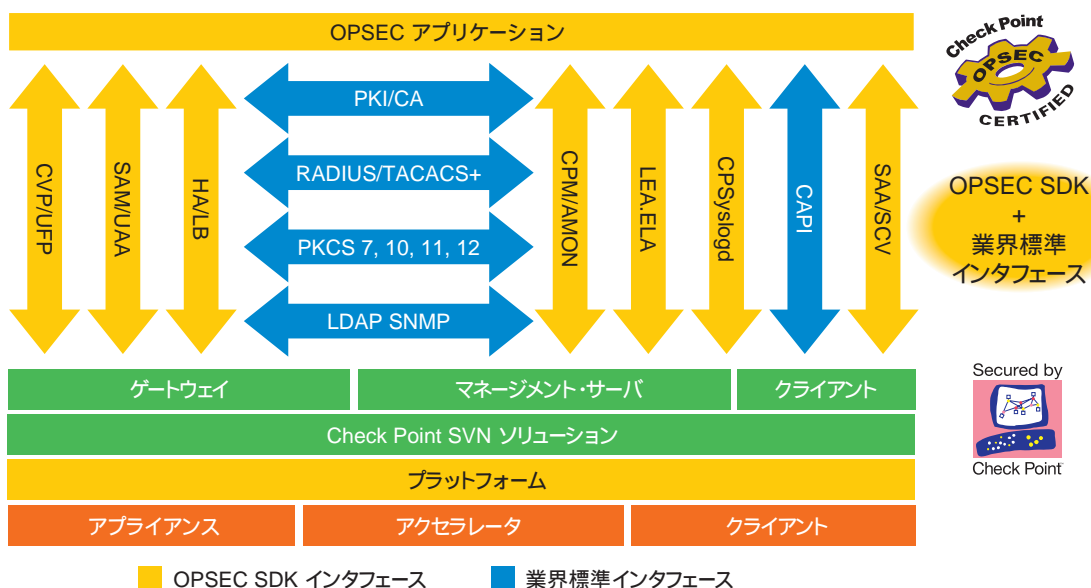
Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

OPSEC APIは包括的で、業界標準プロトコルを利用しています。

OPSEC SDK  
+  
業界標準  
インタフェース

Secured by



Check Point

次の表は、一部のOPSEC APIの概要を示しています。

API名	説明	機能	使用アプリケーション
CVP	Content Vectoring Protocol	メッセージおよびファイルまたはアプレットのアタッチメントのコンテンツ検証とチェックに使用	コンテンツの検査
UFP	URL Filtering Protocol	外部Webサイトへのアクセス制御の実施に使用	URLフィルタリング製品
SAM	Suspicious Activity Monitoring	ファイアウォール・ゲートウェイを動的に再設定可能にするためにサード・パーティ製アプリケーションが使用	IDS
UAA	User Authority API	アプリケーション間でユーザのシングル・サインオン認証に使用	SSO
CPMI	Check Point Management Interface	チェック・ポイントの集中管理用オブジェクト・リポジトリとのインタフェースに使用	すべてのアプリケーション





API名	説明	機能	使用アプリケーション
AMON	Application Monitoring	チェック・ポイントおよびサード・パーティ製アプリケーションの監視に使用	すべてのアプリケーション
LEA	Log Export API	外部アプリケーションがリアルタイムと履歴ログ情報を取得するために使用	すべてのアプリケーション
ELA	Event Logging API	外部アプリケーションがチェック・ポイントのログ・データベースにイベントを記録するために使用	すべてのアプリケーション
SAA	Secure Authentication API	認証デバイスおよびソフトウェアをVPNクライアントに統合するために使用	認証製品
SCV	Secure Configuration Verification	デスクトップ設定をエンタープライズFW/VPNに統合するために使用	リモート・アクセス

## チェック・ポイントのOPSECフレームワークの利点

### 包括的なセキュリティ

チェック・ポイントのOPSECセキュリティ・フレームワークには、最良のセキュリティ・パートナーが含まれ、すべてのセキュリティ・アプリケーションに一元化された整合性のあるセキュリティが実施されます。企業は、非常に多くのOPSEC認定アプリケーションから選択することにより、すべてのコンポーネントで最適な連携が保証されている単一の包括的なセキュリティ・インフラストラクチャを導入することができます。カテゴリ別のパートナーと認定ソリューションの一覧については、<http://www.opsec.com/solutions/index.html>をご覧ください。

### 集中管理

管理をシンプルで簡単なものにするために、OPSECフレームワークでは、チェック・ポイントのSMART™ 管理コンソールから直接、統合されたマルチベンダ・セキュリティ管理を行います。SmartCenterファミリに属するチェック・ポイントのSmart OPSEC Managerは、管理維持機能、すなわち"OPSEC認定"アプリケーションのポリシー管理、セキュリティ・プロビジョニング、インシデント管理を一元化してTCO (Total Cost of Ownership) を大幅に削減します。

### ポリシー管理

ネットワークには非常に多くのデバイスとセキュリティ製品があるため、セキュリティ・ポリシーを中央で作成、管理し、複数のネットワーク・ポイントで実施することが重要です。ポリシーの実施を自動化することにより、人間が介在することによって生じるエラーを大幅に減少させることができます。

今日では、チェック・ポイントのSmartCenterを使用して、OPSEC認定製品すべてに対するセキュリティ・ポリシー全体を管理することができます。チェック・ポイントの集中管理アーキテクチャにより、SmartCenterから直接起動できるベンダ固有のツールを利用しながら、マルチベンダ・アプリケーションの動作とパラメータを単一のコンソールから管理することができます。



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

このネットワーク・セキュリティ管理モデルは、企業での最適なセキュリティの確立を支援し、セキュリティ問題の発生リスクを著しく低下させます。このオープン・アプローチは、整合性のある単一の管理コンソールおよび統合されたパラメータや管理機能を提供する一方、各ベンダ独自の機能とツールを100パーセント活かします。

### セキュリティ・プロビジョニング

セキュリティ・アプリケーションは、すばやく、シームレスに展開する必要があります。新規アプリケーションは、展開時に自動的に構成され、既存インフラストラクチャとのプラグ・アンド・プレイ機能を備えていなければなりません。

今日、管理者はSmartCenter™を使用して、チェック・ポイントの簡単な"One-Click"技術により、複数の"OPSEC認定"セキュリティ・アプリケーションをすばやくネットワークに統合することができます。"OPSEC認定"されたアプリケーションは、手動で構成する必要がなく、セキュリティ・インフラストラクチャとのプラグ・アンド・プレイが可能です。

セキュリティ・プロビジョニングにより、企業は時間をかけずに、エラーの少ない一元化された効率の良い展開を行うことができます。

### インシデント管理

攻撃の特定、侵入の隔離、脅威へのすばやい対処、再発の防止は、すべての企業とは言わないまでも、大多数の企業にとって大きな課題です。

現在、チェック・ポイントのSmartCenterは、"OPSEC認定"セキュリティ・アプリケーションおよびネットワーク・デバイスからイベント・ログをインポートして統合し、外部管理システムにエクスポートします。将来、セキュリティ管理者は、自動的にイベントを相関させて、リアルタイムで自動応答させることができるようになるでしょう。

統合されたセキュリティ・ログを表示して分析できれば、侵入への対処が容易になり、異常なアクティビティが発見された場合、ポリシーと対処方法をリアルタイムにすばやく実施ポイントへ伝達することができます。

### パフォーマンスとアベイラビリティ

ゲートウェイ・セキュリティ製品としてのファイアウォールは、ほとんどの企業にマルチギガビットのスループットを提供できなければなりません。パブリック・ネットワークから入ってくるすべてのパケットを検査する必要があるため、ファイアウォールのダウンタイムは厳禁です。チェック・ポイントのNext Generation™ ( NG )SecureXL™アーキテクチャにより、チェック・ポイントとOPSECパートナーは、マルチ・ギガビットのスループットと99.999%のアベイラビリティを持つシームレスな接続を提供します。ネットワーク・デバイスとアプリケーションが生成するログ・ファイルは、チェック・ポイントの管理コンソールにインポートして、パフォーマンスとアベイラビリティの向上に利用できます。チェック・ポイントとOPSECパートナーの技術を組み合わせることにより、OPSECソリューションは、常に第一級のパフォーマンスとアベイラビリティを実現します。

### OPSECによるTCO( Total Cost of Ownership )コストの大幅な削減

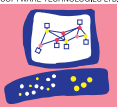
情報セキュリティは、企業が高い競争力と収益性を維持するために欠くことのできないビジネス上の手段になりました。包括的なセキュリティ・インフラストラクチャの導入を成功させるには、統一されたセキュリティ・アーキテクチャで管理される複数ベンダの優れた製品が必要です。

OPSECフレームワークは、企業の投資を保護し、包括的なセキュリティ・インフラストラクチャの導入に必要なTCOを大幅に削減します。最新の優れたソリューションは、インフラストラクチャを根本から変更する必要がなく、低いTCOで新しいハードウェア・ベースのセキュリティ・プラットフォームに統合することができます。ユーザは、製品の旧式化や相互運用性を心配することなく、時間をかけてセキュリティ・インフラストラクチャを構築し、拡張することができます。

包括的セキュリティ・ソリューションの構築についての詳細は、[www.opsec.com](http://www.opsec.com)をご覧ください。



Intelligent Security

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・テクノロジーズは、インターネット・セキュリティ分野において世界をリードする企業で、VPNおよびファイアウォールの世界市場においてマーケット・リーダーとして評価されています。同社のセキュア・バーチャル・ネットワーク(SVN)アーキテクチャは、独自の技術により、安全で信頼性の高いインターネット通信を可能にするVPNおよびセキュリティのインフラストラクチャを提供します。SVNソリューションは、同社の次世代製品ファミリに組み込まれて、企業ネットワーク、リモート社員、ブランチ・オフィス、パートナーを結ぶエクストラネットにおけるビジネス通信とリソースを保護します。SVNの機能を拡張したものがチェック・ポイントのOPSEC(Open Platform for Security)で、業界をリードする350社以上のBest-of-Breedソリューションを統合、相互運用するための業界のフレームワークを提供します。チェック・ポイントのソリューションは、149カ国で認定された2,500社のパートナーによって販売、統合、保守が行われています。詳細については、チェック・ポイントのWebサイト(<http://www.checkpoint.co.jp>または<http://www.opsec.com>)をご覧ください。



**Check Point**<sup>TM</sup>  
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 建成新宿ビル6F  
<http://www.checkpoint.co.jp/> E-mail : [info@checkpoint.co.jp](mailto:info@checkpoint.co.jp) Tel : 03(5367)2500

©2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Point Express, Check Pointのロゴ、ClusterXL、ConnectControl、FireWall-1、FireWall-1 GX、FireWall-1 SecureServer、FireWall-1 XL、FloodGate-1、INSPECT、INSPECT XL、InterSpec、IQ Engine、Open Security Extension、OPSEC、Provider-1、Safe@Office、SecureKnowledge、SecurePlatform、SecureXL、SiteManager-1、SmartCenter、SmartCenter Pro、SmartDashboard、SmartDefense、SmartLSM、SmartMap、SmartUpdate、SmartView、SmartView Monitor、SmartView Reporter、SmartView Status、SmartViewTracker、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、およびVPN-1 VSX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および5,835,726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。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。

P/N 700601-J-1 2004.2



Intelligent Security