



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

# 内部ネットワークで比類なき 強固なセキュリティを実現

Check Point InterSpect



Intelligent Security

チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

# Contents

本書の内容

はじめに	3
内部ネットワーク：保護されたリソース	3
内部ネットワーク特有のセキュリティ課題	4
内部ネットワークのセキュリティに求められる機能	4
内部ネットワークにおいて最適化されていない既存ソリューション	5
パッチ	5
アンチウイルス・ソフトウェア	5
スイッチ・ベースとルータ・ベースのセキュリティ・ソリューション	5
ファイアウォール	6
侵入検知および侵入防御システム	6
Check Point InterSpect：内部ネットワーク固有のセキュリティ課題への対応	6
InterSpectとLANの配備オプション	7
Intelligent Worm Defender	7
ネットワーク・ゾーン・セグメンテーション	8
疑わしいコンピュータの隔離	8
MicrosoftおよびLANプロトコルの包括的な防御機能	9
攻撃に対する事前の保護	9
集中管理	9
エンドポイント・セキュリティ・インテグレーション	11
高いパフォーマンス	11
プラットフォームの選択	11
結論	11

## はじめに

ITセキュリティ管理者は長らくネットワークの境界に対する防御に専念してきました。また、境界のセキュリティに重点を置くことに加え、急増するワームなどの攻撃がモバイルデバイスや無線デバイスによってネットワークの内部に持ち込まれるのを防ぐため、内部ネットワークのセキュリティの必要性を認識しています。境界セキュリティソリューションの構築と運用に使用される基本方針は内部ネットワークにも適用できますが、内部セキュリティはより複雑で、さらに高いパフォーマンスと固有の要件が求められます。このため、既存の境界セキュリティソリューション（パッチ、アンチウイルスソフトウェア、スイッチ、ルータベースのソリューション、従来のファイアウォール、侵入検知および侵入防御システムなど）では、内部システムのセキュリティについては十分とは言えません。

この技術白書では、内部ネットワークのセキュリティ要件について詳しく説明し、既存の境界セキュリティソリューションではこの要件を満たすことができない理由について解説します。また、本書では、Check Point InterSpect™ の実証済みの新技術、手法、アプローチによる、内部ネットワーク固有のセキュリティ課題への対処方法についても解説します。

Check Point InterSpectには、以下のような機能があります。

- Intelligent Worm Defender: ネットワーク内部でのワームや攻撃の拡散を防止します。
- ネットワーク・ゾーン・セグメンテーション機能: 攻撃を隔離してネットワークへの拡散を防止します。
- 疑わしいコンピュータの隔離
- LANプロトコルの包括的な防御機能: アプリケーションの接続を維持しながら内部リソースを攻撃から保護します。
- 攻撃に対する事前の防御: 脆弱性の搾取や侵入者より一歩先を行く防御です。
- 統合管理: 拡張性が高く、容易な管理を提供します。
- エンドポイント・セキュリティ・インテグレーション: ルールを順守するユーザにのみネットワークへのアクセスを許可します。

## 内部ネットワーク: 保護されたリソース

従来、ITセキュリティ企業は、ネットワーク境界のセキュリティ・リソースに重点を置いていました。しかし、強力な境界セキュリティを採用している企業でも、正規に認証を受けたユーザがモバイルデバイスや無線デバイスによってネットワーク内部に持ち込む攻撃により、犠牲になる場合があります。これらの攻撃は、一度ファイアウォール境界の内側に入り込むと、アンチウイルスなど限られた内部制御を簡単にすり抜けることができます。例えば、通常内部ソースによって持ち込まれてからネットワーク・ユーザの間で感染を拡大するBlasterワームは、5億ドル(USD)を超える経済的損失をもたらしました(出展: Computer Economics, Inc.)。これを防ぐため、企業は内部の「バックエンド」環境を直接規制できるようにし、既存の境界セキュリティソリューションを補強する必要があります。

## 内部ネットワーク特有のセキュリティ課題

各企業・組織は、ファイアウォール、認証、侵入検知およびアンチウィルスの各ソリューションを組み合わせ、ネットワーク境界にDMZ(非武装地帯)を構築し、アクセスを制御し、攻撃に対する防御を行っています。同様の機能は内部ネットワークのセキュリティ・ソリューションにも必要ですが、他にも対処すべき問題があります。

内部ネットワークの特徴は、外部ネットワークよりも規模が大きく、複雑な点です。管理者は、ネットワーク境界のセキュリティを確保しながら、複数のシステムと数百メガバイトのトラフィックがあるネットワーク環境で作業しています。これに対して、内部ネットワークには数千のシステムと数ギガバイトのトラフィックがあり、潜在的なセキュリティ・リスクも高くなります。

外部ネットワークのアプリケーション環境には、数十のアプリケーションと関連プロトコルがあります。これらの明確に定義された標準的なアプリケーションは、プロトコルに厳密に従い、クライアント/サーバ構成で実行されます。これに対して、内部ネットワークにはより広範なアプリケーションとプロトコルがあります。内部アプリケーションには独自に開発されたものも多く、プロトコルに厳密に従わず、セキュリティ的な考慮も「強化」されていません。

また、外部ネットワークの管理環境におけるユーザ区分はそれほど多くないため(外部と内部の大別など)、管理者は通常ファイアウォールを設定して未知のトラフィックをブロックします。一方、内部管理環境には、はるかに多くのユーザ・ロールとグループが存在し、ポリシーや管理の設定も大幅に複雑となります。内部ネットワークのトラフィックは自由に流れる必要があり、管理者がトラフィックを分類別にブロックすることは不可能です。内部ネットワークの業務に支障を来さないよう、管理者は攻撃および明らかに不適切なトラフィック以外を除き、すべてのトラフィックを許可しなければなりません。

内部セキュリティを提供するソリューションは、上記の違いを念頭において考慮する必要があります。

## 内部ネットワークのセキュリティに求められる機能

内部ネットワークの要件を満たすため、セキュリティ・ソリューションには以下の機能が必要となります。

- ・ 正規ユーザがネットワークに放出する可能性のある、ワームや複合的な脅威など、一般的で厄介な攻撃に対する防御(これらの攻撃はアプリケーション層で頻発します)。
- ・ ネットワークを分離したセキュリティ・ゾーンにセグメント化し、1つのサブ・ネットワークで発生する攻撃を抑え、企業内のユーザがアクセス権限のないデータに対するアクセスを防御。
- ・ 攻撃を受けたデバイスを切り離すため、疑わしいあるいはパッチ処理を行っていないコンピュータの隔離。
- ・ ネットワーク層およびアプリケーション層から攻撃トラフィックを排除しつつ、基幹アプリケーションの通信を継続。
- ・ 既知および未知の脆弱性および攻撃に対する事前の防御を提供。
- ・ 境界と内部の両方のセキュリティ・ソリューションを簡単に管理でき、拡張性の高い集中管理機能の提供。
- ・ 大規模な企業セキュリティ環境の一環として、簡単な配備の実現。
- ・ ネットワークのコアからデスクトップに至るまでセキュリティ・ポリシーを実施し、攻撃を受けたデバイスから被害が拡大することを防ぐ、エンドポイント・セキュリティ・インテグレーションの提供。
- ・ 内部ネットワークに必要な高いスループットに対応する、優れたパフォーマンスの実現。

## 内部ネットワークにおいて最適化されていない既存ソリューション

パッチ、アンチウイルス・ソフトウェア、スイッチ・ベースとルータ・ベースのソリューション、ファイアウォール、侵入検知と侵入防御のソリューションなど、従来型のセキュリティ製品やアプローチの多くは、内部セキュリティにも適用できます。しかし、これらのソリューションは、内部ネットワーク固有の要件に完全に対応できるよう調整されたものではありません。

### パッチ

内部システムを保護するために用いる一般的な手法として、アプリケーション・パッチのインストールが挙げられます。パッチのインストールは、特定の脆弱性の排除には効果的ですが、内部ネットワークの完全な防御ソリューションとはなり得ません。第一に、パッチはいつでも入手できるわけではありません。この2年間で、脆弱性が最初に発見されてから、この脆弱性を搾取する攻撃が作られるまでの期間が劇的に短くなりました。このため、脆弱性を標的とする攻撃に対して、その回避に間に合うようにパッチを提供できない場合もあります。

さらに、パッチを入手できたとしても、その管理とインストールは大きな負担になります。パッチによっては粗雑な場合も多く、企業は、パッチごとにネットワークで問題が発生しないことを検証するテストを行わなければなりません。パッチ管理プロセスは現在もその場しのぎの手作業で、大規模ネットワークの全システムにパッチをインストールするには、多くの時間とリソースを必要とします。さらに問題を複雑にしているのは、業界の傾向として、ソフトウェア・ベンダが大量のセキュリティ・フィックスとソフトウェア・フィックスをリリースしていることです。この傾向は今後も続き、パッチの数が増えるにつれ、パッチ管理プロセスはさらに手ごわい課題となることが予測されます。

また、脆弱性の原因は設計エラーやコーディング・エラーだけではありません。不完全なセキュリティ・ポリシーの構築など、構成の不備に起因するものもあります。この場合、パッチの適用は意味がありません。

### アンチウイルス・ソフトウェア

アンチウイルス・ソフトウェアは、多くの既知のウイルスからデスクトップやサーバ・マシンを保護する、ユビキタス(いつでもどこでも使用可能)な重要なセキュリティ対策です。しかし、アンチウイルス・ソフトウェアがワームに対する防御として貧困であることはよく知られるところです。アンチウイルス・ソフトウェアはシグネチャ・ベースであるため、まったくの事後対処型であり、新しい未知の脅威を防御することはできません。このような理由から、アンチウイルス・ソフトウェアは既知のウイルスへの感染という迷惑行為を防止する、「迷惑防止」ツールと考えることができます。しかしながら、新たな攻撃によって脆弱性を搾取される前に未然に防御しようとする、アンチウイルスには大きな限界があります。

### スイッチ・ベースとルータ・ベースのセキュリティ・ソリューション

スイッチ・ベースとルータ・ベースのソリューションでは、スイッチやルータを通過するすべてのトラフィックにセキュリティ機能を適用します。このソリューションでは、攻撃を検知すると、侵害されたポートへのアクセスが完全に遮断されます。内部ネットワークにおいて、この対応を受け入れることができません。また、これらのソリューションが攻撃を検知するのはネットワーク・プロトコル層のみであり、アプリケーション層での攻撃は検知できません。内部ネットワークにスイッチおよびルータのセキュリティ・ポリシーを設定することも、管理者が特定のトラフィック種別を明示的に許可する(これは時間がかかるプロセスです)必要があるため、極めて困難です。

## ファイアウォール

企業におけるファイアウォールは主要な境界セキュリティ・アーキテクチャの中心的な役割として利用されています。適切に定義したセキュリティ・ポリシーの実施により、ほとんどの攻撃を撃退できるからです。ファイアウォールは効果的な境界セキュリティを提供しましたが、アプリケーション・プロトコルの検査と攻撃に対する事前の防御の機能の点では、ベンダごとに実装が大きく異なりました。また、ファイアウォールは、通常特に許可されていないトラフィックをすべてブロックするように設計されています。内部ネットワーク環境には多数のアプリケーションとプロトコルがあり、その多くは独自に作成されたものです。このため、境界ファイアウォールを使用して「許可する」内部トラフィックを設定するのは至難の業です。境界ファイアウォールには、内部ネットワーク・セキュリティに不可欠な内部隔離機能もありません。

## 侵入検知および侵入防御システム

侵入検知システム (IDS) は、攻撃を示すパターンと異常性に対してデータを照合し、アプリケーション・レベルの攻撃を検知するよう設計されています。検知後、IDSソリューションは、疑わしい、あるいは異常なトラフィックが検知されたことを告げ、ユーザが介入してそれを解決するのを待ちます。IDSは従来からセキュリティ・ポリシーの微調整やセキュリティ問題発生後の対応に使われてきましたが、事前の防御機能は備えていません。

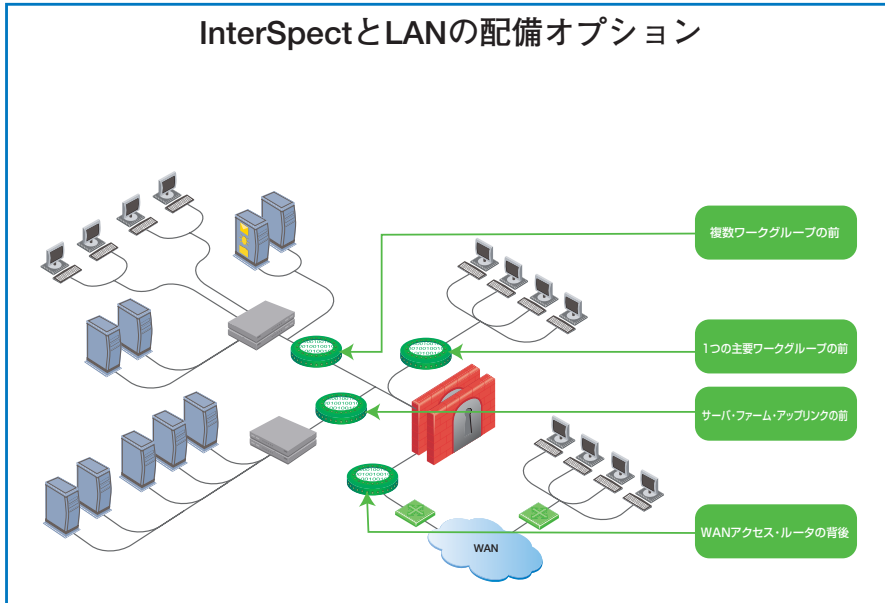
侵入防御システム (IPS) は、主に境界ファイアウォールを補完する技術です。IPSは侵入検知の技術を発展させたもので、同様のシグネチャをベースとして、ネットワークに対する脅威をリアクティブにブロックします。ほとんどのIPSで、エンドポイント・セキュリティ・ソリューションとの統合を実現できません。IPSもシグネチャ・ベースの技術に大きく依存しているため、他のシグネチャ・ベースのソリューションと同様、未知の脅威に対して事前の防御を実施することは困難です。

## Check Point InterSpect :

### 内部ネットワーク固有のセキュリティ課題への対応

先進のセキュリティ管理アーキテクチャおよびインテリジェント・セキュリティ・ソリューションで評価されるチェック・ポイントは、業界初で唯一の完全な内部セキュリティ・ゲートウェイであるInterSpectにより、内部ネットワーク・セキュリティに特有の課題に取り組んでいます。InterSpectは、LANに特化して設計された技術を他の実績ある技術と組み合わせ、以下の機能によりコア (内部) ネットワーク内で多層の攻撃防御を提供します。

- Intelligent Worm Defender: ネットワーク内部でのワームや攻撃の拡散を防止します。
- ネットワーク・ゾーン・セグメンテーション: 管理者が定義したセキュリティ・ゾーンへの攻撃を抑え、従業員の無秩序なアクセスを最小限にします。
- 隔離機能: 攻撃を受けたデバイスを隔離し、パッチ処理を行っていないサーバを切り離します。
- MicrosoftおよびLANプロトコルの包括的な防御機能: ネットワーク内部で使用されるプロトコルとアプリケーションをサポートして、アプリケーションの接続を維持します。
- 攻撃に対する事前の防御: ゲートウェイに既知および未知の脅威に対して事前の防御が可能な機能を備え、搾取される前に脆弱性を防御します。
- 集中管理環境: 内部と境界の両方のセキュリティ・デバイスを管理します。拡張性が高く、操作性のよい管理を提供します。
- エンドポイント・セキュリティ・インテグレーション: ネットワークのコアからデスクトップに至る詳細な防御、およびエンドポイント・セキュリティ・ポリシーを実施します。
- 高いパフォーマンス: ネットワークのスループットに影響を与えません。



## Intelligent Worm Defender

ワームは、現在の内部ネットワークに対する最もユビキタな脅威です。InterSpect Intelligent Worm Defenderは、業界で最もインテリジェントで順応性のあるインスペクション技術であるCheck Point INSPECT™ により、ワームや攻撃の拡散をブロックします。特許取得済みのCheck Point INSPECTエンジンは、ステートフル・インスペクションとApplication Intelligence™ の技術を使用して、InterSpectゲートウェイでセキュリティ・ポリシーを実施します。InterSpectはアプリケーション層全体を検査し、ネットワーク構成、セキュリティ・ルール、通信とアプリケーションの状態に関する累積データをもとに、通信試行を評価します。InterSpectはLANベースとWindowsベースのアプリケーションのネットワークにおける使用法を理解した上で、ネットワーク・トラフィックがプロトコル標準と想定使用方法を順守することを確証します。また、他のソリューションが接続性とセキュリティのどちらかを犠牲にせざるを得ない中、InterSpectではMicrosoftアプリケーションを安全に使用できます。例えば、BlasterワームがMS-RPCプロトコルを搾取しても、InterSpectは危険性のないRPC接続を許可し、しかも悪意のあるRPC接続はブロックすることができます。

InterSpectゲートウェイはネットワークに流入する段階でトラフィックを監視するため、他の技術では検知や抑止が不可能な、急速に拡散するワームを捕獲することもできます。例えば、アンチウイルス・ソフトウェアは、悪意のあるファイルが自身をディスクに書き込もうとした場合のみ、システムを防御することができます。SQL Slammerはディスクに書き込まれない1つのパケットであるため、アンチウイルス・ソフトはこの種の攻撃の防御には役立ちません。IDSソリューションはSQL Slammerを認識できますが、ユーザの介入が求められるため、防御に間に合うよう迅速に対処できません。

## ネットワーク・ゾーン・セグメンテーション

内部ネットワークには数千の個々のシステムが存在することがあります。InterSpectは、インフラストラクチャのさまざまなポイントに配備して、ネットワークを複数のセキュリティ・ゾーンにセグメント化することができます。ゾーンは物理的・仮想的セグメントで定義し、ゾーン間のアクセスや通信を制御できます。InterSpectはネットワーク全体で必要なトラフィック・フローを確保しながら、セグメント間の不正使用(故意または過失による)を防ぎます。

最も広範なネットワーク・トポロジの要件を満たすため、InterSpectは、VLANベースの仮想ネットワークをサポートし、既存のVLANセグメンテーションに対する投資を有効に活用することができます。このため、ネットワークのコアに近い場所で、より柔軟な配備が可能です。仮想ゾーンにより、InterSpectは地理的に離れたゾーンも多数防御できます。防御ゾーンごとに固有のセキュリティ・ポリシーを適用し、1つの装置で数千のセグメントを保護することが可能です。企業は物理的・仮想的なゾーン・セグメントを設定し、ゾーン・ベースのセキュリティ・ポリシーを実施して、組織別または部門別のセキュリティ・ゾーンを実現できます。

## 疑わしいコンピュータの隔離

InterSpectの隔離機能により疑わしいシステムを切り離し、攻撃を抑止できます。攻撃の被害を受けた時点でそのコンピュータを自動的に切り離すように隔離機能を設定し、他のシステムへの感染を防ぐことができます。ネットワーク管理者はこの隔離機能を使用してサーバを切り離し、パッチ処理前、および処理中のリスクを軽減できます。以下の例でこの2つの隔離シナリオについて説明します。

### シナリオ1：InterSpectによる疑わしいコンピュータの隔離

1. InterSpectは、ネットワークを個別のセキュリティ・ゾーンにセグメント化します。
2. InterSpectはセキュリティ・ゾーンの中から疑わしい、または、感染したコンピュータを特定します。
3. そして、ネットワークから疑わしい、または感染したコンピュータを切り離し、他のゾーンのコンピュータへの感染を防ぎます。

### シナリオ2：InterSpectによるパッチ処理前のコンピュータの隔離

1. InterSpectは、ネットワークを個別のセキュリティ・ゾーンにセグメント化します。
2. 管理者はパッチ処理されていないサーバ・グループを特定します。
3. 管理者はパッチ処理されていないサーバに対する隔離を設定します。
4. 管理者は隔離されたサーバをパッチ処理し、その間も、InterSpectはネットワークの他のサーバを確実に保護します。

システムが隔離された場合、InterSpect固有の通知機能により、隔離されたユーザに通知メッセージを送信します。隔離されたユーザがテクニカル・サポートに電話をかけて接続性の問題をトラブルシューティングする必要がないため、InterSpectゲートウェイの総所有コストを削減できます。また、InterSpectは煩雑な管理を避ける1つの方法として、隔離を一方向としています。つまり、隔離マシンは発信できませんが、着信はできます。一方向の隔離では、疑わしいコンピュータから発信して他のコンピュータに感染が拡大するのを防ぎながら、リモート操作で駆除を行ったりパッチを受信させることができます。

## MicrosoftおよびLANプロトコルの包括的な防御機能

内部ネットワークでは、境界ネットワークより多くの、そして異なるプロトコルを使用しています。内部ネットワーク・セキュリティ製品を活用し、攻撃のトラフィックをブロックして他のトラフィックを流すためには、MicrosoftおよびLANプロトコルに対する詳細な知識が必要です。InterSpectは、チェック・ポイントのApplication Intelligenceおよびステートフル・インスペクションを使用して、MicrosoftおよびLANプロトコルに対する業界で最も詳細で包括的なサポートを提供します。サポート対象のプロトコルには、Microsoft RPC、CIFS、MS SQL、DCOM、DCE RPC、HTTPなどがあります。

## 攻撃に対する事前の保護

損害をもたらす攻撃は、既知や未知の脆弱性を利用します。現在の市場におけるほとんどのセキュリティ・ソリューションは、既知の脆弱性に対する保護しか提供できません。しかし、チェック・ポイントは、プロトコルの使用や誤用に関する深い理解に基づく製品を提供し、セキュリティに対するプロアクティブ（事前予防型）なアプローチによって、既知および未知の脅威を防御します。

Check Point InterSpectはステートフル・インスペクションとApplication Intelligenceを組み合わせ、積極的に既知および未知の攻撃から内部ネットワークを防御します。新型の脅威が続々と出現していることから、チェック・ポイントは脆弱性に関するフォーラムを監視し、アプリケーション・ソフトウェア・ベンダと共同して、脆弱性を特定し、それが搾取される前に適切な防御策を開発しています。脆弱性の発見前に防護策を開発することもあります。

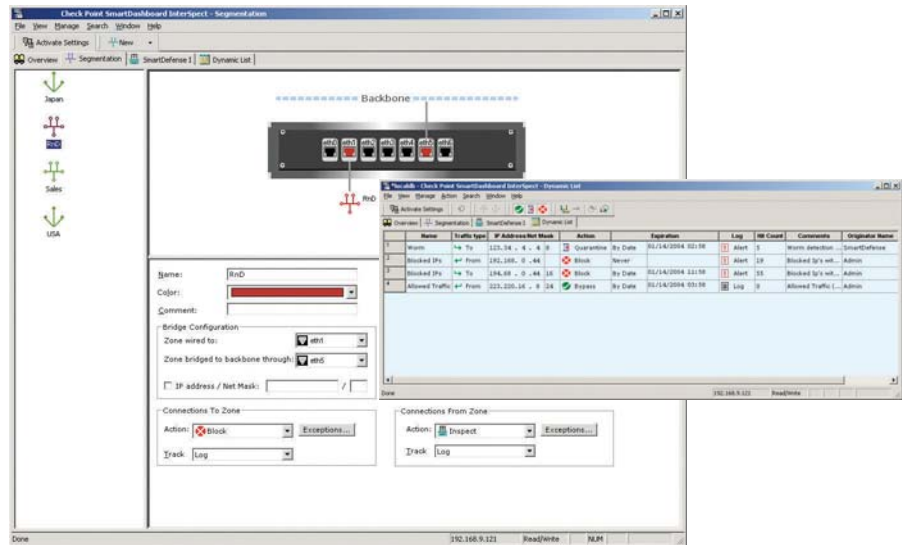
チェック・ポイントは、開発の結果を反映させて、SmartDefense™ のサブスクリプション・サービスによって、設定済み防御のアップデートを提供し、多くの効果を発揮してきました。チェック・ポイントは、HTTP 1.1、SIP、CIFSおよびDCE RPCの新しい、または潜在的な脆弱性が公開される前にこれに対する防御策を提供しました。また、多くの場合、脆弱性が発見される前に防御策を提供してきました。

## 集中管理

InterSpectは、SmartCentersおよびProvider-1 / SiteManager-1™ の技術を備えたCheck Point Security Management Architecture (SMART) をベースとした集中管理を行い、管理の簡素化と生産性の向上を実現できます。

シームレスな管理機能がInterSpectの継続的配備パラダイムに統合され、既存のネットワーク環境のほぼすべてで、簡単に配備し、管理することができます。InterSpectを継続的に配備するための機能には以下のものがあります。

- 複数の直列配備モード（ブリッジ、スイッチ、または、ルータ）：詳細については以下で説明します。
- Monitor-only機能：トラフィックをブロックせずにインラインで配備します。この機能により、システム管理者は製品を直列で「テスト」し、捕獲すべき悪意のある、または望ましくないコンテンツを決定できます。ただし、実際にはブロックしません。Monitor-only機能を有効にすると、ログとレポートが生成され、システム管理者は防御機能を適切に微調整できます。管理者が防御しやすければ、monitor-only機能からfully activeモードに切り替えます。monitor-only機能は、防御の種類別に設定できます（例えば、ある防御にmonitor-onlyモードを設定し、他の防御にfully activeモードを設定するなど）。
- 例外リスト：特定のトラフィックまたは通信を常に許可、また常にブロックするよう設定できます。



InterSpec管理インターフェースは内部セキュリティに特化され、ネットワーク・ゾーンのセグメント化と例外ポリシーの設定に使用する簡単かつ強力なインターフェースを提供します。

企業が最良の方法でネットワークにゲートウェイを配備できるように、InterSpecはブリッジ・モード、スイッチ・モード、ルータ・モードのいずれかのモードの配備が可能です。

ブリッジ・モードは内部ネットワークを防御ゾーンに分割して保護します。InterSpecは、2つのスイッチ間のトランク・リンクにおいてブリッジ・モードで稼働し、1つの物理リンクでの複数のVLANを実現します。各ゾーンは1つまたは複数のイーサネット・セグメントをバックボーンにブリッジします。これは、IPネットワークからは見えません。仮想ゾーンは一意的VLAN IDによって認識され、ゾーンに属するパケットはこれに従ってInterSpecで処理されます。ブリッジ・モードでは、企業は簡単に迅速なセグメント化、継続的な配備、従来のファイアウォールのアプリケーション層の防御を実現できます。

スイッチ・モードはInterSpecのデフォルト設定です。この設定で、InterSpecからネットワーク・スイッチを切り替えることができます。スイッチ・モードでは、InterSpecは、すべてのポートをリンクして1つのゾーンにまとめる、マルチ・ポート・スイッチの役割を果たします。企業はゾーンの設定などを一切行う必要がありません。完全なセグメント化が不要な場合、すべてのネットワーク・セグメントにワームに対する防御機能、および隔離機能を透過的に配備するため、スイッチ・モードを使用できます。

ルータ・モードでは、InterSpecを使用してルータを切り替えることができます。切り替え前のルータと同じIPアドレスを使用して、各アクティブ・ポートを設定できます。ルータ・モードには、VLAN IDで定義された仮想ゾーンを含む複数のセキュリティ・ゾーンを実現する、高度なネットワーク・ゾーン・セグメンテーション機能があります。これで物理的な配線をなくし、ネットワーク・ギアの必要性を最小限に抑えます。

## エンドポイント・セキュリティ・インテグレーション

InterSpecはコア・ネットワークに強固なセキュリティを提供していますが、境界およびコア・ネットワークを超えて詳細な防御にまで高めるには、デスクトップすなわちエンドポイントにまでセキュリティを拡大する必要があります。保護されたネットワークを出入りするラップトップなどの「ルーージュ・デバイス」は、内部ネットワーク全体に対する直接的な脅威です。このような場合、配備されている境界セキュリティとまったく関係なく、感染したデバイスが直接LAN

に接続され、ネットワーク全体に攻撃を拡散させる危険性があります。チェック・ポイントのプロアクティブなエンドポイント・セキュリティ・ソリューションであるIntegrityを配備すれば、セキュリティにさらなる防御層が提供されます。さらに、Cooperative Enforcement™により、InterSpectはCheck Point Integrity™と連携して、ネットワークに接続するすべてのデスクトップとラップトップを防御します。また、Cooperative Enforcementにより、IntegrityはVPNの数百の（VPNからスイッチ、無線アクセス・ポイントに至るまでの）ネットワーク・ゲートウェイ製品との連携が可能になります。

LANだけでなく、ネットワークに接続する有線・無線のデスクトップおよびラップトップに至るまで強化されたセキュリティを提供する、トータル・アクセス・プロテクションを実現できるのはInterSpectとIntegrityだけです。

## 高いパフォーマンス

内部ネットワークは、外部ネットワークよりもトラフィック量が多いため、より高いパフォーマンスのあるセキュリティ・ゲートウェイを必要とします。InterSpectは、内部ネットワークでの使用で高いパフォーマンスを発揮します。InterSpectのINSPECTエンジンはシステム・カーネル内で動作するため、ゲートウェイのオーバーヘッドはごくわずかです。コンテキストの切り替えも必要なく、低レイテンシでの運用を実現します。また、InterSpectにはSecureXL™が装備されています。これは、集中したセキュリティ操作の負荷をサード・パーティのハードウェアや最適化されたソフトウェアに分散させる、オープン・インタフェースです。これにより、InterSpectは内部ネットワークのスループットに影響を与えない、ギガビット級のパフォーマンス・レベルを提供します。

## プラットフォームの選択

Check Point InterSpectアプライアンスの製品ラインのほか、Check PointとCrossbeam Systemsが提携し、Crossbeam X-Seriesセキュリティ・スイッチに搭載されたInterSpectを提供しています。その結果、費用効率のよい、安定したセグメント化機能と隔離機能を提供できるようになりました。これは、99.999%の可用性と最高8ギガビットのパフォーマンスを備えています。InterSpect-on-Xソリューションは、コア、ディストリビューション、アクセス層でシームレスに統合する1つのハードウェア・デバイスを提供します。ポート数が多いため、多数の個別ネットワーク・セグメントを保護できます。また、ブリッジ・モードとスイッチ・モードのいずれかで運用できます。InterSpect-on-Xは、内部ネットワークの防御に、最高の拡張性と最高の可用性を提供するソリューションです。

## 結論

境界防御向けに設計されたセキュリティ製品とは異なり、Check Point InterSpectは内部ネットワーク固有のさまざまな課題に対応する、実証済みのセキュリティ技術を使用しています。Intelligent Worm Defenderは、最も一般的で被害の大きい内部攻撃を防御します。隔離機能とネットワーク・ゾーン・セグメンテーション機能は、多層の攻撃防御とセキュリティ・セグメントを提供します。LANプロトコルの包括的な防御機能は、通常のLAN通信を妨げずに、アプリケーション層の攻撃を防御します。攻撃に対する事前の保護機能は、ソリューションを侵入者より一歩先に進ませることができます。InterSpectとIntegrity間のCooperative Enforcementは、より精度が高く、より安全に保護された内部セキュリティ環境を提供します。これらの機能とともに、InterSpectは内部ネットワークに必要な高いスループットと内部ネットワーク固有の問題に対応する管理機能を提供しています。また、すべてのネットワーク・セキュリティ・システムに対する集中管理機能を提供しています。これらすべての機能を合わせて、現時点で最も包括的な内部ネットワークの防御と機能を実現し、内部セキュリティ配備にかかる総所有コストは低く抑えることができます。

## 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。本書に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。

Providing Unparalleled Security for Internal Networks Check Point InterSpect

P/N:501695-J 2005.6

※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 建ビル6F  
http://www.checkpoint.co.jp/ E-mail: info\_jp@checkpoint.com Tel: 03(5367)2500